Volume 6

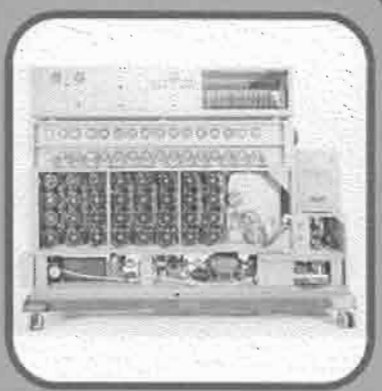
National Security Agency
Central Security Service

CCH-E05-02-01

It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s – 1960s





Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

~~TOP SECRET//COMINT//X1~~

Cover Photos: (U) (clockwise from upper left): Hypo, Vannevar Bush, Harvest, Joseph Desch, Gee Whizzer, Stanford Hooper, Bombe, Samuel Snyder

DOCID: 4057009

UNITED STATES CRYPTOLOGIC HISTORY

Special Series
Volume 6

It Wasn't All Magic:

The Early Struggle to Automate Cryptanalysis, 1930s - 1960s

Colin B. Burke

CENTER FOR CRYPTOLOGIC HISTORY

NATIONAL SECURITY AGENCY

2002

This page intentionally left blank

CONTENTS

P.L. 86-36

This page intentionally left blank

Foreword

(U) Conventional wisdom about NSA and computers has it, as a retired NSA senior officer once wrote me, "In the early days, NSA and its predecessor organizations drove the computer industry. In the 1960s, we kept pace with it. We started losing ground in the '70s, and in the '80s we struggled to keep up with the industry."

(U) True, but underlying this, in each decade the cryptologic organizations experienced a wide range of successes and failures, positives and negatives. If, as slang puts it, "they won some, lost some, and some got rained out," all of this experience is worth serious examination by students of computers, cryptanalysis, and NSA history.

(U) The current volume, Dr. Colin Burke's *It Wasn't All Magic: The Early Struggle to Automate Cryptanalysis, 1930s-1960s,* contains a view of the first decades of computer development that is broad and deep and rich.

(U) It begins in the 1930s as American and British intelligence officials confronted new cryptanalytic and cryptographic challenges, and adapted some intriguing new concepts to their analysis. It carries the story to the flexible and fast systems of the late 1950s and early 1960s.

(U) Dr. Burke follows and links the development of automatic data processing from the critical conceptual work of the 1930s through the practical experiments born of national necessity in the world war to the postwar development and the previously untold story of NSA's postwar computer development. Along the way, he has rescued from obscurity some important successes – and some important failures – in cryptanalytic machinery from World War II.

(U) All too often, discussions of NSA's computer development treat only the mainstream, ignoring the problems, failures, dead ends and might-have-beens, in order to concentrate on successes. In the present volume, however, key components of Dr. Burke's story and important for our knowledge are the machines which didn't work or which never had progeny, and why this was so. Just as important are Dr. Burke's cautionary tales about the influence of international and interservice rivalry on plans and procedures. Technical limitations and technical opportunities shaped much of the development of computing equipment, but the story is also replete with instances of man-made barriers and baleful bureaucratic bypaths that wielded great influence during much of this development.

(U) A word about how this manuscript came to be.

(U) A no less important factor than the information and analysis in this current volume is that it represents an objective view of NSA's computer history by a writer not from NSA or one of the Service Cryptologic Elements. The author, a university professor, had no stake in either defending or besmirching decisions made fifty years ago or the organizations or people who made them.

(U) The Center for Cryptologic History, between 1990 and 1999, administered a program to bring outside academics or researchers to the CCH for special projects. The CCH sponsored six Scholars in Residence in that period; of the six, the first two received security clearances for work on classified projects. The others remained uncleared and worked only with declassified materials.

(U//~~FOUO~~) Dr. Colin B. Burke was the second of the two cleared scholars.

(U//~~FOUO~~) Dr. Burke's professional biography is given at the end of the book. Note that as a professor of both history and computer research techniques, Dr. Burke became one of the pioneers in the field of computer history.

(U//~~FOUO~~) As background reading, I recommend not only Dr. Burke's own unclassified publications, available commercially, but two classified histories available from the Center for Cryptologic History: Thomas R. Johnson, *American Cryptology during the Cold War* (4 vols) and Michael L. Peterson, *BOURBON to Black Friday*.

DAVID A. HATCH
Director,
Center for Cryptologic History

(U) Introduction

(U) Before NSA Opened Its Files

(U) I am one of those "outsiders" I talk about so much in the later chapters of this book. I was fortunate to be brought into the National Security Agency as one of the Center for Cryptologic History's first Scholars in Residence. I was borrowed from my university because I had spent a decade working on the history of computers at NSA's predecessors. I even had the courage to write a book about the subject.[1]

(U) That monograph was on the machines, policies, and relationships that led to the U.S. Navy's cryptanalytic machine (computer) program in World War II. The book was also about the first major attempts to automate the American library. It had to be about both because the same people built bibliographic and cryptanalytic machines.

(U) My study covered events in the history of the machines through the 1940s, but its focus was on the period between 1930 and 1945. An important conclusion was that the relationship between the efforts of America's codebreakers and the emergence of the modern digital electronic computer was more complex than had been thought. The navy's cryptanalysts were in a push-me, pull-me situation. Their work made mechanization a necessity, but the pressures of war and the refusal of the government bureaucracy to sponsor long-term research and development programs prevented the navy from becoming the inventor of the modern computer.

(U) During World War II American cryptanalysts built some of the most sophisticated electronic machines in the world, but the need to address cryptanalytic crises blocked them from creating the general-purpose digital electronic computer.

(U) Just as my book was published, I was asked to come to the National Security Agency. One purpose of my year in residence was to see if it was possible to write a complete history of computers at the Agency. The goal was a monograph that covered the entire life of NSA and its predecessors. The thought of finally being able to see the many highly classified documents that had been withheld from me more than balanced the pledge I had to give: I had to promise to refrain from publishing without the approval of NSA's censors.

(U) The Stacks Were Not All They...

(U) I began my residency by surveying the Agency's archive holdings and by rereading the few synthetic works that had been declassified. The comprehensiveness of the archive holdings was critical because unless enough of the correct type of documents had been saved and indexed, there was little chance to produce a history of the post-World War II era. Useful documents from the 1950s through the 1980s were of special importance because the Agency had allowed almost nothing about its operations in the last forty years to be made public. There was not even a counterpart to the informative but very unhandy collection of documents on the pre-1946 period released to the National Archives, the Special Research History series.

(U) As I examined the collections, I was pleased to find that the materials I needed to

~~Derived From: NSA/CSSM 123-2~~
~~Dated 24 February 1998~~
~~Declassify On: X1~~

revise my earlier work were plentiful and well organized. There were several contemporary studies of computer efforts up to 1945 that were technically as well as historically enlightening.

(U) I was also happy to discover that although I had not been correct in all the details about the early American cryptanalytic machines, I had come quite close. I concluded that I had drawn an acceptable overview of the computer efforts of the army and navy cryptologic agencies up to 1950.

(U) But I was less than content with the materials for the postwar era. I decided that it would be impossible to tell the type of story about the forty-five years since the Korean War that I had done for the earlier period, at least not within one year.

(U) However, there were many documents, several oral histories, and the work of Samuel S. Snyder to provide a basis for a history of computers within NSA up to the early 1960s.

(U) Ask What the Agency Did for...

(U) Samuel Snyder was one of the founding fathers of machine cryptanalysis. He joined the army's cryptologic unit in the 1930s and remained at the Agency, becoming important to many of its computer projects of the 1940s and 1950s. His experience, his desire to document the Agency's computer history, and his commitment to the welfare of NSA, made its administrators receptive to his requests to be allowed the time and resources during the late 1960s and early 1970s to write about the Agency's computer history.

(U) Mr. Snyder completed several works. They ranged from sketches of the history of the army's first electronic computer, Abner, to a survey of the general-purpose electronic computers the Agency had built or purchased. The study of the "gp" computers seemed so important and fit so well with the Agency's desire to obtain good publicity that it was declassified and, in various forms, published in the open literature.[2]

(U) Mr. Snyder's work showed the contributions of NSA to the development of computer technology and to the emergence of the American computer industry. It made it clear that NSA had been a major sponsor of technical advances. Like several other large government agencies, its computer purchases and its research and development contracts helped establish America as the world's leading computer manufacturer. He also made it clear that NSA had been at the cutting edge of computer technology and architecture.

(U) I was very tempted to just deepen Sam Snyder's work on post-1950 automation, but as I went through the hundreds of record boxes at the archives and as I began to reflect on their contents, I decided that I had to do something different. I had to take an alternative view of the Agency's computer history.

(U) Because of the need to guard NSA's cryptanalytic methods, Mr. Snyder could not discuss the reasons for the development of the devices he included in his published works. Just as the Agency cannot reveal its cryptologic successes without endangering them, Snyder could not give either the "why" or, in many cases, the "what" of the Agency computers to the public. The jobs the NSA computers had to perform and the decision processes that led them to be part of the famous collection of machines that once resided in the Agency's "basement" had to be left out of his studies.

(U) He certainly could not discuss what were and are the most intriguing machines at NSA, its dozens of special-purpose computers, ones whose architecture embodies a cryptanalytic process. Doing more than listing their cover names would have revealed what methods the Agency was using and what targets it was attacking. Neither the NSA nor the British intelligence agencies were responsible for the initial release of information

about MAGIC and ULTRA. The stories were told by others.

(U) The restrictions on Mr. Snyder had another influence. Because he was forced to divorce SIGINT and computer history, the machines he described seemed to have emerged as a result of an indestructible synergy between the Agency, the computer industry, and America's scientific community.

(U) My knowledge of the course of technological advancement in the cryptologic arena in the 1930s and 1940s led me to doubt that the postwar era's machine history was so smooth and problem free.

(U) There was something more fundamental about Mr. Snyder's approach that led me to search for alternative ways to interpret the documents that were emerging from the NSA archives and the offices of old hands at the Agency. Although Snyder's articles are invaluable, his interpretation seemed unlikely to be able to bring together the policy, the cryptanalytic, and technological histories of SIGINT computerization.

(U) The emphasis in his public articles was on what the Agency's computer efforts did for others, especially the computer industry. But I had a clear sense that I could tell the story of computers only by using an approach that was the near opposite of Sam Snyder's. Focusing on NSA's role in transferring technology and supporting commercial computer development, I concluded, hid as much or more than it revealed.

(U) Ask Not What the Agency Can Do for...

(U) To understand computerization at NSA, the question should not be "what did NSA do for the computer industry?" but "what was it that the industry could not or would not do for NSA?"

(U) The second question leads an investigator into the many technical, institutional, and political struggles that the Agency faced as it attempted to keep up with the cryptologic capabilities of its adversaries. It helps to explain why NSA has had to build so many special computers, why it invested in several technological misadventures, and why it had to involve itself in some unusual relationships with private industry and academia. The question also helps to integrate the political history of NSA with its drive to advance mathematical cryptanalysis.

(U//FOUO) For example, using the "couldn't do" approach to Agency projects led me to an understanding of NSA's great computer adventure, the Harvest system. It also helped uncover the Agency's reason for creating its high-powered mathematical think tank at Princeton. Both the computer and the institution were the result of much more than a desire to extend the reach of formal cryptanalysis; they were born of intense political pressures on the Agency, and they were grand compromises rather than perfect solutions to abstract problems.

(U) Spotlighting what the computer industry could not do for signals intelligence also helps to integrate the Agency's computer and cryptanalytic histories. Putting them together shows that inventing and developing an effective technology for SIGINT has been difficult and, at times, agonizing.

(~~TS//SI//REL~~) The "couldn't do" question also illuminates one of the most fascinating aspects of the history of computers at the National Security Agency: the drive to define and implement a computer architecture that was radically different from the classic design that is now called the von Neumann architecture. Since at least 1946, American cryptanalysts have done much more than use parallel and pipeline processing; they have sought, and came close to achieving, a unique architecture for a cryptanalytic general-purpose computer. Because the computer industry was unwilling to develop machines that served only one customer, NSA was forced to

design and build not only single-purpose machines but its own versions of a general-purpose computer. Its Sled and Dervish family of high-speed devices reflects the Agency's special needs and challenges. Unfortunately, creating an all-purpose special NSA computer was too much for the Agency, given its resources. Its famed Harvest computer, for example, was only a partial representation of a true "cryptanalytic" computer, partially because the computer industry could not focus on Agency needs.

(U) When the "couldn't do" question is extended to American universities, it becomes easier to understand the difficult relationship between NSA and "outside" scientists and their institutions. Finding and utilizing academic talent was very difficult for the Agency. Professors did not rush to NSA before or after World War II, and they did not pursue much research that was of direct help to operational cryptanalysis. Devising ways to preserve the Agency's secrets and its independence while channeling the contributions of academics proved to be very difficult.

(U) Inspiration and Patience

(U) Something besides the relationships with the commercial computer industry and academia has to be called on to explain NSA's computer history. To show why the Agency created its own computer architecture and why it accepted some technological retrogressions calls for a bit of cryptanalytic muckraking. The craft of code and cipher breaking has to be stripped of its romanticism.

(U) The stories of the successful American attack on Japan's diplomatic ciphers before World War II (PURPLE-MAGIC) and the triumph over the German ENIGMA-ULTRA are used as popular models for the way cryptanalytic work proceeds. The popular view shares much, in terms of fundamentals, with the public view of Agency computer development.

(U) In the typical story, codebreaking successes such as MAGIC and ULTRA came about because of the quick and intense work of a handful of geniuses armed with brain power and little else. The common image is that once the likes of William F. Friedman and Alan Turing had their flashes of insight, a flow of precious information (and only valuable information) was captured, processed by a hastily constructed but ingenious machine, and then directed to decision makers.

(U) Such an image of a heroic cryptanalysis is far from being true or useful. Cryptanalytic and technological victories have not come as easily as that. Even during the glorious codebreaking days of World War II, America's cryptanalysts barely kept up with their enemies.

(U) There have been moments when great breakthroughs have led to critically important messages. And the penetration of some systems, such as the U-boat "E," led to a stream of immediately important information. But typical cryptanalysis was and remains a continuing struggle to discover patterns and to make sense out of mountains of raw data.

(U) Most cryptanalytic solutions have come only after years of the most tedious and disdainful work. The intellectuals that Britain gathered at Bletchley Park had to perform mind-deadening menial computing tasks hoping that all their labor would reveal mistakes by the German cryptographers and patterns within message texts. They had no magical mathematical formula that eliminated the need for massive data processing. Even when a system was penetrated, creating useful information from intercepts called for large-scale data handling.

~~(S//SI)~~ During the first decades of the Cold War, when America's enemies made the ENIGMA systems seem like cryptanalytic child's play, NSA could not re-create a MAGIC. It had to wring information out of traffic analysis, plain text, and even clear voice messages. That forced the Agency

to become one of the world's largest data processors.

(U) On top of the special computing needs of cryptanalysis, NSA's insatiable need for what many times was unique data processing equipment, made it a computer leader.

(U) The National Security Agency has not been such an important influence in computer development because of its mathematical wizardry or because it has a mandate to transfer technology to the private sector. The Agency's contributions have come because of the unique nature of cryptanalysis and SIGINT and the increasing difficulty of fulfilling a central responsibility: the production of signals intelligence. The Agency has sponsored supercomputers for mathematics since the 1940s, but so have many others. The critical contributions of the Agency have come because of the special needs of operational cryptanalysis and SIGINT data processing.

(U) There Wasn't Enough Magic

(U) In addition to the "couldn't do" perspective, a useful way to understand the history of NSA's computers is to place them within the context of the struggles to overcome the particular machines and methods of America's determined and increasingly clever opponents.

~~(U//FOUO)~~ The National Security Agency has never bought or built computers for abstract reasons. Its computers, even those for its hush-hush think tank at Princeton, were acquired to respond to very practical and immediate needs and opportunities. From the early 1930s, when the first IBM tabulating machines were brought into the secret rooms of the Navy's OP-20-G, to NSA's massive computer projects of the 1950s, and to the 1990s when the NSA computer building is filled with massively parallel and pipe-lined special-purpose computers, the Agency's machines have been for the solution of problems. There have been moments when the Agency has been allowed a bit of a luxury to pursue long-term and general technological explorations, but they have been rare and were always under the threat posed by a shift in national, political, or military policy.

(U) Despite all that, NSA has arguably been the largest single user of advanced computing machines in the world. It had to be. And because of the unique problems it faced and methods it used, it also became one of the most sophisticated sponsors of new computer and electronic equipment. To do its job it had to invest hundreds of millions of dollars into research and development.

(U) A Story with Only a Few Acronyms

(U) The story of the Agency's struggle for automation from 1930 to the beginning of the 1960s could become an exercise in the use of acronyms. NSA and its predecessors were bureaucracies with dozens of subdivisions and name changes. The designation for the army's crypto branch, for example, was altered several times before the end of World War II. Following such changes is too much to ask of a reader who wishes to gain the "big picture" of cryptanalytic computer history.

(U) To keep the text readable, I decided to use as few names as possible for agencies and their subdivisions. For example, the army's cryptanalytic branch is called the SIS until the formation of NSA.

(U) I have also kept the goal of readability in mind when describing machines and processes. I have tried to use common terms whenever possible, even at the cost of glossing over some technical distinctions. I have even used the terms SIGINT and COMINT interchangeably, except in the contexts in which the differences between the two are significant to understanding NSA's history.

(U) Two Decades before the Computer

(U) I have also tried to use consistent terminology, although the story of the struggle to automate American cryptanalysis begins two decades before the modern electronic digital computer emerged. NSA's automation story begins in 1930 when a bright and devoted navy man, Stanford Caldwell Hooper, realized that mechanized cipher-making was outpacing cryptanalysis. In his attempt to modernize the navy's cryptanalytic branch, OP-20-G, he engaged a problem that proved difficult for America's codebreakers for over a generation: How can a secret agency find and use the best talents and technology in the outside world? Hooper tried to solve that problem by creating a new type of relationship with academics, specifically the man who became the czar of America's new Big Science of World War II and the first years of the Cold War – Vannevar Bush of MIT.

Colin Burke
December 1994

(U) Notes

1. (U) Colin B. Burke, *Information and Secrecy: Vannevar Bush, Ultra, and the Other Memex,* Metuchen, NJ, & London: The Scarecrow Press, 1994.

2. (U) For example, Samuel S. Snyder, "Computer Advances Pioneered by Cryptologic Organizations," *Annals of the History of Computing* , 2 (1980): 61.

Chapter 1

(U) An Academic in Need of the Navy ... Until

(U) America's communications intelligence services were even more dependent on outsiders during the 1930s than they were during the Cold War. Neither the army nor the navy had enough resources to be technological innovators. They could not afford their own research and development programs, and they did not have enough money to tempt the scientific and industrial sector into concentrating on the cause of advanced military technology. All the army and navy branches suffered, but those whose functions were not highly valued by the military found innovation far beyond their reach. Communications intelligence was among the disinherited.

(U) When it appeared that technology was about to outrun the established cryptanalytic methods, the American army and navy's communications intelligence services had to find ways to compensate for their inadequate budgets and the absence of relevant research and development departments within the military.

(U) The navy was the first to try to muster new technologies to conquer advances in code and cipher systems. As early as 1930, one of its more progressive leaders, Stanford Hooper, sought ways to overcome the financial and organizational constraints on innovation in cryptanalysis. The barriers were so great that Hooper could not take a direct route to the creation or even the acquisition of modern calculating and data processing instruments. He did not have the funds to underwrite an independent development project within the navy or within the leading corporations. He had to do the best he could with what help could be obtained and do it without obligating the navy to any major financial or institutional burdens.

(U) Hooper's odyssey led him to all those he thought might be willing to give the navy help without asking too much in return. Among the many contacts he made during the 1930s, one was of special importance to the history of computers and the cryptanalytic rapid analytical machines (RAM). Hooper was able to make an arrangement with Vannevar Bush of the Massachusetts Institute of Technology.

(U) To understand the complex, near byzantine histories of the development of computers for cryptanalysis, especially the path-breaking RAM program, and to appreciate the difficulties of linking science and codebreaking, the biography of one of the leading high-tech universities is required. As well, the life of one of the most important figures in the history of applied science, Vannevar Bush, needs to be sketched. Of special importance is the work Bush had begun for other purposes. His attempts to build innovative machines for scientific calculation and for data retrieval determined what technologies he recommended as the basis for the first modern cryptanalytic machines.

(U) An Institution for the Real World

(U) Since its birth on the eve of the Civil War, the Massachusetts Institute of Technology had been devoted to applying science to practical affairs. Its founders rejected much of the curricula of the traditional American liberal arts college as well as the simple vocational program of the trade school. They made MIT an example of how practical men who worked in cooperation with the new institutions of science and industry could turn a university into a force for positive change. Its founders, such as William Barton Rogers, wanted to create men of vision, men who would bring the benefits of technology to a backward

America. Rogers and his colleagues were the builders of some of the most important instruments of the American industrial revolution. Their famous Comparator, for example, allowed the exact replication of mass-produced parts.[1] The name "Comparator" was probably selected for Bush's 1930s cryptanalytic machine because of the earlier MIT device created by the Institute's founders.

(U) Rogers initiated MIT's long-term policy of conducting research for business and government agencies and of having its faculty actively engaged in technological and business efforts. MIT was badly hit by the recession of the 1870s, and its future remained unsure until the watershed years of American life in the 1890s. Then, with a more secure financial condition and a growing body of alumni and friends who had benefited from the work of its faculty, the Institute expanded its curricula, acquired modern equipment, and established itself as a force in American academic and industrial life. The Institute gained a solid reputation in civil and mechanical engineering, architecture, naval construction, chemistry, and electrical engineering. By the 1920s the sparkling electrical engineering department added a focus on the new fields of electronics and communications. The inauguration of Samuel W. Stratton as MIT's president in 1923 accelerated the shift to electronics and reinvigorated the school's attempts to create measurement devices for industry and science. Stratton's background and interests blended with those of MIT. Stratton's interests and goals fit with those of the Institute's faculty, especially some of the younger men who sought administrative approval of their visions for MIT. All at the Institute seemed to agree that more support should be given to research, and most hoped that the school would become a center for the application of formal mathematics to engineering problems. One of the junior faculty with such a hope was Vannevar Bush. The harmony between Bush's and Stratton's views had much to do with the younger man's success. Bush received critical support from Stratton, allowing him to become one of the most important men in the history of American science and technology.

(U) A Man for All Technologies

(U) A generation later, at the end of World War II, Vannevar Bush was one of the most powerful scientists the world had ever known and a man familiar to most Americans. The heritage of his policies continues to shape the organization of academic research in America. Although his plan for a federal role in science was not completely fulfilled, the National Science Foundation is testimony to his influence.[2] Bush was important because of his influence in such matters as the beginnings of the atomic bomb project and the establishment of the National Defense Research Committee (NDRC) and the National Science Foundation. Despite his enormous contributions while at MIT, despite his influence within the inner circles during World War II and the Cold War, and despite his role in shaping the nature of Big Science, and thus the modern American university, little was written about him until very recently.[3]

(U) Vannevar

(U) The new interest has taken a rather unexpected turn. Instead of focusing on his policy contributions, the spotlight has been on Bush's role in the emergence of computers and information processing. The research on his contributions to computers arose as the new field of computer history was born in the 1980s. The seemingly more

intense interest in his role in the birth of information science was generated by the rediscovery of Bush's work on automatic data retrieval. His ideas for a mind machine, Memex, are now treated as the origin of hypertext and similar knowledge systems.[4]

(U) More Than an Ingenious Yankee

(U) Bush merged science with tinkering, if not technology. He was an inventor and a natural at putting technology together in different combinations to fulfill a need. His efforts were always goal-oriented because he realized that inventions required a market to be successful. Bush paid attention to the commercial aspects of technology and built an enviable list of patents on devices ranging from thermostats and typewriters to electronics.[5]

(U) After receiving bachelor's and master's degrees in engineering from Tufts, Bush gained some shop-floor experience while working for the giant General Electric Corporation. He pushed himself to complete a joint Harvard-MIT doctoral program in electrical engineering. He suffered through a great deal of tedious calculation for his thesis. Naturally, he searched for shortcuts to complete his mathematical analysis of complex electrical circuits and applied some of the many tricks mathematicians used before the advent of the modern computer. The doctoral degree and the favorable impression Bush made on Dugald Jackson of MIT soon proved of great value.[6]

(U) Just out of school, Bush became associated with World War I's New London Research Laboratory where the famous Robert Millikan brought the nation's best men to focus science on the critical U-boat threat. Bush contributed to the research with a significant detection system, joined the Naval Reserve, and became at least a junior member of the national military-scientific establishment.

(U) A complex path eventually led to Bush's being one of the creators of Raytheon, a company that was able to challenge RCA's patent monopoly over radio. Raytheon became one of the many important companies tied to MIT and its students.[7] Bush's postwar entrepreneurial ventures did not end his academic ambitions, however. He accepted a position as an assistant professor in MIT's Electrical Engineering Department. It was understood that he would concentrate on the problems of high-power transmission, a focus that was sure to attract support from the private power companies which were beginning to construct large regional networks. A string of articles on power problems and the mathematical techniques useful for their solution advanced his academic standing.

(U) The Politics of Mathematics and Engineering

(U) Although Bush was a practical man, he was also a missionary for the application of mathematics to engineering and science. He realized he had limited formal mathematical skills, but he compensated by supporting the work of men like the renowned Norbert Wiener. Wiener was brought to MIT to integrate advanced mathematics with teaching and engineering research. Bush also encouraged his students to expand the frontiers of mathematical engineering, with some great results. Claude Shannon, a father of mathematical information theory, was one of the many young men influenced by Bush and Wiener. Bush successfully courted the leaders of almost every high-tech related corporation in America. General Electric, Eastman, NCR, General Motors and many other large corporations were familiar Bush stomping grounds. Significant yet unexplained, Bush did not develop cordial and profitable connections with the two major manufacturers of calculating equipment, IBM and Remington Rand. History would have been different if IBM had chosen MIT over Columbia and Harvard Universities for its attention and if

Remington's leader had made a commitment to academic research.

(U) Within a decade after his MIT appointment, Bush was a member of the most important scientific organizations. Although the United States did not have truly powerful scientific institutions, ones with the financial resources to shape the course of research, such bodies as the National Academy of Sciences, the National Research Council, and the National Advisory Committee for Aeronautics could influence what science policy there was. They also provided invaluable contacts for their members. By his late forties, Bush had become more than a member of such groups. He was a statesman of American science.

(U) The Manager of Science

(U) After a long stint as dean and then as vice president of MIT, Bush became a significant national influence. In 1938 he became the head of the Carnegie Institution, one of the most important scientific research agencies in the world. That led to his assuming the leadership of World War II's very powerful National Defense Research Committee. The NDRC filtered hundreds of millions of dollars of government funds to privately directed research for the war effort.[8] The NDRC was an improved and vastly expanded version of the World War I submarine project and was the fulfillment of some of Bush's long-held dreams about research in America. The NDRC allowed academics something close to the best of all worlds: They received government funding free of most bureaucratic direction. It also fit with Bush's belief that the military would change only in response to outside pressures. By the end of the war, Bush was the most powerful man in American science and was a force the military had to recognize.[9]

(U) Bush and Stratton's Dream

(U) Bush began his work at MIT with research on electrical systems. In the early 1920s, Bush directed his students to expand the reach of analog computing. They began with rather simple combinations of rods and gears to create machines for the automatic calculation of differential equations, but those first integraphs were more than extensions of the old wire and cone contraption that had made Stratton's reputation. The young men edged towards solving the major mechanical problems that had prevented the engineer's friend, the planimeter, from becoming a truly powerful tool. By the late 1920s, Bush and his men were convinced they had overcome the critical problem of torque. They persuaded Stratton and the other influentials at MIT that a new and startling version of Lord Kelvin's machines could be constructed and put to productive use in a few years.

(U) Bush was allowed to assign the best graduate students to the creation of the Differential Analyser. In 1931, he announced to the scientific community that the world's largest and most powerful calculating machine stood ready at MIT to advance science and engineering. It brought international fame to Bush and MIT. International visitors came to the Institute and clones were built in Europe and America. Aberdeen Proving Grounds and the University of Pennsylvania built versions, and General Electric found it so useful it invested in a copy for itself.

(U) Bush Confronts Little Science

(U) Just as Bush's Analyser was given so much by the Institute in the late 1920s, the school lost its state subsidy. Worse, Stratton's hopes that America's largest corporations would donate a constant stream of funds to MIT proved unrealistic. MIT found it more and more difficult to finance research with its own resources, and its leaders feared that it might be forced to retreat to the vocational model of technical education. The

faculty, including Vannevar Bush, was on its own and all had to struggle for the means to continue research and to finance their graduate students. The Institute's new president of 1930, Karl T. Compton, was as much a part of elite science as Stratton, but he was more academic in orientation. A famous physicist, Compton arrived with a mandate to turn the Institute back towards a true scientific curricula and to integrate the latest science with both teaching and research. Wishing to reduce the growing ethical and educational problems stemming from the staff's business activities, and hoping to secure the funds needed to allow internal financing of research, Compton let it be known that he desired more effort for the Institute and less for faculty pocketbooks and corporate sponsors.[10] Informally, faculty were asked to conduct research of general, not particular, import. Formally, consulting fees were to be shared with the Institute, and patents were to become the property of the school if the work had been internally funded. To control the increasingly complex patent problems and to avoid the dangers inherent in a university holding patents, MIT decided to turn to the Research Corporation of New York City. It was to handle all patent matters (including determination of patentability and allocation of shares to MIT, sponsors, and faculty) and was to deal with all related legal questions.

(U) Even the great Vannevar Bush found it difficult to raise funds until the second half of the 1930s. Bush launched upon an almost frantic search for combinations of technologies that might attract sponsors. Among other attempts of the 1930s, he toyed with a machine to identify fingerprints; he tried to devise a high-speed pneumatic printer; he played with the use of high-speed metal tape and wire systems to send secret messages; and he tried to find ways to automate libraries. But he suffered through many years without the kind of financial support that Stratton's earlier policies had promised, and, most telling, he could not find the financing needed for what emerged as his grand plan for the Institute.

(U) Bush's Great Plan

(U) After testing reactions at the Rockefeller and Carnegie Foundations, and after considering his possible role in Compton's drive to make MIT scientifically respectable, Bush put together a grand plan. It was one he thought would attract a wide range of donors, would be applauded by the scientific community, and would lead to a permanent source of support for the Institute. As well, it would call upon the experience and talents of faculty from several of MIT's departments. Bush decided to make MIT the national center for calculation and for the development of path-breaking scientific calculation devices. If Bush had his way, MIT, not the National Bureau of Standards (NBS), would realize Stratton's dream.

(U) Bush knew that his Analyser had taken mechanical technology to its extreme, so his plan for the Center of Analysis included much more than proposals to extend mechanical analog calculation. Electronics, photoelectricity, and new memory media were to be developed and combined to produce revolutionary computers. Bush also wanted the center to explore the new markets for what would later be called "data processing." His plans included digital calculation and machines to solve the escalating problem of file management in science and bureaucracy.[11] He announced that he would create machines that would outdistance all competitors, especially the IBM tabulator.[12] Supported by a group of gifted junior faculty and a cadre of adoring graduate students, he joined together all of the existing measurement and calculating projects at the Institute and began to weave new ideas for future devices.[13]

(U) Beyond Analog Mechanical Machines

(U) Mechanical analog devices were approaching their limits of precision and speed in

the 1930s. Although there were no commercial competitors for such huge devices as the Differential Analyser, [14] Bush saw little worth in cloning it in slightly improved form. If support was to be found, he had to make a major technological leap in analog computing. But there was a more fundamental challenge and opportunity for the center: the growing demand for digital calculation, something MIT's machine builders had not yet explored. The rise of the social sciences was creating a market for digital calculators, and even engineers and physical scientists, who had been so well served by analog devices for more than a century, were tackling problems that called for digital methods. Bush also knew of the increasing need for high-speed digital calculation in the bureaucratic and business worlds. He sensed opportunity because there had not been a major innovation in large-scale digital machinery since Hollerith patented his Tabulator.

(U) The call for digital processing merged with another growing need, information retrieval. Business and governmental files had grown to unmanageable proportions. The hand, mechanical, and electromechanical methods of data retrieval were not satisfying bureaucratic demands.[15] Influential researchers in many sciences found it increasingly difficult to keep up with their areas of interest because of the deluge of articles. Bush and many others lobbied for projects that would allow scientists and engineers to take the lead in the new field of Documentation.[16]

(U) Bush decided to concentrate on the exploitation of three technologies: photoelectricity, digital electronics, and film. Although new, these technologies were much closer to being ready for application than the still delicate magnetic recording. By focusing on the application of these technologies to scientific calculation problems, Bush hoped to be innovative and to avoid conflict with commercial firms.

(U) Responding to positive reactions by the Rockefeller Foundation, Bush sketched a radical new design for an Analyser and, by mid-1936, succeeded in raising the funds he needed to build the next generation of his great analog machine. The Rockefeller Differential Analyser was to be much faster and much easier to program than the mechanical version. Although it remained an analog device, it incorporated electronics, digital circuits, some photoelectric parts, and program tapes. These allowed Bush to eliminate most of the cumbersome mechanical components of the first model. The new Analyser soon became a very demanding, over-budget, and behind-schedule drain on the resources of the Institute and a burden to its students and faculty. The long-delayed appearance of the Rockefeller Analyser also became a threat to the credibility of Bush and the electrical engineering department.[17] However, based on the new developments in electronics, photoelectricity, and film, he was moving into digital calculation and what we now call information retrieval. By the mid-1930s, Bush had rough plans for an electronic "programmed" computer and refined ideas about information machines.[18]

(U) Two Men with a Need

(U) A visit by Admiral Stanford C. Hooper and his young assistant, Joseph Wenger, would lead to one of the most bizarre episodes in American history, would complicate Bush's task of establishing his center, and would link MIT's foray into information machines with the world of secrecy. The Hooper-Bush agreement for the development of radically new cryptanalytic machines for the navy's codebreakers had the potential to set a positive role for academic scientists in the invention and evaluation of military technology. Its promise was not realized, however. The project turned into an exercise in bureaucratic bickering. More than half a decade was spent dealing with organizational problems rather than with the technical barriers that were holding back the realization of the potentials of electronic technology. Despite all the efforts of Stanford C. Hooper,

Joseph Wenger, and Vannevar Bush, the United States lost an opportunity to complete the first electronic data processing machines and to make them operational before the attack on Pearl Harbor.

(U) A Man for the Navy

(U) Stanford C. Hooper prided himself on being an innovator, and he devoted his career to introducing new technology to a usually reluctant United States Navy. Graduating from Annapolis in the early 1900s and assigned to the Pacific fleet, he immediately began to create the navy's first radio system. Transferred to Washington, he stole hours to study at Samuel W. Stratton's new National Bureau of Standards. Mastering the latest radio science, Hooper then lobbied for the establishment of the navy's own radio research division. Hooper's expertise and advocacy of electronic communications soon thrust him into military and civilian policy making. Although still a young man and a junior officer, he was instrumental in creating the Radio Corporation of America, the giant electronics corporation formed at government request at the close of World War I.

(U) Stanford C.

(U) Because of its need for worldwide command and control, the navy had a special stake in the success of RCA. Hooper hoped that RCA's special position would make it confident enough to overcome the fear that government work would threaten its patents. The hopes of RCA serving as a research branch of the navy were not completely fulfilled, but Hooper continued to use its men and facilities while he searched for help from others.

(U) By the early 1930s Hooper was advancing through the navy's ranks, was a much-honored figure in electronics, and was an acquaintance, if not friend, of the leading scientists and inventors of the nation. He used such contacts and his expertise to devise and forward plans for a fully integrated and modern information system for the navy, one which was to include every advanced technology. He had an even greater vision: to permanently wed science and the navy.[19] He was determined to prevent the navy from being as unprepared as it was for World War I. Hooper became tied to those in favor of centralized administration and increased power for the Chief of Naval Operations (CNO). Hooper began to develop a strategy, one somewhat different from the plans of other of the navy's new progressive reformers. He was willing to depend on outsiders. Although he helped give birth to the Naval Research Laboratory and was able to create special research sections, such as the Code and Signal desk in the Bureau of Engineering, he believed the navy would have to rely on the new research centers that were emerging in the largest corporations and universities.

(U) Ending his stay as head of the Bureau of Engineering's radio section, where he fought for a radio modernization program, Hooper moved from technical to more general policy concerns. His appointment as Director of Naval Communications in 1928 gave him an opportunity to aggressively pursue his vision. And, when he assumed the newly created position of special scientific advisor for the navy in the mid-1930s and chaired its Technical Research Liaison Committee, he had the chance to expand his reach well beyond the traditional boundaries of communications. All science-relat-

ed fields, ranging from ballistics through medicine and atomic energy, became part of his domain.[20]

(U) He and his most trusted proteges toured the nation seeking ideas and establishing contacts with scientists. As part of his plan, he laid the bases for permanent cooperation with laboratories and executives at Eastman, AT&T, General Electric, and a host of other corporations. To create a similar link with the universities, he found a way to award special military commissions to academics so they could remain in the universities, yet be a part of the navy's modernization effort.[21] In addition, he collaborated with the National Research Council aiding it by finding projects and having it help the navy by identifying qualified investigators.

(U) The identification of willing scientists and new technologies was only a small part of his task. A crucial and politically sensitive step was to convince the various divisions of the navy to accept the civilian men and ideas. The way Hooper handled that had a great deal of influence on the long-term history of the automation of American cryptanalysis and wedded the history of such machines as Vannevar Bush's Comparator and Selector to the broader struggle for professional control within the navy.

(U) Hooper's admiration for the country's top men led him to attempt to force ideas upon unwilling navy bureaucrats and skeptical technicians. As a result, he alienated many powerful men. By 1937 serious complaints reached the naval hierarchy about what was seen as interference in the affairs of the various bureaus. Hooper had to defend himself to the Chief of Naval Operations. After the confrontations and the complaints to the CNO, Hooper softened his approach, but he continued to advocate the types of technological innovations that did not fit with the service's existing bureaucratic structure. He went ahead with his effort to modernize and professionalize the navy, but the political battles of 1936 and 1937 took their toll on him.

(U) Even when ill health and perhaps some political complications arising from his worries about America's military readiness[22] led to a reduction of his efforts in the 1940s, he remained an important advisor on technical and scientific matters and a member of such high science and big budget organizations as the National Advisory Committee for Aeronautics. By the time he formally retired in 1943 he had, along with a few other senior officers, laid the intellectual if not organizational foundations for the Office of Naval Research. The ONR became the organization the navy successfully used to bring academic science into the military after World War II. The ONR became one of the major sponsors of applied mathematics and computers in the United States.[23]

(U) Hooper's influence did not end in 1943. Although retired, he continued as a consultant to major corporations and became deeply involved with a company founded by some of his admiring young men. The fascinating postwar Engineering Research Associates (ERA) was planned as a showcase for some of Hooper's dreams. It was to be a private company serving the advanced scientific needs of the military. ERA became the torchbearer for the navy's advanced cryptanalytic computers.

(U) Another Plan for Science and the Navy

(U) Hooper's model for research, which centered on cooperation with the private sector, was not the only one put forward by navy reformers. During the 1930s, one of the navy's progressives was much less trusting of outsiders. Harold Bowen, one of the fathers of the Office of Naval Research, put his energies to strengthening the navy's own science and development capabilities. While chief of the Bureau of Engineering from mid-1935 to 1939,[24] Bowen came in conflict with the Bureau of Construction and its allies, the pri-

vate shipbuilders. The issue was the design of the navy's new destroyers. Bowen was the political loser and he remained convinced that the secretary of the navy's order to merge Engineering and Construction into one new agency, the Bureau of Ships, was a victory for the technical and political Mossbacks.[25]

(U) Like Hooper, Bowen made many enemies because of his fight to keep the navy up to date by bringing in new ideas from industry and academia. Bowen wanted more research within the navy and had faith in a revitalized Naval Research Laboratory. One of his last acts as chief of the Bureau of Engineering was to create its Office of Research and Inventions. With the experienced Lybrand Smith and some very enthusiastic young officers on its staff, the ORI began to do what Hooper bad been advocating for years: integrate Engineering with the most talented men in private industrial research laboratories and universities. The Office of Research and Inventions became the navy's organization to coordinate with Bush's NDRC. That led Lybrand Smith and Vannevar Bush to become quite close despite the growing frictions between Bush and Bowen over research policies. Smith also became an important player in the history of OP-20-G's first cryptanalytic machines.

(U) By the end of World War II, Smith and Bowen had convinced the navy to create something Hooper had always wanted, the Office of Naval Research. Bowen made sure the ONR had the money, power, and contracting laws to control the relationships it established. The ONR would use academia and industry to bring science to the navy, but it was given enough power to allow the navy, not civilians, to direct research. Bowen hoped that it also had enough power to withstand the protests of the old bureaucrats and politicians.[26] One of Bowen's motives for establishing the ONR was to allow the navy to develop its own program for atomic energy which, he hoped, would lead to an atomic-powered ship program.

(U) Hooper Confronts the Bureaucracy, Again

(U) Stanford Hooper viewed science, research, and innovation as significant to every naval activity, but he maintained a special interest and role in naval communications. His plans for advancing radio communications led him to become involved with the navy's cryptanalytic branch, OP-20-G. Hooper became a crusader for the expansion and modernization of American interception, codebreaking, and all other signals intelligence capabilities. It was that involvement that eventually led Hooper to MIT in late 1935.

(U) As with his electronics work, Hooper's plans for cryptanalysis came to center on institutionalized scientific research. At the same time, he supported the expansion of the navy's cryptanalytic operating division, OP-20-G.

(U) For historical reasons, Communications (OP-20) rather than the Office of Naval Intelligence housed the cryptologic department that became known as OP-20-G.[27] And for other bewildering reasons, OP-20-G depended upon the Bureau of Engineering for the design, purchasing, and manufacture of its equipment. Another naval branch handled contractual details. To further complicate the bureaucratic tangle, OP-20-G's Research Section (Y) was the small group charged with communications security and, significantly, the exploitation of the lack of security of the communications of other nations. On top of that, and despite OP-20-G-Y's mandate, yet another research group was set up within Engineering to explore related technological questions. Adding to the confusion over power and domain was the Naval Research Laboratory. Although their core functions were under the direct command of the CNO in the critical years of the 1930s, communications and cryptanalysis had a tough go of it in the navy.

(U) A Few Men and Women for Secrecy

(U) The navy's very small cryptologic group, OP-20-G, began its life during World War I but was not active until the mid-1920s.[28] One reason for its inaction was that just as it was founded, the incredible Herbert Yardley was lobbying for the creation of what became the famous American Black Chamber. His group was to serve the cryptanalytic needs of the army and the State Department, and, to some unknown degree, the navy. Stealing resources away from the private cryptanalytic group that had been developing at the estate of the flamboyant millionaire, Colonel Fabyan, Yardley achieved some amazing victories. He broke the codes and ciphers of the major powers. That allowed the United States to predict the bargaining positions of the important players in the naval arms limitation negotiations of the 1920s. Yardley's work made him some good friends but also some enemies. A few rash decisions on his part also led to the closing of his Chamber in 1929 and the transfer of its files to the army's old code organization under William Friedman. Yardley then decided to take one of the most fateful steps in the history of American cryptanalysis. He published a book that told the when, what, and why of American cryptanalytic success. One horrible consequence was that the Japanese began to change all their code and cipher systems.[29]

(U) OP-20-G did not receive much official navy support. Until the mid-1920s, when it came under the command of a young and bright officer, Laurance F. Safford, it was almost a shadow organization. Safford arrived just in time to take advantage of the "acquisition" of a copy of part of Japan's secret naval code. The code proved invaluable, and OP-20-G began providing critical information to the navy. But that did not mean recognition of the potentials of communications intelligence or adequate funding. "G" might not have survived if it had not been for a supersecret fund set up at the end of World War I.

(U) OP-20-G's interactions with the Office of Naval Intelligence were, at times, ones of strain as well as frustrating dependency. ONI did much of the needed dirty work to obtain codebooks and information about cipher machines,[30] and it had the responsibility for interpreting the intentions of America's enemies. But the ONI and OP-20-G were bureaucratically separate, and at key times there was mistrust. "G" also had less than satisfactory relations with naval commanders. The use of "G's" information was dependent upon the decisions of local commanders, and OP-20-G relied upon their willingness to supply intercepts to Washington. Even serving only a technical cryptanalytic role was difficult for "G." It took many years for it to acquire any control of what radio systems were to be monitored.

(U) Captain Laurance F. Safford, USN

(U) The Search for Pure Cryptanalysis

(U) Through his academic and corporate contacts, Hooper learned of the potentials of mechanized automatic control and of the increasingly mathematical nature of science and cryptanalysis. His awareness of the expanding reach of statistical techniques, the potentials of high-speed

calculators, and the use of light-sensitive devices in astronomy were perhaps sharpened by visits and discussions with Vannevar Bush.[31] Whatever the particular source of his knowledge, Hooper believed that the new electric and mechanical ciphering devices introduced by the major powers, including the United States, would force cryptanalysts to become statisticians. They would have to perform seemingly impossible feats of calculation to penetrate the ciphers produced by such complex machines as the Kryha and the Enigma.[32]

(U) As soon as he assumed command over Communications, OP-20-G informed Hooper of its progress against the cipher machines. The cryptanalysts were quite proud of their secret and clever techniques, ones they thought were essential because of the impracticality of a pure mathematical approach.[33] Although they employed statistical techniques, they had effective short cuts such as finding a copy of a secret message sent in a known code; locating often repeated phrases (cribs); or uncovering the pattern of the way an enemy announced the wheel settings for a cipher machine network. They were also quite proud of their craftsmen's tools, such as paper wheels, long strips of wood with alphabets painted on them, and overlay sheets with punched holes for attacking ciphers. But Hooper and his new right-hand man, Joseph Wenger, were not impressed by the tricks, and they thought that OP-20-G's technology, if not methods, were woefully behind the times. In late 1930 Hooper suggested to OP-20-G and the Bureau of Engineering that they begin to develop automated cryptanalytic machines and, by implication, to formalize their approach to analysis.[34]

(U) Hooper wanted machines that would free OP-20-G from tricks and dependencies and that would allow the use of advanced mathematics. Those machines would have to be innovative because the new cipher devices presented cryptanalysts with problems far different from those of code systems. Codes were secret lists of words (or (combinations of numbers) that stood for other words. In contrast, cipher machines dynamically changed letters into different ones with no predictable relationship between the original and the cipher letters. The limited vocabulary of a code meant that acquiring a copy of its codebook was an effective solution, unlike the situation with sophisticated cipher machines in which having a copy of the enemy's machine was only a small step toward reading messages. The key method an analyst used to solve a code was to identify the relationships between a particular code word and other words. Correlation analysis and the use of a decoded word to predict the meaning of another were viable methods.

(U) The new cipher systems demanded less obvious approaches. The cipher system designers' goal during the 1920s and 1930s was to avoid the meaning embedded in any code system. The American Hebern cipher machine and its European cousins, such as Enigma, took the old principle of random substitution of one letter for another to a new level. They went far beyond the centuries-old cipher tables and handy substitution algorithms.

(U) All of the new machines relied upon sets of wired rotors (or relay analogs of them) whose internal electrical connections produced a unique substitution cycle of such complexity and length that it could be penetrated only through time consuming analysis of forbidding amounts of data. Unless the operators of the encryption machines made a mistake, or the cipher breakers had a constant source of information on the settings of the cipher wheels, incredible amounts of calculation were needed for pure cryptanalysis. Hooper was sure that the growing use of the new cipher machines and the shortage of experienced cryptanalysts meant an end to the power of informal methods. He saw no alternative but to develop formal techniques and advanced machines.

(U) More than an abstract faith in scientific cryptanalysis led to Hooper's drive for new

machines. There were very practical reasons. "G" had to be made independent and ready for an emergency. Older methods, for either codes or ciphers, demanded too many experienced codebreakers who had spent years working on particular systems and on information supplied to OP-20-G by others such as Naval Intelligence. Automation and formal procedures would have to substitute for professional skill and experience as well as the old codebreaker's standby, intuition.

(U) But in 1930 the navy's bureaucracy and even the crew at OP-20-G were less than accepting of formal analysis and machinery. The codebreakers at OP-20-G were aware of the emergence of the new ciphering devices and, in fact, were building their own versions as well as tackling the systems of other nations. Because of their direct experience with automatic enciphering devices, Hooper's September 1930 "suggestion" about methods and automation was not too well received. OP-20-G's principal civilian cryptanalyst, Agnes Meyer Driscoll, did not like the idea at all. Additionally, the cryptanalysts felt insulted because Hooper's request contained an implicit criticism of their work and skills. They thought that formal methods, while helpful, would never replace an experienced codebreaker. And their years of work had taught them that decryption was usually dependent upon some type of informal initial entry into a system, whether it be a psychological insight, a theft of materials, or the transmission of a message in both clear and enciphered form.[35] In addition to the codebreakers' distrust of those who proposed unrealistic methods and machines, the small OP-20-G staff was too busy analyzing Japanese code systems to deal with methodological speculations.[36]

(U) Hooper thought he would eventually tempt OP-20-G into applying formal methods by presenting it with a demonstration device. Hooper soon arranged to have the Bureau of Engineering create a new section for advanced code and signal research [37] and then made sure that someone who would pursue his goals filled the post. A young officer who had been one of the first students in OP-20-G, who had experience as a seagoing communications officer, and who was already a protege of Hooper, was selected. Joseph Wenger, a thirty-year-old Annapolis graduate, followed Hooper's cues and began a search for new technologies for all aspects of communications with, of course, an eye open for new devices for ciphering and deciphering messages. With some interruptions caused by shifting naval assignments, Wenger continued that search through the 1930s and 1940s, and he became the driving force behind what became the most technically advanced cryptanalytic agency in the world by the late 1940s.[38]

(U) Joseph

(U) From Electronics to Electromechanics

(U) In the early 1930s Hooper's academic contacts turned him towards something much more innovative, the electromechanical tabulating machines built by companies such as IBM and Powers. Hooper successfully prodded the Chief of Naval Operations into sending a very specific and strong directive to the Bureau of Engineering in late 1931.[39] It ordered the Bureau to devote resources to study the new optical sorters and special devices for blind reading and came close to demanding that such technologies be used to build a deciphering device.[40] The CNO's mandate included more than cryptanalytic investigations; it was a signal to Hooper to intensify his efforts to

link science to the navy. Under pressure from Hooper, the Bureau provided Wenger with the money needed to make a grand tour of America's research laboratories. During his visits, Wenger encountered fantastic new technologies that had at least long-term promise for solving the difficult cryptanalytic problems, but most seemed to demand a protracted and expensive development period.[41] Wenger was especially disappointed when he realized that optics and electronics were not quite ready to produce a cryptanalytic machine.

(U) Perhaps because of that and because of a sudden realization by OP-20-G that it would need some type of mechanical aids, Wenger turned his attention to a more established technology. The Hollerith and Powers electromechanical tabulating and sorting machines were evolving into quite sophisticated devices by the late 1920s. In addition, they were machines that were immediately available for use and were commercially produced. Wenger examined the Remington-Rand Powers tabulators used by OP-20-G in 1932 and did enough research to allow Hooper to again, but more authoritatively, suggest that OP-20-G investigate them. It was difficult for the officer in charge of OP-20-G, Laurance Safford, to ignore Hooper's urging any longer.[42] But Hooper's grand dream suffered a temporary yet important setback.

(U) Just as Wenger was exploring the various technical possibilities, it was discovered that the Japanese had replaced their Red Code with a completely revised set that could not be penetrated. Perhaps because of Yardley's indiscretions, seven years of work on the previous code had become valueless! OP-20-G's codebreakers knew they would be unlikely to obtain a copy of the Blue Japanese code and the three other new systems [43] and decided to take on the formidable task of breaking the code through pure methods. The Japanese continued to use the old type of superencipherment, the modular addition of random numbers to the code groups, so it was a relatively easy target. But the code itself, Wenger knew, would demand years of work. Over 100,000 words had to be decoded. Such an effort called for either vastly increased manpower or mechanical aides.[44] Everyone knew that "G" was unlikely to be allocated more men.

(U) In early 1932 OP-20-G's cryptanalysts studied Wenger's tabulator survey and decided to select the type centered upon electrical rather than mechanical reading of cards. Seeing Remington-Rand's system as inflexible, they hurried to rent the electromechanical IBM tabulating devices, ones built to handle alphabetic characters as well as numbers. The punch card era seemed to have begun at OP-20-G.

(U) Then the navy hierarchy declared that it was unwilling to fund the experiment! Safford and Wenger did not give up. OP-20-G pressured the Bureau of Engineering to scrape some funds from its already slim budget,[45] but the Bureau was able to raise only a few hundred dollars, not several thousand, to start the project. It continued to piece together small amounts during the 1930s to support the tabulators. But it always felt that OP-20-G did not fully appreciate its efforts.[46] Only a machine or two arrived at OP-20-G, and their experimental use, which soon turned into a necessity in the eyes of many at OP-20-G, survived only as a near underground activity.

(U) Despite the hand-to-mouth funding of its few machines, the OP-20-G tabulator crew continued with its work and made major contributions to the penetration of the new Japanese codes. The navy also explored new ways to store data on IBM cards, and during the war it helped develop special tabulating machines.

(U) Ironically, OP-20-G's early 1930s tabulator-related achievements had a negative influence. Although the search for cryptanalytic technology and methods had been motivated by Hooper's deep fears concerning the new automat-

ic ciphering machines, including Britain's,[47] the crisis caused by the change in Japan's older code system shifted attention to more immediate problems and forced a commitment to available devices. The more sophisticated machine options were dropped in favor of the tabulators. The tabulators were well suited to many decoding procedures, especially those calling for sorting and, later, collating operations, but they were not the mathematical or truly high-speed statistical devices needed to break into the new cipher machines.

(U) The leasing of a few tabulators did not link IBM to any long-term commitments to OP-20-G or Engineering. Although IBM played a significant role in certain extensions of electromechanical technology before and during World War II, it did little truly far-ranging research for the cryptanalysts during the 1930s. While the use of tabulators was a great step in the history of cryptanalysis, the commitment to tabulators took away much of the incentive to make the great technological leap Hooper had desired. The very hard-pressed staff at OP-20-G had more than enough to do to learn how to exploit the IBM equipment.

(U) Then, when older cryptanalytic methods triumphed over Japan's new cipher machine, the Red, there was little excuse for an emergency development program. The success against Red undermined arguments that an advanced in-house developmental group should be established within the Bureau.

(U) A Young Man for the Future

(U) Something else helped to turn the navy away from Hooper's plans for truly advanced automated cryptanalysis. Joseph Wenger, Hooper's man in the Bureau or Engineering, who had become an ardent believer in the value of science and technology, was returned to sea duty in mid-1932. He had supplied Hooper's grand outline for communications with the details needed for OP-20-G's technical and organizational future.[48] As significant, while on sea duty, he refined and codified the important method later known as traffic analysis (T/A). He combined direction finding, callsigns, and traffic flows into a highly effective tool.[49] To prove the worth of the approach, he reconstructed the Japanese naval maneuvers without being able to read the contents of the radio signals.[50] Although not appreciated by outsiders, even Hooper during the early 1930s, T/A became a major factor in the American victory in World War II.

(U) The Dream Postponed, Again

(U) Wenger's transfer to sea duty in 1932 allowed him to help unravel Japan's naval tactics and to refine America's eavesdropping capability in the Pacific, but it was near devastating to the cause of automating code and cipher breaking. Almost as bad for Hooper's cause was Laurance Safford's assignment to sea for four years. His absence until 1936 stretched the resources of OP-20-G to the breaking point and left Hooper without an in-house advocate. When Safford returned to Washington, the growing crisis in the Pacific, including the sudden change of a major Japanese code in 1936, left him with no time for experimentation. Despite OP-20-G's dependency on the Bureau of Engineering for hardware development, the engineering branch was left without a spokesman for advanced cryptographic technology. What men Engineering could spare became involved in the difficulties of inventing and manufacturing electromechanical encryption devices. The bureau, along with the Naval Research Laboratory, also faced increasing demands and few thanks for radio and radar developments. At the same time, OP-20-G became deluged with new and more difficult code and cipher problems as Japan carved out its Asian empire. The tiny crew had little time for technological or mathematical speculation.

(U) The Dream Reborn, for a Moment

(U) It was only Wenger's return in mid-1935 and the Roosevelt-Vinson decisions to expand the navy that allowed Hooper to again pursue his cryptanalytic goals. Wenger had the experience, the energy, and the desire to restart the program, and naval expansion hinted at the possibility of funding.[52]

(U) The changes at OP-20-G in 1935 extended to more than the renewed hopes for new research machinery. Wenger was made the head of OP-20-G's new research desk. The new "Y"section was to be devoted to the application of science to cryptanalysis and to the type of long-term planning development that the CNO was encouraging in all parts of the service.[53] Then, when Safford came back to Washington in 1936, Wenger began another round of visits to the centers of American science and technology. Among those Hooper visited in 1935 and then recommended to Wenger was a man he had known for years, Vannevar Bush.[54]

(U) Bush, Wenger, and Hooper joined forces at a time when their interests seemed to be in perfect harmony and when they thought they had the resources and power to initiate and complete a major program. Bush's scientific status was perhaps the major reason why Hooper looked to MIT rather than to the large corporations such as National Cash Register or IBM or RCA or to the National Bureau of Standards for help in automating American cryptanalysis. On a gentlemen's agreement, Bush began to draft a plan for the navy, and Wenger returned to Washington filled with enthusiasm. He was convinced that the $10,000 consulting fee Bush expected was a great bargain. Bush dashed off his report and submitted it in the first weeks of 1936. He was able to respond so quickly because of the optics-film-electronics work he and his colleagues at MIT had been doing for several years. Of great importance, he had begun thinking of and lobbying for the development of electronic cryptanalysis well before 1935.[55]

(U) Bush's initial proposition was not for the production of specific equipment. Rather, it defined his role as that of a consultant to the navy. He sketched the general outlines for a long-term project centered about the creation of high-speed optical-electronic devices which would be hundreds of times more powerful than the tabulators. He recommended that the navy design and develop what became known in the intelligence community as Rapid Analytical Machines (RAM). Everything finally seemed to be falling into place for them and Bush in early 1936.

(U) Little Science Meets the Little Navy, Again

(U) Hooper thought he was having Bush subsidize his great plan for the navy. Bush thought the navy would subsidize the beginnings of MIT's calculation center and its entry into digital processing. Wenger thought he had a set of ideas that would launch the navy on a full-scale development project. None of them realized there were built-in conflicts. Hooper probably did not know of the financial pressures on Bush and MIT during the 1930s. In turn, Bush did not suspect that Hooper and Wenger had not convinced the navy of the worth of their approach to introducing innovations.[56]

(U) Just as the prospects for Bush's center rapidly brightened and as Hooper was receiving signals that his comprehensive plan for all communications activities would be approved, the navy made an unexpected, critical, and disappointing decision. For a second time the attempt to revolutionize cryptanalysis seemed to have been defeated by the tangled navy bureaucracy and the men Bowen called "mossbacks"! Before Bush's navy project truly got under way, he and his naval allies became involved in an organizational nightmare. Bush thought freedom from interference was essential if academia and the

military were to join together, and he believed that no absolute timetables and guarantees could be given for truly innovative work. Hooper and Wenger agreed that heavy-handed bureaucratic oversight would doom any creative effort. Wenger hoped that Bush's status and persuasive powers would be able to break the navy bureaus' resistance to outsiders. But the naval bureaucracy had a different opinion.

(U) The Bureau of Engineering men very bluntly told Hooper and Wenger that Bush's plans were unrealistic and his demands outrageous. They were soon joined by the contracting arm of the navy, which declared many parts of Hooper's model for academic/military cooperation ill advised, if not illegal. They would not give the needed approval, and the project that could have led to the creation of the first electronic digital data processing device seemed dead in early 1936.

(U) A Man for Statistics

(U) Just as Stanford Hooper was facing the defeat of his hopes of creating a new technology for cryptanalysis, another major figure in the history of American codebreaking was becoming entangled with automation. William F. Friedman, the head of the army's cryptologic section, finally convinced the army to allow him to use tabulators. Although their introduction into the army's Signal Intelligence Service (SIS) came almost five years after Hooper and Wenger had brought them into OP-20-G, the arrival of the IBM machines at the SIS offices seemed revolutionary.

(U) In 1929-30, just as Hooper was trying to refurbish naval communications, the army had to fill the void left by the disintegration of Yardley's Black Chamber. Instead of creating an entirely new organization, it gave additional mandates and some additional resources to the man it had previously hired to safeguard its own communications, William F. Friedman. Unlike Wenger or Hooper, Friedman had not come to code work through the military; rather, he stumbled into it because of his college courses in genetics.

(U) The son of a Hungarian-Russian-Jewish immigrant, Friedman attended an advanced technical high school where he delved into electrical engineering. But his interest in the new field of scientific agriculture led him to one of America's centers of applied science, Cornell University. After finishing heavily statistical courses in genetics, and gaining experience in research at one of the prestigious Carnegie centers, Friedman decided to postpone gaining a Ph.D. He wanted and needed a job. He accepted a position as a research geneticist for one of America's most influential agricultural businessmen, Colonel George Fabyan. Assigned to Fabyan's estate at Riverbank, Illinois, just as Europe was becoming engulfed in war, Friedman soon found himself busy with Fabyan's private cryptanalytic projects rather than with the development of hybrid cottons. When Fabyan offered his staff and his estate to the United States government for cryptanalytic training for the war effort, Friedman's future was set.

(U) William F. Friedman

(U) His energies were turned to applying the new statistical techniques he learned at Cornell to cryptanalysis. His cryptoattacks and his training methods became legendary. As a result, after the war the United States Army asked him to establish a code agency. Because Herbert Yardley's Black Chamber held the mandate for listening to

the communications of others, Friedman was asked to focus on the protection of army communications and on the preparation of training manuals for wartime cryptanalysis. Although concentrating on those tasks, Friedman did not abandon code and cipher breaking. He was called on to test various proposed systems, including cipher machines the navy thought of purchasing.[57]

(U) Friedman's role began to change in 1929 when Yardley's group was under political threat. The army decided to found its own operational cryptanalytic group. It gave Friedman the funds he needed to hire a group of young civilians, and it gave him Yardley's files. Perhaps it gave him access to Yardley's old sources of intercepts. Friedman trained his young men in codebreaking and made sure they learned about formal statistics and foreign languages by enrolling them at a local university. Meanwhile, his wife, also a Riverbank alumna, became the cryptologist for the Coast Guard.[58] While her crew worked on the clandestine messages of rum runners and other criminals, Friedman's team examined as much diplomatic and military traffic as it could obtain through the very limited intercept capabilities of the army.[59]

(U) Together, the Friedmans blended practical experience with statistics to develop more powerful cryptanalytic tools. Although Friedman did not attempt to make the direct links with elite academics that Hooper was forging for OP-20-G, he was proud of the "scientific" character of his methods.

(U) Those statistical methods and knowledge of many of the machine activities at "G" soon led Friedman to seek a means of automating the army's codemaking and codebreaking work. Beginning a few years later than the navy, Friedman tried to acquire IBM tabulators for his office. He faced almost as many frustrations as Hooper and Wenger but finally acquired some machines in late 1934.[60] By 1937 he and his crew had developed several tabulator methods that became classic means of cryptanalytic attack, and they began to turn the tabulators into more specialized cryptologic tools. He and one of his young men, Frank Rowlett, invented an attachment for the tabulating equipment that allowed it to generate "random" code.[61]

(U) Friedman began to develop visions of a greater technological future for cryptanalysis. But, unlike Hooper and Wenger, he did not seek help from outsiders, at least not in the 1930s. Perhaps that was because his research ambitions, even more than "G's," were smothered by the military bureaucracy. Friedman did not have a Hooper to run interference for him with the Signal Corps. For whatever the reasons, Friedman's automation efforts were less adventurous and more limited than Wenger's. He had no Vannevar Bush and no ties to the nation's scientific elite.

(U) In the mid-1930s Friedman concentrated on plans for putting teletype tape readers, relays, and plugboards together in various combinations. Some of those became outlines of his own versions of Index of Coincidence machines and isomorph locators (pattern finders).[62] And, at the end of the decade, he somehow found the money to hire an MIT electrical engineer, Leo Rosen. Rosen had a solid background in electronic tubes and circuits. Perhaps Friedman hired him with an eye to beginning his own version of the navy's electronic RAM program.

(U) Science and the Navy Need Other Friends

(U) In early twentieth century America, corporations and private foundations were more important than government or higher education. As a result, corporate research policies and decisions by the leaders of the philanthropic foundations played a determining role in the history of Bush's and Hooper's crusades. Decisions by Eastman-Kodak, AT&T, IBM, and especially the National Cash Register Company were critical to

the emergence of the machines for cryptanalysis and for the library. As late as the 1930s, the scientists' lobbying efforts to make pure science one of the targets of federal support were failures. They were rebuffed by Congress as well as by the usually open-handed Franklin D. Roosevelt. As a result, there was no pure science program in the nation.

(U) The Private World of Science

(U) During the first forty years of the twentieth century, the nation's scientists looked to two sets of foundations, those created by Andrew Carnegie and John D. Rockefeller. Their fortunes, generated by the technological revolution of the nineteenth century, became the fuel for American academic science.

(U) Their decision in the 1920s to finance research within the elite American universities was critical to the history of American science. As important, they created the first bureaucracies designed to manage long-term, very expensive scientific programs. Those programs accounted for perhaps as much as 90 percent of such activity during the 1920s and 1930s, and their managers became key players in the shaping of scientific institutions during and after World War II.[63] The administrators of the 1930s private foundations, including Vannevar Bush, became the overlords of 1940s science and then became the leaders of the early Cold War scientific and high-tech agencies.

(U) As outside research became more attractive, the Carnegie and Rockefeller foundations turned to the old national science institutions for help. The National Academy of Sciences and the National Research Council were energized with foundation monies and began to act as scientific go-betweens. The NRC managed many projects for Carnegie, advised other foundations about national needs, and recommended worthy scientists.[64] After those first steps, the foundations began to help some individual academic researchers just as MIT's new president launched his faculty, including Vannevar Bush, on a sweep for research funds. Very important to Bush were the decisions by one of the new young administrators at the Rockefeller Foundation, Warren Weaver.

(U) A Man for Applied Mathematics and Information

(U) Warren Weaver was one of those new bright scientific men brought to the foundations to reformulate policy. Central to Weaver's plan for the revamped natural science division of the Rockefeller Foundation was the creation of instruments to encourage the use of mathematics in every field. By the mid-1930s Bush convinced Weaver that the world of science was ready for new generations of Analysers. Then Weaver successfully lobbied his superiors for a $10,000 study grant for Bush's proposed partially electronic machine. Just a year later, he secured an astounding $85,000 for the Rockefeller Analyser project at MIT.[65] Half a dozen years later, Weaver again showed his faith in MIT when he funded another huge computer project at the Institute, one for an electronic digital programmed computer.[66]

(U) American Science and the War – the NDRC

(U) Only a few in America realized that Germany was inventing a new type of high technology warfare and that fundamental science might be needed to combat the horrors of atomic weapons and long-range bombers. Vannevar Bush and his close scientific friends were among those few. Never a man to sit by and let the world determine his fate, Bush sought ways to ensure a flow of academic contributions to the war effort.[67] Bush energized what became one of America's first modern science interest groups and began to lobby the government to support a wide range of new programs. Bush convinced President Roosevelt to create the powerful and well-funded

National Defense Research Committee (NDRC) in June 1940.Within a year, its scope and its powers to initiate and control projects were vastly expanded. The new Office of Scientific Research and Development was a dream come true for Bush. It was almost the perfect science foundation for elite American academics.

(U) The NDRC was responsible to the president, not the military or Congress, and its scientists could determine what projects to begin or end. Hundreds of millions of dollars came under the control of the NDRC. The NDRC and elite science were subsidizing science as well as potential weapons. Administrators of foundation science, who were friends of the universities, were selected to head the major branches of the NDRC. The old Carnegie-Rockefeller circle, which included the leading men from the leading universities, moved from private to military philanthropy during the war and, along with Bush, were able to circumvent the "mossbacks" in the military and the older organizations of science. In the fall of 1940, the NDRC began to explore defense technologies that were too speculative for the military or its older industrial allies. Of great importance was the computer effort headed by Warren Weaver.

(U) Because of Weaver's mathematical background and his prewar experience evaluating computing proposals, Bush made him head of the mathematical and scientific instrument section of the NDRC. One of his first chores was to develop a program to solve technical problems created by the advance of German military technology. There was a vital need for automatic control of antiaircraft weapons, high-speed counters for ballistic tests, and scientific instruments to monitor atomic processes.[68] In each case Weaver turned to electronic solutions. He called upon all those known to have worked in electronic counting and launched a program for the development of special purpose devices. He soon had the computer builders George Stibitz and Sam Caldwell to help him supervise the work. As important, he was able to pursue another opportunity. He created a center for applied mathematics. It would permanently change academic mathematics in America.

(U) The NDRC was a blessing to Bush and his academic friends, but to others it was a politicized and unnecessary organization that threatened the military research agencies such as the Naval Research Laboratory.[69] To Admiral Bowen, Bush was leading a group bent on playing favorites among the military services and the universities. He soon concluded that the NDRC worked to the disadvantage of the navy. To Admiral Hooper, however, Bush and the NDRC appeared, at least at the beginning, to be the only way the intelligence community could acquire the advanced machines it needed. But computers were far down on the NDRC list, and cryptanalysis entered its world only because of the long chain of associations between Bush, the navy, and the corporations and universities that were at the center of the NDRC.

(U) Corporate Charity

(U) Vannevar Bush looked to the major corporations when he began his search for support for his calculation center in the early 1930s. General Electric had a research branch that was a leader in applied mathematics, but it decided to keep most of its work in-house rather than make any large investments in Bush's center. Paralleling General Electric's reaction, Western Electric and Bell Laboratories were willing to supply critical parts for the Rockefeller Analyser and to give advice on the type of tools and services mathematicians desired. But they did not offer major financial support to Bush's 1930s projects.

(U) The Eastman-Kodak Corporation of the 1930s was not as generous with MIT as its founder had been, but it remained a very good friend of the Institute. Of even greater importance to the nation was Bush's relationship with a corporation that did not have a reputation for research. Why Bush became so close to a compa-

ny that made cash registers is explained by Bush's friendship with the famous team of Colonel Edward A. Deeds and Charles Boss Kettering. That friendship linked National Cash Register, MIT, the NDRC, and the Ultra secret.[70]

(U) Bush first came in contact with Deeds and Kettering through the institutions of American science. Bush and Deeds served on important advisory committees that steered aeronautical research in the United States, such as the precursor to NASA, the National Advisory Committee for Aeronautics. In 1931 Deeds consented to serve as chairman of the board of National Cash Register (NCR).

(U) For someone trying to rebuild NCR, the best opportunities were those that demanded a technology not found in the corporation's offerings of the 1920s. NCR needed new machines to move deeper into information processing. Inventory, retail sales, and personnel management, for example, had demands met only by devices that had some sort of large-scale memory. The failure to create offerings to compete with IBM was one reason for the demand for a thorough shake-up at National Cash Register in 1936.

(U) While Deeds slashed expenditures in many parts of the company, he increased allocations for research. He pushed the efforts to move NCR into the electrified bank-posting and billing machine business, and he looked forward to finding a technology to challenge IBM's grip on automated file management. Previously, Deeds had applauded NCR's very quiet acquisition of the rights to a fantastic machine for the era, the Hofgaard relay computer.[71] Both the 1930 and 1938 NCR relay computer patent applications cited a machine with an architecture quite like that of the modern serial computer. It had a central processing unit and addressed storage. It performed at least three of the four basic arithmetic functions and had the ability to calculate, store, and print totals and subtotals for many different items. Although Hofgaard's machine was quite promising, Deeds ordered NCR's research director, Harry N. Williams, to drop the project and investigate other technological options. Deeds was probably advised to do so by Vannevar Bush, who was aware of the Hofgaard patents and who had just completed his survey of computing technologies.[72] Bush advised a jump into electronics. The men at NCR learned much about the progress of electronics and film-optical combinations in scientific measurement from Bush. They were certainly interested in the MIT work on smaller and more reliable tubes because of the value of low power and fast miniature tubes for machine design.[73] Their positive reaction to the operation at MIT resulted in an endorsement of Bush's suggestion to use the Institute as a resource for NCR.

(U) The Navy Comes in Second

(U) After all the disappointing appeals to the foundations and the troubled negotiations with the navy, Bush finally gained a pliable and generous sponsor. Bush turned to Deeds requesting money for the proposed universal electronic computer, the revolutionary Rapid Arithmetical Machine. Explaining that it was still on paper, but underscoring that other work had already led to the building of successful electronic circuits, Bush was able to get Deeds's attention.[74] The first discussion about the electronic computer may have started with hints that MIT could immediately build an electronic calculator for NCR. But the beleaguered Rockefeller project led Caldwell and Bush to scale down their ambitions. Bush, already very busy, had a limited role in the Rapid Arithmetical project. He restricted himself to writing overviews of its architecture. Like the other projects at the institute, the Rapid Arithmetical Machine fell behind schedule.

(U) Despite his patience and Caldwell's promises, Deeds could not leave the future of his company in the hands of an academic institution. Following Bush's suggestion, NCR established its own electronics research laboratory in the spring

of 1938,[75] headed by Joseph Desch. Desch and his few assistants taught themselves about the latest electronic developments.[76] He completed an electronic digital calculator by 1940 and explored the application of electronics to many types of business machines.[77]

(U)
Joseph Desch

(Courtesy of the NCR Archive at the Montgomery County, Ohio, Historical Society)

(U) Then just as Desch's work was leading to the construction of hardware, the crisis in Europe and Deeds's patriotism ended Desch's commercial projects. His expertise in electronics and, as important, his unique manufacturing abilities, attracted the attention of the men in Weaver's group at the National Defense Research Committee. Before the end of 1940, Desch became part of the rise of Big Science. Within another year, he became central to the history of Bush's Comparator and to OP-20-G's future.

(U) Notes

1. (U) Karl L. Wildes and Nilo A. Lindgren, *A Century of Electrical Engineering and Computer Science at MIT, 1882-1982* (Cambridge: MIT Press, 1985), 7. Samuel C. Prescott, *When MIT Was Boston Tech, 1861-1916* (Cambridge: Technology Press of MIT, 1954).

2. (U) James M. Nyce and Paul Kahn (ed.), *From Memex to Hypertext: Vannevar Bush and the Mind's Machine* (Boston: Academic Press, 1991).

3. (U) Larry Owens, "Straight Thinking: Vannevar Bush and the Culture of American Engineering," (Ph.D. Thesis, Princeton University, 1987). Larry Owens, "Vannevar Bush and the Differential Analyser: The Text and Context of an Early Computer," *Technology and Culture* 27 (1986): 63-95. Montgomery B. Meigs, "Managing Uncertainty: Vannevar Bush, James B. Conant and the Development of the Atomic Bomb, 1940-45," (Ph.D. Thesis, University of Wisconsin, Madison, 1982). Stanley Goldberg, "Inventing a Climate of Opinion: Vannevar Bush and the Decision to Build the Bomb," *ISIS* 83 (1992): 429. G. Pascal Zachary, "Vannevar Bush Backs the Bomb," *Bulletin of the Atomic Scientists* 48 (1992): 24.

4. (U) James M. Nyce and Paul Kahn (ed.), *From Memex to Hypertext: Vannevar Bush and the Mind's Machine* (Boston: Academic Press, 1991), 235-353, especially, Linda C. Smith, "Memex as an Image of Potentiality Revisited," 261-286. Adele Goldberg (ed.), *A History of Personal Workstations* (Reading, Mass.: ACM Press, 1988). On Bush's science policies in the post-WWII era, Daniel J. Kevles's preface to Vannevar Bush, *Science: The Endless Frontier* (Washington: NSF, circa 1992), ix.

5. (U) Bush's patent history was traced through the historical files at the U.S. Patent Office's Crystal City, Virginia, facility.

6. (U) Bernard Williams, "Computing With Electricity, 1935-1945,"(Ph.D. Thesis, University of Kansas, 1984), 48.

7. (U) Otto J. Scott, *The Creative Ordeal: The Story of Raytheon* (New York: Atheneum Press, 1974).

8. (U) Vannevar Bush, *Pieces of the Action*. NDRC and its successor, the OSRD, were very elitist and Big Science oriented. James Phinney Baxter, *Scientists Against Time* (Cambridge, Mass.: MIT Press, 1968), and Irvin Stewart, *Organizing Scientific Research for War: The Administrative History of the Office of Scientific Research and Development* (Boston: Little-Brown, 1948).

9. (U) Vannevar Bush, *Pieces of the Action*.

10. (U) Larry Owens, "Straight Thinking: Vannevar Bush and the Culture of American Engineering," 289-90.

11. (U) An overview of the results of his attempts, from the 1930s to the postwar era is found in MIT Archives, AC4 Boxes 30 and 36, Center of Analysis.

12. (U) Vannevar Bush, "Instrumental Analysis," *Bulletin of the American Mathematical Society*, 42 (October, 1936): 649. Karl L.Wildes and Nilo A. Lindgren, *A Century of Electrical Engineering and Computer Science at MIT, 1882-1982*, 230-3.

13. (U) Smithsonian History of Computers Interviews, "Gordon S. Brown," January 27, 1970, provides a fascinating overview of many of the efforts at the Institute in the 1920s and 1930s.

14. (U) There were several companies that made similar devices for gun control systems for the military, however. See the Barber-Coleman and Hannibal Ford companies. Note that Ford was interested in building a version of an analyser and, perhaps, donating it to Cornell University. See press releases by the Sperry Corporation, "Hannibal Ford," "Ford Instrument Company." On Ford and Bush, Rockefeller Archives, RG12.1 Diaries of Warren Weaver, March 3, 1935.

15. (U) We have yet to have a technical history of the "tab" era that shows how they were used, but general overviews of needs and demand are found in James R. Beniger, *The Control Revolution* (Cambridge, Mass.: Harvard University Press, 1986), and in the brilliant Martin Campbell-Kelley, "Industrial Assurance and Large-scale Data Processing," *Technohistory of Electrical Information Technology* (Munchen: Deutsches Museum, 1991).

16. (U) Irene S. Farkas-Conn, *From Documentation to Information Science* (New York: Greenwood Press, 1990).

17. (U) Larry Owens, "Straight Thinking: Vannevar Bush and the Culture of American Engineering," 78. A valuable insight into the new Analyzer project is Charles Babbage Institute, Interview by William Aspray with Dr. Frank M. Verzuh, February 20 and 24, 1984.

18. (U) Bush's acceptance of digital calculation, as evidenced by the plans for the electronic calculator, the Selector, and the Comparator, calls into the question the thesis that he was wedded to analog models and calculation. See Larry Owens, "Vannevar Bush and the Differential Analyser: The Text and Context of an Early Computer," *Technology and Culture* 27 (1986): 63-95.

19. (U) NSA RAM File, Hooper to OP-20-G, "Cryptanalytic Machines," September 26, 1930, and Library of Congress, Papers of Stanford Caldwell Hooper, Box 18, Hooper to Secret Naval Board, "Staff Corps Personnel," February 7, 1936.

20. (U) Library of Congress, Papers of Stanford Caldwell Hooper, "Memorandum on Johns Hopkins Group Visit," November 3, 1937, Box 17.

21. (U) Rockefeller Archives RG12.1, Diaries of Warren Weaver, "Visit of Hooper and Lemmon," June 10, 1938.

22. (U) Wheeler, *Yankee from the West*, 18-20, 386, and Farago, *The Game of the Foxes*, 477-8.

23. (U) The ONR became a blessing to the universities after World War II when it replaced the NDRC to subsidize research until the National Science Foundation was created. Harvey M. Sapolsky, *Science and the Navy: The History of the Office of Naval Research* (Princeton, NJ: Princeton University Press, 1990). The ONR is put into perspective in Thomas A. Guniston and Roger L. Geiger (ed.), *Research and Higher Education: The United Kingdom and the United States* (Buckingham: Open University Press, 1989), 3-17.

24. (U) Paolo E. Coletta (ed.), *The American Secretaries of the Navy*, Vol. III, 1913-72 (Annapolis: Naval Institute Press, 1980), 663, dates the height of the conflict in 1933-34. But Harvey M. Sapolsky, "Academic Science and the Military: The Years Since World War II," in Nathan Reingold (ed.), *The Sciences in the American Context* (Washington: Smithsonian Institution Press, 1979), 379-399, describes a longer battle.

25. (U) Harold G. Bowen, *Ships, Machinery and Mossbacks: The Autobiography of a Naval Engineer* (Princeton, NJ: Princeton University Press, 1954), 119-20.

26. (U) Ibid, 45. Bowen's role in the evolution of the ONR is traced in Harvey M. Sapolsky, *Science and the Navy: The History of the Office of Naval*

Research (Princeton: Princeton University Press, 1990).

27. (U) NARA RG457: SRH-150 "Birthday of the Naval Security Group"; SRH-305, "The Undeclared War: History of RI," by Laurance Safford; SRMN-084 "Evolution of the Navy's Cryptologic Organization;" and SRH-152 "Historical Review of OP-20-G, 17 February 1944."

28. (U) David Kahn, "Pearl Harbor and the Inadequacy of Cryptanalysis," *Cryptologia* 15 (1991): 274.

29. (U) Louis Kruh, "Tales of Yardley: Some Sidelights to His Career," *Cryptologia* 13 (1989): 327-356. NARA RG457, SRMD-018 "Mexican Intercept Messages 1912-1924 MI-8." (U) NSA CCH Series XI K, Sam Snyder, draft of proposed history "Machines in U. S. Cryptology Before World War II," 27 June 1975. (U) NSA CCH Series XII Z, "Memoranda on SIS, Formation of Cryptanalytic Group" from CCH Series XI K, Box 13, circa 1929-1939.

30. (U) More and more cases of important "acquisitions" during the 1920s and 1930s are coming to light. See Parker, *Pearl Harbor Revisited: United States Navy Communications Intelligence, 1924-1941*, 12.

31. (U) Interviews and correspondence with Waldron S. MacDonald, 1987-91. MacDonald stated that Bush was the one that convinced the navy to investigate highspeed devices. It is more than likely that Bush was in touch with Hooper before 1930 about such matters. See also Library of Congress, Papers of Stanford Caldwell Hooper, Box 21, August 17, 1945, "Rough Draft of Comment," 3.

32. (U) A useful history of the introduction of these machines is NARA RG457, SRH-004, "The Friedman Lectures on Cryptology."

33. (U) Deavours and Kruh, *Machine Cryptography and Modern Cryptanalysis*, 212, 218. NARA RG457, "The Undeclared War: The History of RI," 15 November, 1943, by Laurance F. Stafford, Captain, U.S. Navy, and SRH-355, "Naval Security Group History to World War II," 161. *A History of Communications Intelligence in the United States With Emphasis on the United States Navy* (NCVA), 12. A wonderful insight in OP-20-G's methods is in Lt. L. F. Safford, "The Functions and Duties of the Cryptologic Section, Naval Communications," *Cryptologia*, 16 (1992): 265-281.

34. (U) NSA RAM File, Hooper to OP-20-G, "Cryptanalytic Machines," September 26, 1930.

35. (U) A book that overstates the case against the historical importance of formal analysis but which is still useful is Nigel West, *The SIGINT Secrets: The Signals Intelligence War, 1900 to Today, Including the Persecution of Gordon Welchman* (New York: 1986). A very revealing and important document for the history of OP-20-G and American cryptanalysis is found in Louis Kruh, "Why Was Safford Pessimistic about Breaking the German Enigma Cipher Machine in 1942?" *Cryptologia* 14 (1990): 253.

36. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 80. C. A. Deavours, "The Black Chamber: A Column: La Methode Des Baton," *Cryptologia* 4 (1980): 240-247.

37. (U) Hooper's power to do this may have been based on the connections he established earlier in his career when he was the head of the Bureau of Engineering's new radio-sound division.

38. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 80. U.S. Navy-Office of Information, Biographies Branch, 13 February 1958, "R. Adm. J. N. Wenger, USN, Ret."

39. (U) NSA RAM File, OP-20-G to Chief of Naval Operations, "Cryptanalytic Machines – Photocells," November 11, 1931.

40. (U) Photoelectric sensing for "sorting" has a long and complex history. See, for example, the patents of Michael Maul of Berlin dating from at least 1927 which were assigned to IBM. See U.S. patents 2000403-4. A Westinghouse engineer created an optical card sorter that caught Hooper's interest, *Electronics* 3 (October, 1931), 157. The 1930s work of the German, Emanuel Goldberg, who also invented the microdot, became of great significance to Bush's plans after World War II. Michael K. Buckland, "Emanuel Goldberg, Electronic Document Retrieval, and Vannevar Bush's Memex," *JASIS* 43 (1992): 284.

41. (U) Among Hooper's and Wenger's recommendations was the exploration of the new statistical-mathematical techniques being used in the

advanced sciences. Although professional mathematicians were not brought into OP-20-G until the onset of World War II (such as Howard Engstrom, Andy Gleason, and Marshall Hall), at least the younger men at OP-20-G were sent back to school for classes in statistics in the mid-1930s. NARA RG457, SRH-355, "Naval Security Group History to World War II," 268. The influence of Lester Hill during the prewar years remains to be traced.

42. (U) By the early 1930s, some scientists were using tabulating machines for advanced calculating. G. W. Baehne (ed.), *Practical Applications of the Punched Card Methods in Colleges and Universities* (New York: Columbia University Press, 1935) gives an insight to some of the uses and some of the special devices attached to the tabulators. Also useful for an understanding of precomputer calculation are William Aspray (ed.), *Computing Before Computers* (Ames, Iowa: Iowa State University Press, 1990), and Arthur Norberg, "High Technology Calculation in the Early 20th Century: Punched Card Machinery in Business and Government," *Technology and Culture* 31 (1990): 753.

43. (U) NSA RAM File, McClaran to Director of Naval Communications', January 7, 1932. NARA RG457, SRH-355, "Naval Security Group History to World War II," 75. The code was put into operation in December of 1930 and, luckily for the Americans, used until late 1938.

44. (U) The pressures on OP-20-G multiplied because of a bizarre occurrence in 1930-31. The former head of the State Department's and Signal Corps' cryptanalytic agency, Herbert Yardley, published his infamous book, *The American Black Chamber*. It revealed the United States' ability to read various Japanese code and, perhaps, cipher systems. NARA RG457, SRH-151, "Military Study: Communication Intelligence Research Activities," 9.

45. (U) NSA RAM File, "McClaran to Director of Naval Communications," January 7, 1932.

46. (U) NSA RAM File, Huckins to Bureau of Engineering, "IBM Rental," May 15, 1933.

47. (U) Deavours and Kruh, *Machine Cryptography and Modern Cryptanalysis*, 212. Hooper was especially worried about Britain's new shipboard cipher machines in the early 1930s. NSA RAM File, Hooper to OP-20-G, "Cryptanalytic Machines," September 26, 1930.

48. (U) NARA RG457, SRMN-084, "The Evolution of the Navy's Cryptologic Organization," and SRH-264, "A Lecture on Communications Intelligence," by Capt. J. N. Wenger, USN, August 14, 1946."

49. (U) NARA RG457, SRH-151, "Military Study: Communication Intelligence Research Activities," 008.

50. (U) NARA RG457, SRMN-083, "Military Study of Secret Radio Calls, January 1938."

51. (U) Howeth, *History of Communications Electronics in the United States Navy: With an Introduction by Chester W. Nimitz*, 538.

52. (U) John C. Walter, "William Harrison Standley," in Robert William Love, Jr. (ed.), *The Chiefs of Naval Operations* (Annapolis: Naval Institute Press, 1980), 93.

53. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 99.

54. (U) Vannevar Bush, *Pieces of the Action* (New York: Morrow, 1970), 71, and Library of Congress, Papers of Stanford Caldwell Hooper, Box 16, "Binaural Sons of the C," June 1, 1934. One of Hooper's most valuable connections with the scientific elite was the "alumni" club for those who had worked at the two major sonar development sites during World War I. He quite possibly met with Bush in its informal context. He certainly had later contacts with Bush when they were both associated with the NACA. MIT was a major training resource of the navy during WWI, and it had the Pratt School of Naval Architecture. Karl L. Wildes and Nilo A. Lindgren, *A Century of Electrical Engineering and Computer Science at MIT, 1882-1982* (Cambridge: MIT Press, 1985), 393.

55. (U) NSA was unable to provide copies of the four Bush reports and the rest of files on Bush's work for the navy in the 1930s. As will be discussed, the later four general reports were for the design of the machine that became known as the Comparator. Bush's initial report to Hooper and Wenger was probably much more general and was most likely concerned with very broad issues of communications technology. Bush's oral history version of the negoti-

ations does not quite fit with other evidence, MIT Archives MC143 111a to 116.

56. (U) A useful long-term view of academic-military relations is Henry Etzkowitz, "The Making of An Entrepreneurial University: The Traffic Among MIT, Industry, and the Military, 1860-1960," E. Mendelsohn, et al., (ed.), *Science, Technology, and the Military* 12 (1988): 524.

57. (U) Ronald W. Clark, *The Man Who Broke Purple: The Life of the World's Greatest Cryptologist, Colonel William F. Friedman* (London: Weidenfeld and Nicolson, 1977).

58. ~~(C)~~ David P. Mowry, "Listening to the Rum Runners," *Cryptologic Quarterly*, 2 (1983), 27-50.

59. ~~(C)~~ Friedman seems to have found a way to make sure that Yardley would be unable to join the new army group. NSA CCH Series XII Z, "Memorandum on SIS, Formation of Cryptanalytic Group" from CCH Series XI K, Box 13, circa 1929-1939. David P. Mowry, "Listening to the Rum Runners."

60. (U) NSA CCH Series XI K, Sam Snyder, draft of proposed history "Machines in U.S. Cryptology Before World War II," 27 June 1975.

61. (U) NSA CCH Series XII Z, William F. Friedman, "Addenda on the IBM Sorter," circa August 1935.

62. ~~(C)~~ NSA CCH Series XII Z, William F. Friedman, "Invention of a Cryptanalytic Coincidence Counter," Signals Intelligence Section, 14 April 1937. NSA CCH Series XII Z, William F. Friedman, "Description of the General Principles of an Invention for Locating Idiomorphs and Isomorphs in Cryptanalysis," 14 April 1937.

63. (U) Robert F. Kohler, *Partners in Science: Foundations and the Natural Sciences, 1900-1945* (Chicago: University of Chicago Press, 1991). Robert F. Kohler, "The Ph.D. Machine: Building on the Collegiate Base," *ISIS* 81 (1990): 638-662.

64. (U) Robert F. Kohler, *Foundations and the Natural Scientists, 1900-1945*. Roger L. Geiger, *To Advance Knowledge: The Growth of American Research Universities, 1900-1940* (New York: Oxford University Press, 1986).

65. (U) Larry Owens, "Straight Thinking," 78-79.

66. (U) Rockefeller Archives, RG12.1, Diaries of Warren Weaver: May 1, 1940 "Atanasoff Visit"; October 24, 1939, "Tour of Computing Centers"; "Visit to Boston," October 29, 1939; October 5, 1939, "Howard Aiken Visit"; May 24, 1939, "Visits of Harrison and Caldwell"; and January 1, 1939, "Visit to MIT."

67. (U) Daniel J. Kevles, *The Physicists: The History of the Scientific Community in Modern America* (New York: Knopf, 1978), 296.

68. (U) An important article on the history of both mechanical and electric-electronic fire control devices is A. Ben Clymer's, "The Mechanical Analog Computers of Hannibal Ford and William Newell," *Annals of the History of Computing* 15 (1993): 19-34.

69. (U) Carroll Pursell, "Science Agencies in World War II: The OSRD and Its Challengers," in Nathan Reingold (ed.), *The Sciences in the American Context: New Perspectives*, 359.

70. (U) On Deeds, Isaac F. Marcossen, *Wherever Men Trade* (New York: Dodd-Meade, 1948), and *Colonel Deeds: Industrial Builder* (New York: 1947).

71. (U) Copies of his patents were located in Bush's files at the Library of Congress.

72. (U) Library of Congress, Papers of Vannevar Bush. Bush had copies of various Hofgaard patents in his papers.

73. (U) There is no evidence on whether or not Bush and Deeds knew that IBM was beginning to explore electronic calculation, but they must have been aware, because of patent claims, of IBM's growing interest in microfilm and allied devices, including a "statistical" machine. Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* Trial Records, Chronological File, March 1937, letters re: visit of Green and Sullivan to MIT to view electronic work.

74. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* Trial Records, May 19, 1938, Bush to Deeds "Center of Analysis." A general overview of the machine and project is in Brian Randell (ed.), *The Origins of Digital Computers: Selected Papers*, 3rd ed., 294, and Bernard Williams, "Computing With Electricity, 1935-1945," (Ph.D. Thesis, University of Kansas, 1984), 137-170.

75. (U) Hagley Museum and Library, Accession Records, Deposition of Joseph Desch; Electronics Research that Bush asked if he wanted a job at NCR. *Honeywell v Sperry Rand* Trial Records "Report of Joseph Desch on Electronics Laboratory to H.N. Williams." August 16, 1938, Eugene Kniess, "First Lab Rediscovered," *NCR Dayton* 6 (1973): 1-3.

76. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* Trial Records, Desch Deposition, "Report of Joseph Desch on Electronics Laboratory to H. N. Williams," August 16, 1938.

77. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* Trial Records, Desch Deposition, and Reports of April 28, 1939 and March 25, 1940. Smithsonian Interviews with Desch and Mumma.

Chapter 2

(U) The First Electronic Computer: Perhaps

(U) A Reminder of Hooper's Hopes and Frustrations

(U) The development of new cipher machines and the maturation of radio led to a critical data problem for America's cryptanalysts. There was more and more data, and it was overwhelming those who were charged with turning it into useful information for policymakers. The failure to predict the attack on Pearl Harbor, for example, was the result of too much data. The thousands of intercepted Japanese naval messages could not be analyzed with the men and equipment available to Laurance Safford's OP-20-G.[1]

(U) Vannevar Bush realized the similarity between the challenges facing the cryptanalysts and the ones faced by those who were trying to reform the way the nation handled scientific information. He believed the two groups could share technology and methods. Captain Stanford C. Hooper might not have been aware of the trends in scientific literature, but he was certainly frightened by increasingly sophisticated cipher machines being introduced by potential enemies. That was what led him and his protege, Joseph Wenger, to Bush in late 1935.[2] Despite Hooper's vision and Wenger's efforts, OP-20-G began World War II without any operating high-speed devices. The Rapid Analytical Machine project had to begin over again in 1942 and in conditions ill-suited to long-term development.

(U) The reasons for the failure of Hooper's 1930s plans for the application of scientific/mathematical methods to codebreaking are complex. Bureaucratic tangles, bad luck, personality clashes, Bush's stubbornness, international crises, and the intransigence of technology partially account for the lost opportunity. But the major factor was institutional. Above all else, the military had not yet placed great faith in the kind of information that cryptanalysis or other signals intelligence could provide.[3]

(U) The Institutional Context

(U) By the mid-1930s, Hooper and his admiring young officers feared that America would be dragged into a war while Naval Communications was unprepared for a face-off with any power. Hooper's 1930s strategy, to collaborate with universities and corporate centers, was an attempt to compensate for the lack of money needed to prepare for a modern war. The Chief of Naval Operations supported his plans, but the CNO approval did not mean smooth sailing for Hooper and his men. To Hooper's regret, OP-20-G continued to have to depend on the Bureau of Engineering because navy law and "G's" pauper budgets allowed little else. More independence and money might have come to OP-20-G if there had been widespread faith in signals intelligence. But despite the contributions of Herbert Yardley's Black Chamber during the 1920s, then OP-20-G's penetration of Japanese naval codes, and then the cracking of Japan's diplomatic messages, codebreaking remained a stepchild of the American military.[4] Ironically, the reading of the Japanese naval and diplomatic code and cipher systems during the 1920s and 1930s masked the need for the long-term programs required for the development of advanced methods and machines. Even the navy's operating cryptanalysts did not lobby for such a program.[5] Only two men, Hooper and Wenger, saw the need and were willing to suffer the possible career penalties imposed on those who became advocates for unpopular causes.

(U) Hooper and Wenger had never abandoned their 1930 hopes for machines that would

be much more advanced than the tabulators.[6] In late January 1936, Wenger met with Bush and discussed OP-20-G's hopes and problems.[7] Bush presented Wenger with a handwritten eight-page outline of his plan for automating OP-20-G's cryptanalytic section.[8] Within a week, Wenger had secured the new Director of Naval Communications's approval of the proposed relationship with Bush.

(U) The First Defeat: Bush Is Rejected

(U) Just as Wenger proudly submitted his own visionary outline for the reorganization of OP-20-G, he received a slap in the face. The Bureau of Engineering refused to approve the agreement with Vannevar Bush![9] There was reason for the bureau's alienation. What Bush demanded and what Hooper and Wenger agreed to were startling. Bush demanded having the government pay the bill while he remained free of supervision. He wanted the relationship with the navy to match the ideal relationship between university researchers and major private foundations. The researcher would submit a general proposal and then be funded without any interference from the grantor. Following on his beliefs, Bush had refused to sign a typical navy contract or to make any promises about the results of his work.

(U) In addition, the original understanding did not include a promise to construct any machinery. Bush and Wenger had also agreed to ignore the regulations demanding competitive bidding on naval contracts. In addition, Bush requested what was an enormous amount of money in the era, at least for the navy. To hire Bush meant taking precious resources from the bureau and from OP-20-G.

(U) A Machine Too Soon

(U) There were also serious technical objections. Although only the barest sketch, Bush's early 1936 proposal showed that he wanted the navy to use optical scanning, high-speed data tapes, electronic computing, and microfilm in a series of increasingly complex cryptanalytic machines. Such technologies, Bush emphasized, would allow processing speeds from ten to one hundred times faster than the tabulators. Engineering thought that his recommendations were speculative and liable to be very costly failures. Engineering's staff had good reason to be worried about the technical ideas. The core technologies Bush recommended were, to significant degrees, still experimental.

(U) Also, the bureau's engineers claimed they had their own solution to the problem of automatic cipher machines. They were reluctant to give Wenger even a hint of their approach, however.[10] Whatever its secret alternative to Bush's proposals, engineering had accepted the tabulator. It was an off-the-shelf technology that had a stable manufacturer. IBM knew the ropes of government contracting and was investing in ongoing development with its own funds. Many of engineering's men were already creating significant and clever modifications to IBM's machines, making them more effective cryptanalytic tools.

(U) In addition, the views of OP-20-G's cryptanalysts were not in complete harmony with Wenger's. The operational cryptanalysts wondered who could steal the time to devise the new procedures necessary to make such strange technology useful. By the mid-1930s, Laurance Safford and Jack Holtwick became more allies than enemies of Hooper's long-term plans, but the remainder of the staff were willing to join with engineering in seriously questioning the value of Bush's machines.[11] All the objections and emotions meant that by mid-1936 the attempt to bring electronics to American cryptanalysis was deadlocked, if not defeated. But Stanford Hooper, Vannevar Bush, and Joseph Wenger collected the needed political support, drew up a new plan, and outflanked the bureau and the conservative cryptanalysts.

(U) Hooper and Wenger developed a new strategy to surmount any remaining objections. To placate the engineers, Hooper agreed to ask Bush to submit a more detailed and specific proposal. The new Bush proposal was submitted to a special research group in the navy rather than to engineering. In September 1936, within a week after he received the new plan, Hooper reported to Bush that the prestigious research board had approved his project. Wenger and Bush developed compromise positions on the bureaucratic and legal objections, then presented the new proposal to engineering. The bureau gave in, but it took almost all of October and November 1936 to draft an acceptable contract.

(U) Under 1937's formal contract, Bush agreed to focus on the details of a particular device so that engineering could have something concrete. He was to submit four reports, each detailing a major component of the proposed machine. The commitment to details and the year and one-half time limit for delivery of all the reports helped to satisfy the bureau's demand for a scheduled product.[12]

(U) The Decision to Build a Machine

(U) Bush had become attached to Wenger and Hooper, and their pleas convinced him to make a gentleman's promise that he soon regretted. He told them he would try to build a machine, and if he succeeded he would give it to the navy at no additional cost, except for shipping charges for the finished machine.[13] It had become very important to Wenger to have a device. To ensure that his project would not die when Bush's contract ended, Wenger needed a machine to prove that photoelectronics was practical.

(U) Bush was not sure that he could build a machine in time, but in early 1937 he was absolutely sure of one thing: MIT's work for OP-20-G would be cut off by mid-1938 when the contract with the bureau terminated. During the year of bickering with the navy, Bush became involved in an increasing number of projects that were critical to the Institute's planned analysis center and his career. One consequence was that the navy's project became more of a burden than an opportunity.

(U) Bush spent much time on the initial designs for an astounding general-purpose electronic digital computer. He sent his students and colleagues the first of several outlines of the proposed digital device, soon to be called the Rapid Arithmetical Machine, in January 1937.[14] In the three years after the first contacts with the navy, Bush and his men had put all the years of struggle behind them. Bush had his "boys" immersed in three highly innovative digital projects: the electronic Rockefeller Analyser; the electronic, programmable Rapid Arithmetic Machine; and the Rapid Selector.

(U) Bush and Wenger Select a Problem

(U) Bush consulted with Joseph Wenger and opted for a device to help OP-20-G apply the latest statistical techniques to the cipher problems.[15] Bush knew that if a machine was built, it had to be one that was reliable enough to convince the bureau to fund a long-term RAM project. Furthermore, Bush knew that any machine he created would have to outperform OP-20-G's tabulators and the special mechanical devices [16] that had become so dear to many of its staff. His machine had to be much faster than the electromechanical devices.[17]

(U) There were many advanced cryptanalytic methods for Bush to select from. Perhaps unknown to Bush or Wenger, the United States Army's cryptanalyst, William F. Friedman, was toying with ideas about the use of optical scanning. In April 1937, just as Bush was filling in the design of his machine, Friedman filed a patent for a system. The application did not mention cryptanalysis, and its examples of possible use were related to analog business applications, such as the sorting of packages, but Friedman must have

realized that optical scanning had great potential for cryptology.[18] Despite such projects, Bush was facing the great challenge of creating what was the world's first high-speed cryptanalytic machine. Balancing all the factors, including his almost unshakable commitment to the three technologies of film, optics, and electronic counting, Bush decided to automate one of the most central new statistical methods, the Index of Coincidence.

(U) The Index

(U) The method Bush and Wenger selected for the machine, the Index of Coincidence, was the most ubiquitous of the new theoretically justified statistical procedures. It was a formal and universal method that could not be made worthless by a slight change in a cipher system. It was based on the laws of probability. The Index was rugged and independent because it needed only intercepted cipher text and because it could attack any type of cipher system.[19] It also had a wide range of powers.

(U) The Index allowed an analyst to identify messages or portions of messages that were produced by the same settings of an encryption device. That was a first step to determining the wiring and settings of the encrypting components of the machines. The Index of Coincidence could then be put to work to identify a cipher key or the order of the cipher wheels in a machine. Such new methods were essential to an independent attack on the cipher devices. The stepping switch and wired-wheel machines, such as the Japanese Purple and the German Enigma, were designed to be unbeatable. They had cascades of transposing rotors which repeatedly changed one letter to another. Although each rotor was simple, together they produced a long sequence of letter substitutions without repetition or pattern.

(U) Such machines as Red, Purple, and the Enigma came close to creating a random sequence, but not quite. They appeared to be random because of the length of the cycle of unique substitutions created by the three or four rotating enciphering wheels or switches. But after 26 x 26 x 26 or more rotations, the wheels returned to their initial positions, and the machine began to repeat its letter substitutions. That made them technically nonrandom and allowed many nations to use Index methods against the simple Enigmas of the Spanish Civil War.[20] However, every nation was improving its cipher machines. Additional wheels with unique transpositions, varied latches that turned a neighboring wheel erratically, and plugboards to further disguise a machine's input-output relationships were added to many devices. The combinations of wheels, wheel settings, and plugboard links meant that trillions of possibilities had to be explored.

(U) In response, cryptanalysts countered with various forms of automation. But most, like Poland, bet on limited methods and machines, ones to exploit the quirks of particular cipher machines or the procedural errors of the enemy. There was good reason for such a turn away from science. The German specialists in charge of the Enigma, who were aware of the laws of probability and also of the speed of film and optical machines, were confident that it would take any formal attack too long to be of use to an enemy. Given the special defenses built into the Enigma, they calculated that it would take any machine so long to perform a statistical analysis that by the time a setting was identified, its messages would be of no military value.[21]

(U) When Wenger met with Vannevar Bush in 1937 to decide exactly what type of machine to design, his goal was the creation of a device so rapid that pure statistical analysis would be practical. After balancing the needs of OP-20-G and the technological possibilities, he and Bush decided to automate the heart of the IC method, coincidence counting.

(U) A coincidence was the appearance of the same letter in the same relative position in two or

more messages or in an offset of two copies of the same message. The method could be extended to the identification and counting of more than single letter matches, but the essence of the Index was the counting of single coincidences. If the number of matches exceeded the number expected from a random distribution of letters, then both messages were probably a product of the same wheels, wheel settings, and portion of the encryption machine's cycle.

(U) As the enciphering machines became more complex, the Index developed an almost insatiable demand for data. The Index could be computed with electromechanical machines, such as a counting sorter or a tabulator with additional relay circuits. But even with the IBM machines, the process was very slow and labor intensive; a long message could take days to analyze. One of the reasons the Index was selected as the method for Bush to automate was that it was so difficult to perform on electromechanical equipment.

(U) An Added Bonus, Possibly

(~~S//SI//REL~~) Wenger and Bush were committed to mechanizing the IC method, and both wanted to encourage the navy's codebreakers to apply mathematics, but Wenger realized that the operating codebreakers had to use some less than "scientific" approaches. If Bush could automate them, the MIT machine and statistical methods might receive a friendly evaluation by the crew at OP-20-G. Bush agreed to sketch machines for those rather crude methods, and he hinted that he would try to have the proposed Comparator (for the IC) be able to perform two of them. Both methods, the Brute-force search and Symmetrical-sequences, asked for a search through massive amounts of data to "locate," not count, coincidences. The coincidences sought were not based on individual letters, but matches between relatively long strings of cipher text or long strings of text whose letters had been transposed into their position relative to the starting letter of the string. Both approaches were ways to identify messages that were likely to have been produced by the same key. They were used to find messages that were in "depth." No mathematics was required; a machine just had to sense the long coincidence and then inform its operator where it was located.

(U) Bush Outlines the Machine and Sets Difficult Goals

(U) After the navy contract was signed in January 1937, Bush took time away from his other duties to work on the architecture of his Index machine, the Comparator. He decided to divide the project into four major parts corresponding to functional units of the proposed machine. Then, he chose what hardware was to be used in each. Last came an equally challenging step, finding the four men he needed to fill out his sketches and, perhaps, build a machine.

(U) Bush had a frustrating time finding qualified men. The need for secrecy made it almost impossible to locate men and still maintain good relations with the faculty. Only three people at MIT, really two, knew what the work was for. Bush and the project manager knew details, but MIT's president learned only that secret work was in progress. The men who were to build the components and their regular faculty supervisors were not told of the navy connection. Once employed, they were instructed to be confidential about their work but not told why. They would never be informed as to what their components were for.[22]

(U) Two graduate students received the initial assignments. Jerry Jaeger, who had a background in machine tools and automatic controls, was given the first task, to build the critical input mechanism. Richard Taylor, who was already important to the Rockefeller project's electronics and who would soon take charge of the Center of Analysis, was chosen to be responsible for the electronic circuits. The third man, who was asked

to develop the component to read the data tapes, was in a somewhat different position at the Institute than Jaeger or Taylor. Herbert E. Grier was a graduate of 1933 who remained at the Institute as an unpaid research associate. Bush was unable to find the needed fourth man among the student body. He turned to one of the Institute's machinists, Walter Kershner, to design and construct what seemed to be the least challenging part of the Comparator, its data input device. Kershner probably had been working on a similar automatic tape punch for the Rockefeller Analyser.

(U) Finding a manager for the project was a greater challenge. It was not until early summer 1937 that Bush thought he had a lead on a qualified engineer: Waldron Shapleigh MacDonald.

(U) MacDonald was one of the most unusual and fascinating of MIT's students, and he remains an unrecognized figure in the birth of the modern computer. MacDonald first appeared at MIT in the early 1930s when he enrolled as a special undergraduate student. His initial year in Cambridge was spent trying to prove to the electrical engineering faculty that his lack of formal preparation was not a barrier to academic success. Although he performed well in his classes, he was unable to surmount bureaucratic hurdles, illness, and the depletion of his savings. He had to leave MIT without a degree. But he quickly found very well-paying work as an engineer and began a lifelong career as an innovator in computers and automatic controls.

(U) Bush offered MacDonald a professional salary and help in obtaining a master's degree in electrical communications at the Institute. In return, MacDonald was asked for a firm commitment to come to MIT to see the navy's project through to completion. But MacDonald needed time to fulfill his existing responsibilities, and he did not arrive at MIT until September 1937, leaving only some ten months to become oriented, to check and revise the Comparator's parts, prepare reports, and assemble and test the historic machine.[23]

(U) MacDonald's ingenuity and his hands-on engineering ability were needed on the navy's 1930s project, but his role was not a truly creative one. Well before he arrived in late 1937, the design of the machine and the schedule for the project had been determined. His job was to make what Bush had specified come to life and to do it before the end of the navy contract. Unfortunately for MacDonald, he inherited a fixed design, components which were hastily made by others, Bush's order to "get the job done on time," and full responsibility. By September 1937 Bush was already too busy with his other work to attend to the now rather inconsequential navy project. Among other things, Bush was readying himself to assume the leadership of the powerful Carnegie Institution.

(U) The Comparator Really Doesn't Go to Washington

~~(U//FOUO)~~ Bush and Wenger were very wise in setting the limited goal of a machine for the Index of Coincidence. Electronic computation was having its birth pangs, and no one had a way to create a machine whose hardware could be made to imitate any process. A major reason why all the 1930s computers were limited in function was the absence of a viable memory technology.[24] A universal data computer, one that worked on large volumes of input and that had high-speed memory, did not appear until the 1950s. Then, machines such as the UNIVAC depended upon very demanding, slow, and expensive, magnetic tape memory systems.[25]

~~(U//FOUO)~~ Bush's first sketches of his Comparator reflected the limitations of the memory and electronic technologies. Each of the Comparator's four major components had its own very significant practical challenges. The state of the technology did not allow elegant solutions to the problems of high-speed input, sensing, count-

ing, and recording. Because of the conduct of the 1930's Comparator project and the nature of OP-20-G's early wartime efforts, it was not until late 1943 that America had more than the patched-up Bush Comparator to represent its nearly fifteen years of attempts to build sophisticated electronic codebreaking devices.

(U) Too Much to Ask of Mere Machines

~~(TS//SI//REL)~~ The Index was a demanding cryptanalytic method. To tally all the possible single letter coincidences in two messages calls for (n*(n-1)) comparisons.[26] If two four-letter messages are examined for coincidences, twelve comparisons must be made; 500 messages demanded almost 250,000 tests; a 2,000-letter message called for almost 4,000,000. Complete analyses of long messages could take days or weeks by hand and tabulator methods. Compounding the challenge of raw speed was Wenger's demand that the Comparator be able to handle the longest messages. There was good reason for that because the more characters in a message the more likely that something of value would emerge from an analysis. Fortunately, cryptologists around the world knew that messages with too many words posed a danger to their systems and instructed that messages be limited to as few words possible. The very upper limit was 2,000 characters. Messages of 200 characters were typical, but the need to analyze longer ones in a timely way made speed and a large memory important goals.[27]

(U) Combined with Bush's desire for a minimal number of electronic components, the call for speed created unexpected challenges for the students at MIT. One of them was printing. To maintain speed, printing had to be done while the tape was running. The solution Bush and his men devised was sensible but crude, and it led to a need for an even faster mechanical tape drive. Printing was to take place while a blank portion of tape was running. In practice, this meant that approximately one half of each tape was blank, thus halving the number of possible comparisons during a run of the tape. Because of that, Bush's men had to double the originally planned speed of the drive to achieve the processing goals.[28]

(U) Even without the tape handicap, Bush had to outdo much existing technology to achieve his minimum Comparator speed.[29] Bush wanted the machine to deliver data to the reading station at over thirty times the rate of standard telegraph equipment and sixty times faster than a movie projector if it was to reach the goal of 20,000 comparisons a minute. Even in the late 1940s, the most sophisticated high-speed transmission "baud rates" were in the range of 1,800 characters a minute – or more than ten times slower than Bush needed in order to make the navy machine an attractive alternative. There were special high-speed drives for sending bulk messages, and during World War II "flash" systems were developed. Those devices, however, were not proven in the mid-1930s. The talking picture industry did not provide much help. In the 1930s, moving picture film was moved at less than 300 feet per hour.[30] The Comparator had to sense and route data at rates forty times greater than an IBM sorter and 160 times faster than a tabulator.

(U) Wenger thought that he might overcome the bureau's protests if Bush could add parallel features to his essentially serial machine. Wenger asked him to try to include what would be needed to make isomorphic and three- and four-letter (polymorphic) coincidence tests that had been discussed earlier.

~~(TS//SI//REL)~~ Wenger also gave his approval for the "locating" feature. It would allow what the World War II cryptanalysts called "brute force" searching. Masses of data could be scanned at every position of two messages with the hope of finding indications that two messages had been enciphered with the same key.

(U) No Thanks for the Memories

(U) Because the Comparator was a data-dependent machine, the greatest problem facing Bush's students was how to store and retrieve information. The Comparator needed a large-scale and very high-speed memory, but such memories did not exist in the 1930s.[31] What was on the technological horizon was not encouraging. Storage in massive banks of capacitors or resistors, which some computer designers were thinking of using, was too expensive, and such banks took too long to load and unload.[32] The rumors about the use of special versions of television tubes as memory were just that in the mid-1930s. And no one thought that delay lines would ever be able to hold more than a few bits of information. In 1937 work was just beginning on magnetic memories, and storage of large amounts of data in two or multistate electronic tubes or relays was out of the question.[33]

(U) Unfortunately for Bush and Wenger, there had been few advances in tape technology since the introduction of modern automatic telegraph readers in the early twentieth century. Standard teletype technology had not evolved into a competitor to the punch card.[34] In early 1937 the only option seemed to be microfilm.

(U) Bush thought his men would overcome the difficulties caused by film shrinkage and distortion when the film was sped past a reading station.[35] Unfortunately, microfilm proved too difficult for a machine that could meet the mid-1938 deadline for the delivery of the Comparator. As a result, in mid-1937 Bush sent his students on a hurried search for another medium and a way to move it at incredible speeds. The MIT men chose a unique 70mm-wide paper tape that Eastman-Kodak used for packaging its movie film. It was strong, wide enough to accommodate Bush's coding scheme, and, very important, it blocked light because of its acetate coating and its alternate red-black layers.[36] Also, early tests indicated the tape would maintain its structural integrity after being punched. All those features justified the high cost of the Eastman product although it was soon learned that its data capacity would not be much more than that of telegraph tape.[37]

(U) The disappointingly low density meant that much effort had to be put into the development of a high-speed tape drive, one burdened with some very special demands. In addition to the need for ultra-high speeds, the tape transport had to pass two tapes in perfect alignment over the reading station, then step one tape one character relative to the other until all possible comparisons had been run.[38]

(U) The Limits of Mechanics

(U) The first man on the summer crew was given the responsibility of creating the mechanical combination needed to compensate for the low data-carrying power of the Eastman tape. Already familiar with the drives in the machines used in the cloth and newspaper industries, the young engineer decided to center his component on a four-foot long frame to hold the tapes. Pulleys were to maintain the required tension on the loops of tape. Driven by a fast electric motor and a system of shafts and gears, the tape was guided by both rollers and sprockets.[39] The entire transport was mounted on tall legs and stood some four feet off the ground to ease the chore of changing tapes.[40]

(U) The tape transport was well designed and was delivered on schedule, but it did not reach the speeds Bush desired. At its best moments it ran at less than two and a half miles an hour, not the five or more needed for a truly rapid machine. The tape was the machine's timer and set many of the requirements for the other major components. Once its features were known, work on the reading station and electronic counters could be completed. Armed with Bush's previous instructions and the specifications for the tape drive, the next man tackled the problems of photoelectric sensing.

(U) Let There Be Light, But Not Too Much

(U) One of Bush's first technical commitments was to the sensing of the presence of light rather than its absence. Following on that, he ordered his men to code each letter of a message by punching a hole in a column of the seventy-millimeter wide tape. There was to be only one hole to a column of twenty-six fields. An additional field in each column served as a timer. If a column held data, this extra field was punched. When two active columns overlapped, light was directed to a timing cell which then readied the sensing photocells to examine many data columns simultaneously.

~~(C//SI//REL)~~ There were to be at least ten data columns, thus letters, packed into a linear inch of tape. To accommodate Wenger's need for counting more than single coincidences, ten letters were to be read at one time. This called for ten photocells for message characters, one to each column.

(U) The engineer had to create a mask to ensure that light that shone through the first tape did not drift before it fell on the lower one. He also had to find a lens that would direct the light beams from overlapping holes, one for each column, onto the correct sensing photocell. An allied problem was more challenging: he had to keep light from a coincident column from spilling over into the area of another column's photocell. The state of photocell technology did not allow easy solutions to any of the reader's problems. Among other problems, they remained fairly large. As a result, the young MIT engineer could not put ten of them directly under the columns of the Comparator's tapes. They had to be placed far under the reader and were arranged in a "U" pattern. That meant that the straight, parallel light from the coincident columns had to be accurately deflected. Moreover, complete electronic packages for the photocells were not supplied by manufacturers. The MIT engineer had to tune each photocell and build the amplification circuits to turn the signals from the photocells into the discrete pulses needed by the third major component of the Comparator, the electronic counters.

(U) The Most Difficult Problem of All, But It Wasn't

(U) With the knowledge of the tape and photocell systems, the third young man began his work on the final details of what everyone thought would be the most difficult part of the project, its electronic counting system.

(U) Precise digital counting with electronics was in its early years, and all attempts at creating tube-based calculating circuits were risky. Electronic tubes were designed for analog work, and it was only empirical tweaking that allowed them to be on-off switches. As late as 1940, the best experimental electronic counters worked at 20,000 decimal counts a second during their cooperative periods.

(U) One of his greatest challenges was the circuitry for the Comparator's parallel-processing feature. It was needed to allow the machine to perform the simultaneous multiple letter tests that were so valuable to the cryptanalysts. Without parallel processing, the machine's power would be reduced by a factor of four. The student engineer had to construct five independent electronic counters which were to tap the data from the reading station at the same time. The young man took the safe technological route, choosing to stay with the predictable and familiar gas-filled Thyratrons.

(U) The choice of architecture for the counters was also driven by the need to send the navy at least a feasible design, if not a machine, by mid-1938. Like the other electronic computer builders of the era, the young MIT engineer decided to imitate mechanical calculating machines.[41] His counters were decimal, not binary. Although such a design limited the range of the application of a computer, it was known to work and was simpler

to construct than binary circuits. Each of the decimal counters was to consist of three or more rings of ten tubes with the needed electronics for arithmetic carrying, power, and control.

(U) Providing the option of performing several different analyses at one time meant additional challenges. Bush had designed the machine to allow the analysts to select the particular tests for each run. To permit this, the young engineer incorporated a set of "and" circuits that could be set to test for the desired combination. The Comparator's Rossi "and" circuit was the key to the machine's flexibility and parallelism.

(U) In addition to the counters and the "and" circuits, the third engineer was handed another tough job. He was given the responsibility for creating the banks of electrical relays needed to stand between the high-speed tube counters and the much, much slower printer. At the end of each pass, the counters had to be polled for their contents and numbers sent to the relays. The relays worked as a short-term memory, sending pulses to the magnets that controlled the print bars.[42]

(U) The Easiest Becomes the Most Difficult

(U) There was a fourth man. He was in charge of the crucial data-entry system. The punch for the data tapes proved to be the Achilles heel of the Comparator. The problem was a perhaps inescapable result of the use of paper tape, as was Bush's inefficient 1 of 26 coding scheme.

(U) The technology of the 1930s led him to reject a method of coding that could have increased densities on the tapes by at least a factor of five and that would have led the Comparator's codes to fit with the navy's modern communication system. The use of a five-field character code, the Baudot code, would have allowed at least five letters to be placed on a line (column) of the 70mm tape. But the size and sensitivity of holes and photocells, the problems of aligning tapes, and the desire to limit the electronics of the machine precluded the use of that coding pattern.[43] Bush's special coding scheme demanded a custom-made and very complex mechanism.

(U) An MIT machinist was instructed to make a keyboard-operated device to simultaneously punch two exact copies of a message. It had to keep the two tapes in perfect synchronization and to make precisely spaced tiny holes in each column and row. The punch had to advance the tapes with absolute precision. Most challenging, it had to maintain the integrity of its tiny and sharp needle-like punching arms despite the impact as the arms struck the Eastman tape. The machinist was asked to devise tape cutters and the means to ensure that the spliced ends of the tapes would not pull apart during the runs. Unfortunately, the punch was the last component of the Comparator to be turned over to the project manager and then it was "not satisfactory."[44] The punch's inadequacies cannot be blamed on the machinist; the responsibility has to be placed on the original design for the Comparator. Between 1938 and 1945 several teams of engineers tried to produce a viable data entry system for the paper tapes; none was able to build a rugged and reliable punch.

(U) Beyond Murphy's Law

(U) When Waldron MacDonald arrived in September, three student engineers had already sent their work to local machine shops. Bush trusted their judgment so much that, without examining the parts, he put MacDonald to writing the descriptive reports for the navy. MacDonald took Bush's first schemes for each component, added what the students had done, and sent the reports to the navy for payment.[45] The reports, including the final one submitted in the spring of 1938, were upbeat and gave the specifications for what everyone thought would be the first operating electronic data processing machine.[46]

(U) Although the reports contained a bright picture, the Comparator project had fallen victim to a host of problems. But the main reason for the problems in 1937 and 1938 was the technologies Bush so admired. They were not ready to be turned into useful machinery. Unfortunately, the results Bush and his young men expected on the basis of their early bench tests did not carry through to the parts they gave to MacDonald. The Comparator was far from ready for assembly. And only MacDonald was left to rescue it! MacDonald had much, much more to do than simply link the components together. Almost every component had to be reworked.

(U) MacDonald put much thought and energy into reshaping the electronic components, and he more than fine-tuned the tape transport. More basic work had to be done on the reader. The optical system needed a complete overhaul, and it took much of MacDonald's attention. To bring the correct amount of light to each of the ten cells, he devised a 1930's version of fiber-optics.

(U) Thus, MacDonald's assignment turned into something much more demanding than either he or Bush had imagined in mid-1937. MacDonald was not sure that he could solve all the problems of the transport, counters, and optical sensors. Then chance compounded an already difficult situation. In a friendly game of touch football, MacDonald was knocked out by an unlucky "poke on the jaw." MacDonald remained unconscious and confined to bed for several weeks. His energy was seriously drained for months afterwards.[47] Despite the injury, Bush chose not to replace MacDonald.

(U) What Hooper had complained about for so many years, the lack of appreciation of science in the navy, again struck the Comparator. Wenger, the strongest voice for a revolution in the technologies of signals intelligence and cryptanalysis, readied himself to leave for sea duty in mid-1938. Wenger had to spend the five months before he was rotated putting the finishing touches on the detailed reports for Hooper's grand proposal for a modern communications system. Wenger left the country just a month before MacDonald shipped the troubled Comparator to Washington.

(U) In spring 1938, MacDonald began test runs on the rebuilt parts.[48] He also had the chore of instructing the engineer the navy sent to learn about the machine. Wenger had arranged for a bureau technician to spend some time at MIT. During the spring, Frederick Dulong, one of the many ex-navy men who stayed on in Washington as civilian employees, was sent to MIT.

(U) Wenger considered Bush very generous for having constructed a machine and approved Bush's suggestion that MacDonald be hired by the navy to fine tune the Comparator once it was in Washington. The bureau agreed and requested MacDonald to travel to Washington with the Comparator and to stay for three months. He was to adjust the machine and to instruct both technicians and cryptanalysts in its use. Safford, now in charge of the Comparator, was pleased that the bureau promised to give him some additional, if not permanent, help.

(U) As soon as Bush signaled that a machine would be sent to Washington, Wenger began expensive preparations. He requested the money for tapes and lights and extra tubes, and he readied an area for the Comparator within OP-20-G's secret rooms. In a few weeks, additional funds were requested for the hardware necessary to prepare the tapes for the Comparator.[49] Wenger went much further. Describing a new era in cryptanalysis, he convinced the navy brass to give serious consideration to funding more devices.[50] By the end of 1938, OP-20-G's budget request included more than $20,000 for additional Bush devices and special additions to the first machine.[51] In addition, "G's" new war plans contained a request for a Comparator for the pro-

posed major cryptanalytic station at Pearl Harbor.[52]

(U) Spring Is a Time for Love, Not Machinery

(U) When the Comparator arrived in Washington in late June, a month late, it would not start.[53] As bad, two of its most important parts had not been shipped – the punch and printer. About a month behind schedule and still only "semifinished," it found a new and well-intentioned guardian. But Fred Dulong could not give full attention to the machine. By mid-July, Dulong was able to run the counting circuits,[54] but any more work was stalled because of the missing punch and printer. Unknown to anyone, they had been placed in a Cambridge safe-deposit box by MacDonald to await his return to the country in August[55] following a honeymoon.

(U) The cryptanalysts certainly did not have the time to wet-nurse the Comparator. While the bureau's men bewailed the results of becoming entangled with an impractical professor, the cryptanalysts in charge of the day-to-day work were coming under incredible pressures to penetrate all of the sophisticated Japanese code and cipher systems. Japan's invasion of China in 1937 had made it clear that war was imminent,[56] and by 1938 OP-20-G was facing crisis conditions. The sinking of the *Panay* in December led to a scramble to protect American codes. In addition, there were hints that Japan was about to make another sweeping change in its codes and to introduce its Purple cipher machine.[57] What energies OP-20-G had were necessarily devoted to developing techniques and machines that gave immediate results. Its faith was, quite naturally, placed in the direct analogs of Japan's enciphering machines, and its men wanted resources devoted to modernizing the tabulators.

(U) Thus Waldron MacDonald did not arrive in Washington at the right time for any experimentation at "G" or the bureau. Driving from Cambridge in August 1938, he had the Comparator's punch and printer in the back of his station wagon. Working in OP-20-G's downtown offices, MacDonald attempted to save his and Bush's reputation.

(U) He hurried the Navy Yard's effort to build tape duplicators and splicers and soon convinced the bureau to build a new punch. The one from MIT could not be coaxed into working. Don Seiler took on that challenge.[58] Then MacDonald began working on the other components. Although no major changes were made to the Comparator, it took an unexpected fourth month of work to announce a finished machine in November.

(U) In late 1938, OP-20-G's leader, Safford, congratulated Bush and informed him the cryptanalysts and the bureau's men planned to spend the next year experimenting with the wonderful and reliable machine. Possibly because they now realized how much a well-schooled optical electronics engineer would cost, OP-20-G did not make an effort to hire a replacement for the MIT engineer or, as planned earlier in the year, to construct at least one more Comparator.[59]

(U) RAM Project Seems to Die, Late 1938

(U) With Wenger gone, no one pressed for an immediate extension of the program.[60] Bush, in turn, quickly fended off another attempt by the navy to link him to "G's" projects. The consequences of the failure to continue on with the Comparator project in 1938 were severe. Soon after MacDonald left Washington, the Comparator again became inoperable. It was so temperamental that the only attention it received was from Dulong, whose many other duties allowed just part-time work.[61] It was listed on OP-20-G's equipment roster in 1939, but it was never used, not even on the type of important project for which it had been designed, the breaking of the Japanese Purple cipher machine.[62] Its technical problems become so great that it was removed from the cryptanalysts'

quarters and sent to the Navy Yard where it could be tinkered with.

(U) Although overworked because of the Japanese code and cipher crises, Safford had asked for a report on the Comparator and received some very disheartening news. Dulong responded that nothing but the electronic counters proved reliable, and the machine had not been functional long enough to allow in-depth development of procedures. The Navy Yard's men did not think there was any possible quick fix for the device. Most ominous was the failure of the data entry component, the punch. Even the second version of that purely mechanical and supposedly simple mechanism could not be made to produce precise tapes. There was little hope of basing an entire system of analytical machines around the original Bush design if there was not an efficient and reliable data entry device.[63] In 1940, Safford, who two years before declared the Comparator a reliable and useful invention, had to admit the machine never worked and that the entire project had not progressed as planned.

(U) A Comparator There May Never Be

(U) In late 1940 Bush gained another chance to prove the power of optical-electronic machines and the ability of academics to create the technologies of defense.[64] He arranged for MIT's John Howard and his men to rescue the first paper tape Comparator and to design the long-promised microfilm version.

(U) This second MIT OP-20-G project of late 1940 is of extreme historical importance because it became the foundation for the United States Navy's incredible Rapid Machines Program of World War II. That little known adventure rivaled Britain's famous work on the Bombes and the Colossus.

(U) Tragically, that program is also important because of its failures. Although it began with expectations of producing electronic digital machines to attack the feared cipher devices of the Axis powers, it turned to older technology and logic. To be able to provide anything of value to OP-20-G, Howard's men had to step back from electronics, digital techniques, and microfilm. Although the navy's cryptanalysts began World War II with promises that electronics could be made to work, they had to wait for almost two years after Pearl Harbor before any machines appeared that affirmed that Bush's ideas had potential.

(U) The story of John Howard's navy project has to begin with the crises in Europe and Asia, policy decisions in the White House and London, and the organization of American science in World War II.

(U) Big Science Begins to Emerge

(U) Bush's high-science friends were active in more than the cause of research. They were among the nation's earliest supporters of a positive response to the German threat. They lobbied for the creation of the National Defense Research Committee (NDRC). The NDRC was the realization of Bush's ideal of how to link academia and the military. Given almost complete power by Roosevelt to shape the NDRC, Bush laid down ground rules that gave power to academics to begin research projects and to be free of military control. Having its own funds and being a presidential creature, the NDRC and its more powerful extension, the Office of Scientific Research and Development, could initiate blue-sky programs and carry them through to development.

(U) One of those programs interlaced the NDRC with American cryptanalysis, but only after it had dealt with a long list of projects of much higher priority. Atomic power and radar were the leading problems, and the scientists at the most prestigious universities and corporate research centers received the first calls from the NDRC's leaders.

(U) The executives at the NDRC realized that atomic research and the development of the potentials of radar called for advanced computation, but, alone, those problems would have led to a minimal NDRC involvement in computers. It was a lower priority challenge that plunged the NDRC into computer research and established who would participate in the navy's future Rapid Machine effort. Atomic scientists were calling for electronic control devices, but most important for the history of OP-20-G was the hope that radar could be used to automatically control antiaircraft weapons. That led to the NDRC's involvement in the development of electronic fire control computers in the early 1940s.[65]

(U) The exploration of such electronic digital machines was the perfect type of work for the NDRC because it centered on unproven and experimental technologies. The NDRC's scientists believed that digital electronics had potential, and they rekindled the fire control projects. Hundreds of thousands of dollars were poured into fire-control computer and atomic-counter work in the first two years of NDRC's life.

(U) Fire Control

(U) The NDRC began the first stages of its fire control project in June 1940. Bush's old friend Warren Weaver of the Rockefeller Foundation assumed command. The research at RCA, which had led to the design of the fastest binary circuits in the nation, if not the world, was picked up by the NDRC. Then Weaver coordinated the work at RCA with wide-ranging explorations at Eastman, MIT, Bell, and, to some extent, NCR. Of significance for the history of OP-20-G's machines, IBM was again left out of the NDRC circle although its centers of electronic research were working on quite advanced components and systems.[66]

(U) Because of the NDRC's stimulus, by the time of America's formal entry into the war, RCA, Eastman, Bell, and MIT had several proposals for digital-based fire control systems, ones the NDRC evaluators thought had great promise. In the spring of 1942, meetings were called, and all participants shared their knowledge and designs.[67] The reports of the fire control projects were made available to the American technical community, which now included John Howard. He was made aware of the designs for the most advanced computer components.

(U) Many of the fire control developments would find their way into cryptanalytic machines and into such pathbreaking computers as the ENIAC. By mid-1942, there were great hopes for the development of at least a prototype electronic gun controller. But Warren Weaver and his assistants concluded that digital electronics was too good. It was too fast and too precise for the guns used by the military. In July 1942 the fire control program was dropped – but with three important exceptions. The development projects for the Eastman film-based analog-to-digital signal convertor and RCA's fabulous multifunction Computron tube were to be continued, as was NCR's counting circuit research. Although they were viewed as long-term projects, the three efforts were financed for only a few more months because the press of other work forced the NDRC to abandon them.[68]

(U) The Second Comparator

(U) Meanwhile, just weeks after the work on high-speed electronic counters and fire control computers had begun, Bush and OP-20-G came together. A visit with Bush in early summer 1940 indicated a reawakening of interest in the original Comparator, which had sat unused at the Navy Yard for almost two years. But it was not until October 1940 that anything was done about its future.

(U) A limited and secondary role for MIT was unacceptable to Bush, however. He returned to his old demand for freedom from bureaucratic control, and, within a few weeks, he was able to reshape the first murmuring about a new

Comparator into a project that satisfied his ambitions. Bush wanted a prototype of a microfilm Comparator. While the first Comparator would continue to be a paper-tape, the second generation Comparator was to be centered about microfilm. Bush soothed Laurance Safford's anxieties about optical and electronic machines and told him that the new microfilm version of the Comparator would be delivered in time to be of use in the coming war. In late 1940, Safford encountered little resistance to the idea of transferring the project to MIT. The navy's cryptanalysts were too busy battling the Japanese naval code, and too worried about taking on the German systems to care about the loss of control over unusable machinery.

(U) OP-20-G and Ultra

(U) As early as mid-1940, the most important Americans were informed of some of Britain's promising though still limited powers over a few German cryptologic systems. But OP-20-G was not told how to break the Enigma or other important ciphers. Despite the British promise to share the information from Ultra, the Americans feared a British monopoly over Enigma. In addition, in early summer 1940 there were fears that Britain would collapse. OP-20-G's cryptanalysts worried they would have to assume responsibility for Enigma, something for which they were totally unprepared.[69]

(U) The U-boat threat had already led to British pleas that OP-20-G and Naval Intelligence shift their scarce resources to direction-finding and traffic analysis to compensate for their inability to read any significant German naval system.[70] The cryptanalysts in Washington thus had little time to waste on what some of them regarded as Bush's technological fantasies. The navy's engineers, already overworked creating analogs of encryption machines, building advanced radio equipment, and helping to revise OP-20-G's tabulators, were happy to be rid of the "college professor's" folly.

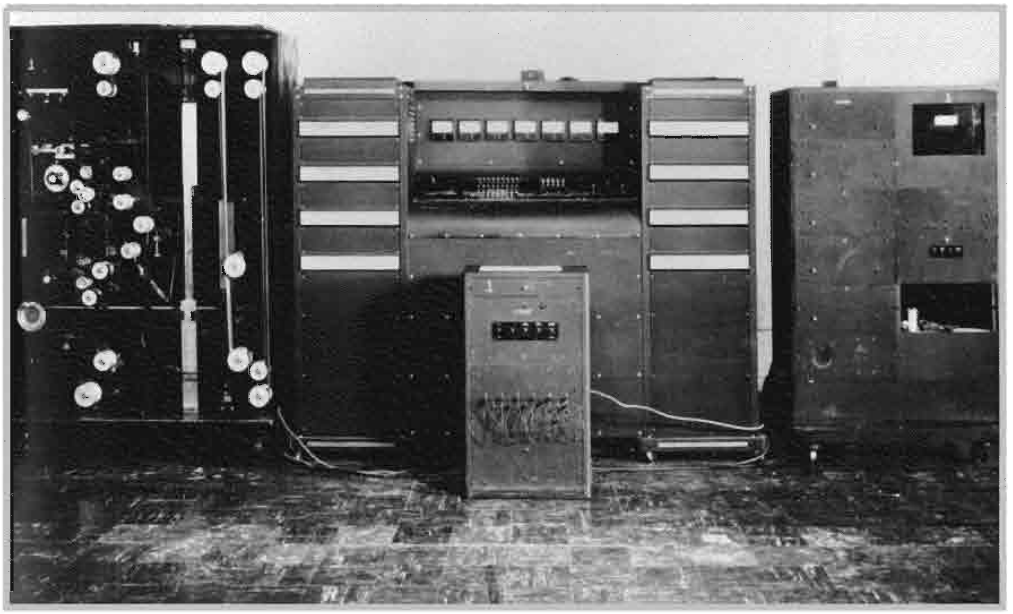
(U) The navy's bureaucrats were less happy about yielding control. They agreed to most of Bush's conditions although they did want a contract and agreed to have the MIT work coordinated through the navy's Office of Research and Inventions. The BuShips' (Bureau of Ships) demands in late 1940 were much less severe than in 1935, but it took some additional political maneuvering to put the Rapid Machine project back into the hands of the MIT students.

(U) Under the 1940 agreement with the Bureau of Ships, Bush had full control of the new Comparator project, and his men were to work at MIT, not at the Navy Yard. The navy also agreed to wait for the results of the new MIT work before considering the construction of any more Rapid machines with or without MIT involvement.

~~(S//SI//REL)~~ OP-20-G may not have told Bush, but it was not relying solely upon his ideas for machine processing; it had to protect itself through the use of older and proven technologies. The experienced cryptanalysts had insisted on a tabulator program, one that was to remain under their direct control. MIT's men were to have no say about the new tab projects. In early 1941 IBM was contacted about making the major changes in its machines required to allow its equipment to perform new tests. For example, relays were added to the machines to strip superencipherments from the Japanese code and to flag repetitions of code groups. By mid-year IBM was asked to do much more and to give OP-20-G very special attention.[71]

(U) Bush was finally able to circumvent the bureaucracy and go his own way, perhaps with ambitions to create a full Rapid Machine center at the Institute, one free of military interference.[72] The old Comparator was to be shipped to MIT for repair, and a new one was to be designed and constructed in Cambridge.

(U) Howard quickly became the man in charge of the Comparator project. Although the



(S) 70mm Comparator

future of Bush's ideas rested upon the new microfilm Comparator, the old paper tape machine and its punch became the focus of attention. The punch was a critical problem because its two previous versions were failures. Understandably, Howard urged his men to use caution as well as creativity, but the slow tempo of his project soon generated concern within the Bureau of Ships. During the first months of 1941, as time passed without results, the navy found it more and more difficult to accommodate having its project run by a civilian agency.

(U) So Long for So Little

(U) It took almost a full year to redo the old Comparator, the only Rapid Machine. It arrived in Washington three weeks after the Japanese struck at Pearl Harbor.[73] It may have taken longer than expected to deliver the old Comparator because of adding one new feature to Bush's 1938 design. The "locator" performed a function the navy had thought of adding in the late 1930s. It allowed the use of a transverse tape to find more complex pattern matches than was possible with the original system. With the locator, the codebreakers could quickly identify which messages held important code or cipher groups.[74]

~~(S)~~ In the private language of the codebreakers, "locating" was a Brute Force approach to finding possible "depths."

(U) Once in action in mid-1942, the old Comparator did help crack the Japanese naval attaché cipher machine, but the Comparator's newest punch also malfunctioned.[75] In addition, the machine's bad temper called for a visit by one of the MIT men, Larry Steinhardt, who had to simplify the device to achieve reliability.[76]

(U) The Search for the Second Comparator

(U) While struggling with the old Comparator, the young men at MIT paid attention to its new microfilm version. In early November 1941, the MIT-NDRC group was so positive about the future of a microfilm Comparator that Bush obtained another signifi-

cant grant from the NDRC.[77] Then, although the NDRC was not supposed to be involved in production, Howard awarded a $25,000 contract to National Cash Register's electronics laboratory. Joe Desch agreed to build as many as thirty copies of the sets of new high-speed counters and fast printers needed for the future microfilm Comparators.[78]

(U) In a November 1941 meeting, it was declared that construction was ready to begin on the next Comparator. Expecting to see the newest Comparator in a few months and viewing the MIT group as a long-term resource, the OP-20-G analysts outlined needs for other devices. One of those outlines had a hidden significance. It would connect the MIT men to the Ultra Secret although they did not know of Britain's ability to crack the Enigma nor of the critical negotiations between OP-20-G and Britain over sharing intelligence secrets.

(U) Not Equal Partners in Ultra

(U) Agreements were made at the very highest levels in 1940 and 1941 for Britain and America to share cryptanalytic methods as well as the military information that came from signals intelligence. However, England's wizards did not have a mathematical solution to the Enigma! Without good guesses as to key words in messages and knowledge of the inner workings of the Enigma radio networks, Britain could, and would, become deaf.[79]

~~(C//REL)~~ Perhaps it was the fragility of the solutions that made the British somewhat less willing to share their secrets with the Americans. Whatever the reason, the Americans began to think it was necessary to have their own anti-Enigma capability. In late 1940, OP-20-G shifted their one professional cryptanalyst, who had just made the first entries into the Japanese fleet code, to the German problems. The venerable Agnes Meyer Driscoll and three young navy officers began an attack on the frustrating German naval Enigma. However, they made little progress toward what the Americans needed, a purely mathematical cryptanalytic solution.

(U) Although she had helped break into similar devices, was informed of some of the British methods, and labored for almost a year, Driscoll could not find the ways and means for an American Enigma solution. Fortunately, she was willing to ask for help. During the November 1941 meeting between MIT and OP-20-G, she described her needs, and Howard was asked to think of ways to automate her "problem." She was determined to develop a method more permanent than the ones Britain had chosen. Apparently, that called for a machine somewhat different from the Comparator. Howard accepted the responsibility, and Driscoll was happy with the promises by the young men from MIT.[80]

(U) Agnes Meyer

(U) Another Machine That Wouldn't

(U) The cordial meeting with Howard in early November 1941 impressed OP-20-G's people. But OP-20-G and the Bureau of Ships became very worried and skeptical about university work when, just a few days after the Washington conference,[81] Howard wrote the navy that experiments were showing the new Comparator's microfilm to be deforming when used in test

assemblies. The navy must have wondered how it could have taken the MIT group so many years to discover its primary technological assumption was untenable. They may also have asked how OP-20-G's need for revolutionary cryptanalytic devices could be fulfilled if the responsibility continued to be left in the hands of the inexperienced NDRC and the young MIT students – people who failed to test underlying assumptions before wasting a critical year's work.

(U) The Revenge of Mechanics: the First Rounds

(U) While John Howard had been facing up to the failures of photo-optics and electronics, some practical men were creating immediate "mechanical" solutions to cryptanalytic problems. Beginning in late 1940, the engineers in the army's and navy's cryptanalytic branches began to work closely with IBM and its engineers. The outcome was the first operational special-purpose cryptanalytic machine and the first of a long and important series of modifications to IBM's standard offerings.

~~(TS//SI//REL)~~ By spring 1941, the army had its Gee Whizzer working on the transposition ciphers of several nations, and the navy was about to receive the first of its special IBM Navy Change Machines.[82]

~~(TS//SI//REL)~~ Logs and Relays – the Gee Whizzer

~~(TS//SI//REL)~~ The Gee Whizzer had been the first to arrive. In its initial version it did not look impressive; it was just a box containing relays and telephone system type rotary switches. But when it was wired to one of the tabulating machines, it caused amazement and pride. Although primitive and ugly, it worked and saved hundreds of hours of dreadful labor needed to penetrate an important diplomatic target. It proved so useful that a series of larger and more sophisticated "Whizzers" was constructed during the war. The last of the four versions had an electronic matrix and was in operation throughout the decade. The navy admired the Whizzer so much that it built its own version, the Jeep.[83]

~~(TS//SI//REL)~~ The Gee Whizzer was born because of a specific problem that arose in early 1941. It was the Japanese diplomatic service that had caused the SIS group to search for a new type of technological solution. When the Japanese made one of their diplomatic "transposition" systems much more difficult to solve through hand anagramming (reshuffling columns of code until they made "sense"), the American army did not have the manpower needed to apply the traditional hand tests.

~~(TS//SI//REL)~~ Friedman's response was to try to find a way to further automate what had become a standard approach to mechanically testing for meaningful decipherments. His search did not include electronics. Rather, he told Leo Rosen to find quick ways to extend the power of

(TS//SI) Gee Whizzer

the IBM machines that were beginning to arrive at his offices in greater numbers. Rosen's first task was to learn how automatic anagramming worked.

(~~TS//SI//REL~~) One of the most traditional ways of hiding the plain language or even the codes in a message was to transpose the columns of the text. With columns moved around in a random way, it was very difficult for those who might intercept a message to realign the text to its original order. The old hand attack had been to move one column after another against each other with an analyst making continuous judgments as to whether the new alignments were building towards a meaningful plain language arrangement. That was a tedious and time-consuming process.

(~~TS//SI//REL~~) During the 1930s the SIS had made some progress towards easing the analysts' burdens. Statistical studies of various languages had been made and a system of weights had been calculated. Turned into "logs"(logarithms) so that addition rather than multiplication could be used to build scores for combinations of letters, log weights were assigned to each letter in a transposed message. As each of the columns was rearranged, the weights were summed and an evaluation was made as to whether the sum approached that expected for a column of plaintext. If the logarithms of the statistically expected frequencies of the combinations were high, it indicated that the correct order of the text columns had been found. The results were double-checked by an analyst to see if the realigned columns made plain-language sense.

(~~TS//SI//REL~~) The log weight method had been implemented on the tabulating machines, but the process entailed much special card-punching and many runs of the cards to align all the columns. Worse, the tabulator method did not include an automatic test for plain-language "build-up." That meant that bad column sequences might be run for too long and, worse, all results were printed out. All of those usually worthless printouts had to be examined by an analyst.

(U) The method worked, but it was very, very labor intensive even with the use of tabulators. It took too much time to feed the round after round of cards that were required to test all columns of a transposed message against all others.

(~~TS//SI//REL~~) Rosen and the IBM consultants realized that not much could be done about the cards; there was no other viable memory medium. But it was thought that it might be possible to eliminate all but significant results from being printed. Rosen and his men, with the permission and help of IBM, turned the idea into the first and very simple Gee Whizzer. The Whizzer's two six-point, twenty-five-position rotary switches signalled the tabulator when the old log values that were not approaching a criterion value should be dropped from its counters. Then they instructed the tabulator to start building up a new plain-language indicator value.

(~~TS//SI//REL~~) Simple, inexpensive, and quickly implemented, the Gee Whizzer reinforced the belief among the cryptoengineers in Washington that practical and evolutionary changes were the ones that should be given support.

(U) The Navy Gets Some Changes

(~~U//FOUO~~) OP-20-G's enlisted grade in-house engineers felt the same way and argued for the help they needed to turn their imaginative ideas for true cryptanalytic machines into hardware. Their requests reached the office of the Director of Naval Communications and in mid-1941 Captain Redmond informed them that he had used his personal influence to get IBM's Tom Watson to agree to help the navy.

(~~U//FOUO~~) An IBM executive immediately came to Washington, listened to the ideas of Pete

Deffert and Lou Holland, and gave his blessing to their hopes for advances more radical than just attaching relay boxes to standard machines. An IBM engineer was soon assigned to duty at "G," and he began to refine the navy engineers' suggestions and to forward them to IBM's designers.

~~(TS//SI//REL)~~ Within a few months the first Naval Change (NC) was up and running. The NC-1 automatically sensed the beginning of a series of cards and then punched an increasing serial number in each successive card. IBM delivered a more complex machine just a few weeks later. The new automatic cross-footer also worked from the day it was installed. It provided a high-speed means of decrypting additive cipher systems, such as those used by the Japanese Navy.

(U) The NC series was continued throughout the war. The thirteen different machines became progressively more complex, but each worked, and none were burdens to the maintenance engineers at "G." [84]

(U) The Greatest Kludge of All, But It Worked

~~(S//SI//REL)~~ The navy's enlisted men were involved in something more ambitious: the construction of the mechanical contraption that worked, the M4. The Washington Code and Signal Section's electricians and machinists put fifty wheels, each having thirty contacts and ten stepping notches, together with ten banks of lights and a set of hand cranks, to provide an automatic way to identify what additives had been used in Japanese messages. The machine exploited a weakness in Japanese systems – all the code groups had to be divisible by three.

~~(S//SI//REL)~~ To find a likely additive, ten code groups were set on the machine; then the additive was entered with the cranks, and finally the machine was ordered to find out how many of the resulting deciphered code groups were divisible by three. The lights told the operator which groups were "over," "under," or "divisible." [85]

(U) Trying to Save Bush's Reputation

(U) John Howard was probably not told of the triumphs of the practical navy engineers and the old technologies, but he knew that he had to do something to save Bush's dream. He came up with a very rudimentary substitute for the film comparator.

(U) He advised the bureau that photographic plates could be substituted for microfilm. [86] Although very pessimistic, Howard did not give up on the Comparator entirely. But the new Comparator project seemed to be another very embarrassing disaster. The bureau certainly was unhappy, and the navy's cryptanalysts thought they might be left out of the electronics revolution.

(U) Bush was upset that his plans for electronic cryptanalysis were in trouble. There was almost nothing to show for a decade's work. And John Howard's bad news could not have come at a worse time for the navy. He made his confession about the microfilm Comparator just as the American intelligence agencies were frantically searching for the final clues to where Japan would attack. In a few weeks OP-20-G had to face the consequences of the failure to predict Pearl Harbor. But a combination of factors gave Bush's young men yet another chance. The ability of Howard to continue on independently (because he had a year's NDRC funding remaining) was important, but a more significant reason was the combination of the return of Joseph Wenger and the political influence of Vannevar Bush.

(U) Yet Another Chance

(U) Wenger returned from sea duty in the summer of 1941. Although assigned to OP-20's war plans section,[87] he contacted the cryptanalysts and Bush about the outcome of the year of

NDRC work. After hearing of the situation, and despite Howard's bad news, Wenger talked with his contacts at OP-20-G and pleaded for a continuation of the relationship with MIT.[88] His urging and the navy's dread of alienating the head of the NDRC, Vannevar Bush, allowed Safford to begin a program that would be vastly expanded when Wenger was sent back to OP-20-G in early 1942.

(U) When the Ciphers Can't Be Broken

(U) Wenger's influence at OP-20-G was the result of his long involvement in modernizing naval communications. He had a reputation as an expert in all communications fields. He was America's leading advocate of a high-tech alternative to cryptanalysis. In the 1930s, Wenger predicted that unless massive breakthroughs were made in cryptanalysis, such as the construction of a full range of Rapid Machines, it would be foolish to rely upon direct communications intelligence such as codebreaking. Until America built a truly innovative mathematical cryptanalytic capability, he argued, other signals intelligence resources had to be exploited. Wenger argued that codes and ciphers were becoming too complex to crack with available techniques, and, as important, an enemy's frequent changes of systems would always create blackouts at the most critical moments.[89]

(U) Wenger had become America's advocate for what became known as "traffic analysis." He had spent years studying and developing T/A. In traffic analysis, the concern was not with the content of messages but with the easily identified callsigns of senders and receivers, the timing and numbers of messages in a network, and the shifts in patterns of transmissions.[90] Although not as glamorous or exciting as cryptanalysis, traffic analysis was not a low-tech activity.

(U) Many aspects of T/A called for more esoteric and expensive hardware than traditional codebreaking. The method depended upon sophisticated direction finders to locate enemy stations and on other expensive radio equipment.[91] It was also very demanding in terms of personnel and data processing equipment.

(U) The first step for T/A was the ability to intercept enough messages. Revolutionary automatic scanners searched for active channels, oscilloscopes helped identify stations and operators, and very sensitive receivers plotted transmissions.[92] The hardware was not the end of it, however. Optimal radio interception and plotting called for advice from physicists; the exploitation of the intercepts needed advanced statistical-analytical techniques. The intercepts and location estimates had to be correlated and subjected to time-consuming analysis. The tabulators were frequently called upon to compile the necessary interaction matrices. The expense and manpower T/A needed seemed worthwhile. Wenger's reconstruction of Japanese naval maneuvers from T/A analysis during the mid-1930s was a triumph.

(U) By 1940 OP-20-G's intercept crews were logging thousands of messages a month from the Pacific and the Atlantic, and the method was considered essential. The SIS had also begun to appreciate T/A and sent its top men to the Canal Zone and Hawaii to establish intercept and processing sites. Those investments were inescapable. With America and Britain unable to read the most important German systems, T/A was the only hope in the West.[93]

(U) T/A had its limits, however. It could not reveal long-term plans; it gave just a picture of immediate intentions. It had other imperfections as well. The most important was a dependency on very frequent communications. If a station did not broadcast, it could not be identified and located. Tragically, in 1942 T/A was unable to deal with the German submarine onslaught because the submarines off the American coast followed a routine of radio silence.

(U) Wenger to the Rescue

(U) Joseph Wenger's influence at OP-20-G was not diminished by the failure of T/A to live up to its promise. In 1942 he was granted the power he needed to implement his plan for a centralized organization for naval communications intelligence. Wenger's ideas were quickly accepted.[94] Along with the approval of his plan came his appointment as the operating head of "G." In February 1942 he began to reorganize "G" and to revive Hooper's dream of bringing science and cryptanalysis together.

(U) But those were difficult times for Wenger. In early 1942 the U-boats began to slaughter dozens of freighters in sight of the American coast. The U-boat threat to the Atlantic convoys was growing so fast that a continuation of the sinkings threatened Britain's survival. Britain was unable to penetrate the new naval four-wheel Enigma, and OP-20-G remained without any power over German systems.

(U) Mathematics to Meet the Great Challenge

(U) The Atlantic crisis had a strange impact on OP-20-G's future. It both helped and hindered Wenger's crusade for the Rapid Machines. In its first phases, the crisis aided him. As part of his outline for the expansion of OP-20-G, Wenger had planned for the creation of a special research group. Its mission was to apply formal mathematics to cryptanalysis. OP-20-G had never before had a professionally trained mathematical team. In February 1942 Wenger brought together the few professional mathematicians who had already been called to service and had them join the "M" section. Of significance for World War II and the history of the Rapid Machines, they were handed more than mathematical responsibilities. They were ordered to take on some technical radio problems. In addition, they were given some of the responsibility for the critical German systems.

(U) Next, the "M" section was handed Wenger's pet, the Rapid Machines project. Luckily, Wenger found the right man, Howard Engstrom, to direct the third major attempt to make optics and electronics into cryptanalytic tools. When first called for the war crisis, Engstrom was asked to give advanced technical advice to OP-20-G's radio intercept and direction finding group.[95] That T/A assignment was a very important and demanding post. But heading "M" turned out to be much more of a challenge. The new job called for political as well as technical skills. By spring 1942 the Rapid Machines had again become political creatures.

(U) The apparent failure of Howard's 1941 microfilm Comparator had not ended his work or the interest of OP-20 in cryptanalytic machinery. But it did reopen the old battles over control of innovation in the navy.

(U) Bureaucracy vs. Science, Again

(U) Pearl Harbor, despite the blame hurled at the army and navy intelligence agencies, led to the release of funds and energies for cryptanalysis. For the first time in its history, OP-20-G had enough money to pursue technological dreams. In response, in early 1942, Safford, still the head of OP-20-G, initiated a survey of needs and wrote out a wish list that included Rapid Machines. There was enough money to explore all options. The first choice of the operating cryptanalysts was IBM electromechanical machinery. They asked for more standard equipment and for the development of a host of special attachments. Safford, not yet having an "M" section, and very short of personnel, turned to the Bureau of Ships for technical and administrative help.

(U) He found it easy to convince the bureau to deal with the trustworthy IBM. Very soon, the Bureau of Ships established what it saw as a harmonious three-way relationship between IBM, the old hands at "G," and itself.

(U) In the first weeks of 1942 the bureau decided to allow OP-20-G to invest navy funds in an exploration of Rapid Machines, but it demanded a heavy price, one which included a radical change in the relationship between MIT's men and the navy. The bureau's men, not those from OP-20-G, were to run the technical and financial parts of the program. Above all, the bureau wanted the projects out of the halls of MIT. Its officers demanded that all work be done by established corporations that followed the navy's standard procedures. But in early 1942 it began to take charge of the NDRC project, giving, it thought, badly needed managerial direction.

(U) Meanwhile, the bureau explored ways to decrease its dependency on Bush's group. Then the bureau decided to show its power. It took the Comparator away from Bush and MIT. In March 1942 Bush's structure for linking the military and academia, at least for cryptanalytic machines, began to be dismantled. The work at MIT, perhaps with the exception of the designing of a punch, was ended, and the secret workshop was shut down!

(U) A Seeming Victory for Science

(U) As soon as Wenger had returned to "G" and learned of the bureau's actions, he feared that the corporate projects would produce machines the cryptanalysts could not use. Wenger began an attempt to shift power back to OP-20-G. A search was begun for experienced engineers to augment the "M" group. By the end of 1942 OP-20-G had some of the leading men in computer electronics. Through formal and informal means, the name "M" came to mean machinery as well as mathematics.[96]

(U) Wenger convinced the bureau to give OP-20-G's Rapid Machine program near autonomy as well as its own facility and workforce. But it took a major intelligence crisis to achieve that. Wenger would not have been so successful and there would not have been a Naval Computing Machine Laboratory at the NCR factory in Dayton, Ohio, if the British had been able to conquer the German submarine Enigma system or if the White House had insisted that OP-20-G remain dependent on Britain's Ultra.

(U) The establishment of the Naval Computing Machine Laboratory and the increased power of the Rapid Machine group did help OP-20-G to build a series of innovative cryptanalytic machines, including the American version of the Bombe. By the end of the war, the American navy had some of the world's most advanced electronic machines.

(U) Notes

1. (U) A recent study of the messages intercepted by the Americans in 1941 concludes that if there had been the manpower to decode all the messages it would have been clear that Pearl Harbor was a target. Frederick D. Parker, "The Unsolved Messages of Pearl Harbor," *Cryptologia* 13 (1991): 295.

2. (U) Library of Congress, Papers of Stanford Caldwell Hooper: March 3, 1933 to January 1, 1935, Correspondence with Redman and Jewett: "Contact scientists"; June 1, 1934, "Binaural Sons of C"; October 20, 1935, "Travel to Laboratories"; Box 18, Hooper to Secret Naval Board, "Communications Plan," February 7, 1936; June 10, 1935, "McDowell, Contact scientists"; and November 20, 1935, "Travel to Boston." Navy Biographies Section OI-140, 27 April 1945, "Rear Admiral Stanford C. Hooper, U.S. Navy, Deceased." NARA RG457, SRH-355, "Naval Security Group History to World War II," 269.

3. (U) Note that Hooper's plan came almost a decade before the British began their now famous project at Bletchley Park to develop automata for cryptanalysis. For an example of the results of his efforts to modernize OP-20-G, NARA RG457, SRMN-083, "Military Study of Secret Radio Calls," January 8, 1938, by Joseph N. Wenger.

4. (U) The navy did not include signals intelligence in its formal war plans until 1937. NARA RG457, SRMN-084, "The Evolution of the Navy's Cryptologic Organization," 3. On the attacks against military and

diplomatic codes in the early 1930s, NARA RG457, SRH-159, "Preliminary Historical Report of the Solution of the 'B' Machine," 12. RG457, SRH-355, "Naval Security Group History to World War II," 82. NARA RG457, SRH-305, "The Undeclared War: The History of RI," 15 November 1943, by Laurance F. Safford, Captain, U. S. Navy.

5. (U) See Harold G. Bowen, *Ships, Machinery and Mossbacks: The Autobiography of a Naval Engineer* (Princeton: Princeton University Press, 1954), on the battle over high-pressure steam and formation of combined bureau in 1939. NARA RG457, SRMN-084, "The Evolution of the Navy's Cryptologic Organization," 3. A very useful survey is David Kahn, "Roosevelt, Magic and Ultra," *Cryptologia* 16 (1992): 289-319.

6. (U) Library of Congress, Papers of Stanford Caldwell Hooper: June 10, 1935, "McDowell, Contact scientists"; November 20, 1935, "Travel to Boston"; Box 18, "Johns Hopkins Atomic Energy," November 3, 1937; and March 3, 1933 to January 1, 1935, Correspondence with Redman, Jewett, "Contact scientists." NARA RG457, SRH-355, "Naval Security Group History to World War II," 268-269.

7. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 269, "Hooper to Wenger" November 1935, 270. January 2, 1936, "Bush Report." Office of Naval Research, Bush Comparator Patent file, #2,873,912.

8. (U) A thorough search of the OP-20-G archives and the holdings of the NRL and, by implication, those of the Bureau of Ships, did not lead to the recovery of a copy of the original outline or Bush's first sketches of the Comparator. ~~(S)~~ However, citations to the Bush documents were located on the old catalog cards of the NSA Technical Library. NSA, CCH, Card Catalog for Technical Library: Correspondence File: Bush Comparator 1936-38; Early Comparator Design Proposals: Bush Comparator 1936-37; Machine Proposals and Miscellaneous Material: Bush Comparator, 1936-1938; Navy Correspondence File and Historical Summary Bush Comparator, 1936-45; Six Project Reports: Bush Comparator, 1937-8; Bush Comparator Drawing #1-87 and Index, 1937; Summary of Materials on Symmetrical Sequences: Bush Comparator; Bush Comparator Drawings #88-153, 1937. f[3005]. (U) NSA CCH Series XII Z, "Memoranda on SIS, Formation of Cryptanalytic Group" from CCH Series XI K, Box 13, circa 1929-1939.

9. (U) NSA RAM File, January 28, 1936, DNC to Bureau of Ships, "Support Bush proposals," and July 21, 1936, Bureau of Engineering to OP-20-G, "BuEng refuses Bush." NARA RG457, SRH-355, "Naval Security Group History to World War II," 269.

10. (U) There is some indication the Bureau's men eventually outlined their solution, but no documents have been released. In the absence of any specifics, one can only guess at their alternative. Wenger remarked that the Bureau never really understood what he wanted. NARA RG457, SRH-355, "Naval Security Group History to World War II," 269.

11. (U) Susan M. Lujan, "Agnes Meyer Driscoll," *Cryptologia* 5 (1991): 47. James Rusbridger and Eric Nave, *Betrayal at Pearl Harbor* (New York: Summit Books, 1991). Cipher A. Deavours, and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, Mass.: Artech House, 1985), 218. NARA RG457, SRH-355, "Naval Security Group History to World War II," 161, 247. The Holtwick M-1 machine was in operation by mid-1937, perhaps earlier.

12. (U) Jeff Wenger interview with W. S. MacDonald, March 1991.

13. (U) Interviews with Waldron S. MacDonald. NARA RG457, SRH-355, "Naval Security Group History to World War II," 404.

14. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, Carton 67, William Radford, "Report on An Investigation of the Practicality of Developing a Rapid Computing Machine," October 15, 1939, Appendix III, List of Numbered References. Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, NCR Depositions, Bush to Deeds "Analyzing Equipment," May 19, 1938. Radford had been one of the "boys" at MIT who survived on the 1930s version of "soft money" being a research assistant there from 1932 to 1939. Caldwell put him to work on the Rapid Arithmetical problem in early 1937, and he produced his report on "The Practicality of Developing a Rapid Calculating Machine," October 15, 1939. Rockefeller Archives, Papers of Warren Weaver,

January 16, 1946, letter, S. H. Caldwell to Weaver, "Center of Analysis," 4.

15. (U) The machine did not have a name until some years later. Who borrowed the name Comparator from the nineteenth century MIT device remains unknown.

16. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 208, 247.

17. (U) NSA RAM File, OP-20-G to Bureau of Engineering, "Plugboards for Reproducing Punch," July 7, 1936. NSA, Lou Holland, "Development of Machine Processing in the Naval Security Group," 9. Holtwick had created several small mechanical machines that cost less than $300 each for Japanese problems. The Bureau helped build them. NARA RG457, SRH-355, "Naval Security Group History to World War II," 210, 257, 261.

18. (U) The patent claim was filed on April 22, 1937. William F. Friedman and Vernon E. Whitman, Electric Control System for Tabulating Cards, Documents and the Like, U.S. Patent 2,224,646, December 10, 1940.

19. (U) NARA RG457, SRH-274, "Military Cryptanalysis." NARA SRH-004, "The Friedman Lectures on Cryptology."

20. (U) David Kahn, *Seizing the Enigma*, (Boston: Houghton-Mifflin, 1991), 87, and Cipher A. Deavours, "The Black Chamber: A Column: La Methode Des Baton," *Cryptologia*, 4 (1980): 240-247. There are reports that the Americans, including the Coast Guard group charged with attacking the ciphers of the rum-runners, were able to break into the simple commercial version of the Enigma during the 1920s. Malcolm F. Willoughby, *Rum War at Sea*, (Washington: GPO, 1964).

21. (U) David Kahn, *Seizing the Enigma*, (Boston: Houghton-Mifflin, 1991), 141.

22. (U) W. S. MacDonald Interviews.

23. (U) Letter to author from MIT registrar's office. In his first interview, MacDonald stated that he went to MIT in June 1937. But in his second interview he cited September as the month he began his duties. I have accepted the second date because it makes more sense in light of the previous pace of the work and MacDonald's desire to also enroll in the graduate program in the department.

24. (U) Paul F. Ceruzzi, *Reckoners: The Prehistory of the Digital Computer* (Westport, Conn.: Greenwood Press, 1983).

25. (U) Michael R. Williams, *A History of Computing Technology* (Englewood Cliffs, N.J.: Prentice-Hall, 1985). Nancy Stern, *From ENIAC to UNIVAC: An Appraisal of The Eckert-Mauchly Computers* (Bedford, Mass.: Digital Press, 1981).

26. (U) Because the Comparator read ten data columns at a time, more sophisticated IC tests could be done at the same rate as single letter tallying. Bush and Wenger may not have realized the potentials of the modified tabulators. The Comparator had five counters as did tabulators. Thus, several fields could be processed in parallel. The navy may not have analyzed all the (n*(n-1)) combinations, but may have been satisfied with only a portion of the possible offsets of the messages.

27. (U) In some systems, messages were much, much longer. Thinking their Fish system was beyond attack, the Germans sent very lengthy reports on it. F. H. Hinsley et al., *British Intelligence in the Second World War Vol. III*, 1 (London: Her Majesty's Stationery Office, 1984), Appendix 2, 477.

28. (U) Bush gave about one second for each line of printing. This time was estimated via the description in the NSA RAM File, "M.A.C. Outlines # 17, 70mm Comparator," and my knowledge of the 1938 Comparator.

29. (U) Table 7.1 shows the power of various devices, including the Comparator (run at various projected speeds) relative to tabulators operating at their typical 120 comparisons a minute. A cell entry in the table gives the worth of the alternative machine in terms of the hypothetical raw power of the number of tabulators. Thus, a sorter running at full speed was worth three tabulators while the speed of a typical teletype system of the era was five times greater than the tabulators.

30. (U) On tape speeds and densities, Hagley Museum and Library, Accession 2015, Remington-Rand, ERA materials, S. Ruebens, "Investigation of Solid Acoustic Delay Lines," Contract Nobs 28476, August 1, 1947, 1. The Colossus read at 5,000 characters a second. Brian Randell (ed.), *The Origins of Digital Computers: Selected Papers* (New York:

Springer-Verlag, 1982), 349. It is not certain that this means that 5,000 serial characters passed the reading head of its tape scanner. The Robinsons, the British versions of the tape-optical machines (but ones for binary comparisons), read at 2,000 a second. Tape readers used by the navy in WWII ran at about ten characters a second. The 1948 figure is in Samuel S. Snyder, "Abner: The ASA Computer, Part I: Design," *NSA Technical Journal* 25 (1980), 59.

31. (U) A very important spinoff of the navy Comparator was a 1938 project at NCR. Desch used 35mm film with punched holes on an optical comparing device for a utilities billing machine. Hagley Museum and Library, Accession 1825, Honeywell v Sperry-Rand Trial Records, August 16, 1938, Desch to Williams, "Laboratory work" and August 30, 1939, Desch to Williams "Work at Laboratory."

32. (U) Bernard Williams, "Computing With Electricity, 1935-1945," (Ph.D. Thesis, University of Kansas, 1984). Final OSRD Report, Div. 17, George E. Beggs Jr. and F. L. Yust, "Development and Application of Electronic Counting Circuits," 1946, especially Chapter 9.

33. (U) Several late 1930s projects at MIT explored magnetic memory and many variations of storage based on electrical charges. See Hagley Museum and Library, Accession 1825, Honeywell v Sperry-Rand Trial Records, Carton 67, William Radford "Report on An Investigation of the Practicality of Developing a Rapid Computing Machine, October 15, 1939."

34. (U) William Aspray (ed.), *Computers Before Computing* (Ames, Ia.: Iowa State University Press, 1990).

35. (U) Michael K. Buckland, "Emanuel Goldberg, Electronic Document Retrieval, and Vannevar Bush's Memex," JASIS 43 (1992): 284. On the 1937 and 1940 patents and their history, Hagley Museum and Library, Accession 2015, unprocessed ERA materials from Sperry Archive, November 1, 1949, Memo to File, Selector Infringement Search, and Accession 1825, *Honeywell v Sperry-Rand* Trial Records, August 13, 1937, Bush to Deeds, and October 25, 1937, Research Corporation to Deeds.

36. (U) NSA RAM File, OP-20-G to Bureau of Engineering, "Rapid Equipment," March 29, 1938.

37. (U) A density of ten or eleven per inch was assumed as indicated by the description of the later army version of 1944 which reached twelve and one-half per inch with an average over the entire tape of six and one-quarter per inch. On the cost of the Eastman tape, NARA RG457, SRH-355, "Naval Security Group History to World War II," 276, and NSA RAM File, CNO to Bureau of Engineering, April 29, 1938.

38. (U) In later models of the Comparator, the stepping could be from one to ten characters after each pass. NSA RAM File, "M.A.C. Outlines #17, 70mm Comparator," April, 1947.

39. (U) Howard Aiken's early computer, the ASCC, used a tape rig similar to the one chosen for the Comparator. During World War II the Americans and the British also used a pulley and loop system for the follow-ons to the Comparators, indicating that it was a sound method. Michael R. Williams, *A History of Computing Technology* (Englewood Cliffs, N. J.: Prentice-Hall, 1985), 245. Brian Randell, "Colossus: Grandfather of the Computer," in B. Randell (ed.), *The Origins of Digital Computers* (New York: Springer-Verlag, 1982), 350.

40. (U) Interviews with W. S. MacDonald.

41. (U) Paul F. Ceruzzi, *Reckoners: The Prehistory of the Digital Computer* (Westport, Conn.: Greenwood Press, 1983). Charles S. Bashe, et al., *IBM's Early Computers* (Cambridge, Mass.: MIT Press, 1985), 36-39.

42. (U) Waldron MacDonald claimed he had to rework all the circuits and that binary switching speeds did not exceed 5,000 per second. MacDonald interviews, 1987-1991.

43. (U) The navy's later Letterwriters and its Copperheads used a modified baudot coding. NSA RAM File: "Machine Comparisons," June 1946; Communications Intelligence Technical Paper 42, "Copperhead I Theory and Copperhead I Equipment"; and Communications Intelligence Paper 41, "Copperhead I Punch and Copperhead I Scanner."

44. (U) NSA RAM File, July 18, 1938, Safford to Bush, "Machinery Arrived."

45. (U) NSA RAM File, Wenger Report, "Bush Visit" April 25, 1938. Waldron S. MacDonald interviews. NARA RG457, SRH-355, "Naval Security Group History to World War II," 299.

46. (U) Interviews with Waldron S. MacDonald, 1987-1991.

47. (U) Library of Congress, Papers of Vannevar Bush, Box 67, MacDonald to Bush, July 25, 1939. And interviews with MacDonald.

48. (U) Office of Research and Inventions patent application sheet of 10-29-46 lists April 1938 as the time of the first successful witnessed run. ONR, patent file for Bush Comparator, #2,873,912.

49. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 272, 276. NSA RAM File, OP-20-G to Bureau of Engineering. "Rapid Equipment," April 29, 1938, and May 17, 1938, "Comparator Equipment."

50. (U) NARA RG457, SRH-151, "Military Study: Communication Intelligence Research Activities," 022, indicates that the first Bush machine was paid for out of a special fiscal 1938 allocation. The proposed budget for 1939 contained a request for a similar amount, but it may have been for a "payback" for the first expenditure.

51. (U) NRA RAM File, September 16, 1938, OP-20-G Bureau of Ships, "Budget Request."

52. (U) The exact amounts spent and budgeted for the Comparator in 1938 and 1939 remain unknown. NARA RG457, SRH-355, "Naval Security Group History to World War II," 276, 240. The budget request for fiscal 1939 included items for building new machines and new components such as a rapid "locator." This may have been a means of locating code groups, a function later embodied in the machines designed by Lawrence Steinhardt, or it may have been an automation of the methods of overlay sheets to determine code-wheel orders and setting as used by Mrs. Driscoll. RAM File, CNO to Bureau of Engineering, September 16, 1938, "Development of Special Communications Devices."

53. (U) The machine arrived at the Navy Yard on June 24. It had been badly jostled on the trip and refused to run. NSA RAM File, July 18, 1938, OP-20-G to Bush "Machine Has Arrived." It took Dulong some three weeks to tease the machine into its first non-MIT test run. NRL, Bush Comparator patent application file, October 29, 1946, 1.

54. (U) NSA RAM File, July 18, 1938, Safford to Bush, "Machinery Arrived." NRL patent application file, October 29, 1946, 1.

55. (U) NSA RAM File, May 17, 1938, "Comparator Equipment," and July 18, 1938, Safford to Bush, "Machinery Arrived."

56. (U) Jack Sweetman, *American Naval History* (Annapolis: Naval Institute Press, 1984), 156.

57. (U) Jeffery M. Dorwart, *Conflict of Duty: The United States Navy's Intelligence Dilemma 1919-1945* (Annapolis: Naval Institute Press, 1983), 93, 99. NSA RAM File, OP-20-G to Bureau of Engineering, March 22, 1938 and June 24, 1938, "IBM Purchases." Cipher A. Deavours, and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, Mass.: Artech House, 1985), 212. NSA, Theodore M. Hannah, "Frank B. Rowlett: A Personal Profile," 116. Rear Admiral Edwin T. Layton, *And I Was There: Pearl Harbor and Midway – Breaking the Secrets* (New York: William Morrow, 1985). NARA RG457, SRMD 019, "The *Panay* Incident."

58. (U) NSA RAM File, May 17, 1938, "Comparator Equipment," and CNO to Bureau of Engineering, September 16, 1938, "Development of Special Communications Devices."

59. (U) Ironically, MIT would soon provide the army's cryptanalytic group with an electrical engineer, Leo Rosen, who quickly became the leader of the group that constructed a model of Purple and that became the electronics research group in the SIS. NSA, Theodore M. Hannah, "Frank B. Rowlett: A Personal Profile," 18.

60. (U) NSA RAM File, Safford to Bush, December 10, 1938, "Fine Job on Comparator."

61. (U) NARA RG457, SRH-355. "Naval Security Group History to World War II," 300.

62. (U) NSA RAM File, OP-20-G, "List of statistical machinery," December 1, 1939.

63. (U) Library of Congress, Papers of Vannevar Bush, Box 67, MacDonald File, Bush to MacDonald "OP-20-G Project," August 31, 1940. NARA RG457, SRH-355, "Naval Security Group History to World War II," 270, 405.

64. (U) Daniel J. Kevles , *The Physicists: The History of the Scientific Community in Modern America* (New York: Knopf, 1978), 296.

65. (U) Ronald W. Clark, *Tizard* (Cambridge: MIT Press, 1965).

66. (U) Charles S. Bashe, et al., *IBM's Early Computers* (Cambridge, Mass.: MIT Press, 1985), Chapter 2.

67. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records April 16, 1942, "Conference on fire-control projects." The ENIAC used a "memory" system from RCA that was quite like what was used on some OP-20-G and SIS machines and a counting circuit invented by one of RCA's men, Igor Grosdoff. N. Metropolis, et al., (ed.), *A History of Computing in the Twentieth Century* (New York, 1980), 467. Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, May 19, 1938, September 18, 1944. "Army seizes Grosdoff patent."

68. (U) Bernard Williams, "Computing With Electricity, 1935-1945," (Ph.D. Thesis, University of Kansas, 1984), 317. Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* Trial Records, June 6, 1942, Weaver to participants "Cancel fire control work."

69. (U) The fear of defeat was quite real. Bletchley Park had scores of buses at the ready to race its staff to port cities where they were to board fast ocean liners for the United States and Canada.

70. (U) Laurance F. Safford, "Rhapsody in Purple," by Dundas P. Tucker, *Cryptologia* 6 (1981): 196, 220. NSA, Theodore M. Hannah, "Frank B. Rowlett: A Personal Profile," 18. NSA RAM File, Part H of Report to J. N. Wenger, Capt. USN, "Resume of the Dayton, Ohio Activity During World War II," (presumably a continuation of the Meade Report), 1. In contrast to Safford's interpretation and on America's first contact with British Enigma achievements, NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 019-021, 272. NARA RG457, SRH-145, "Report of the Technical Mission to England," April 11, 1941, 002-004. But on how little Enigma ability OP-20-G had as late as the summer of 1943, NARA RG457, SRH-403, "Selections from the Cryptologic Papers of Rear Admiral J. N. Wenger, USN," 072-3.

71. (U) Rear Admiral Edwin T. Layton , *And I Was There: Pearl Harbor and Midway – Breaking the Secrets* (New York: William Morrow, 1985), 78.

72. (U) NARA RG227, OSRD, Office of the Chairman, Box 1, Bush to Safford, October 28, 1940, "Project Agreement." NSA RAM File, Safford to Radio Division, Bureau of Ships, November 2, 1940, "Bush Project." NARA RG457, SRH-355, "Naval Security Group History to World War II," 404.

73. (U) NSA RAM File, January 2, 1942, Safford to Howard, "Comparator Received 12-24," and January 6, 1942, BuShips to CNO, "Manual for Comparator."

74. (U) Again, this may also have been a means of automating the use of the sheets used to attack wheel settings.

75. (U) The punches were redesigned and remanufactured several times during the war. After MIT made a try in 1940-41, the Gray manufacturing company made a version; then NCR redid them; then new designs were drawn for the postwar era. NSA RAM File, Communications Intelligence Technical Paper-42, "Copperhead I Theory and Copperhead I Equipment." NSA RAM File, OP-20-G to NCML-NCR, February, 1945.

76. (U) NARA RG457, SRH-355, "Naval Security Group History to World War II," 430. On Steinhardt visit, Smithsonian Institution, History of Computers Project, Interview with Howard Campaigne, 19.

77. (U) Some $25,000 was promised to NCR in November 1940. Some of it may have come from the original NDRC grant, but Bush apparently secured an additional grant for some thirty copies of the counters although the NDRC was not to become involved in production. NARA Suitland, OSRD Contract Files, OEM 275 November 28, 1941, "NCR-MIT counters." Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, December 2, 1941, NDRC D3 to Desch-NCR, "30 counter printers."

78. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, January 29, 1942, Desch to NCR "Secret Work," and February 21, 1942, Desch, "Report to Management."

79. (U) Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes* (New York: McGraw-Hill, 1982). David Kahn, *Seizing the Enigma* (Boston:

Houghton-Mifflin, 1991). The role of captures in the long-awaited break into Japanese army systems is discussed in the very impressive Edward J. Drea, *MacArthur's Ultra* (University of Kansas Press, 1992).

80. (U) On the state of American readiness and some hints about the roles of Mrs. Driscoll and the team at SIS, compare James Rusbridger and Eric Nave, *Betrayal at Pearl Harbor* (New York: Summit Books, 1991), and the more scholarly Edward J. Drea, *MacArthur's Ultra* (University of Kansas Press, 1992). NARA RG457, SRH-355, "Naval Security Group History to World War II," 440, 442. NSA RAM File, OP-20-G to OP-20-A, "Meeting with Dr. Howard," November 5, 1941. However, Howard was told that the Driscoll problem was not of high priority. NSA RAM File, BuShips to Howard, November 11, 1941.

81. (U) NSA RAM File, November 3 and 5, 1941, Howard OP-20-G Reports on Meetings, and November 14, 1941, Bureau of Ships to Howard.

82. ~~(TS//SI)~~ M.A.C. Outlines #1, April 1947, Electroanagrammer ("Gee Whizzer"), stored in CCH Series XII Z. Leroy Wheatley, "Brief Description of Analytic Equipment, Fourth Installment," 20 September 1954, "NC MACHINES," stored in CCH Series XII Z.

83. ~~(TS//SI//REL)~~ Samuel S. Snyder, "Famous First Facts: Part I: Pre-Computer Machine Cryptanalysis," unpublished, stored in CCH Series XII Z. "Gee Whizzer," circa 1947, stored in CCH Series XII Z.

84. (U) S. Snyder Interview with Lou Holland, circa February 2, 1972, stored in CCH XI K, Box #10, Famous First Fact folder. Wheatley, "Brief Description of Analytic Machines, Fourth Edition," 20 September 1954, "NC Machines."

85. (U) NSA S 337/348 "Additive Machines-Historical Summary Of," Stored in CCH Series XII Z. The first M4 was operational at the end of 1941. It worked well for a time, but had to be replaced.

86. (U) Photographic plates for data entry had been used on the Cinema Integraph and were being explored for use in the Analyser and the electronic computer at the Institute. NSA RAM File, January 5, 1942, Howard to OP-20-G, "Report: Glass Plates." Arnold Dumey letters to Brian Randell, 1975, "deformation."

87. (U) NARA RG457: SRH-279, "OP-20-G File Communications Intelligence Organization, 1942-46:" SRMN-084, "The Evolution of the Navy's Cryptologic Organization," 2; and SRH-306 "OP-20-G Exploits and Commendations World War II."

88. (U) Interview with Jeff Wenger, 1991.

89. (U) NARA RG457, SRMN-083, "Military Study of Secret Radio Calls, January 1938."

90. (U) All other major nations used the same techniques and had done so since World War I, but Wenger was America's advocate. NARA RG457, SRMN-083, "Military Study of Secret Radio Calls, January 1938."

91. (U) NARA RG457, SRH-083, "Military Study of Secret Radio Calls, January 8, 1938 by J. N. Wenger."

92. (U) On automatic direction finding equipment. NARA SRH-197, "US Navy Communications Intelligence, Organization, Liaison and Collaboration 1941-1945," 38.

93. (U) Some reports indicate that in late 1941 the vast majority of the "G" workforce was busy with T/A rather than cryptanalysis. NARA RG457, SRH-403, "Selections from the Cryptologic Papers of Rear Admiral J. N. Wenger, USN."

94. (U) NARA RG457, SRH-279 "OP-20-G, Communication Intelligence Organization 1942-1946."

95. (U) NARA RG457, SRH-305, "The Undeclared War: The History of RI," 15 November 1943, by Laurance F. Safford, Captain, U. S. Navy.

96. (U) NARA RG457, SRH-403, "Selections from the Cryptologic Papers of Rear Admiral J. N. Wenger, USN," 60. BuShips, NXs329 (945) 5-6-43, Pulse Spotter Equipment, Philco Corporation. The remainder of the war. Library of Congress, Papers of Vannevar Bush, Box 52, Howard to Killian, March 21, 1946, "rapid selector."

This page intentionally left blank

Chapter 3

(U) Bush's Dream Does Not Come True

(U) A Look Ahead to Peace

(U) America's entry into the war led to the release of torrents of money for codebreaking. A surprisingly large allocation was given to the Bureau of Ships for cryptanalytic machine development. Unfortunately, "G" and the bureau were not prepared, and they were unable to immediately establish a well-coordinated project that could compensate for the years of lost opportunities. The funds came too late to set up a long-term development program, and "G's" resources had to be devoted to cryptanalytic fire-fighting. Until very late in the war, OP-20-G's computer activities were driven by emergencies. Until late 1943, "G's" brilliant mathematicians and engineers did not even have the time to think of machines that went beyond Bush's mid-1930s ideas or to plan their move from analog to electronic digital technologies.

(U) After they made their great electromechanical contribution to the Ultra problem, the Bombe, they had more time. They built a few path-breaking digital electronic machines, and they began to lay plans for a long-term computer program. However, by the end of the war they had not been able to turn Bush's faith in microfilm into advanced and reliable machines.

~~(S)~~ One important consequence of the absence of the ultra-fast digital machines was that Hooper's dream of relying upon pure statistical and mathematical cryptanalytical techniques had to be deferred. Like England, the United States had to rely upon the most expedient cryptanalytic as well as technological solutions. During 1942 and 1943, OP-20-G's "M" group was unable to become a think-tank for pure methods. They and the cryptanalysts had to depend upon "what worked." And what worked in cryptanalysis were brute force techniques that called upon massive data processing and hunch playing. At the same time, the engineers at "G" and the Bureau of Ships had to choose the easiest hardware solutions to meet the demands of the hard-pressed codebreakers.

(U) A series of increasingly complex and powerful devices began to emerge in early 1944. But it was not until 1945 that OP-20-G's young engineers could begin to think of creating a multipurpose Rapid Machine, and when "M" could begin the exploration of the frontiers of mathematical cryptology. There were more than technical reasons for the gap between what Wenger and Hooper wanted and what was achieved during the war. OP-20-G's World War II machine effort began in crisis, had to respond to immediate cryptanalytic needs, and continued to be driven by rapidly shifting demands.

(U) January 1942: Too Much Too Late

(U) Soon after Pearl Harbor, the bureau gained the funds to support all the ideas that had been put forward by the various groups in OP-20-G and at the Navy Yard. Contracts were let to IBM for more tabulator equipment and for the creation of a host of new special attachments. Those at the bureau and OP-20-G who favored electromechanical equipment received recognition when IBM was also awarded a very large contract to develop a set of new machines to automate the processing of incoming data. At the same time, a group of navy engineers in Washington was allowed to build some electromechanical analysis machines of their own design.

(U) The bureau had enough resources to prevent Bush's Comparator from being locked away to die in the secret workroom at MIT. The bureau

made an arrangement with Eastman-Kodak to work on all the microfilm and plate ideas. This meant that Howard and his group were to be helpers not supervisors for the teams Eastman hastily put to turning ideas into machines.[1] When Joseph Wenger returned and established the "M" group under Howard Engstrom, he tried to regain control over the automatic machines. But it took some time to organize "M." In fact, if it had not been for the crisis in the Atlantic and the attitude of Ralph Meader, the man the bureau had assigned to supervise the machine contracts, Wenger would not have been able to reassert OP-20-G's power over machine development.

(U) In the first months of 1942, Meader ran a freewheeling one-man operation for the bureau. Despite his freedom, he began to experience the frustrations that had led Hooper and Bush to try to throw off the heavy hands of the navy's bureaucracy in the 1930s. He came to feel that the companies were unresponsive, and he compiled a list of complaints.

(U) A Giant Step Backwards

(U) When the bureau went to Eastman in early 1942, no one had expected frightening delays or a need for radical redefinitions of "G's" machines. Eastman's technical and managerial reputation pointed to a speedy solution to the problems that had halted the work at the Institute. Thus, it was natural for the bureau to turn to it when Howard seemed to admit that he could not solve the problems of the proposed microfilm Comparator. But Eastman would not meet the bureau's expectations.

(U) With help from John Howard's men, Eastman was able to ship the first version of what became known as the Index of Coincidence Machine before 1943.[2] The IC Machine was a relatively simple plate-based device that looked more like the early 1930s astronomers' instruments than Bush's Comparator.[3] The IC Machine did its job, but it was not automatic, and it was certainly not a machine that was leading, as were the Bush designs, to the use of digital circuits.

(U) The machine was electrical, not electronic. Eastman's team realized that a pulse-based system, even with the plates, would be too complex. Thus, an electric measuring system was built into the IC machine. There was no counting, just a recognition that enough light had penetrated to the photocell. The analyst would then tally the overlapped dots or find their locations within a message.[4]

(U) Although comparatively simple, the IC machines had deficiencies. It was very difficult to coax the data camera to place the dots on the plates in perfect alignment; that problem continued throughout the war. The IC machines themselves had to be redesigned and reworked during 1943. Perhaps as many as one half of all the machines were inoperable at any one moment.[5]

(U) Haste and Confusion

(U) Eastman's work began in haste, was not well supervised, and, as a result, was not adequately documented. As a consequence, even the military services were confused about the names of the machines Eastman proposed or delivered before 1943.[6] Some of the first lashed-together models are only vaguely remembered. But the documents that remain reflect the desperation to produce machines.

(U) One of those was a version of a Bush IC machine constructed during 1942. When it ran, it shook the entire laboratory; perhaps that is why it never appeared in OP-20-G's machine center. The device did not use the ideas for tape drives that Bush and Howard had explored. Rather, two large message tapes were wound around a large hydraulically controlled drum. As the drum spun at a very high speed, the tapes inched back and offset themselves. When the photoelectric detector sensed a "hit," the drum slammed to a stop.[7]

~~(S)~~ Some other alternative concepts for machines came from the groups at Eastman as they searched for ways to make Howard's original suggestions turn into hardware. Trying to help the navy in its attack against the very stubborn Japanese additive code systems, the Eastman engineers drew up initial plans for a combination of tape readers, electronic circuits to strip the additives, and a set of whirling disks that were to hold frequently used code groups. An Edgerton flash lamp was to help to see if the stripped text groups matched one of the codes on the disks.[8]

~~(S//SI)~~ The disk contraption was not delivered to the navy, but Eastman's initial attempt to turn Bush's Rapid Document "Selector" (Information Machine) ideas into a useful military machine arrived in Washington before the end of 1942. Tessie was Eastman's first great contribution. Tessie began as an attempt to finally turn the architecture and the fundamental technologies of the microfilm Selector into a machine that worked. But Tessie became another pragmatic compromise. Bush's ideas were too difficult to put into practice. They could not be changed into hardware quickly enough to meet the pressing cryptanalytic needs of the first years of the war.

(U) Tessie Wouldn't Either

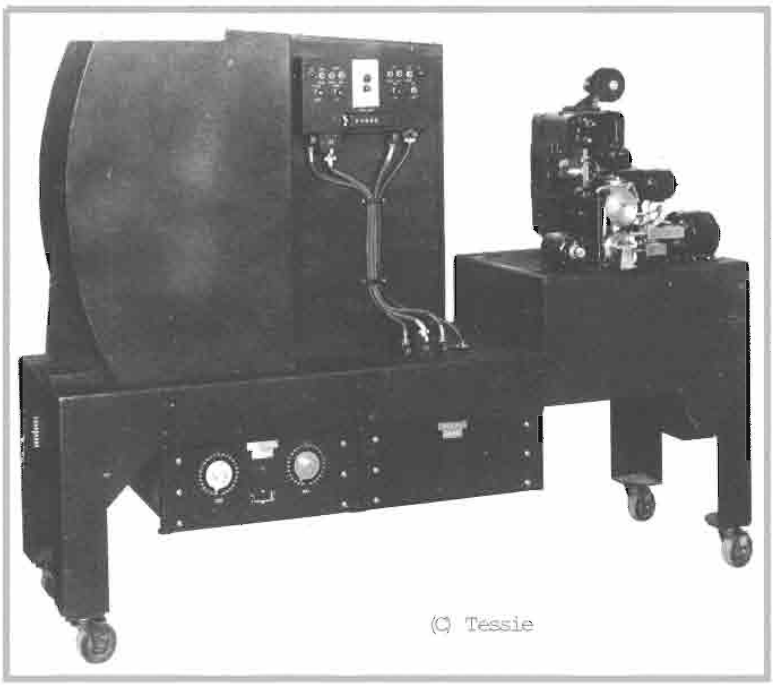
~~(S)~~ John Howard made sure that Eastman knew what he wanted well before the formal contracts with the Bureau of Ships were signed. He told the men in Rochester that in order to deliver something of value, in what was hoped was a reasonable time, the new military "Selector" was to be a special purpose device to perform an important but minimally challenging cryptanalytic function. Its job was to locate four-character code groups (tetragraphs), not to count them. Finding and giving the location of groups was a "quick and dirty" version of IC analysis. "Locations" pointed to the possibility that two messages were in "depth." [9]

~~(S)~~ Tessie's logic and architecture were like those of a Selector rather than a Comparator. It used two 35-millimeter films. One sped past an optical reading station while the other remained stationary and acted as an identification mask. After the fast film made a complete revolution, the mask film was stepped one frame. If a desired tetragraph was located, a signal was emitted. Then, a strobe circuit signaled a high-power Edgerton flash to send light through the identification portions of the two data films. The light would register the location of a matched group. After the run was completed, the new film was to be quickly developed, then sent to the analysts who would trace the groups and begin their attempt to break the codes.[10] There was no ability to reproduce the code groups, and there was no ability to tally. Those features, Howard knew, would ask too much of the engineers working under pressure – even of Eastman's experts.[11]

(U) The Eastman group put in a great deal of overtime and was able to send a machine to Washington in September 1942. RAM-2, or Tessie I, was a large and ungainly thing that was more than six feet long and almost as high. On one end was the drive mechanism for the data microfilms. On the other was a huge round canister-like component that housed some of the electronics and the photographic reproduction equipment. On top of the canister was a rack of tubes that could not be squeezed into the machine's frame.[12]

~~(S)~~ Although ugly, Tessie raised expectations about the Eastman portion of the RAM program. A great deal of equipment was ordered to support Tessie's work. Fifty- and sixty-foot metal developing trays, film drying racks, and hundreds of pounds of chemicals began arriving at the cramped "G" headquarters.[13]

~~(S)~~ Tessie failed, however. In its first runs it missed almost all the coincident tetragraphs. When it did find a "hit," it refused to produce the record of it on its internal film. The Edgerton-



(C) Tessie

type flash system would not function. Even the Washington, D.C., water supply refused to cooperate in the film development process of the two "data" films. Chemical imbalances in the water were making the tiny dots the Tessie light bank data camera produced spill over onto each other, making recognition impossible. That added to the difficulties of making the camera light bank behave. Some of the problems with the camera were fixed, but it took longer to find a way to compensate for the chemistry of the District's water supply.[14]

~~(TS)~~ One of Tessie's weaknesses was very embarrassing for the engineers. It missed "hits" that were too close together. The special warning circuit Howard and his men had devised to solve the problem would not behave.[15]

~~(S)~~ Throughout fall 1942 Tessie was too unreliable to be used as an operational machine. Finally, it was decided to make a major investment in its repair. It took Larry Steinhardt and his crew in Washington almost all of January 1943 to replace many of the circuits and to design a new flash system. The machine did begin to do a bit of work. It was put to use in an attempt by the Americans to attack the Enigma by searching for tetragraphic repeats.[16] Tessie proved of some use in the next few months although it continued to misbehave. Because of continued problems, it was replaced as soon as possible and changed into an even greater analog retrogression.[17]

(U) Tessie's New Hat

~~(TS)~~ The navy's Tessie was turned into a machine to perform a very simple type of search for "isomorphs." As a result, the new Tessie used only a few ideas from Bush's 1930s proposal for a navy "Symmetrical Sequence" engine. In its new life, it no longer reproduced hit locations on film. The flash camera was abandoned in favor of a punch.[18]

~~(TS//SI)~~ Codebreakers search for anything that is nonrandom. When they can find patterns that are obviously not produced by chance alone, they have at least a beginning of an attack on an enemy system. Repeats of phrases or even words are one of the signals that additional analysis might lead to a successful understanding of an enemy's cipher. One of the ways cryptanalysts located repeated messages, or repeated groups within messages, was to search for what the army called "isomorphs" and the navy called "symmetric sequences."[19]

~~(TS//SI)~~ Because cipher machines or additive systems are designed to hide repeats of words, looking for exact matches in small amounts of text is usually a waste of time. But what may be

found are patterns. If the word "BATTLE" is treated as a sequence of letters and recorded as "ABCCDE," an analyst may search for a repeat of the pattern. The pattern may appear despite the ability of additives to disguise the underlying code group.

~~(TS//SI)~~ Isomorphic attacks are expensive "long-shots." They were time-consuming because of the need to recode message texts, and identifying an isomorph only led to a probability that a depth had been found. But the method had proven of value to the American cryptanalysts since at least the 1930s.

~~(TS)~~ When the first Eastman Tessie was outclassed as a locator of exact match, four-character groups by its replacement, Icky, OP-20-G decided to have Tessie turned into an emergency Symmetric Sequence Machine. What emerged from the workshops in early 1944 became known as Tessie SS. The reborn Tessie was still a six-by-seven-foot monster, but it had been stripped of many of its most sophisticated components. However, it finally worked, and it saved a great deal of analyst and, as important, recoding time.[20]

~~(TS//SI)~~ The new Tessie had a small reel for the 35mm message film and one for a mask that contained patterns for the letters A to Z. The photoelectric scanning system's first task was to identify the first character of text on the film. Then, it scanned twenty characters of the message as the alphabetic mask film sped by. If it found a repeat of the first of the twenty characters, it signaled that the other half of the machine should get to work.

~~(TS//SI)~~ At the other end of Tessie SS was that original huge round canister. But now it contained a roll of plain 70mm paper tape and a roll of the black-red tape that Bush had used on his paper tape Comparator, not unexposed film. Instead of the strobe system for reproducing the location codes for a hit, there was a punching mechanism like the ones built for the paper tape Comparator. When the photocell spotted a repeated letter, it ordered the two tapes to be punched with tiny holes. When the entire six-character-per-second run through the message was completed, the paper tapes were removed, placed on a viewer, and searched for patterns of red dots that would indicate where an isomorph had been found. Tessie SS was much less elegant than the original, but it functioned successfully.

(U) You Can Use Some of the Technology Some of the Time, But...

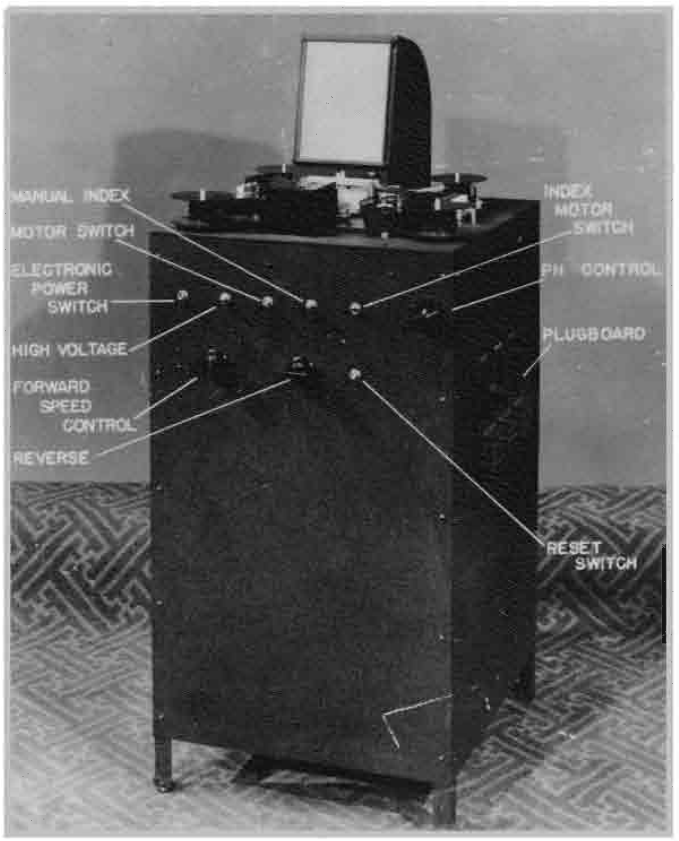
(U) Soon after the original Tessie was delivered to Washington in fall 1942, it was realized that it would never be a success. A radical redesign would be necessary. A very different design was needed if the navy was to have a successful high-speed microfilm machine.

(U) Eastman assigned a new crew to the task in early 1943, but the company was unable to deliver a machine, Icky, until October 1943. Then it took another few months for the men in Rochester to develop an efficient camera to produce reliable microfilms for the new Icky.

~~(TS)~~ As they were designing a better camera system, the Eastman group received some more depressing news. After its first rounds of tests in Washington, Icky needed to be reworked. It had to be shipped back to Rochester because of the great amount of repair and redesign that was needed.[21] On its return to Washington, the machine became an important tool for OP-20-G; but its success depended on its being, in some ways, another retrogression.

~~(TS//SI)~~ First, to allow it to be of immediate and reliable use, it had been designed to be much more limited than the Comparator or even Tessie.[22] Icky was a film version of the IC plate machine, and it was able to do a primitive analog IC test, but it just located. It did not make copies or count. It had no reproducing cameras and it

had no counter-printer. When enough light was registered, the machine lit a signal lamp and stopped. Its operator used a hand crank to turn the films back towards the identified coincidence. At the point where "enough" light came through the two films another signal lamp was lit. Then the operator used a screen to read the location marks printed on the margins of the films.



(C) Icky

(U) From its beginnings as a bench model, Icky evolved into a chest-high box as wide as a refrigerator. On its top was a screen to view the located messages. Next to the screen were the reels and rollers for two 35mm microfilms. Underneath were the mechanisms that sped one of the films past the other and the ratchets that stepped the index film after each pass of the fast tape. Icky's optical sensing gate was designed to allow the location of message patterns of up to thirty columns of data. Typically, a bright light was pointed through masks and lenses which segregated the light into thirty parallel columns. If light penetrated the two films, it was directed to thirty small mirrors, which then sent the light beam to their photocells.

(U) The light management portion of the machine was complex and demanded perfect alignments. It was the demands of that photocell system that led to Icky's having only forty columns of data per inch of film, a density far less than Bush had promised the navy.

(U) More significant, Icky was not a digital machine. Like OP-20-G's other World War II microfilm devices, it wandered back to the use of analog circuits. But it did have a plugboard and resistor matrix system that allowed the selection of many different combinations of coincidences. Polygraphs of long lengths, or patterns of identical subgroups, or single-letter coincidences could be identified.

(U) Icky had another feature that went beyond the original Selector. Its coding system could be changed and its circuits switched so that it responded to the absence of light rather than its presence.[23] The navy's men found the blackout method much more efficient when the job was to search for coincident areas (such as code groups) rather than single columns of data. With its use, they could pack more than one letter in a column. They could register a five-letter (or number) message group.

(U) In the blackout system, the two tapes were reciprocally coded so that a matched column would admit no light. A two-of-five character

code allowed the use of that reciprocal scheme, but Icky's scanner could also accommodate Bush's older one-of-twenty-six pattern.[24]

(U) A Machine for Mrs. Driscoll's Special Problem

(U) Eastman designed and built another of the very few types of microfilm machines used by OP-20-G during the war. The Hypo assignment came in a rush, and, like Tessie, it took a year to complete.[25] The first Hypo was not in operation until October 1943.[26]

(U) The name, Hypo, came from the "Hypothetical Machine" proposal drawn up in response to the early requests by Mrs. Driscoll's Enigma group.[27] The project languished for a time, but ideas were formalized in March 1942. Machine design began six months later.[28] Hypo's task was to help Driscoll's small team make a traditional attack on the German Enigma. It was the first machine designed especially for the American work against the "E" machine.

~~(TS//SI)~~ In early 1942, the United States had hopes of cracking the Enigma in the same way it had broken earlier Japanese cipher machines — through methods that included what some called "statistical" analysis. Once the entire wheel wiring of "E" became known, it was hoped that large files (catalogs) could be constructed showing how each combination of enciphering wheels would "develop" high frequency letters, digraphs, or very common words. This "catalog" approach was not considered a "cribbing" attack; it was seen at the time as a statistical method although counting was not required.[29]

~~(TS//SI)~~ Constructing catalogs was very laborious. There had to be a card for each wheel combination and order, and for each position of the wheels. Such catalogs ran to hundreds of thousands of cards. Some filled an entire wall with file drawers. When put into book form, the heavy volumes demanded a long set of shelves.

~~(TS//SI)~~ Searching through all the entries to find those indicating which wheel settings might have produced the enciphered text was also very labor intensive.[30] That was why cryptanalysts around the world turned to the use of overlay sheets. They allowed a speedier and less demanding way of identifying the possible settings of the enciphering machines.[31] But they were limited and everyone wanted a faster method.

~~(TS//SI)~~ Investing in the construction of catalogs seemed very wise in 1942 because the United States did not have Bombes or the capability to continuously find the long and trustworthy cribs that made the British Bombes so powerful. The Americans did not even have the command of the techniques that had allowed Alan Turing to apply his indicator- (not crib-) based Banburismus IC-like system to "E" since the late 1930s.[32]

~~(TS//SI)~~ The Americans knew that Hypo would not be a cure-all machine, but they had little else to rely upon. The enormous amount of labor required to prepare Hypo's "database," the catalog, seemed worthwhile. Turning the catalog into a form that could be used by a high-speed machine meant creating a separate roll of film for each wheel combination. One was needed for each combination of the Enigma's slow and medium wheels and its reflector. Each frame on a film recorded the output of high frequency letters for a wheel position. A minimum set of the master films was fifty-six, each with over 17,000 frames.[33]

~~(TS//SI)~~ The preparation of the message film involved as much cryptanalytic persistence as did creating the "catalog" films. In one of the most common uses of Hypo, ciphertext was partially deciphered by pulling out the influence of the presumed stecker and fast wheel.[34] Then, the new text was put through a crude Letterwriter tape machine that recorded the text as tiny dots on microfilm. After that, an analyst had to wait the many minutes while the film was developed,

dried, and checked for possible defects. Producing the message film grew so burdensome that IBM and Eastman were ordered to cooperate to build a very expensive but labor saving card-to-film camera system for Hypo.[35]

(U) The Americans were so desperate for their own solution to the Enigma problem in 1942 that they did not want to admit to the limitations of the Hypo method. Hypo was not powerful. A Hypo run needed prior knowledge of the stecker, reflector, and wheel order used for an "E" message. With that information it could point out a "likely" starting position (window setting) for the Enigma wheels.[36] That was all it could do, and that was why only two Hypos were built by Eastman during the war.[37] Although OP-20-G's leaders might have envisioned rooms full of Hypos, each running a catalog film against a message, they soon came to treat the Eastman machine as only an adjunct to the Bombes.[38]

(U) Hypo looked and behaved much like Icky. It used two 35mm films. It was based on dot coding and the light bank data entry system.[39] The Hypo camera (for dot registration) was an improvement over Icky's, however. Data cards or tapes signaled which one of the lights in each column would be lit, and the tiny dots were recorded on the films with great precision.

(U) The men working on Hypo also conquered some of the problems of the film stepping mechanisms. That allowed a more precise and speedy comparison of the films. When the catalog and message films were placed on the machine, one was held stationary while the other flashed by it. As in Tessie and Icky, when the second film completed a revolution, the first was stepped one increment. That took less than five seconds.

(U) The "statistical" test in Hypo was a desired level of coincidence between text and master film spots. As in Tessie, Hypo's photocells monitored a zone rather than an individual column. The likely enciphering-wheel positions were identified simply by enough light reaching a photocell. When the machine stopped, its operator wrote down the location of the hit.

~~(TS//SI)~~ Hypo

(U) Hypo was an analog machine designed to locate. It was not coaxed to tally until the end of the war. Even then, it remained a very simple device. Despite that, Hypo proved as useful as Tessie did, though neither machine solved any systems by itself. Copies of Hypo were supplied to the army's cryptanalysts, and a second and more complex version was constructed for OP-20-G later in the war. By early 1945, Hypo was also being used against Japanese systems, after it had undergone some significant modifications.[40]

(U) A Paper War, Perhaps

(U) Hypo did not seem a winner in 1943, however. The delays in delivering Icky and Hypo had made Meader and Wenger fearful that Eastman would be unable to produce any device except the crude analog and plate IC Machine. In the critical first two years of the war, they also feared that IBM would not deliver its promised data conversion machines. In addition, there were signs that the next model of the Bush Comparator was in serious trouble. At the beginning of the war, OP-20-G was hedging all its technological bets. Although Howard had advised against a paper tape machine, the navy ordered him to stop his exploration of microfilm and draw up the essentials of an upgraded paper tape Bush Comparator. Howard helped draft a sketch of a slightly revised version of the old Comparator and sent it to the bureau's contractors, NCR and Gray Electric.[41] NCR and Gray set out with a great deal of enthusiasm, and the navy looked forward to a third version of the Comparator in a few months.

(U) Using the older 70-millimeter paper tape, but with room for thirty-two rather than twenty-six characters, the new Comparator tallied and it employed parallelism. It was able to handle and record up to five pattern tests at once. Its circuits and plugboards were more complex than the earlier model, and it was given an important new capability: it could locate. One tape could be held stationary while the other sped past it. The stationary tape then moved one increment for another pass of the second tape, stopping when a match was sensed.

(U) Four copies of the new paper tape Comparators were constructed between 1943 and 1945.[42] They seemed so promising when they were first designed that Britain asked for two. Later, its codebreakers decided against the machines, and the two were sent to the army's men at Arlington Hall.[43]

(U) The World War II paper tape Comparator proved an essential tool for the jobs that needed tallying, but, unfortunately, the new machines could not be convinced to run appreciably faster than the 1938 Comparator. The 1943-1945 models continued to have a relatively slow speed, eighty-five characters a second.

(U) One irksome feature of the Comparators was corrected by the end of the war. Like the original Bush Comparator, the 1943 device printed every result, appreciably slowing its performance. To speed it, an electronic circuit was added that allowed printing only when a highly improbable level of coincidence was computed.[44]

(U) The task of making a reliable punch was probably turned over to a Bass River, Massachusetts, firm. But even an expert private manufacturer could not overcome the punch's difficulties. The Oano Company had a tough time with the design and soon separated itself from the Comparator project.[45]

(U) By late 1942, the Comparator seemed destined to fail again. There was too much for Meader and Howard to keep under control.

(U) The Comparator Dies, Again

(U) John Howard spent the first months of 1942 traveling from place to place with Ralph Meader trying to force progress on the Eastman and NCR-Gray machines. By mid-1942 Meader and Wenger sensed that something was wrong with the Gray-NCR-MIT effort. When all the components were finally delivered to Washington, they did not fit together. The situation was so bad that the Comparator was returned to New York where the Gray and navy engineers redid most of its parts.

(U) When the Comparator was finally sent back to Washington, the navy engineers had to spend a great deal more of their valuable time

reworking the comparing and counter-printer units. That further delayed putting it to use.[46]

(U) The new Comparator did not go into operation until November 1943.[47]

(U) By then, the relations between Gray and OP-20-G had become quite tense. What the navy interpreted as disorganization in New York had much to do with its alienation.

(U) One explanation of why only four copies of the new Comparator were built is the difficulty "G" had controlling Gray's work. The lack of control became quite evident in mid-1944 when Gray Manufacturing took out a full-page advertisement in a widely read electronics journal. It showed the world what kind of tasks Gray had been doing for the government that had earned it an Army-Navy E award. The bottom third of the advertisement caused an emotional outburst in Washington. The last two items on the page stated:[48]

> (U) Optical work including the design and construction of various units in the projection field including photographic technique, motion picture, and optical systems involving condensers, prisms, and associated reflector equipment... communication equipment, electrical counting and calculating devices, including communications devices for producing or operating from perforated, inked, and coded tapes of various kinds.

(U) The advertisement infuriated the crew at OP-20-G. On top of all the manufacturing problems, Gray had endangered the security of "G's" RAM program. Larry Steinhardt could not contain himself when he read the advertisement. He tore it out of the journal and immediately sent it to Howard Engstrom with a message he wrote on it that said, "Note below an excellent description of the 70mm junkpile this outfit built. Please pass to Meader." Although the way the contractors had organized their work had much to do with the Comparator's problems, the underlying cause of all of the difficulties was stubborn technologies. They made it impossible for the nation's best engineers to fulfill Bush's promises.

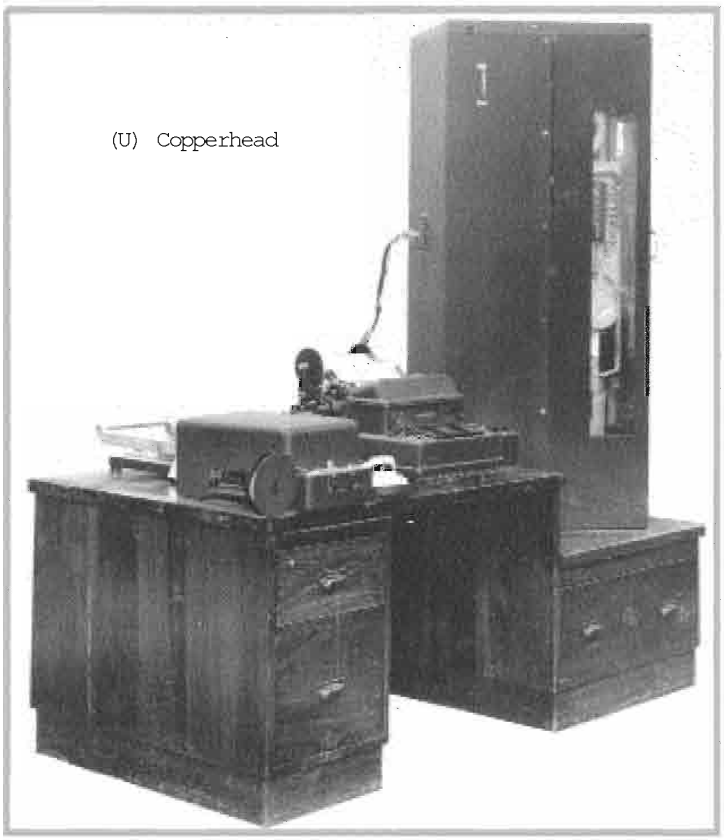
(U) The machines built between late 1943 and the end of the war had to be retreats from Bush's visions. The Copperheads, for example, had to be compromises between an engineer's pride and cryptanalytic needs. Other machines, such as Bulldozer and Duenna, were advances on the state of the electronic art, but they were based on ideas and techniques that were very different from those Bush had championed.

(U) Almost Another Digital Machine

(U) The other major attempt by the navy's team to fulfill Bush's promises was the Copperhead series.[49] Several different Copperheads were designed, and five copies of one of the series were built under Lawrence Steinhardt's direction at National Cash Register and at "M's" Washington engineering laboratory. Construction began in late 1943. Unfortunately, all of the more ambitious plans for the Copperheads had to be put aside because of technical problems and cryptologic emergencies. Only the copies of the rather simple Copperhead I were built.

(U) In 1943 the Atlantic crisis eased somewhat, giving "M" a bit of time to turn to Japanese problems. Lawrence Steinhardt was assigned the job of designing Rapid Machines to attack additive systems. Additive systems were codes with random numbers added or subtracted from the underlying numeric codes. Among many others, the major Japanese naval codes used additives. The fleet operational code, JN25, was of very special importance to American intelligence. But it had proven to be a very difficult adversary, especially because the Japanese frequently changed the long list of additives used to superencipher its messages.

(U) Discovering those additives was a tedious process. "G" had to call on many different methods of attack. IBM equipment had been modified to speed the identification of the superencipherments, but the process remained very slow and seemed in need of Rapid Machines. In 1943 it was decided to start an additive RAM program. Following the new habit of using the names of snakes for Japanese problems, the project was called Copperhead.



(U) Copperhead

(U) Still excited about optical-electronics, Steinhardt prepared the outlines for at least five different devices for the Copperhead problems. In his plans, the more complex models were to be able to add and subtract and to test statistical weights at electronic speeds.

~~(TS//SI)~~ Copperhead II, for example, was designed to be able to add clusters of additives to message text, then compare the results against a long list of known high-frequency code groups.

~~(S)~~ Copperhead V was a truly grand vision. If it had been built, it would have been twenty feet square. It would have had to have been that big to be able to match strings of additives against cipher text, then perform a true statistical test for nonrandom letter frequencies.[50] That called for sophisticated electronics and very high-speed input. The complex job assigned to "V" seemed to call for microfilm for input and perhaps for a vast memory. But Steinhardt was aware of the problems at Eastman, and at the onset of the Copperhead project he decided that the older punch tape approach would be best.

(U) More than a year was spent searching for a new tape and designing a revolutionary punch. After testing many materials, including aluminum foil, a 70mm opaque polystyrene tape was selected. It had the stability needed for very high-speed transport past the scanning station and did not distort when there were humidity changes. Of great importance, it could accommodate a data density about twice that of the Comparator's paper tapes.

(U) The Copperhead punch was a major engineering feat. Its main cabinet was over six feet tall and was wider than a phone booth. It was packed with delicate mechanical and electronic parts that perfectly aligned two tapes and then punched a reciprocal code. Each column on the tape had room for twenty-five tiny dots for message characters and several others for identification of the message. The punch was designed around the blackout system. Learning from earlier microfilm explorations that the absence of light was easier

to monitor than its presence, one tape was punched to be the complement of the two-of-five code on the other. The designers were so pleased with the Copperhead's punch, they built modified versions of it for the older Gray-NCR Comparators.

(U) Copperhead I used two sets of sophisticated motor-driven reels. It had a sensor system to manage the end-of-tape condition and the mechanical components needed to automatically rewind and step the tapes. Also, the machine was a landmark in optical sensing. It was built to scan one hundred message columns at a time!

(U) As with Icky, the Copperhead team had to take some significant backward steps to produce a machine to meet the war crises. Only one version of the Copperheads was built, and it was unable to count; it simply located message groups. As many as five of the Copperhead I machines were constructed and in operation by the opening of 1945. But they were very limited punched tape versions of the IC Machine and Icky.

(U) The Old Technologies Are the Best Technologies, for a Time

(U) In the spring of 1942, the Copperheads were not yet well-formed ideas, and all other Rapid Machines were in trouble. Even the refurbished 1938 Comparator, the only working Rapid machine, was not proving its worth. Lawrence Steinhardt had to strip it of many of its original functions to make it reliable enough for use in mid-1942.

~~(S)~~ By October, Steinhardt had built a crude prototype and had drawn the outlines for a much more sophisticated machine to identify Japanese code groups based on frequency criteria.

~~(S)~~ For the emergency machine, 700 of the most frequent groups were stored on film in descending order of frequency. The meaning of the group and its known relative frequency were listed next to the group's number and language equivalent. The "selector" was a simple relay store with "pin" settings indicating the frequency of the various code groups in the message being analyzed. When the message group and its frequency matched the composition of a group on the memory film, the film's entry was recorded by a fast-flash system. After the run, the new film was developed and sent to an analyst who used the information to help decrypt the message.[51]

~~(TS//SI)~~ After the first lash-up came a series of increasingly complex "Full Selectors." By the end of 1942, the first model had been modified through the addition of more sophisticated relay boxes; and by that time there were plans for a much larger and powerful device, Mercury.

~~(TS//SI)~~ Although the hopes for a huge electronic version were defeated, Mercury became a room full of relay racks that performed a sophisticated "weighted dictionary look-up" test to identify code groups.[52] Unfortunately for the navy, Mercury was not working until the summer of 1945.

(U) Meanwhile, the Tabulator's Revenge

(U) While Wenger worried about the absence of functioning Rapid Machines, those who had advocated the development of older technologies seemed to be vindicated. The old timers were in charge of tabulator development, and in 1942 they were the ones delivering cryptanalytic results.[53]

(U) IBM sent all the tabulators and sorters and collators OP-20-G could make room for, and the company began to create a host of very powerful additions for its machines. After "G" moved to its new quarters at an elegant girls' school on Nebraska Avenue and had adequate space, OP-20-G became one of the world's largest users of IBM equipment. "G's" IBM machines were count-

ed in the hundreds, and they used millions of punch cards a week.[54]

(U) Acquiring standard IBM machines was relatively easy. Alone among almost all business machine manufacturers, IBM had been permitted to continue manufacturing its products during the war. Its "tabs" remained stock items, and OP-20-G already had high priority status.

(U) But gaining IBM's commitment to continue to alter its machines (or to allow OP-20-G to do so) proved more difficult. Joseph Wenger had to make a personal visit to Tom Watson to convince him to grant OP-20-G's requests special attention. By the end of the war, IBM and the armed services' engineers, many of whom were drafted from IBM and were sent directly to Washington, had created modifications that allowed the electromechanical machines to perform all the cryptanalytic functions. Because of those modifications, IBM's equipment remained the foundation of OP-20-G's operations throughout the war.

(U) With the outbreak of war, the tabulator group at "G" was able to expand and to convince IBM to produce specialized equipment. IBM and the navy began a cooperative effort that lasted throughout the war.[55] A number of IBM men went to Washington, and a host of new attachments were developed. Some allowed more efficient additive stripping. New devices provided more effective multiple key sorting and the offset and comparison of messages for IC analysis. The location of code words was made faster by other additions to the tabulators, sorters, and punches.

(U) Although IBM played an important role in OP-20-G's war, it was not asked to take a significant part in the Rapid Machine program.[56] One reason for not calling on IBM was that OP-20-G was already asking a great deal of the company. In 1942 the requests by the tab group at "G" for electromechanical and relay devices were enough to keep the company's best men busy. The OP-20-G/Yard crew did not demand the creation of an all-purpose tabulator or a general-purpose relay computer, but they asked for some challenging engineering advances. The requests indicate the old-timers had long had their own alternatives to Bush's mid-1930s Rapid Machine proposals.

(U) As well as the special electromechanical attachments for OP-20-G's tabulators, IBM created ambitious relay additions. The new IBM devices were better able to identify and tally particular code groups and to search for repetitions of character patterns. Among the more ambitious proposals for IBM equipment were the Navy Change (NC) machines.

(U) The NC machines were more than standard tabs with a few additions hung on them. Some of the thirteen types of Navy Change machines came close to being special relay computers. Others had special high-speed electromechanical accumulators and some had electronic tubes.[57]

(U) IBM's Most Special Contribution

(U) During 1941 and early 1942, before Engstrom's group gained real power over machine development, and as the Eastman and Gray-NCR projects were faltering, IBM and the men at "G" created another innovative system, the Letterwriters. Those devices brought OP-20-G's data handling into the modern era because they linked teletype, tape, card, and film media. The Letterwriter system tied special electric typewriters to automatic tape and card punches and eventually to film processing machines.

(U) Before the war the radio intercept personnel wrote out the messages they heard on forms, then forwarded them by mail or keyed them as telegrams. Because OP-20-G had just begun to develop teletype and radio networks, it took

weeks to send all but the most vital messages from the Pacific.[58]

(U) There are somewhat conflicting stories about the origins of the Letterwriter (CXCO) equipment, perhaps because its prehistory was linked to so many different groups within the navy. The timing is not entirely clear, but sometime in late 1940 Hooper's previous connections to the man who had sold his advanced electric typewriter business to IBM led to some interest in perhaps modifying his machines to turn them into data processing devices.

(U) The interest was turned into action in early 1942 when a young IBM engineer entered the navy and was assigned to OP-20-G. John Skinner had worked on a special typewriter-teletype project at IBM. When he had enough experience to appreciate "G's" data processing problems, he contacted his ex-boss and arranged to have some equipment shipped to Washington.[59] After IBM engineers arrived with the devices and demonstrated their potential, there was an immediate request that IBM launch a major project. Within less than a year, the first production Letterwriter devices were delivered to the cryptanalysts.

(U) The timely appearance of the first machines was a result of IBM's earlier commercial efforts at its Electromatic division.[60] The system centered on a special electric typewriter, a tape punch, and a tape reader. It was hoped they would eventually allow the creation of machine-ready data directly from "G's" new international telegraph system.

(U) The Letterwriters were not intended to be analysis machines, but to fill the gap left by the delayed RAM program. The engineers in Washington turned the Writers into much more than data entry devices. By adding simple plugboards, the engineers made the machines produce worksheets for the cryptanalysts and change one code into another.[61] By 1942 the Letterwriters were evolving into machines for analysis. First, the typewriters were modified to allow the printing of more sophisticated worksheets. Plugboxes were added which allowed complex substitutions

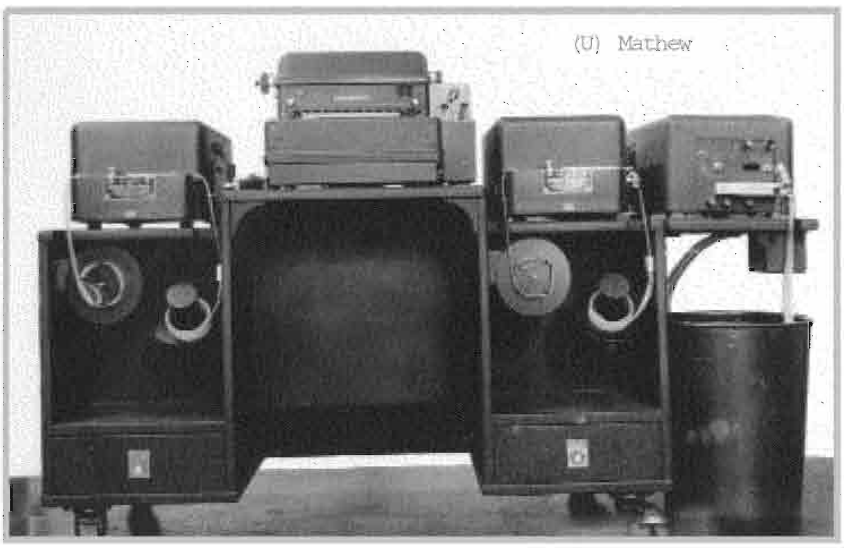
of one character for another. This helped determine the settings of the letter-changing plugboards on encryption machines. In addition to being useful for the analysis of steckering, the modified Letterwriters helped to strip cipher wheel patterns from messages.

(U) Simple changes made the Letterwriter equipment useful for another very important but time-consuming task, the analysis of wheel settings. When an analyst thought he had found the correct combinations on an enemy system, he would set up a copy of the encryption machine's wheels, lugs, and plugboards and type in parts of the encrypted message. He then examined the output to see if it was sensible. By coupling a Letterwriter tape-reader to one of the American copies of a foreign cipher machine, an analyst would not have to repeatedly enter a message through the machine's keyboard.

(U) In the Absence of Rapid Machines

(U) The delays in the delivery of the Rapid Machines led to another use for the Letterwriters. The Yard's men decided to build more far-reaching extensions of them. The first of their 1942 creations was a frequency counter. Aptly titled The Simple Frequency Counter, it was among the first of the new machines to be delivered to OP-20-G. The Simple Counter and its descendants had a power Bush's machines did not possess: they were able to recognize and record individual letters. The recognition, counting, and recording of particular letters and polygraphs demanded too many complex electronic circuits and parts for computer technology of the early 1940s.

(U) The Counter saved preparing IBM card decks and the many steps involved in repeated sorting. It was such an effective design that in 1943 a grand extension of the Counter was constructed at NCR. The NCR machine, Mike, tallied digraphs. Despite the low speed of such devices as Mike, the inability to deliver any Rapid Machines led the Yard's men to create yet another type of relay-electromechanical analyzer. They designed a machine, Mathew,[62] to perform additive stripping. Like the Counter, the Mathews proved reliable and were used throughout the war. Mathew was so rugged that it was applied to more than traditional stripping.[63] It was used on such jobs as removing the influence of a cipher wheel from an encrypted message. Over the years, the many Mathews (at least four were constructed) proved useful against a majority of the encryption systems attacked by OP-20-G. Mathew was not a general-purpose machine, however, and its technology dated from the 1920s. Its processing power was limited by the speed of its tape readers and its typewriter. But it was able to perform faster than the tabulators and to fulfill functions too complex for the electronic Rapid Machines of the era.



(U) Notes

1. ~~(S)~~ Almost all the documentation on the first year of the Eastman work and its first machines has been lost. For an insight into the problems of rushing into development and lack of coordination among the Eastman teams and the navy, see Rowley's comments about his mid-1943 tour of the Eastman projects, (S) NSA CCH Series XII Z, "Inspection of RAM Under Construction at NY and Rochester," 31 May 1943.

2. (U) The estimate of when the IC machine was ready is based on very circumstantial evidence. But it is clear that it was in use well before any other Rapid device, including the American Bombe. NSA RAM File, Report of R. I. Meader, Captain USNR, to J. H. Wenger, Captain, USN, "14 Days Training Duty, Report of," January 21, 1949, and Communications Intelligence Technical Paper l.a, "Technical Report: The Index of Coincidence Machine" March 1945.

3. (U) Typically, there were other precursors of the IC machine, including patented devices intended for business applications. See, for example, H. Soper, U. S. Patent 1,351,692, August 31, 1920.

4. (U) NSA RAM File, OP-20-G to OP-20-A, "Meeting with Prof. Howard," November 5, 1941, and Communications Intelligence Technical Paper 1-a, "Technical Report: The Index of Coincidence Machine" March 1945. ~~(TS//SI)~~ The first of the plate IC machines was delivered in August 1942. But it needed some fine-tuning and then had to be used in a controlled area rather than, as planned, at the crypt-analysts' desks. The device was redone several times before the end of the war, and the army group at SIS used several copies. Eventually, it adapted to the use of film as well as plates. ~~(S)~~ NSA CCH Series XII Z, Herbert W. Worden, "EDP Machine History." ~~(TS//SI)~~ CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. ~~(TS//SI)~~ CCH Series XII Z, copies of various MAC Outlines, circa 1953. (TS//SI) CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944 [sic].

5. ~~(S)~~ AHA ACC 1890, February 27, 1943, "Accuracy of the I.C. Machine." AHA ACC 1890, "New I.C. Equipment and Alterations Made on Old Equipment." AHA ACC 1890, August 2, 1943, "Electronic Use of I. C. Projectors." AHA ACC 1890, D-GM-5 to GM-5 "Changes Made on I.C. Reader and Camera."

6. ~~(TS//SI)~~ On the confusion over the first of Eastman's film machines, Tessie, S 409, Brief Descriptions of RAM Equipment, Navy Dept, Washington, D. C., 1947, and Leroy Wheatley, Brief Descriptions of Analytic Machines, NSA 34, 1954. AHA ACC 1890, GM-2 to G-50, "Tetra Projector #2 (RAM-5): Name for." AHA ACC 1890, February 27, 1943, "Accuracy of the I. C. Machine."

7. ~~(C)~~ NSA CCH Series XII Z, NSA OH 16-85, Oral History Interview with Capt. John A. Skinner, 25 September 1985, 24.

8. ~~(S)~~ NSA CCH Series XII Z, J. A. Skinner, "Proposal for Decoding Device," OP-20-GM, 16 February 1943.

9. (U) Four-character code groups were used in important German and Japanese systems. It is not known if Tessie was originally built for use against both of them. The Japanese high-level fleet code used a four-digit code. The very important U-boat short signal code was used to flash location messages and was tapped by the Allies for cribs. The short signals were also used as cribs into the four-wheel Enigma systems. Tessie was modified later in the war specifically for the German short signals. RAM File, History of OP-20-G /NCML/4e, 106.

10. ~~(S)~~ AHA, ACC 1890, OP-20-GM-10 to OP-20-GN, January 23, 1943, "Ram-2, Improvements on Performance Of." AHA, ACC 1890, M-4 to CM-5 March 6, 1943, RAM-2, "Changes in Operation of." AHA, ACC 24880, CIT Technical Paper 9, Tessie SS, Vol I, CNO, Navy Dept, Washington, D.C., May 1945. AHA ACC 1890, "RAM-2 Operating Procedures."

11. (U) Near the end of the war, counting circuits were added to the device, making it a weak version of a microfilm Bush Comparator. NSA RAM File, History of OP-20-G/NCML/4e.

12. ~~(TS)~~ AHA, ACC 24880, CIT Technical Paper 9, "Tessie SS, Vol I," CNO, Navy Dept., Washington, D.C., May 1945.

13. ~~(S)~~ AHA, ACC 1890, Special Applications Section, Bureau of Ships, to OP-20-GM, August 11, 1943, "Equipment Developed by EK Co."

14. ~~(S)~~ AHA Acc 1890, "Report on Enigma Test Run on RAM-2, January 7-8, 1943." AHA ACC 1890, OP-20-GM-10 to OP-20-GM, January 23, 1943, "RAM-2, Improvements on Performance of." AHA ACC 1890, GM-4 to GM, June 23, 1943, "RAM-2, Technical Details of recent work on." AHA ACC 1890, GM-4 to GM, June 30, 1943, "Ram-2, Comments on Performance of" and July 20, 1943, "RAM-2 Camera #4, comments on design of."

15. ~~(TS)~~ NSA AHA ACC 1890, GM-4 to GM, June 23, 1943, "RAM-2 Technical Details of recent work on."

16. ~~(S)~~ NSA AHA ACC 1890, GM-10 to GM, January 23, 1943, "RAM-2, Improvements on Performance of." AHA ACC 1890, GM-4 to GM, "24-hour trial run in E traffic using RAM-2."

17. (U) Letters from Joseph Eachus circa 1988. Near the very end of the war, counting circuits were added to the device, making it a weak version of a microfilm Bush Comparator. But until then it did not even record the place where a "hit" occurred. NSA RAM File, History of OP-20-G/NCML/4e.

18. ~~(S//SI)~~ NSA RAM File, Report of R. I. Meader, Captain USNR to J. N. Wenger, Captain, USN, "14 Days Training Duty, Report of," January 21, 1949. On Tessie's rebirth as the Symmetric Sequence Machine in 1944, ~~(S)~~ NSA CCH Series XII Z, RAM list and Conference at Dayton, 11 April 1945, ~~(TS)~~ NSA AHA ACC 24880, CIT Technical Paper 9, "Tessie SS, Vol I," CNO Navy Dept. Washington, D.C., May 1945. AHA ACC 1890, GM-2 to G-50, May 25, 1944, "Tessie: More Complete Conversion to symmetrical sequence work."

19. ~~(TS//SI)~~ On the meaning of the terms, NSA CCH Collection, "Army-Navy, Descriptive Dictionary of Cryptologic Terms," Headquarters, Army Security Agency, February 1947.

20. ~~(TS)~~ NSA CCH Series XII Z, "Brief Description of RAM Equipment," Navy Dept. Washington, D. C., October 1947, 37.

21. ~~(S)~~ NSA CCH Series XII Z, A. W. Tyler, "Tetragraph Machine II," (ICKY) 21 February 1944.

22. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. ~~(S)~~ NSA CCH Series XII Z, "ICKY," circa 1944. ~~(TS//SI)~~ NSA CCH Series XII Z, "Hypo I - Hypo III," March 1954.

23. (U) NSA RAM File, "M.A.C. Outlines #17, 70mm Comparator," April 1947. The German inventor, Goldberg, had chosen the blackout methods. Emanuel Goldberg, U. S. Patent 1,838,389, Statistical Machine, December 29, 1931, Filed April 5, 1928.

24. (U) NSA RAM File, Communications Intelligence Paper 6, ICKY, Washington, D.C. April, 1945.

25. ~~(TS//SI)~~ Hypo was delivered to OP-20-G in October 1943, just as the bombes became operational. ~~(TS//SI)~~ NSA CCH Series XII Z, "Hypo I - Hypo III," March 1954.

26. ~~(TS//SI)~~ NSA CCH Series XII Z, "Hypo I - Hypo III," March 1954.

27. (U) NSA RAM File, "List of Equipment for Enigma Problems." Note that high-level policy had led the navy to place little emphasis on Hypo during 1941. Howard was told that Mrs. Driscoll's problem was "not that important" and to place emphasis on other machines. NSA RAM File, November 14, 1941, Bureau of Ships to Howard, "Driscoll's problem not that important."

28. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [sic], 51.

29. ~~(TS//SI)~~ Hypo's initial outlines contained an explanation of how it might be constructed so as to be used as a true crib device. ~~(TS//SI)~~ NSA CCH Series XII Z, CNO CIT Technical Paper TS-10/E-3, "Enigma Series: Vol. #, Statistical Studies," January 1946.

30. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [sic], 117.

31. (U) Britain also had statistical methods, such as Banburismus, which brought forth some ideas about a film machine in England, perhaps as early as 1939. England may have built film devices that equaled or exceeded those built in the United States during the war. Andrew Hodges, Alan Turing: The Enigma (New York: Simon and Schuster, 1983), 178, 233.

32. ~~(TS)~~ NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945." On the state of American knowledge of Enigma methods at the outbreak of the war, ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [sic].

33. ~~(TS//SI)~~ NSA CCH Series XII Z, CNO CIT Technical Paper TS-10/E-3, "Enigma Series: Statistical Studies," January 1946, E3-12.

34. ~~(TS//SI)~~ Two different uses of Hypo are described in the existing literature. For the one described here, see ~~(TS//SI)~~ NSA CCH Series XII Z, "Hypo I - Hypo III," March 1954, and for the other more crib-like description see, ~~(TS//SI)~~ NSA CCH Series XII Z, CNO CIT Technical Paper TS-10/E-3, "Enigma Series: Statistical Studies," January 1946.

35. ~~(TS//SI)~~ NSA CCH Series XII Z, "Hypo I - Hypo III," March 1954.

36. ~~(C)~~ NSA CCH Series XII Z, Descriptions of NSA Early SPDs and Computers, as compiled from various NSA sources. ~~(TS//SI)~~ NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. ~~(TS//SI)~~ NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953.

37. ~~(C)~~ However, Lawrence Steinhardt completed another in 1946 and a fourth in the early 1950s. (C) NSA CCH Series XII Z, Descriptions of NSA Early SPDs and Computers, as compiled from various NSA sources.

38. ~~(S)~~ Hypo was modified for use against the Japanese 157 Jade machine. ~~(S)~~ NSA CCH Series XII Z, H. H. Campaigne "Use of Hypo on the JN-157," 21 February 1944.

39. (U) NSA RAM File, CNO, USNC, CITP TO-33 "Overhaul of Hypo #1," Washington, D.C., June 1945. Letters to author from Joseph Eachus. Microfilm and Hypo.

40. (U) NSA RAM File, W. A. Wright to OP-20-G February 21, 1944, "Comparison of Army and Navy Enigma Equipment." NARA RG457, SRH-200, "Army-Navy Collaboration 1931-1945," 216-8. For later models and use against Japanese systems: NSA RAM File, June 16, 1947, OP-20-G Research Committee Meeting; January 5, 1945, "Hypo Stepping Switch"; "History of OP-20-G /NCML/4e"; and CNO, U.S. Naval Communications, CITP TO-24 "JN-37 Problem on Hypo," Washington, D.C., May 1945.

41. (U) Hagley Museum and Library, Accession 1825, Honeywell v Sperry-Rand, Trial Records, Deposition of Joseph Desch. NARA Suitland, OSRD Contract Files, OEM-275 November 28,1941, "NCR-MIT counters." NSA RAM Files, Joseph Desch to OSRD, February 12,1943, "Only Navy work at NCR."

42. (U) The estimates of the number of Comparators built during the war vary from six to as many as twenty-eight. Four is the correct figure. The reason for the high estimate was probably that all the later postwar Comparator-like machines were included.

43. ~~(S)~~ Office of Naval Research, Patent File on "Electronic Comparator, Vannevar Bush." V. Bush, U.S. Patent, February 17, 1959, "Electronic Comparator," 2,873,912. Of importance for the postwar history of the Rapid Selector, the Comparators became the basis for the navy's patent claims over optical-electronic devices. ~~(S)~~ On the British and army comparators, ~~(S)~~ NSA CCH Series XI E, Hagelin, Box 2, Folder, "Comparators.."

44. ~~(S)~~ On the rare event circuit, (S) NSA CCH Series XII Z, J. H Howard, "70MM Comparator & Rare Event Circuit," 27 October 1944.

45. ~~(TS//SI)~~ NSA CCH Series XI E Hagelin, Box,"Notes on various topics."

46. ~~(S)~~ NSA CCH Series XII Z, "Inspection of RAM Under Construction at NY and Rochester," 31 May 1943. ~~(S)~~ NSA CCH Series XI E, Hagelin, Box 2, Folder, "Comparators."

47. (U) NSA RAM File, Report of R. I. Meader, Captain USNR to J. N. Wenger, Captain, USN, "14 Days Training Duty, Report of," January 21, 1949. NSA RAM File, CNO, U. S. Naval Communications, CITP TS "Machine Descriptions," Washington, D.C., circa 1945. "Mike, Comparator." NCML-CSAW Message File, April 14, 1944, "Punch being modified at Gray." The Americans were not the only ones to have problems with tape machines. Britain's attempts to create similar machines, the Robinsons, faced even greater difficulties. As the new Bush Comparator was going into operation, Britain was still testing its first two tape

systems and would soon turn away from such devices because coordinating the tapes was too difficult. Allen W. M. Coombs, "The Making of Colossus" Annals of the History of Computing 5 (1983): 254. Brian Randell, "The Colossus," in N. Metropolis et al. (ed.), A History of Computing in the Twentieth Century, (New York, 1980), 47-92.

48. ~~(S)~~ NSA CCH Series XII Z, Gray Manufacturing Co., "Design Advertisement," June 1944.

49. (U) NSA NCML-CSAW Message File, messages to and from Dayton and Washington, November 1943 to March 1945. NSA RAM File, "Final Report, Copperhead II," Communications Intelligence Paper 24, and Communications Intelligence Paper 41, "Copperhead I Punch and Copperhead I Scanner."

50. ~~(S)~~ NSA CCH Series XII Z, RAM list and Conference at Dayton, 11 April 1945. (S) Steinhardt, L. H., "Copperhead II (Project M-230) Final Report," 9 November 1944. ~~(S)~~ NSA CCH Series XII Z, "Use of RAM on Jap Naval Problems of BII type," 9 June 1944.

51. ~~(S)~~ NSA CCH Series XII Z, L. R. Steinhardt, "Full Selector," 31 October 1942.

52. ~~(S)~~ NSA CCH Series XII Z, L. R. Steinhardt, "Full Selector," 31 October 1942. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

53. (~~TS//SI~~) The group of practical engineers were probably the ones who built the rather crude but useful electromechanical Shinn and Ely machines during 1941 and early 1942. ~~(S)~~ NSA CCH Series XII Z, OP-20-G War Diary, OP-20-GS, Machine Processing, February 1942-January 1945. (~~TS//SI~~) NSA CCH Local Archive, "Army-Navy Descriptive Dictionary of Cryptologic Terms," Army Security Agency, February 1947. The descriptions of these machines were not located. IBM aids OP-20-G, 1942.

54. (U) NARA RG457, SRH-349, "Achievements of the SSA In World War H," 18. In January 1941 OP-20-G Washington had 16 IBM machines, in 1945, some 200. NARA RG457, SRH-197, "US Navy Communications Intelligence, Organization, Liaison and Collaboration 1941-1945." University of Pennsylvania, Van Pelt Library Archives, Papers of John Mauchly, October 11, 1944, "Mauchly notes on meeting with Kullback of ASA."

55. (U) NSA RAM File, OP-20-G to Radio Sound Branch, September 5, 1941, January 16, 1942. NSA, Tabulating Machine File, July 24, 1941 and December 6, 1941 to Radio Sound Branch, Design Division, Bureau of Ships. On frictions with IBM, CNO to BuEng 1-3-24; "Conference With IBM," May 23, 1934.

56. (U) NSA, Tabulating Machine File, OP-20-G to BuShips, July 24, 1941.

57. ~~(TS)~~ NSA CCH Series XI E, Hagelin, Box 2, "NC Machines." The various types of NC machines were

NC 1: consecutive numbering device

C2: relay adder to mechanize decryption of additive cipher

NC3: "single eliminator," which selected duplicate cards in a deck leaving only unique ones; it used vacuum tube circuits and read 300 cards a minute (NC 12 replaced it).

NC4: selective punch whose relay additions allowed a variety of substitutions to be punched on cards

NC5: pattern punch whose abilities included searching for isomorphs

NC6: column differencer whose amazing accumulator could hold up to 400 items, recognize the largest, and punch an indicating card. It also matched high frequency text against stripped code

NC7: percentage selector whose special relay box allowed round-robin repeat searches and selected them on a percentage of coincidence basis

NC8: automatic circuit changer, which allowed automatic switching of alpha or numeric data among as many as twenty-five plugboards and the rearrangement columnar data

NC9: only a prototype of this special substitution punch was built.

NC10 and NC11: typewriter-like near off-the-shelf devices

NC12: replaced the NC3

NC 13: converted IBM cards to and from microfilm, if it worked; the conversion from microfilm to cards was a true innovation at the time

58. (U) Interview with Fred Parker, and his award-winning article, "The Unsolved Messages of Pearl Harbor," *Cryptologia* 13 (1991): 295.

59. (~~TS//SI~~) NSA CCH Series XII Z, John A. Skinner, "The CXCO Story," NSA *Technical Journal*, VXI (Fall 1971), 21-37.

60. (U) IBM would offer similar equipment to commercial users after the war. For a list of Letterwriter CXCO equipment available from the newly named Justo-writer division of IBM in 1947, see Hagley Museum and Library, Accession 2015, ERA Materials, "Seminar Meeting, Tuesday, March 11, 1947."

61. (U) Private Paper on NSA Machinery, 1985. NSA RAM File, CNO, U. S. Naval Communications, CITP TS Machine Descriptions, Washington, D.C., circa 1945. "Letterwriter." NSA RAM File, CNO, U.S. Naval Communications, CITP, "Machine Comparisons," June 1946.

62. (U) The name was frequently spelled as Matthew.

63. (U) NSA RAM File, CNO, U.S. Naval Communications, CITS Technical Paper TS-48, "Machine Comparisons," June 1946.

Chapter 4

(U) Meeting the Crisis: Ultra and the Bombe

(U) Looking Ahead – Ultra Saves RAM and OP-20-G Creates a Science Company

(U) The history of OP-20-G's cryptanalytic machine program would have been very different if Britain had had the power to read the German U-boat messages during 1942. On the chance that its men could beat the British to a reentry into the U-boat Enigma, OP-20-G was granted its long-sought Rapid Machine program and its own factory and workforce. But the establishment of what became known as the Naval Computing Machine Laboratory came at a price. Because the American navy had not attended to the Enigma and because Hooper and Wenger's pleas for machine development in the 1930s were not fully heeded, OP-20-G had to defer its attempts to create advanced electronic computers for pure cryptanalysis. To solve the "E" problem, the machine group spent most of its first year and one-half, and much of the next two years, coaxing electromechanical components into doing things never before expected of them. The conglomeration of electrical, mechanical and electronic parts called Bombes turned Engstrom's men away from solving the fundamental problems associated with Bush's designs, and away from an exploration of the possibilities of a general-purpose electronic machine.[1]

(U) The "E" Machine

(U) The Bombe was the example of the need for a technological retreat to deal with a cryptologic emergency. Despite Germany's destruction during World War I and the crippling burdens imposed on it under the peace, it built a strong codemaking capability during the 1920s and 1930s. At the center was the Enigma encryption machine, the workhorse of its military communications networks.

(U) The Enigma was a typewriter-size device that could be used in the field as well as in an office. It was electromechanical and used batteries to provide the electric current which passed through a series of shifting transposition rotors (commutators) to yield an extremely long encryption cycle. Physically, Enigma consisted of a keyboard to enter letters, a cascade of moving wheels that scrambled their inputs, a reversing wheel that sent the electrical impulses back through the wheels, a plugboard that further mixed the letters, and a series of lamps that showed the final result of the encryption.

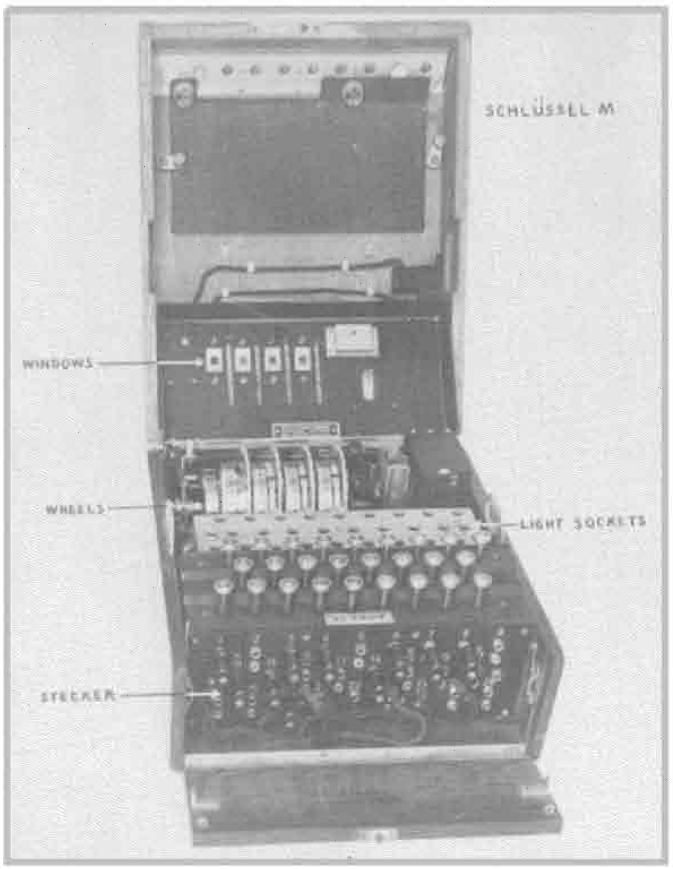
(U) The Germans felt safe because they calculated that even if the wiring of the code wheels were known, it would take impossibly long for an enemy to identify the particular "key" settings of a message. In its early configuration, with just three of five available code wheels being used and no plugboard, Enigma had over one million possible settings.[2]

(U) When the plugboard was added to the military versions, the Germans felt even more confident. The possible combinations jumped into the range of two hundred million million million! That made intellectually blind attacks on the machine an impossibility.[3]

(U) One World War II cryptanalyst explained why there was a critical need for revolutionary methods, and machines which could reduce the number of possible "E" settings that had to be examined, by stating:[4] "If every man, woman and child in the British Isles were given an Enigma machine, they would have to try 3,000,000 pos-

sibilities on each starting position on each wheel order and would work their whole life to break one key."

(U) The Germans constantly changed the "E" to make it stronger. They enhanced the system by increasing the number of wheels to choose from. By the end of the war, German codemen could choose from as many as nine main scrambling wheels when selecting a setup for their machines. In 1942 the Atlantic U-boat system added a fourth wheel inside its machines. Later in the war, the Germans made the machine more robust when they changed the plugboard and attached the Uhr box. The Uhr added another level of complexity by eliminating some of the cryptologic weaknesses of the plugboards.



(U) Enigma

(U) Perhaps most frightening to the Allies was the "pluggable reflector" which appeared on some German air force and army networks near the end of the war. It created more combinations to hunt through than had the introduction of a fourth wheel.[5]

(U) The Germans were particularly sensitive to a weakness in all encryption systems, the vulnerability of internal indicators. Indicators were the brief instructions in each transmission that told a recipient how to set the remaining components of his Enigma, the ones not specified in a network's instruction books. Unlike the keys specified for all users in a network, indicators were selected by operators and changed with each message. Unfortunately for the Germans, they found no way to prevent their enemies from using those indicators to penetrate some of the "E" networks. The exploitation of the indicators was one of the most important ways that Poland's cryptanalysts entered the Enigma systems in the early 1930s.

(U) The Poles were helped by stolen documents and used many more approaches than the attack based on the indicators.[6]

(U) Only a Few Were Able and Willing to Tackle "E"

(U) Poland created what Stanford Hooper and William Friedman yearned to have in America: an office devoted to pure cryptanalysis. Poland's codebreaking bureau was able to recruit several bright young mathematicians who, as early as 1930, began to apply group theory and other advanced mathematical and statistical techniques to the German Enigma system. With the help of stolen documents provided by the French, the Poles began to understand and then penetrate the Enigma. They

were reading many German systems by the mid-1930s. By supplementing their mathematical analyses with the weaknesses of some of the operational uses of the Enigma, such as repeating the indicators for a message or picking keys in a non-random way, the Poles were able to avoid using brute force searches that tested every possible "E" setting. They even learned how to avoid using data-heavy statistical analysis. A significant and fundamental discovery by the Poles was that the forbidding and seemingly impregnable plugboard was irrelevant in some cryptologic contexts. The discovery about the plugboard reduced the number of tests needed to identify an Enigma's setup by millions.

(U) The Poles Automate Cryptanalysis in Their Special Way

(U) The Polish group also called upon automation in the early 1930s. Much work and genius went into the invention of an electromechanical machine, the Cyclometer, which automatically generated all the patterns produced by various Enigma settings. The Cyclometer was not a statistical machine or a device that could lead to a modern computer, however. It was an electromechanical rig that produced a card catalog so analysts, in just a few minutes, could go from the indicators in a message to the Enigma setup.

(U) In 1938, to meet a change in the way the Enigma's settings were communicated, the Poles invented their version of an electromechanical automaton, the Bomba.[7] The Bomba was a set of linked Enigma machines that tested for the letter cycles produced by the setting indicators in Enigma messages.

~~(S)~~ One explanation for the use of the strange name, Bomba, is based on the mechanical crudeness of the first Polish machines. To save precious construction time and parts, when the Bomba found a hit, a weight on the side of the machine was dislodged and dropped to the concrete floor with a very loud "bang."[8]

(U) The special-purpose Bomba was based upon a negative logic and used a special "crib" composed of the message indicators. The Bomba's goal was to eliminate the wheel orders and wheel positions that could not have produced the letter-to-letter cycles in an indicator.

(U) The Poles had constructed six of the Bombes, one for each possible wheel order. That was adequate when the Enigmas came with only three encryption wheels to choose from. But just as the first Bombas were put into operation, the Poles had to face an increase in the number of Enigma wheels, then an alteration in the use of the "E" plugboard. Those changes demanded ten times the number of Bombas for a timely search. The Poles were too exhausted to produce so many additional machines. Their attempt to reenter Enigma through new statistical and hand methods was frustrated by a lack of manpower and time.[9]

(U) Keeping the Bomba Secret for Too Long

(U) When the invasion of Poland seemed imminent, and when the Warsaw team could not sustain its automation efforts, the Poles started to pass their secrets to their friends.[10] It was not until late summer 1939, when the Poles had to have help in producing more of their vital overlay sheets and Bombas, that Britain and France were informed of how the Polish men had been able to read Enigma messages.

~~(TS//SI)~~ The British representatives were grateful for the information, but they also were very upset that they had not been told the secrets when they had met with the Poles in February 1939. Their anger almost led to a break between the two sets of codebreakers. One high-level British codeman, not realizing the Poles understood English, vented his frustration by berating them while in their limousine. Fortunately, the

diplomatic skills of his countrymen calmed the Poles.[11]

(U) Despite the affront, the Poles gave the Englishmen copies of the Enigmas they had reverse-engineered and told them of the many ways to identify the various German Enigma radio networks. But on the eve of the invasion of Poland, the Germans made several more shattering changes in their Enigma systems, which made Britain's task nearly impossible. After France was overrun, Britain was left with the responsibility for making a new beginning against the Enigma.[12] To exploit both her own previous work and the gifts of the Poles, Britain expanded its Government Code and Cypher School (GC&CS) and established the now famous Bletchley Park.

(U) A Fresh Start against "E"

(U) Despite the belief among many British influentials that the German code and cipher systems, especially their naval ones, would never be broken, Britain made a significant commitment to cryptanalysis.[13]

(U) Teams of brilliant men and women were recruited from the universities to work on the various Axis systems. Alan Turing was only one of the Bletchley wonders who were recognized experts in mathematics and logic.[14] Under intense pressure, by 1940 he and others at GC&CS began to create the many invaluable techniques and electrical devices that eventually gave birth to the Ultra Secret. For example, the first Bletchley version of its Bombe was in operation in early 1940.The next important configuration, with the ingenious diagonal board for the critically needed simultaneous testing of plugboard settings, was running by August.[15] That Turing-Welchman Bombe of 1940 was a cousin, but a very distant one, of the Polish Bomba.

(U) Turing explored many varieties of possible solutions, hoping to find one that would withstand changes in "E" and its usage. Although actively seeking pure methods to attack the Enigma, Turing eventually had to accept the use of a dependent and near brute force approach.[16]

(U) At first he thought he had discovered a relatively pure method. In 1939 when he went to the naval section at Bletchley Park, Hut 8, Turing sought a robust and universal means of attack. After learning as much as possible about Enigma, he called on his knowledge of statistics and probability. He arrived at a method quite like the one Wenger and Bush had chosen for the Comparator, the Index of Coincidence. The name given to his cluster of statistical methods was "Banburismus."

~~(TS)~~ Turing focused his statistical powers on the German naval systems because they had been the most intransigent. He thought that if his "Banburismus" methods proved of worth against them, they could be generalized to all cipher machine systems.[17] The general logic of Banburismus was, like the IC, based on the statistical characteristics of language. The goal of both approaches was also the same: to identify messages that had been enciphered with the same "key" or machine setting. Once such a "depth" had been pinpointed, the machine setting could be found and the cipher messages turned into readable text.

~~(TS)~~ More than the logic and goals were similar. The techniques were essentially the same. Two messages that were thought to have been produced by the same key (as suggested by such evidence as the same callsigns and indicators), were placed one above the other. Coincidences were then counted and evaluated against the number expected by chance. The counting was repeated for each of the offsets. Turing even mechanized the process through the use of overlay sheets. Holes were punched in the sheets to represent the text. When the two sheets were superimposed, the coincident holes were very easy to identify. That allowed relatively unskilled labor to be used to tally the results. The overlap

method could also be used to exploit the information that could be drawn out of the indicators in the messages.

(~~TS~~) Turing went further with his ideas. He developed his IC-like approach into an elegant predictive system. His "bans" were statistical estimates of how likely it would be that two messages would prove to be of value in identifying the cipher keys. Such estimates allowed the cryptanalysts to make rational decisions about allocating their very precious time. They could concentrate their skills on the messages most likely to yield results.

(~~TS~~) Banburismus was Britain's initial method of attack on the German naval Enigma and continued as its most powerful tool until 1942. Helped by other techniques, such as "scritching,"[18] it was the way Hut 8 identified two of the three wheels used in an Enigma setting. Once the wheels were specified, the analysts could attack the other parts of the Enigma "key."

(~~TS~~) Unfortunately, while Turing's Banburismus was an advance on the state of cryptanalytic art, it was not strong enough to be a timeless and independent conqueror of Enigma. Its target of the early 1940s, the naval Enigma, was too rugged. The success of Banburismus depended, despite Turing's hopes, on knowing the contents of the very special "E" instruction sheets the German Navy used. From 1939 to the end of 1942, when Banburismus was no longer employed against the naval systems, the British had to capture or, with a great expenditure of manpower, reconstruct bigram and other complex tables that were used to superencrypt the naval "E" indicators. Banburismus went blind several times when the Germans changed the tables.

(~~TS//SI~~) As used against the naval systems, Banburismus was also dependent upon having a very large number of messages in "depth." As many as 300 messages might be needed to allow the identification of the Enigma wheels.[19] Even with enough messages, Banburismus needed more help.

(~~TS//SI~~) Banburismus was elegant, but it was not self-sufficient. Wheel wiring had to be known, and "cribs" and much hand testing were required to identify the plugboard connections and wheel turnover points.[20] A very large investment had to be made in compiling a catalog of all the possible enciphernents of the German word for "first." It was needed to supplement the statistical analysis with primitive cribbing. That "Eins" catalog drained the resources of Bletchley Park, but it did not prove as timesaving as hoped. Moving from the suspected location of the crib word "Eins" to the catalog entry for its possible setting and then testing to see if the key had truly been found were too demanding.[21]

(~~TS~~) In near desperation, Turing turned to a full-blown crib approach. He relegated Banburismus to being an adjunct to his version of the Bomba. By 1940 he had designed a machine that was to be a high-speed, automated, and near universal "catalog." His device would take any long crib and test it against all possible wheel settings of an Enigma and do it within minutes.

(U) Given the technology available to him, this rather crude method seemed the only alternative. Thus, while he explored the application of other statistical methods to the "E" problem, he sketched out a new Bombe.[22] It used some of the ideas of the Polish Bomba, but the British Bombe and its logic were special.

(U) Turing's Bombe was an electromechanical analog of the Enigma.[23] It was based on identifying logical contradictions as represented by flows of electricity. Its banks of interconnected high-speed "E" wheels spun until they found a setting that might have produced the crib setup on the machine. Like the Bomba, it needed to search through all the wheel settings, and it accepted the

consequences of relying upon a special-purpose machine.

(U) Turing's Bombe needed a great deal of prior information about German networks and their keys. His crib attack was premised on knowing the wiring and turnover pattern of each "E" wheel, and it needed insights into the plugboard and other settings of each Enigma net. Turing knew his Bombe could have been made as useless as the Polish machine if the Germans significantly increased the number of letters changed by the "E's" plugboard, if they stopped using stereotyped phrases at the beginning of their messages, or if they ended the practice of sending "E" messages on simpler cipher systems. He also knew that his machines would be expensive and that their construction would perhaps ask too much of Britain's manufacturers.

~~(TS)~~ Turing faced some stiff opposition when he requested that a program be funded. Although he explained that Banburismus would reduce the number of wheel combinations that had to be tested from more than 300 to fewer than thirty, thus calling for only a dozen Bombes, administrators at Bletchley had serious concerns.[24] They did not want to waste money and time on the construction of a machine that had to correctly scan hundreds of circuits within a fraction of a second. They knew the dangers in trying to construct a reliable machine that was to have ten miles of wire, a million soldered connections, and a clutter of mechanical parts.

(U) More than the machinery was at risk. To find the right kind of cribs for the Bombes called for the creation of a new and large group of analysts to constantly mine German intercepts for new leads.[25]

(U) Turing made his machine as universal as possible. Although it followed the logic of pointing to the wheel settings that could not be eliminated, it tested the settings against letter loops from within relatively long plaintext phrases (cribs) in messages. Relying upon words within messages rather than indicators guaranteed a longer life to his Bombes and promised fewer false drops.

(U) A bit of luck made the Bombe even stronger. Before Turing had finished his design for a machine to attack the three-wheel Enigmas, a young mathematician appeared at Bletchley Park whose insight multiplied the Bombe's abilities. Gordon Welchman's suggestion for the "diagonal board" allowed an instantaneous test for the influence of the plugboard setting and allowed the effective use of relatively "weak" cribs, ones without long letter loops.[26]

(U) Analog and Parallel May Be Fast, But ...

(U) Although electronics was tempting and although men like Turing knew that digital processing would become the basis for modern computers, a large number of machines had to be put in operation in weeks, not years. Britain needed working machines immediately. In late 1939 GC&CS's managers had to turn to someone who could produce immediate and sure-fire technical results. They found the right man: "Doc" Harold Keen, the head engineer at Britain's version of IBM, the British Tabulating Machine Company. Keen built a prototype in a few weeks and was able to begin sending some operational Bombes to GC&CS in a few months. One reason for his fast work was the use of standard, tried-and-true parts and analog logic.

(U) To match Turing's logic, Keen designed new five-inch commutator drums that were hard rubber and metal contact imitations of a double Enigma wheel.[27] The drums were arranged in banks of three, each being a double analog of an Enigma scrambler unit. One wheel in each bank was run continuously, another moved after a full revolution of the first, and the last stepped after the other two had completed their cycles.

(U) As the Bombe's wheels spun over the commutator connections, they created instantaneous multiple electrical pathways through the other banks. Then the electrical charges went to the relays that matched the flows against the crib. At the same time, they surged through the Welchman diagonal board to test the assumptions about the setup of the "E" plugboard.

(U) In the first models a great deal was expected of the operators. To identify the wheel positions when a hit was encountered, they had to touch the relays. Eventually, a small printer was attached to the machines.

(U) Keen's engineering task was made more difficult by the need to test for another type of logical impossibility. To make the test, he had to pass the output of the wheels through the diagonal board. The diagonal board was a twenty-six by twenty-six matrix of resistors that instantaneously sensed inconsistencies such as two different input letters being enciphered into the same output letter.

(U) To test all possible wheel combinations against just one crib for a three-wheel Enigma called for at least sixty machines. The Germans ran dozens of systems, and only hundreds of Bombes could have provided unaided coverage of them all. Turing's method of reducing the number of wheel combinations that had to be tested was soon overwhelmed by improvements in the German systems and by the proliferation of encryption networks.

(U) Unfortunately, BTMC faced too many shortages of men and materials to keep up the early pace of production. Keen was able to send less than a machine a month to Turing during 1940 and 1941. In early 1942, the record was not much better. Bletchley had only sixteen bombes and production had slowed.[28] To produce two of the Bombes a month stretched Britain's productive capacity. Bletchley Park was unable to build up enough of an inventory of them to seriously challenge any Enigma system until the end of 1942 and in the first days of 1943 GC&CS still had fewer than fifty machines.

(U) But it was not until mid-1942 that Britain's leaders decided to commit massive resources to the Bombe program. Only when they seemed essential to victory in Africa and to the safety of the Middle Eastern oil supplies was "Doc" Keen given new factories and a large workforce. That allowed BTMC to produce some 200 three-wheel Bombes by the end of the war.[29]

(U) Although Britain did not have much of an Ultra Secret in the critical months of 1940-41, she wanted to keep what she had to herself. Britain's codebreakers feared revealing their methods, even to the Americans, whose military aid had become essential to their nation's survival.[30] They had a not unwarranted fear that sharing with America would lead to breaches of security and the demise of Ultra.[31]

(U) The World War II relationship between the British and American cryptanalysts began in confusion and mistrust. It took several years to reach workable accords, and the formal, long-lasting agreements came after, not during, the war.

(U) The trust that became the foundation of the Cold War cooperation between the two nations did not come easily. There were critical months in late 1942 and mid-1943 when it appeared that what had been achieved since 1940 would be lost. The combination of British reluctance, America's divided armed services, misunderstood agreements, and lost messages almost led to an end to the joint intelligence program.

(U) Ask and Then Not Receive

~~(S)~~ Britain's leaders had begun making overtures about sharing "scientific" information as early as February 1940. When the suggestions reached the American Army and Navy codebreak-

ers, they did not reject the possibility of some sort of exchange. But Safford and his superiors in Naval Communications soon cooled to the idea, leaving William Friedman as the only advocate among the cryptanalysts.[32]

(U) Friedman could not deal face-to-face with the British; frustrations grew and there was a break in the negotiations. There may have been vague promises of full cryptologic cooperation between Roosevelt and Churchill in mid-1940, but they did not lead to any significant exchanges among the codebreakers.[33]

(U) Then after Britain began to send the United States Navy information on the disposition of German forces, it appeared that an agreement about an exchange of secrets was imminent.[34]

(U) In September 1940 William Friedman drew up a detailed plan for cooperation between the two nations only to encounter a wary American navy that again blocked its implementation.

~~(S)~~ But the navy did not have its way. The War Department's representatives made agreements for "full" exchange of information in December and exerted enough political pressure to sweep away the navy's objections.[35] OP-20-G was given orders to cooperate. It was told to select two men to join an army and FBI team that was to sail to England.

~~(S)~~ The navy was unhappy about being forced to exchange its secrets in spring 1941. Then when the Americans concluded that what Britain was willing to show the Americans was much less than expected, some in the American cryptanalytic community became furious over the balance between what America gave to GC&CS and what it got in return.[36]

(U) Gave All and Got...

(U) The delegation of American cryptanalysts from OP-20-G, the army's SIS, and the FBI had sailed for England in late January. They handed over two extremely valuable analogs of the Purple machine for the Japanese diplomatic ciphers, two copies of another Japanese enciphering machine, and all the other keys to the top secret Magic system. In addition, all that the United States had on major Japanese attaché, navy, and consular codes was surrendered. As with the Purple machines, giving those paper copies of the codes to Britain meant fewer were available to America's own codebreakers.[37] The American generosity did not end there, however. Britain was promised a continuous flow of cryptologic information, including the American Coast Guard's methods of tapping the German clandestine systems."[38]

(U) In return, GC&CS opened its doors and made the American visitors feel quite welcome. But it gave them very little of real value, at least about "E."

~~(TS//SI)~~ At first the Americans thought the British were completely open. Although the Americans were told to pose as Canadians, they felt that few restrictions had been imposed on them. They accepted the order against taking any notes on what they were shown and took having to sign a binding security oath as reasonable.

~~(S)~~ They felt they had been told all about the British attack against Italian, South American, and Russian systems.[39] GC&CS also shared its work on Japanese naval systems. And the Americans were shown the Bombe. The navy's men were given a paper version of an Enigma, were handed a copy of a few days' worth of old keys, and given a part of a "short" catalog.

(U) The army's representatives were given similar information, and they and the navy men were informed of the earlier successes against the

German air force's "E" and the system Germany had used during the Norwegian campaign.[40]

(U) What they did not get was what many had thought the trip across the Atlantic was really for, the cryptanalytic keys to the naval Enigma. The Americans did not obtain an Enigma machine or enough cryptanalytic information to allow the United States to break into the submarine "E" on its own.[41]

(U) What Happened After

(U) Although the American visitors to Bletchley Park may have left too soon to be told of the successes of mid-1941, the British could have been much more open than they were during the remainder of the year.

~~(TS)~~ Despite GC&CS's proclamation that full cooperation was in force, the American navy men had not been given an adequate explanation of the logic of the Bombe during their visit, were probably not indoctrinated into Banburismus, and were told little about the art of obtaining cribs for the naval Enigma attack.[42] The FBI and army representatives were also not told all.

~~(TS)~~ A U. S. Navy historical report on the "E" problem stated:[43] "Prior to the outbreak of the war with Germany, the nature of the German machine employed by the Atlantic U-boats was known in that the British had supplied to this Division diagrams of the wiring and the wheels of the device, together with a description of the way in which it moved. Beyond this and some few examples of plain text, nothing was known as to the usage of neither the device nor the method in which the keys could be recovered. It was then known that the British had conducted a successful attack, but the details of it were unavailable to the American Navy, due to the reluctance of the British to discuss the same."

~~(TS//SI)~~ The desire of the British to safeguard their secret powers was reflected by their failure to communicate the news or details of their achievements to the Americans after March 1941. Little cryptanalytic information crossed the Atlantic although some vigorous protest came from OP-20-G beginning in July 1941.[44] Even a visit to America in late summer by a very important British cryptanalyst did not lead to the Americans being told of the ways to attack "E."[45]

(U) Trust Builds Very Slowly

(U) For a year after the American delegation left England, there were few direct contacts between the two nations' cryptanalysts. There were some negotiating sessions about the range and degree of cooperation, but during the remainder of 1941 it seemed to many Americans that Britain became less, not more, willing to yield its growing pool of Enigma secrets.[46]

~~(TS)~~ The situation became quite tense by November. OP-20-G's men convinced the Director of Naval Communications to send a very strong protest to England. He told GC&CS he thought that the earlier agreement was not being fulfilled and demanded an immediate flow of cryptanalytic information. The British responded with true diplomacy explaining that all that had been promised had been sent to the United States and that it would be impossible for them to send everything that the American navy "might" want. It was better, they said, for the Americans to request specific information. Then if the British judged it was really of import to the United States, it would be sent. A quite similar message was forwarded to the American army. Although England began to send information on German diplomatic systems to Friedman's group, England continued to keep its "E" methods a secret.[47]

(U) Agreements and Agreements and Agreements, But....

~~(TS//SI)~~ OP-20-G was, of course, very unhappy about being required to ask for specifics; they did not know enough to compile a list. But the

tension was relieved by some end-of-year exchanges. When Laurance Safford finally received some replies to his earlier inquiries, when Britain hinted they would soon send a copy of their "machine" and a technician to America, and when GC&CS apologized for losing some American letters within its bureaucracy, "G" sensed it was going to be made a full cryptologic partner.[48]

(U) Under some prodding from the United States, additional agreements were made in early and mid-1942, ones that began to move the two nations toward a level of unprecedented cooperation. Then the sweeping October 1942 accords eased some tensions raised by an American navy threat to go its own way on Enigma. After that, the BRUSA pact of May 1943 was a major step toward openness with the army.[49]

(U) But it was not until the UKUSA agreement of 1946 that the two nations forged that unique relationship of trust that was maintained throughout the Cold War.[50]

(U) There were more than a few frictions on the road to BRUSA and UKUSA; during 1942 and 1943 the British were slow to reveal all about Ultra, especially during 1942. The American cryptanalysts had interpreted the agreements of 1941 to mean that Britain was to share all and that America was to become a full partner in Ultra. Although negotiating separately, both "G" and the SIS concluded the same thing. They expected that Britain would give them all they needed, if they wished to read "E" systems. A copy of the British Bombe designed for the older three-wheel machines was expected by "G" before the summer of 1942, and some Americans thought that all British information on new Bombes for the naval four-wheel Enigma would be immediately sent across the Atlantic. The British did not seem to agree.

(U) Going Separate Ways?

~~(TS//SI)~~ When "G's" frantic February 1942 plea for help against Enigma in the Atlantic did not get a response, tempers flared again. OP-20-G's new commander, Captain Redman, under intense pressure from Admiral King to do something about the Atlantic submarine crisis, concluded that GC&CS had been giving America the "runaround." It did not take him long to secure permission to begin another and very determined series of negotiations with the British. With Joseph Wenger at his side, Redman began to make it very clear that unless cooperation began immediately, the American navy would go its own way despite any of the danger that two uncoordinated attacks on Enigma might pose.

~~(TS)~~ When the Americans came to realize that the U-boat commanders had made a radical change in their "E" systems and that the British claims of imminent reentry were far from true, they began to take action. [51]

~~(TS)~~ Britain sensed there was a crisis and decided to send one of its most important codebreakers to America. He was told to calm the Americans without, however, giving them GC&CS's great secrets. When Colonel John Tiltman arrived in April 1942, he found it impossible to agree with official British policy. The American navy's codemen were so adamant and their threats to go their own way were so credible that Tiltman advised England that it must yield.[52]

~~(TS)~~ The final breakthrough seemed to come in May 1942. Promises came from England that a Bombe and a technician would be in America before autumn and that men from "G" would be invited to Bletchley Park.[53] There was some hope that the American army's cryptanalysts might be allowed into the "E" circle. GC&CS signaled that it would accept some help from Leo Rosen, SIS's electronics expert.[54]

~~(TS)~~ But the May promises did not end American suspicions, nor did they lead "G" to trust the solution of "E" to the British. Adding to the tensions, there was disagreement over the details of when and how "G's" experts were to be allowed back into Bletchley Park. Then, when a copy of the latest English Bombe was not shipped to America on schedule, when it took six months of requests to obtain promised blueprints, when Britain kept insisting that the United States work only on Japanese problems, and when it was clear that England did not want to give anything to the SIS, some American codebreakers again became very skeptical of British intentions.

~~(TS)~~ The suspicions led to action. Despite the recent accords, in August 1942 OP-20-G felt it had to protest about the failure of the British to keep their promises. Also, the relations between SIS and GC&CS became very tense. The army-British relationship became so strained that protests reached the White House.[55]

(U) America without an Ultra

(U) At its entry into the war, OP-20-G had only the most rudimentary knowledge of the Enigma and was not at all sure about the contours of the new U-boat system.[56] Some disgruntled American officers blamed Britain's unwillingness to share, but the reasons why American cryptanalysts were helpless lay in America, not Europe.[57]

(U) Since the turn of the century, America's strategic planners had seen Japan as the enemy. Some in the American military did worry about Germany, but it seemed beyond imagination that France and Britain would be unable to contain her on the continent. Few thought they would fail to block Germany's navy and air force from making the Atlantic unsafe for America. The concentration on Japan led to another dangerous assumption: No matter what the enemy did, the United States would have the time to prepare itself for war.

(U) Those assumptions were accompanied by ones about the nation's economy. Fundamental was that American industry would automatically provide any great technological advances needed by the military. It is no wonder that the calls by men such as Hooper and Bowen for ongoing research and Bush's drive to establish government-sponsored science remained largely unanswered.[58]

(U) Despite a lack of resources, by spring 1941 American naval ships were involved in dangerous scrapes with German U-boats in the Atlantic. By autumn the Americans were ordered to escort England-bound convoys.

(U) OP-20-G was as unprepared as the rest of the navy. To fulfill its obligations in the Atlantic, it expanded its interception net. To please England, it put most of its men on tactical analysis rather than codebreaking. At the same time, the navy's cryptanalytic ally, the Coast Guard, launched an attack on German clandestine messages. But the spy messages and the bits and pieces from some cracks in the German diplomatic systems yielded little about the German navy. OP-20-G had no effective Atlantic cryptologic power, and the navy had to rely upon British supplied intelligence.[59]

(U) When the U-boat command changed its Enigma and Hitler unleashed his American war, OP-20-G's cryptanalytic weakness became intolerable. When it was realized that Britain was closed out of the U-boats' new M4 Enigma Shark system and as Britain seemed more interested in the German army and air force systems, OP-20-G decided to find its own way to penetrate Enigma.

(U) An American Ultra, Perhaps

~~(TS//SI)~~ In spring 1942 the American navy was ordered to start forging its own "E" capability. Despite the crisis in the Pacific and the old hopes of building general-purpose computers, Howard's men and those in "M" were ordered to

focus on the Atlantic Shark problem and to produce an immediate solution.[60]

(U) When the decision was made to create its own "E" solution, OP-20-G was very short-handed and had to turn much of the work over to Engstrom's group of college men in the "M" section.[61] They began with few tools and the burden of Britain's fears of an independent American Ultra capability.

(U) Faster Than a Speeding Relay

(U) Bletchley Park's very overworked men had let almost a year slip by without focusing significant resources on a Bombe for M4, the four-wheel U-boat Enigma.[62] The Germans' introduction of additional encryption wheels an operator could choose from also presented a great challenge. Changes in the related German codes, radio networks, and procedures compounded the problems.

(U) GC&CS called on the famous Wynn-Williams and asked him to explore the use of electronics for a super-bombe. Williams spent many frustrating months trying to create an electronic Bombe. His efforts stretched into spring 1942 with little more to show than a breadboard model of a primitive "E" wheel. While he was asked to make a fresh start on his ideas, GC&CS turned back to "Doc" Keen and BTMC. Immediately the pragmatic Keen rejected an electronic solution and began to give some thought to alternatives.[63] He created the outlines of a new four-wheel Bombe but advised GC&CS that it might take more than a year to design and build the first model.[64] His prediction proved correct. Britain would not have the first of its very few temperamental electromechanical four-wheel Bombes until early summer 1943.[65]

(U) Great British Expectations

(U) Meanwhile, Wynn-Williams continued to plod along with his ideas; by midyear he began to construct a prototype of his Bombe. To his disappointment, it had to rely as much on mechanics as on electronics.

~~(TS//SI)~~ Williams had decided to build a complex attachment for the regular three-wheel British Bombes. His Cobra was to be a large box that was to contain his new high-speed electronic wheel and newly designed control and "hit" location devices. At first he bet that he could coax electronics to do the entire job. It took a long time to admit even partial defeat, but he had to back away from his original plan. He turned his Cobra into a combination of very high-speed commutators (3,000 rpm) and electronic memory and control circuits.

~~(TS//SI)~~ The compromise did not lead to immediate success, however. Williams had asked a great deal of electronics and mechanics. The Cobra was planned to be exceptionally fast. In addition to the tube circuits and the new wheels, run time was to be shortened by recording "hits" without stopping the Bombe. All that was too much for Williams' small team. His first machine had to suffer the indignity of a thorough reworking at the end of 1943 before it had done any operational work. Although a dozen of his new Bombes were eventually employed in England, they remained temperamental.[66]

(U) Great American Expectations

(U) While Williams and Keen were rushing to find their technological answers to the M4, GC&CS learned of America's Ultra intentions. Frightened by what it discovered, in spring 1942 it rushed a group of its leaders to the States hoping to reach an understanding that would protect its Ultra monopoly.

(U) March 1942 saw Britain strike the first of a series of new bargains. It assured OP-20-G that Shark was about to be beaten, and it agreed to share more Enigma information with the navy. In exchange, it asked "G" to concentrate on the

Japanese problems and let Britain manage European intelligence. The Americans desired cordial relations with the British, but they would not abandon Enigma. "G" agreed to cooperate but stood by its commitment to an American program.

(U) Despite two years of "understandings" with the British, OP-20-G launched into its own Enigma and Bombe programs without a true understanding of the Atlantic Enigma or the British Bombe. The historic OP-20-G directive of April 1942 gave a very incomplete view of Enigma, Shark, and the British Bombe. America's experts were able to outline only the workings of the older three-wheel plugboard version of Enigma, and they seemed uncertain about a key component, the reflector. Furthermore, OP-20-G's memorandum contained only the most general ideas about the British Bombe's logic.[67]

(U) While waiting for the promised information from England, "G's" men were told to define a true American Bombe. Given all they did not know about Turing's and Welchman's methods and machines, the first plans for the American Bombe do not seem too bizarre.[68]

~~(TS//SI)~~ OP-20-G made Howard Engstrom's young men responsible for the Bombe project. The closest "G" had to an Enigma expert, Lieutenant Commander R. B. Ely, was charged with devising the logic of the machine. After reviewing all the methods he knew to attack "E," he suggested that "G" might have to turn to a crib-based approach.

~~(TS//SI)~~ Ely, armed with only a few hints about how the British machine worked (gained through some test problems the British had previously sent over), independently arrived at a primitive version of the architecture Turing had designed three years before. As soon as he was able to sketch the logic of his machine, he sought an engineer. Not unexpectedly, one of the young men from MIT was selected.

~~(TS//SI)~~ John Howard was asked to solve the hardware and manufacturing problems. While Howard discussed possibilities with men such as Joe Desch of NCR,[69] Ely asked for help from others in Engstrom's section. He wanted assistance to check his ideas against cryptanalytic needs. And he wanted help finding, if it was possible, an architecture for a computer more universal than Turing's. Soon Ely's original ideas were reshaped.

~~(TS//SI)~~ The conception of what the American navy's Bombe would be was logically primitive but technically grandiose. In spring 1942 "G's" men knew so little about the Enigma systems they did not include the important instantaneous stecker setting tester in their design, and they thought their machine could use permanently fixed "wheels." As important, they thought they would have to have either a separate Bombe for each of the wheel combinations and permutations or one truly giant machine.

~~(TS//SI)~~ Apparently, as late as early summer 1942, Britain had not informed them of the "diagonal board," the many methods its codebreakers had devised to reduce the number of wheel combinations to be tested, nor how many different wheels the Germans made available with the M4. "G" did not know that the British had found it wise to leave tests for Enigma ring-settings and wheel starting-points off their Bombes.[70]

~~(TS//SI)~~ "G's" technical visions were far from backwards, however. As soon as the idea of an American Bombe had emerged, electronics became the focus of attention. A breadboard model of a "wheel" was begun. Completing it would not be easy because the Enigma wheel was difficult to imitate, and constructing a universal one was a daunting task. Cloning one wheel with known wiring meant having twenty-six tubes connected to twenty-six others and having a rack of supplementary circuitry. A universal "wheel" needed 26 x 26 tubes and all the circuitry needed to switch them as needed to imitate any of the possible wiring connections.

~~(TS//SI)~~ But Howard and the other navy engineers were so confident about electronics that as early as April 1942 Wenger was informing the British that American electronics might save their Bombe program. The faith in an electronic solution continued well into the summer, and some thought the American Bombe might turn out to be a single high-speed and complex tube machine that would do as much as or more than all of the British mechanical monsters.[71]

(~~TS//SI~~) Such a machine could save much time because it would also automatically reset the wheel(s) for each run and would never have to stop to record "hits." It was to have a high-speed system to photograph the diagonal board and a set of counters that would record the wheel positions at each hit.

(~~TS//SI~~) Those time-savers were secondary, however. What was important was the speed of electronics. In early spring it was thought that the American Bombe could do its job if it performed 10,000 tests a second. Faith in the machine's speed was necessary because it was going to be asked to do much more than Turing's Bombe. It would test for the some 300 possible wheel orders, the 440,000 [*sic*] stecker possibilities, and the ring settings.[72]

(~~TS//SI~~) Soon it was realized that even greater faith in electronics was required. When the run time for all that was recalculated, the need for much faster electronics was realized. Given the way the Americans were designing their Bombe at the time, one large one, a feasible machine called for circuits that could make millions of tests per second. That kind of speed was far beyond the electronics of the 1940s, but there was no indication that frightened the Americans. They had such engineering optimism and knew they could command so many resources that, if one electronic machine would not do the job, perhaps 300 or so of their special electronic "cribbers" could be built.[73]

(U) While Engstrom's men were exploring their options and while they waited for the expected flow of information about the Bombe and allied methods from England, "G" continued on with its fight to achieve Wenger's old dream of using pure techniques. OP-20-G's new college men intensified their search for advanced pure statistical and mathematical methods and machines. Hypo, Tessie and the Comparator were still seen as general- rather than special-purpose alternatives.

(U) But as summer arrived, the crew at "G" started to become angry and worried. Little helpful information had come from England, and the two men OP-20-G planned to send to Bletchley Park were not scheduled to leave until July.[74]

(~~S//SI~~) GC&CS was being more open with the Americans and informed them of the Fish systems. But Britain's codemen still seemed to hold back on the Bombes and what was necessary to their success, the methods of finding surefire cribs. Although offering GC&CS full information on all the advanced high-speed cryptanalytic machines it was developing,[75] OP-20-G was made to wait for a reply to its specific requests and for a clear statement of British policy on cryptanalytic cooperation.[76] Especially frustrating were the delays in providing Bombe details. Requesting blueprints of Britain's "latest" machines in May, the Americans hoped their examination would prevent them from committing to an American Bombe that was inefficient or simply unworkable. The prints did not arrive as promised.

(~~TS//SI~~) The Americans were under too much pressure to accept the continued stream of British "excuses." By the time Ely and Eachus were ready to depart for GC&CS, Joseph Wenger and his superiors became convinced that Britain would never finish the four-wheel Bombe they had promised to have working by mid-1942. Worse, they thought that the British had not lived up to the agreements that had been made since America entered the war. Less than guarded

words were used in some of the exchanges between "G" and England.[77]

~~(TS//SI)~~ The British reacted to the American protests by sending more information, hoping that "G" would reverse its decision to build its own anti-Enigma capability. OP-20-G gradually learned more about Britain's cryptanalytic methods, including those used to avoid testing all "E" wheel combinations. And when the two men from "G," Ely and Eachus, reached Bletchley Park, they began shipping home the detailed information the navy had sought for the last two years.

~~(S//SI)~~ But the Americans remained very worried. They feared they would be unable to build their more universal machine or their own version of the English Bombe. Worse, OP-20-G's leaders deeply feared that even if they built such a Bombe, they would always remain dependent upon Britain for the necessary copies of captured "E" wheels, codebooks, and cribs.[78]

(U) Trying to Step Forward, Not Back

(U) A few at OP-20-G were convinced that America could beat England's famed Wynn-Williams to a super-high-speed electronic machine, but others in the OP-20-G group were less sure of an independent American success.

(U) Although Ely and Eachus were sending back important information, the navy continued to have to formally request much on the English Bombe and the emerging new solutions to the Enigma systems. More fundamental, by the end of the summer the Americans became concerned that Britain would never devote enough resources to the Atlantic U-boat problem.[79] There was some foundation for the American anxiety.

(U) Britain's Own Version of Bush's Electronic Dreams

~~(TS//SI)~~ In late spring 1942, as part of the reallocation of GC&CS resources, Wynn-Williams was asked to turn his Bombe work over to someone else and to take on another job: devise a high-speed engine to crack the binary additive system of the Fish machines. He agreed, and while continuing on with his electronic Bombe work he designed the first of the Robinson rapid analytic machines.[80] Very soon, the designs were turned into hardware, electronic hardware.

~~(TS//SI)~~ The first Robinson (Heath) was delivered in early 1943, well before any of the newest models of Bush's Comparators reached OP-20-G's headquarters. They were based on a statistical attack, not the type of crude crib-bashing of the Bombes.[81] Robinson used high-speed punched tapes, photoelectric readers, and some one hundred gas-filled tubes to keep track of results.[82] The Robinsons shared something else with Bush's machines, the very serious problem of keeping the tapes in alignment. There were differences, however. The Robinson's target was a binary additive system. That called for a different use of the tapes. One tape was for a message; the other held the stream of "key."

~~(TS//SI)~~ Fortunately for the British and the history of computers, that binary stream presented an opportunity to avoid the difficulty of aligning the tapes. When it was realized that the second Robinson tape was a stream of algorithm-generated bits, it was suggested that a machine be constructed that substituted tube circuits for the additive tape. Reckoning that the number of tubes needed for the generation of binary combinations was reasonable, GC&CS gave the green light to construction of the Colossus.[83]

(U) The Colossus was something of a miracle of project management. It took less than a year to create what many consider the finest electronic pre-computer. Colossus kept 2,500 tubes and a high-speed photoelectric paper tape reader in synchronization. It could even be coaxed into performing some primitive program steps and "if" statements.

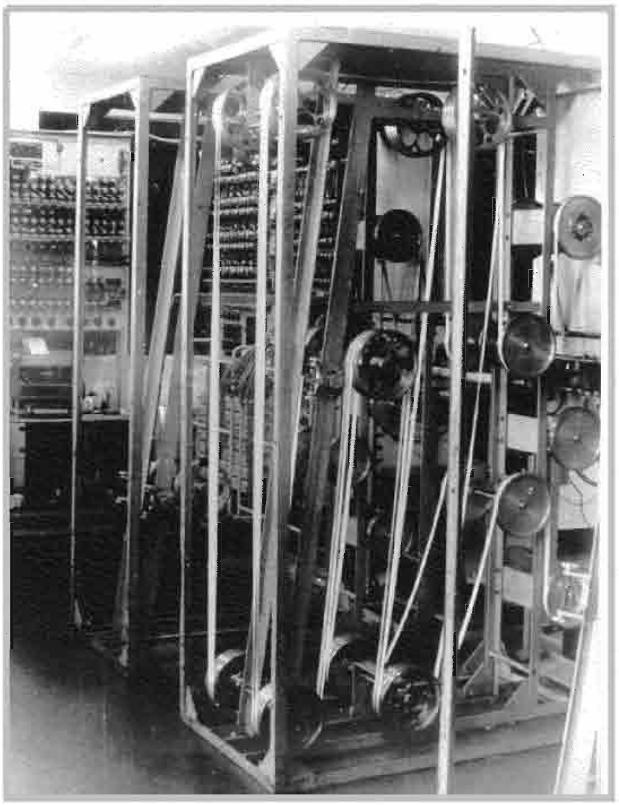
~~(TS//SI)~~ Colossus was very smart. It followed some of Turing's maxims about how to save search time. It had an electronic circuit that polled its counters to see if the results of the run were building to a significant outcome. This "sigmage" circuit saved hundreds of hours of machine and analyst effort. It also prevented Colossus from printing the result of every pass of the tapes, something the wasteful Comparators and the first Robinsons could not do.[84]

(U) The first of more than ten versions of Colossus was put into operation in January 1944.[85]

(U) The Americans Almost Beat England to Electronics

(U) The U-boat rampage in the Atlantic led to extreme criticisms of the American navy while the army was becoming worried that its men would go into battle in Africa and Europe without an "E" capability. Politically dangerous, Britain was giving them far less than the already meager ration of Enigma information it was providing the navy.

(U) Responding to all the various pressures, OP-20-G put even more resources into its frantic effort to conquer the U-boat "E," and the army began to think of the machines it might need for what it called the "Yellow Problem."[86] The army's SIS had difficulties obtaining information and resources and did not launch a machine program until the fall, but at the beginning of summer 1942, OP-20-G hinted it had a solution to the M4. Within another two months it announced that its men had beaten Britain and the great Wynn-Williams to the creation of the heart of a fully electronic Bombe.[87] The circuit wasn't the universal machine "G" wanted, but no time was lost in trying to exploit the development. NCR was taken over by the navy to be a research center and possibly a production site. John Howard's old group became an integral part of Howard Engstrom's



(U) Colossus

"M" as it was reorganized to oversee the electronic Bombe work at NCR.

(U) Wenger, Engstrom, and their like had to show some results.[88] The Bombe became important to "M's" survival as well as to the Battle of the Atlantic.

(U) No Time for Electronic

(U) In late summer 1942 the engineers of the "M" group decided their work was far enough along to submit it to an experienced production engineer for examination. Of course, they turned to Joe Desch. He spent almost two months examining their bench model and their designs for an electronic Bombe.[89] He came to a devastating conclusion: An electronic Bombe was an impossibility![90] A universal machine would need thousands more tubes and even higher speeds. The

thousands of tubes would be difficult to acquire, would create too much heat, and would demand more electrical power than could be supplied.[91]

(U) A Crisis of Organization and Technology

(U) Desch commanded so much respect that the responsibility for a new design was shifted to him. Necessarily, he was informed of one of America and Britain's great secrets, Ultra. After additional study of what was known about the Turing Bombe, he promised that he would be able to produce an electromechanical machine that could tackle the Shark M4. He declared he could create an original American Bombe but a non-electronic one.

(U) Immediately, a new effort, the second American Bombe project, was begun. As a result, Wenger's dream of a Rapid Machine program was saved. For most of the remaining war years, the electromechanical Bombes devoured the energies of "G's" engineers. To fulfill the commitment to Desch's necessary backward technological leap, all the truly advanced projects and ideas were made stepchildren.

(U) The second American Bombe project almost faltered, but it eventually became a triumph for OP-20-G and the American intelligence community. The success of the Bombes and the Allied work on machines for the Pacific war finally established the credibility Wenger needed to try to make research a permanent part of OP-20-G's peacetime operations.

(U) Searching for a Place in Ultra

(U) The second American Bombe project was part of an attempt to readjust the relationship between Britain and America's codebreakers. Desch may not have known it, but his Bombe was essential to OP-20-G gaining a greater role in the Ultra Secret and to becoming a producer of operational information. Without an American Bombe, the United States would have remained a consumer of British-controlled Ultra information, and OP-20-G would have continued under the old understanding: Both nations could pursue independent (unaided) research, but Britain would control all operational activities. Although Britain had begun to ask for American help on the Atlantic problems, with the failure of the second Bombe project it would have been very reluctant to make OP-20-G an equal partner.[92]

~~(TS//SI)~~ The friction with Britain over Ultra intensified soon after the approval of Desch's sketch of a modified British machine. The navy's men became intolerant of what they considered broken promises by the British about their four-wheel Bombe.[93] OP-20-G more than hinted that it would build as many as 350 of the Desch machines before spring 1943 when the U-boats were expected to launch a mass attack. America was notifying Britain that no matter what it took, the United States would win the U-boat war.[94] The Americans declared they intended to build enough machines to test all Shark wheel orders simultaneously.[95]

(U) The Power of Innocence

(U) Given all that the Americans did not know about the Bombes and all that was required to make them useful, miracles were required. Joseph Desch's first description of the proposed "G" Bombe and its powers reveals how much the American Bombe program was based upon the type of optimism that comes from innocence, if not ignorance.[96]

~~(TS//SI)~~ Some of the detailed plans of the three-wheel British Bombes had begun to reach the United States in late summer 1942, but Desch's design was his own. He had begun his plans before the British had revealed more than the bare essentials of their machine and the crib-based "menus" that made it work.[97] And he arrived at his first design before he had been able to test his assumptions about the way the essential components of his Bombe would behave.

~~(S//SI)~~ Desch's plans were technically optimistic. He thought it possible to create a drive system that could keep twenty-four double-ended Enigma analogs (ninety-six commutators) in perfect synchronization. A large electric motor would drive a high-speed shaft that would directly turn the shafts for the fast wheels. Gears, machined for complex ratios, would connect the high-strength rods for the slower wheels to the main shaft. The gears and shafts had to be of the highest quality material and workmanship to stand the stress placed on them when the machine suddenly stopped and restarted.

~~(S)~~ That was one unique feature of the proposed American Bombe that would put Desch's faith in mechanics to a severe test. He proposed an automatic stop, rewind, and restart system. That would save critical running time and, as important, avoid having the machine's operators having to hand-crank the device when a "stop" was sensed.

~~(S//SI)~~ Once the testing circuits identified a possible "hit," his machine would cut the power to the main shaft, apply brakes and bring the commutators to a halt all within a fraction of a second. Then a second motor would immediately drive the commutators backwards until another circuit signaled that the possible "hit" position had been reached. The machine would then perform another series of circuit tests, including a diagonal board search. If those tests indicated there were no contradictions, the commutator positions and the diagonal board indicators (the "story") were printed. Fortunately, "G" had not asked Desch to build a machine that tested for the ring settings as well as for the wheel orders and steckers.

~~(S//SI)~~ Immediately after the "stories" were printed, the motor would be restarted, the clutch on the central high-speed shaft would be engaged, the gears would mesh, and the commutators would turn in synchronization until another set of wheel positions indicated an Enigma setting that might have produced the crib.

~~(S)~~ Desch did not seem to worry about the stresses that the quick stop, rewind, and restart systems would put on the shafts and gears, but Alan Turing certainly did. When he visited NCR in December, he warned "G" that it would be unlikely that any machine could be kept in working order when it was asked to defy the laws of inertia.

~~(S)~~ Desch did not back away from the automatic rewind system nor did he change his mind, during fall 1942, about having three complete Bombes in a single rack. Such a configuration would save precious space (336 Bombes with 32,000 commutators in 112 racks). He was convinced that the frames would tolerate the heavy vibrations from the three machines, which would be independently starting and stopping.

~~(S)~~ Desch also kept his faith in the ability of American technology to make the "G" Bombe more flexible and many orders faster than those in operation in England. His Bombes were to be very rapid, several times the speed of the British three-wheel bombes and twice the speed of England's proposed four-wheel machines.[98] The fast wheel was to revolve at 3,400 rpm. The others would run at proportionately lower speeds, turning only when their faster mate had completed a full turn. The second wheel, for example, would take one step after the fast wheel had made a complete twenty-six-point revolution, plus additional revolutions to compensate for the time the other wheels needed to turn over.

~~(S)~~ When desired, the Bombe could be turned into a three-wheel enigma analog, and, Desch hoped, it could be run at various speeds.[99]

~~(S)~~ Joseph Desch premised his design on the power of America's mass production methods to make all parts of the Bombes interchangeable. NCR's machinists had assured Desch that he could achieve his critical goal of having every commutator fit on any of the thousands of spindles on the Bombes. That was a critical feature. If

commutators had to be tailored to each machine, his system would be impractical. That would demand too many highly skilled workers for commutator construction and too many commutators, perhaps as many as 60,000.

(S) Desch promised to make electronics as well as mechanics go beyond normal expectations. He said he could overcome the problems that had led most engineers to avoid the use of tubes. A multitube Rossi detector circuit would monitor the machines for possible "hits," another circuit would remember where the "hit" occurred, one would control printing, and, he hinted, another very complex one would handle the "diagonal" test. He was not sure in September 1942 how many tubes each Bombe would have, but his memoranda hinted that his electromechanical machine would need perhaps as many as 1,500 electronic components.[100] The high-speed diagonal board alone might need more than 1,000 tubes.[101]

(S) His September design asked more than could be expected of gas-filled or vacuum tubes in the early 1940s. His faith translated into the blind hope that the navy's engineers could keep more than 300,000 tubes running at one time. "G" wanted to run each wheel order simultaneously. That meant 336 Bombes with perhaps 1,000 tubes each running without a flaw for perhaps as long as an hour.

(S) The electronics posed a serious challenge to the navy engineers. They would have to find ways to handle the heat generated by the electronic components and create methods of identifying troublesome tubes before they failed. Desch went ahead, believing that the "G" would find a way to overcome all the problems that had kept men like Vannevar Bush from trying to build large-scale electronic machines.

(S) Joe Desch had to believe in the future of electronics; his machine could not work at what he thought was a minimum speed without electronic switches. He could not build a "memory" for the machine out of high-speed commutators, relays were too slow for the "diagonal" test, and simple capacitors seemed unable to do the job.

(U) The Power of Ignorance

(S) Desch thought the navy needed so many Bombes that ran so fast because the Americans had not yet learned of the methods GC&CS used to select the Enigma wheel orders that had to be tested on the Bombes. GC&CS had discovered many ways of telling which wheel orders the Germans would not use during a crypto period. They had also developed many cryptanalytic techniques, which eliminated particular wheels and wheel positions.

(S) As significant for the history of the American Bombe project, in autumn 1942 "G's" experts did not fully understand the methods Britain had developed to allow the Bombes to quickly beat "chance." As a result, they had concluded that the United States had no alternative but to invest millions of dollars in machines that were very inefficient.

(S//SI) The Bombes would be valuable only if used properly. When they were given enough information, they speedily reduced the number of Enigma wheel orders that had to be examined by the analysts. But if used improperly, they could not sort out the wheel orders and stecker settings that could have produced the cribs by accident from those settings that were "causal." With only relatively short crib-plain combinations to test, twenty or so letters, a Bombe with a weak menu might filter out only a small proportion of the incorrect settings. Desch, for example, feared that typical menus would force analysts to comb through a third of a million possibilities after a run of the 336 Bombes to locate the setting that was the true Enigma key.[102]

(U) Using analysts to search for Enigma settings was time-consuming and expensive. Tests

took from seconds to hours, and some of them demanded skilled if not just very devoted personnel. From the list of combinations that were not eliminated by the Bombes, analysts used other machines and hand methods to see which was the unique one that produced plain text from crib. Thousands of analysts would be needed if the Bombes did not eliminate all but a very few of the Enigma settings.

~~(S)~~ To be useful the Bombes had to eliminate more than just those combinations that could not possibly have produced the crib-plain combination; they had to filter those that were unlikely to have done so. The only valuable pay-off from the use of the Bombes was a very short list of very likely "keys." Unless the list was short, there would be no significant savings in time and manpower.

~~(TS)~~ The only way to that short list was through the location of long and accurate cribs and the creation of powerful "menus." Starting with relatively long cribs, a menu was built through searching for letter combinations and connections (closures) between plain and cipher that would allow the Bombe's circuits to differentiate "chance" relationships from those that were caused by the true Enigma setting.

~~(TS//SI)~~ By mid-1942 GC&CS's wizards had turned menuing into a mathematical art. They had discovered much since Turing's first insights. They had tables showing what types of menus were needed to produce the desired short lists; they found that wisely selected cribs reduced the need to run all thirty-two of the Enigmas in their Bombes; they could calculate how many time-consuming machine stop and circuit checks would be expected per menu; and they could predict how many possible wheel order and stecker settings would be printed per run.

~~(TS)~~ Strong menus were a necessity. Otherwise, the Bombes might stop their wheels and demand a return to the possible "hit" position so frequently that runs would take several hours.[103]

~~(S//SI)~~ The British had also learned how counterproductive it was to run the Bombes without having 100 percent accurate cribs (a goal that called for a vast infrastructure) that yielded robust menus. They reserved their Bombes for menus that would produce no more than a handful of "stories" per run. By mid-1942 they had learned how to select fifteen letter cribs that prevented the Bombes from stopping more than a dozen times and printing more than five possibly true "settings" during a run. When the Germans made the mistake of providing excellent cribs, the Bombe could identify "the" and only "the" setting.[104]

~~(S//SI)~~ But Desch and the Americans had not learned enough about cribs and menus by September to envision or wait for Bombes that would point to only a handful of possible solutions. In September Joseph Desch estimated that his ultra-high-speed Bombes would take, using typical menus, thirteen and one-half hours to test one wheel order on one Bombe. The reason: He calculated that a Bombe would have to stop 3,000 times per run, perform its circuit tests, and then decide whether or not to print its declaration that it had found a highly probable solution. On the average, Desch estimated, the Bombe would suggest that one of three stops had found a wheel order that should be tested by an analyst.[105]

~~(S)~~ If, as envisioned in early fall 1942, "G" was to run its 336 machines simultaneously and continuously, the Bombes would spew out some 300,000 "probable" settings twice a day. How "G" was to wade through all that was not divulged.

~~(S)~~ Even with the use of the best possible menus, Desch's Bombes seemed to demand great manpower investments for the production of timely intelligence. The navy's commitment to becoming a partner in Ultra is underscored by the

acceptance of the consequences of Desch's most optimistic menu scenario. After consulting with OP-20-G's Enigma expert, Lieutenant Ely, Desch held out some hope that "G" would eventually be able to provide menus that would cut each machine's running time to three hours and the number of its stop-rewind sequences to less than 700 per run, per machine. That meant that "G's" experts would need to test some 40,000 prints each day.[106]

~~(S)~~ The Americans were desperate. They accepted the Bombe program despite Desch's estimates. They were willing to invest millions in hardware and more in manpower for a system that was very inefficient. Despite Desch's estimates of how long the Bombes would take to produce so few results, his report on the design of the American Bombe was quickly approved.[107]

(U) The Cousins Will Have Their Way...to A Degree

(U) Although they questioned the ability of "G" and its engineers to build a significant number of Bombes and to devise the menus needed for them, the British had no choice but to take "G" seriously and to make the best of the situation. They quickly dispatched another cryptologic delegation to the United States.

~~(S//SI)~~ Accepting what seemed to be the inevitable, GC&CS agreed to help the Americans. But they continued to argue that European intelligence should be left to them. The British explained more of their methods of avoiding the need to run all the Bombe's wheel combinations and orders to test a message. They dropped hints that "G" could expect a steady flow of valuable cribs and solutions.

~~(S//SI)~~ The British seemed to be even more generous when they agreed to a new arrangement in the Pacific. But they gave up very little and gained much by allowing OP-20-G to run the cryptanalytic and intercept operations in the area.

~~(S//SI)~~ In exchange for Britain closing down some minor centers and allowing the Americans to direct the codebreakers in Australia, the American Navy promised to send, if practical, all raw and processed information about the Pacific to the British. Given how few resources Britain had in the region, it gained more than it relinquished.

~~(S//SI)~~ The Americans offered even more. They volunteered to provide GC&CS with copies of "G's" newest RAM devices and to train its technicians in their use.[108]

~~(S//SI)~~ In contrast, the Americans obtained much less than they hoped for in the Atlantic. It was agreed that the British would accede "to U.S. desires with regard to work on the German submarine and naval problem," but Britain, in effect, would be "the coordinating head in the Atlantic theater as the U.S. will be in the Pacific."

~~(S//SI)~~ The previous pledge to give "G" advice on analytical machinery was reaffirmed, and it was agreed "in principle" that Britain would collaborate with "G" and send needed cribs, menus, and intercepts as long as the security of Ultra was not endangered.[109]

~~(S//SI)~~ In response to Britain's bowing-out in the Pacific, to its providing more knowledge of Bombe techniques, and to its obvious determination to keep control of the European Ultra, the Americans tentatively agreed to build only one hundred Bombes.[110]

~~(S)~~ One hundred in this case meant a total of 100 four-wheel Enigma analogs, in contrast to the Desch plan to have 100 racks with three Bombes each.

~~(TS//SI)~~ They also agreed to keep their Bombe design very fluid so they could respond to emergencies. "G's" technicians were also made aware they might be asked to play a backup role for GC&CS. Like the rest of Britain's military,

GC&CS began to think it could depend upon America's industrial capabilities. In late 1942 there were indications it might be forced to. "Doc" Keen's factories were stretched beyond their limits. America would be needed to handle cryptanalytic machine emergencies.[111]

(U) "G" seemed ready to accept that role. It also did not reject Britain's suggestion that all Ultra-based naval actions be coordinated ones. There certainly was no hesitation when GC&CS asked the navy for a firm pledge to do everything needed to make Ultra America's most guarded secret.[112]

(U) The October 1942 negotiations did lead to Britain giving "M" a somewhat greater operational role, or at least preparing them for one. GC&CS's representatives set "M's" men to using hand methods on various German systems and gave them more instructions on how to prepare menus (setups) for the Bombes.[113] During the next few months more and more technical details about Ultra flowed to the United States, and more of Engstrom's bright young men in "M" traveled to England to work at GC&CS. But the British retained the power to decide what information would and would not leave Bletchley Park.[114]

(U) A Long Apprenticeship

~~(TS//SI)~~ A year after the October 1942 agreement, at the end of 1943, "G" remained an appendage to Britain's European Ultra. In November Howard Engstrom traveled to England to hear something quite like a lecture about "M" wasting valuable resources by running the Bombes on very weak American-devised menus. He had to agree to a return to using British cribs and menus. It was not until much later in 1944, after "M" had enough good intercepts, and after its cryptanalysts had honed their menuing skills, that "M" was granted effective independence concerning the Atlantic U-boat problem.[115]

(U) It took a long time for "G's" men to gain the necessary skills and to build an effective anti-Enigma organization. There was progress, but it came slowly. In early 1943 American cryptanalysts were applying GC&CS paper and tabulating machine techniques to crack some German messages intercepted by the British.

~~(TS//SI)~~ But most of the first half of 1943 was a long practice session for the Americans. Using GC&CS-supplied keys, they deciphered and analyzed the large American backlog of intercepted Atlantic traffic. Then GC&CS forwarded new messages and their keys.

~~(TS//SI)~~ To aid the deciphering process, the navy's men in Washington built a new electromechanical device, the M8. The M8 was not an analytical machine, but soon after its appearance in October 1942 it became an invaluable tool for "G's" analysts. More refined models began to appear in spring 1943. The M8s were reworked versions of the Americans' own automatic wheel-based encryption machine, the ECM. The navy yard's engineers added a plugboard, Enigma wheels and Letterwriter equipment to turn the ECM into an automatic and relatively high-speed "translation" machine. Once the wheels and plugboard were set, the "stories" from the Bombes could be rapidly tested, or entire messages could be deciphered at rates up to 600 letters per minute. A few months later the M9, another simple Enigma analog, appeared. The M9 was a very sparse combination of wheels and plugboard that was extremely useful once the Bombes were in operation. An M9 was later placed near every set of Bombes, allowing their operators to make immediate checks of printouts and to locate missing Enigma plugboard settings.[116]

~~(TS//SI)~~ But much of the American Ultra effort of 1942 and 1943 proceeded without the help of automation. Enormous human resources were put into a paper version of a bombe: a 1,000,000-page catalog that could be used to

drag a short crib through wheel settings to find possible Enigma keys.[117]

(U) In late 1942 Alan Turing began a series of visits to America telling "M" more about Ultra and the construction efforts on the latest British Bombe.[118] The two nations' intelligence services and the two Bombe projects became closer as 1942 ended. But Desch's Bombe was an American product.[119]

~~(S)~~ By the time he received adequate information about Wynn-William's work and that of "Doc" Keen on his four-wheel "Mammoth" Bombe, Desch had his design relatively fixed.[120] He was convinced that the automatic rewind feature was essential, and he did not wish to halt his work while the British proved that all "hit" circuit tests could be done without rewinding the wheels. He was convinced that his steel shafts would be more reliable than belt drives and that menu setting should be done with a set of switches rather than clusters of hand-inserted Jones plugs.

(U) Desch and his NCR men and the young engineers in John Howard's "M" group took the very heavy responsibility of creating a unique machine and a path-breaking production line to defeat the U-boats.[121]

(U) Desch Takes Charge

(U) As soon as his general design was approved in September 1942, Desch began to refine his ideas and looked forward to immediately building a prototype.[122] At the same time, the old engineering group from MIT was ordered to put the other OP-20-G machine projects on hold until the critical Bombes were ready. Financing was not a problem, and the second American Bombe project, which at one point would employ over 1,000 manufacturing workers, received the highest priorities for personnel and material. The Bombe project had its own building in Dayton with armed Marines and special secret rooms to manufacture and use the Bombes.

(U) Wenger Gets His Organization

(U) The Bombe was so important that the Bureau of Ships had to grant all the wishes of Wenger, Engstrom, and Desch. OP-20-G was able to convince the Bureau to create a new administrative organization for all the high-speed machine projects: the Naval Computing Machine Laboratory (NCML) at Dayton, Ohio. In formal terms the Bureau's NCML was the boss of the Dayton work, but by early 1943 it was really a support organization for OP-20-G's group of engineers and scientists.

(U) The "M" group was also gaining power. The country's best mathematicians, physicists, and engineers were brought into OP-20-GM. That allowed Engstrom to have a self-contained machine development group that easily challenged the Bureau's technical authority. Of importance to the nature of the postwar RAM program, the "M" engineers were integrated with the NCR workforce. That gave the machine designers the freedom to merge research and production and, combined with the virtual takeover of NCR, it allowed Wenger a constant interaction with and power over the manufacturing process.

(U) Of Tires and Transmissions and a Disappearing Laboratory

(U) Such freedom and the massive resources the navy was willing to pour into Desch's project were not enough to sustain the hopes of September and October 1942, however. At the opening of 1943 a prototype of his Bombe had not been assembled, and there were serious questions about the practicality of the components that had been constructed.[123] The rejection of the plan for an electronic machine and the reversion to the electromechanical technology of the British Bombes had not led to the easy solutions "G" had

expected. The Bombe and Rapid Machine projects were in trouble again.

~~(S//SI)~~ Joseph Desch's first designs had called for a Bombe that was a close analog of the Enigma, but it was to be a very, very fast one. There were to be more than twenty sets of four wheels each in a Bombe. Each of the four wheels was to be of the same size and was to be constructed out of typical materials of the era. The Bombe's commutators were to be made of either hard rubber or Bakelite, standard insulated housings of the 1940s.

(U) Inserted within the inner face of those wheels were rather large copper contact bars. Joe Desch knew he would have to make them of special lengths and shapes to prevent spurious electrical contacts from being registered as "hits."

~~(S//SI)~~ The fastest of the four wheels was to spin around more than sixty times a second. That rate of speed seemed essential. And also essential was the complex gearing that would be required to pace the movement of the slower commutators. The gearing requirements included the difficult-to-machine-and-maintain Geneva gears and a stepping control system that reminded one experienced engineer of the complexity of the recently invented automatic transmissions for automobiles.[124]

~~(S//SI)~~ Although a challenge, the group at NCR had few doubts about creating the Bombe. September's optimism about such mechanical and electrical parts did not last long, however. The first serious disappointment came quite soon. It was found that the commutators could not tolerate such high speeds. The fast wheels were blowing apart. The problem could not be overcome, Desch concluded, so he significantly altered the design of the Bombe.

~~(S//SI)~~ By December he envisioned a machine that would have two small "fast" wheels. The smaller wheels, he hoped, would rotate at least at 1,800 rpm without disintegrating. Soon he had to admit to other problems. He warned Engstrom that the commutators might not be interchangeable from Bombe to Bombe. Production difficulties might cause something worse. The commutators, Desch said, might have to be permanently attached on each spindle.[125]

~~(TS//SI)~~ The decision to create a Bombe with two fast wheels created near panic in Washington. Since any of the Enigma wheels might be assigned the "fast" position, each of the eight known Enigma commutators would have to be cloned by two, not one Bombe commutator. Howard Engstrom let Desch know in the strongest terms that he disapproved of the two-wheel design. It would create a logistics nightmare, wrote Engstrom. More than 40,000 or 50,000 of the expensive commutators would have to be immediately stockpiled and made available for use. If the Germans altered the wiring on their wheels or added new ones, no manufacturer could respond quickly enough to produce the new wheels.[126]

(U) Desch promised that he would do his best to make the wheels interchangeable from Bombe to Bombe, but he could not guarantee that he could produce a Bombe of any significant speed without the dual fast wheel feature.

~~(TS//SI)~~ Then a very great gamble was made. Washington declared that a solution be found. The American Bombe would have only one size wheel! Desch and his men had their orders, but no solutions. They began an intensive search. Their reward was disappointment. Prototype after prototype kept disintegrating when put at the high-speed position even when the revolutions per minute were reduced to less than half than originally planned.

~~(TS//SI)~~ The answer eluded everyone. It was not until some of the young officers stationed at NCR realized the similarities between the commutator's problems and those of automobile tires

that there was a glimpse of hope. How were tires able to hold together during auto races? The answer seemed to lie in a new product, rayon. The officers learned that webs constructed from it were being used to reinforce new types of rubber tires.

~~(TS//SI)~~ There were visits to local tire companies and some tests. The situation appeared hopeful, but no one was sure that the experiments could be translated into a mass production system for the commutators.[127]

~~(TS//SI)~~ Because they had no choice, Desch's team went ahead with the rest of the Bombe project while they waited for word about the commutators. As they did, they confronted another problem whose solution was also tied to the automobile industry.

~~(TS//SI)~~ The gearing system for the Bombe proved more complex and temperamental than expected. No one seemed able to correctly align the components. Finally, the more senior engineers asked some of the younger men in Dayton if they had any experiences with gearboxes. One, whose engineer father had worked for Tom Edison, had some hands-on experience with the new automatic transmissions. When he examined the Bombes, he saw much that related to his previous experience. He volunteered to try to solve the gear assembly problems.[128]

~~(TS//SI)~~ There was another important problem with the Bombes that almost halted development. Desch had rejected the idea for a fully electronic bombe, but had no alternative other than to rely upon electronics for many parts of his 1942 device.

~~(TS//SI)~~ Desch's September design suggested a need for perhaps as many as 1,500 tubes in relatively complex circuits. The fast diagonal board to test for stecker settings might call for over 1,000 tubes. Given the size of tubes of the early 1940s and the heat they generated, an alternative to off-the-shelf technology had to be found. Desch's past experience led him to believe that small multipurpose tubes might be created. He made some attempts to refine his previous designs, but his many other responsibilities pulled him away from the needed solution. He had to have help. Fortunately, the NCR project had such high priority and such vast resources that one of the nation's leading tube experts could be summoned to Ohio and allowed to order everything he needed to create an advanced laboratory. His work proved successful, and he was able to deliver the specifications to manufacturers for the special tube. It was a tiny four-in-one tube that became the basis for the ultra-fast diagonal board. It would be produced in carload lots, and it reduced the number of separate tubes in the Bombes to fewer than 500.[129]

(U) While the "G" group waited for the solutions to the commutator, gearing, and tube problems, they faced a very chilling possibility. For a time, some in "M" worried that their opportunity had been lost because GC&CS was able to reenter the Atlantic U-boat system at the beginning of 1943 without the use of any four-wheel Bombes. The reentry came through the capture of documents from a U-boat and the discovery of some very sloppy procedures on the Shark network. As a consequence, the British were able to read the four-wheel Enigma messages using their old Bombes and hand techniques.

(U) But the British and the Americans soon realized how temporary the new solution was. As the spring U-boat offensive opened, the Germans changed some of their codes and tightened up their procedures so that the Allies were again shut out of the submarine systems. They remained blind for a frightening ten days during what became the worst month in the history of the battle of the Atlantic.

(U) Saving the American Bombe

(U) At least three months before that ghastly March 1943 U-boat slaughter, OP-20-G realized that Desch's machine was in serious trouble. Pressure was put on the staff at NCR to work overtime. Joe Desch was told to drop his many other electronics projects for the NDRC, Aberdeen, and the army. And the navy went over the head of the new president of NCR and wrote directly to Colonel Deeds to make sure that NCR gave the Bombe project all it needed. Under prodding from the Chief of Naval Operations, Deeds quickly ordered Dayton to devote less time to its other and more profitable war work and give the Bombe all of its attention.[130]

~~(TS//SI)~~ The first design for the pilot model of the Bombe was submitted in January. Joe Desch and John Howard responded to British suggestions and incorporated them in a second design even as they rushed to construct the first prototype. But the men in Dayton were not keeping pace with the war.[131] As the great Atlantic battle began in March, all that had emerged from some seven months of work were two wheezy prototype machines.

~~(TS//SI)~~ Their commutator racks sat on sawhorses, and their other components were scattered around the workroom, connected by scores of wires that were soaked with the oil that flowed out of their drive shafts' housings. Their commutators continued their obstinacy, and the crew of engineers endured repetitions of lowering the fast wheels' "rpm," then having to dodge their fragments as they splintered. No one was sure that the two models, Adam and Eve, would prove themselves and serve as test beds for the vital production machines. Nonetheless, Washington decided it could wait no longer and in early April Desch committed to a final design for the production version of the American Bombe although he was not sure that it would work.[132]

(U) There was progress at Dayton during April and May, but no machines! The group at NCR could not even tempt the two Bombe prototypes to run for more than a few inadequate minutes. Fortunately, escort carriers, airborne radar, a central command center for subhunting (the Tenth Fleet), and changes in the once vulnerable Allied convoy codes began to bring the Atlantic under control. Enigma cracking played its part, but not through the promised American technological wonders, the Bombes.

(U) A Bombe Too Late

(U) Order was restored in the Atlantic before the first American Bombe was even put to its tests. The problems in the Atlantic and the coming European offensives called for another readjustment in the rules for cooperation in the intelligence field. The BRUSA agreement made the United States Army a partner in the Ultra Secret, but a very junior one. OP-20-G and the United States Army again agreed to focus on the Japanese problems and to allow GC&CS to determine what the Americans would do or would not do against the Enigma and Fish systems.

(U) As the mid-May 1943 negotiations came to a close, Joseph Wenger remained unsure of OP-20-G's future. Even if "G" was too late to be the savior of the Atlantic, there was still much to do to counter the U-boats. The German Army, Air Force, rocket development team, and police agencies showed signs of changing over to four-wheel Enigmas. And, in the systems continuing to use the three-wheel machines, anticipated alterations in procedures and in the use of their plugboards threatened another round of crises. If the American Bombes could be made to work, they still might play a significant role.

(U) In late May Wenger ordered Desch to allow the two temperamental prototypes to be used on messages sent from Washington. The results were to be forwarded to the British as

examples of American abilities.[133] Howard Engstrom, in charge of the new Enigma message work, felt defeated when Adam and Eve refused to run for more than a few hours without spurting oil or developing incurable cases of faulty electrical contacts.[134]

(U) A Program Based on Another Technological Bet

(U) Adam and Eve continued their tantrums as June approached,[135] and the production model was yet to be assembled. The tension mounted when it was learned that as Dayton again faltered, Britain completed its first four-wheel Bombe, put its first tape and electronic Robinson to use, and began the construction of the advanced electronic COLOSSUS.[136]

(U) Adam and Eve, the prototypes, were in too much trouble and were too vital to working out critical technical problems to be used by the cryptanalysts in Washington. Desch's crew and Howard's NCML engineers put in longer hours using Adam and Eve to unravel the problems with the parts for the production machines. The commutators were reworked and the drive-mechanisms altered.[137] By mid-June there were hopes that all the problems had been conquered.

(U) However, the production crew had still not released the first two copies of the final model, Cain and Abel. Desch pushed his people harder, and the NCR factory began to assemble components at an even faster pace. They could only hope the parts would function when put together in the Bombe.

(U) July 26: a Day of Defeat

(U) It took Joe Desch another month to send the first two production models to the test floor.[138] Then he was able to have thirteen more of the new Bombes assembled by the last week of July, but none would work![139] July 26, 1943, was a critical day in the history of OP-20-G and the NCML. At the very last minute, Desch made a discovery that revived hope. Running the Bombe's Bakelite code wheels at extreme speeds was again causing invisible distortions leading to false electrical contacts. Desch predicted that careful storage, handling, and refurbishing would solve the problem.[140] Apparently, Desch had replaced the small fast wheel on the first prototypes with ones the same size as the others to please Engstrom. Again, his judgment was trusted. The wheels were reworked and production was resumed based on his hope that the last-minute modifications would provide a permanent cure.

(U) A Victory, a Bit Too Late

(U) Despite all the false starts, delays and problems, Desch built one of the most complex machines in the world. The 1943 Dayton Bombe was a seven-foot-high, eight-foot-long, two-foot-wide and 5,000-pound marvel. It housed sixteen four-wheel sets of Enigma analogs and the Welchman diagonal board. Its sixty-four double-Enigma wheel commutators each contained 104 contact points, which had to be perfectly aligned when they touched the copper and silver sensing brushes. Such alignment and synchronization were difficult to achieve, especially for the fast wheel. The achievement was more remarkable because Desch was able to keep his promise of making the commutators interchangeable.

(U) There had been some compromises in order to convince the machine to work. It was much slower than hoped for. Fewer than 2,000 revolutions a minute had to be accepted because even the reinforced commutators could not stand up to higher speed. And running the Bombe's main shaft even at the lower "rpm" without creating the sparks and short circuits that ruined a test continued to be a problem.

(TS//SI) It was quite embarrassing to have had to install a conduit system under the machine to catch the oil that was sprayed on the main shaft to keep it from overheating. And the engineers

did not like the idea of having to pour a quart or so of oil into the machines every day.[141]

(~~TS//SI~~) There had been some other compromises. The NCR devices did not incorporate a means of producing irregular stepping of the slower wheels, and the summer 1943 Bombes were not the compact three complete units-per-frame devices Desch had sketched in the previous year. Trying to balance the engineering demands with cryptologic power had led to the Bombes being composed of sixteen, not twenty, units, and having only one Bombe per frame.

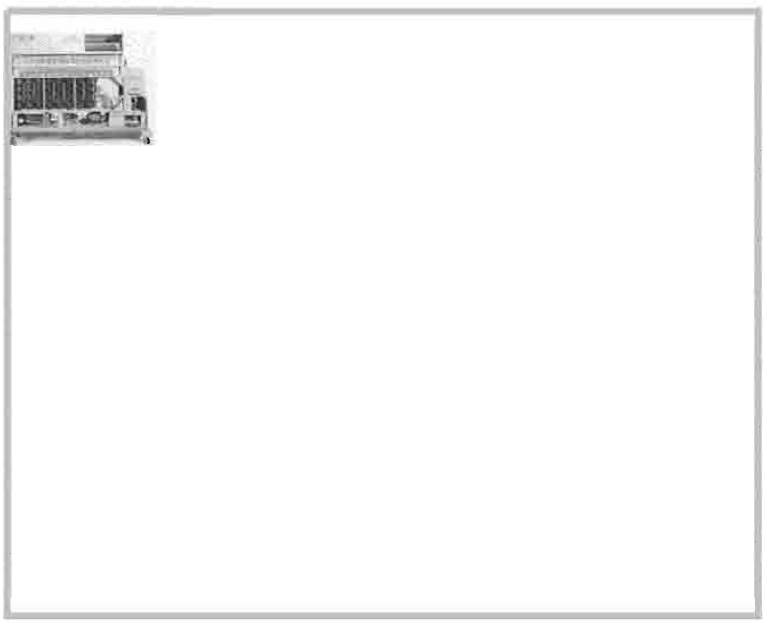
(~~TS//SI~~) Sixteen "Enigmas," one diagonal board, and fewer testing circuits made the American Bombes much less discriminating than the new British ones (thirty-six Enigmas and two boards); but Desch's Bombes were much more reliable and needed remarkably little maintenance once they were broken in.[142]

(~~TS//SI~~) Although Desch's model was based on the logic, parallel architecture, and hardware of the British Bombe, his machine was an original. The truly distinctive part of Desch's machine was its electronics.

(~~TS//SI~~) He did not rely upon the designs of the new Keen Bombe, the Mammoth, nor did he copy Wynn-Williams' ideas.[143]

(~~TS//SI~~) Although Wynn-Williams' partially electronic machine, the Cobra, was more sophisticated in some ways than Desch's, Desch's was more effective. Wynn-Williams' device printed solutions on the fly, but it proved somewhat unreliable. Desch's Bombe also proved more trustworthy than Keen's latest electromechanical one.[144]

(~~TS//SI~~) Desch was forced to bow to some other technological limits since his Bombes contained sixteen not twenty-four (or, like the British machines, over thirty) Enigma analogs. Each of the sixteen units was housed in a separate rack, which took up as much space as the three-per-rack configuration that had been the goal in September 1942.



(~~TS//SI~~) Bombe

(~~TS//SI~~) Although the American Bombes did their jobs, they could not use long and discriminating cribs of more than sixteen letters, as could the British devices. Desch had balanced his understanding of the power of short cribs against the mechanical difficulties of driving a large number of commutators.[145]

(~~TS//SI~~) The information about cribs and menus that had been revealed after October 1942 also helped Desch decide against attempting to incorporate a helpful but challenging feature: automatic slow-wheel turnover. Desch did not build a means of kick-

ing the slower wheels to a new position relative to its mates after a faster wheel had completed a full revolution. Relying upon the probabilities that hits could be discovered before the fast wheel reached the point where the next wheel should be pushed ahead one or more letters, hand-setting of displacements during the commutator setup, and the use of a two-part menu allowed the Bombe design to remain manageable.[146]

~~(TS//SI)~~ However, this meant that when "hoppity" menus (fast-wheel turnover positions known) were run, the Bombe operators had to stop the machines, then reset wheel positions by hand and restart the Bombe.[147]

(U) Ignorant No More

(U) However, with the help of his electronic memory system and the maturation of "G's" Enigma cryptanalytic skills, Desch came very close to achieving all the hopes for the American Bombe.

~~(TS//SI)~~ Because of his engineering skills and the use of strong menus, the NCR Bombe took twenty, not fifty, nor the worst case, 380 minutes, for a run. A major reason was that the British cryptanalysts (and later "G's" experts) were able to supply menus that produced on the average five- or so prints or "stories" per run – not 40,000.[148] The menus eliminated so many of the possibilities that the Bombes stopped, rewound, and restarted very infrequently. That saved significant amounts of time.

~~(TS/SI)~~ In terms of raw speed, Desch's 1943 machine was 200 times faster than the Polish Bomba, at least twenty times faster than the Turing Bombe, and at least thirty percent faster than Britain's 1943 four-wheel Bombe.[149] His machine was able to run either three-or four-wheel tests.

~~(TS//SI)~~ As important for the success of the NCR Bombes were the menus for them. Unfortunately, it took the Americans many, many additional months before they learned how to consistently supply "strong" menus. Fortunately, by late summer 1943 the British were willing to wire cribs and other Bombe instructions directly to "G's" Washington headquarters. They forwarded them as soon as they located the reencodements and other German procedural errors that were allowing them into the Shark system.[150]

(U) The Bombes at Work

(U) Desch's manufacturing techniques gained the respect of the once skeptical British. By mid-November Washington had over fifty bombes in operation and thirty more on site.[151] The American navy finally began to be a truly productive Ultra member. By the end of the year, the first contract was completed,[152] and Engstrom began to turn his crews to other technical and cryptanalytic problems.

(U) Although the second American Bombe project, from the first investigations to the last delivery, took almost a year longer than expected, Desch and OP-20-G received applause, not criticism, in late 1943.[153] As a result of Dayton's achievement, the British found it impossible to continue on with a condescending attitude. The Americans soon became the guardians of the U-boat work, and Britain felt confident enough to concentrate on the Fish system and German army traffic.[154] From mid-1943 to the end of the war, M4 was open to America and Britain.[155]

(U) But the American Bombes were born a bit too late. By the time the Washington center received its machines, the four-wheel U-boat traffic was light.

~~(TS//SI)~~ Or at least the British thought so. They complained that the Americans were running their precious Bombes against low-priority messages and were using menus that were highly unlikely to produce a break. They more than suggested that Engstrom should agree to a true

"sharing" of Bombe resources. They wanted the American navy to run important German air force and army problems and to help with the "European" part of the war.[156]

(~~TS//SI~~) Productive work was found for the more than one hundred American machines. The navy's men soon began the analysis of other German Enigma systems. Although somewhat worried about breaching the agreement with Friedman's American army group, OP-20-G took on much German three-wheel air force work.[157]

(~~TS~~) By autumn 1944, 60 percent of the navy's Bombe time was devoted to German air force and army problems as presented by the British.[158] OP-20-G contributed more to the non-naval work. After rejecting a British plea to quickly construct another fifty Bombes and complaining that England had not contributed enough to the four-wheel effort, NCR built another two dozen Bombes. The new machines were somewhat more sophisticated than the first version.[159] Britain did place more and more responsibility for four-wheel bombes on the Americans, even announcing at one point that Keen would return to building three-wheel machines. The second series of American Bombes had a "double input" feature that eliminated more false hits.

(U) In addition to constructing the new Bombes, NCR built a series of attachments for them and the older machines. As well, they put into use other devices needed to automate the final steps in identifying Enigma keys.

(~~TS//SI~~) An Enigma attack was aimed at discovering seven things about an Enigma setup: [160]

1. Rotor wiring
2. Reflector plugging
3. Stecker setting
4. Rotor order
5. Window setting (starting point)
6. Ring or core setting
7. Notch pattern (turnovers)

(~~TS//SI~~) Given a strong crib of about sixteen letters, knowledge of the rotor wiring, a correct guess as to the reflector's plugging and a large number of Bombes, analysts could expect to get back some very good indications of the stecker setting, the rotor order, and some indirect help on the window setting, the ring setting, and the notch pattern. The Bombe was a relatively strong and quick means for a solution. But it needed some help.

(U) More to It Than the Bombe

(U) The Bombe was a powerful anti-Enigma tool, but by itself could not yield all that needed to be known about Enigma settings. On the other hand, it was, in some contexts, an example of overkill. When several elements of an Enigma setting were already known, other machines were much more efficient.[161]

(~~TS~~) For example, Hypo, the microfilm machine that had been constructed so that a pure statistical attack could be mounted against the Enigma, was called into service as a "locator."

(~~TS//SI~~) When the Bombes had done their jobs and the rotor order and wiring, the stecker, and the Uncle Walter were known, Hypo was used to find the window setting through a letter frequency test.[162] Hypo helped in certain tough cases, but it took a great deal of time. Developing its film took forty minutes, and a "three-wheel" Hypo test took seventy minutes. And Hypo demanded humidity- and light-controlled rooms.[163]

(~~C//SI~~) The navy group at NCR found a faster way to handle such tasks. They built electrical attachments for the Bombes. These "Grenades" were large panels containing pluggable switch banks, which were used to control the Bombes. Their most frequent applications called for only a few of the sixteen banks on a Bombe and ran very

quickly. In most instances a Grenade run took fifty seconds.[164]

(~~TS//SI~~) There were many varieties of Grenades. One of the firsts was for the window settings when the other Enigma crypto-variables were known. Mrs. Driscoll had outlined the logic for the first American Grenade to John Howard a month before the Bombe project had been approved in September 1942. He implemented those ideas in the technology of the Bombes as well as in the film machines.[165]

(~~TS//SI~~) The Driscoll-Howard Standard Grenades appeared as soon as the Bombes came into operation. They were a great help because they reduced the effort needed to identify the window settings for succeeding messages once the Bombes had found the daily key. With the known daily key, all that was needed was a short four- or five-letter crib.

(~~TS//SI~~) The usefulness of the Standard Grenades was increased when "G" discovered how to put them to exploiting German errors such as selecting wheel orders in a "Cilly" or non-random way. The Standard was also helpful in discovering why certain messages would not yield to the regular Bombe attack. The Grenades became a major way of exploring such "dud" messages.[166] The Standard became a necessity at "G," and one was built into each of the second, 1944, models of the Bombes.[167]

(~~TS//SI~~) Once "G's" men had the opportunity, they began to build a series of additional Grenades; each provided an efficient solution to a particular Enigma problem, and each extended the power of the Bombes.

(~~TS//SI~~) The Parallel Grenade allowed four short cribs to be used simultaneously to find the window settings. The Drag Grenade went further. It tested the four cribs, position by position, against a sixteen-letter cipher text. Its sister, the Polygrenade, was more powerful. It dragged the crib twenty-six positions at a time. The simpler Jones Dudbuster imitated the large paper catalogs by dragging a common word such as "eins" through the text.[168]

(~~TS//SI~~) The Sliding Grenades expanded the Bombe's power by handling those Enigmas with rotating reflector wheels. The Pluggable-Series Grenade was quite clever; it found the wheel order and ring setting for traffic produced using a double indicator.[169]

(~~TS//SI~~) The most impressive of the Grenades was the Universal Plugboard. It was so flexible that it was used to explore many different ideas. Its main operational use was to try up to twenty-six cribs over thirteen letters – quite an imaginative use of plugs and wires.

(~~TS//SI~~) Some of the Grenades were asked to solve more complex problems. To do so they used all of a Bombe or two Bombes lashed together. The Query found settings from the indicators on the messages. The Cilly automated the exploitation of nonrandom selection of part of a message setting.[170]

(~~TS//SI~~) Electronic devices were also used to make the Bombes more effective. Tube circuits were added to the first (N530) Bombes to compensate for weak menus that were producing too many stops. That Self-Detector was a set of the special four-in-one tubes attached to the original diagonal board. It suppressed stops that did not have a particular diagonal board connection: a letter connected to itself, that is, unsteckered. Statistical analyses had shown that it was very unlikely that a stop without such a connection would lead to the unraveling of an Enigma key.[171]

(~~TS//SI~~) The electronic Squelcher incorporated a more general test to eliminate stops unlikely to produce key. It was a substitute for the original electronic amplifier system in the N530 Bombes. It was conceived when the worries about weak menus were intense. Once the Americans learned

the tricks of menu building, they decided that only a few of their old Bombes needed to have the Squelchers.[172]

(U) The success of Grenades and Squelcher circuits were only two of the indicators that Engstrom's group was beginning to overcome the chaos of 1942 and early 1943. By the fall of 1943 things were going much, much better for Wenger's dreams for a permanent RAM program. In addition to the Bombes, OP-20-G finally began to receive the Gray-NCR and the Eastman machines. The first of the new Bush Comparators was put into operation in September. The new Comparator had a somewhat rocky career, however. When it arrived in Washington, it had several flaws, including the incompatibility of its major components; incorrect specifications had been sent to the contractors. It also proved to be much slower than desired. But the complaints about the machine's failings were turned to "M's" advantage. The critics were assured that placing the next developments in the hands of the OP-20-GNCML group would prevent such mistakes.[173] The failings of Eastman-Kodak's devices were also used as arguments for an expansion of "G's" own research and development.[174] All in all, by January 1944, OP-20-G's RAM group seemed vindicated and ready to return to the extension of the microfilm and digital electronic technologies. Some hoped there would be time to search for a general-purpose cryptanalytic machine, one that went beyond the Bush Comparator.

Notes

1. (U) NSA Bombe File, U.S. Navy OP-20-G/OP-20-2, Memo to Station X, "Decision regarding future E policy," app. May 1942.

2. (U) Gordon Welchman, *The Hut Six Story* (New York: McGraw-Hill, 1982), 51.

3. (~~TS//SI~~) On the Enigma, (TS//SI) NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*].

4. (~~TS//SI~~) NSA AHA 17580, Telford Taylor to Clarke and Corderman, "Early E. History," 10.

5. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. (~~TS//SI~~) NSA CCH "P" Collection Box CC067, RIP 608, CITS Paper TS-10/E-6, "Enigma Series Vol. 6, Duenna," CNC-OP-20, January 1946.

6. (~~TS~~) NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945," 12. (S) NSA AHA ACC 35701, "German Communications," 11 October 1943.

7. (U) Jean Stengers, "La guerre des messages codes, 1930—1945" *L'Historie*, 31 (1981): 19-31. Cipher A. Deavours, and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, Mass.: Artech House, 1985), 117.

8. (~~S~~) NSA AHA ACC 35701, "German Communications," 11 October 1943.

9. (~~TS//SI~~) Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 175. Thomas Parrish, *The Ultra Americans: The United States' Role in Breaking the Nazi Code* (New York: Stein & Day, 1987), 49. Cipher A. Deavours, and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, Mass.: Artech House, 1985), 117. (~~TS~~) NSA CCH Series IV.7.20, A. P, Mahon, "The History of Hut Eight, 1939-1945." (TS//SI) NSA CCH Series XII Z, GCCS, "OP-20-G Contribution."

10. (U) Wladyslaw Kozaczuk, *Enigma* (Frederick, Md.: University Publications of America, 1984). Jean Stengers, "Enigma, the French, the Poles and the British, 1931-1940," in Christopher Andrew and David Dilks (ed.), *The Missing Dimension* (London, 1984). Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 170-175.

11. (~~TS//SI~~) NSA AHA 17580, Telford Taylor to Clarke and Corderman, "Early E. History."

12. (U) Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 176. Some of the Scandinavian nations may have had sporadic successes against Enigma and Fish, which they shared with Britain. But the true burden had to be carried by the British. *Cryptologia*, 12 (1988): 39, review of W. M. Carlgren, *Svensk Underrattelsetjanst 1939-45*, (Stockholm, 1985).

13. (TS) NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945."

14. (U) Alan Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983). A. G. Denniston, "The Government Code and Cypher School between the Wars," *Intelligence and National Security*, I (1986): 48-69. Christopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York: Penguin, 1987).

15. (U) Martin Campbell-Kelly, *I C L: A Business and Technical History* (Oxford: Clarendon Press, 1989), 118. Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes* (New York: McGraw-Hill, 1982), 295. Cipher A. Deavours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, Mass.: Artech House, 1985), 119, 124.

16. (U) David Kahn, *Seizing the Enigma* (Boston: Houghton Mifflin, 1991), 141. Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 233. At one point Turing may have considered building a film machine for the method rather than using punched overlay sheets. It would have speeded the search or "coincidences" as did Bush's machine. But note that for Banburismus to be effective, captures of tables of some of the Enigma settings were vital. In 1938, the British used another statistical test called SAGA. It also appears to be the kind of approach used by Mrs. Driscoll in America.

17. (TS) NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight," 1939-1945."

18. (TS) Scritching looked for contradictions produced by assumption, concerning the settings of a cipher machine. It reduced the number of possibilities that have to be examined. (TS//SI) CCH Series XII Z, "Army-Navy, Descriptive Dictionary of Cryptologic Terms," ASA February, 1947.

19. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

20. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

21. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

22. (TS) On other statistical methods, (TS) NSA CCH Series IV, 7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945."

23. (TS) A very readable and complete description of the British Bombe is found in NSA CCH Series XII Z, "The General Cryptanalytic Branch."

24. (TS) NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945."

25. (TS) NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945," 28.

26. (TS//SI) Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 176. Gordon Welchman, *The Hut Six Story: Breaking the Enigma Codes* (New York: McGraw-Hill, 1982), 295. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

27. (U) Such commutator systems had been used in electrical timing instruments, but Keen did truly creative work.

28. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

29. (TS//SI) Martin Campbell-Kelly, *I C L: A Business and Technical History* (Oxford, Clarendon Press, 1989), 119. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

30. (U) There are some different interpretations in Bradley F. Smith's, *The Codebreaker's War: The Ultra-Magic-Deals* (Novato: Presidio Press, 1993). Because of my evidence I remain convinced, for example, that the Americans took the lead in their Bombe program and that they intended to produce more than 300 machines. See Smith, 247. 26. F. H. Hinsley, *British Intelligence in the Second World War, Volume II* (New York: Cambridge University Press, 1981), 747.

31. (U) Jurgen Rohwer, *The Critical Convoy Battle of March 1943* (London: Ian Allan, 1977), 240. Nigel West, GCHQ, the *Secret Wireless War*, 1900-86 (London: Weidenfeld and Nicolson, 1986), 201, 210. F. H. Hinsley, *British Intelligence in the Second World War*, vol. III, Part I, (1984), 52.

32. (S) NSA CCH Series XII Z, Robert L, Benson, "The Origin of U.S. British Communications: Intelligence Cooperation (1940-41)," NSA *Cryptologic*

Spectrum, 4 (Spring 1944): 5-8. (S) NSA CCH Series II Z, "History of GET (TUNNY) Research."

33. (U) NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 017. Louis Kruh, "British-American Cryptanalytic Cooperation and an Unprecedented Admission by Winston Churchill," Cryptologia, 13 (1989): 123-134. Nigel West, GCHQ, 201. F. H. Hinsley, *British Intelligence in the Second World War*, Vol. I (London: Her Majesty's Stationery Office, 1979), 155. NSA RG457, SRH-197, "U. S. Navy Communications Intelligence, Organization, Liaison and Collaboration, 1941-45." But both Britain and the Dutch provided the Americans with intelligence and cryptanalytic help on Japanese systems earlier than previously thought. See Rear Admiral Edwin T. Layton, *And I Was There: Pearl Harbor and Midway: Breaking the Secrets* (New York: William Morrow, 1985), 206. John W. M. Chapman, "Pearl Harbor: The Anglo-Australian Dimension," *Intelligence and National Security I (* 1989), 451-481. James Rusbridger and Eric Nave, *Betrayal at Pearl Harbor* (New York: Summit Books, 1991).

34. (U) NARA RG457, SRH-141, "Papers from the Personal Files of Alfred McCormick, Part 2, March 4, 1944," "Memorandum for General Bissel, Army-Navy Agreement Regarding Ultra." NARA RG457, SRH 152, "Historical Review of OP-20-G.

35. ~~(S)~~ NSA CCH Series XII Z, Robert L. Benson, "The Origin of U.S. British Communications Intelligence Cooperation (1940-41)," NSA *Cryptologic Spectrum* 4 (Spring 1944), 5-8.

36. ~~(TS//SI)~~ Laurance Safford, "Rhapsody in Purple," by Linda P. Tucker, Cryptologia, 6 (1981), 193-229, and 346-367. James Rusbridger and Eric Nave, *Betrayal at Pearl Harbor* (New York: Summit Books, 1991). NSA SRH-391, "U.S. ~~(TS//SI)~~ NSA CCH Series XII Z, "Washington E Traffic, Notes on Correspondence" circa February 1942.

37. (U) David Kahn, *Seizing the Enigma* (Boston: Houghton-Mifflin, 1991), 235-6. NARA RG457, SRH-145, "Collection of Memoranda on Operations of SIS Intercept Activities and Dissemination 1942-1945," "Report of the Technical Mission to England" April 11, 1941, 002-013. Greg Mellen (ed.), "Rhapsody in Purple: A New History of Pearl Harbor by Dundas P. Tucker," *Cryptologia*, 6 (1981), 193-228. More balanced views are in Rear Admiral Edwin T. Layton, *And I Was There: Pearl Harbor and Midway: Breaking the Secrets* (New York: William Morrow, 1985) and Edward J. Drea, *MacArthur's Ultra* (University of Kansas Press, 1992). The Americans did not give everything to the British, however. NARA RG298, Box 39, Memorandum of R. W. Sylvester to L. Terman, April 11, 1942, tells Terman not to disclose any cryptological work to the British. And the Americans also kept their very important SIGCUM enciphering machine from the British during much of the war. See NARA RG457, RMA003, May 19,1944, Memorandum for Assistant Chief of Staff, G-2 from Office of the Chief Signal Officer.

38. (U) NARA RG457, SRH-270, "Army Navy FBI COMINT Agreements of 1942" by Robert L. Benson, and the very useful SRH-005, "Use of CX/MSS Ultra."

39. ~~(S)~~ NSA CCH Series IV V 10.1, "Report of the Technical Mission to England," 11-4-1941.

40. (U) NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," and SRH-145, "Collection of Memoranda on Operations of SIS Intercept Activities and Dissemination 1942-1945," 'Report of the Technical Mission to England' April 11, 1941, 002-013. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] ~~(TS)~~ NSA CCH R Collection, Box CCO 66, OP-20-G-A, "American Cryptanalysis of German Naval Systems," 7 July 1944.

41. ~~(S)~~ Laurance Safford, "Rhapsody in Purple," by Dundas P. Tucker, *Cryptologia*, 6 (1981), 193-229, and 346-367. NARA, RG457, SRH-361, "History of the Signal Security Agency," 259, 261. There is some reason to believe that Britain did pass on the ways to crack the simpler 1940 German air force systems. NSA RAM File, "Report to J. N. Wenger, Capt. USN, Resume of the Dayton, Ohio Activity During World War II," and, J. T. Pendergrass, "Cryptanalytic Use of High-Speed Digital Computing Machines," ~~Top Secret,~~ 1946. ~~(S)~~ NSA CCH Series IV V 10.1, "Report of the Technical Mission to England," 11-4-1941.

42. ~~(TS)~~ NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. ~~(S)~~ NSA CCH

Series IV V 10.1, "Report of the Technical Mission to England," 11-4-1941. (TS) NSA CCH R Collection, Box CCo 66, OP-20-1 to OP-20-GY-A, 7 July 1944, "American Cryptanalysis of German Naval Systems."

43. (TS) NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944.

44. (TS//SI) NSA CCH Series XII Z, "Washington E Traffic, Notes on Correspondence" circa February 1942. (TS) NSA AHA.ACC 35701 "History of the Bornbe Project," 16 February 1946."

45. (TS) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946.

46. (U) David Kahn, *Seizing the Enigma* (Boston: Houghton-Mifflin, 1991), 237.

47. (TS) NSA ARA ACC 35701 "History of the Bombe Project," 16 February 1946. (TS) NSA CCH Series IV V 10.6, Chief Signal Officer, "A Chronology of the Cooperation Between the SSA and the London Office of GCCS," 2 June 1946.

48. (TS//SI) NSA CCH Series XII Z, "Washington E Traffic, Notes on Correspondence" circa February 1942.

49. (S) An invaluable document on British-U. S. Army relationships, NARA RG457, SRH-005, "Use of CX/MSS Ultra," and of equal value, "History of 3-US," as in John Mendelsohn (ed.), *Covert Warfare: Intelligence, Counterintelligence & Military Deception During the World War II Era* (Garland, 1989). (S) NSA CCH Series XII Z, Wenger to OP-20, October 1, 1942, "Collaboration of U. S. and British radio Intelligence organizations on Japanese and German projects." Robert L. Benson, *A History of U. S. Communications Intelligence during World War II: Policy and Administration*, Center for Cryptologic History, NSA, 1997.

50. (U) For the complaints by the American army's SIS, see NARA RG457, SRH-361, "History of the Signal Security Agency" Vol. II. 249-275.

51. (TS) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. (TS) NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944. (S) NSA CCH series XII Z, Redman to OP-20, 2-28-1942, "British not cooperating."

52. (TS) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. (TS//SI) NSA CCH Series XII Z, (Sl2OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] (TS) NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944.

53. (TS) NSA CCH Series XII Z, Travis to OP-20-G, 13 May 1942 – "Will Send Bombe to you in August or September."

54. (TS) NSA CCH Series XII Z, Travis to OP-20-G, 13 May 1942 – "Will Send Bombe to you in August or September."

55. (TS) Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon. and Schuster, 1983), 191. Laurance Safford, "Rhapsody in Purple," by Dundas P. Tucker, *Cryptologia*, 6 (1982), 216-17. NSA RAM File: OP-20—G to GC&CS, July 7, 1942; OP20-G to OP-20 September 3, 1942; J. N. Wenger to OP-20-GM, August 6, 1942 "We wish to construct..."; and Wenger to Ely, August 5, 1942; Engstrom to Meader re Turing visit, January 5, 1943. F. H. Hinsley, *British Intelligence in the Second World War*, Vol. 1, 56. Joseph Eachus, letter to the author, March 24, 1989. "History of 3-US," in John Mendelshon (ed.), *Covert Warfare* (Garland, 1989), 010-012. (TS//SI) On the continuing problems, it SIS, (TS) NSA CCH Series IV V 10.6, Chief Signal Officer, "A Chronology of the Cooperation Between the SSA and the London Office of GCCS," 2 June 1946. On the August protest by "G," (TS) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. (S) NSA CCH Series XII Z, Eachus to Wenger, 2 August 1942, "Full Wiring Diagram on Way." (S) NSA CCH Series XII Z, Wenger to Op-20-GM, 6 August 1942, "Nature of E machine."

56. (U) The group at Bletchley Park cracked the new four-wheel system by December 1942. But the break was not a pure cryptanalytic one. It depended upon the capture of documents and the continued failure of the German system managers to follow basic security procedures. David Kahn, *Seizing the Enigma* (Boston: Houghton-Mifflin, 1991), 111.

57. (U) Laurance Safford, "Rhapsody in Purple," by Dundas P. Tucker, *Cryptologia*, 6 (1982), 193-229, and 346-367.

58. (U) Even Britain waited what now seems too long to organize its research. Ronald Clark, *Tizard* (Cambridge: MIT Press, 1965).

59. (U) The Coast Guard, which had been in charge of decrypting rumrunner and other clandestine traffic for years, had as its chief cryptanalyst William Friedman's wife. The clandestine system the Coast Guard attacked must have been very simple compared to the Enigma.

60. (~~TS//SI~~) NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] 51, 53. (~~TS~~) NSA CCH R Collection, Box CCO 66, OP20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944.

61. (U) NARA RG457, SRH-306, "OP-20-G Exploits and Commendations in World War II" 016. NSA RAM File, "Report to J. M. Wenger, Capt. USN, Resume of the Dayton, Ohio Activity During World War II," and J. T. Pendergrass, "Cryptanalytic Use of High-Speed Digital Computing Machines," Top Secret, 1946. (~~TS~~) NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944.

62. (~~TS//SI~~) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution." GC&CS learned of the possible introduction of the fourth wheel in May 1941 but did not get Wynn-Williams to work until very late in the year. His work proceeded at a very slow pace. Doc Keen was not put to work to think about a high-speed Bombe for the four-wheel problem until late spring 1942.

63. (~~TS~~) NSA CCH Series XII Z, Hut 6, 4 October 1942, "Electronics for Bombe not Working."

64. (U) Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 225-7.

65. (~~TS//SI~~) Keen built several new versions of his original Bombes. The new Mammoths and Jumbos handled the standard three-and four-wheel Enigma problems, while the Giants, Ogres and Twinns were, like some American variants, commutator-based machines for special Enigma variation problems. (~~TS//SI~~) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution." (~~TS//SI~~) NSA AHA ACC 17738, "E Operations of the GC&CS, list of machines," 25 February 1945.

66. (~~TS~~) Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 227. (~~S~~) NSA CCH Series XII Z, Eachus to Wenger, 18-9-1942, "British four wheel design not progressing." (~~TS~~) NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945. (~~TS~~) NSA CCH Series XIII Z, Hut 6, 4 October 1942, "Electronics for Bombe not Working." (~~TS~~) NSA AHA ACC 35173, CNO, CITS TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Navy Dept., Washington, September 1946.

67. (~~TS//SI~~) NSA Bombe File, "It is desired to construct..." April 25, 1942, and August 5, 1942, Wenger to Ely. (~~TS//SI~~) NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*].

68. (~~TS//SI~~) NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] 51, 53.

69. (~~TS~~) NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944. (~~TS~~) NSA AHA 35529, Friedman to Corderman, 29 March, 1944, "Comparison of our "003" type of "Bombe" with the rotary type.

70. (~~TS~~) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. (~~TS//SI~~) Navy Dept., Office of Chief of Naval Operations, RIP 607, Enigma Series, volume 5., CIT TS-10-E-5, "Bombe Computations." (~~TS~~) NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944. (~~TS//SI~~) NSA CCH P series Box CCO 67, RIP 607 shows that when "G" did finally incorporate a diagonal board it looked for hot-points; the British looked for coldpoints.

71. (~~TS~~) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. (~~TS//SI~~) Navy Dept., Office of Chief of' Naval Operations, RIP 607, Enigma Series, volume 5., CIT Ts-10-E-5, "Bombe Computations."

72. ~~(TS//SI)~~ Navy Dept., Office of Chief of Naval Operations, RIP 607, Enigma Series, volume 5., CIT Ts-10-E-5, "Bombe Computations."

73. ~~(TS//SI)~~ Navy Dept., Office of Chief of Naval Operations, RIP 607, Enigma Series, volume 5., CIT Ts-10-E-5, "Bombe Computations." ~~(TS//SI)~~ NSA CCH Series XII Z (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] 51-3. ~~(TS)~~ NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944.

74. (U) NSA RAM File, "Decision Regarding Future E Policy," app May 1942, and "For GC&CS" August 5, 1942.

75. (U) NSA RAM File, app. May, 1942, OP-20-G to Station X, "Latest Thoughts on Electronic Developments."

76. (U) Much of the information on GC&CS's actions and intention remains in closed archives, and some informed historical guesses have to be made. One of those is that GC&CS's failure to send requested documentation was as much the result of the slow pace of its four-wheel Bombe program and a desire to keep face as it was the result of a desire to monopolize all the "E" work.

77. ~~(TS)~~ NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946, 4.

78. ~~(S)~~ Britain sent more assurances to the United States in August, but they were too late to stop "G" from going ahead with its Bombe program. ~~(S)~~ NSA CCH Series XIII Z, Eachus to Wenger, 2 August 1942, "Full Wiring Diagram on Way." ~~(S)~~ NSA CCH Series XII Z, Wenger to Op-20-GM, 6 August 1942, "Nature of E machine."

79. (U) NSA RAM File, OP-20-G to GC&CS, July 7, 1942, "Eachus & Ely," and August 5, 1942, "Send Wiring Diagram." NARA RG457, SRH-306, "OP-20-G Exploits and Commendations in World War II," 23, "Shark was not all." Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 236. F. H. Hinsley, *British Intelligence in the Second World War*, Volume II (New York: Cambridge University Press, 1981), 55-57.

80. ~~(TS//SI)~~ The Robinsons were independent creations but were much like the Bush comparator machines. However, they were built to handle the codes used on teletype systems, and they were not strict embodiments of the IC method but of Turing's new Delta method, which searched for statistical biases in the distribution of binary values. However, Delta shared much with the IC approach. ~~(TS//SI)~~ (Laconic, Nocon) NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," ~~(TS//SI~~ NSA CCH Series XII Z, H. H, Campaigne, "Reading TUNNY," NSA *Technical Journal* (Fall 1962). ~~(TS//SI)~~ NSA CCH Local Archive, "Army-Navy Descriptive Dictionary of Cryptologic Terms," Army Security Agency, February 1947.

81. ~~(TS//SI)~~ Letters from Howard Campaigne to Brian Randell circa 1975. Thomas H. Flowers, "The Design of Colossus," *Annals of the History of Computing*, 5 (July 1983), 224. I. J. Good, "Early Work on Computers at Bletchley," *Cryptologia* 3 (1979), 65-77. ~~(TS//SI)~~ NSA CCH Series XII Z, H. H. Campaigne, "Reading TUNNY," NSA *Technical Journal* (Fall 1962).

82. ~~(TS//SI)~~ The Robinsons, also called "bedsteads," became more and more powerful and rapid. Some models used vacuum tubes, and by the war's end, one of the Robinsons used four tapes. ~~(S)~~ NSA CCH Series XII Z, GCHQ, "Machine Solution of TUNNY Traffic (Robinson)," 22 August 1943. ~~(TS//SI)~~ NSA CCH Local Archive, "Army-Navy Descriptive Dictionary of Cryptologic Terms," Army Security Agency, February 1947.

83. (U) NSA CCH XI K, S. Snyder, Box, II, B. Randell, "The Colossus," June 1976. ~~(TS//SI)~~ NSA CCH Series XII Z, "Theory of Rectangles: Photostat of British Paper describing breaking of the TUNNY Machine by Means of Rectangles," 4 September 1944. ~~(TS//SI)~~ NSA CCH Series XII Z, "Fish Notes," December 1944. (TS//SI) NSA CCH Series XII Z, "Colossus, Instructions and procedures used in setting FISH messages on the Colossus," 14 December 1944.

84. ~~(TS//SI)~~ NSA CCH Series XII Z, "Colossus, Instructions and procedures used in setting FISH messages on the Colossus," 14 December 1944.

85. (U) Thomas H. Flowers, "The Design of Colossus," *Annals of the History of Computing* 5 (July 1983): 240. Allen W. M. Coombs, "The Making of Colossus" *Annals of the History of Computing* 5

(1983): 253-259. W. W. Chandler, "The Installation and Maintenance of Colossus," *Annals of the History of Computing* 5 (1983): 260, Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 268. Although their documentation is still classified, there were additional electronic machines in GC&CS's arsenal by the end of the war. Apparently, they went beyond Colossus.

86. (U) NARA RG457, SRH-349, "Achievements of the SSA in World War II," and SRH-361, "History of the Signal Security Agency."

87. (U) NSA RAM File, OP-20-G to GC&CS, app. May, 1942, 'Future E Policy,' and Wenger to Ely, August 5, 1942.

88. (U) Ronald Lewin, *The American Magic* (New York: Farrar, Straus, Giroux, 1982), 85. Rear Admiral Edwin T. Layton, et al., *And I Was There: Pearl Harbor and Midway: Breaking the Secrets* (William Morrow & Co., Inc., 1985), 95. W, J. Holmes, *Double-Edged Secrets* (Annapolis: Naval Institute Press, 1979). One story is that Washington found different additives from their JN-25 analyses and thought that Hawaii was far off base regarding the recovered code groups.

89, (U) NSA RAM File, August 5, 1942, Wenger to Ely. NSA RAM File, Part II of Report to J. N. Wenger, Capt. USN, "Resume of the Dayton, Ohio Activity During World War II." Hagley Museum and Library, Accession 1825, Honeywell v Sperry-Rand, Trial Records, August 19, 1942, Desch to Engineering Department, "Special Switch," and September 18, 1942, "Change in Specifications."

90. (U) NSA RAM File, Part II. of Report to J. N. Wenger, Capt. USN, "Resume of the Dayton, Ohio Activity During World War II."

91. (U) A simple electronic American Bombe would have sixty-four fixed double wheels calling for at least 7,000 tubes, probably twice that. Amplifiers and control electronics would probably have called for another 10,000 or so. A universal machine, in which all wheels could be automatically set, would have needed close to 100,000 tubes. Correspondence with Joseph Eachus. NSA RAM File, Wenger to GC&CS, September 4, 1942, "Electronic Device."

92. (U) F. H. Hinsley, *British Intelligence in the Second World War*, Volume III (New York: Cambridge University Press, 1981), 56. For the independent research agreement, interview with Joseph Eachus. The situation with the American army may have been even more critical. It was a pure consumer of Ultra and much other intelligence during the North African invasion and as late as February 1943, it was dependent on GC&CS for German signal intelligence. NARA RG457, SRH-364, "History of the Signal Security Agency, Volume One Parts 1 and 2, 1939-1945. A Declaration of Independence."

93. ~~(S)~~ NSA CCH Series XII Z, Eachus to Wenger, 18-9-1942, "British four-wheel design not progressing."

94. ~~(TS)~~ NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946, 4. ~~(TS)~~ NSA CCH Series XII Z, Engstrom to Desch, September 23 1942, "Your Bombe plan approved."

95. (U) NSA RAM File, September 3, 1942, Wenger to OP-20, "Cryptanalysis of the German (Enigma) Machine." F. H. Hinsley, *British Intelligence in the Second World War*, Volume II (New York-, Cambridge University Press, 1981), 57. Hagley Museum and Library, Accession 1825, Honeywell v Sperry-Rand, Trial Records, September 18, 1942, Desch to Engineering Department. Compare the Americans' promised production rate with Keen's output. Martin Campbell-Kelly, *I C L: A Business and Technical History*, (Oxford: Clarendon Press, 1989), 118-119. If the United States had built the 350 machines rather than the 100 in the first batch, the cost would have been a staggering $16,000,000 based on the $45,000 per machine for the production run.

96. ~~(S)~~ NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electro-mechanical analytical machine," 15 September 1942.

97. ~~(S)~~ NSA CCH Series XII Z, Report of Dr. Turing, "Visit to National Cash Register Corporation of Dayton, Ohio," circa Dec. 1942.

98. ~~(TS)~~ NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945," 63, states that the later versions of the British high-speed Bombe had fast wheels which moved at 10,000 revolutions per minute. But this figure may be a typographical error. Most other sources give a much lower rpm for the British four-wheel Bombe. See ~~(TS)~~ NSA CCH Series XII Z, Hut 6, "Electronics for Bombe not Working,"

which in late 1942 gives a projected speed of 2,000 rpm. Also see (~~TS~~) NSA CCH Series XII Z, Joan Murray, "A Personal Contribution to the Bombe Story," *NSA Technical Journal*, 20 (Fall 1974): 41.

99. (~~S~~) NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electro-mechanical analytical machine," 15 September 1942.

100. (~~S~~) NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electro-mechanical analytical machine," 15 September 1942, 9.

101. (~~S~~) A full diagonal board would be a 26 x 26 matrix, which would need 676 primary tubes and a score of complementary electronic components. (~~S~~) NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electromechanical analytical machine," 15 September 1942, 9.

102. (~~S~~) NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electro-mechanical analytical machine," 15 September 1942, 1.

103. (~~TS//SI~~) Navy Dept., Office of Chief of Naval Operations RIP 607, Enigma Series, volume 5, CIT Ts-10-E-5, "Bombe Computations."

104. (~~TS//SI~~) NSA CCH Series XII Z, "Cryptanalytic Report #2: The "Yellow Machine," 50-52. (~~TS//SI~~) Navy Dept., Office of Chief of Naval Operations, RIP 607, Enigma Series, volume 5, CI'F Ts-10-E-5, "Bombe Computations." (~~TS//SI~~) NSA AHA 16331, "6812th Signal Security Detachment (PROV) Apo 413 Army," 15 June 1945.

105. (~~TS~~) NSA CCH Series XII Z, Engstrom to Desch, September 23, 1942, "Your Bombe plan approved," (~~S~~) NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electro-mechanical analytical machine," September 15, 1942, 2.

106. (~~TS//SI~~) The men at "G" were not able to intercept and interpret strong menus for quite some time, they sent very weak menus to the Bombes throughout much of 1942 and 1943, They realized they were dependent upon the British for the types of menus that made the Bombes useful by having very few "stories" produced per run. (~~TS~~) NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946. (~~TS//SI~~) NSA CCH Series XII Z, GCCS, "OP-20-G Contribution." (~~TS//SI~~) Navy Dept., Office of Chief of Naval Operations, RIP 607, Enigma Series, volume 5., CIT TS-10-E-5, "Bombe Computations." (~~S~~) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 50-52.

107. (~~TS~~) NSA CCH Series XII Z, Engstrom to Desch, September 23, 1942, "Your Bombe plan approved." (~~S~~) NSA CCH, Series XII Z, Joseph Desch to OP-20-G, "Memo of present plans for an electro-mechanical analytical machine," September 15, 1942, 2.

108. (~~S~~) NSA CCH, Series XII Z, Memorandum for OP-20-G, "Collaboration of U. S. and British Radio Intelligence Organizations on Japanese and German Projects," J. N. Wenger, October 1, 1942.

109. (~~S~~) NSA CCH, Series XII Z, Memorandum for OP-20-G, "Collaboration of U. S. and British Radio Intelligence Organizations on Japanese and German Projects," J. N. Wenger, October 1, 1942.

110. (U) Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, September 18, 1942, Desch to Engineering Department. F. H. Hinsley, *British Intelligence in the Second World War*, Volume II (New York: Cambridge University Press, 1981), 56. NARA RG457, SRH 361, "History of the Signal Security Agency," 274. NSA RAM File: OP-20-G to GC&CS July 7, 1942; OP-20-G to OP-20 September 3,1942; J. N. Wenger to OP-20-GM, August 6, 1942; Wenger to Ely, August 5, 1942; and "Engstrom to Meader re Turing visit," January 1, 1943.

111. (~~S~~) NSA CCH, Series XII Z, Memorandum for OP-20-G, "Collaboration of U. S. and British Radio Intelligence Organizations on Japanese and German Projects," J. N. Wenger, October 1, 1942.

112. (U) Of course, the Americans did not suspect that Britain had its own Russian informant who was telling all to Stalin. Christopher Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev* (New York: Harper Collins, 1990), 304.

113. (U) NARA RG457, SRH-306, "OP-20-G Exploits and Commendations in World War H," 19. F. H. Hinsley, *British Intelligence in the Second World War*, Volume II (New York: Cambridge University Press, 1981), 57. Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 243.

~~(S)~~ NSA CCH Series XII Z, Wenger to OP-20, October 1, 1942, "Collaboration of U. S. and British radio Intelligence organizations on Japanese and German projects."

114. (U) Very useful on the question of the U. S. Army's Ultra struggle is "Origins, Functions & Problems of the Special Branch, M. I. S.," in John Mendelshon (ed.), *Covert Warfare: Intelligence, Counterintelligence and Military Deception During the World War II Era* (Garland, 1989).

115. ~~(TS)~~ NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945," 90.

116. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944 [*sic*], cites October 1942 as the date of arrival of the first M8, but other sources claim it arrived in spring 1943. On the M9, interview with Philip J. Bochicchio, 14 September 1994.

117. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] ~~(TS//SI)~~ NSA CCH "P" Series, Box CC067, CITS, "E" Series, Vol. E-7.

118. ~~(TS//SI)~~ Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 236. NSA RAM File, January 5, 1943, "Report on Turing Visit to Dayton." (S) NSA CCH Series XII Z, Dr. Turing of G.C. & C.S., "Visit to National Cash Register Corporation," December, 1942. ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G "Memoranda on Bombe and the relationship of the U. S. and U. K.," circa 1943.

119. ~~(S)~~ Turing remarked about Desch's apparent decision not to use some features already planned for the new British four-wheel Bombe. ~~(S)~~ NSA CCH Series XII Z, Report of Dr. Turing, "Visit to National Cash Register Corporation of Dayton, Ohio," circa Dec. 1942.

120. ~~(S)~~ NSA CCH Series XII Z, Eachus to Wenger, 18 September 1942, "British four wheel design not progressing.'" ~~(S)~~ NSA CCH Series XIU Z, Report of Dr. Turing, "Visit to National Cash Register Corporation of Dayton, Ohio," circa Dec. 1942.

121. ~~(TS)~~ On British comments besides those of Turing, NSA CCH, shinn box, "Desch."

122. ~~(TS)~~ NSA CCH Series XII Z, Engstrom to Desch, September 23, 1942, "Your Bombe plan approved."

123. ~~(S)~~ NSA RAM File,, January 5, 1943, "Report on Turing visit to Dayton"; January 20, Engstrom to Meader, "Change Bombe Design"; and March 17, 1943 Prototypes constructed.. ~~(S)~~ NSA CCH Series XII Z, Report of Dr. Turing, "Visit to National Cash Register Corporation of Dayton, Ohio," circa. December 1942. ~~(S)~~ NSA CCH Series XII Z, Dr. Turing of G.C.& C.S. "Visit to National Cash Register Corporation," December 1942.

124. ~~(S)~~ On the gearing, interview with Philip J. Bochicchio, 6-14-94.

125. ~~(S)~~ NSA CCH Series XII Z, Dr. Turing of G.C. & C. S., "Visit to National Cash Register Corporation," December 1942.

126. ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G "Memoranda on Bombe and the relationship of the U.S. and U.K.," circa 1943.

127. (U) Interview with Philip J. Bochicchio, 6-14-94.

128. (U) Interview with Philip J. Bochicchio 6-14-94.

129. ~~(TS)~~ Interview with Philip J. Bochicchio, 6-14-94. NSA, CCH Series XII Z, CNO, CITP 88, "Technical and Theoretical Report of N-530 BOMBE, Navy Dept., Washington, D.C., September, 1946.

130. ~~(TS//SI)~~ NSA RAM File, December 11, 1942, Horn to Robinson, "Procurement of Materials for 7892," and December 28, 1942, CNO to Deeds, "Help needed on special project at NCR." ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G "Memoranda on Bombe and the relationship of the U. S. and U. K.," circa 1943.

131. (U) NSA RAM File, January 5, 1943, Wenger to Meader, "Turing Visit,"Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 236.

132. ~~(TS)~~ NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946.

133. (U) NSA NCML Message File, for example, June 4, 1943, "Use most Adam-Eve time for real tests."

134. (U) NSA NCML-CSAW Message file, May 24, 1943, "DC has sent test problems for prototypes," and

May 29, 1943, "Adam Eve have serious technical problems." The first British four-wheel Bombe was completed in June 1943. F. H. Hinsley, British Intelligence in the Second World War, Volume II (New York: Cambridge University Press, 1981), 748.

135. (U) NSA NCML-CSAW Message File, May 29, 1943, "Shorts and opens," and May 31, 1943, "Can use part of machine only."

136. ~~(TS//SI)~~ NSA NCML-CSAW Message File, May 20, 1943,"Redman Visit," and May 29, 1943 "Adam and Eve problems." F. H. Hinsley, *British Intelligence in the Second World War*, Volume II (New York: Cambridge University Press, 1981), 748. Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 267. W. W. Chandler, "The Installation and Maintenance of Colossus," *Annals of the History of Computing* 5 (1983): 261. ~~(TS)~~ On the date of England's first four-wheel Bombe, ~~(TS//SI)~~ NSA CCH Series XII Z, GCCS, OP-20-G Contribution.

137. (U) NSA NCML-CSAW Message File, June 14,1943, "Cain and Abel."

138. (U) The first "formal" production model was turned over to the navy at Dayton for testing on July 4, 1943, and its first test run was on July 23, 1943. Cain and Abel were off the line in the first week of July but were not ready for final testing until the last week of the month. Another complication was the delayed completion of the new building in Washington. Desch did make some minor changes after Engstrom's request. NSA NCML-CSAW Message File, July 6, 1943, July 26,1943, and July 23, 1943, "Status of Bombes."

139. (U) NSA NCML-CSAW Message File, July 26, 1943, Dayton to Washington 'Bombes may not work.'

140. (U) NSA NCML-CSAW Message File, July 29, 1943, Desch to Engstrom, July 29, 1943, "Fast wheel running too hot, bombe may not work."

141. (U) Interview with Philip J. Bochicchio, 6-14-84.

142. ~~(TS)~~ NSA AHA ACC 35173, CNO, CITS TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Navy Dept., Washington, September 1946.

143. (~~TS~~) NSA CCH Series XII Z, Hut 6, 4 October 1942, 'Electronics for Bombe not Working.' ~~(TS)~~ NSA CCH Series XII Z, Engstrom to Desch, September 23, 1942, "Your Bombe plan approved."

144. (~~TS~~) NSA CCH Series XII Z, Joan Murray, "A Personal Contribution to the Bombe Story," *NSA Technical Journa*l, 20 (Fall 1974): 41.

145. ~~(S)~~ NSA CCH Series XII Z, Joseph Desch, "Plan for the American Bombe," September 15, 1942. ~~(TS//SI)~~ NSA CCH Series XII Z (S-2568) "Tentative Brief Descriptions of Cryptanalytic Equipment for Enigma Problems," Circa 1945.

146. ~~(TS//SI)~~ NSA CCH Series XII Z (S-2568) "Tentative Brief Descriptions of Cryptanalytic' Equipment for Enigma Problems," Circa 1945.

147. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944. [*sic*] ~~(S)~~ NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 50-52.

148. ~~(TS//SI)~~ Navy Dept., Office of Chief of Naval Operations, RIP 607, Enigma Series, volume 5., CIT Ts-10-E-5, "Bombe Computations," 5-14. ~~(S)~~ NSA, CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 12, 16. ~~(TS//SI)~~ NSA AHA 16331, "6812th Signal Security Detachment (PROV) Apo 413 Army," 15 June 1945. ~~(TS)~~ NSA, CCH Series II Z, CNO, CITP 88, "Technical and Theoretical Report of N-530 BOMBE," Navy Dept., Washington, D.C., September 1946.

149. ~~(S)~~ NSA CCH Series XII Z, "Cryptanalytic Report #2 The Yellow Machine," 3, 54.

150. ~~(TS)~~ NSA CCH Series.V.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945."

151. (U) NSA NCML-CSAW Message File, November 12, 1943, "85 Bombes in D.C."

152. (U) The first Bombe contract was terminated on December 1, 1943, but some of the first models continued to trickle into Washington as late as Summer 1944. NSA RAM File, History of OP-20-G /NCML/4e, June, 1944, "n530 bombes."

153. (U) NSA NCML-CSAW Message File, November 29, 1943, 'Bombe shipment from Dayton.'

154. (U) H. F. Hinsley, et al., *British Intelligence in the Second World War*,Volume II (New York: Cambridge University Press, 1981), 57-8 and 752.

Andrew Hodges, *Alan Turing: The Enigma* (New York: Simon and Schuster, 1983), 262.

155. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944, [sic] 23.

156. ~~(TS)~~ NSA CCH Series IV.7.20, A. P. Mahon, "The History of Hut Eight, 1939-1945."

157. (U) H. F. Hinsley, et al., *British Intelligence in the Second World War*, Volume II (New York: Cambridge University Press, 1981), 752. NARA RG457, SRH-141, Papers from the Personal Files of Alfred McCormick, Part 2," March 4, 1944, "Memorandum for General Bissel, Army-Navy Agreement Regarding Ultra" Thomas Parrish, *The Ultra Americans: The United States' Role in Breaking the Nazi Code* (New York: Stein & Day, 1987), 79. NSA RAM File, February 21, 1944, W. A. Wright to OP-20-G,"Comparison of Army and Navy Enigma Equipment."

158. ~~(TS)~~ NSA CCH R Collection, Box CCO 66, OP-20-GY-A, "American Cryptanalysis of German Naval Systems," 7 July 1944. ~~(TS//SI)~~ NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol. III, German Cryptographic Systems and Their Solution."

159. ~~(TS)~~ NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946, 9. ~~(S)~~ NSA CCH Series XII Z, 21-2-1944, OP-20-G to British Admiralty Delegation, "U.S. Will Increase Efforts." ~~(TS//SI)~~ NSA CCH Series XII Z, Alexander to Lt. Church, 24 March 1944, "British will emphasize building three-wheel bombes."

160. ~~(TS//SI)~~ NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. ~~(TS//SI)~~ NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953,

161. (U) NSA NCML-CSAW Message File, July 20, 1943, "New procedure, grenade," and August 14, 1943, "Progress on grenade." The grenades were also used on the four-wheel problems when it was thought that one of the wheel settings was known.

162. ~~(TS//SI)~~ NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. ~~(TS//SI)~~ NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953.

163. ~~(TS//SI)~~ NSA CCH Series XII Z (S-2568) "Tentative Brief Descriptions of Cryptanalytic Equipment for Enigma Problems," circa 1945.

164. (U) NSA NCML-CSAW Message File, July 20, 1943, "New procedure, grenade," and August 14, 1943, "Progress on grenade." ~~(C)~~ NSA CCH Series XII Z, Descriptions of NSA Early SPDs and Computers, as compiled from various NSA sources.

165. ~~(TS//SI)~~ NSA CCH "P" Series, Box CCo06, CNO CITS TA-10-E-1, Volume 1, The Click Process, January 1946. She pointed to the use of the message indicators as the "crib," but other cribs could be used by the Grenades.

166. ~~(C)~~ NSA CCH Series XII Z, Descriptions of NSA Early SPDs and Computers, as compiled from various NSA sources.

167. ~~(TS//SI)~~ NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. (TS//SI) NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953.

168. ~~(TS//SI)~~ NSA CCH Series XII Z, 'Le.Roy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953 and various years. ~~(TS//SI)~~ NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953.

169. ~~(C)~~ NSA CCN Series XII Z, Descriptions of NSA Early SPDs and Computers, as compiled from various NSA sources.

170. ~~(TS//SI)~~ NSA CC' Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953 and various years. ~~(TS//SI)~~ NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953.

171. ~~(TS)~~ (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March 1945.

172. ~~(TS)~~ (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March 1945. "A Time of Triumph."

173. (U) NSA RAM File, CNO, U.S. Naval Communications, "Brief Descriptions of RAM Equipment," Washington, D.C., October 1947. NSA RAM File, Report of R. I. Meader, Captain USNR to J. H. Wenger, Captain, USN, "14 Days Training Duty, Report of," January 21, 1949.

174. (U) NSA RAM File, CNO, U, S, Naval Communications, CITP TP-33 "Overhaul of Hypo #1," Washington, D.C., June 1945.

This page intentionally left blank

Chapter 5

(U) A Search for Other "Bombes"

(U) The arrival of the United States Navy's Bombes in Washington in autumn 1943 allowed OP-20-GM to turn its attention to Japan. It also gave some of its men time to think of advancing beyond electromechanics. But the tenuous control over the Enigma systems and the challenges of the very stubborn Japanese codes and ciphers meant that electromechanics and the Bombes continued to demand much of the energies of the Americans.

(U) OP-20-GM explored many electronic and photo-optical possibilities during the last two years of the war as it attempted to conquer Japan's systems, and as it responded to Britain's cries for help to fight changes in Germany's codes and ciphers. In a few instances "M" was able to go beyond the technology of the Bombes, but in most cases it had to relegate electronics and advanced film-based processing to small exploratory projects. Only when there was a combination of an inescapable demand for ultra-high speeds and a possibility of coaxing electronics into behaving would "G" allow its engineers to try to turn their electronic dreams into hardware.

(U) The army's SIS also had to drop its ambitious early plans for advanced electronic devices. Like the navy's cryptanalysts, its men had to turn to quick and rather clumsy solutions during the first years of the war.

(U) Meanwhile, the Army

(U) In late 1942, while OP-20-G's cryptanalysts were establishing their place in European communications intelligence, the American army's codebreakers struggled to gain just a foothold. Unlike the navy, the army was not involved in European-related action until well after the outbreak of the war. It had a more difficult time than the navy in intercepting enemy messages, and the British were much less in need of its cooperation.[1]

(~~TS//SI~~) The British had begun to share their knowledge of German and Italian diplomatic traffic before the war, but they were more than reluctant to allow the American army a role in the German army and air force systems.[2] At first, the Signal Corps and the SIS were not worried about their inability to read the German military traffic. Just before Pearl Harbor they indicated they were not interested in working on the army and air force problems. But when troops were committed to North Africa, attitudes changed dramatically. The Americans realized the shortcomings of depending on intelligence supplied by another nation. The SIS wanted its own control over Enigma, but it had few capabilities.[3]

(U) Founded to replace Herbert Yardley's infamous Black Chamber in the late 1920s, the army's Signal Intelligence Service (SIS) began with what Joseph Wenger yearned for, a core of young and talented civilian mathematicians. Under William F. Friedman they became respected for their use of statistical methods.[4] Much of their time and expertise was devoted to creating codes and ciphers for the army. But they devoted an increasing amount of effort to operational cryptanalysis.

(U) Although separate from OP-20-G, the SIS had a gentlemen's agreement about cryptanalytic turf. Friedman's group agreed to focus on enemy army systems but to share a rather ill-defined zone of diplomatic and clandestine traffic with "G." The Coast Guard's cryptanalytic office, led by Friedman's wife, and the FBI's codebreaking

group shared in tapping the diplomatic and clandestine traffic in the Americas. Like OP-20-G's crew during the 1930s, the SIS's men were directed to concentrate on Japan's secret systems but not given the resources to fulfill the charge.

(U) The difficulty of intercepting enough military messages extended to the SIS's attack on Japan's army systems. Unlike the use of high-powered radio by the navies, the armies and air forces of the world used low-power systems and sent relatively few messages that could be intercepted from a great distance. Even after the SIS constructed listening posts in the Pacific and the Canal Zone,[5] it could not acquire military messages in enough "depth" for code or cipher breaking.[6]

(U) As a result, Friedman's talented men and women spent much of their time during the 1930s on diplomatic communications. After months of intense work, in 1940 they laid the foundation for America's Magic by successfully attacking Japan's new Purple enciphering machine system. It carried Japan's most important diplomatic messages to and from the world capitals. Although Friedman's group received help from the navy in attacking Purple, Magic was seen as an SIS triumph by the nation's leadership.

(U) Friedman's group had employed modern as well as traditional cryptanalytic techniques against Purple. A few years after OP-20-G began to use tabulating machines, the SIS established its first automation foothold.[7] Although it did not begin an OP-20-G-like Rapid Machine project before the war, the SIS hired a newly minted MIT electrical engineer at a critical stage in the Japanese diplomatic problem. That graduate of MIT's electrical engineering department, Leo Rosen, helped break into the Japanese diplomatic machine and constructed its first analog.[8]

(U) Although William F. Friedman's group had ideas for teletype-tape comparators, isomorph machines, and relay attachments for tabulators, it did not have the resources to turn them into hardware. It did not go beyond building direct analogs of enemy machines.

(U) The Search for Another American Ultra

(U) When war broke out, the SIS had little cryptanalytic capability, few intercepts, and little machinery. It had no Enigma proficiency, it was unable to read the major Japanese or German military codes, and it had few messages or machines with which to analyze them. In fact, it appeared that it would be some time before the SIS would have much to work on.

(U) It did get one assignment but through default. "G" was overworked because of its efforts against critical German and Japanese naval systems. Out of necessity, it turned all of the Japanese diplomatic problem over to the SIS.[9] That Purple diplomatic challenge took much of the army's attention in the first year of the war, although the system had already been solved. Purple had become a relatively easy system to exploit. It needed a few new electromechanical analogs, but it demanded little else. Even Britain cooperated. It sent intercepts and cryptanalytic advice to Friedman's Japanese experts. The attention was well rewarded. Much was learned about Germany, as well as Japan, from the radio and cable messages to and from Japan's embassies in Axis and neutral nations.

(U) The German problems were very different. Its diplomatic systems proved difficult to enter, and its military codes and ciphers resisted attack. As important, the British, who held many secrets to entering Enigma and other German ciphers, did not wish to grant the SIS power over Germany's army or air force systems.

(U) The SIS badly needed Britain's help. It began World War II with as little, perhaps less, potential to enter German systems as OP-20-G. When the SIS finally decided to establish an Enigma program and demanded to become a

partner in Ultra, it found that it had little to negotiate with. Its main bargaining chips, Purple and Magic, had been given away in early 1941.[10]

(U) The SIS had a much more difficult time than OP-20-G in gaining GC&CS's trust. Throughout the war the SIS men felt they had to fight much harder than the navy for British concessions on Ultra.[11] They worried that the British promises of full cooperation that had been made as early as the autumn of 1940 might never be kept. In a way, their fears were correct. GC&CS never granted the United States Army's cryptanalysts as much independence as it did the navy's men.

(U) And while playing a tug-of-war with Britain to gain knowledge of the German ciphers, the SIS was tormented by the Japanese army code problem. It was not until the spring of 1943 that the SIS centers in Washington and Australia were able to tap a major army system.[12] Perhaps it was the need to devote its energies to the Japanese codes, and a belief that traditional methods were the only alternative for such problems, that led the SIS to be much later than the navy in establishing a formal group to develop rapid machines for statistical and mathematical cryptanalysis.

(U) Its delayed start led the SIS to rely on the navy to supply most of its initial RAM equipment. But it then launched perhaps an overly ambitious attempt to create a very advanced RAM, one that, it was hoped, would leap-frog the navy's technology.

(U) A Great Electronic Adventure, the Freak

~~(TS//SI)~~ Like the ex-MIT engineers at OP-20-G, some of the SIS's technicians had great faith in advanced electronics. Their first dream at the outbreak of the war was for a new type of machine to perform one of the most tedious but important general cryptanalytic functions, frequency counting. Their goal was to create a relatively small and super-fast machine to count and record all simple and digraphic frequencies. The machine was to do that in one pass through a message. Tabulators, because they had so few counters, demanded much sorting and many card runs to complete a full count. Many of the standard tabulator frequency-counting procedures used in the attacks against Purple, Hagelin and, later, some teletype systems took sixty to ninety hours.[13]

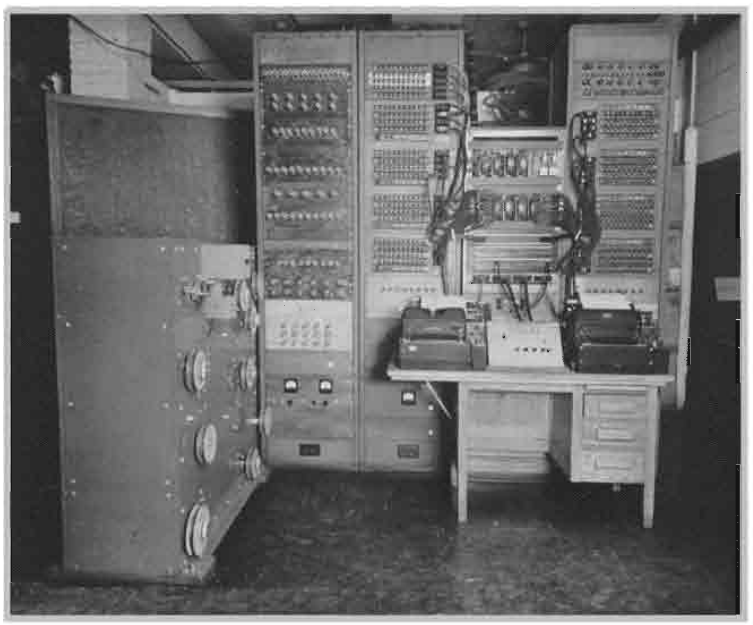
(U) To go beyond the "tabs" for such complex counting was a challenge. For one thing, it called for the creation of a new type of memory. Readily available technological options, such as using industrial counters to store results, meant accepting slow processing and a machine that would be the size of a room.[14]

~~(TS//SI)~~ In mid-1942 Leo Rosen decided to take up that challenge. Recently put in charge of a group of engineers, he decided to establish an SIS RAM program. He thought that it should begin with fundamental contributions. He was determined to develop a large high-speed electronic memory. In addition, he told his men to create electronic circuits that could perform analytic

(U) Leo Rosen

functions, such as a sigmage test, that were an integral part of all the frequency-based crypto-attacks.[15] Together, he hoped they would provide the basis for the high-speed counting machine, Freak, a device that OP-20-G seemed unwilling to produce.

~~(TS//SI)~~ Unfortunately, Rosen picked a much too ambitious goal for the army's first RAM adventure. It took a year and a half before Freak I emerged from the SIS workshop; then, it proved too delicate for operational work.



(U) Freak

~~(TS//SI)~~ Freak's design and components were major advances in the technology of calculation. Rosen's group had decided to use more than 7,000 condensers for the machine's mass "memory." One thousand twenty-four sets of seven condensers each were the "counters" in Freak.[16] By using the binary counting system, every set could hold a count of up to ninety-nine. The enormous number of condensers accounted for much of the size of Freak I. The machine was nine feet high by eight feet long.[17]

~~(TS//SI)~~ There were great hopes that Freak would speed all types of counting and analysis. As the data were read in from two tape readers and processed through a relay system, the appropriate counters were incremented. Then the advanced electronic digital circuits calculated running frequencies and the critical SUM (N(N1)/2). The circuits also scanned the counters and controlled an electromatic typewriter which printed the results.

~~(S//SI)~~ The use of the binary system, the memory technology, and the digital calculations were advanced for the time.[18] Freak I, unfortunately, did not have a long or useful life. The counters proved unreliable, and the electronic circuitry was troublesome. The machine was so uncooperative that it was dismantled in mid-1944, just six months after its birth.[19]

~~(TS)~~ The defeat on the first Freak tempered the SIS's faith in electronics, but its engineers decided to try again. They constructed a second version that began twenty operations in spring 1945. It proved more reliable than its predecessor.[20]

(U) Tabulators and Traffic: A Data Processing War

(U) Despite the affection for electronics, the SIS placed its faith in older technologies during the first critical months of the war. The SIS made an agreement with IBM and soon had scores of tabulating machines. Many IBM engineers were

sent to Washington to make significant modifications to the tabs and sorters, and IBM's factories were kept busy producing special devices. By the end of war, the SIS had close to 400 IBM machines using a million IBM cards a day.

(~~TS//SI~~) The workforce for the machines grew from fewer than 100 at the end of 1942 to 600 a year later. By the end of the war the SIS's tab rooms had close to 1,200 workers.[21]

(~~TS//SI~~) As the SIS waited for intercepts from the Japanese military systems and hoped for information from the British on the Enigma, they did their best to produce intelligence from the few sources besides Purple that were available to the agency.[22]

(~~TS//SI~~) One of those sources was the intercepts of diplomatic messages sent on Germany's GEC system. The army's radio men had been collecting them on their own for some time, as well as receiving information on them from the British. But collecting was easier than solving the system. The GEC codes were tough. The Germans used code words doubly enciphered with additives.

(~~TS//SI~~) The tabulator group at SIS began an attack on the system using labor-intensive techniques similar to those the navy had developed to breach the Japanese navy's additive systems. The going was difficult, however. The usual attacks did not seem to work. The Germans had a very clever keyword system for specifying the additives that proved difficult for the Americans to penetrate during their first year of IBM attacks. Fortunately, the British had acquired some pages of additives from a French agent and decided to pass them to the Americans in early 1942.

(~~TS//SI~~) With the hints about the system, the Americans launched their first new tabulator attack of the war. Their work on GEC led them to develop machine methods, such as the search for double repeats, that were transferred to the Japanese military problems once a flow of intercepts began.[23]

(~~TS//SI~~) But the SIS had to wait quite some time before the army could supply enough Japanese material. Then the SIS cryptanalysts found that Japan's military had, perhaps unwittingly, been wiser than its diplomats. Japan's diplomats had made a mistake by basing their secret communications system on a machine. By turning to the latest technology, they had made their ciphers more vulnerable than if they had used, for example, crude one-time pads.

(~~TS//SI~~) In contrast, the Japanese military had decided to stay with older methods. In doing so, they frustrated the British and American codebreakers and forced them to turn to very "data heavy" methods. The Japanese army's code-with-additive systems were vulnerable to capture, but neither the Americans nor the British acquired any significant amounts of material during the first years of the war.

(~~TS//SI~~) A cryptanalytic attack without captures, or quite evident "busts," demanded enormous numbers of intercepts, analysts, and machines. It meant that the SIS had to engage in a frustrating data processing war.

(~~TS//SI~~) Despite the allocation of massive amounts of resources to the problem, the Japanese army's systems resisted longer than its navy's. The difficulty of intercepting its messages, its use of complex additive systems, and its clever ways of hiding the information contained in the message preambles led to a near cryptanalytic blackout during 1942 and 1943.

(~~TS//SI~~) The inability of the Allies to read the major army systems through cryptanalysis led the SIS to rely upon traffic analysis; as a consequence, IBM tabulators and methods quite like those in business data processing became essential to its operations.[24] Throughout the war hundreds of machines and people were kept busy

sorting, counting, and listing frequencies of communications among units. Even when some of the major army systems had been penetrated, 20 percent of the total machine hours in SIS were devoted just to the analysis of the message headings.

(~~TS//SI~~) Keypunching and the physical maintenance of card files for the traffic analysis processing were demanding by themselves. Recording and analyzing 300,000 messages a month for traffic analysis was not uncommon. Huge decks of cards had to be carefully loaded into the tabs and sorters for the first of the many steps in each analysis routine, then reloaded several times to complete a process. The pressures all that created were so great that the SIS Machine Branch had to endure a critical personnel problem: after several weeks of training, machine operators quit. The young civilian women were apologetic, but insisted they be allowed to leave. The night shifts were especially difficult to staff, and it was only the arrival of WACS, who were allowed to live on base and who were unable to resign, that allowed the machine room to continue its twenty-four-hour work day.[25]

(U) Making the Tabs More Powerful

(~~TS~~) The IBM tabulators remained the foundation of the SIS's operation and for more than traffic analysis. The continued dependency on the tabs was reflected in the intense efforts the SIS made to increase their power. By the end of the war, the Arlington Hall engineers had helped to develop an impressive array of specialized IBM equipment as well as a whole series of complex relay attachments.[26]

(~~TS//SI~~) Modified "tabs" were the technology for the SIS's work on Japanese code problems. Some twenty-three different relay attachments were used to attack Japanese army systems. In many instances, the attachments were so powerful that the "tabs" were relegated to being mere input-output devices serving the relay cabinets.

(~~TS//SI~~) The complex relay circuits placed on the tabs automatically stripped additives, applied possible encryption squares, and even searched to see if the results of additive removal had led to the appearance of high-frequency code groups. The more complex attachments received names, such as Brute Force, Camel, JMA, the Selective Square, or the Limited Selector.

(~~TS//SI~~) The modifications that automatically decoded upwards of 2,500 messages a day were of special pride to the SIS's machine branch. They allowed the timely exploitation of the captures of cipher text and key that began to flow into Arlington Hall during 1944.[27]

(~~TS//SI~~) One of the most impressive of the SIS's tabulator modifications was the Slide Run machine. Its origins illustrate why most of America's codebreaking history is so unlike the thrilling story of MAGIC, when a brilliant insight supposedly led to a near instant victory over a major communications system.[28]

(U) Slides, Runs, and Endless Decks of Cards

(~~TS//SI~~) The mature Slide Run machine of mid-1944 was a combination of a 405 Tabulator and a huge chest-high, multipanel cabinet full of advanced relay circuits, telephone crossbar relays, counters, and plugboards. But the Slide Run did not begin as an elegant example of IBM's best work. The first two of the devices were hurriedly built by the "F" Branch in late 1943 as an emergency response to the requests of the cryptanalysts. The "cryppies" thought they might have found the techniques and some of the additive keys needed to attack the Japanese army systems.

(~~TS//SI~~) Although hastily built to exploit a particular opportunity, the machines proved so valuable that a development and production contract was signed with IBM. The new Slide Runs were to be used on a variety of problems. By early 1944, IBM was constructing six more Slide Run

machines, each more sophisticated than its predecessor. [29]

~~(TS//SI)~~ The Slide Run machines were badly needed because of the continuing difficulties with Japanese army systems. The Japanese army problem was very difficult and all attacks were extremely labor intensive. Hundreds of cryptanalysts at SIS had been working since the beginning of the war to discover the numeric additives and the codegroup meanings. The tabulators had been called upon to process files of as many as 3,000,000 cards.

~~(TS//SI)~~ Copperhead-like brute force searches, keyword searches, and repetitive additive stripping and testing kept machine-room double shifts busy for months. Despite all the effort, there was little more than frustration until April 1943 when the Japanese army's indicator system was broken. That allowed the identification of the enciphering squares that were used in the indicators. With that breakthrough, it was possible to identify messages that were enciphered using the same additive pages. With knowledge of the pages, an attempt could be made to place messages on overlaps by tabulator-based, brute-force searches.

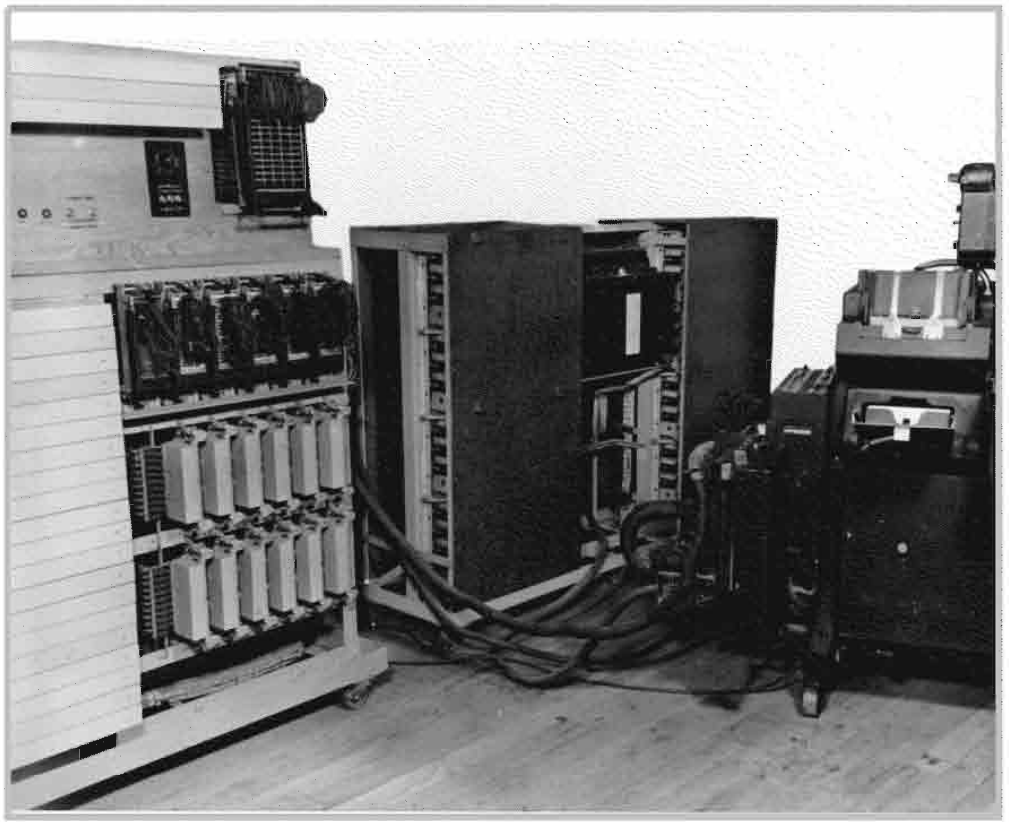
~~(TS//SI)~~ At first the search for the repeat of the same cipher groups at the same intervals in two messages (brute force) had to be done through the tedious repetition of card duplication and endless sorting.The most efficient attacks still demanded files of almost 200,000 IBM cards. All that processing was tolerated just to try to find messages that had a probability of being enciphered with the same set of additives. The job became too much, even for the SIS's hundreds of tabulators and sorters. A way to automate the process had to be found.

~~(TS//SI)~~ In response to the need, a relay attachment was built for the brute-force search; but the Japanese army attack continued to demand round after round of card punching, reproduction, collating, sorting, addition, subtraction, multiplication, and printing. For example, one procedure developed in the summer of 1943 hoped to recover additives by using four copies of a file of 430,000 cards. The files were run three shifts a day until the end of the year.

~~(TS//SI)~~ By fall 1943 the many tabulator attacks and an increasing number of captures of Japanese material allowed the accumulation of a file of additives. The next logical steps were to try to locate the messages that used particular additives and to strip the additives to reveal clear numeric codes. From there, the cryptanalyst could recover more code meanings and decipher more messages.

~~(TS//SI)~~ The automation of the process came gradually. At first, the "slide run" procedure was just a new way to use the existing tabs. It was developed to replace the old hand methods of applying a known additive to a length of code, then testing to see if a sensible result emerged. If an unlikely group appeared after the additive had been removed, the additive was tried against the next offset of the text. If a juxtaposition of additive and cipher yielded a likely result, it was tested against a file of frequently used code groups. When a match occurred, the cryptanalysts concluded that it was probable that the additive they were trying might have been used to encipher the current message.

~~(TS//SI)~~ The "slide" was a common sense but powerful technique. But even when it was implemented in IBM methods, it stretched human as well as machine resources. When regular tabulator equipment was used, the routine was quite complex. A series of five likely keys (additives) was punched on cards so that they could be tested against all possible positions in thousands of messages. When the key produced, in two of the five tested positions, code groups found among the already known most frequent 250, the tabulator printed the message number and the five code groups.



(~~TS//SI~~) Slide Run

(~~TS//SI~~) What came to be called the Slide Run machine was developed to reduce the size and number of required card files and to speed the "slide" testing process. The first step towards the eventually very sophisticated device was the invention of a code-recognition component. To further automate the process and to reduce the number of cards that had to be handled, a conversion unit was constructed. Its relay circuits stripped the additives to produce the code sent to the recognition unit.

(~~TS//SI~~) In the Slide Run machine, banks of relays were wired to hold as many as 250 code groups; later versions held as many as 1,500. The recognition unit tested each stripped group coming from the tabulator's arithmetic section to see if it completed any of the code circuits. If it did, the machine recorded a "hit."[30]

(~~TS//SI~~) More and more "intelligence" was built into the Slide Run machines. New models appeared which included sensitive and labor-saving statistical threshold tests. They prevented the printing of unprofitable reports. The first of the postwar versions went further. It used a log-weighting method to reduce the number of "prints."[31]

(~~TS//SI~~) The Slide Runs were of great value to SIS, but they were not exceptionally fast nor easily "programmed." The best of the World War II versions read cards at a rate of 150 a minute, and it took from three to five days of work to set the

codes in the recognition units. Then it took hours to run the cards for a series of messages.[32]

(~~TS//SI~~) The impossibility of increasing the rate of card-sensing much beyond what had been accomplished by 1944 is what led the SIS, in June 1945, to make a request for a RAM 70mm film version of the three "tab" machines that had proven so useful against the Japanese systems: the Slide Run, the Isomorph, and the Brute Force machines. Unfortunately for the men within Leo Rosen's section who, as we will see, became the torchbearers for Bush's ideas, the army decided the Eastman designs should not be funded.[33]

(U) The Other Bombe Program

(U) Well before any progress had been made on the Japanese military problems, the SIS decided that it had to gain a share of the European Ultra. And like the navy, it wanted control over its own intelligence resources. But it was ill prepared in terms of skills, equipment, or political power

(~~TS//SI~~) The SIS did not begin its Enigma battle technologically prepared, nor did it have any plans for advanced anti-Enigma machines. At the beginning of the war, the SIS's men were told of OP-20-G's RAM contracts with Eastman and Gray. As a result, Rosen and Friedman became interested in the possibilities of microfilm-based machines, and they agreed to at least examine their possibilities. Soon, they heard a few things about the navy's Bombe ambitions.[34]

(~~TS//SI~~) But during the first months of 1942 the SIS focused on expanding its tabulator section; it was not until late in the year that it decided to create a machine research group that had the manpower needed to examine, let alone create, new technologies. The MIT graduate, Leo Rosen, was placed at the head of a small team that began its work in the basement of an old house at Arlington Hall Station.[35] One of his first actions was to advise his superiors that the SIS should join in the RAM program. He convinced the army to purchase almost $200,000 worth of copies of the OP-20-G-sponsored machines from Eastman and Gray.[36] The army gave the Bureau of Ships the funds needed to purchase machines similar to Tessie, the IC machines, and, later, a Gray-NCR Comparator. Letterwriters were also supplied by the navy. As within "G," they became an essential part of SIS's data processing services.

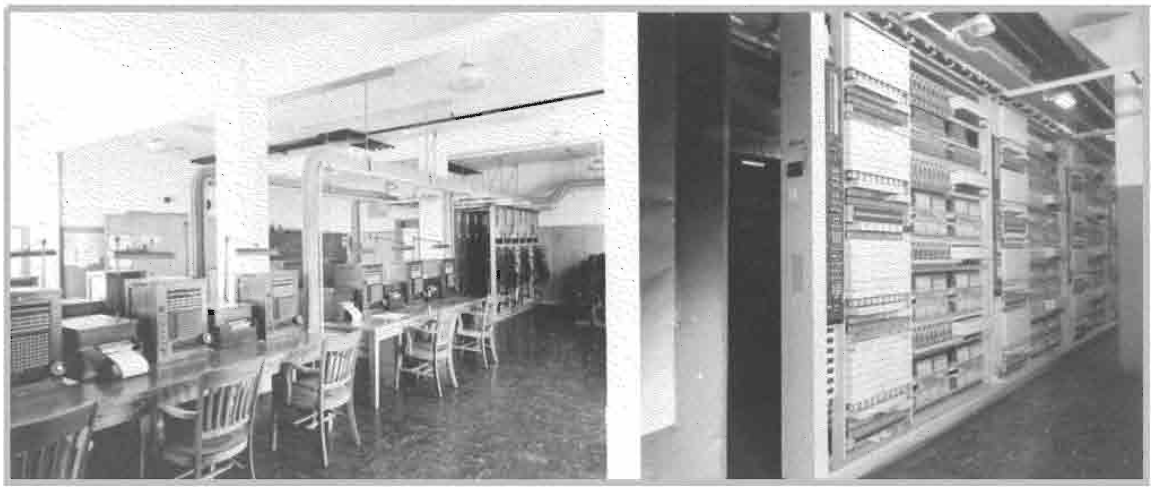
(U) Another Step Back

(~~TS//SI~~) Rosen's major assignment, however, was to produce a machine to give SIS the kind of power the army thought OP-20-G was gaining over GC&CS through its emerging Bombe program. By summer 1942 he gained approval for an SIS Bombe program. He began to assemble a force of enlisted engineers and technicians but soon realized that the army would be unable to build or even design a Bombe by itself.[38] His staff remained too small through 1942, and he had to confine its work to preliminary investigations and minimal construction projects.

(U) One of the first of its preliminary studies was on the possibility of a new type of Bombe for the army and air force Enigma problems; that turned out to be a major task. Soon Rosen thought enough had been learned to allow a commitment. In October 1942 the SIS decided it had to have its own version of a Bombe, and it was to be acquired independently of Britain and OP-20-G.[39]

(~~S~~) Rosen's "F" team explored an electronic Enigma while Friedman made the rounds of the scientists associated with the NDRC's fire control computers.[40] Rosen's electronic option would be put aside for the same reasons OP-20-G had dropped electronics during the summer. But the SIS's hope for a tube-based solution lasted a bit longer.[41]

(~~TS//SI~~) Belief in the potential of electronics led to Rosen's team hiring experts from the telephone company. They worked on an electronic



(~~TS//SI~~) Madame X

Bombe until December 1943. Then frustration with the disappointing results led to an end of the contract. However, SIS's faith bounced back, and it began the hunt for another high-speed rotor after its "E" crisis had passed.[42]

(U) While Rosen and the Western Electric experts explored electronics, one of the alternatives recommended by the NDRC's researchers was approved. What became known as Madame X followed the general logic of the Turing attack on the Enigma, but it was significantly different from the British and the OP-20-G Bombes. The machine first appeared as a breadboard demonstration unit in early 1943, passed its first tests that summer, and was available as an operational model in October 1943.[43]

~~(S//SI)~~ Madame X (also called "003") was huge. It was so large because the SIS had decided to be more elegant and innovative than the navy. It wanted one grand Enigma-fighting machine, 300 uncoordinated ones. Although it did not meet all its original goals, the "003" was an impressive machine.[44] It contained 144 Enigma scrambler units, as compared to the sixteen in the standard OP-20-G Bombe. "003's" banks could be divided into different size groups so that as many as twelve useful menus could be run at one time.[45] The army cryptanalysts knew that the longer a crib and its chains, the fewer the false hits. A large number of units linked through a flexible central control system would allow several shorter cribs to be run simultaneously.[46]

(~~TS//SI~~) The "003" was designed for more than simultaneous runs, however. It was intended to be easier to use than the navy Bombe and to have a much faster setup time. Some of those goals were achieved. When the "003" was completed, the army's technicians sat in a "turret" room and set plugs and switches on small control boards rather than having to place dozens of commutators on the machine as the navy's operators had to.

~~(TS//SI)~~ The "turret" system was quite innovative. There were a dozen of the switching stations in the room. Each "turret" was a small version of a telephone switchboard with an addition, a set of push buttons. Each board could control its own part of the "003" if simultaneous runs were desired. Such simultaneous use seems to have been the norm once the SIS learned that well-selected short menus could be powerful. Strong menus sent from England allowed the use of only a few of the "E" units (perhaps fourteen) per test. Typically, some ten problems were run at one

time. On its best days, "003" completed 1,200 of the short three-wheel runs."[47]

(~~TS//SI~~) The switchboards were used to select which subset of the frames were to be active during a run. The push buttons were truly a unique and potentially valuable feature. Through them wheel orders could be changed in one-half a second. That allowed wheel orders to be tested in rapid succession. Unfortunately, the other parts of the setup, including the menu, had to be done by hand on the individual Enigma frames. That led to the setup time for the "003" being much more than hoped for – some twenty minutes for a test when more than wheel orders had to be changed. At peak efficiency, a crew could place and run twelve new menus a day.[48]

(U) A very innovative and important feature of the "003" was its ability to automatically control the stepping motion of its "wheel" analog. The relay circuits allowed the machine to use "non-metric" motion.[49]

(U) More to It Than the Madame

(~~S~~) Like the navy's Bombe, Madame X could not work alone. Before it could be efficiently used, the SIS had to have cribs and a list of what wheel orders would not have to be tested. Then, after a "hit" was found, the SIS had to do as much or more hand-testing than the navy. Several machines to speed the hand work were built. They performed the same type of functions as the navy's M8 and M9.

(~~TS/SI~~) The army needed a special aid to help "003" because of what might be called a design oversight in late 1942. The design of Madame X had begun before the SIS knew all about the British Enigma attacks and before it had enough experience to realize how necessary it was to have machines that eliminated all but a very, very few possible keys and settings. Thus, the original Madame X did not have a full "diagonal board" test built into it.

(~~TS//SI~~) SIS's men thought their bombe would be useful even though its list of "stops" would not be filtered by a thorough test for stecker inconsistencies as was found on the British Jumbo Bombe. As a result, they thought that a celluloid grille would be sufficient to search for "contradictions."

(~~TS//SI~~) That was incorrect. That hand "diagonal board" test proved so time-consuming that the first of the SIS's versions of grenades was constructed.[50] But as more was learned about the navy's and GC&CS's machines, Rosen's team decided to build an attachment that would automate the entire consistency-checking process.[51]

(~~TS//SI~~) The American Machine Gun had its first tests in September 1943, a month before the second half of "003" was completed. Built of the same technology as its host, the Machine Gun searched for stecker inconsistencies and suppressed all the "stops" that were logically impossible given the nature of the Enigma plugboard. The "Gun" speeded SIS's work but caused some discomfort for those assigned to "003's" rooms. It was a very noisy device, as was what had inspired it, Britain's older grenade.[52]

(~~S~~) Some other special devices were attached to the original "003." Like many of the navy's grenades, the army's add-ons took advantage, whenever possible, of German procedural errors. But some of the attachments and alterations were designed to apply new general cryptanalytic knowledge to speed "003" processing.[53]

(~~TS//SI~~) Many of the ideas for the new attachments came from the British, who were creating similar devices for their Bombes. Their CSKO switch, for example, had been very helpful. Once on "003," it helped exploit a German air force procedural rule forbidding linking any checkerboard letter to its neighbor. For example, B could not be checkered to A or C. The Consecutive Stecker Knockout circuits checked for such illegal

connections and prevented a "stop" from being indicated.[54]

~~(TS//SI)~~ Madame X was given another helpful attachment, the Double Input. It was an application of more sophisticated knowledge of the probability aspects of cribbing. This allowed two relatively weak menus to be run simultaneously and to approach the power of the usual sixteen-letter menu with "closure" on the crib-plain combinations.[55]

~~(TS//SI)~~ Alterations to "003" allowed it to drag cribs so that it could run Swiss and Spanish Enigma problems. And the Clambake attachments were for short runs for "grenade cribs." The "003" was allowed to perform more flexible tests by using the Oyster Schuker attachment. In addition, methods to exploit Cillys were developed, and "003" was, at times, rewired to handle special Enigma reflector runs.[56]

~~(S)~~ There were several attempts to make Madame X more powerful; some were very successful. A difficult goal was to expand the powers of "003" by lessening its dependency on cribs. The first appearance of the idea for a probability-based way to find wheel settings, as well as to deal with garbled cipher, emerged before "003" was completed.[57] Taking similar British methods into consideration,[58] the SIS cryptanalysts and engineers decided to use thirty-six of "003's" own "M" frames to test for the frequency of appearance of the sixteen most unlikely letters within a fifty-two letter test decipherment. Just the cipher text was entered. If fewer than nineteen of the fifty-two letters that resulted from a deciphering at a particular starting point were on the high frequency list, a "stop" was printed.[59]

~~(TS//SI)~~ Unfortunately, such use of "003's" regular frames led to the machine being monopolized by special tests. One of the worst of them was "dudbusting." Duds were messages that should have been readable given knowledge of their keys, but were not. They were usually the result of operator errors such as the use of an incorrect key on a system.

~~(TS//SI)~~ Because dudbusting was one of the more important tasks assigned to the "003," and because the job took so long, a decision was made to create a new dudbuster with its own "frame," and, perhaps, a bank of electronic counters.[60] The electronics proved a bit too much for an emergency situation, but a more efficient and quite impressive electromechanical (relay) Arlington Dudbuster became an essential part of the SIS's machine rooms. The Dudbuster worked on the principle of recognizing plain language through a simple frequency test. Based on the characteristics of the German language, including the absence of "X," each plain letter was assigned a weight. If the summed weights equaled a threshold value, text was printed, then examined, to see if true German was a result of the wheel settings.[61]

~~(TS//SI)~~ There was also a film RAM version of the SIS statistical Dudbuster. Its birth led to some friction between SIS and OP-20-G. Independently of OP-20-G, the SIS cryptanalysts conceived of their own film Hypo. When they informed OP-20G of their great discovery in mid-1943, "G's" men became quite embarrassed. They were forced to admit that they had thought of the Hypo method earlier, had a machine in development, but had not informed either the SIS or GC&CS.

~~(TS//SI)~~ Despite some help from the navy, it took a long time for the SIS to turn their Hypo dudbuster idea into hardware. It was not until late 1944 that a special camera was linked to an "M" frame to generate the images of the distribution of high frequency letters from each Enigma setting. Those master films were then run, as in Hypo, against cipher text to find the point of greatest coincidence.[62]

~~(TS//SI)~~ The film dudbuster and Hypo were often called "Grenades." Their success led the SIS

to explore the possibilities for more ambitious film attachments and supplements for "003." Unfortunately, some of the most ambitious Grenade ideas could not be implemented. The high-speed Azalea and Bachelor attachments were never completed, and the plans for a super-speed film cribdragger probably did not turn into a project.[63] It is certain, however, that neither the army nor navy ever built a Grenade that matched the grand achievement of the British in late 1943, its electromechanical Fillibuster. It tested four cribs on eighty messages simultaneously.[64]

(~~TS//SI~~) The alterations to Madame X did make it more efficient, but the American army's Bombe continued to make many demands on the SIS. Its manpower requirements were not as great as the navy's Bombe, but it was a labor-intensive machine. It needed more than twenty operating personnel and forty maintenance men.

(~~TS~~) Despite the large maintenance crew, the machine had a bit of a tendency to lose its concentration. During its first few months, all runs were duplicated on a second control board. And well into 1944 it could not be coaxed into running at the originally hoped-for speed. It had been designed to run, if desired, at sixty pulses a second for short periods, but its typical operating speed was half that, thirty pulses per second.[65]

(U) Thus, despite its great flexibility, "003" was not a perfect solution. Its successes certainly did not change the navy's mind about Bombe architecture. When OP-20-G decided to build a second set of fifty machines, it found Desch's commutator design much faster and more efficient than a relay-based machine.[66]

(U) "003" could not be switched to a four-wheel mode, and twenty-six separate runs had to be done to test a four-wheel message. As objectionable to the navy's engineers was "003's" slow operating speed. The automatic control system in Madame X did not fully compensate for its long run times.

(U) The "003" had another feature that did not prove as powerful as hoped. The army machine had the circuits necessary for the "locator" task done separately by the navy's Hypo machine, but the navy's engineer-cryptanalysts did not find "003's" automatic locator that attractive.

(~~TS~~) Near the end of the war, Joseph Wenger requested another comparison of the army and navy "E" machines. Wenger decided that the OP-20-G Bombe complex was, on average, fifty times more productive than the army's machine in Arlington.[67]

(~~TS//SI~~) The main reason why only one "003" was built was the SIS's inability to convince the British to yield the messages and techniques needed to keep the machine busy.

(U) A Machine Looking for Work

(~~TS//SI~~) Madame X's construction began just as GC&CS and the American army reached a low point in their relationship. Britain's refusal to inform the SIS about anti-Enigma methods led to an impasse. The situation became quite tense. The Americans, for example, refused to let Alan Turing see their new voice scrambler system until Britain yielded her secrets. For a time, SIS even withheld what it was discovering about Japanese systems.

(~~TS//SI~~) Friedman's group certainly must have resented Britain's request that it build a super-Bombe for GC&CS while she would not share her cryptanalytic secrets. There must have been complaints about being asked to construct advanced machines to attack the Fish system's Geheimschrieber yet not being allowed to have the desired intercepts and cryptanalytic information on Enigma.[68]

(~~TS//SI~~) The tensions were reduced in May 1943 after a series of conferences, but there was no immediate flow of cryptanalytic secrets to

America, nor was there enough high-priority work assigned to Madame X. The result was that it seemed to be an expensive machine without a purpose. Then, when it was finally put to work, it served as a secondary aid to GC&CS.

~~(TS//SI)~~ The SIS had not expected such a minor role for their great computer. Its best cryptanalysts had spent much of 1942 and 1943 trying to develop their own "E" attacks, using up 1,000 hours of "003" time. But after all that effort they had to admit defeat and had to yield to England's monopoly of methods and its control of intercepts. The home grown "Yellow" project for which "003" was built became a subunit of Bletchley and, to make matters worse, most of the SIS's involvement with "E" came through the team of men it sent to England in late 1943. Americans were as busy running British Bombes in a small town near Bletchley as they were running Madame X in America. Perhaps as depressing for Rosen and his group, England was probably sending as many German air force jobs to OP-20-G as it was sending to Arlington Hall.[69] As a result, Madame X stood idle much of the time. For many days it had to be assigned only to "research problems."

~~(TS)~~ Such disappointments with the SIS Bombe program were perhaps what forced Friedman to write a very defensive report about Madame X in early 1944. He tried his best to show that Madame X was superior to all the other anti- "E" devices. He hammered at every weakness of the commutator Bombes, British as well as American. They were susceptible to mechanical stress, they were not good at solving "duds," and they took much too long to record the "hits," he said. He continued by citing "003's" need for fewer maintenance personnel and by stating that the British Bombes took twice as long as "003" to run an entire problem.

~~(TS)~~ But he could not hide the deficiencies of Madame X. He admitted that at the very least, the "003" was five times as expensive as the British Bombes and that it was really slower than the American navy's machines. He tried to conclude his report on an upbeat note, but his final statement helps explain why Madame X was torn down at the conclusion of the war:[70] "It is thought fair to state that, for purely operational purposes, the rotary type of bombe is the most efficient but for research and development of new solution methods, the relay type, because of its greater flexibility, is far superior." Madame X did win some victories, however. As an engineering project and as an example of America's mass production capabilities, it captured the respect of the British engineers. It also served as a backup system for GC&CS. It was kept busy from 1944 to the end of the war running noncritical or stubborn jobs sent to it by the British.

~~(TS//SI)~~ "003" cost only one-fifth of the yearly construction budget for a system that also found itself with much less than the expected amount of work. The huge voice encryption system the Signal Corps and the "F" section were building, the Sigsaly, had a $5,000,000 budget in 1943.[71]

(U) As a result of "003's" demonstration of the SIS's engineering abilities, Britain asked the agency to help solve more complex engineering problems and gladly accepted some American machines within GC&CS.[72] By the end of the war, the SIS was busy creating very advanced machines and, like OP-20-G, was hoping for a permanent in-house computer program.[73]

(U) More Emergencies and More Compromises

(U) The engineers at "G" and the SIS may have wanted to launch a far-reaching electronic development program at the end of 1943, but the Allies faced too many cryptological crises to allow the pursuit of any grand ambitions. Emergencies continued to drive the efforts at NCR and Nebraska Avenue, as well as at Arlington Hall. Some of the crises dictated the use of very

advanced technology, but others were handled by relying upon traditional components and architecture.

(~~TS//SI~~) Relays remained essential for many devices. The army put together increasingly powerful versions of the "Joos polygraphic counter" using the SIS's versions of the Letterwriter equipment. Arlington Hall's men also lashed together machines such as the Kryha Decipherer and the Longitudinal Differencing machine. The navy helped with the desktop

devices, and it went much further by putting new types of relays to work in its electrical crib-tester for the Purple system, the Purple Dudbuster.[74]

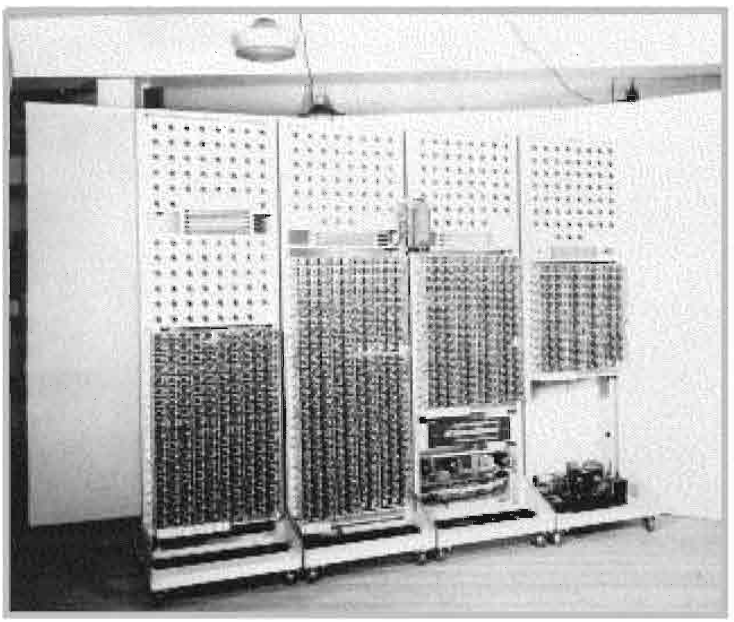
(U) Relays and plugboards were used in larger, stand-alone machines. Most of them were quite powerful, although some were bizarre combinations of primitive components. The need to create instant, yet reliable, cryptanalytic firefighters justified their crudeness.

(~~TS//SI~~) One crisis machine that had an almost vulgar look was the embodiment of a quite elegant statistical attack. The machine was the SIS's Dragon. It took almost a year to wire together all its components.

(~~TS//SI~~) Dragon was the crib-dragger SIS sent to England in late 1944 to help GC&CS attack the German Tunny enciphering machine. It was made of four large racks of relay panels, rows of switches, a tape reader, a large control panel, and a set of indicating lamps. A crib was set up on a plug-board, then the known settings and motions of Tunny wheels were entered through 200 switches. The message was read in by a standard tape reader. The crib, usually six to ten "letters," was tested against the message. When the machine calculated that a significant match (psi patterns) had been made, it stopped. The lamps indicated the Tunny wheel positions.

(~~TS//SI~~) The Dragon proved so useful that GC&CS built a second version after the American Dragon ate itself up. The noisy machine, which contained more than 2,000 cross-point relays, had a tendency to consume all the electrical power at GC&CS and to wear out its real contacts within a few weeks.[75] Despite its faults, it seemed such an achievement that it was sent back to the states after the war and was proudly displayed in the SIS museum.[76]

(~~TS//SI~~) Advanced statistical powers were added to the Dragons. If the war had not ended, the Dragons might well have evolved into machines whose sophistication rivaled the COLOSSUS.[77]



(~~TS//SI~~) Dragon

(U) The Other Purples

(U) In some ways the battle against the German military code and cipher systems was easier than the one against Japan's navy. The Germans' reliance on the Enigma allowed a concentration of cryptanalytic effort. Japan was not as cooperative. Its military did not use either a single code or a single encryption machine. Although much was shared among Japan's systems, the American and British codebreakers felt they had to start from the beginning with each new code, cipher, or communications subdivision system they encountered.

~~(TS//SI)~~ Despite the earlier successes against the Purple enciphering machine and the insights gained from prewar work on the Japanese navy's JN25 operational code, OP-20-G never had a secure entry into any of the major Japanese systems.[78]

~~(TS//SI)~~ Some of the Japanese naval systems yielded secrets more valuable than those gained from Purple, but that information came at a great cost. Even the rather old-fashioned code-plus-additive systems were as or more difficult to enter than Japan's high-level diplomatic machine. Japan's habit of frequently changing code and additive books compounded "G's" problems.

(~~TS//SI~~) The Japanese navy used 184 systems between December 1941 and the end of the war. And some 1,000 different ciphers appeared on them.[79] Triumphs in uncovering the underlying logic of systems did not ensure they could be read. An American cryptanalytic victory could be reversed overnight by a change in additives or, more permanently, by the introduction of new code books.

~~(TS//SI)~~ Although the navy had its RAM machines, tabulators, and the special "NC" machines to help discover the structures of the code and cipher systems, some of the most important ones remained unreadable until the latter months of the war. One of the reasons why OP-20-G hurriedly constructed so many relay, plugboard, and Letterwriter combinations in late 1944 and 1945 was the need to immediately exploit the systems that had taken so long to enter.

(U) But even in 1942, the least resistant and quickest technological path was the most rational choice for a search for an Ultra in the Pacific. Only when the tried-and-true technologies proved too slow was there an attempt to use digital electronics.

(U) In certain instances, avoiding the risk involved in applying electronics to the Japanese problems led to machines that should have been named after Rube Goldberg's inventions, rather than after snakes or jewels or flowers. The mandate to stay ahead of possible changes in the famous Japanese fleet operational code system, JN25, the rush to exploit Japan's long unreadable strip-cipher system, and the search to identify mysterious naval cipher machines led to some of World War II's most unusual cryptanalytic machines. Viper, Python, Gypsy, Opal, Mamba, and their relatives were clever throwbacks, but still throwbacks.

(U) New Guys and Old Guys, New Techniques and Old Insights

(U) After OP-20-G and GC&CS had reached an agreement about the Enigma problem in early fall 1942, the old-timers at "G," such as Mrs. Driscoll, were transferred back to the more familiar Japanese puzzles. The German naval problem essentially was turned over to Engstrom and his team of bright but young and cryptanalytically inexperienced "outsiders." "G's" leaders, such as Joseph Wenger, thought that with all the mathematical skills in "M," with its advanced machines, and with help from the British cryptanalysts, their weak background in practical attack on systems could be overcome.[80]

(~~TS//SI~~) The great American responsibility, the Japanese cryptanalytic problem, was given to "G's" professional cryptanalysts and the naval officers who had worked on the Pacific tasks before the war. They were in a separate subgroup, "GYP,"[81] which maintained a rather well-calculated distance from the young men working under Howard Engstrom. There was another group in Hawaii which continued on with its earlier work. The British frequently gave cryptanalytic advice and sent intercepts to both centers and to the cryptanalysts working in Australia.

(~~TS//SI~~) Washington was where cryptanalytic research and machine design were conducted for both European and Asian problems. But being in one center did not lead to agreement about crypto-methods or hardware. Those working on the Japanese problems had different perspectives from the young men in the "M" group. The distance between "M" and "P" included approaches to cryptanalysis. "P" was not as enthusiastic about abstract mathematical methods and RAMs as was "M." "P's" cryptanalysts did accept the reality that codebreaking had become a mass production operation, but they wanted tried-and-true methods and machinery, such as "differencing," the IBM equipment, and simple and reliable electromechanical analog.[82]

(~~TS//SI~~) Those preferences led to delays in the design and construction of advanced machines for the Pacific crypto-wars. "P's" reluctance to turn to new technologies was only one reason for the delays. And it was only one of the reasons for the many failures in the Pacific machine project. Technological barriers and the difficult nature of the attacks against additive code systems led to a string of well-intentioned projects that were unable to produce machines of the stature of the Enigma Bombes.

(U) A Matter of Machines and Control

(~~TS//SI~~) The differences over cryptanalytic methodology led to some frictions between "M," which thought, like Hooper, that advanced statistical methods were cures for all crypto-problems, and the old hands in "P," who trusted their long experience with Japanese cryptologic systems.

(~~TS//SI~~) An example of the results of the different approaches to codebreaking came in fall 1943 when frustration over the inability to even identify a new Japanese system led to a blunt exchange between the two types of cryptanalysts.[83] The frictions had been building for some time, with "M's" newcomers more than suggesting that on a routine basis messages should be run through the IC, Comparator, Tessie machines, and the advanced tabulators to identify "busts" or misuses of systems. By October 1943, suggestions about such routine "clinical" procedures to find "non-random" behavior in new systems were turning into recriminations.

(~~TS//SI~~) There was a suggestion in late 1943 that unread systems always be given to a new group separate from the "Y's" cryptanalysts. The proposed "GO" section would guarantee the application of all the new statistical methods to the recalcitrant traffic, no matter its country of origin or its underlying subject matter. It would, of course, take control over new systems away from those who were immersed in operational cryptanalytic and codebreaking attacks against families of systems.

(~~TS//SI~~) The suggestion for setting up "GO" did not have to wait long for a response. Commander L. W. Parke, one of the more experienced men in the organization, replied with a rather guarded criticism of the proposal. But it included more than a hint that it was "cryptanalytic experience" rather than "casual observation" that usually led to solutions. Parke soon became much more direct.[81]

> The author of the subject paper shows such a lack of comprehension of what goes on in GY that it [*sic*] does not deserve serious consideration....As to the variation from random idea [*sic*]

> a far more profitable attack is to be found in successive trials of known and probable methods of encipherment. In other words cryptanalytic experience cannot be supplanted by casual observers [*sic*] armed with machines and/or degrees of higher learning. The subject report is typical of the ideas that have come from GM's cryptanalytical research group during the past year. Although a few ideas have been useful, they were not worth the time spent in trying to help GM personnel to a better understanding of the problems involved in solving Japanese naval ciphers.

~~(TS//SI)~~ A rejoinder to Parke's criticism of the intellectuals reached the desk of one of the old-timers who, apparently, decided it was best to mark the top of each page of the renewed proposal for "GO" with the words "GM BURN BEFORE READING."

~~(TS//SI)~~ More than pride and turf wars were involved in the tensions between the operational and analytic types of cryptanalysts. At times the differences in approaches led to serious interpretive problems. The now relatively well-known battle between the analysts in the Pacific and those in Washington over the JN25 additives was only one of several conflicts.[85] A quite similar one took place in the summer of 1942.

~~(TS//SI)~~ The JN39 Japanese Merchant Ship/Navy additive system was introduced in August 1941 and was broken by the cryptanalytic group in Hawaii.[86] But understanding the system did not mean instant success. The recovery of the critical additives was progressing very slowly. Then Washington decided that it would apply its machines and analytic techniques to the problem. It used its own method of machine "differencing" to generate six times as many additives as Hawaii was producing by hand. Washington insisted its additives were correct.[87]

~~(TS//SI)~~ When code and additive books were finally captured, it was learned than some three-quarters of the Washington machine-produced additives were incorrect. A retrospective on the problem found that the pure analytic and machine methods were too simplistic and that "speed" of processing was no substitute for such vital activities as making sure that the recoveries actually led to readable traffic.[88] The discovery about the results of Washington's machine attack on "39" was linked to similar problems with its work on JN25.

(U) Such incidents perhaps restrained the operational cryptanalysts from requesting that the "M" sections engineers create advanced machines to help them break into the Japanese codes and ciphers. As a result, most of the machines built for the "P" group followed in the tradition of Purple, a direct analog to aid the decryption process after a system had been solved through traditional techniques.

(U) The Snake That Died Too Young, Viper

(U) Among the many frustrations "G" had to endure was the struggle against what was thought to be one of the most important Japanese cipher systems. In late 1942 it appeared that the Japanese navy might be on the verge of introducing a new cipher machine – one for the most important naval officers and ships. It had the potential to become another Purple for the Americans, a single machine-based system that would be relatively easy to read once the nature of the enciphering machine was established. The Americans called the system and machine Jade.

(U) There were, perhaps, some overly hopeful fantasies at OP-20-G that Jade would soon replace the Japanese Navy's important operational code, JN25. That additive code was being read, but with great effort and much worry. OP-20-G always fretted that the next change in it would be the one that permanently locked out the allies.

(U) JN157 (Jade) first appeared in December 1942. "G" could tell from messages on other systems that it was carrying very important high command communications. But the frustrations created by the unsuccessful attack on another Japanese cipher machine, Coral, led "G" to conclude that Jade was unbeatable. Until mid-1943 only minimal attention was paid to JN157

~~(U//FOUO)~~ Then there were a series of very lucky discoveries. Some busts were identified which gave a few clues to the nature of the Jade machine and which pointed to sources for cribs.[90] The belief that it was perhaps a solvable telephone stepping-switch machine (like Purple), and an increase in the amount of traffic on the system, led to a major attack on Jade.[91]

~~(TS//SI)~~ Statistical attacks were supplemented with crib-based "menuing." "G's" engineers lashed together a primitive stepping switch version of a new bombe to aid in the search for daily settings of the machine.[92] With the help of such machines, the attack on Jade yielded results within a few weeks.

(U) By October, 4,000 messages were being read by the Americans each month. The messages contained much about logistics and, later, many intelligence items. The cryptanalysts at "G," impressed by the high-level addresses on the messages, anticipated that Jade would soon carry the most important operational orders and would become more significant than the unpredictable JN25.

~~(TS//SI)~~ The optimism about the possibility of conquering Jade had led to the speedy creation of the Viper, an electromechanical analog of it, and the construction of several handy crypto-aids.[93] To speed decryption of all the messages, several more copies of Viper were built. The later models were quite advanced and expensive desktop automatic decipherers. Two copies were sent to England.

(U) Viper was in the tradition of Purple, although Lawrence Steinhardt was its top designer. A special Kana electric keyboard was connected to a large bank of electric stepping switches, relays, and plugboards. A Letterwriter typewriter was at the other end and served as the printer for the system. The Vipers looked much like the later versions of the Purple analog. The Vipers saved hundreds of very precious hours of analysts' time. But they were special-purpose machines.

(U) Because of the apparent value of JN157, a major project was begun to create more than an analog of the system. OP-20-G put the groups at NCR to work designing an ultra-high-speed "grenade" to speed the final and most difficult steps in discovering the keys to the Jade setups. The machine was to be powerful enough to overcome changes the Japanese might make to the system.

(U) Unfortunately, although the Americans continued to penetrate the JN157 Jade system, it did not carry the expected high-level operational messages. By early 1944, "G's" investment was not paying great returns. Then one of the great disappointments of the war occurred.

(U) Jade turned out to be an experiment by the Japanese, one that did not please them. The Jade JN157 system was cancelled in mid-1944, just as more advanced cryptanalytic machines to attack the system were being delivered to OP-20-G.[94]

(U) It seemed that more than a year and one-half of intense work had been wasted. In retrospect, however, it was decided that Jade had not provided that much important information. So its closing was not that critical from the operational side. And the work on it did make something of a secondary contribution to OP-20-G. It gave the cryptanalysts hope that another system which had resisted the most sophisticated attacks for many years might finally be conquered. On the

basis of the work on Jade, the Coral system project was restarted.

(U) A Snake in Hand, Perhaps – Python

(U) Japan had placed naval attachés in many of its embassies after World War 1. Their job was to report on the capabilities and intentions of foreign navies.[95] The Japanese hierarchy valued their communications so much that the attaché system was given one of the nation's first encryption machines, the Red. With the onset of World War II, the attachés assigned to the Axis nations assumed an expanded role in Japan's intelligence system. If their messages could be read by the Allies, they would provide insights into the plans and the technical prowess of all of the Axis powers.

(~~TS//SI~~) The attachés had many ciphers to communicate with (eighty-three over the course of the war), but two seemed of special importance to the British and American cryptanalysts, JNA10 and JNA20. They appeared to be the ones that carried the most valuable information to and from the attachés. The first was a very difficult version of Japan's many code-plus-additive systems; the other, the "G" and GC&CS teams discovered, was a new type of cipher machine that would not respond to the attacks that had broken Red or Purple. They called their new adversary "Coral."

(~~TS//SI~~) Through increased attention to the problem in Washington and England, the beginnings of an entry into JNA10 (the code and additive system) came in late 1943. However, full reading of all the links between the attachés and Tokyo was delayed for many months because special additive books had been assigned for communications between foreign capitals and Japan. They proved even more resistant to statistical attacks than the standard additives.[96]

(~~TS//SI~~) There was elation when the fortunate discovery of some cribs led JNA10 to open up to the Allies. The entry came too late to be of value, however. JNA10's main use was for transmission of information gained through espionage. By 1944 Japan's spy networks had withered, and the system yielded little information.

(U) However, the attack on JNAIO did give some encouragement to those who had attempted to read the much more important system, JNA20-Coral. JNA20 had frustrated "G" for many years. The navy needed a successful attack against it because it was used to report important technical information concerning all the military: land, air, and sea. As significant, its transmissions came from such vital points as Berlin and Moscow.

(~~TS//SI~~) JNA20 had a long, long history, but the Coral machine had first appeared in 1939 replacing the Red machine. It was soon distributed to all of Japan's attachés. The revised JNA20 system immediately came to the attention of the British. Although unable to read the traffic, they continued to intercept messages throughout the war. OP-20-G also took notice of the 1939 change in JNA20, but it was unable to intercept enough of the transmissions from Europe to Japan to begin an attack. That put the Americans at a disadvantage compared to the British codebreakers; in addition to the shortage of manpower, the lack of intercepts prevented the Americans from acquiring the necessary cryptanalytic "depths."[97]

(U) The desire to penetrate Coral remained high. Because OP-20-G had been reading Coral's predecessor, the Red machine, its officers realized how significant the Coral was. As many men and machines as could be safely taken off of other systems, such as the one for Japanese naval operations, were assigned to the new attaché problem in 1940.

(~~TS//SI~~) "G" tried all the standard statistical approaches. The messages that were available were frequency analyzed to see if Coral had the

same kind of statistical split between consonants and vowels as the old Red and Purple machines.[98]

~~(TS//SI)~~ Sadly, there was no return from the investment before the summer of 1941. Even then, the results were slim and less than encouraging. The time-consuming statistical tests showed the analysts only that Coral's inner workings were not just slight variations on the old Red machine. Coral, they knew, would be a very demanding problem.

(U) The task seemed daunting, so resources were shifted to other problems. However, when workloads allowed, "G's" analysts were encouraged to apply the most advanced methods to uncover the fundamentals of Coral. Some signs of progress appeared. They led to the reestablishment of a Coral program.

~~(TS//SI)~~ Many different statistical analyses and all the available RAM machines were applied during the next two years. The new IC machine was put to use, then Tessie. Some 100,000 message letters were counted and matched, again and again. Digraph counts and strip studies were done to see if Coral was related to the Enigma. Index of Coincidence tests were made on five months' worth of intercepts. Round Robin tests, matching every message from a day with every other, were made. A few prewar "obtained" plain texts were also analyzed. Isomorphic runs were done, and searches for tetragraphic repeats were made using all the messages for July 1941. All types of IBM tabulator indices were produced. The British joined in with their own methods, applying Turing's advanced hypothesis-testing concepts.

~~(TS//SI)~~ The work in England and America went on throughout 1942. But all that was determined was that Coral might be employing telephone stepping switches, as did other Japanese devices.

~~(TS//SI)~~ The attack stopped again. The RAMs and statistical techniques had let OP-20-G down. It seemed fruitless to devote any more effort to JNA20, despite the apparent value of its messages. The situation seemed hopeless. There was little possibility of either a theft of a machine (they were all in enemy territories) or a major misuse of the system.

(U) The victory over JN157-Jade in fall 1943 led, however, to renewed interest in Coral. Based on what was being learned about Jade, there was a hunch that Coral was a Roman-letter version of the JN157 machine. As soon as possible, the Jade team was reassigned and ordered to beat Coral.[99]

~~(TS//SI)~~ They joined with their counterparts in England on a six-month major statistical attack that again called on all the RAM machines. The goal was to reconstruct the wiring of the Coral stepping switches. The work was intense, but little came from it. By spring 1944 many were ready to declare that Coral was unbeatable. Mathematics again seemed unable to fulfill Hooper's promises.

~~(TS//SI)~~ Then, perhaps to the embarrassment of the mathematical types, a new member of the Coral group decided to retry some cribs. He asked a translator to see if he could place them, expecting not to hear from him for days, if not weeks. To everyone's surprise, the translator returned within a hour with a report of success. Then a longer crib was placed and the Coral wirings were recovered.[100] In early March 1944 Coral was beaten and began to yield intelligence treasures.[101]

(U) "G" had already been preparing for the triumph over Coral. The "M" group had been ordered to start designing an analog well before the break occurred. The result, the Python, was a relatively crude, quickly built desktop cousin of the Viper. Two Letterwriter typewriters were the

input and output mechanisms. Between them was a plugboard and a large bank of relays that could be set to imitate the "wheels" and motions of Coral.

(U)) Python was put to use in mid-1944, automatically decrypting messages and helping to test possible solutions to Coral settings. Several more were built and served until the end of the war. While relatively slow, the Pythons did their job with the reliability that could not be expected from more advanced and costly electronic devices. It was soon helped by a special analysis machine that had originally been built for the abandoned Jade system.

~~(TS//SI)~~ Supported by an ongoing statistical attack suggested by the British, and by a home-grown crib method that broke daily keys, Coral was made to yield some of the best intelligence of the war. The cargo-carrying submarines that ran high-priority material between Japan and Germany became easy targets. The German "buzz" bomb, radar, and other great secrets became known to the Allies through the reports sent to Japan by the attaché in Berlin.

(U) That attaché did more for the Allies. He gave a precise description of all the defenses on the French coast. In addition, his messages told the Allies what the Germans thought about the timing and location of the Allied invasion of Europe.

(U) Of Strips and Stripper

(U) Japan did not trust cipher machines as much as Germany did; it employed several rather old-fashioned systems on many of its important communications channels. Some of those primitive systems caused as much trouble or more than Enigma or Jade or Coral. One of Japan's alternative encryption devices, JN87, led to as much technological soul-searching at OP-20-G and National Cash Register as had the cipher machine problems.

(U) The Americans had suspected that the Japanese navy was going to initiate the use of a new shipboard encryption system in mid-1944. But beyond a hint that it would be a sort of hand-operated "strip" device, nothing was known. When the Japanese began using the system, "G" was unable to read any of its messages. Then a capture was made by Filipino troops. The instruction books and parts they seized in November 1944 were quickly sent to "G." The captures and analysis of JN87 intercepts led to a partial but important solution by early December.

(U) JN87's device was quite like the American Navy's own strip cipher. The '87 had a plastic board holding strips that had alphabets printed on both sides. There was a stock of one hundred two-sided strips to chose from. Thirty at a time were placed in the board, with their particular vertical and horizontal arrangement set according to complex specifications given in a book of instructions.

~~(TS)~~ The JN87-based fleet communications became so numerous that hand deciphering was an impossibility. Thousands of intercepts began to pile up; the backlog seemed to contain items of importance. To solve the problem, "G" instructed Lawrence Steinhardt to build a reliable machine as quickly as possible. His design reflected how little time he had to complete the analog. At least he was able to show a sense of humor: he gave the machine the name of the famous American strip-tease dancer, Gypsy Rose Lee.[102]

~~(S)~~ The NCML's engineers at NCR were given the responsibility for construction. They worked on the control portion of Gypsy, a formidable task. Ralph L. Palmer was in charge, and he was determined that his team would overcome all the difficulties. His crew worked double shifts and stayed on the job through the Christmas holidays. That allowed them to solder the required 40,000 connections in Gypsy's-central cabinet.[103] Meanwhile, the navy's engineers and, perhaps, some WAVES were wiring the many "strips"

(plugboards) as quickly as the cryptanalysts could recover them from analysis of JN87 depths.

(~~TS//SI~~) Both teams were successful. Gypsy was in operation a month after it was ordered. Unfortunately, just as Gypsy began its work, the Japanese altered their system, and the boards had to be rewired. The Washington unit became very efficient at that; the Japanese began to change all the strips every three months or so.[104]

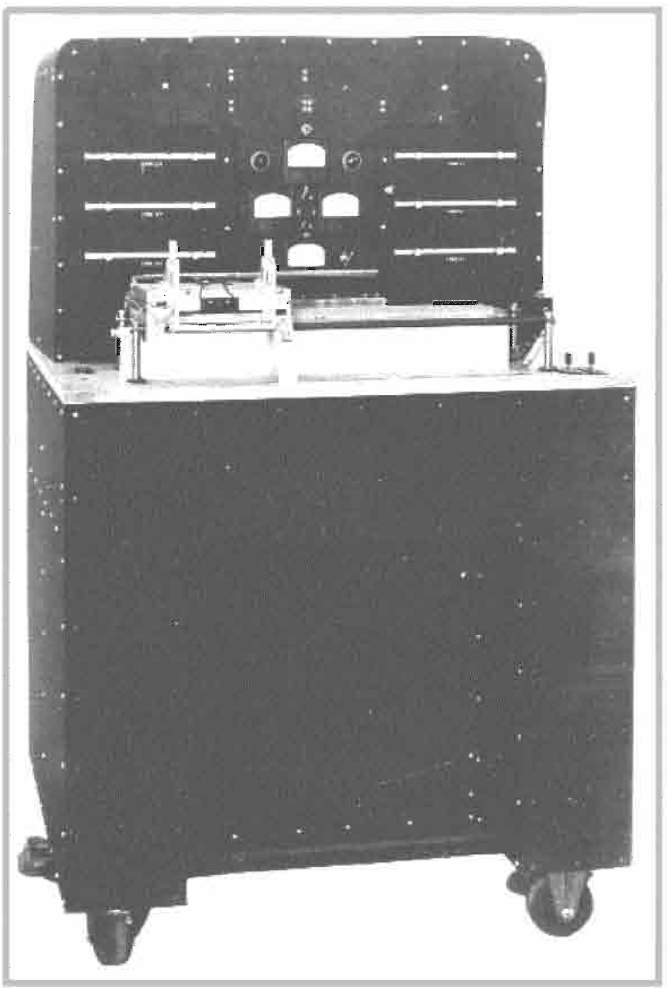
(~~TS//SI~~) Steinhardt's Gypsy was a get-the-job-done machine. It was a large, 4,000-pound relay, stepping-switch, and plugboard combination that required a central control unit and five separate six-foot-high bays. Each of the bays contained five large plugboards. Each board was hand-wired to represent four of the JN87 strips. Because the strips were two-sided, the Gypsy plugboards were constructed to represent eight choices.

~~(TS//SI)~~ The control unit had switches to select the desired "strips" and which of their sides were to be used. The Gypsy's operator could also automatically shift the "strips" and set other crypto-variables. Banks of lights signalled which boards and which off-sets had been selected. Then the enciphered message was typed on the machine's Kana input typewriter. If the message was free of garbles and Gypsy was correctly set, clear text was printed on a Letterwriter typewriter. The JN87 messages seemed so important and Gypsy so useful that another model was ordered. It was to be used in Hawaii. It was planned to have a tape reader as input to speed processing.

(U) Strips without Strippers

~~(TS)~~ Two other machines built for "strip" problems did not have such a happy career. Topaz and Mamba became examples of the danger of relying upon special-purpose machines, even when they could be built quickly with tried-and-true parts. Both Topaz and Mamba arrived after their target problems had disappeared.

(U) Topaz was quite similar to Gypsy in its architecture and purpose. It was another huge plugboard and relay combination for semiautomatic deciphering through removal of the influence of "strips." But its task was a bit different than Gypsy's. The "strips" used by the Japanese



~~(TS//SI~~) Mamba

on their navy merchant marine JN11 communications represented additives. JN11 was a superenciphered code system and a very important one which often served as the window into Japanese communications when other codes were unreadable.

(U) Topaz was clever. It removed the additives and printed the resulting code. But the two models of Topaz were rarely used. They arrived too late to be employed on current JN11 traffic, and, despite their being modified to work on the famous JN25 system, their short lives were spent working on old JN11 messages.[107]

~~(S)~~ One of the most unusual machines that OP-20-G brought into its RAM collection was Mamba. It combined IBM cards, relay circuits, and analog decision making in a five-foot-high metal cabinet. It looked like a friendly, many-eyed monster because of its two round signal lights and its small voltage meters.[108]

~~(S)~~ Mamba's unique feature was its input system, an electromechanical card scanner. Located on a shelf at the center of the machine, the scanner shifted IBM cards holding cipher over a set of others punched for key. Mamba sensed how many of the 2,400 tiny metal brushes (ten digits in eighty columns in three cards) made contact as the message cards were moved, column by column, over the key cards. Mamba's goal was to exploit a weakness in many of the Japanese code systems, one that had become important to the American attacks. All legitimate code groups were evenly divisible by three.

~~(S)~~ Mamba's electrical weighting component could be set to stop the machine when accumulated "scores" exceeded a threshold value. When enough of the brushes made contact through coincident holes in the cards, the scanner's power was cut off. Once the machine stopped, its operators recorded the source of the "hits" by hand.

~~(S)~~ Although relatively crude, and useful only when the cryptanalysts had a good idea of which page of additives had been applied to a message, Mamba seemed so promising that two were constructed at NCR. They were delivered to the navy in the last days of 1944.

~~(U//FOUO)~~ It was expected that Mamba would vastly reduce the amount of hand work needed for the JN11 system. But the Mambas arrived after the specific system they were designed for "died." To salvage some of the investment, at least one was modified to perform what was called a "maximal-minimal" attack on JN25.[109]

(U) The Attack on the Many JN25s

(U) The new automatic enciphering machines, such as the Enigma, Jade, and Coral, have been crypto-historians' favorites. The machines and the attack on them have an inherent attraction. The mechanical complexities are fascinating, and the logic of the attacks are intellectually challenging. In addition, the machines that were built to fight them, the Bombes and the Colossi, are symbols of the coming of the new information age. The Bombes and Colossi are also physical reminders of how difficult codebreaking had become by the 1940s.

(U) But more important in terms of the war in the Pacific than the automatic enciphering machines were old-fashioned systems, such as the Japanese Fleet General-Purpose Code, and JN25. Codes like "25" proved as or more difficult to penetrate than machine ciphers. JN25, an additive system, took so much effort that a special and very large "G" cryptanalytic group was created early in the war.

(U) In Washington alone, some 800 people were working on "25."[110] By the later months of 1943, Howard Engstrom's "M" group became

involved. It began to devote much of its time to finding practical designs for very, very rapid machines with enormous amounts of memory to handle the special demands of the JN25 problem.

(U) Because of the special challenges posed by code systems, "G" was unable to create an equivalent to the Bombe for the Japanese codes. And they were unable to devise electronic devices. "M" had to concentrate on creating "memory" machines from what was technologically at hand. Although compromises, the machines they came up with promised to be more productive than the standard tabulators, the navy's NC machines, or the relay-tabulator Slide Run machines that were used by the army.[111]

~~(TS)~~ JN25 was a difficult problem for several reasons. The primary one was the general nature of well-fashioned code plus additive systems. They left analysts awash in unknowns, forcing them to grab at cryptanalytic straws to make any progress. Although codes can be analyzed through frequency tests quite similar to those used on the distributions of letters in cipher systems, doing so is quite demanding and usually yields less rewarding answers. Counts of code groups in large collections of messages can yield good pointers to frequently used words in a language, such as "to" or "the," and to word combinations typically found in military messages such as "Fleet orders."

~~(TS)~~ Identifying one group can help find the meaning of another. But codes with thousands of groups, several of which stand for the same plain language word, usually do not open up as a result of frequency tests.

(U) The frustrations involved in trying to solve a code system without the aid of captures or operator errors grow exponentially when the underlying codes are themselves enciphered. Adding or subtracting numbers tends to mask the frequencies of the code groups. If the "additives" are from a long list or, worse, are randomly generated, there is little chance of removing their influence.

(U) Additive systems have been in use around the world for generations, and attacks on them began when they first appeared. Some very complex methods had been developed to help identify additives. Attacks such as "differencing" were relatively freestanding. To begin the arduous process of rounds of subtraction and cycle analysis, differencing only asked for messages that were in "depth." But much depth was required. Differencing needed bulk cipher-text that was known to have been enciphered with the same key. But the method had at least the potential for automation.[112]

(U) In contrast to differencing, most other approaches were based on common sense, were difficult to automate, and were useful only after some significant breakthroughs into the additive and code systems had been achieved. A frequently used one was to assume that some additives were known, then subtract them from the cipher, then match the resulting plain code against a long list of known and highly frequent code groups. If a match, or a significant number of matches, was found, additional effort was invested in producing a plain text and increasing the list of known code groups.

(U) Other methods demanded the use of very experienced codebreakers. They required knowledge of military systems and a craftsman's insight once additives had been removed. For example, an analyst might begin his attack by assuming that previously known stereotyped phrases or usages were in the messages. After seeing if his intuition led to an interpretation that made sense, a tentative meaning would be assigned to a code group. Then other messages would be searched to double check the hunch. If consistency was found, many messages would be processed in order to construct a file of appropriately weighted "high frequency" code groups. That file would be checked and updated in an endless cycle as it was

used to see if correct additives had been discovered, and to see if meanings could be attached to more of the recovered numeric codes.

(U) The Americans had used all those methods in the 1920s and 1930s, and they applied them to Japan's World War II systems. But JN25 had its own particular difficulties, ones that challenged the traditional attacks. First, it had a very lengthy code book. Its first one, of 1939, contained over 30,000 groups; later versions had more than 50,000 of the five-digit codes. That meant that even when a clear code group was intercepted, its meaning was very difficult to determine. More than one code number might stand for the same word or phrase. In addition, the Americans thought they might be facing a system in which one code group could have different meanings depending upon context.

(U) None of the old cryptanalytic standbys appeared in JN25's early years. Unfortunately for "G," JN25 code books were not "obtained," there were few operator mistakes, and OP-20-G was unable to discover many cases in which a JN25 message was sent on a system that was being read. The only recourse OP-20-G had was to try to intensify the application of the tedious and frustrating traditional attacks it had used before the war.

(U) The Japanese did not make things easy for "G," although they did employ a few techniques that deviated from the rule of randomness. One of the errors the Japanese made, but an important one, was to facilitate the detection of garbled messages by making legitimate code groups divisible by three.[113] The use of that "pattern" vastly reduced the number of true code groups the Americans had to identify, and it also eased the search for additives.

(U) The Americans had achieved some brilliant but temporary successes against JN25 using old-fashioned hand methods supplemented by the IBM tabulators. Enough of JN25 was understood in mid-1942 to give "G" its first great triumph.[114] With only a handful of people and a few tabulating machines, "G's" branch in Hawaii was able to contribute vital information on the coming Midway and Coral Sea battles. The contribution was marked by controversy, however.

(U) The analysts in the Pacific had disagreed with the conclusions by "G's" experts in Washington about the correct interpretation of the codes and additives. The analytic group in Hawaii had faith in "experience" while Washington relied more upon formal analytic methods. Unfortunately for the chief analyst in Hawaii, Joseph J. Rochefort, being correct about the contents of JN25 did not prevent him from being disciplined for deviating from prescribed reporting practices.[115]

~~(TS//SI)~~ But there was much in the JN25 systems that made them very, very difficult. The codes were hidden by the use of nearly random additives that were contained in lengthy books. The first of the additive books had 300 pages, each holding 100 five-digit numbers. A complex and very opaque indicator system was employed to communicate which page and which starting point were to be used for a message. All JN25 indicators were scrambled in one way or another, and their encryption algorithms were frequently changed.

(U) More than indicator systems were altered to thwart cryptanalysis. During the first two years of its life, the JN25 code was replaced once and the additive books were changed six times. The replacement of the additive books continued throughout the war. Worse, the code itself was changed at very critical moments. That meant the need to reconstruct the code meanings all over again. When the Japanese changed additives, codes, and indicator systems all at the same time, it was devastating for the Americans. That was the reaction in 1944 when there was a total change in "25."

~~(TS//SI)~~ Despite all the experience it had gained, in mid-1944 "G" worried that it might never reenter JN25. Only errors on the less valuable JN11 systems allowed it into operational messages while its crew frantically tried to determine the meanings of the thousands of new "25" codegroups.[116]

(U) The difficulties caused by the JN25 system changes were multiplied as the Japanese divided the "25" system into more and more separate networks or "channels." Each had its own procedures. Entry into one was not a guarantee that others would be read.

(U) The Comparators That Weren't: the Copperhead Proposals and the Victory of Electromechanics

~~(S)~~ It had become clear to OP-20-G and the SIS, which was tackling similar problems, that automation was needed to handle the Japanese codes. The first responses were predictable. Both the army and navy turned to mechanics, tabulators, and relay devices. The SIS engineers and their allies at IBM extended the reach of the relay tabulator combinations through the Slide-Run machines. "G" counted on similar devices until "M" began to involve itself with JN25. It recommended the construction of a host of permutations of Bush's ideas. Unfortunately, only one was accepted, and it evolved into a punch tape, not a microfilm machine.

~~(S)~~ The navy had asked the practical engineers at the Navy Yard under Don Seiler for help fighting code systems before the war began. By 1940 he built a fifty-wheel cam and gear device that was driven by hand cranks. It tested cipher and additives for divisibility by three.[117] The next response by both the army and navy was to modify the tabulators. The goal was to speed up the false subtraction processes used in both differencing and additive stripping. The navy's NC machines began arriving before the war broke out, and the army quickly drafted plans for its Slide Run machines. Those combinations of complex relay boxes and tabulator equipment were difficult to build, however, and did not come into operation until the last months of 1943.[118]

~~(S)~~ OP-20-GM's team wanted to create machines faster and much more powerful than the NCs or the Slide Run devices. Lawrence Steinhardt was given the responsibility. He helped draft a series of proposals in mid-1942. Each fit with his and John Howard's previous work at MIT. While the designs were being mulled over, Steinhardt rescued the idea that film and photoelectric technology could be used for frequency tests against JN25. Apparently such a hope had almost been killed in early 1942.[119]

~~(S)~~ One of the first challenges Howard Engstrom had presented to Eastman-Kodak was to produce a machine for additive code systems. With the ex-IBM engineer John Skinner acting as the liaison, Eastman quickly arrived at an ambitious design for an "automatic decoder." The device was to strip additives, locate the plain code in a large dictionary, and set down the meaning of the code. Eastman was not sure whether electronics or older technologies would be used to do the stripping; but it was committed to developing optical discs to store the code meanings and to a fast-flash system to print the results. To "G's" disappointment, just as Engstrom thought of asking Eastman to prepare a detailed design, the company announced it was too busy with the IC and Tessie projects.[120]

~~(S)~~ Given the difficulties at Eastman, Engstrom turned to Lawrence Steinhardt.[121] He handed him the responsibility for the additive systems. He began exploring machine alternatives in mid-1942. But he was not allowed the opportunity to turn his general ideas into specifics until mid-1943. The Atlantic problem took all of "M's" resources until then.

~~(S)~~ Steinhardt's initial suggestions relied upon Bush's favored technologies. They were

sometimes referred to as the Copperhead proposals. The first of them was for a photo-optical machine that was to be a high-speed replacement of Seiler's device. It was to have base-three tube ring counters. Its job was to subtract suspected additives code groups found in messages already aligned in depth. Its goal was to point to the most likely additives through the "divisible-by-three" criterion. It took a year after the initial sketch to produce a detailed design. Then when it was examined, it was abandoned, declared to be too electronically adventuresome.

~~(S)~~ The next plan, also envisioning photo-optical technology, was more architecturally ambitious. It was intended to automate the sophisticated method of "Jeeping." It was a means of identifying likely additives and then code groups. "Jeeping" was an extension of the differencing method; an extension that called for a large amount of high-speed memory and near-endless rounds of running messages against each other. It was based on the probability that if cipher texts that had been enciphered with the same "keys" were subtracted from each other, an identifiable "difference" would lead to plain code and correct additives. The difference could be checked against a huge catalog containing all the possible differences between high frequency code groups in a system. "Jeeping" was a valuable method, but it soaked up hours of effort to process just a few "differences."

~~(S)~~ Although "Jeeping" was a method that should have been automated, the photo-optical machine, with the high-speed photographic reproduction of hits that it demanded, was too much for "M." The detailed mid-1943 plan for the proposed Mark II was shelved. Even a simplified version, without automatic recording, was abandoned.

~~(S)~~ Bush's fundamentals received another setback when Copperhead II was rejected as too complicated. It was a film version of a Slide Run machine. Its job was to subtract known additives in a system from masses of cipher text, then run the results against a huge file of already known high-frequency plain codes. If enough matches resulted, the machine was to issue a signal and record the hit. With that information, an analyst could align more text and add to the files of known additives and codes.[123]

~~(S)~~ Even a reduced version of Copperhead II was rejected. The Mark V was to have a smaller "memory," although its matching decisions were to be based on a complex weighting system derived from studies of language and code frequencies. The debates over the merits of those "Hall" and "Shinn" weights may have been one reason why the Mark V was not completed.

~~(S)~~ The only one of Steinhardt's designs that was accepted and turned into hardware was Copperhead I. And its technology was a major compromise. It became a punched tape, not a film machine. That it was built at all is an indication of how much JN25 worried the cryptanalysts.[124]

~~(S)~~ Copperhead I was a device to aid them when they had no entry into a system. It was an embodiment of a "Brute Force" method that was used in moments of desperation. Its purpose was to fill the void when the cryptanalysts did not have enough recovered additive or code values to even begin using tools such as differencing or "Jeeping." A large volume of cipher text was run in the hopes of finding "double repeats" which would indicate which messages and their offsets were in depth. A double repeat was when the same two encrypted code values appeared in two texts at the same distance apart from each other. It was calculated that locating such matches vastly increased the probability that a depth had been found.[125]

(U) Beyond the Copperheads – the JN25 Crisis and "M's" Response

~~(TS//SI)~~ Howard Engstrom would have ordered Lawrence Steinhardt to turn to other problems after the Copperhead defeats, but there were signs that JN25 and other Japanese additive systems were undergoing a series of changes. There was fear they might become unreadable. High-speed machines to meet the new Japanese challenges seemed essential. As a result, Steinhardt was ordered to explore all types of alternatives to Bush's favored technologies.

~~(TS//SI)~~ As Steinhardt searched for new possibilities, including digital electronics, other engineers at SIS and "M" moved towards electronic solutions to German challenges. Like Steinhardt, they were pushed by cryptanalytic needs that could not possibly be met with the older technologies. By 1944 both the army and navy were moving far beyond the original Bombes and Bush's Comparator.[126]

Notes

1. (U) Bradley F. Smith's *The Codebreakers War*, (Novato: Presidio Press, 1993) details the struggles of the army to gain entry into Ultra.

2. (~~TS//SI~~) NSA CCH Series XII Z, "Washington E Traffic, Notes on Correspondence" circa February 1942. (~~TS//SI~~) NSA CCH Series XII Z, "Green Analog," May, 1953. A most important source showing the concentrated work SIS did on the complex German diplomatic systems is found in (~~TS//SI~~) NSA CCH Series XII Z, "History, Machine Branch," np. nd. (~~TS//SI~~) NSA CCH Series IV B-1-11, "History of the Signal Security Agency, Volume 11, The Machine Branch," October 29, 1947.

3. (~~TS//SI~~) NSA AHA ACC 16844. "History of the Special Projects Branch, SIS ETOUSA."

4. (U) NSA release, Theodore M. Hannah, "Frank B. Rowlett: A Personal Profile," 522. NARA RG457, SRH-004, "The Friedman Lectures on Cryptology."

5. (U) Thomas Parrish, *The Ultra Americans: The United States' Role in Breaking the Nazi Code* (New York: Stein & Day, 1987), 45.

6. (U) NARA RG457, SRH-361, "History of the Signal Security Agency," Volume II, 82, and SRH-362, "History of the SSA Vol. III, The Japanese Army Problems: Cryptanalysis, 1942-1945." Edward J. Drea, *MacArthur's Ultra* (University of Kansas Press, 1992), 10. NARA RG457, SRH-145, "Collection of Memoranda on Operations of SIS Intercept Activities and Dissemination 1942-1945," 01, and SRH-361, "History of the SSA," Vol. II, 250, 272. Ronald Lewin, *The American Magic*, 38 (New York: Farrar-Strauss, 1982). (~~S//SI~~) NSA CCH Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982.

7. (U) NARA RG457, SRH-004, "The Friedman Lectures on Cryptology," 171.

8. (U) Cipher A. Deavours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, Massachusetts Artech House, 1985), 238. NARA RG457, SRH-305, "The Undeclared War: The History of RI," 15 November 1943, by Laurance F. Safford, Captain, U.S. Navy, and SRH-159, "Preliminary Historical Report of the Solution of the B Machine."

9. (U) Edward J. Drea, *MacArthur's Ultra* (Lawrence: University of Kansas Press, 1992), xii, 61-2.

10. (U) Again, the documents found in the Garland Covert Warfare series are most rewarding. See "History of 3-US," 010-026, and "Origins, Functions and Problems of the Special Branch, MI." Useful background on army intelligence is in Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff: 1775-1941*, (University Publications of America, nd).

11. (~~S~~) NSA RAM File, June 23, 1943, OP-20-G to OP-20, "Army has agreed to tell England too much." NARA RG457, SRH-349, "Achievements of the SSA In World War II," 31, and SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 11-22, 250, 276-283. (~~S~~) NSA CCH Series XII Z, "History of GET (TUNNY) Research."

12. (U) Edward J. Drea, *MacArthur's Ultra* (Lawrence: University of Kansas Press, 1992), xii.

Geoffrey Ballard, *On Ultra Active Service* (Richmond, Australia: Spectrum Publications, 1991), 194-231.

13. (~~S~~) Perhaps it was SIS's first failure with Freak that led Joseph Desch to accept the design for Mike, the huge mechanical counter NCR built later in the war. (~~S~~) NSA CCH Series XII Z, Inventories of RAM Equipment, 1945.

14. (~~S~~) Perhaps it was SIS's first failure with Freak that led Joseph Desch to accept the design for Mike, the huge mechanical counter NCR built later in the war, f[0058].

15. (~~TS//SI~~) NSA CCH Series XII Z, "M.A.C. Outlines #11, Freak." (~~TS~~) NSA CCH IX.B.1.9, SSA, "History of the Signal Security Agency, Volume Nine, History of the Development Branch," 10 February 1953.

16. (U) The use of condensers for such storage was "in the air" at the time, including at MIT, and similar systems were used in the ENIAC.

17. (~~TS//SI~~) The seven condensers could hold 128, but Freak counted only up to 99. (~~TS//SI~~) NSA CCH Series XII Z, "M.A.C. Outlines #11, Freak."

18. (~~S~~) Many of the storage uses of condensers were based upon setting constant values by hand. Thus, Freak was quite an adventure.

19. (~~S~~) NSA CCH Series XII Z, "Freak I," May 1953.

20. (~~TS~~) NSA CCH IX.B.1.9, SSA, "History of the Signal Security Agency, Volume Nine, History of the Development Branch," 10 February 1953, 83.

21. (~~TS//SI~~) NARA RG457, SRH-349, "Achievements of the SSA In World War II," 18. University of Pennsylvania Van Pelt Library Archives, Papers of John Mauchly, 2B-10:a 209, 14, October 11, 1945 and April 14, 1945 "Visit to SIS and Cryptologic Problems." NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 237. (~~TS//SI~~) NSA CCH Series XII Z, "History, Machine Branch," np. nd. (~~TS//SI~~) NSA CCH Series IV B-1-11, "History of the Signal Security Agency, Volume 11, The Machine Branch," October 29, 1947.

22. (~~TS//SI~~) NSA CCH Series XII Z, "History, Machine Branch," np. nd., 30-37.

23. (~~TS~~) NSA CCH Series IV, V 10.6, Chief Signal Officer, "A Chronology of the Cooperation Between the SSA and the London Office of GCCS," 2 June 1946. (~~TS//SI~~) NSA CCH Series XII Z, "Washington E Traffic, Notes on Correspondence" circa February 1942. (~~TS//SI~~) NSA CCH Series IV B-1-11, "History of the Signal Security Agency, Volume 11, The Machine Branch, October 29, 1947.

24. (~~TS//SI~~) NSA CCD Series IV B-1-11, "History of the Signal Security Agency, Volume 11, The Machine Branch," October 29, 1947, 84.

25. (~~TS//SI~~) NSA CCD Series IV B-1-11, "History of the Signal Security Agency, Volume 11, The Machine Branch," October 29, 1947, 22-23, 88. (~~TS//SI~~) NSA CCH Series XII Z, "History, Machine Branch," np. nd., 24.

26. (~~TS~~) NSA CCH Series IV B, "History of ASA Equipment (Development Branch) History," December 1942, 30 June 1944.

27. (~~TS//SI~~) f[42211] (~~TS//SI~~) NSA CCH Series XII Z, "History, Machine Branch," np. nd., 51, 62.

28. (~~TS//SI~~) NSA Series XII Z, MAC Outlines, "The Slide Run Machine."

29. (~~TS//SI~~) NSA Series XII Z, MAC Outlines, "The Slide Run Machine." (~~TS//SI~~) NSA CCH Series IV B-1-11, "History of the Signal Security Agency, Volume 11, The Machine Branch," October 29, 1947. The first "F"-built machines had two cabinets.

30. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. Other relay-tab combinations such as the JMA and the "deciphering machine" were built by SIS to perform similar tasks for additive systems.

31. (~~TS//SI~~) NSA CCH Series XII Z, MAC Outline #4, "The Slide Run Machine."

32. (~~TS//SI~~) NSA CCH Series II Z, MAC Outline #4, "Slide Run Machine."

33. (~~S~~) NSA CCH Series XII Z, OP-20-G, "SSA Proposal for 70mm Film I. C. Machine," 8 June 1945.

34. (~~TS//SI~~) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 272.

35. (~~TS~~) NARA RG457, SRMA011, "Senior Staff Meeting Notes," August 18, 1942, Friedman memorandum "Establish Section F." David J. Crawford, The Autoscritcher and the Superscritcher, forthcoming. *The Annals of the History of Computing* illustrates the advanced technical achievements of "F." In fact, "F"

may have forged a bit ahead of OP-20-G in respect to the use of digital electronics. One reason may have been that "F" was under less pressure to solve immediate cryptologic crises. Again, NSA SRH-391, "U. S. Cryptologic History," contains dates somewhat different than those found in RAM file documents and other relevant SRH volumes. ~~(TS)~~ ASA CCH Series IV B, "History of ASA Equipment (Development Branch) History, December 1942 – 30 June 1944." ~~(S//SI)~~ NSA CCH Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 96.

36. (U) NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 287.

37. ~~(TS//SI)~~ NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 272.

38. ~~(TS//SI)~~ NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 258.

39. (U) NSA SRH-391, "U. S. Cryptologic History," 120, provides a hint that the SIS's relay machine may have first been explored by the British and shown to the Americans under direct order from Churchill. Other sources, such as a letter from George Stibitz to the author, suggest the relay machine was an American idea.

40. ~~(TS//SI)~~ NSA RAM File, J. N. Wenger to OP-20-G, September 3, 1942, "Part II of Report of J. N. Wenger, Capt. USN," 1. Letter to the author from George R. Stibitz, June 7, 1987. NSA RG457, SRH-361, "History of the Signal Security Agency," 250, 257, 272-3. At least one source claims that the American army's cryptologists were informed of and worked on the FISH traffic as early as August 1942. That source also claims that some machines were built in America for the automated solution of that binary system. However, there is no claim that the army built anything like the Colossus for the problem. See NARA RG457, SRH-349, "Achievements of the SSA In World War II," 18.

41. ~~(S)~~ Rosen did not lose faith in electronic solutions. In June 1943 he suggested a machine solution for the commercial Enigmas that would include a frame from the relay Madame X bombe and as many as fifty-two "counters" made of vacuum tubes. ~~(S)~~ NSA CCH Series XII Z, Robert O. Ferner, "Rapid Analytic Machinery Needed for Research," June 3, 1943.

42. ~~(TS//SI)~~ NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 258. ~~(TS)~~ NSA CCH Series IV B, "History of ASA Equipment (Development Branch) History, December 1942-30 June 1944. f[4221]. The contract with Western Electric was for only about $2,000. The F branch annual report for 1944 listed a project for a high-speed rotor for the period May – November 1944. ~~(S)~~ NSA CCH Series XII Z, Annual Reports, Development Branch, 1943-4.

43. ~~(TS//SI)~~ NARA RG227, Box 73, February 29, 1944, Stibitz to NDRC, "Secrecy re NCR product." Williams went on to build many huge relay computers for the military ordnance groups during World War II, and he designed and patented an electronic computer. Michael R. Williams, *A History of Computing Technology* (Englewood Cliffs, New Jersey: Prentice-Hall, 1985), 225-240. Hagley Museum and Library, Accession 1825, *Honeywell v Sperry-Rand* , Trial Records, February, 1942, S. B. Williams to NDRC, "Fire control proposal," and Reports on Electronic Computer Designs by S. B. Williams, November 1941, January 1942, March 13, 1942. NSA RAM File, September 3, 1942, "Wenger to OP-20-G, bombe project;" September 9, 1942, "Machine Research Section (F)"; "Part II of Report of J. N. Wenger, Capt. USN," 1 and October 10, 1942, "Enigma Machine Contract." Letter to the author from George R. Stibitz, June 7, 1987. The army's single machine cost over $1,000,000. NSA RG457, SRH361, "History of the Signal Security Agency," 257, 272-3. NARA RG457, SRH-349, "Achievements of the SSA In World War II," 29. NARA RG457, SRH-61, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 251.

44. ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G "Memoranda on Bombe and the relationship of the U. S. and U. K.," circa 1943. In addition to not fulfilling all the expectations of automatic setups, 003 did not incorporate some features suggested after its first design was set. In mid-1943 one of the SIS cryptanalysts suggested that a Madame X frame be combined with electronic counters to allow a purely statistical

attack. A later machine, the SIS Dudbuster did have something like that configuration, but it became a separate machine, not an integral part of 003. (S) NSA CCH Series XII Z, Robert O. Ferner, "Rapid Analytic Machinery Needed for Research," June 3, 1943. Technical details of 003 may be found in an early report, (S) NSA CCH Series XII Z, "X-68003, Bell Laboratories Report, April 2, 1943." (S//SI) NSA CCH Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982..

45. (TS//SI) After some experience with the 003, a menu with a sure crib of twelve letters was considered useful although it would produce more false hits than a strong menu of fifteen or so letters

46. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982.

47. (TS//SI) NSA CCH Series XII Z (S-2568), "Tentative Brief Descriptions of Cryptanalytic Equipment for Enigma Problems," circa 1945.

48. (TS//SI) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 265. (TS) (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March, 1945. (S) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 3, 54.

49. (TS//SI) NSA RAM File, February 21,1944, W. A Wright to OP-20-G, "Comparison of Army and Navy Enigma Equipment," and January 18, 1943, to OP-20-G/da, "Report of Meeting on Army Bombe."

50. (S) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 50-52.

51. (TS//SI) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 265. For insight into how much SIS had learned about Enigma methods by the end of 1943, see (S) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," especially pages 31 and 35. These suggest that the British had developed their own "machine guns." (TS//SI) NSA CCH Local Archive, "Army-Navy Descriptive Dictionary of Cryptologic Terms," Army Security Agency, February 1947. (S) NSA AHA ACC 16890N, "Bombe Operations, Control, and Testing, Duds and Railway E."

52. (TS//SI) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 265. (S) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 35.

53. (S) NSA AHA ACC 16890N "Bombe Operations, Control, and Testing, Duds and Railway E."

54. (TS//SI) NSA AHA 16331, "6812th Signal Security Detachment (PROV) Apo 413 Army," 15 June 1945, 35. (S) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 40.

55. (TS//SI) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 265.

56. (TS//SI) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years.

57. (S) The SIS cryptanalysts, Ferner and Small, worked on several statistical and technological approaches to a "Dudbuster." (S) NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine." (S) NSA CCH Series XII Z, Robert O. Ferner, "Rapid Analytic Machinery Needed for Research," June 3, 1943.

58. (TS//SI) NSA AHA ACC 13657, "G.C. & C.S. Naval SIGINT. Vol III, German Cryptographic Systems and Their Solution," 204.

59. (TS//SI) NSA CCH Series XII Z, copies of various MAC Outlines, circa 1953, MAC Outline # 12, "The Arlington Dudbuster."

60. (S) NSA CCH Series XII Z, Robert O. Ferner, "Rapid Analytic Machinery Needed for Research," June 3, 1943.

61. (TS//SI) NSA CCH Series XII Z, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 266. (TS) (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March, 1945.

62. (TS//SI) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 266.

63. (TS//SI) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years.

64. ~~(TS//SI)~~ NSA AHA ACC 13657, "G.C. & C. S. Naval SIGINT, Vol III, "German Cryptographic Systems and Their Solution."

65. (~~TS~~) (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March, 1945. ~~(S)~~ NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 52.

66. (U) NSA RAM File, Part II of Report to J. N. Wenger, Capt. USN, "Resume of the Dayton, Ohio Activity During World War II," and "History of NCML and OP-20-G-4E, June, 1944," "n530 bombes in operation."

67. ~~(TS)~~ NSA AHA ACC 35701 "History of the Bombe Project," 16 February 1946.

68. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12OO8) Navy Dept., Office of Chief of Naval Operations, DNC(OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944 [*sic*]. On Britain's request to SIS to build a Bombe and to build analog of the "G" machine, ~~(TS)~~ ASA CCH Series IV B, "History of ASA Equipment (Development Branch) History, December 1942," 30 June 1944, 42-44

69. ~~(TS//SI)~~ NSA CCH Series XII Z, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems." ~~(TS//SI)~~ NSA AHA ACC 16844. "History of the Special Projects Branch, SIS ETOUSA." ~~(S)~~ NSA CCH Series XII Z, "Cryptanalytic Report #2: The Yellow Machine," 44.

70. ~~(TS)~~ NSA AHA 35529, Friedman to Corderman, 29 March, 1944, "Comparison of our "003" type of "Bombe" with the rotary type."

71. ~~(S)~~ NSA CCH Series XII Z, Annual Reports, Development Branch, 1943-4.

72. (U) F. H. Hinsley, *British Intelligence in the Second World War, Volume I* (New York: Cambridge University Press, 1979), 58. NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problem," 15, 243, 269, 277.

73. (U) David J. Crawford, The Autoseritcher and the Superscritcher, forthcoming, *The Annals of the History of Computing* , NARA RG457, SRH-361, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 269-270.

74. ~~(TS//SI)~~ MAC Outline 30, MAC Outlines 103, SATYR. ~~(S)~~ NSA AHA ACC 26373, Chief, "F" Branch, "RAM Equipment," 29 March 1945. The first model of Satyr was built at Dayton in late 1944. Four additional models were made by the navy and the SIS group built its own version. All of them were quite direct analogs of the popular Hagelin machine. They even incorporated wheels from an actual Hagelin. Relays and plugboards eased the task of setting the machine.

75. ~~(S)~~ NSA CCH, G. O. Hayward "Operation Tunny: Deciphering German Teleprinter Traffic in WWII at Bletchley Park," 14 July 1989, Z/1396GW/9000/5, 9.

76. ~~(TS//SI)~~ NSA CCH Series XII Z, CNO, CIT Paper TS47, "Report on British Attack on FISH," Washington, May 1945. ~~(TS)~~ NSA CCH Series XII Z, "Fish'Dragon Notes," February 1945. ~~(TS//SI)~~ NSA CCH Series XII Z, "Fish Notes," 17 January 1945. ~~(TS//SI)~~ NSA CCH Series XII Z, "M.A.C. Outlines #21, Tunny Dragon."

77. ~~(TS//SI)~~ NSA CCH Series XII Z, "M.A.C. Outlines #21, Tunny Dragon."

78. ~~(TS//SI)~~ NSA CCH Series IV.W.I.5.13, "The History of OP-20-GYP-1, 1939-1945." The very serious and frightening blackouts caused by changes to Japanese systems, especially the trauma of fall 1944, are well described in ~~(TS//SI)~~ NSA CCH Series IV.W.1.25.12, "General History of OP-20-3-GYP," new Chapter III, espec. 24.

79. ~~(TS//SI)~~ NSA CCH Series IV.W.1.5.12, "History of OP-20-3-GYP," new Chapter III, 2.

80. ~~(TS//SI)~~ NSA L-5660 CCH Series IV.W.1.5.12, "General History of OP-20-3-GYP," Appendix 1, 5.

81. ~~(TS//SI)~~ Most of the following discussion refers only to the group that was based in Washington and which had a designation of GYP-1. ~~(TS//SI)~~ NSA CCH Series IV.W.1.6.8, S163287, "The History of GYP-1." The cryptanalytic or "Y" section of OP-20-G subdivided several times and its bureaucratic history is quite complex.

82. ~~(TS//SI)~~ NSA L-5660 CCH Series IV.W.1.5.12, General History of OP-20-3-GYP, Appendix 1, 7.

83. ~~(TS//SI)~~ NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," Ely memorandum 3 October 1942 and attached memoranda dating to 1 November 1943.

84. (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," 1 November 1943, "Further Remarks on the Proposed Clinical Attack." The quotations are from ibid., L. W. Parke, "Clinical Attack on Unknown Cipher System..." 23 October, 1943.

85. (U) Rear Admiral Edwin T. Layton, U. S. N. (Ret.) et al., *And I Was There: Pearl Harbor and Midway-Breaking the Secrets* (New York: William Morrow and Company, Inc., 1985), 409.

86. (U) There are some unconfirmed rumors that success was partially due to the theft of a codebook from a Japanese ship docked in San Francisco.

87. (~~TS//SI~~) NSA CCH Series IV.W.1.5.12., "General History of OP-20-3-GYP," new chpt. V, 6.

88. (~~TS/SI~~) Such problems may have led to the search for machines that would perform Slide Run type dictionary checks.

89. (~~TS//SI~~) NSA CCH Series IV.W.1.5.12., "General History of OP-20-3-GYP," new chpt. V, 6. "the significant reasons for this" [the JN39 error] "were three (experience with similar processes in JN 25 show that generalizations are feasible):...."

90. (~~TS//SI~~) NSA CCH Series XII Z, "General History of OP-20-3-GYP."

91. (~~TS//SI~~) "G" obtained a badly damaged copy of the machine in December 1944. NSA AHA ACC 17480 "Final Report, Project P123, Original J.N.157 Machine," February 1945, OP-20-G-4-D-3E.

92. (~~S~~) NSA CCH Series XII Z, H. H. Campaigne "Use of Hypo on the JN-157," 21 February 1944, gives an insight into how the general-purpose RAMs were employed to attack Jade. The Hypo was used to set the starting positions of Jade's three moving stepping switches. Jade had three moving stepping switches, two immobile ones, and a stecker. (~~TS//SI~~) NSA CCH Local Archive, "Army-Navy Descriptive Dictionary of Cryptologic Terms," Army Security Agency, February, 1947. A machine, Jasmine, whose details seem to have been lost, was built to test cribs against Jade. A very primitive electrical and stepping switch device, Mortor, was quickly constructed to allow hand testing of cribs to see if crib-plain pairs completed a circuit.

93. (~~TS//SI~~) The first Viper was proposed as soon as it was thought that Jade might be conquered. While it was being built, a handy but clumsy "bombe" for Jade was built, the Mortor. It was a cluster of stepping switches and wires to handtest menus to solve Jade settings. It would be replaced by the Rattler, a machine described below. (~~S~~) NSA CCH Series XII Z, "Viper, Plans for Construction of, Steinhardt, L. R.," 7 Sept. 1943.

94. (~~TS//SI~~) NSA CCH Series XII Z, "General History of OP-20-3-GYP."

95. (~~TS//SI~~) NSA CCH Series IV W.1.5.12, "General History of Op-20-3-GYP."

96. (~~TS//SI~~) NSA CCH Series IV. W.1.5.12, "General History of OP-20-3-GYP."

97. (~~TS//SI~~) NSA CCH Series XII Z, "History of (NAT) JNA20 CORAL," Vol. III, and NSA CCH IV.W.1.5.12, "General History of OP-20-3-GYP."

98. (~~TS//SI~~) NSA CCH Series XII Z, "General History of OP-20-3-GYP."

99. (~~TS//SI~~) NSA CCH Series XII Z, "History of JNA20 Coral (NAT) Volume IIII." 74.

100. (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," memorandum on "Personnel in GM-2," November 1943 indicates that some significant NAT busts were also discovered by new or inexperienced personnel. Busts were also important to the entry into JN157.

101. (~~TS//SI~~) NSA CCH Series IXW 1.5.12, "General History of OP-20-3-GYP."

102. (~~TS~~) S338 NSA CCH Series XII Z, L. R. Steinhardt, OP-20-G-4a-5, "A proposed form of Gypsy..." 13 Dec. 1944. NSA CCH XII Z, "Project M-312, Gypsy," 28 February 1945, NCA, Washington, DC.

103. (~~S~~) NSA CCH Series XII Z, "Viper, Plans for Construction of, Steinhardt, L. R.," 7 Sept. 1943.

104. (~~TS//SI~~) NSA AHA ACC 17480 "Final Report, Project P123, Original J.N.157 Machine," 28 February 1945, OP-20-G-4-D-3, 5.

105. (~~TS~~) NSA CCH Series XII Z, "Proposal for a Tape Reader on Gypsy," 2 April 1945.

106. (~~TS//SI~~) NSA CCH Series XII Z, CBO CIT Paper TS-31, "TOPAZ," Washington, December, 1945. (~~TS//SI~~) On the history of JN11, NSA CCH Series IV W.1.5.12, "General History of OP-20-3-GYP," new Chapter III, 20.

107. (S) NSA CCH Series XII Z, Inventories of RAM Equipment, 1945. The first TOPAZ seems to have been completed in March 1945. (TS) NSA CCH Series XII Z, CBO CIT Paper TS-31, "TOPAZ," Washington, December, 1945, 2. A smaller but similar machine, ASP, had an even shorter life in 1944, when the Japanese changed their callsign systems.

108. (S) NSA CCH Series XII Z, "Cryptanalytic Phases of Mamba," GM-2 6 April 1944. (S) NSA AHA ACC 26373, "Inventory of RAM Equipment," January 1945.

109. (TS//SI) NSA CCH Series XII Z, "Mamba." (TS//SI) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948. (S) NSA CCH Series XII Z, RAM list and Conference at Dayton, 11 April 1945. (S) NSA/CCH Series XII Z, "Cryptanalytic Phases of Mamba," GM-2 6 April 1944.

110. (TS//SI) NSA CCH Series IV.W.1.5.12, "General History of OP-20-3-GYP," Appendix 1, 7.

111. (TS//SI) NSA AHA ACC 543 "M.A.C. Outlines #4, Slide Run Machine."

112. (U) NSA, Lambros D. Callimahos and William F. Friedman, *Military Cryptanalysis, Part II*, NSA, 1959, 230-238.

113. (TS//SI) NSA CCH Series IV.W.I.5.13, "The History of OP-20-GYP-1, 1939-1945," 1, points out that the sum of the digits had to equal three. Divisibility meant without carry.

114. (TS//SI) OP-20-G did make some other early contributions. A theft of books had allowed it into the Japanese merchant ship systems from 1929 through the summer of 1941. With the experience gained from that, reentry into such systems began again during 1942. Throughout the war, the information from such systems, including those handled by SIS, proved of great significance to America's submarine fleet in the Pacific. See (TS//SI) NSA CCH IV.W.1.5.12, "General History of OP-20-3-GYP," new chpt. V, 4-5.

115. (U) Rear Admiral Edwin T. Layton, U. S. N. (Ret.) et al., *And I Was There: Pearl Harbor and Midway; Breaking the Secrets* (New York: William Morrow and Company, Inc.), 1985, 409.

116. (TS//SI) NSA CCH Series IV.W.1.5.12, "General History of OP-20-3-GYP."

117. (S) NSA CCH Series XII Z, L. R Steinhardt, "Additive Machines: Historical Summary of," 27 November 1944.

118. (TS) f[4233] f[4222].

119. (S) NSA CCH Series XII Z, L. R. Steinhardt, "Full-Selector," 31 October 1942.

120. (S) NSA CCH Series XII Z, OP-20-GM J. A. Skinner, "Proposal for a Decoding Device," 16 February 1942.

121. (S) NSA CCH Series XII Z, OP-20-G, "SSA Proposal for 70mm Film I. C. Machine," 8 June 1945 (TS//SI) NSA CCH Series XII Z, OP-20-G "Analysis of Analytical Machine Attack on JN-37," 24 March 1945. (TS//SI) NSA CCH Series XII Z, R. A. Rowley, "Preparation of Weighting Film, Secondary Stage Problem," Op-20-G, 2 August 1945. OP-20-G and the SIS would return to Eastman later in the war with proposals for sophisticated film-based machines. Two were turned into hardware by Eastman, the Amber and the 5202, before or close to the end of the war. They are discussed in the next chapter.

122. (S) NSA CCH Series XII Z, L. R. Steinhardt, "Additive Machines: Historical Summary of," 27 November 1944. (S) NSA AHA 1505, John N. Seaman, "Memorandum for Major Edgerton, Liaison with Navy # 3, Use of Ramon Jap Naval Problems of B II Type," 9 June 1944. Note that the Gray-NCR Comparator was also used on the JN25 problem. However, it performed the required tests very slowly. (S) NSA CCH Series XI E, Hagelin, Box 2, Folder, "Comparators."

123. (S) Steinhardt, L. H., "Copperhead II (Project M-230) Final Report," 9 November 1944. This a fascinating description of the proposed design. It was to have a long film tape with the text and additives run against each other. As they did so, the subtraction process would yield a "mask." The known groups would be on another long film. As its contents were projected against the mask, photocells would register how much light passed through. They would trigger electronic counters which, once reaching a threshold value, would indicate the position of hits.

124. (S) NSA CCH Series XII Z, L. R. Steinhardt, "Additive Machines: Historical Summary of," 27 November 1944, indicates that the NCR-built special desktop electromechanical machine was

a result of the "additive" problem design effort. Some sixty of those Mark IV or "fruit" or "Big Adam" machines were constructed. ~~(S)~~ NSA CCH Series XII Z, OP-20-G, "Additive Theory, Folder IV, Miscellaneous, Part A," 1942-43, gives details on a hand-held system using IBM cards (6,000 to a set) as stencils to visually identify divisible by three code-additive combinations. It also contains "G's" ideas for other types of additive machinery.

125. ~~(S)~~ NSA CCH Series XII Z, OP-20-GH-F, 13 November 1943, Steinhardt, L. R. "JN-25 Double Pentagraph High Speed Machine for Locating." ~~(S)~~ NSA CCH Series XII Z, OP-20-G, "Additive Theory, Folder IV, Miscellaneous, Part A," 1942-43, points out that Japanese errors frequently played a role in allowing "G" to recover enough additives to begin analysis. But it argues that with high-speed machinery, analysts would no longer have to depend upon them.

126. ~~(TS)~~ OP-20-G-4-A5, 23 November 1944, L. R. Steinhardt, "Possible Engineering Solutions for Full Selector Problems." ~~(TS//SI)~~ NSA CCH Series IV.W.1.5.12. "General History of OP-20-3-GYP," New Chpt. III, 18, 23. The JNII and JN25 crises also led to proposals for "quick-fix" mechanical devices, See ~~(TS)~~ NSA CCH Series XII Z, L. R. Steinhardt, "JN-11 (George Molecular Attack) Machine Aid For," 27 July 1945.

Chapter 6

(U) Beyond the Bombes and Beyond World War II

(U) Some of the cryptanalytic emergencies the British and Americans confronted pushed them to create machines that were close to being computers; at least the machines contained hints of the great potentials of electronic calculation. But despite the wish of many of the young army and navy electrical engineers to "show their stuff" and create the most advanced machines possible, the pace of innovation was determined by cryptanalytic needs rather than by electronic visions. "G" and "F" were arms of operational agencies, not research organizations. The two groups built some of the most complex electronic computing machines in the world during the war, but their duty was to solve problems rather than invent perfect automata. That led them away from serious consideration of either a universal programmable machine or a binary-based computer.

(U) Perhaps that was a wise decision. Those in America who had committed to an attempt to create universal machines saw their projects yield quickly outdated technological patchworks. For example, Vannevar Bush's Rockefeller Analyser was a conglomeration of electronic, electrical, and mechanical components that was put to rest soon after the war ended. The Harvard-IBM project under Howard Aiken depended upon the craftsman's art of combining IBM card-reading equipment, relays, pulleys, and shafts. Even the wartime project at the University of Pennsylvania, which began with a commitment to the use of electronics, ended with a batch of special-purpose calculation boxes linked by huge cables rather than by a software program. None of the grand attempts created the ultra-high-speed and full universal machines that had been hoped for.

(U) Although OP-20-G and the SIS did not aim for the great prize of a single computer for every function, they achieved a great deal. By the time Japan surrendered, the Americans were building electronic machines using twice as many tubes as the British Colossus. The advances in electronics at the cryptanalytic centers were amazing. But in several ways the Americans' achievements were limited. The cryptanalytic problems they solved with digital electronics were not memory dependent, and some of the new electronic machines they built were based on very clever ways to make analog technology imitate digital methods. And the new machines were not true data processors. Although the navy had its Copperheads and Comparators, large files remained in the domain of the tabulators and sorters.

(U) After the Bombe

(U) In late 1943, just as the first OP-20-G and SIS Bombes were being completed, another stage in the development of cryptanalytic machines began. Both American engineering groups returned to a consideration of digital electronics. At the same time, they began to pay attention to the Japanese problems.

(U) The war in the Pacific was an American show, and the cryptanalytic work was not cluttered with the kind of difficulties that complicated the European relationships. OP-20-G and SIS had much more freedom, and the British were more cooperative. Despite the greater independence, the Pacific never received as much attention from OP-20-G's and SIS's machine builders as did the Atlantic. There was no crash program to develop expensive devices to conquer the Japanese code and cipher systems. However, the engineers in Washington and Dayton put a great deal of work into solving problems for the cryptanalysts assigned to the Asian traffic.

(U) Most of the work on special machines for the war against Japan was done in OP-20-G. And much of that was directed by one of Vannevar Bush's ex-students, Lawrence Steinhardt. He had been left in Washington during 1942 and 1943 to design what became the Copperhead tape scanning systems and to start building very advanced analogs of several different Japanese encryption machines. He was also charged with the responsibility for the machines for all major Japanese code systems.

(U) Every Which Way: The Code Challenge Continues

(U) The Japanese additive code problems challenged OP-20-G's capabilities throughout the war. But there were moments of urgency that led to bursts of activity with the army's and navy's engineering groups. In mid-1944, when there were signs that Japan might begin yet another series of alterations that might close its most important systems to the Allies, "G" intensified its search for methods and machines. Lawrence Steinhardt was again detailed to seek out technological solutions. What he recommended indicates how deeply code solutions had become dependent on massive data processing.

~~(TS//SI)~~ The cryptanalysts had no easy ways to solve code and additive systems. Even the most advanced methods of the time demanded tens of millions of tests and massive amounts of memory. Probable additives had to be stripped, the results run against a large dictionary, and a judgment made as to whether a true code group had been recovered. Then meaning had to be attached to the clear code. There were no great mathematical shortcuts for codebreakers. Even the most efficient methods called for exceptional amounts of labor, or powerful machines, ones that did not exist in 1944.

~~(TS//SI)~~ If "G" wanted a machine that could go beyond the army's tabulator-relay Slide Run, it would have to ask its engineers to stretch the limits of computing technology. Mass memory was the key. Lawrence Steinhardt realized that. After consulting with the OP-20-G cryptanalysts about what new methods they wished to implement, he returned to his superiors with an estimate of the probable cost for a code machine. It was high. But he was told that his proposed expenditure of $500,000 would be acceptable. That was one-half of what Madame X had cost and the price of eleven Bombes. But a solution to problems such as JN25 was worth many millions of dollars.

~~(TS//SI)~~ Steinhardt began a survey of technical possibilities for a machine that would allow "G" to employ its various new and more powerful versions of the additive stripping/high frequency tests or, if desired, the Jeeping method. This time he did not even bother to determine if film or even punch tape systems were "memory" possibilities. The sour experience with the earlier Copperheads and the delays in the Eastman Kodak film-based code device effort led him to explore other alternatives for the critical high-speed mass memory called for by the cryptomethods.

~~(TS//SI)~~ Steinhardt evaluated all the technologies used by aspiring computer builders, including some that would become integral parts of the first modern computers. He did not discover any ready-made solutions to the high-speed memory problem, however. Nor could he find an easy solution to the challenge of constructing the switching system needed to select memory elements. His frustrations grew when "G's" cryptanalysts asked him to focus on a particular problem and to turn one of their most demanding methods into hardware. They asked him to design and construct a machine to attack JN25 and to do it within a few weeks.

~~(TS//SI)~~ The machine the cryptanalysts dreamed about for the JN25 code problems was an ambitious one. What was later called the "Selector" was to read at least 100 enciphered five-digit code groups at a time, rapidly subtract

either additives or another set of codes, check for divisibility, and then perform the critical step: compare the resulting clear groups with a list of scientifically weighted code groups[1] (100,000 of them) and calculate whether or not a statistical threshold had been reached.[2] If the combined "weight" scores for the matched groups summed to or exceeded a specified level, then the device would signal that true additives might have been found.

(~~TS//SI~~) A critical part of the required machine was a method of quickly changing the scores associated with the "dictionary" of code groups. The cryptanalysts wanted to modify the scores as they learned more about the system or when they desired to switch the machine from a weighted frequency to a Jeeping mode.

(~~TS~~) With those requirements in mind, Steinhardt called upon his past experience at MIT, talked with his contacts on World War II computer projects, such as the one at Harvard, and reviewed what he had learned on earlier OP-20-G assignments.

(~~TS~~) One of the first options he explored was for what seemed a wild scheme for a fast memory. Although it had first been proposed as an alternative to the commutators used on the Bombes, the option was soon recognized as a significant "memory" possibility. It was a primitive version of what later came to be called the electrostatic storage tube, a television-like device that used a charged spot to hold a "bit" of information.[3]

(~~S~~) To follow up on the idea, in 1944 "M" had begun exploring the possibilities of a modified oscilloscope. Its beam would be electronically deflected to any one of several hundred spots on its face; then small metal patches pasted on the face of its screen could sense which "bits" were active.[4]

(~~S~~) By November Steinhardt decided that he had learned enough about the "scope" and other technological possibilities and that he had to begin construction of a machine. He drew up a list of recommendations. He reported on six possibilities for a machine for JN25 and its relatives, ranking them in terms of the probability they could be finished in time to meet the Japanese code emergencies.

(U) The Navy's Madame X – the Strangest Selector

(~~S~~) Although Steinhardt's report mentioned some very advanced alternatives, such as the oscilloscope memory, it argued for the use of conservative technologies and architectures. They could "get the job done" and quickly so. As far as the cryptanalytic requirements would allow, Steinhardt wanted to use sure-fire parts and analog circuitry, but in a unique combination.

(~~S~~) Steinhardt proposed a "telephone exchange" version of a new type of "Selector." The first of Steinhardt's recommendations was for the use of a technology the SIS had used in some of its machines, including Madame X, the new crossbar relays. With them, Steinhardt's proposed Selector had the potential to become one of the most powerful machines "G" or any other computer organization ever built.

(~~S~~) Steinhardt knew about the telephone company's advanced relays before he went to OP-20-G. The late 1930s Differential Analyser project at MIT had used some of the "crossbar" systems the Bell engineers had developed for their switching centers. All the young MIT engineers had learned of impressive logical powers of the "bars."

(~~S~~) The crossbars were miniature switching stations. A crossbar may be thought of as a square array of ten horizontal and ten vertical input positions. The appropriate output is selected at the intersection of the input positions. If crossbars were hooked together, they became powerful

selectors of electrical pathways. When two crossbars were connected in tandem, they could trigger the selection of one out of 10,000 switching paths and do it very rapidly.

~~(S)~~ Steinhardt applied his knowledge of crossbars to the code-to-dictionary phase of additive testing. He realized that with the addition of ten small relays to a tandem setup of two crossbars, a five-digit code could be translated, almost instantly, to the electrical "address" of any one of 100,000 locations. If the locations contained code groups' "weights," he reasoned, a rapid test for high-frequency groups might be performed.

~~(S)~~ His creativity led him much further, to the outline of a unique memory search methodology. He thought of a way to do what was, for the time, massively parallel "look-ups." He proposed that 100 of the crossbar-relay combinations be linked together. That would allow 100 code groups to simultaneously link to their frequency "weights." It was a brilliant concept. His new Selector would be a parallel processor.

~~(S)~~ The crossbar provided the basis for a very reliable and fast digital memory Selector. But Steinhardt also had to find a practical way to match calculation speed to the rapid memory search. After examining electronic digital methods of summing weights and performing threshold tests for the detection of statistically "good" code groups, he concluded that the most efficient approach was to return to the use of analog methods and equipment.

(U) A Wall of Knobs

~~(S)~~ The cryptanalytical method for the additive code systems dictated a digital switching system to find locations of values, but it did not require a digital memory. Taking hold of that opportunity to simplify his machine, Steinhardt turned to an extension of previous ideas for building high-speed memories. Electrical components had been suggested as means of holding constant values in digital form for input for calculations in various early precomputers. The army's Freak had tried to go beyond that, employing a two-state version based on condensers to act as a dynamic digital memory. That had been an ambitious and none-too-happy exercise, however.

~~(S)~~ When Steinhardt estimated the number of components that would be required by a digital memory for the weights for 100,000 code groups, he correctly decided to retreat to an analog memory. If he had chosen an approach like that in Freak to store values as on-off representations of numbers, the components for the code Selector's memory would total to the millions. To avoid that, he proposed an alternative that reduced engineering demands. But even his clever alternative called for a heroic and complex machine.

~~(S)~~ The Selector "memory" was to be a set of 100,000 variable resistors, each with an external knob which was to be used to set the electrical "weight" for a code group. Using resistors reduced the number of components; only one resistor would be needed for each memory location. But even with one component per memory location, the memory would be an engineering challenge. The banks of resistors and knobs would have to stretch across a large room, reaching up to its ceiling.

~~(S)~~ Steinhardt's proposed resistor memory would be fast. But, given the amount of available time and manpower, Steinhardt did not plan to make it satisfy one of the cryptanalysts' important specifications. It was not to be made fully automatic. It would require a great deal of man-and-woman-power to set the "weights." Whenever a problem changed or when the cryptanalysts revised their list of weights, the memory would have to be "programmed" by resetting the 100,000 dials.

~~(S)~~ When Steinhardt first described the proposed machine option and the need to set the memory's values by hand, his superiors hesitated.

Steinhardt admitted that it would take a crew of twenty WAVES a full duty watch to reset all the resistors. But, he argued, given the comparative speed and ease of construction of a resistor memory, the eight- to ten-hour wait before a new problem could be attacked was reasonable. Given the operating speed of the new Selector, a ten-hour setup time still left his machine with a major advantage over any other method of additive attack.[5]

~~(S)~~ Steinhardt's crossbar-resistor design included another way of avoiding the size and complexity of digital electronics. The "arithmetic" of the machine's "frequency check" was to be analog, like the IC plate machine. One hundred values would be sent in parallel to a circuit that tested electrical values for "enough," not how many.

~~(TS//SI)~~ The simplicity of the analog arithmetic circuits helped make the proposed crossbar machine quite fast and made its construction seem feasible. If the machine was set to test for only the weights and not strip the additives, Steinhardt explained, 18,000 of the 100-group tests could be performed in an hour. That was quite an advance over the army's Slide Run machine and the navy's NC4. And, Steinhardt argued, the machine could be in operation within less than a year because it was based on known technologies.[6] But he also wanted "G" to consider other options.

(U) Walls of Tubes

~~(S)~~ An inherently more attractive alternative, especially to a young electrical engineer, was to rely upon electronics. Electronic tubes, whether gas-filled or vacuum, were orders faster than any other digital technology of the time. Although Steinhardt believed that standard tubes could not be used for the Selector's memory, he thought they might be a possibility for the switching (selection) process. Therefore, his second design option for a JN code machine had electronic switching, but retained the huge resistor "electrical" memory.

~~(S)~~ As part of the JN25 project, Howard Engstrom had asked other "M" engineers to help Steinhardt by making another thorough investigation of the possibilities of electronic circuits. With an eye on the potential for finally creating an electronic Bombe, as well as building machines for the "weighting" attack, new tube technologies and circuit designs were examined.

~~(S)~~ What they reported was not good. The first depressing news was about the possibility of building an electronic wheel. The report on an electronic matrix which could act as a substitute for the Bombe commutators contained a bleak conclusion. With the two most reliable digital circuit designs and standard hardware, a twenty-six by twenty-six matrix demanded over 1,000 tubes. The engineers also reported little hope for multifunction tubes. The many projects on radically new designs had not led to vast improvements. The available special tubes and circuits, such as the strobotron and Duenna circuits, still called for over 500 tubes per matrix. As a result, they reported that an electronic selection matrix seemed an improbability.

~~(S)~~ The number of tubes and the likely maintenance problems seemed so great that "M's" tube experts again turned away from digital electronics. They thought they had little chance to build an electronic Bombe before the war was concluded, and they had similar thoughts about the chances for an electronic JN25 machine.

~~(S)~~ They recommended another analog solution. They pointed to an esoteric "frequency conversion" circuit as an alternative to the on-off digital designs.[7]

~~(S)~~ Lawrence Steinhardt did his own review of digital possibilities before giving the "frequency conversion" idea serious consideration. He put the electronic matrix report together with his past

experience and weighed the advantages of electronic switching for the JN code problem. He did not like the results of his review, but he had to accept them.

~~(S)~~ His first disappointment was over the speed of electronics. He found that if he used a single matrix of tubes instead of the set of 100 crossbars for switching and selection of weights, the electronic machine would be only twice as fast as the electric design. It would have to cycle so many times to find a correct pathway in the memory that its advantage in raw speed would be vastly reduced. Of course, if the single tube matrix was replaced with, as in the crossbar design, 100 matrices, the electronics would make the machine perform not 3,600 tests per hour, but over 3,000,000.

~~(S)~~ That made an electronic selector very attractive. But such an advanced machine would need more than 100,000 tubes. Steinhardt realized that was too much to ask in the mid-1940s. Tube failures were too frequent. Based on the average life of standard tubes of the time, Steinhardt calculated that under the best conditions ten tubes would cease functioning every hour; by the time they were located and replaced, at least three more would go bad. That made the full electronic switch design for the proposed Selector unacceptable.

~~(S)~~ Steinhardt's concerns about tubes were based upon more than theoretical calculations. He had direct experience. He had worked with digital electronics at MIT and on the Duenna project at "G." [8] The Duenna project had led the navy's engineers to many insights on how to extend tube life. But even with the knowledge that most failures were caused by turning tube machines on and off, Steinhardt believed that unless very special types of tubes with extra long life were developed, 3,000 tubes were the limit for an operational machine. And he quite correctly saw little chance that either long life or sufficiently complex multifunction tubes could be developed in time to fight the Pacific code war.[9]

(U) Into the Beyond and the Past, Rooms of Wires and Disks

~~(S)~~ As a result of the disappointments with electronics, Steinhardt took another look at older technologies. His survey made him more than a bit pessimistic about building any type of Selector. He had encountered some discouraging facts about the use of the most reliable of technologies, standard relays. When he had calculated how many relays would be needed to select and test the required 100 code groups simultaneously, he was overwhelmed. Still envisioning the machine's memory as the collection of 100,000 resistors and their knobs, he concluded that even more relays than electronic tubes would be needed for the selecting system.

~~(S)~~ A "prohibitive" number would be required and maintenance of such a machine, he reported, would be as much of a chore as keeping Madame X running.

(U) Desperate Options and a Conservative Selector

~~(S)~~ Although Steinhardt would eventually recommend the use of crossbars and resistors, that alternative was not really attractive to him. The thought of 100,000 resistors for the Selector's memory was especially troubling. So he asked other engineers at OP-20-G and NCR to explore additional possibilities. Some of the recommended alternatives approached the bizarre.

~~(S)~~ There were last-gasp attempts to reintroduce microfilm memory and suggestions for optically read glass disks.[10]

~~(S)~~ There was also a brief revival of the idea of turning automobile parts into computers. While the commutators on the Bombes were distant relatives of distributors, the idea for the JN25

machine suggested a much closer relationship between computers and automobile electrical systems. It was possible, some engineers said, to create a high-speed switching system (500 operations per second) using ignition distributor technology.[11]

~~(S)~~ That suggestion does not seem to have been taken too seriously by Steinhardt. But another one that seemed to be as far-fetched did capture his attention. A young "G" engineer, Lieutenant Noble, responded with an idea that became the seed of one the most advanced and unusual research projects "G" undertook during the war.

~~(S)~~ Noble's idea centered upon the new and relatively untried technology of digital magnetic recording. OP-20-G had magnetic wire recorders that were used to copy the most important analog intercepts. Noble believed he could coax them into becoming the basis for a mass digital memory.

~~(S)~~ He thought his proposed magnetic wire scanning devices could overcome the problems encountered with other moving media such as microfilm. To provide information at rates matching electronics, they all required such high transport speeds that they could not be precisely sensed. Despite all sorts of experiments, film, disk, and tape transport systems remained relatively slow and problematic.

~~(S)~~ Noble, however, thought that he had found a solution, at least for wire recording. He thought he could line up one hundred of his relatively small wire recording devices in such a way that sensing difficulties would be avoided. In his plan, two of the differenced code digits would cause the switching system to select the correct recorder; then a sensor would select the correct weight as the recorder cycled through its 1,000 values. Because each magnetic recorder held a few densely packed entries, processing would be very speedy. Resetting weights would be painless because the magnetic wires, Noble stated, could be interchanged.[12]

~~(S)~~ Fortunately, Steinhardt was not forced to immediately choose among the many technological alternatives for the Selector. The JN25 problem had eased somewhat. In addition, the mathematicians at "M" found it impossible to agree on which of their complex weighting schemes should be employed. As a result, operational cryptanalytic attention shifted to other high-level Japanese naval systems. That allowed Steinhardt's team to avoid making any hasty technological decisions.

~~(TS//SI)~~ However, they and the cryptanalysts decided to begin to build a experimental version of a new Selector. It was to be a limited four-digit version, almost a bread-board model. The four-digit version vastly reduced the potential power and speed of the device and made it unsuitable for a JN25 attack. But it reduced the number of required components. That made the use of the inexpensive and reliable simple relays practical.[13]

~~(S)~~ The search for a high-speed Selector was not ended, however. JN25 and the intellectual challenge of the Selector problem had captured the attention of many at OP-20-G, including Howard Engstrom. He gave the green light to two very adventurous projects. Both tried to push existing technologies far beyond their limits in an attempt to find the high-speed memory and circuitry that an operational Full (five-digit) Selector would need.[14]

(U) Walls of Pipes and Thousands of Dots

(U) The development of radar during World War II had led to a very unusual memory device, the acoustic or "sonic" delay line. The delay line's job was to hold and recycle signals so that a radar operator's display screen could have refreshed and stable images. The "lines" were tubes filled with chemicals. At each end of the tube was a transducer. An incoming electrical signal was transformed into a pulse within the tube. The

transducer at the end of the tube changed the pulse back into an electrical signal. The chemical medium within the tube, typically mercury, circulated while holding the data pulses.

(U) Unfortunately, delay lines could hold only moderate amounts of data; they were very temperamental about the amount of heat they were exposed to; and much about their behavior remained a mystery. But they presented data at rates several orders faster than other media of the era.[15]

~~(S)~~ Howard Engstrom, still in search of a capable machine for the Japanese codes, had decided to take some great chances. With Enigma and the Fish machines under control, he determined it was safe to assign some of his most valuable men to work on a delay-line Selector.

~~(S)~~ One of the rooms at "G's" Nebraska Avenue center soon had a very strange appearance. A box full of electronics stood in front of a wall of metal tubes. The young naval engineers spent weeks trying to gather the electronic switching system, the chemical delay lines, and the prototype calculating units into a functioning machine.

~~(S)~~ While the group in Washington was on its adventure, something more technically courageous was taking place within the secret rooms of the NCML in Dayton. Two of "M's" brightest engineers had been allowed to work on a very special version of the Selector when they were not busy with emergencies. Ralph Palmer, the engineer from IBM who later played a critical role in its computer history, led a team that was attempting to build a magnetic memory and advanced photo-optical Selector.[16]

~~(S)~~ The Palmer-Reid Selector seems a very strange contraption today, but in the mid-1940s their prototype was seen by visitors to Dayton as an exciting alternative, partially because it was another attempt to develop and apply electrostatic memory. Their Oscillograph Full Selector had the potential to become one of the most powerful and fastest of all the RAM machines.

~~(S)~~ Their Selector was to consist of 100 magnetic disks (a technology yet to be born), electronic circuitry, a heat-sensitive printing system, and ten very special oscilloscopes. The disks were to be divided into two sets of fifty each, one set for possible additives and the other for message text. One hundred groups would be on each message disk. The two sets of disks were to spin in synchrony, then be offset to accomplish a full overlap test. Advanced electronic circuitry would difference the two data streams and then select one of the ten oscilloscopes. Those ten "memories" were to hold the 100,000 code weight entries.[17]

~~(S)~~ The electronic circuits of "Palmer's special project" would, through a coordinate system, select one of the 10,000 spots on the face of the proper oscilloscope, then turn processing over to an analog system.

~~(S)~~ The electrostatic storage was to be very smart. Each of the screen's dots was to have one of a number of possible densities representing the assigned weight for each code group. To register a score, the oscilloscope was then to be imaged onto a photographic mask. The amount of light passing through the mask would be proportional to the code's weight. A photocell system would sense the amount of light and then throw a particular amount of current to a condenser. When all the groups in an overlap had been tested, the amount of charge on the condenser would serve as a measure of the probability that correct additives had been located.

~~(S)~~ Another subsystem in Palmer's Selector was to be used to dump a charge onto a "master" condenser and, at the same time, 200 others. Each of those 200 was a "memory" for the goodness of each of the possible overlap tests. The amount of the charge on each of the condensers would determine how long its particular associat-

ed printing head would rest on the teledotos paper in the Selector's printer. The greater the charge, the longer the print line.

(S) Palmer did not complete his machine before he returned to IBM to lead many of its computer projects, including its magnetic "tape processing" developments. But his Selector project was not wasted. His experiments with magnetic disks provided a basis for the navy's pivotal magnetic recording development projects after the war.

(U) The Relay Selector Gets an Electronic Face Lift

(TS) While the delay line and oscilloscope designs were being drafted, the final design and construction phases of the safe-and-sure simple relay Selector continued. But as the machine's design progressed, the commitment to a pure relay technology or to relay switching with a resistor memory dissolved. The engineers wanted to experiment, and they were allowed to do so as the Pacific war was ending. The Selector became a conglomeration of old and new technologies. Within a few years after the war, it had grown to be, like Madame X, a room full of relay banks and plugboards, but it had a special addition, digital electronic components.

(TS) The shift to the use of some digital electronics came as a result of an increased trust in the technology and a realization that a pure relay machine would be too slow. But the Mercury Full Selector of June 1945 was neither a showpiece electronic device nor an example of advanced engineering imagination. Mercury did move away from analog calculation, but it was relatively slow, and it continued in the OP-20-G tradition of using the least resistant technological combinations. However, it was hoped that the machine and the cryptanalytic method it embodied would justify building a fully electronic version.[18]

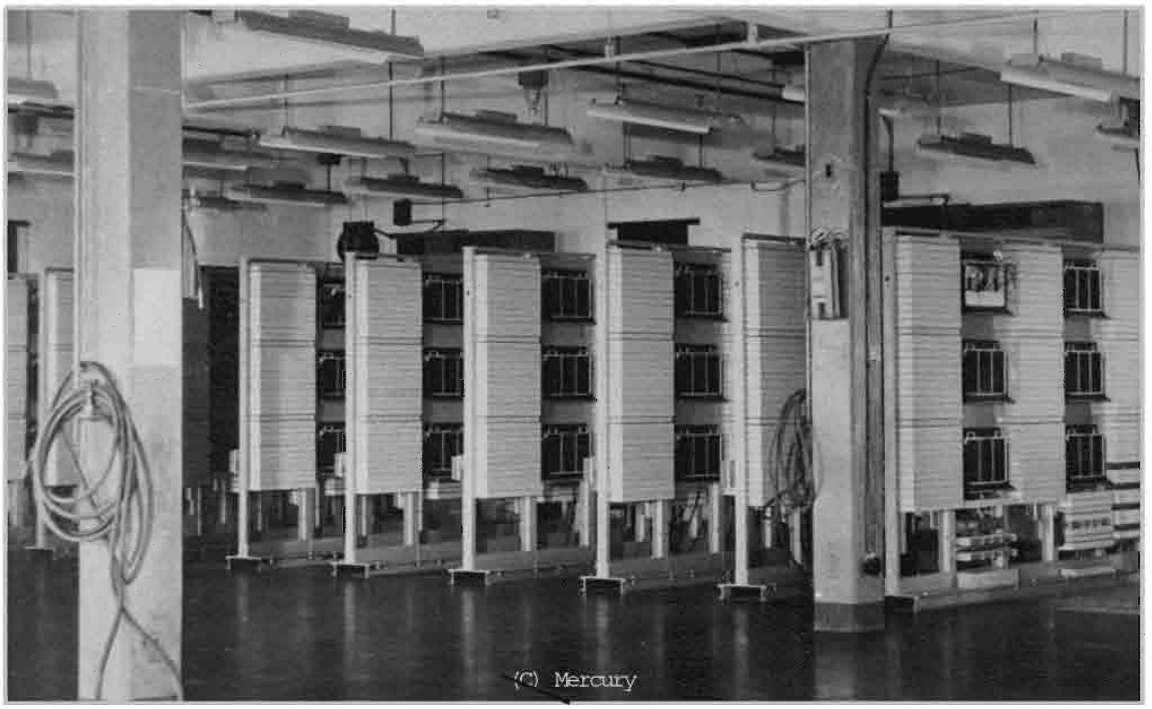
(TS//SI) When Mercury first appeared, it was a quite impressive seven-foot high by fourteen-foot-long bank of relays that was served by two cabinets of electronics. It grew even larger. Within a few years it approached the size of Madame X. Its expansion was due to postwar operational cryptanalytic needs and the continued reluctance to build an electronic code Selector. The number of Mercury's relay banks was increased tenfold in order to turn it back into a five-digit machine and to expand its dictionary of stored code weights to the required 100,000 values.

(TS//SI) The front end of the mid-1945 Selector was quite conventional. An IBM collating machine with its two card readers was the input device. Code and possible additive were read in simultaneously, one value on each card plus an identification sequence. The readers were not exceptionally fast. In fact, descriptions of the machine bemoaned the Selector's slowness because of the low speed of the collator.

(TS//SI) The next part of the machine was a bit more innovative, but it was a mixture of the old and new. The pulses from the card reader were passed to eighty gas-filled tubes. But they were connected to a small relay matrix that was, in turn, connected to familiar plugboard matrices. They were called upon when false addition or subtraction was needed for additive stripping.

(TS//SI) The number that emerged from the plugboard then entered a tree-like structure of some 1,000 relays. That was the "selector" in the system. The relay system then passed the code value to a true technology throwback, a bank of plugboards with 10,000 entry points. The plugboard banks were Mercury's "memory."

(TS//SI) Each of those points was in turn connected by a plug wire to one of twenty "weight" relays. Every time the profile of weights changed, the engineers had to rewire those connections. Each known code group had a value from zero to



nineteen associated with it. Despite some tricks that reduced the number of code values that had to be plugged in, the change of wiring was a massive job that took several days of effort. Perhaps the difficulty of the plugging was one reason why the 1945 Mercury was restricted to a memory of only ten thousand "weights." But the replugging was probably less time-consuming overall than trying to maintain and change a condenser type of memory.[19]

(~~TS//SI~~) Some parts of Mercury were technologically up to date. After the weights left the relays, Mercury began to be something of an electronic digital processor. Inside one of its cabinets was a large electronic ring counter (something quite like what Bush had used in his Comparator) that summed the digital values that were "selected" by the suspected plain codes. Next to that counter was another one quite like it, but the "threshold" digital electronic component was unusual for a "G" machine. With the aid of a plugboard and a rotary switch, the second ring counter could calculate a simple regression equation ($Y = a + bx$). The resulting value, which changed as each card was read, served as a benchmark for a test of significance of the accumulated weights. The parameters of the equation were usually set to the average weight value of accumulated messages.[20]

(~~TS//SI~~) A third set of electronic tubes, called the "overlap counter," counted the number of weights sent to the accumulator during a run.[21]

(~~TS//SI~~) When the electronic evaluation unit that stood between the accumulator, the overlap counter, and the regression unit was activated (it could be set to check the results after every card was read), Mercury became a "smart" machine. The machine itself decided what was or was not a set of probable additives. If the accumulator-overlap balance did not match the value in the comparison unit, no results would be printed. The machine might also be ordered to automati-

cally run a new set of cards that had been stacked in back of the first deck.[22]

~~(TS//SI)~~ The postwar Mercury, although an ugly kludge, proved useful to the navy for almost half a decade. It was used for cipher vs cipher attacks and was even coaxed into becoming a version of the old Gee Whizzer. It could be made to test for the frequency of digraphs and thus give insights into transposition systems.[23]

(U) The Biggest Snakes of All – The Navy Almost Builds an Electronic Bombe

(U) While the "M" group at OP-20-G continued to search for machines to breach the Japanese code systems in 1944 and 1945, they and Friedman's crew had to respond to new challenges posed by the enciphering machines of the Axis powers. Germany threw the most curves at the cryptanalysts in Washington, but the Japanese also made changes in their systems that led to a search for new RAM.

(U) The complex analogs of the Japanese cipher machines that "G" constructed during 1943 had proved very helpful, but they were not analytic machines. They essentially were decryptors, machines to be used after a system had been solved. The cryptanalysts wanted more: a machine to attack the systems, especially the JN157 enciphering device, Jade.

~~(TS//SI)~~ Busts and other operator errors had led to a general knowledge of the machine, to the ability to guess daily "wheel" orders and stecker settings, and, by late 1943, even to the discovery of the wiring of its stepping switches.

~~(TS//SI)~~ All that presented a tantalizing opportunity for analysts such as Frank Raven and Lieutenant Braun, but also frustration. They still had to find the starting positions of the important parts of the machine in order to read the Jade messages. The task was formidable. In its worst moments "G" thought it might have to explore as many as 10,000,000 to 30,000,000 possibilities for each daily "system" even though its attack was based upon cribbing.[24]

~~(TS//SI)~~ That demanded too much of the tabulators, even of the NC machines. So Lawrence Steinhardt was asked to devise a "Grenade" for the Japanese cipher machines, or at least one for the stubborn JN157.

(U) He quickly chose a name for the proposed machine. He called it "Rattler." But it took some time before the architecture and hardware of Rattler were selected. There were many twists and turns before Rattler became an electronic version of a "bombe," at least a bombe for the Japanese stepping-switch problems.

~~(TS//SI)~~ Because of the pressure to deliver a machine as soon as possible, Steinhardt at first wanted the NCR group assigned to build Rattler to use standard technologies. He wrote Joe Desch in early 1944 recommending that Rattler was to be "entirely nonoptical and non-electronic in character." Although it was to have old-fashioned components, Steinhardt thought it could perform the required minimum of 10,000,000 tests within eleven minutes.[25] Calling on in-hand technology had a greater benefit. By using the electromechanical stepping switches from Viper and some relays and plugboards, Steinhardt thought a Rattler that tested a short crib against cipher could be in operation within three weeks.

(U) But some disadvantages to using old components surfaced and the construction of Rattler was delayed. The drawback to the first proposal was that it called for the coordination of 108 electromechanical stepping switches. Joe Desch thought that a bit too much too ask. He also wondered if the stepping switches could be made to work as fast as Steinhardt imagined. After reviewing the first design with Desch, Steinhardt also had doubts. So he approved delaying the project while other options were explored.

(U) After two very tension-filled days, Steinhardt presented another design. It was even more committed to old, trustworthy technology.[26] Steinhardt's second design was also driven by the need to deliver a machine to the cryptanalysts within a few weeks.

(U) He had thought of a handy alternative to the stepping switches. As a substitute for at least some of them, Steinhardt suggested that Desch develop what Howard Aiken had used on his Harvard-IBM protocomputer, a very high-speed tape version of the IBM card.

(U) Using the uncut IBM paper stock as the input medium and six slightly modified versions of the readers from IBM sorting machines, it would be possible, Steinhardt claimed, to eliminate most of the stepping switches and perform the crib tests in perhaps half the time the first design required. The six input tapes would be representations of the letter developments of the crib letters.

(U) Joe Desch considered the second proposal and quickly responded with a long list of objections and alternatives. As a result, the Rattler became something much more technically advanced than anyone had imagined a few weeks before. But as a result of Desch's recommendations, it took an additional half year to turn Rattler into an operational machine.

(U) The Rattler that emerged was very, very different from Steinhardt's early conceptions. Rattler became one of the most advanced electronic machines of the SIGINT war. The necessity for speed drove Steinhardt and Desch to take the risk of relying on electronics.

(U) The electronics needed for the JN157 problem was much less demanding than for the Enigma, however. The critical component of Japan's Jade machine was a telephone stepping switch which had, at most, twenty-six possible positions. Its electronic analog needed the same number of "positions." An Enigma wheel was a much more complex mechanism to imitate. To mimic it called for a matrix of over 670 "positions" and allied circuits. That meant approximately 1,000 tubes to imitate an "E" commutator.

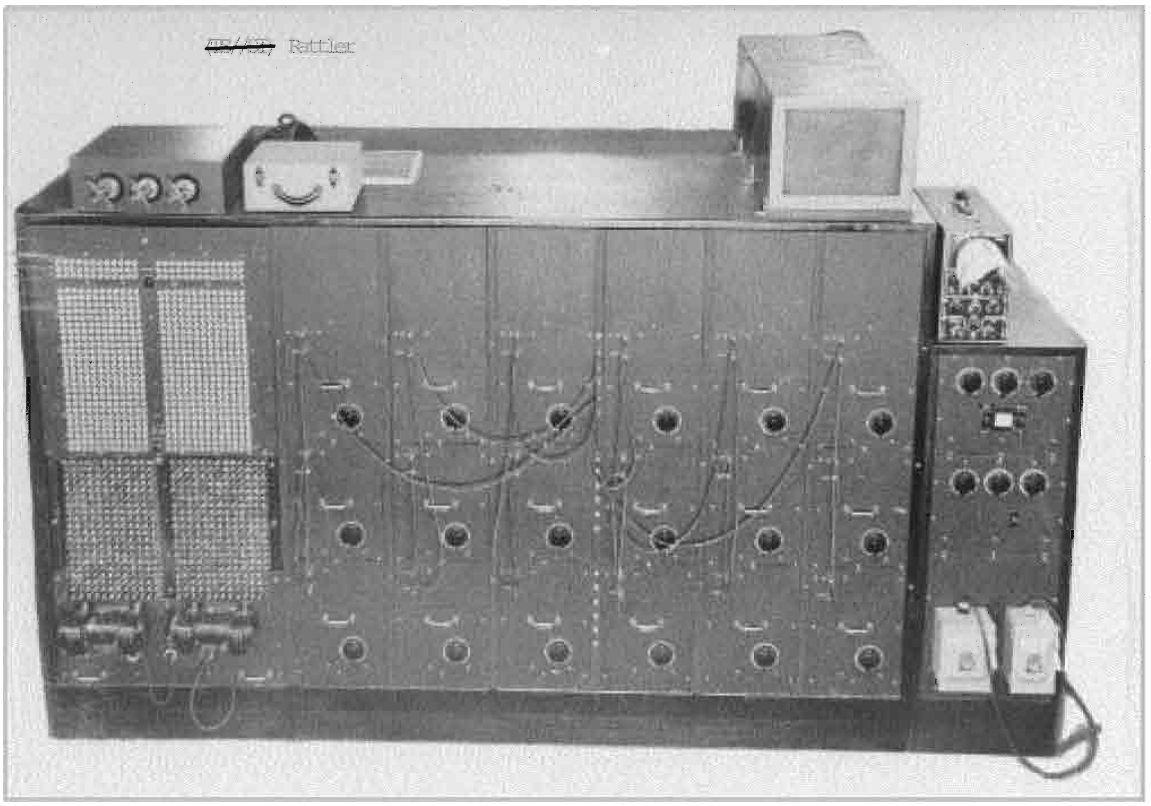
(~~TS//SI~~) The limited number of tubes needed to imitate a stepping switch allowed Desch and Steinhardt to think that an electronic Jade "bombe" was a possibility. With faith in their ability to build electronic "rings" because of their previous work on the counting circuits of the Comparators, they began to design a minimal version of an electronic crib tester. Electronics was used where essential, but some of the oldest technologies were incorporated when they proved most efficient.

(~~TS//SI~~) The Rattler that appeared in May 1944 was an electronic stepping-switch version of a very, very fast crib testing bombe. But it was limited in function, as were the Enigma Bombe's Grenades. In addition to demanding a known wheel order, Rattler needed to be told what "stecker" had been used. It did not have a diagonal board test as did the Bombes.

(U) Rattler had at least 1,000 tubes. Its heart was six banks of electronic stepping switches (ring counters) which were analogs of the electromechanical versions used by the Japanese. There was another electronic component, the large cabinet of detector circuitry used to identify a hit.

(~~TS//SI~~) A huge bank of lights allowed the machine's operator to see the positions of the various stepping switches when crib matched cipher text.[27] Rattler had other technological throwbacks. The electronic switches fed into banks of relays, and much of the setup of the machine was done through rows of plugboards. Twenty-five of them were used for the final "switching" function of the two "fixed" steppers in Jade.

(U) Rattler was a technical and operational success. It was able to run through all the posi-



tions of the switches and test for a crib-cipher match in ten minutes. It proved so valuable that a second model was built and modifications soon allowed Rattler to be used to attack other Japanese cipher machine systems.

(U) But Rattler did not turn out to be as small as Lawrence Steinhardt had promised. In fact, it was a giant; it was seven feet high and nine feet long.[28] However, it was puny when compared to two other machines Lawrence Steinhardt began to pursue during late 1944.

(U) The Serpent and Friends

(U) Lawrence Steinhardt had been frustrated throughout the war by having to continually react to emergencies. He became tired of hastily building machines he saw as crypto and engineering compromises. Like his ex-mentor, Vannevar Bush, he felt that the navy should have a stock of a few types of fast and versatile machines that were suitable for the full range of cryptanalytic challenges.

(U) In 1944 Steinhardt was able to spend some time on that concept; by the end of the year he had a proposal for a machine that would surpass the Comparator's ability to attack many different types of problems. He called his all-purpose machine "Serpent."

(U) The Serpent would have been a great surprise and a disappointment to Vannevar Bush: it turned against his favored technologies and favored reliability and flexibility over speed. Worse, it was to be centered on IBM components. Steinhardt openly declared that photoelectric technologies were too temperamental and micro-

film too demanding, at least for a machine that needed many simultaneous inputs.[29]

~~(S)~~ Serpent was to have at least thirty-two input stations. Each would read the "tapes" made of uncut IBM tabulator card-stock formed into an "endless" IBM card. The reading heads were to each have eighty brushes so that each hole in the "tape" could be read simultaneously. In each of the reading stations, as many as 100 of the heads could be installed. How many were to be active at one time was to depend upon the cryptanalytic problem.

~~(S)~~ In addition to the thirty or more 100-level reading stations, at least two more would be available for multitape operations such as done on the Comparator.[30]

~~(S)~~ A control system was to allow the tapes to be driven synchronously, or in any of the Comparator motions (stepping-sliding), or in such a manner as to imitate a matrix. The varied stepping would allow Serpent to have many uses. It could be a Copperhead or a Comparator or a Bombe or a Rattler or an IC machine – or even a Tessie.

(U) Steinhardt's Serpent rejected more than photoelectric reading technology and microfilm. He did not want to bother with electronic counting, either analog or digital. Because the machine's input was relatively slow, the rate of an IBM sorter, there was little need to bother with the pesky tubes. Rather, Steinhardt recommended that a set of relay boxes be constructed. Each would perform, like the SIS IBM machines, a particular set of functions.

(U) Steinhardt admitted that Serpent would not be able to perform some attacks as fast as the advanced photoelectric RAM, but its chameleon-like quality would, he claimed, more than compensate. It would, he said, be a perfect type of machine for research and for the postwar era when emergencies no longer drove OP-20-G.

~~(S)~~ In some cases, he said, it could compete as an operational machine. While Serpent would take three or four hours to do a full four-wheel Enigma run (compared to twenty minutes on the Bombes), it would, according to Steinhardt's calculations, be as fast as the electronic Rattler on the Jade and Coral problems. As well, he said, Serpent would be as fast as most of the photo-optical machines, at least the ones that used punch tape or photoplates. When the time needed for photoprocessing was taken into account, Steinhardt claimed, Serpent would be as efficient as the microfilm Tessie and Hypo.

~~(S//SI)~~ But competing with those two machines was not important to Steinhardt; he and others had concluded something that would have offended Stanford Hooper: "The cryptographic value of polygraphs and I.C. runs . . . is now admittedly open to question."[31] The significance of Serpent would be its ability to quickly test out such cryptanalytic applications to see if they were worthwhile. Serpent would prevent investing in costly special-purpose machines, ones that had little payoff.

~~(S//SI)~~ Steinhardt concluded his report on the proposed Serpent with some very prophetic advice: Serpent would be needed for the navy's next great challenge, the Russian code and cipher systems.[32]

(U) Lawrence Steinhardt's suggestion for the IBM Serpent was not followed through, although he continued to work on it and the design for the electromechanical counting machine that became the postwar monster, Alcatraz. Importantly, he was returning to the fold of the believers in electronics; he had begun work on an all-electronic ciphering machine, just as his colleagues were again forced to try to overcome the weaknesses of digital electronic components.[33]

(U) The Revenge of the Enigma – or Electronics Is Inescapable

(U) Although OP-20-G and the SIS turned to the Pacific after 1943, the Enigma problem returned to plague them. Actual and feared changes to the Allies' old nemesis were what drove the army and navy to commit massive resources to solving the problems of large-scale electronic systems.

~~(TS//SI)~~ The alterations to the Enigmas and their operational systems, especially the Luftwaffe's decision to make its reflector's wiring "pluggable," demanded so many tests that only electronics could perform the attack. The "reflector" problem of 1945 forced the development of devices that came close to being electronic Bombes.

~~(TS//SI)~~ At first it appeared that even the best technology could not overcome the new Enigma threat. Fortunately, a cryptanalytic attack on the changeable reflector was created that did not demand a fully electronic version of the Bombe; that would have been an impossible goal for the army, the navy, or the British. But the Duenna, the Superscritcher, and the Giant machines they constructed for the problem were "the" electronic cryptanalytic devices of World War II. They went far beyond the Comparators or even Rattler.[34]

~~(TS//SI)~~ But the electronic solution was a long time coming. The Americans did not leap from Joe Desch's electromechanical Bombes and Madame X to electronic machines. They tried to conquer "E" operational changes and then the "reflector" problem with traditional technologies. OP-20-G made several alterations to the original Bombe design before it accepted the necessity of the electronic Duenna, and the SIS built a huge new relay machine before it started building its electronic Scritcher.[35]

(U) OP-20-G's changes to the Bombes were evolutionary. The first major ones came after the British made an emergency request for an additional set of American Bombes, at least fifty of them. Joe Desch took the request as an opportunity to improve the standard #530 Bombes. He produced some two dozen of the new #1530s in 1944. They used the same logic and technology as the 1943 machines, and they ran at the same speed as the #530s, but were mechanically stronger and had additional circuitry to eliminate false stops.[36]

~~(TS//SI)~~ However, even before Desch made those significant technical improvements in the original Bombes, he began constructing the "Fire Engines." Those eight machines were the same as the original Bombes except that the vertical order of the commutators was "inverted." The fast wheel on the Enigma became the slow wheel on the Fire Engine, and the slow wheel on the Enigma was in the fast position in the Bombe. Nothing else was significantly different from the #530s. But the "inversion" was powerful. It allowed quicker runs when the identity of the fast wheel was known, and, more importantly, it allowed what were called "hoppities" runs during which the operators could stop the machine, then advance a wheel one step by hand.

~~(TS//SI)~~ That cumbersome process was necessary because the Bombes were unable to automatically imitate the turnover action of the "E" wheels. When Enigma wheels reached a certain position, they "kicked" the adjoining wheel one or more steps ahead, thus breaking the regular metric motion of the Enigma.[37] The Fire Engine "hoppity" method was very crude, but very helpful. It allowed the use of weak menus and ones which travelled over probable turnover positions.

~~(TS//SI)~~ A more complex extension of the commutator Bombe was Grandad, the double unit Bombe. It had thirty-two, not just sixteen, "E"s linked together. The use of twice as many "E" units in Grandad decreased the probability that an incorrect setting would result in a "hit." Arriving in Washington in late 1944, Grandad

permitted the use of much weaker cribs than demanded by either the regular or the inverted Bombes. It was designed to find solutions when a set of short indicators was used as the crib, when there were unknown stecker connections, or when the crib consisted only of cipher letters that were known to represent the same plaintext letters.

(U) Beyond Cribs: the Statistical Bombe

(U) The most ambitious revamping of the Desch Bombe was the Bulldozer. Delivered in early 1945, it had been desired, if not planned, since the navy first accepted the commutator Bombe in late 1942. It was a mechanical answer, and a very clever one, to the demands that "G" move towards a pure attack on "E."

(~~S//SI~~) Although everyone at OP-20-G had to accept using a crib-based method against Enigma, many argued for a continued search for a "pure" attack. Some were committed to statistical analysis out of professional pride; others cautioned against the danger of depending upon Britain for cribs. They warned that if the Germans tightened their security, even GC&CS could not supply what the standard Bombes needed.[39]

(~~TS//SI~~) In early 1943, a search for what was generically called a "statistical" solution was begun, but it was a very limited effort.[40] There was too much else to do to allow anyone within "G" to focus on an abstract problem. But when there were hints in summer 1944 that the Allies might not be able to count on good cribs in the future, more resources were poured into developing a machine for something very radical: a cipher-only attack.[41]

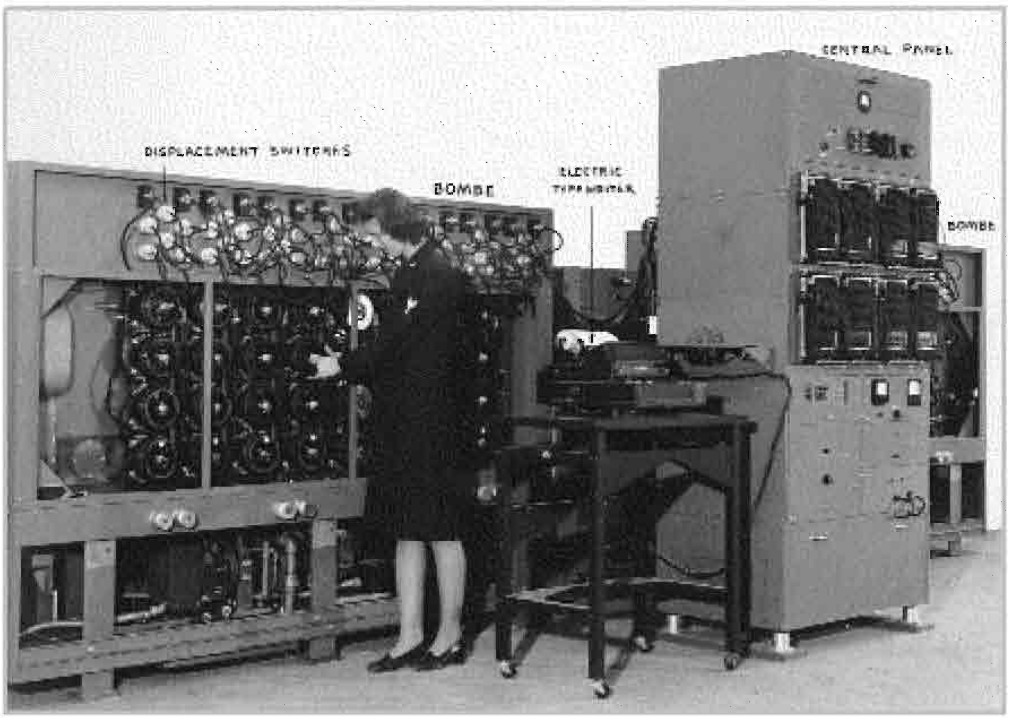
(~~TS//SI~~) Because at least a prototype machine was desired as soon as possible, Joe Desch's crew was asked to see if a regular Bombe could be turned into a "statistical machine." It took some time to refine the method and to revamp the Bombes, but a Bombe to identify German plain language became operational in March 1945. It was called Bulldozer because of the mechanical power a cipher-only attack demanded.

(~~TS//SI~~) The impressive Bulldozer was a cross between the hardware of a double Bombe (Grandad), the logic of a Mercury Selector, and the electronic analog circuits of an IC machine. Although it used a somewhat less mechanically demanding "recognition" method than did Mercury, Bulldozer's power to identify probable plain text was significant.

(~~TS//SI~~) Much energy had gone into devising the algorithms that had to be built into a crib-free Bombe. Hundreds of hours were put into the analysis of German military language. And "G's" best mathematicians spent weeks integrating those findings with probability studies to arrive at Bulldozer's test for the appearance of plain text.[42]

(~~TS//SI~~) The method finally embodied in Bulldozer demanded much that was new. Bulldozer's test began with the entry of the intercepted cipher. Then the machine's wheels were spun. At each position, the letters that emerged from the wheels were electrically weighted and summed. Next, a comparison was made as to whether the square of the weighted frequencies of each letter summed to equal or exceed a value that was typical of good plaintext messages.[43]

(~~TS//SI~~) The earlier statistical studies had determined that Bulldozer needed a long crib to be able to differentiate random text from true "language." Thus, the machine was, like Grandad, a double Bombe. To give the new machine additional power to tell order from chance, its thirty-two double banks of four-wheel "E" units could be changed into sixty-four single units to accommodate a longer cipher. Bulldozer was also like the Fire Engine: its banks were inverted. That was to help make "hoppity" type runs. Significantly, unlike the other Bombes, Bulldozer did not have a diagonal board."



~~(TS//SI~~)
Bulldozer Bombe to identify German plain language

~~(TS//SI)~~ Bulldozer called on electronics as well as electromechanics. After the cipher had been set on the machine's dials, all the letters that emerged from the commutators were sent to a small bank of twenty-six tubes. They stored the accumulated electrical weight for each letter. Before any of the wheels were moved, the value in each tube was squared and passed to an analog summing circuit. When the combined value of the output from the commutators at a particular setting exceeded the assigned threshold value, the machine stopped and then did something quite different from the other Bombes: it printed out the full text of the deciphered crib on a Letterwriter typewriter.

(~~TS//SI~~) Bulldozer's pure attack took more time than a crib vs cipher one. At its very best, it took twice as long to run a grenade test. That was because its motor was set at one-half the typical speed of the Bombes. That limitation was compounded by the nature of Bulldozer's tests. When the frequency weighting system confronted an uncooperative cipher, the machine might stop and type out probable clear text so frequently that its running time increased to as much as eight times that of the regular Bombes. That was one reason it was rarely used for more than a grenade run to establish starting points after all the other Enigma settings had been discovered.

(~~TS//SI~~) Full Bombe runs were much more forbidding. Given the special assumptions that had to be made about the stecker in a full run, Bulldozer might have to make as many as twenty-six separate four-hour runs to produce a solution.[45]

~~(TS//SI)~~ Although it probably never broke an Enigma system, the cryptanalysts were quite impressed with Bulldozer. Its weighted test seemed so promising for the future that "G's" cryptanalysts informed OP-20 that a Bulldozer attack might well make the navy's own advanced cipher machine, the ECM, vulnerable. Bulldozer

seemed so able that "G" did not tell the British about its powers until well after the war.[46]

(U) No Escaping Electronics, Enigma Meets the Cobra

(U) It was not a fear of what the Germans might possibly do with Enigma in the future but a true emergency that finally drove the army and navy's cryptoservices to take a chance on large-scale electronic machines. The emergency arose in 1944. It was the German air force's change in the internal workings of its three-wheel Enigma.

~~(TS//SI)~~ Fortunately, the Germans had given the British codemen some hints in late 1943 that the Luftwaffe was going to switch to the use of a pluggable reflector. That had caused a great deal of worry. Somewhat later, when the British learned the German Army was to do the same, worry turned into near panic.

~~(TS//SI)~~ The new reversing wheel was a major threat. With the pluggable reflector, any letter could be quickly rewired to produce any other letter. Although the new reflector was stationary once it was placed within an Enigma, its ability to be any possible wheel made it worse than the fourth wheel in the M4. It called for examining an additional 150,000,000,000,000 possibilities when attacking the air force's and army's "three wheel" machines.

~~(TS//SI)~~ The challenge was daunting, and there were some thoughts of not even attempting to conquer the pluggable wheel. But when it was learned that the Germans would alter the wheel's wiring on a ten-day cycle, not every day or with every message, a decision was made to face the problem.[47]

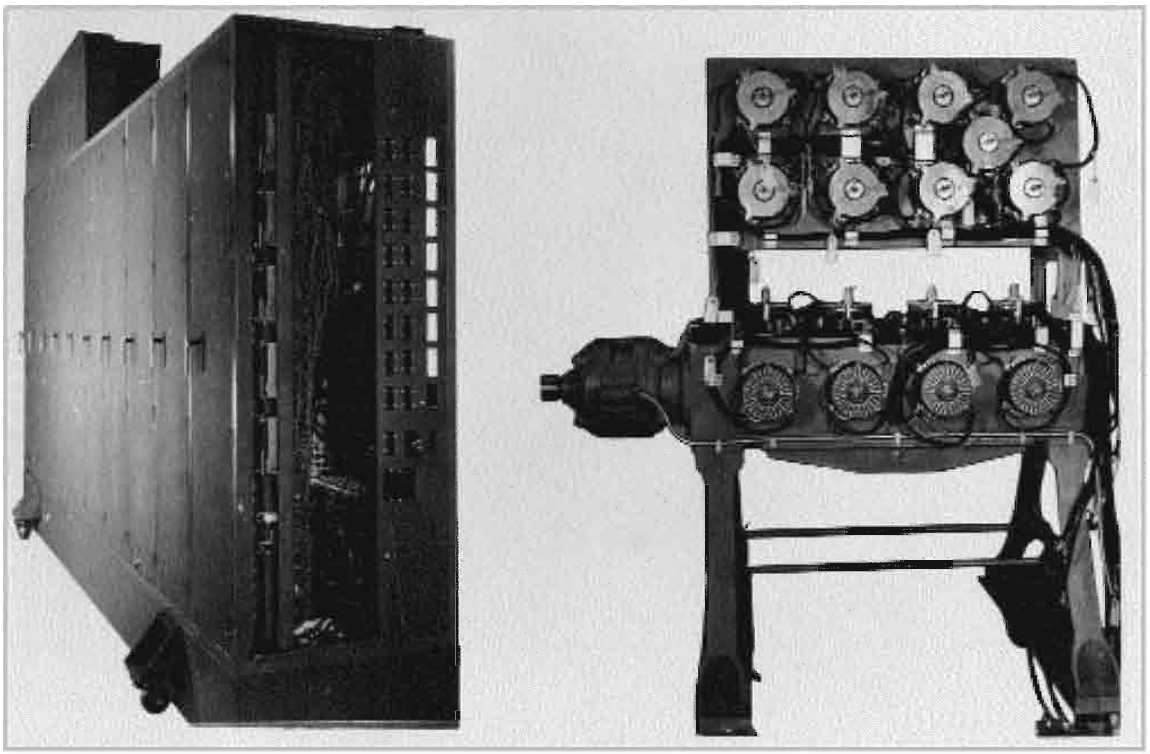
~~(TS//SI)~~ The British were the first to attack the new wheel. They did the best they could against the German communications subsystems which employed the new reflector, but the challenge was too much for their limited resources. Under the best conditions, it took five top Bletchley Park mathematicians two weeks of "hibernation" to get a solution to a single rewiring. The most powerful of the British Bombes were of little help. A slightly modified one took sixteen days for a simple problem, and the more elaborate Giant took three to four weeks to complete a full menu. That meant that Luftwaffe traffic could no longer provide much important tactical information. That traffic had become vital to the Allies. With the end of the U-boat war and the retreat of the German army into the homeland where messages were carried by cables, air force transmissions were a prime source of radio intelligence.[48]

~~(TS//SI)~~ A technological solution was required. But in mid-1944 the British were tired and stripped of resources; they needed help. Unlike the situation in 1942, they did not hesitate to inform their American cousins of the new danger and of possible methods of solution. The navy was notified of the "scritcher" test, then the army. Both American agencies immediately got to work trying to turn the probability-based scritcher method into hardware.

(U) The Navy's Duenna

~~(TS//SI)~~ The navy's first thought was to make another simple modification of the commutator Bombes. It was to be called "Mona." Mona was to have just one traditional Bombe wheel. The rest of the Bombe was to test the huge number of assumptions needed to try to identify the reflector wiring and the stecker pluggings. Mona quickly proved itself incompetent.[50]

~~(TS//SI)~~ More thought went into the method and possible machines. After modifying one of the Enigma analogs at "G" by adding the "Cobra," an attachment that allowed the analysts to change the reflector wirings by hand, "G's" analysts put the British method through a series of exploratory tests. Soon, they decided that only a two-wheel test and a great deal of electronics could do the



~~(TS//SI)~~ Duenna

job. Preliminary specifications were drawn in August. Then, very quickly, the proposed "Duenna" was under construction at the NCR facility.

~~(TS//SI)~~ Duenna became a twenty-foot-long and eight-foot-high mixture of a small version of a two-wheel commutator Bombe and a cabinet with over 3,000 advanced electronic tubes. The first Duenna of November 1944 had to be huge and cutting-edge because of the demands of the scritcher test; so did its four sisters.[51]

~~(TS//SI)~~ One of "G's" bright young mathematicians, Howard Campaigne, made important contributions to the logic of scritching. [52] His modified OP-20-G[53] version of the British attack was hardwired into Duenna's complex circuits. It was necessarily a very efficient attack, but it demanded a great deal. It required as much as a 100-letter menu (cribs vs cipher pairings in this case); it worked under the assumption that the slow "E" wheel would not turn over at critical points in the menu; and, unless prior knowledge allowed "G" to avoid it, a full test required as many as fifty-six separate runs to test all the possible two-wheel combinations.

~~(TS//SI)~~ Duenna demanded so much because it was expected to work much harder than the original Bombes. The Bombes were pampered. They were well fed with known wheel wirings and the reflector plugging and asked to yield stecker, rotor order, and, with some help, the window setting. All that Duenna was told was the wheel wirings. Yet it was asked to produce the same information as a successful Bombe run plus the plugging pattern of the new reflector.

~~(TS//SI)~~ Duenna's job was tough, and it had to be "smart." With the crib in place, it made an assumption about the stecker setting of two or

three high-frequency letters. Then, with its two imitations of the faster "E" wheels, its electronics serially tested the plain-crib pairs against successive combinations of stecker and reflector pluggings. Duenna had several electronic versions of steckers and reflectors to perform those tests.[54]

(~~TS//SI~~) A stecker-reflector check for a given stecker assumption took twenty minutes; an average "run" took an hour and a half. But the need to run different wheel combinations to isolate the fast wheel turnovers called for a day's work. The complete set of tests needed for difficult systems might keep a Duenna busy for two weeks.[55]

(~~TS//SI~~) Although Duenna had advanced electronics and circuitry, it might have taken much longer to do its job if the "scritcher" test had not been so inherently intelligent. Other of "G's" World War II machines had hardwired decision algorithms, but Duenna had the most complex one. Duenna's smartness was based on something like the diagonal board test: it looked for contradictions or impossibilities given the data and assumptions fed into it. Its intelligence went beyond the diagonal board's, however. Because the searching in Duenna followed a logical progression, a "branch" of a search could be abandoned very early. The machine did not have to wait until all possibilities had been examined. That saved enormous amounts of time.

(~~TS//SI~~) As the machine tested the assumed and, then, the recovered steckers and reflector links against the crib-plain pairs, it checked for contradictions as well as building up a "recovery number." The recovery number was changed with each sweep (step) through the "E" analog. That number was compared with the recovery score from the previous sweep. If no additional recoveries of compatible steckers and reflector pluggings had been made, Duenna's circuits compared the recovery "buildup" number with a preset threshold value. If that value was exceeded, Duenna tested for another critical factor. If that "links and tacks" test was passed, Duenna printed the information about its "hit" and went on to search through another stecker assumption. If the threshold was not met, Duenna skipped the printing stage and went on to examine another stecker assumption.[56]

(~~TS//SI~~) Although it was a very strange looking combination, Duenna became a valuable tool. Even before the first model was completed, the navy ordered that several clones of the original be delivered as soon as possible. The crew at Dayton wished to build a more elegant machine, perhaps with electronic wheels, but they followed orders.[57]

(~~S//SI~~) But there were attempts to persuade "G" to allow the creation of a full electronic Duenna.[58] Some looked upon the Duenna project as the challenge that would force a do-or-die commitment to such electronic components. But an electronic "wheel" again proved too much of a challenge for its "E" wheels.

(~~TS//SI~~) What was inside Duenna's main cabinet was very different. The vacuum and gas-filled tube circuits were innovative. There were high-speed digital counting rings, "selection" matrices, electronic stepping switches, and an electronic version of the conflict-testing diagonal board system. Duenna's critical threshold testing circuit was very advanced for the era, and the ability to enter the crib via dial switches saved much set-up time.[59] Especially important, the Duennas proved very reliable and maintenance free.

(U) From Relays to Tubes, Rosen Gets His Chance

(~~TS//SI~~) The SIS engineers under Leo Rosen also found the pluggable reflector problem an exciting challenge. In fact, it was the difficulty of the problem that led the "F" section to become a significant force in research and development. The pressure on the SIS to deliver a machine to help the British, combined with the decision not

to hire an outside contractor as had been done with Madame X, gave Rosen the power to require the army to send him a cadre of bright young engineers who already had experience in advanced electrical and electronic engineering. He very quickly built up a remarkable group, many of whom went on to become important figures in the postwar computer industry.[60]

(~~TS//SI~~) Rosen had been notified of the pluggable reflector (Uncle Dick) threat in early 1944. While the SIS cryptanalysts were put to work scratching by hand methods, he and his close aides, such as Captain C. R. Deeter,[61] began a design for a supermachine. Like the navy's engineers, Rosen's men thought electronics was the logical route.[62] Then they were forced to weigh engineering ambitions against cryptanalytic needs. The result was another compromise – the relay Autoscritcher (also known as Grapevine) of 1944.[63] And even its follow-on, the electronic Superscritcher, had to face up to the limits of digital electronics in the mid-1940s.

(~~TS//SI~~) Because the German army and air force "E" modifications were the same and because Britain had provided both the American army and navy with the same crypto-methods for an attack, the logic and architecture of the SIS's device were similar to Duenna's. But the hardware was very different: a longer crib was used, the build-up to a hit was different, and the test for branching out of a search was simpler.[64] In several ways, the army's relay Autoscritcher was more of a throwback than Duenna, and it was slow: "running time was as much as ten to fourteen days, three shifts a day." Although it performed twenty-five tests a second, a single wheel order test took three and one half hours.[65]

(~~TS//SI~~) The most incongruous part of the Autoscritcher was its "wheel" unit which fulfilled the same function as the rack of commutators in the Duenna. The army machine had twenty banks of two special Enigma wheels, not commutators.[66] Each served as the moveable fast wheel and as a static combination of the medium, slow, and reflector wheels. These rotors were grouped into sets which, along with allied relay circuits and stepping switches, formed the basis for "branch" testing.

(~~TS//SI~~) To save design and construction time, no automatic stepping controls for those rotors were included in the Autoscritcher. Given the length of time it took the machine to search through steckers and to test for contradictions, it was thought[67] hand-turning of the rotors would be acceptable.

(~~TS//SI~~) The Autoscritcher's very long crib was entered on a huge plugboard. Assumptions based on frequent cipher-plain pairs were entered into the machine. Then a bay of relays and electromechanical stepping switches serially tried all the possible steckers, passing control to the two bays of electronic equipment. They included the matrices that checked for diagonal-board type contradictions. A long chain of crib-plain pairs was used (each with its own rotor pair). An analog threshold test made the final decision as to whether a "hit" had occurred. That test, however, was not as complex as in the Duenna. And an operator had to copy the "hit" settings by hand.[68]

(U) Engineering Pride and Peacetime Priorities

(~~S//SI~~) The SIS engineers had begun the Autoscritcher as a learning project. Once they tested out their ideas with its older technology, they expected to begin the design and construction of an electronic machine that would be more useful and which would be a source of engineering pride. The goal was a purely electronic machine that would be at least one hundred times faster than the Autoscritcher."[69]

(~~TS//SI~~) The "F" group was given the go-ahead for such a machine in early 1945.

The machine soon acquired the name "Superscritcher." Its designers were thrilled when they realized that it might be as much as 500 times faster than its relay predecessor.[70]

(~~S//SI~~) Designing new circuits was exciting for the young engineers assigned to the "Super" project. Although the "Super" had the same architecture as the Autoscritcher, made similar hardwired "if" decisions, depended upon the plastic and copper "E" wheels, and performed the same type of cryptanalytic test, it was a far different and more innovative fixed-purpose computer.[71] A purely electronic stepping switch, improved electronic ring counters and circuits [72] and electronic controls for automatic stepping of the rotors emerged before VE Day.

(~~TS//SI~~) The electronics in the "Super" were not exclusively digital, but they were major advances in the state of the art. Over 3,500 tubes were mounted in eighteen eight-foot-high bays. A large air conditioning system stood by to protect them and the operators. There even was a means for printing the settings when a "hit" was found.[73]

(~~TS//SI~~) But the "Super" was not operable when Germany surrendered, and the Enigma traffic for which it was designed disappeared. There were demands that the project be abandoned. Fortunately for the "F" group's morale, the commander of Arlington Hall Station decided that some useful function could be found for a completed machine. He approved a continuation of the project. Several stubborn electronic problems were overcome and the Superscritcher's power was turned on in December 1945. To the surprise of many, it was used on various problems for the next five years. And it did prove itself to be 500 times faster than the Autoscritcher.[74]

(U) Keeping the Faith: the Return of the Film Machines

(U) The term "RAM" had a more precise meaning for some in OP-20-G and the SIS than "high-speed cryptanalytic machines." Especially for the army's engineers, RAM meant the type of microfilm and photoelectric machines that Bush had promised to Admiral Hooper in the 1930s, a series of machines the SIS group came to want for themselves by 1944. In fact, in 1944 it was the army's cryptanalysts, not the navy's, who became the strongest advocates for film-based devices. By then, the navy's men in "G" had become a bit wary of both film-related technologies and the difficulties involved in producing reliable microfilm. The navy had not abandoned Bush's ideas, but it pulled back from Eastman Kodak and microfilm in 1943. After Icky arrived, the navy did not order any additional film machines, at least during the war.[75] One reason for that was the last one on its 1942-43 shopping list refused to be turned into hardware in a timely way.

(~~TS~~) What became known as "Amber" did not arrive until late 1945. It took so long because of the cryptanalytic difficulty of the system Amber was asked to attack, as well as the stubbornness of microfilm technologies.

(U) The Revenge of the Codes, Again

(~~TS//SI~~) The Japanese JN25 additive code had led to some desperation-driven technical solutions at "G." The many Copperhead I's searched through thousands of messages in the hopes of finding two identical cipher groups spaced equally apart in two messages so that the analysts might be able to identify "depths" and go on to break into a system. The huge and expensive Mercury, with its walls of relays, was also an example of trying to do the impossible. Thousands upon thousands of additives were stripped every hour; then its huge memory was searched for frequent code groups with only a glimmer of hope that a hint of a possible solution might emerge.

(~~TS//SI~~) JN25 was not the only difficult and demanding Japanese additive code system, however. By the last year of the war, the attempt to

read the JN37 weather code continuously raised more cryptanalytic and technological frustrations than had the fleet system.

(~~TS//SI~~) Reading the combined weather report grew more and more important to the American navy as it raced towards Japan. The fleet was moving so fast that American weather stations could not be established quickly enough. The only good source of critical weather information about many areas was the Japanese reports. How valuable they were became tragically evident when one of Admiral Halsey's task forces was caught by a typhoon in December 1944. The storm took almost 800 American lives." [76] If all the Japanese reports had been read in a timely way, the disaster might have been avoided.

(~~TS//SI~~) JN37 seemed to be the most efficient way to tap the reports. It was the system the Japanese used to bring together local weather bulletins, then transmit them as a group. The system was cryptanalytically strong, but it had a few potentially exploitable weaknesses. The underlying four-digit numeric code for the system remained fairly stable throughout the war, and it was known that the messages were very stereotyped. Cribs and code-meaning identification were possibilities because temperature, humidity, and wind speed remained much the same in various areas during a season. That meant a great deal of repetition of code groups.

(~~TS//SI~~) Some JN37 variants had been read. But there was a tough part to JN37, its superencryption. There were many additives, and they were frequently changed. With those changes came blackouts, such as those of 1944. In the JN37 version that led to so much pain in that year, the additive book had 900,000 entries.[77]

(~~TS//SI~~) "37" had yielded, at times, to traditional tabulator methods supported by busts, knowledge of indicators, and captured data. As long as there were busts and captures, the old methods worked. But even before the traumas of 1944, there were serious concerns that more frequent changes of the additive books and alterations of indicators might cause a permanent lockout.

(~~TS//SI~~) In response, in early 1944 Howard Campaigne, one of OP-20-G's bright young mathematicians, began examining the practicality of various pure attacks against JN37. He sought an attack that did not depend upon knowing indicators, the additive book, or usual cribs. He experienced much disappointment. For example, he calculated that an Index of Coincidence assault with existing equipment would take three years at three shifts a day for any type of breakthrough. Quite logically, he suggested a search for better methods and high-speed machines. There was not much progress.[78]

(~~TS//SI~~) Then the cryptanalysts had some good fortune. The discovery of an active JN37 additive book gave some hope that a practical method could be devised. The capture of the additive book allowed "G's" best young mathematicians and analysts to understand the logic of the system used in 1944 and, among other things, what the probabilities were that particular code digits would appear in certain positions of messages.[79]

(~~TS//SI~~) A quite elaborate theory was developed, one based upon advanced Bayesian statistical methods. The statistician argued that if "G" was willing to make a very costly investment in calculating the "centiban" weights and creating a machine to apply them, then at least a minimal but consistent entry into JN37 could be expected. But the method seemed forbidding. It demanded too much calculation.

(~~TS//SI~~) Other, perhaps less cumbersome, methods of attack were explored, including the dictionary lookup approach of Mercury. But they stood little chance of producing results. By late 1944 the Bayesian "statistical crib" method of

identifying a code group version of "plain text" became the navy's only hope.

(~~TS//SI~~) The "statistical crib" method was the kind that Hooper and Wenger wanted as the basis for all of "G's" work. It would use only cipher and a "scientific" weighting system to pinpoint probable plain text and then point to additive "depth." From there, additional machine runs and statistical and craftsmen's tests could be applied to recreate the additive book and to quickly enter a system." [80]

(~~TS//SI~~) But in 1944 there was no machine for the "statistical crib." Although "G" had attempted to establish a machine program to make the statistical methods practical earlier in the war, little had emerged by the time the JN37 weather code became a priority at "G." The lack of results was one of the reasons why Wenger, Engstrom, and Meader wanted their own cryptanalytic machine "factory." They were frustrated by the slow pace at Eastman Kodak.

(~~TS//SI~~) In early 1943 Eastman had been asked to explore possible technologies for the additive problems. "G" had requested film-based machines for a range of functions. They wanted ones to strip additives, match plain text to a code dictionary, test for likelihood, perform statistical weighting, and to print code meanings. [81]

(~~TS//SI~~) Eastman took up the challenge. Ten of the best men in Rochester were assigned to its new RAM team. They were given a great many resources and much engineering latitude. They explored many, perhaps too many, logical and technological alternatives.

(~~TS//SI~~) But no new film "Japanese" machines emerged from Eastman in 1943 or 1944.

(U) Meanwhile, Lawrence Steinhardt began work on his versions of additive photoelectric RAMs, calling upon the technical expertise at Dayton when he needed practical advice. By the time he turned his first designs into hardware, he had become shy of film. His proposed punch-tape Copperhead series was the outcome. He laid out ideas for a wide range of machines, ones to implement the newest code-system attacks.

(~~TS//SI~~) Two of the proposed Copperheads, Mark V and VI, for example, were aimed at mechanizing weight and dictionary attacks against additive systems. Projects for them were begun, but their complexity led to their abandonment. The other designs also proved too complex. Only Copperhead I, the "brute force" matching machine, was made operational. As a result, "G" was left without much in the way of additive RAM machinery. It was not alone. The army also had ideas of a film machine for the additive problem, but it gave such a machine low priority before 1945. [82]

(~~TS//SI~~) Thus, when reading JN37 became an imperative for the navy, there was no hardware in place that seemed able to perform any of the proposed cryptanalytic attacks, especially the one that seemed best, the sophisticated but costly "statistical crib" method.

(~~S//SI~~) There was another hurried search for a "37" machine in 1944. None of the suggestions seemed reasonable, and none were turned into projects. The situation seemed hopeless. But at the end of the year, it was declared that an answer had to be found.

(U) More Numbers Than Ever Before

(~~S//SI~~) A crisis team was put together to try to force a technical solution. John Howard led the navy group that consulted with the top engineers at Eastman and NCR. He told them of the requirements of the new "statistical crib" attack. Both groups then reviewed the technological possibilities. [83]

~~(TS//SI)~~ What Howard gave as the goals for the new RAM was staggering. But that was inescapable. The Japanese were changing the JN37 additive book three times a year. To recover the new books, Howard explained, called for more calculations than "G" had ever attempted. The pure "Monographic Statistical Method" required, for example, 500,000,000 very complex comparisons of cipher to "crib" to find one correct line-up (the path to one correct additive). To recover just 10 percent of the "37's" additive book within the first half of its four-month life called for six such searches a day.

~~(TS//SI)~~ The job was more difficult than just looking for raw coincidences as the original Bush machine had been built to do. The "Ideal" machine John Howard wanted had to perform more than 200 multiplications, summations, and threshold tests for each of the half billion comparisons made during a run.[84] To complete those trillions of operations six times a day called for something beyond the Bombe, Mercury, or even Duenna. Howard was calling for a supermachine.

~~(TS//SI)~~ Even if a technological answer was found, building the superadditive machine would be a gamble. All the calculation might be for nothing. The eight weeks of 3,000,000,000 daily comparisons would yield a useful bit of information only if all elements of JN37 besides the additives remained stable. If the Japanese made changes besides issuing a new additive book every four months, the calculations might prove useless.[85]

(U) The gamble had to be made. The "G" engineers, NCR's men, and the Eastman group were ordered to look at various technical options and come up with a solution.

~~(TS//SI)~~ One alternative was to base a machine on advanced digital electronic counting/multiplying circuits. When estimates were made of the speed of the best possible vacuum tube machine, the results were shocking. It was found that just one run with the electronic digital device would take sixteen years. When asked if several copies of the device could do the job in a reasonable time, the engineers responded that it would be impossible just to find the parts needed for enough of the machines.[86]

~~(TS//SI)~~ Another possibility was to create a new version of the proposed Full-Selector machine. Instead of the weights being calculated as the cipher was scanned, they would be stored in a fast memory and retrieved for each of the possible 60,000 different cipher combinations that were expected to be encountered during a run. The stored-weight alternative seemed attractive, but it called for ultrafast memory. Without it, the stored-weight approach would take as long as the on-the-fly calculations using electronic digital circuits: years.

~~(TS//SI)~~ The "best" memory technologies, such as delay-lines, seemed inadequate. So it was decided to go back several steps. The only way to achieve the needed speed, it seemed, was to rely upon very densely packed high-speed tapes that carried all the "weighting information" and upon analog and parallel calculations. With the tapes, the machine would not have to multiply; it would just have to scan, search the memory, and sum. And, if enough precision could be obtained, speed could be vastly increased through the use of analog "counting" – the machine would not have to wait while digits were summed, one after the other.

~~(TS//SI)~~ All that seemed to dictate a return to microfilm and photoelectric sensing and calculation. But it took many months to agree upon the exact nature of the machine. NCR and Eastman's team agreed that the general microfilm RAM approach should be followed, but there were significant differences on many details. An important one was whether the "weights" were to be represented by different size spots (the NCR recommendation) or by degrees of opaqueness.

(~~S//SI~~) The debate went on far too long. It was not until the summer of 1945 that agreement was reached and the Eastman team's approach to what became known as "Amber" was chosen. That did not allow enough time to create an operational machine. Amber was not to appear until the war had ended.[87]

(~~TS//SI~~) Eastman's proposed Amber was to be a photoelectric comparator, following in the traditions of Icky and Hypo. It had four scanning photocells that tested two 70mm repeatedly offset and superimposed films against a coincidence threshold. It used the familiar analog circuits but with a sophisticated twist: both positive and negative photosensing was used.[88]

(~~TS//SI~~) Amber was to have a relatively large viewing field so that a long string of code could be tested instantly. It was designed to test eight hundred characters a second. The long field would give Amber speed and more. It increased the probability that "false hits" would be eliminated. More than that made Amber powerful; it had a very special way of implementing the weighting methods used to automatically identify probable "plaintext." The "dots" on one of its films represented the weights through varying densities.

(~~TS//SI~~) Those variable densities called for much to be added to the older "dot" cameras Eastman had made for Icky and Hypo. A special card reader and camera combination was developed. Amber's camera was a sophisticated extension of the light-bank system that had been developed earlier in the war for machines like Icky. As the weight cards were read, one of twenty different voltages was applied to the tiny lamps to achieve the variable densities. Its developers knew that it would be a major chore to keep the system in tune, but that was inescapable. More than the camera was demanding. The data were so densely packed that extra care had to be taken at every step of film preparation and development.

(~~TS//SI~~) In addition, the older analog summing and threshold circuits had to be revised. But Amber was not to be a completely new machine. Only the changes to the older Icky and Hypo concepts that were absolutely necessary were incorporated. Thus, Amber had much of the crudeness of the Icky. When Amber's films were placed in its Icky-like projector, if enough of the code groups had clear "dots," Amber would just stop.[89]

(~~TS//SI~~) Amber's design was very demanding. It needed controlled humidity and correctly monitored ambient lighting. And its film transports had to be much more precisely adjusted than Icky's or Hypo's. One reason for the narrow tolerances was that the very expensive master films containing the "weights" would wear out if there was the slightest friction.[90] Those master films were precious because they carried the critical "weights" that were so labor intensive and difficult to calculate.

(~~TS//SI~~) Amber's creators convinced "G" there was no alternative but to accept the great burdens the "master film" design required. The cryptanalysts knew that the preparation of each log-odd weight film called for millions upon millions of multiplications. Those assigned to the job feared they would never be able to keep up with the task. Although they had the tabs, including a special Multiplier, the job of preparing the long card decks to feed the special film-generating camera seemed overwhelming. A short twenty-three-character message needed almost two million multiplications for its weight film.[91] It took over 800 hours of tabulator and IBM electromechanical multiplier time to create a typical deck. And each of the different types of JN37 messages needed more than a dozen of its own "probabilities" films.[92] Unfortunately, a hoped-for emergency project to create an electronic multiplying machine could not be initiated, and "G" had to accept the prospect of thousands of hours of calculations to prepare for Amber's arrival.[93] Perhaps it was for the best that Amber was delivered just after the war with Japan was concluded.

~~(TS//SI)~~ Amber did not achieve all the goals set for it in 1945, but it was eighty times faster than the proposed digital electronic JN37 machine. And it could be modified to perform other than the "weight" test. It did a simple round-robin test of every message in a group against every other 1,000 times faster than the NCR-Gray Comparators. But its 800 comparison-a-second rate (the original goal had been 35,000 a second)[94] meant that a typical run for the "37" attack might have, at the very least, taken twenty-four hours.[95]

(~~TS//SI~~) Because of Japan's defeat, there would be only two Ambers,[96] not the twenty Howard Engstrom had sought earlier in the year. Some remodeling was needed in 1947,[97] but the Ambers proved useful into the 1950s.[98]

(U) Dr. Bush, Your Best Friend Is Really the Army

~~(TS//SI)~~ The contract for Amber was not a signal that OP-20-G had regained its faith in photoelectric machines. Its frustrations with it and the Gray-NCR Comparator led to a belief that a long development cycle would be necessary before Bush's ideas could be turned into the powerful and reliable machines Joseph Wenger and Admiral Hooper had longed for in the mid-1930s. Although "G" added an electronic "rare-event circuit" to the Gray Comparators and had Icky refurbished, it did not return to Eastman or Gray for more machines during the war.[99]

~~(S//SI)~~ By 1944 the lack of orders from the navy led Eastman to consider reassigning most of its RAM team, leaving only the Amber group in operation.[100] Then the army saved the day.

(~~S//SI~~) Some of the SIS's engineers had become devoted fans of Bush's visions, and by late 1944 they were laying plans for a whole series of microfilm-electronic RAMs, a series that went beyond what the navy had once imagined. They even requested a statistical Rapid Selector: a machine that married microfilm with electronic counting. And by early 1945 their belief in film led to a request that a new camera be constructed to allow the army's Gray-NCR Comparator to become a film rather than a punched-tape machine. The SIS had experienced so many problems with the punches that it was searching for any way possible to prolong the operational life of the Comparator.[101]

(~~S//SI~~) Although it never acquired all that its engineers desired, somewhat ironically it was the army, not the navy, that fulfilled Bush's dream of a "statistical" Rapid Selector. By 1945 the SIS-Eastman teams put electronic counting together with microfilm. And they continued on after the war to be the sponsors of the most far-reaching attempts to create film-based machines for cryptanalysis.

~~(S//SI)~~ Friedman's team had begun its romance with RAMs in early 1943 when the navy allowed the SIS to piggyback orders for a few machines onto the navy's contracts.[102] Close to $200,000 changed hands very quickly for the purchase of IC plate devices, a tetragraph tester and, later, a Gray-NCR Comparator. The first purchases were just that, purchases. The SIS played no role in the design of the machines. But after the RAMs began to arrive in late 1943, the SIS wanted a more powerful voice in machine design.

(~~S//SI~~) Within less than a year, a subcommittee was formed by those in "F" who had become strong advocates of the film-based devices. Many ideas for new RAMs emerged. Eastman soon began creating an SIS version of Hypo (their film Dudbuster) and an upgrade on the Tessie. There were more ambitious plans. The SIS was developing ideas for a film version of a Slide Run machine, an Icky for the Fish traffic, and a special type of Amber. A budget request of $75,000 for research was approved. In addition, funds were allocated for the initial development stages of at least three new machines.

~~(S//SI)~~ Only one of those proposed machines was constructed, but some unexpected film RAMs appeared at the SIS during late 1944 and early 1945.[103]

~~(TS//SI)~~ One of those surprises was the result of lashing together the army's version of the 35mm Icky and the electronic counters used on the Gray-NCR Comparator. Only one of these unnamed machines was built, but it pleased the SIS analysts and encouraged them to make more modifications to existing devices. The army's Tessie, for example, was significantly upgraded. It was made more efficient, but, more importantly, it was made to automatically return to the point on the films where a sought-after complex code or cipher pattern was located. Furthermore, a new camera allowed it to use the "blackout" test for brute-force searches. Later, a more reliable card-to-film converter was requested.[104]

(U) The Great 5202

~~(TS//SI)~~ While the older RAMs were being updated, Eastman was busy with the SIS's major RAM contribution, the "5202." The 5202 was the machine for the Fish system that had been recommended in 1944. It became the most sophisticated and powerful of all the film RAM machines of World War II and after. In fact, the 5202 effort can be considered to be the major catalyst in keeping Eastman-Kodak together after the war. Although it was completed and sent to England too late to make its mark against Germany, the 5202 was used throughout the 1940s[105] and was used to attack the German Tunny enciphering machine.

~~(TS//SI)~~ Among the 5202's advanced features was its much-improved camera system. It took the light-bank principle far beyond the previous versions. Very important, it could pack the patterns generated by analogs of encryption machines much more densely than earlier models. As important, the circuits allied with the pattern generators allowed great flexibility in selecting the data transmitted to the camera. Creating complementary code patterns, for example, was very easy. The camera system went far towards solving a major problem of all the older film systems: the great amount of time it took to generate the films.[106]

~~(TS//SI)~~ The 5202's heart, its reader, was also a technical improvement over the previous Eastman RAMs. Optics were improved. In combination with the dense packing on the films, the improved sensing systems allowed ten times the number of characters to be tested at once as on the other film RAM. The 5202's span of 500 columns was impressive. That made 5202 a more robust cryptanalytic aid than the other RAMs with their relatively short viewing gates.

~~(TS//SI)~~ The 5202 was also versatile. It could be used to "locate" desired patterns as well as to make Comparator-like counts on its electronic banks. It could hold as many as four films at a time; two of those were motor driven. Furthermore, its drive mechanisms were extremely fast and could step films in many different patterns.

~~(TS//SI)~~ The unique feature of the 5202 that gave it the potential to be as valuable as the British Robinsons or Colossi was its ability to test two fields of data at the same time. That allowed it to perform the special cryptanalytic test it embodied. The 5202 could demand that no contradictions in two fields be found at the same time that one or more "confirmations" were located. To do that, the 5202 contained sensing and testing circuits that sought electrical balance among three photocell circuits.[107]

~~(TS//SI)~~ Although designed for the German teletypewriter problem, many different applications were found for the 5202. It was used as a statistical dudbuster, for example.

(U) Beyond the Comparators

~~(TS//SI)~~ Well before the 5202 was delivered, the SIS was drawing up plans for yet another new generation of 70mm film RAM. Their immediate target was to be Japanese code systems, but the machines were intended to be pathbreakers to a new era in microfilm devices.

~~(TS//SI)~~ The first request was for a much enhanced Eastman version of Steinhardt's Copperhead I. That would allow high-speed searches through very long portions of text (hundreds of characters rather than only the thirty in Tessie). Next came a request for a new type of 5202, one to perform isomorphic tests. Most important, according to the "F" group, was a film Slide Run machine with very advanced electronics. It was to be 100 times more powerful than the relay-based IBM versions.

~~(TS//SI)~~ The requests explained that each machine was urgently needed for attacks on Japanese weather and army codes. But the "F" group, to be credible, had to acknowledge that it might take some time to develop the new RAMs – perhaps too long given the signs that the Pacific war was winding down. To avoid losing their machines, they provided a thorough analysis of the role of film computation in SIS's future, hoping that even if the request for specific machines was rejected, research funding would continue.[108]

~~(S//SI)~~ Emphasizing that it was crucial to keep the RAM group at Eastman together, "F" asked for enough money to sustain, at the least, a research effort in Rochester for several years. They admitted that the machines they needed were more of a challenge than the 5202, but they said the future of SIGINT demanded new RAMs.[109]

(U) The Machine That Wasn't

~~(S//SI)~~ There was one challenge that "F" group did not attempt to meet, a possible RAM that was not even mentioned during the war – a machine for traffic analysis. Neither the army nor the navy tried to create a machine for "data processing." The absence of massive fast memories and rapid input-output equipment meant that little attention was paid to creating a revolutionary data processing engine. A "data" machine had to wait until agency priorities changed and until computer readers, printers, and memories with capabilities far beyond those of the early 1940s emerged.

(U) Notes

1. ~~(TS//SI)~~ A glimpse into the complexity of the weighting methods is found in ~~(TS)~~ NSA CCH XII Z, Lt. A. H. Clifford to Lt. J. H. Howard, "Full Selector: operation on a four digit code group differences," 22 February 1945. When a similar method was used against the Japanese weather systems, the required calculations to arrive at the weights for the "statistical" attack proved so numerous that the cryptanalysts asked that an electronic multiplying machine be constructed. (~~TS//SI~~) NSA CCH Series XII Z, R. A. Rowley, "Preparation of Weighting Film, Secondary Stage Problem," OP-20-G, 2 August 1945.

2. ~~(TS//SI)~~ The use of log weights to estimate whether or not plain language was appearing as the result of a decryption process was well established by mid-war. The Gee-Whizzer had been built around the idea. ~~(S//SI)~~ NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1989. The very innovative Bulldozer (discussed below) was a Bombe version of the method. ~~(TS)~~ NSA CCH Series XII Z, CNO, CITS Paper TS-30, "Bulldozer Supplementary Manual," Navy Dept., Washington, November 1945.

3. ~~(TS//SI)~~ NSA CCH Series VII Z, L. R. Steinhardt, "Possible Engineering Solutions for Full Selector Problem," OP-20-G-4-A5, 23 November 1944. The "M" engineering group had kept in touch with all Allies' computer and electronic development projects of World War II. The failure to mention electrostatic memory in the JN25 problem reports was perhaps not a result of ignorance but of a knowledge of both the primitive stage of development of the tech-

nology and the unlikelihood that potentially fast electrostatic memories would hold large amounts of information. Useful for insights into memory technology of the era is James W. Cortada, *Historical Dictionary of Data Processing Technology* (New York: Greenwood Press, 1987).

4. ~~(S//SI)~~ NSA CCH XII Z, OP-20-G-4-A, "Electronic Matrices," 19 September 1944.

5. ~~(S)~~ Such a "memory" was not uncommon at the time.

6. ~~(TS//SI)~~ NSA CCH Series XII Z, Samuel S, Snyder, "Famous First Facts, NSA: Part 1, Pre-Computer Machine Cryptanalysis."

7. ~~(S//SI)~~ NSA CCH XII Z, OP-20-G-4-A, "Electronic Matrices," 19 September 1944.

8. (U) The highly significant Duenna project is discussed below.

9. (U) On the tube reliability question and the success of their use in the machine that is generally held to be the "first" electronic computer (although it had a special-purpose architecture), see Nancy Stern, *From ENIAC to UNIVAC: An Appraisal of the Eckert-Mauchly Computers* (Bedford, Mass: Digital Press, 1981). The ENIAC had some 18,000 tubes and a very high downtime because of that.

10. ~~(S)~~ Ideas for use of photocells and glass plates were suggested in some of the NDRC fire-control proposals. Those seemed impractical to Steinhardt.

11. ~~(S//SI)~~ NSA CCH XII Z, OP-20-G-4-A, "Electronic Matrices," 19 September 1944.

12. (U) Louis A. Gebhard, *Evolution of the Naval Radio-Electronics and Contributions of the Naval Research Laboratory*, (Washington, D.C.: Naval Research Laboratory, 1979), 326-8, also displays a very advanced German acetate tape system that was captured during the war.

13. ~~(TS//SI)~~ NSA CCH Series XII Z, L. R. Steinhardt, "Additive Machines: Historical Summary of," 27 November 1944. ~~(S)~~ Lt. A. H. Clifford to Lt. H. H. Howard, "Full Selector: operation on 4-digit code group differences," 22 February 1945. ~~(S)~~ NSA CCH Series XII Z, "Conferences at Dayton," 11 April 1945.

14. (U) OP-20-G and the engineers at SIS were not the only Americans searching for appropriate "computing technologies" to meet escalating demands. See for example, Chapters two and three, in Kent C. Redmond and Thomas M. Smith, *Project Whirlwind: The History of a Pioneer Computer* (Bedford, Massachusetts: Digital Press, 1980).

15. ~~(S//SI)~~ NSA CCH XII Z, Conferences at Dayton," 11 April 1945. Interviews with Phil Bochicchio, June 1994. (U) W. W. Stifler, Jr. (ed.) *High Speed Computing Devices:* By the Staff of Engineering Research Associates, Inc. (New York: McGraw-Hill Book Company Inc., 1950), 346.

16. ~~(S//SI)~~ NSA CCH Series XII Z, "Conferences at Dayton," 11 April 1945. Lt. Reid was also important to the project. The same type of selector problem drove OP-20-G back to film machines. But the Eastman-Kodak "Amber," described below, was created for the Japanese weather systems.

17. ~~(S)~~ NCML had received a German magnetic disk sometime late in the war, but magnetic disks were already known to Americans. Like the computer itself, magnetic disk technology was "in the air."

18. ~~(TS//SI)~~ NSA CCH Series XII Z CNO CITP TS-32, "Mercury," Washington, D.C.: Navy Department, December, 1945. (R) NSA CCH Series XII Z, "Mercury," May 1953.

19. ~~(TS//SI)~~ NSA CCH Series XII Z CNO CITP TS-32, "Mercury," Navy Department, Washington, D.C., December, 1945. ~~(R)~~ NSA CCH Series XII Z, "Mercury," May 1953.

20. ~~(TS//SI)~~ NSA CCH Series XII Z, CNO, "Brief Descriptions of RAM Equipment," Washington, D.C.: Navy Department, October 1947, 14.

21. ~~(TS//SI)~~ Mercury also had an electronic circuit that could set and record the "slides" the collator performed.

22. ~~(TS//SI)~~ NSA CCH Series XII Z, CNO, "Brief Descriptions of RAM Equipment," Navy Department, Washington, D.C.: Navy Department, October 1947, 14.

23. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. Mercury was retired in March 1949.

24. ~~(TS//SI)~~ NSA CCH Series XII Z, "Report of 3 January 1944 by Lt. L. Steinhardt: JN157 Rattler."

25. ~~(TS//SI)~~ NSA CCH Series XII Z "Report of 3 January 1944 by Lt. L. Steinhardt: JN157 Rattler."

26. ~~(TS//SI)~~ NSA CCH Series XII Z, "Memorandum of 3 January 1944 From Lt. L. Steinhardt, Another Idea for Rattler," 5 January 1944.

27. ~~(TS//SI)~~ OP-20-G-43, "FINAL REPORT, Project M-242, Rattler."

28. ~~(S//SI)~~ NSA CCH Series XII Z, Inventories of RAM Equipment, 1945. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. (U) NSA RAM File, CNO, U.S. Naval Communications, CITP TS-6 "Rattler," Washington, D.C., circa 1945. NSA NCML-CSAW Message File, October 22, 1943, Steinhardt to G, "Viper Design"; November 24, 1943, Ely to Desch, "Design of plugboard to automate Viper stecker analysis" and August 14, 1943, "Python to be shipped to Washington."

29. ~~(S//SI)~~ NSA CCH Series XII Z, L. R. Steinhardt, "General Purpose Machine (SERPENT)," OP-20-GE, 29 September 1944.

30. (U) It is important to note that Steinhardt did not mention the Robinsons, which were multitape machines. Perhaps that was because he had not been told of them.

31. ~~(S//SI)~~ NSA CCH Series XII Z, L. R. Steinhardt, "General Purpose Machine (SERPENT)," OP-20-GE, 29 September 1944.

32. ~~(S//SI)~~ NSA CCH Series XII Z, L. R. Steinhardt, "General Purpose Machine (SERPENT)," OP-20-GE, 29 September 1944, 4. "Rattan problems will demand a truly versatile machine in the early analytic stages. One such problem (involving something like the proposed "Imagination Machine") is now current; this could be handled very nicely on Serpent." By the end of the war, a traditional type of analog machine was built for one of the Russian devices. The Americans called their machine "Ricky."

33. ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G "War Diary Reports: March 1, 1943-May 31, 1948," August 1945.

34. (U) David J. Crawford, The Autoscritcher and the Superscritcher, forthcoming, *The Annals of the History of Computing* , NARA RG457, SRH-361. "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems," 269-270. NSA RAM File, CNO, U.S. Naval Communications, CITP-TS-39, "Duenna Operations Manual," March 1946, and TS-20 "Bulldozer Operating Manual."

35. ~~(TS~~/SI) NSA CCH Local Archive, "Army-Navy Descriptive Dictionary of Cryptologic Terms," Army Security Agency, February 1947, 131, defines scratching as the testing of assumptions by examining its implications for contradictions, eliminating those with contradictions, then "scoring" the remainder.

36. ~~(TS//SI)~~ NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March, 1945. f[4304] 9.

37. ~~(TS//SI)~~ NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March, 1945. f[4607] f[4142] 129 f[4149].

38. ~~(TS//SI)~~ NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G), RIP 425, "The American Attack on the German Naval Ciphers," October 1944 [*sic*], 129. ~~(TS)~~ NSA AHA ACC 17480, CNO CITS TS-17, "The N-800 Bombe," Washington, circa 1946. ~~(TS)~~ (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March 1945.

39. ~~(TS//SI)~~ NSA AHA ACC 35173, (CNO, CITS TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Navy Dept., Washington, September 1946. (TS//SI) NSA CCH Series XII Z, OP-20 to King, Duenna. ~~(TS//SI)~~ NSA CCH Series XII Z, Wenger to OP-20, 10 March 1945, "Statistical Bombe-Installation of."

40. ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G, "Memorandum, Statistical Bombe–Successful Installation of," 10 March 1945. A statistical grenade was the first goal. ~~(TS)~~ NSA AHA ACC 35173, CNO, CITS TS-49, "A Posteriori Remark on the Cryptanalytic Aspects of the Bulldozer," Navy Dept., Washington, September 1946.

41. ~~(TS//SI)~~ NSA CCH Series XII Z, OP-20-G, "Memorandum, Statistical Bombe–Successful installation of," 10 March 1945.

42. ~~(TS//SI)~~ NSA AHA ACC 35173, CNO, CITS, TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Washington: Navy Dept., September 1946, 3.

43. ~~(TS//SI)~~ NSA AHA ACC 35173, CNO, CITS TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Washington: Navy Dept,

September 1946, pages 3 and 8 give the "weights" assigned to each letter based upon analysis of Enigma traffic.

44. (~~TS//SI~~) NSA AHA ACC 35173, CNO, CITS TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Navy Dept., Washington, September 1946, points out that the practical limit in the machine was a forty-five-letter cipher because of the probabilities of Enigma wheel turnovers.

45. (~~TS//SI~~) NSA CCH Series XII Z, CNO, CITS Paper TS-30, "Bulldozer Supplementary Manual," Washington: Navy Dept., November 1945. Because cipher-only attacks could produce so many false hits, using Bulldozer on tests for wheel order and stecker led to extraordinarily time-consuming print checking. The unknown stecker was the truly difficult problem. (TS) NSA AHA ACC 35173, CNO, CITS TS-49, "A Posteriori Remarks on the Cryptanalytic Aspects of the Bulldozer," Navy Dept., Washington, September 1946.

46. (~~TS//SI~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949." The Americans had not yet told the British about the Bulldozer in 1947. On the fears about the security of the ECM, (~~S~~) NSA CCH Series XII Z, OP-20-G to Admiral King, "This may develop."

47. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, indicates that the pluggable reflector was primarily a Yellow system machine. (~~TS//SI~~) NSA (CCH Series XII Z, H. H. Campaigne and J. T. Pendergrass, "Second Report on Cryptanalytic Use of High Speed Digital Computing Machines," OP-20-L, 18 December 1946, Appendix I, shows that both the German Army and Air Force were beginning to use the new reflector. The OP-20-G cryptanalysts built Duenna on the assumption that each problem would take 5 x 10 to the sixth power tests. (~~S~~) NSA CCH Series XII Z, OP-20-GMF, "Report: Proposed Design for Duenna. Mark One," 25 February 1944.

48. (~~TS//SI~~) NSA CCH Series XII Z, "Uncle Walter," circa 1945.

49. (~~S//SI~~) NSA CCH Series XII Z, RAM list and Conference at Dayton, 11 April 1945.

50. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, "Duenna." (~~S~~) NSA CCH Series XII Z, OP-20-GMF, Report: Proposed Design for Duenna Mark One," 25 February 1944, 11.

51. (~~TS//SI~~) The most complete descriptions of Duenna and its allied cryptanalytic process are found in (~~TS~~) NSA CCH Series XII Z, CNO CITS Paper TS-39 "Duenna Operations Manual," Washington, D.C.: Navy Dept., March 1946; (~~S~~) NSA CCH Series XII Z, CNO, CITS Paper TS-39 "Duenna, Theory Manual," Washington, D.C.: Navy Dept., July 1946; (~~S~~) NSA CCH Series XII Z, OP-20-GMF, "Report: Proposed Design for Duenna Mark One," 25 February 1944; NSA AHA ACC 25057, CNO CITS TS-39 "Duenna Electrical Circuits," July 1946.

52. (~~TS//SI~~) NSA CCH "P" Collection Box CCO 67, RIP 608, CITS Paper TS-10/E-6, Enigma Series Vol. 6, Duenna," CNC-OP-20, January 1946, contains the technical description of "G's" version of the scratching attack.

53. (~~TS//SI~~) NSA CCH Series IV B-1-2, History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem, 268, implies that three different methods were developed by OP-20-G and SIS for the reflector problem and that the SIS attack and machines were significantly different from "G's." It also states that GC&CS's Giant machine embodied the SIS attack.

54. (~~S~~) NSA CCH Series XII Z, OP-20-GMF, "Report: Proposed Design for Duenna Mark One," 25 February 1944, 12.

55. (~~TS//SI~~) NSA CCH "P" Collection Box CCO 67, RIP 608, CITS Paper TS-10/E-6, "Enigma Series Vol. 6, Duenna," CNC-OP-20, January 1946, 6-3. Note that quite a different run time needed for Duenna to solve a problem is given in (~~TS//SI~~) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 269. It states that it took Duenna two weeks to test "all constantations" in a problem. The vast difference in time estimates is due to different definitions of "problem" and attack.

56. (~~TS//SI~~) NSA CCH Series XII Z, H.H. Campaigne and J.T. Pendergrass, "Second Report on High Speed Digital Computing Machines," OP-20-L, 18 December 1946, Appendix I. (~~S//SI~~) NSA CCH Series XII Z, OP-20-GMF, "Report: Proposed Design for Duenna Mark One," 25 February 1944, contains a

useful description of the Duenna menuing and of its printing system. The search and test logic is explained in, NSA AHA ACC 25057, CNO CITS TS-39 "Duenna Electrical Circuits," July 1946, 7-11.

57. (~~TS//SI~~) NSA CCH Series XII Z, (S12008) Navy Dept., Office of Chief of Naval Operations, DNC (OP-20-G, RIP 425, "The American Attack on the German Naval Ciphers," October 1944 [*sic*] (~~TS~~) NSA CCH Series XII Z, CNO CITS Paper TS-39 "'Duenna Operations Manual," Washington, D.C.: Navy Dept., March 1946, shows how the commutators' sensing systems were modified to fit the Duenna problem.

58. (~~S//SI~~) NSA CCH XII Z, OP-20-G-4-A, "Electronic Matrices," 1-9 September 1944. f[4253]

59. (~~TS//SI~~) NSA AHA ACC 25057, CNO CITS TS-39 "Duenna Electrical Circuits," July 1946, 13, 32, 44.

60. (U) David J. Crawford and Philip E. Fox (ed.), "The Autoscritcher and the Superscritcher: Aids to Cryptanalysis of the German Enigma Cipher Machine, 1944-1946," IEEE, *Annals of the History of Computing*, vol. 14, No. 3, 1992, 9-22. The Autoscritcher seems to have come into operation in early 1945, some months after Duenna had been brought to life.

61. (~~TS//SI~~) NSA CCH Series IV B-1-2, "History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem," 269.

62. (~~TS//SI~~) NSA CCH IX.B.1.9, SSA, "History of the Signal Security Agency, Volume Nine, History of the Development Branch," 10 February 1953, 76.

63. (~~TS//SI~~) NSA CCH Series IV B-1-2, History of the Signal Security Agency, Volume Two: The General Cryptanalytic Problem, 269, gives the date of first operation as Christmas 1944.

64. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," September 1954.

65. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," September 1954. (~~TS~~) (S2568) NSA CCH Series XII Z, "Tentative, Brief Description Of General Analytic Equipment for Enigma Problems," 26 March 1945.

66. (~~TS//SI~~) One bank was required for each cipher-plain pair being tested. (~~TS~~) NSA AHA ACC 11254, "OP-20-G, "Army Autoscritcher," 29 March 1945.

67. (U) David J. Crawford and Philip E. Fox (ed.), "The Autoscritcher and the Superscritcher: Aids to Cryptanalysis of the German Enigma, Cipher Machine, 1944-1946," IEEE, *Annals of the History of Computing*, vol. 14, No. 3, 1992, 12.

68. (~~TS//SI~~) NSA CCH IX.B.1.9, SSA, "History of the Signal Security Agency, Volume Nine, History of the Development Branch," 10 February 1953, 78. Although the machine proved difficult to maintain, it was used against "E" traffic and, then, attached to the 003 to function as a crib dragger for Swiss Enigma problems. (~~TS~~) (S2568) NSA CCH Series XII Z, "Tentative Brief Description of General Analytic Equipment for Enigma Problems," 26 March 1945, has an explanation of the use of the "cups."

69. (U) David J. Crawford and Philip E. Fox (ed.), "The Autoscritcher and the Superscritcher: Aids to Cryptanalysis of the German Enigma Cipher Machine, 1944-1946," IEEE, *Annals of the History of Computing*, vol. 14, No. 3, 1992, 15. (~~S//SI~~) NSA AHA 16899N, Army Service Forces, C. R. Deeter, "General Specifications and Technical Description: Super-Scritcher," 13 January 1945.

70. (~~TS//SI~~) NSA CCH IX.B.1.9, SSA, "History of the Signal Security Agency, Volume Nine, History of the Development Branch," 10 February 1953, 80.

71. (~~S//SI~~) NSA AHA 16899N, "Super-Scritcher: System and Circuit Details," points to the innovative ways the engineers avoided many of the pitfalls of purely digital circuits.

72. (~~S//SI~~) NSA AHA ACC 16899N, Harry B. Smith, "Ring of Modified Eccles-Jordan Trigger Circuits," 12 January 1945.

73. (U) Many of the electronic circuits were clever variants of digital designs, especially those designed to circumvent the need for hundreds of tubes to imitate or sense rotor signals. See (~~TS~~) NSA AHA ACC 16899N, Army Service Forces, David J. Crawford, "Frequency Sensing in Rotor Outputs: Super-scritcher," 17 January 1945. (~~TS//SI~~) NSA CCH IX.B.1.9, SSA, "History of the Signal Security Agency, Volume Nine, History of the Development Branch," 10 February 1953, 81.

74. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

75. (~~TS//SI~~) After the war OP-20-G did order an upgrade on ICKY, and Eastman reworked Amber and Hypo. (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949." But there was much discontent with film and the maintenance problems of the devices.

76. (U) Samuel Eliot Morison, *History of United States Naval Operations in World War II*, Volume XIII, *The Liberation of the Philippines, Luzon, Mindanao, the Visayas, 1944-1945* (Boston: Little Brown and Company, 1975), 59.

77. (~~TS//SI~~) NSA CCH Series XII Z, OP-20-G "Analysis of Analytical Machine Attack on JN-37," 24 March 1945.

78. (~~TS//SI~~) NSA, CCH Series XII Z, H.H. Campaigne, "JN-37, Prospectus of Attack On," OP-20-G, 27 January 1944.

79. (~~TS//SI~~) NSA CCH XII Z, "Statistical Projects Needed: First Report of," OP-20-G4A, 30 April 1945.

80. (~~TS//SI~~) NSA CCH Series XII Z, "OP-20-G: Analysis of Analytical Machine Attack on JN-37," 24 March 1945. (~~TS//SI~~) NSA CCH Series XII Z, OP-20-G4-A, "JN-7 Strength of Additives from a Two-Deep," 5 September 1945. (~~TS//SI~~) NSA CCH Series XII Z, "Utilization of Available Climatological Data for JN-37 Plain Text Estimates," OP-20-G-4-A, 13 June 1945. (~~TS//SI~~) NSA CCH Series XII Z, "JN-37: Major Computation Needed for Machine Weights," OP-20-G4-A, 3 May 1945.

81. (~~S//SI~~) NSA CCH Series XII Z, J. A. Skinner, "Proposal for Decoding Device," OP-20-G, 16 February 1943. f[4022].

82. (~~S//SI~~) NSA CCH Series XII Z, L. R. Steinhardt, "Additive Machines: Historical Summary of," 27 November 1944. (~~TS//SI~~) OP-20-G-4-A5, 23 November 1944, L. R. Steinhardt, "Possible Engineering Solutions for Full Selector Problems." (~~S//SI~~) NSA AHA ACC 26373, Frank B. Rowlett, "Report By the Subcommittee On the Application of Rapid Analytical Machinery to the Solution of Enciphered Code," 3 November 1944. (~~S//SI~~) Steinhardt, L. R., "Copperhead 11 (Project M-230) Final Report," 9 November 1944. (~~S//SI~~) NSA AHA 1505, John N. Seaman, "Memorandum for Major Edgerton, Liaison with Navy # 3, Use of Ram on Jap Naval Problems of B II Type," 9 June 1944.

83. (~~S//SI~~) NSA CCH Series XII Z, J. H. Howard, "Summary of Conference on the '37' Machine With Eastman-Kodak and NCR Co.," OP-20-G, 9 June 1945.

84. (~~TS//SI~~) NSA CCH Series XII Z, "OP-20-G: Analysis of Analytical Machine Attack on JN-37," 24 March 1945, part I Introduction, 8.

85. (~~TS//SI~~) NSA CCH Series XII Z, "OP-20-G: Analysis of Analytical Machine Attack on JN-37," 24 March 1945.

86. (~~TS//SI~~) NSA CCH Series XII Z, "OP-20-G: Analysis of Analytical Machine Attack on JN-37," 24 March 1945, part I Introduction, 10.

87. (~~S//SI~~) NSA CCH Series XII Z, J. H. Howard, "Summary of Conference on the '137' Machine With Eastman Kodak and NCR Co.," OP-20-G, 9 June 1945.

88. (~~TS//SI~~) NSA CCH Series XII Z, D. L. Noble, "Machine Weight Study for Proposed JN-37 Machine Part I," OP-20-G-4-D, 19 July 1945, and NSA CCH Series XII Z, D. L. Noble, "Machine Weight Study for Proposed JN-37 Machine Part II," OP-20-G, 2 August 1945, give insights into how difficult it was to set and maintain the photoelectric system so that false hits would be avoided and true hits tagged.

89. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, Cryptanalytic Machines in NSA," 30 May 1953.

90. (~~TS//SI~~) NSA CCH Series XII Z, J. H. Howard, "JN-37 Machine: Report of Conference at Eastman Kodak Co. on 25 May 1945," OP-20-G, 26 May 1945.

91. (~~TS//SI~~) NSA CCH Series XII Z, R. A. Rowley, "Preparation of Weighting Film, Secondary Stage Problem," OP-20-G, 2 August 1945.

92. (~~TS//SI~~) NSA CCH Series XII Z, R. A. Rowley, "Preparation of Weighting Film, Secondary Stage Problem," OP-20-G, 2 August 1945.

93. (~~TS//SI~~) NSA CCH XII Z, "Statistical Project Needed: First Report of," OP-20-G-4A, 30 April 1945.

94. (~~TS//SI~~) NSA CCH Series XII Z, "OP-20-G: Analysis of Analytical Machine Attack on JN-37," 24 March 1945.

95. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, NSA CCH Series XII Z, List of Machines and Targets, circa 1945. Actual run-times were not given for "37" jobs on Amber so an estimate had to be made based upon a general idea of the speed of the machine

and the degree of parallel processing built into it. The twenty-four-hour estimate was based on 800 comparisons per second and 100,000,000 tests. This estimate of hours coincides with an official estimate for a round-robin of 1,000 500-letter messages for a general coincidence test.

96. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

97. (~~TS//SI~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949."

98. (~~TS//SI~~) NSA CCH Series XI K, "JN-37 Machine Memoranda," and "Some Uses of Amber in Hagelin Attack," December 1949.

99. (~~TS//SI~~) OP-20-G did give Eastman a significant contract for new models of ICKY and HYPO after the war. However, it took many years for the new models to be delivered.

100. (~~S//SI~~) NSA AHA ACC 26373, SIS, "Minutes of RAM Meeting," 19 February 1945.

101. (~~S//SI~~) NSA AHA ACC 26373, SIS, "Technical Paper, RAM," circa June 1945, 3, 5. The SIS consulted with the navy about the new RAM ideas. (~~S//SI~~) NSA CCH Series XII Z, OP-20-G, "SSA Proposal for 70mm Film I.C. Machine," 8 June 1945.

102. (~~S//SI~~) NSA AHA ACC 26373, Frank B. Rowlett, "Report By the Subcommittee On the Application of Rapid Analytical Machinery to the Solution of Enciphered Code," 3 November 1944.

103. (~~S//SI~~) Apparently, it was men such as Dale Marston who took the lead as Leo Rosen seemed to favor electronic versions of the special-purpose tab-relay machines that IBM was building for the Agency. (~~S//SI~~) NSA CCH Series XII Z, Robert O. Ferner, "Rapid Analytic Machinery Needed for Research," June 3, 1943. On the RAM plans, (~~S//SI~~) NSA AHA ACC 26372, SSA, "Rapid Analytical Machinery," circa October 1943. (~~S//SI~~) NSA AHA ACC 26373 Frank B. Rowlett, "Two Copies of Report on Rapid Analytical Machinery," 3 November 1944.

104. (~~TS//SI~~) NSA CCH Series XII Z, "The Status of RAM," circa June 1945. (~~S//SI~~) NSA AHA ACC 26373, Chief, "F" Branch, "RAM Equipment," 29 March 1945.

105. (~~TS//SI~~) NSA CCH Series XII Z, "The Status of RAM," circa June 1945, (~~S//SI~~) NSA AHA ACC 26373, SIS, "Technical Paper, RAM," circa June 1945. (~~S//SI~~) NSA CCH ACC 26373, "Twenty-Fourth-RAM Report," 1 May 1945.

106. (~~TS//SI~~) NSA CCH Series XII Z, "The Status of RAM," circa June 1945, 7.

107. (~~S//SI~~) NSA AHA ACC 29373, SIS Chief "F" Branch, "Request for RAM Equipment," 23 March 1945, 7.

108. (S//SI) NSA AHA ACC 29373, SIS Chief "F" Branch, "Request for RAM Equipment," 23 March 1945. (~~TS//SI~~) NSA AHA ACC 26373, Frank B. Rowlett, "RAM in Future Cryptanalysis," 3 May 1945.

109. (~~S//SI~~) NSA CCH Series XII Z, OP-20-G, "SSA Proposal for 70mm Film I.C. Machine," 8 June 1945, commented on the army's request.

This page intentionally left blank

Chapter 7

(U) The Magic Continues

(U) Would History Repeat Itself?

(U) Hindsight might lead one to think it would have been easy to predict the future of the United States and its signals intelligence services after World War II. The Cold War and its consequences for America's military, industrial, and academic life seem "natural." The rise of Big Science, the development of a new type of university, and the growth of a massive intelligence establishment intertwined with public and private high technology institutions appear historically inescapable. Even the close relationship among Western nations, as reflected by the formation of NATO, and the exceptional cooperation between the intelligence agencies of Britain and the United States appear to have been foreordained.

(U) But in 1945 all of that was in the future, and much of it came as a surprise to the nation and to the leaders of the American communications intelligence community. For contemporaries, the future was uncertain. No one imagined that America was going to build a multibillion-dollar intelligence bureaucracy that seemed to have a life of its own. In fact, for those in the cryptanalytic organizations in early 1945, there were signs they might return to the isolated and have-not world of the 1930s, an era when American politicians condemned "reading other gentlemen's mail." The concerns about SIGINT's future had some foundation. Communications from the White House were less than subtle reminders that even the Soviets' communications should be treated as sacred.

(~~TS//SI~~) None of the codebreakers wanted a reversion to the attitudes and inadequate budgets of the 1930s, but a few thought that some degree of isolationism might be useful. They reasoned that a way to keep monies flowing to SIGINT would be to end World War II's dependency on Great Britain. A handful of influential men in the intelligence community suggested that the ties to Britain's cryptanalytic organizations be cut. With America's policymakers having to depend only on "G" and the SIS, they reasoned, there would be a decreased chance of their allocations being slashed.[1]

(~~TS//SI~~) Those beliefs were significant and contributed to the rejection of one of the most generous offers Britain ever made to the United States. The British had come to consider their attack on the Fish systems as their great cryptanalytic achievement. They saw it as their intellectual and, because of Colossus, their technological triumph. They also viewed Fish as an example of the cryptanalytic systems of the future. They foresaw the day when most systems would rely upon baudot-teletype, not Morse transmissions.

(~~TS//SI~~) When they offered the United States one of their Colossus machines in the summer of 1945, and more than hinted it would be followed by the cryptosecrets it required, they were shocked to learn their offer was rejected. They found it difficult to understand why and so did some Americans. Joseph Wenger wanted a Colossus in the United States, but the head of the technical arm of the SIS, Frank Rowlett, thought it unwise to accept a machine that was so complex and so expensive to maintain.[2] Combined with the desire for autonomy, Rowlett's objections were convincing.

(U) The rejection did not mean that American SIGINT planners were sure of their technological future. Men like Joseph Wenger had good reason

to fear the consequences of peace. World War II had not yielded permanent solutions to most of the problems that had frustrated him and Bush during the 1930s. The goal of creating a permanent intelligence-gathering capability had not been achieved and, certainly, the grand institutional dreams of Admiral Hooper had not been fulfilled.

(U) And as the war was ending, the achievements that had been made in the previous four years were threatened. It appeared that OP-20-G and the SIS would have to struggle to improve if not just maintain their powers. And they would have to do it alone. America seemed to be returning to a prewar institutional profile. The corporations, the universities, and the military were pulling apart.

(U) Big Science seemed about to be torn down. Vannevar Bush's NDRC had been a generous but only temporary big brother for the military and the aspiring research universities. In 1945, when NDRC funds were being cut off, no one was sure that academics wanted to or could continue to supply intellectual and technical solutions to the military.

(U) A greater cause for worry was the indications that the unity of purpose among the large corporations and the government was about to end. The relationship that had developed during the war seemed to be too costly to maintain. Industry's desire to return to high-profit work appeared to be impossible to overcome. No military agency could guarantee the high and consistent rates of return needed to persuade major corporations to continue to devote themselves to responding to military needs.

(~~TS~~) In addition, the private sector gave few indications that it would support expensive long-term investigations and developmental work that might compensate for the termination of the wartime research programs. Many promising technologies that had appeared during the bounty years of the war stood in danger of being ignored as military budgets declined. It seemed unlikely, for example, that universities would continue the type of research into radio wave propagation that had proven so useful to OP-20-G's interception program. There also seemed little hope that corporate programs would lead to the advanced demultiplexing equipment that the army and navy so desperately needed to tap into the modern transmission systems of their targets.[3]

(U) The prediction of the future of the federal scientific establishment was not comforting. The best forecast seemed one of a return to the lean 1930s. A weak National Bureau of Standards, a small navy Office of Research and Inventions in competition with a feeble ONR, and an army communications research program confined to a hungry Signal Corps might be all that the communications/intelligence agencies could look forward to.

(U) During the last months of the war, the gloomy predictions seemed to be coming true. Although the post-World War II situation would be infinitely better than during the 1920s, the army and navy cryptanalytic agencies would not have the partners, the resources, nor the autonomy they had during the preceding four years. It was not easy for them to continue to be technologically innovative, and, although they had a few more years of cryptanalytic "magic," they soon found it nearly impossible to meet the challenges of their most important cryptologic adversaries.

(U) What There Wasn't

(U) Like the story of OP-20-G and the SIS during the 1930s, the history of computers, automated cryptanalysis, and data processing in the SIGINT agencies between 1945 and the mid-1950s can be understood only in the context of what was not available to America's codebreakers. What wasn't there extends to much more than hardware. The institutional structure need-

ed for a dynamic response to technologically sophisticated mathematical/cryptanalytic confrontations did not exist. As important, World War II had not led to any great cryptanalytic methods revolutions. Although there had been much effort, mathematical cryptanalysis was something that still had to be created.

(U) There is a long list of other particulars. Chief among the "missing" were the modern computer and an industry willing to provide the special types of devices required for codebreaking and traffic analysis.[4] In 1945 the modern electronic digital computer was still a wish whose outlines were just being drawn. There were no commercial firms that were investing large amounts in its development, and academia, though willing, showed little sign of being able to carry the financial burden of bringing the universal computer to life.

(U) And many of those who saw the new electronic computer slowly emerging from university and corporate centers had very serious questions if that "serial" machine could ever have the power needed to conquer cryptanalytic enemies. The critics of the emerging general-purpose computer desired machines with more complex architecture, ones that relied upon multiple processors and parallel action. Such machines seemed unlikely to appear on their own, however. There were no indications that any outside group would even attempt to bring such alternative architecture to life without direct and massive support from the codebreaking community.[5] Worse, few companies seemed willing to take the money OP-20-G and the SIS did have to spend on automation. Both agencies experienced great difficulty before the 1950s in finding responsible contractors who would commit to building the latest generation of special-purpose electronic devices.

(U) Intellectual resources were also absent. The in-house mathematical groups that the two agencies had created had to be vastly reduced in size at the close of the war. There was no ready-made substitute. The American universities had not yet reestablished ways to link themselves to secret military projects, and the armed services and their major contractors had yet to invent the "think tank." The Rand Corporation, with its ability to allow academics to change into strategic planners, remained only a thought in the mind of the most aggressive air force generals.

(U) Institutional power was declining. Neither OP-20-G nor the SIS was sure that it could maintain the degree of autonomy granted to it during the war. The "G" section and the "F" group stood under the threat of losing their freedom to design machines and to select who was to build them.

(U) Despite an immediate postwar generosity that extended the life of some programs, there were indications in early 1945 that signals intelligence might have to remain passive, only waiting on the sidelines while, hopefully, someone else made the great technological leaps needed to match advances in code and cipher making.

(U) Signs of Some Appreciation

(U) However, during 1945 there was some encouraging news. The SIS's and OP-20-G's wartime achievements had made them a few very good and very influential friends in the military. From the most important generals and admirals came words of praise for Ultra. With a little convincing by advocates such as Joseph Wenger, that praise was turned into promises by America's leaders to provide at least some of the resources needed to maintain and, perhaps, improve communications intelligence capabilities.

(U) Although budgets were slashed and work forces seriously reduced, the SIS and OP-20-G were granted more than should have been expected given their treatment in the 1930s. The fifty-percent reduction in the amount of IBM equipment in 1946, for example, still left the agencies

with 300 machines. That was tens of times more than what was on hand at the start of the war.[6]

(~~TS//SI~~) The SIS was allowed a staff of 1,500, and "G" retained some 700 people – infinitely greater numbers than had been allocated to the services during the 1920s and 1930s. That gave some hope that although the United States had not yet decided to take responsibility for policing the entire world, a signals shutdown was unlikely.[7]

(U) Significant for the history of computers and cryptanalysis were the numbers of "technical" slots allocated to each agency. Both had approximately five percent of their staff approved to work on advanced technological and scientific matters. Those ratios were maintained during the postwar period, with the navy gaining a slight but important edge over the army in the numbers of high tech employees.[8] The technical sections were not large enough to support huge in-house production capabilities, but they were capable of pursuing some research and creating smaller machines.

(U) More than numbers of people indicated the value military leaders placed on centralized SIGINT. Although no firm promises could be made in 1945, hints were dropped that none of the cryptotechnologies would be abandoned. Whether the favored technology was the IBM tabulator-relay combinations or the electromechanical components in Madame X, they would be given a chance to develop into more powerful versions of what had emerged during the war.

(U) The most tantalizing hint concerned the possibility of an aggressive new Rapid Machine program. During late 1944 and 1945 the army and navy engineers were allowed to draw up some relatively long-term plans for very advanced machines. Different groups had their favored approaches. Many in the agencies wanted to concentrate on extending the reach of the workhorse tabulating equipment. Others sought continuity through extending the reach of the Bush Comparator. A few continued to have faith in the type of analog and microfilm devices that had been built at Eastman-Kodak. Of course, there were vocal advocates for turning digital electronics into operational machines.

(~~TS~~) There was a consensus on the role of SIGINT in developing all the technologies: "G" and the SIS should play an active part in bringing to life any new hardware. That was almost inescapable. There was much to be done and few on the outside willing to do it. There was no general-purpose electronic device that was a great advance over Bush's old Comparator, and even the mundane, such as input and output technology, remained at the early levels.[9]

(U) More MAGIC: Cryptanalysis Continues as Before

(~~TS//SI~~) The chance to finally build analytic machines that would put America ahead of the technology of encryption seemed favorable during the first postwar years. One reason for that was America's continued cryptanalytic successes. The machines it had in hand were providing intelligence. In several instances "G" and "F" had to hurry to finish new machines, but, in general, the agencies did not have to concentrate, as during the war, on emergencies. For three years after the end of World War II, there was every indication that the kind of triumphs that had been achieved during the early 1940s would continue. As important, even the most dangerous of the nation's adversaries had decided to refrain from creating military crises. Success gave the agencies time to look ahead.

(~~TS//SI~~) The impressive work of the American SIGINT agencies continued on after the Japanese surrender; remarkably, it even seemed to be improving. Every type of code and cipher used by every important nation was or seemed about to be conquered. Despite the introduction of more sophisticated methods and

machines, some 70 percent of the systems of the minor nations were "readable" in 1946 and 1947, and over half of those of the three new major targets were, to a significant degree, open to the United States.[10]

(~~TS//SI~~) With help from the British, some of the most critical and well defended of the Soviet codes and ciphers were yielding information. There was every reason to believe that what had been accomplished against the Germans and Japanese would be repeated against Russia and its allies. Progress seemed inescapable. By 1947, for example, engineers at the army and navy centers could build relay analogs of some of the important Russian cipher devices, just as they had built analogs after Japan's Purple machine had been penetrated.[11]

(~~TS//SI~~) The systems being entered were important. It appeared that, as in World War II, America would be able to gain critical intelligence through the interception and analysis of a relatively small number of messages, ones which would reveal the strategic thinking of the political and military leaders of Russia and its client states.[12] During the first postwar years, old attacks and machines were doing quite well. More than operator errors and busts were leading the Americans and British into the Soviet additive codes, [redacted] Although Russia's new [redacted] machine proved stubborn, there was hope that a persistent search using traditional tools would uncover its wiring and its indicator system.[13]

(~~S//SI~~) That image of a consistent SIGINT future shaped the nature of the immediate postwar machine development programs at the army's and the navy's Washington headquarters. Both agencies sought cryptanalytic, not "data," machines. The goal in the first postwar years was to create new generations of machines to break complex codes and ciphers. Other possible sources of information, including traffic analysis, were left to older machines and methods.

(~~TS//SI~~) Something besides that cryptovision shaped the initial postwar plans. It was thought that, unlike the years of the Atlantic U-boat crisis, no massive and emergency machine construction program would be needed.[14]

(U) A Cryptanalytic Future: Architecture and Ambiguity and Budgets

(U) Everyone saw the future of "G" and the SIS as centered on the traditional cryptanalytic function. Traffic analysis, direction finding, and analysis of enemy clear text might play roles but very small ones. But all was neither secure nor settled, especially in 1945 when plans for both immediate and long-term machine development were being created. Although there was an agreement about general target priorities for the immediate postwar era, the exact nature of the cryptosystems and machines that might be confronted was not predictable.[15]

(~~TS//SI~~) Some trends were evident, however. [redacted] His company's products would probably be used by every nation. The second trend was towards the adoption of on-line machines. Many nations were adopting the type of baudot-teleprinter and multiplexed systems that had formed the backbone of the German Fish networks.

(~~TS//SI~~) In addition, there were at least concerns that Enigma-like wired rotor machines might reappear, and it seemed likely that super-enciphered code systems would not vanish with the fall of Japan.The formidable one-time pad systems that seemed unbreakable when correctly used were known to be a favorite of many diplomatic corps.

EO 3.3(h)(2)
P.L. 86-36

(~~TS//SI~~) But nothing about target systems, with one exception, was so certain, nor the development of the underlying technology for analytic machines so predictable, that a rush to create a host of new special-purpose devices was justified in 1945.[16] There was no reason to build a series of high-tech single-purpose, single-system machines, except for some of those manufactured by

(~~TS//SI~~) The could be dealt with through existing relay, even tabulator equipment, as could many of the remaining additive systems, such as those used by Soviet agencies. Not enough was known in 1945 about the new teletype-baudot devices to warrant the construction of expensive special-purpose contrivances. As well, since the promises of the discovery of effective pure mathematical methods had yet to be fulfilled, launching into an expensive search for a new "calculation" machine seemed unjustified.

(~~TS//SI~~) Only one type of machine, a new deserved special technological attention at the end of the war. It was the series. The Americans knew it was going to be used for high-level systems by many important nations; they had enough knowledge of its inner workings to challenge it; and they were confident they could pick the correct attacks.[17] As a result, although many new machines would be built, the only adventurous special-purpose RAM planned for a specific problem at the end of the war was for the [18]

(U) The Enigma Is Dead (We Think); Long Live the

(~~TS//SI~~) The first step towards a new machine program at "G" and the SIS was to sort out what WWII machines should be abandoned. All but a score of the navy Bombes were destroyed, and the million dollar Madame X was taken apart. The Duennas, the other elaborate Bombes, and the electronic Scritcher were kept, however.[19] It was thought they could be used against other rotor machines or the few Enigmas that might be brought back into use. All the devices that had been effective against the were retained. They were refurbished and readied to attack diplomatic, civil, and military traffic from around the world.[20]

(~~TS//SI~~) The Bombes and the other "E" analogs were useless against

~~(TS//SI)~~ The investment needed to conquer the more [redacted] seemed reasonable. And success would provide invaluable returns. For example, with Germany and Japan defeated, stripped of their colonies, [redacted]

~~(TS//SI)~~ The potential rewards from investing in attacks against other nations' Hagelins were even greater. [redacted] was "the" manufacturer of cryptodevices, and every nation, business, and bank in any part of the world had to rely upon his products. From South America to Northern Europe to Arabia, if automated encryption was being intercepted, it was probably the product of a [redacted]. There was one other very important aspect of the [redacted] one that helped launch the American cryptanalytic attacks against it. The [redacted] machines could be purchased on the open market and their inner workings closely studied.

(U) A Hangover from Another Time

~~(TS//SI)~~ One of the first postwar [redacted] RAMs had a strange beginning. It dated to when the navy still thought it would have to launch a bloody invasion against Japan.[22] "G's" mathematicians needed a large and fast digraph counting machine to attack various Japanese systems. The device had to be much more powerful than the creaky Mike. Although it would be expensive to build, "G" approved a request for the "counter." But the machine was almost canceled when Japan surrendered. Fortunately, the mathematicians were able to convince Engstrom and Wenger to continue the project. They agreed that despite the about-to-appear second Freak at Arlington Hall, the navy needed a universal counting device for its postwar missions. It would help, they realized, in the initial mathematical studies of unbroken systems and machines.[23]

~~(TS//SI)~~ With promises of financing in hand, machine designers were consulted about technological options. It was decided that the original proposal to build a machine to handle an alphabet greater than sixty-four characters was impractical. Also quickly rejected was the idea of basing the counting machine on a film-analog combination as had been recommended earlier.

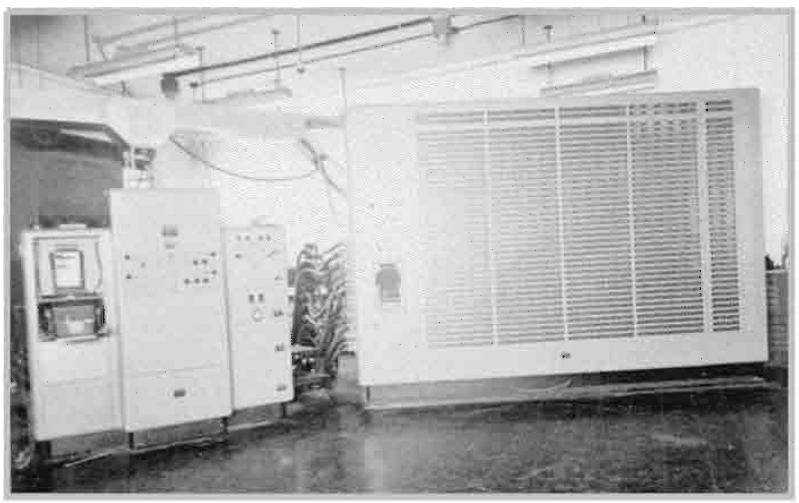
~~(TS//SI)~~ The "G"NCML team explored other possible technologies and then made a surprising decision. Although "G" was filled with advocates of electronics, its engineers decided to let the army's Freak carry the risks of building an "electronic" counter. Whether condensers or tubes were used, said the NCML crew, too many of them would be needed for a useful digraph machine. With a sixty-four by sixty-four matrix and the counters required to handle up to 999, the number of components, they concluded, would be too great. There would have to be more than 3,997 counters, each needing three positions. Temperamental electric or electronic parts meant too many errors and too much "down time." For the navy's engineers, old-fashioned reliable electromechanical counters were the only viable alternative.

~~(TS//SI)~~ They were close to gaining the final approval of the cryptanalysts; then someone calculated the speed of the machine if it used the off-the-shelf industrial counters. The device would be incredibly slow, as sluggish as the old frustrating Mike. There was a standoff. The codebreakers wanted a fast machine, but the engineers would not accept the responsibility of an electronic device. After much wrangling, they arrived at a compromise. The engineers decided they would take the responsibility of designing custom-made mechanical counters that were fast enough to please the cryptanalysts.

(~~TS//SI~~) After outlining the new counters, the engineers sought a contractor. Unfortunately, "G's" two largest World War II contractors, NCR and IBM, did not want to take the project. "G" had nowhere to go, and the machine was put on hold during much of 1945 and 1946.

(~~TS//SI~~) "G" waited until its "captive corporation," Engineering Research Associates, was formed before it put any more effort into the counter-project. But once ERA agreed to take the contract, "G" was sure it would soon have a useful and reliable machine.That was a rather naive assumption, however.

(~~TS//SI~~) What became known as Alcatraz did not appear until 1950, had about half the power originally planned, and was much more expensive than expected. Once in operation, it threw technological tantrums. It had problems with its large printer, and the expense of maintaining the machine led to Alcatraz's very early retirement in 1954.[24]



(U) Alcatraz

(U) Mrs. O'Malley's Wayward Son

(~~S//SI~~) Another of the special devices OP-20-G thought it had to have in order to deal with its postwar targets became, arguably, the largest electronic imitation of an adding machine ever built. Filling half a room with vacuum tubes, relays, a special card reader constructed by the IBM spin-off Commercial Controls, and a tabulator's printer, O'Malley was one of postwar "G's" earliest and most challenging projects.

(~~S//SI~~) Something like O'Malley had been desired since 1942, but it was the growing backlog of messages [redacted] and some technological advances that sparked its final design in 1947. O'Malley was the cryptanalysts' special and very grand version of what IBM had introduced at the end of 1946, an electronic multiplying machine. O'Malley had to be special and had to go beyond IBM's offering because it was to accomplish what Bush and Wenger had agreed was not achievable in the mid-1930s, the automation of the advanced version of an IC test, Chi.

(~~S//SI~~) The cryptanalysts' "Chi" was a very close relative of the Chi Square test. Chi Square is a now familiar statistical method for determining if two distributions came from the same "universe." It seems commonplace and unsophisticated today, but in the 1940s, especially because of the tedious calculations it needed, Chi seemed very advanced. It was one of the most sophisticated ways to identify cipher alphabets produced by the same key.[25]

(~~S//SI~~) As it was used in cryptanalysis, "Chi" was computationally demanding. The frequencies of each letter in one cipher text had to be multiplied against the corresponding frequencies in another text: then the products had to be summed and used in the algorithm which determined whether or not the sum was

likely to have been produced by chance. To isolate probable "same key" messages called for testing each text against all the others. That meant thousands of multiplications, hundreds of additions, and dozens of evaluations for the simplest attacks.

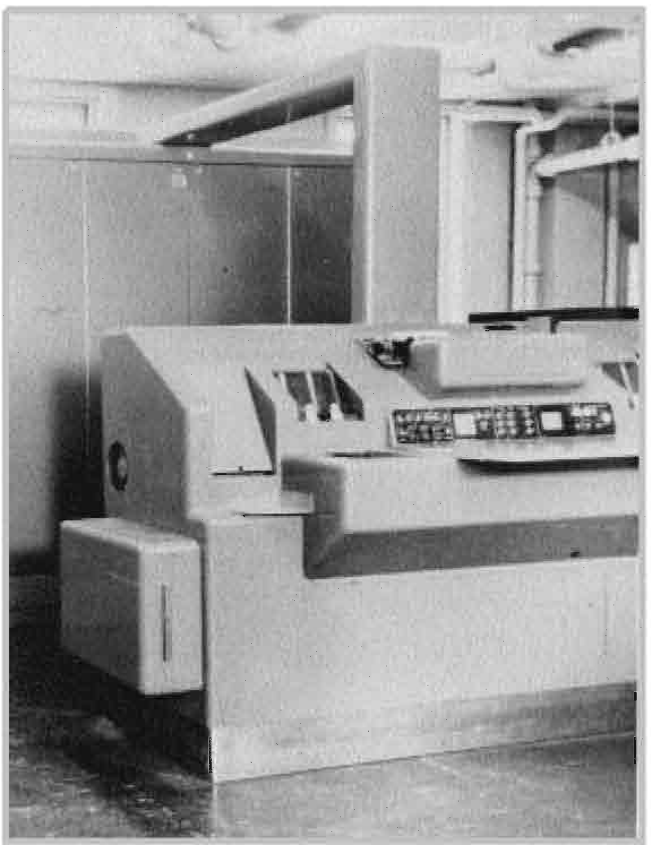
~~(S//SI)~~ The manpower-starved "G" realized that if the World War II victories against [redacted] devices were to be continued, it had to have an ultra-powerful machine for accumulating the frequencies, calculating the sums of cross-products, identifying the "significant" sums, and displaying the results. Given the exploding workload of those charged with keeping up with the [redacted] generated traffic, it was decided that an electronic high-speed multiplier was worthy of an enormous financial investment.

~~(S//SI)~~ The new navy contractor, Engineering Research Associates (ERA), was asked to build a super-fast machine that could recognize individual letters, tally them, and then perform all the thousands of multiplication and summations needed to identify those cipher messages whose letter frequencies "correlated." And it was asked to produce it quickly.[26]

~~(S//SI)~~ That was a demanding request in the technological context of 1947. ERA was expected to produce a machine more powerful than what had been developed by the world's largest and most advanced computing machine company: the IBM 603 electronic calculator, which had been introduced in late 1946.[27]

~~(S//SI)~~ Within a year and one-half, the men in St. Paul were able to build an electronic "calculator" several orders more complex than the IBM device; but the need to shift attention to the production of another machine, one for critical SIGINT fire fighting, led to O'Malley being far below original expectations. To save design and production time, O'Malley became a "get the job done" machine. It was stripped of many of its intended powers so that it could be out into operation as soon as possible.

~~(S//SI)~~ Many of the interesting technical challenges in O'Malley's original specifications were avoided. First, it was decided that, as in the 1930s, recognizing and tallying letters were chores best done by older methods and technologies. Separate machines would prepare the letter frequency counts. O'Malley was deprived of even more functions. It did not include the circuitry needed for an automatic test for the significance of the results. All the summed cross products were printed, leaving the analysts with the need to do much hand calculation. And O'Malley even



(U) O'Malley

needed help reading its input. Given the available I/O technology, a special machine had to be constructed to punch tallies into IBM cards in a special format and the standard IBM readers had to be reconfigured.

(~~S//SI~~) Without that jury-rigged equipment and its special dual teletype tape readers, O'Malley would have taken more years to construct. "G" could not wait, for example, for magnetic drums that could have provided a high-speed means of presenting two streams of data. The quick fixes to the old card and tape technologies had to be accepted.

(~~S//SI~~) O'Malley became part of the tradition of the relay box and tabulator combinations of the NC Machines of World War II. Like them and the new IBM 603, it was a special-purpose (although electronic) calculation box inserted between tabulator-teletype input and output equipment. The inside of the machine also reflected the time pressures under which it was constructed. It certainly did not break any new logical ground; it was a direct imitation of a decimal-based electromechanical calculating machine. It multiplied by following the traditional method of repeated additions.

(~~S//SI~~) Such conservatism did not mean that O'Malley was a minor accomplishment, however. Commercial firms, such as IBM, Remington-Rand, and UNIVAC, based their early electronic offerings on the same philosophy of following known architecture and logic. Ring-counter, decimal machines were the norm. Binary devices were the challenging exceptions that were very slow to appear on the market or even in the laboratory.[28]

(~~S//SI~~) And for its time, O'Malley did its calculations quite rapidly. It was able to form and sum as many as thirty-five cross products in one and one-third seconds. It could have done its work much faster, but it was limited by its lack of memory and its very slow printer.

(~~S//SI~~) O'Malley proved useful for more than its original limited operational job. When O'Malley was asked to serve the needs of research mathematicians, its tubes and relays were persuaded to pretend they could, for example, invert matrices.[29]

(~~S//SI~~) But all in all, economy and a need to obtain the final equipment as soon as possible meant that O'Malley was a compromise that had a short life. Perhaps it was its recurring I/O problems that led to O'Malley's untimely and perhaps embarrassing end. It was allowed a relatively peaceful retirement twenty months after its birth.

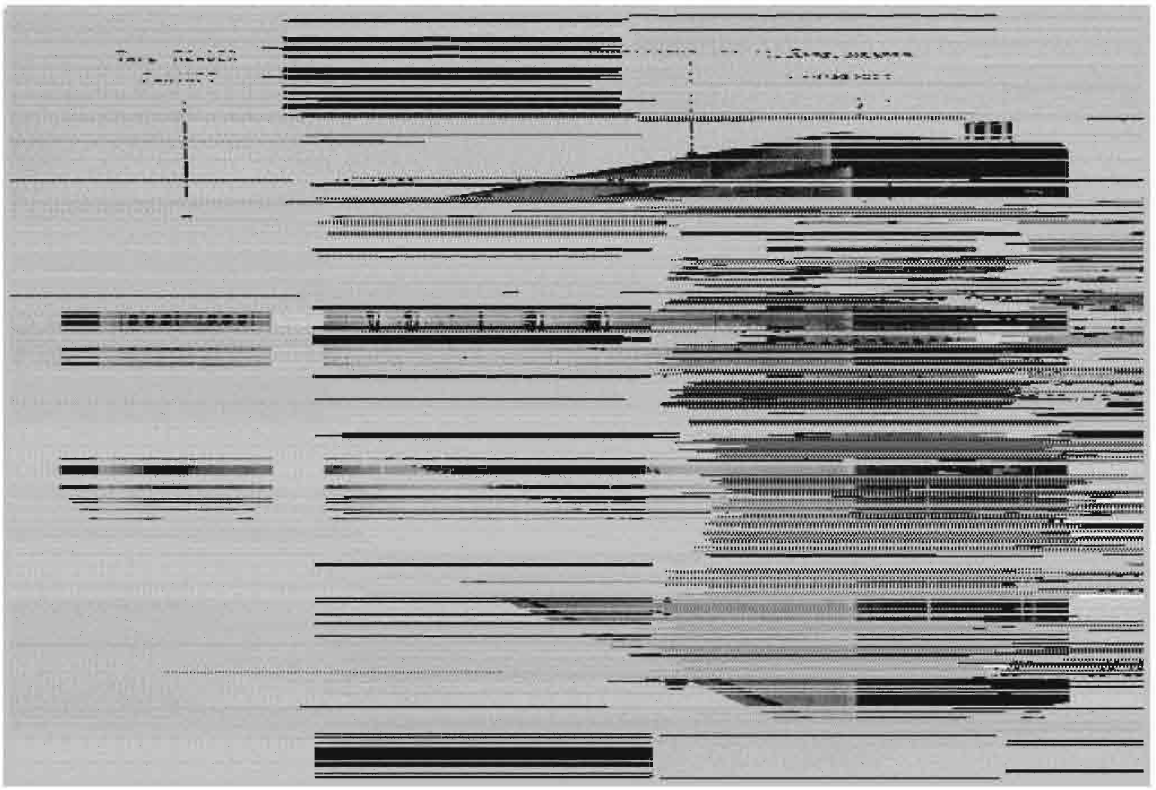
(~~S//SI~~) The Grand [redacted] Machine

(~~TS//SI~~) O'Malley and Alcatraz were not the heart of the planned postwar attack on the [redacted] machines. A very special device had been under consideration well before Germany's defeat. But the central [redacted] Hecate, had to wait until "G" formed its captive corporation, ERA.

(~~TS//SI~~) Hecate was more than two years in the making, arriving in Washington in 1948. Built with the help of the ex-OP-20-G engineers, such as John Howard, Hecate was a combination of the old and new.

(~~TS//SI~~) But even borrowing from the past did not make Hecate easy to complete. It was a huge and expensive combination whose cost estimate of $80,000 became a delivery price of almost $250,000.[30] Its price tag, the cost of five World War II Bombes, was justified by results, however. It and its sister produced a constant [redacted] for more than a decade.[31] Hecate was, in fact, one of the electronic marvels of its time.

(~~TS//SI~~) Hecate contained some true advances, such as its four high-speed electronic tube "rings" that imitated the [redacted] in the [redacted] They ran at a very respectable 200 KC



(U) Hecate

(100,000 trials a second). And Hecate's scritcher-type capability of eliminating branch searches speeded processing enormously.[32]

(~~TS//SI~~) To save construction time, electronics were employed only where demands for speed presented no alternative. Hecate might have been even more innovative, but it was called out of the workshop for immediate operational needs. Most of the machine was composed of the familiar and reliable plugboards and relays, and its essential logic was based upon familiar cryptanalytic-engineering approaches.

(~~TS//SI~~) Hecate was not a digital computer and did not calculate. It was an analog "crib" machine with some "digital" components. Like the Grenades, it used a short ten- or twelve-letter stretch of suspected plain text to identify "starting points." And it was not a complete processor. Much independent statistical analysis of a system was needed before Hecate could find the initial settings for a transmission. And its power was limited to just [redacted]

(~~TS//SI~~) To use Hecate the cribs were set with dials; then a message was read, letter by letter, into Hecate's relay memory through a standard tape reader. When the relay memory had the required number of letters in it, the electronic rings were run through their positions until the parallel flows of electricity through the plugboards and relay circuits signaled that all the crib-plain pairs and ring positions were consistent, or that all the wheel positions had been tested. At a hit, the machine stopped and dials indicated the position of the "rings" and the place of the crib in the message. The dials were used because there

was still no printer that was fast and reliable enough to compete with hand notation.

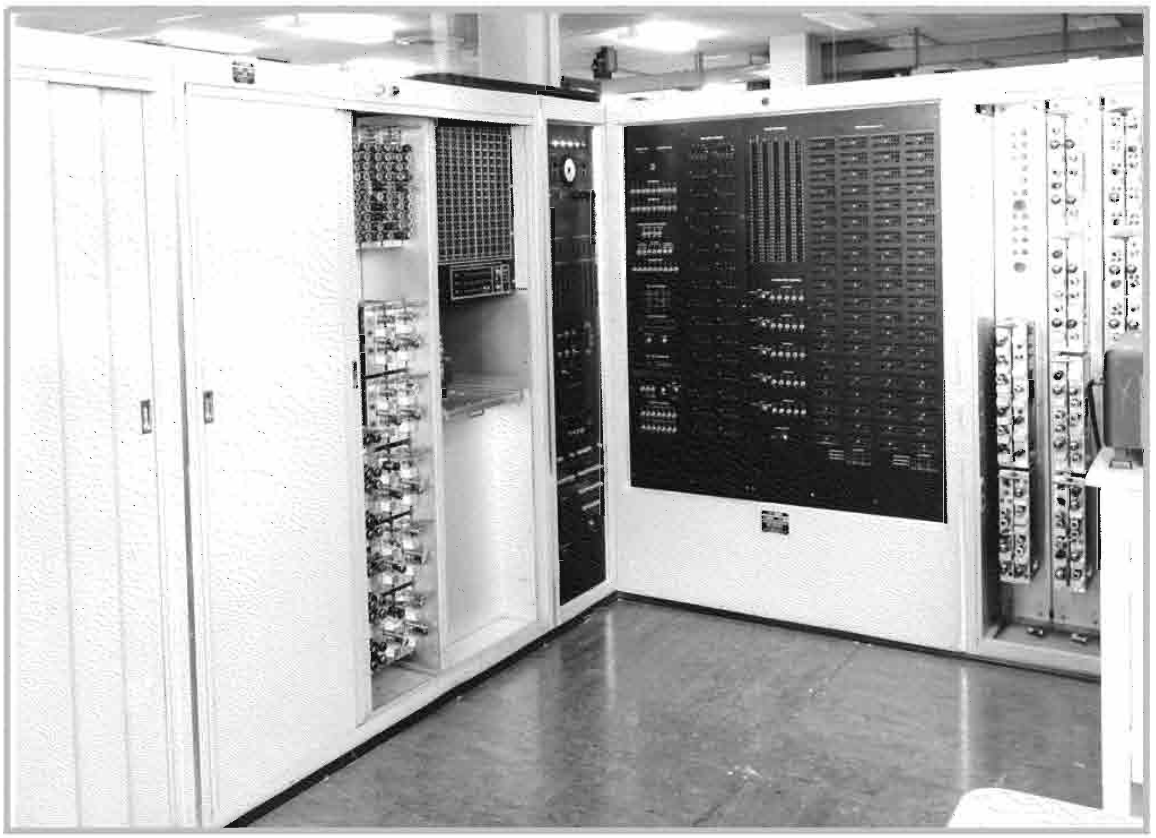
~~(TS//SI)~~ Each of Hecate's offset letter tests took approximately three seconds, excluding the time an operator needed to write down the hit positions. It took a total of approximately twenty minutes to run a 500-letter message.[33]

~~(TS//SI)~~ Hecate was reliable and effective, but, like the Bombes, she had some serious deficiencies. Because of the nature of her test, circuit completion, Hecate could produce too many possible answers. Each had to be examined by a limited workforce. To reduce the list of possibilities required difficult-to-find, very precise, and error-free cribs. Worse, Hecate could be used agains-tonly [redacted]

[redacted]

~~(TS//SI)~~ Hecate's limitations were recognized while it was under construction, but the machine was needed so badly that it could not be abandoned nor radically altered.

~~(TS//SI)~~ OP-20-G had no solution for the [redacted] of intelligence. The go-ahead was given for the development of another special-purpose device, Warlock.



~~(TS//SI)~~ Warlock I

(U) Hecate's Impressive Competitor

~~(TS//SI)~~ Warlock was much more adventurous and costly than Hecate, so much so that it took some four years to design and manufacturer.[34] It was physically big as well as expensive. It was so large that it had to be kept at the ERA factory in Minnesota. Warlock turned St. Paul into something of a remote operations center.[35]

~~(TS//SI)~~ Warlock cost more than $500,000[36] because it called on the sophisticated cryptanalytic test that the Americans had first used in Bulldozer, automatic plain language recognitions.[37] Automatic recognition was demanding in its own way; it called for very, very long cribs. Fortunately, they did not have to be of a specific nature. To avoid the "false hits" that came from short and weak cribs, Warlock used some seventy-five or more ciphertext letters. All of them were needed just to eliminate much of the handtesting Hecate runs called for.

~~(TS//SI)~~ Warlock was a major engineering feat because it was very difficult to turn high-speed plain language recognition into electronics. Warlock was piled full of the latest electronic tubes and circuits. With the cipher text in place, super-fast "digital" electronic wheels sped through [redacted] weighted each resulting letter according to its language frequency, then summed all the results in parallel. An electronic threshold-testing component decided if the settings and a sample of the selected plain text should be printed.

~~(TS//SI)~~ One hundred thousand tests a second were performed, which meant that the plain text could be fully examined in twenty minutes.[38] To run through the [redacted] so quickly called for over 6,000 tubes, crystal diode matrices, trays of relays, flexible electronic matrices, some binary circuitry, the familiar plugboards and relays, and even a magnetic drum.

~~(TS//SI)~~ The first Warlock was a machine that could attack just one or a few [redacted] systems, but its 1953 version was able to do more because of its advanced electronics. Flexible [redacted] machines. For example, Warlock was asked to penetrate the mysterious [redacted] machine that served all of [redacted]

~~(TS//SI)~~ Although Warlock shared many circuits, components, and ideas with the general-purpose computer, it was a special-purpose device with much of the internal logic of Bulldozer. Although very effective, it was a one-function machine, something many in the intelligence community, especially those in charge of budgets, disliked.

~~(TS//SI)~~ Both the money managers and the engineers wanted something else, a multipurpose cryptanalytic computer, one that could perform any or all the cryptoattacks. Such a machine would never sit idle waiting for messages from a particular system, nor would it become a useless dinosaur like Madame X.[40]

(U) The Universal RAMs

~~(TS//SI)~~ Many in OP-20-G and the SIS wanted to start designing such a universal RAM in 1945. They were not abstract types; their RAM was to be tailored to operational cryptanalytic needs. Those advocates for the universal RAMs refused to wait until a mathematical revolution transformed cryptanalysis or a technological revolution made the general-purpose programmed computer a competitive cryptotool.

~~(TS//SI)~~ For those in favor of universal RAMs, extending the general cryptanalytic techniques that had proven so valuable during the war seemed the only reasonable path for "G's" postwar machine program.[41] But they wanted to avoid the waste that went along with creating spe-

cial-purpose machines. Given the unknowns about future cryptotechnology and the need to maximize research and development funds, the wisest choice for them was to create a machine that could perform all the major cryptanalytic functions.

~~(TS//SI)~~ Those major functions fell into a few broad categories. The most important of the crypto-techniques were based upon either locating repeated patterns, tallying massive numbers of letter patterns, stripping possible cipher and recognizing plain text, or performing some form of "exhaustive searching," such as done by the scritcher machines.

(~~TS//SI~~) The universal RAM was not to be a super-calculator for advanced mathematical calculation, or a direct analog of a cryptosystem, nor one that could be called a data processing machine. And although it was agreed it would be digital and electronic, it was to be something very special and unique to the cryptanalytic community.

~~(TS//SI)~~ In 1945 and early 1946, both agencies made a commitment to find, if possible, their own versions of one great multipurpose cryptanalytic engine.[42]

(U) The Illusive Matrix

~~(TS//SI)~~ The call for the universal RAMs became tied with the search for an electronic "matrix." The universal machine needed it and so did a new type of Bombe, one that could attack any type of rotor enciphering machine through a Turing-like analog test. There was also a demand for an electronic matrix that would serve as the heart of all the more digitally oriented dedicated machines of the future, whether they were for wired-wheel or additive attacks.

~~(TS//SI)~~ The concepts of the matrices were not well formed in 1945. In some instances a matrix was described as being high-speed memory, in others as an electronic version of a switch, and in still others as an analog of an encryption wheel. But whatever the purpose, existing tube technology made any matrix design very difficult to construct. The problem that had halted the creation of an electronic Bombe in 1942 continued after the war. The matrices demanded too many tubes to be practical.

~~(TS//SI)~~ As a result, much of the "matrix" effort was concentrated on developing multipurpose tubes and other basic components. That research became essential to other projects, including the search for the multipurpose cryptanalytic machine.[43]

(~~TS//SI~~) In addition to the hunt for the electronic "wheel" for the universal RAM, both services had special-purpose uses in mind for an electronic matrix. Many in the navy wanted, as soon as possible, an electronic version of the valuable but none-too-well-behaved monster, Mercury, and the army desired a vastly improved version of its "look-up" devices, the Slide-Run machines. A few wanted an electronic super Bombe that could tackle many different machine systems through a Bombe-like test.

~~(TS)~~ But the demands for a universal machine continued. And soon its outline became clear. It would be something quite different from the programmable general-purpose computer.

(U) It's a Nice Idea, Dr. von Neumann, But...

~~(TS)~~ As "G" and the SIS focused on their versions of one great device during 1945 and 1946, they came to quite similar concepts of a single machine that could perform all the general attacks that had proven so valuable during the war. Both had visions of a "computer" that performed IC tests, crib-dragging, locating, additive stripping, and weighted plain language testing. The near-universal machines began to be assigned a generic name, a "reconfigurable computer."

(~~TS//SI~~) Neither service was able to build its ideal "reconfigurable" machine during the 1940s because of institutional barriers, the primitive state of some of the underlying technologies, and emergencies that called for energies to be devoted to special-purpose machines. But "G" and the SIS went far towards defining a powerful and unique cryptanalytic computer architecture through their Goldberg and Sled projects.

(~~TS//SI~~) There were differences between the content and progress of the two grand dreams, Goldberg at "G" and Sled at the SIS,[44] but at their beginnings they shared many fundamentals.

(~~TS//SI~~) Neither of the proposed all-purpose machines was conceived of in terms of the architecture of the modern digital computer. Their designs were very different, for example, from what was emerging out of the ENIAC/EDVAC projects at the University of Pennsylvania. They were not single processor, serial, binary, and program-driven machines, the type that later became characterized by the term "von Neumann architecture."

(~~TS//SI~~) Such an architecture seemed very inefficient to the cryptanalysts. Well into the 1960s there were engineers and cryptanalysts who remained committed to the idea that the digital, serial, single memory, program-driven "von Neumann design" for computers was an inappropriate model for codebreaking.

(~~TS//SI~~) Perhaps that was because their concepts of computers were problem, not abstraction, driven. The proposed army and navy machines were not born out of considerations of how to solve any possible logical or mathematical problem. Neither was intended to be a universal logic or mathematical device. They were to be extensions of the hardware and methods that had evolved at the agencies during World War II.

(~~TS//SI~~) The first source of inspiration for them came from the developments in the tabulator sections. Both agencies had invested in the creation of very efficient relay attachments for their tabulating equipment. The special IBM "boxes" became heroic in the eyes of the operating cryptanalysts and their machine room allies. Each of those minicomputers, some of which were much larger than the tabulators, performed a special function. The Slide-Run attachments, for example, stripped additives, then searched a dictionary of high-frequency code groups. The navy's NC tabs were also built from a wide range of functional relay boxes.

(~~TS//SI~~) Another source of inspiration was the RAM program's faith in electronics and film and tape inputs. There had been many thoughts of enlarging the powers of the Comparators and the IC machines through the use of additional circuits, ones that could be accessed through convenient plugboard "programs." Putting the counting abilities and message-offsetting abilities of the Comparators together with the locating powers of the Copperheads and the weighting capabilities of Amber seemed a possibility.

(~~TS//SI~~) Thus, it was a small evolutionary step to the central idea of the postwar Sled and Goldberg machines: embody each of the major cryptanalytic functions in separate hardware packages; create a central switching mechanism; tie the packages together in any desired configuration through the switch; and hook it all to free-standing input/output mechanisms.[45]

(~~TS//SI~~) With a stock of the specialized "boxes," the agencies could instantly create any desired cryptanalytic engine. The cryptanalysts would not have to wait for two or more years for a traditional type of special-purpose machine to be built; expensive machines would not become useless if an adversary changed his system; and the machine rooms would not be cluttered with devices that were used only a few hours a week.

(~~TS//SI~~) In 1945 there seemed, in fact, no alternative to such a machine. It appeared so nat-

ural at the time that it did not have to be justified through a comparison with other possible architecture. Because the "von Neumann" idea was relatively unknown in 1945, it was only later that the supporters of the multipurpose cryptanalytic machine concept justified their ideas through contrasting them to the universal serial computer. But when they did, they outlined an argument that has had a long life within the SIGINT community. The arguments against the von Neumann design have continued for fifty years.

(~~TS//SI~~) By the late 1940s, men in both "G" and the SIS were pointing out how their linked-box architecture would allow parallel processing, the incorporation, whenever desired, of analog computing, and thus much, much faster processing. They explained that the von Neumann design would always be too slow because it had only a single processor to do everything. To be useful, that processor had to be driven by an outside program, step by step by step. Hundreds, perhaps thousands of ticks of a clock had to go by before the most simple of crypto-functions could be completed. Nothing else could be done until the program cycle was finished.

(~~TS//SI~~) However, the special boxes, arranged in the right manner, had the potential to be hundreds of times faster than the single processor device. Hardwired functions would always be performed in fractions of time it took to read and execute programmed instructions. And with the "boxes," while one function was being completed, another could be performed. As important, with a set of function boxes on hand, no one would have to wait the months, or, as it turned out, the years it might take to write a complex program for a von Neumann machine.

(~~TS//SI~~) Most advocates of "reconfigurable" machines agreed on other things in 1945. There was a commitment to use and, if need be, create new components. The functional packages should be built with advanced electronics, if at all possible, and with new input and output equipment. Only electronics could make the machines fast enough to perform the cryptanalytic tests; and for many of those tests, only new I/O devices would allow the electronics to work at optimum speeds.[46]

(U) Faith without Institutions: Slides, Sleds, and Skates

(~~TS//SI~~) In 1945 "G" and "F" did not realize how difficult it would be to follow through on their pledges to create a "universal" cryptanalytic machine. Who would be willing to build something just for the SIGINT community? Who would pay the extra costs that necessarily came when standard, commercially produced equipment was rejected? Who could be trusted with the secrets that were embodied in the special devices?

(~~TS//SI~~) Although "G" and the SIS both sponsored programs to create reconfigurable non-von Neumann machines at about the same time, and although the two agencies were required to coordinate their efforts,[47] their responses to those questions were quite different. The navy began its project immediately, but did not stay with all the original intentions for its Goldberg. The army eventually produced a machine that fit quite well with the original architectural vision, but it was almost a decade before its Sled emerged.

(U) Among the many reasons for the different patterns one stands out: the navy allowed "G" to create, as will be described, a company that had the skills and the mandate to begin work immediately. In contrast, the cryptanalysts and engineers at Arlington Hall were left dependent upon the vagaries of yearly budget allocations and the willingness of commercial corporations to subject themselves to what might become very unprofitable projects.

(~~TS//SI~~) But the army's project did not begin with a cloud over it. Leo Rosen's mid-1945 plea to extend the reach of the tabulator-relay combinations at Arlington Hall received a warm reception.

The conceptual outlines for what was later called Sled were in the making by the end of the year, and there were signs that enough men would be left in his "F" section to design if not build the new all-purpose machine. Not all the functions that were to be turned into hardware were agreed upon, but there was little opposition to the idea that at very minimum, Sled would have to perform the cribdragging and dictionary lookup functions of the invaluable Slide-Run machines of World War II. More ideas were contributed as to what functions should be included and, as important, how they could be designed to meet the goal of having, when desired, plugboard-programmed parallel processing.[48]

~~(S//SI)~~ The evolving ideas even attracted the cryptanalysts and engineers at "G," especially those who had worked with the tabulator and NC machines. Already mandated by the government to coordinate as much research and development as possible, "G" and the SIS agreed they should work together on Sled. Each looked forward to having a Sled with electronic components within a short time.[49]

~~(TS//SI)~~ However, the program ground to a near halt. Not enough resources and equipment remained in the postwar "F" section, and a contractor could not be found to turn rough ideas into specifications and hardware. Specifically, IBM was more than hesitant to accept the responsibility for the Sled program.

~~(TS//SI)~~ IBM had been a good friend to the SIS, and so many of its bright engineers had learned of codebreaking techniques during the war that IBM had seemed the logical choice to turn the "reconfigurable" idea into innovative machinery. There was also a factor of technological continuity. IBM had created the NC and relay-box devices that were to be paralleled in electronic form, and it was the manufacturer of the only efficient equipment for the cards that had become the standard "memory" in the tabulator rooms at both agencies.

~~(TS//SI)~~ IBM was such a clear choice that it seemed to have been the only one thought of by the SIS group advocating the Sled architecture. But IBM was not in the mood to take on such work after the war. Its management was not even extending a welcome to the requests from the Bureau of Ships for more NC machines including a critically needed one to record punch card data onto microfilm and then, if desired, reverse the process.[50]

~~(TS//SI)~~ IBM's rejection of the army and navy's overtures created intense shock at the SIS. The army's men almost felt betrayed. They could make no progress towards a "Sled." The tensions between the SIGINT agencies and IBM were quite evident by early 1947. Even OP-20-G had become alienated. It had become tired of having to bend to the whims of a single supplier and was willing to spend extra monies on machines, training, and support to gain more bargaining power. It was giving very serious consideration to setting up a processing center based on the products of IBM's competitor, Remington-Rand.

~~(TS)~~ The army's machine group was certainly losing patience. It helped draft a protest to the "brass" about IBM's lack of cooperation,[51] and some rather direct words reached Tom Watson. As a result, there was more cooperation. In 1947 IBM's management made sure that ex-members of the agencies who had returned to the corporation were assigned as liaison officers.

~~(S)~~ Men such as James Green and Stephen Dunwell began to do much to restore harmonious relations. They arranged little favors such as having IBM replace the frequently wornout parts of the SIS keypunches at no cost to the government. The cryptoagencies were the only ones at the time to do extensive binary punching. That wore out the punches and die blocks in weeks, rather than in the years that were typical in business data centers.

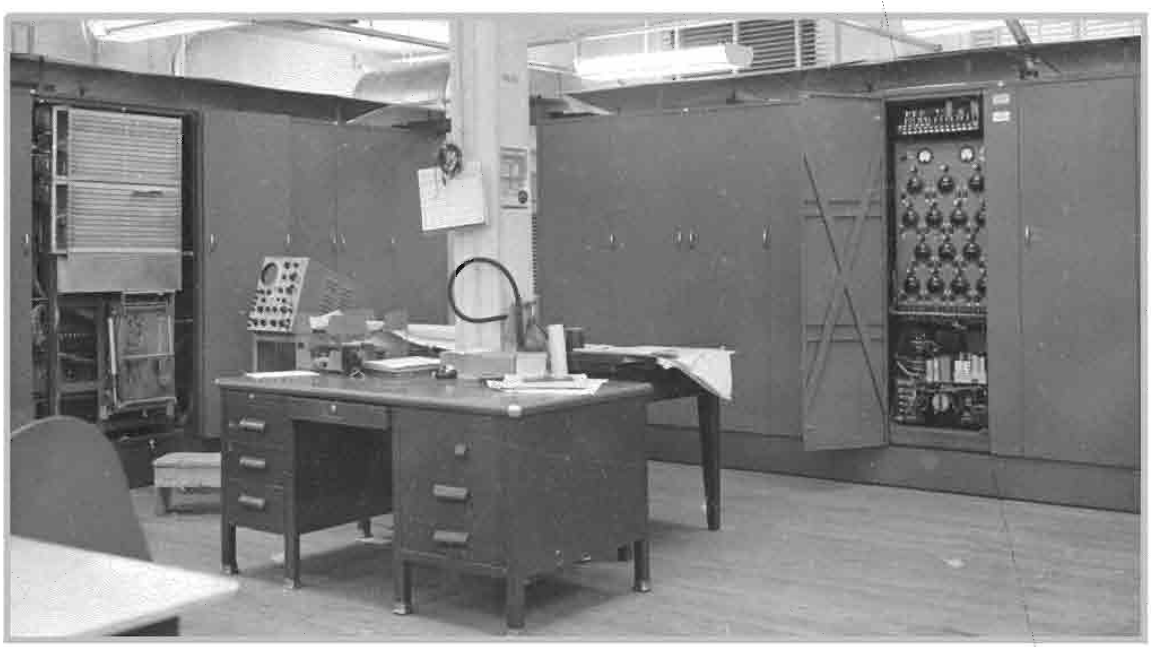
~~(S)~~ Green and Dunwell helped keep "F" informed of new technological options. They made sure that "G" and the SIS were the first to know about such important IBM advances as its 604 electronic multiplier and its very hush-hush line of new tabulators. They did more than pass information from IBM to the codebreakers; they began to act as advocates for SIS and "G."[52] They met with IBM management and argued that the company would benefit from the Sled research.[53]

~~(TS//SI)~~ But it was not until the summer of 1948 that IBM agreed to take on the extensive Sled project.[54] Then it was not until that fall that the first specific designs began to receive approval.

~~(TS//SI)~~ Meanwhile, the frustrations at the SIS had grown to such a level and the need for a Comparator for baudot problems became so pressing that the in-house engineers began designing an emergency version of a Sled. At first called a "tape-comparer," the machine emerged in 1948 as a rather crude jury-rigged machine. But it worked and it evolved step by step into the Connie Comparators of the 1950s. They never became as flexible as Sled; but they were seen by their sponsors as general-purpose comparators.[55]

~~(TS//SI)~~ While the Connie precursor was being constructed, IBM acquired a secure building in Vestal, New York, to work on Sled. IBM sent some of its best men to help with the project, including a future company president, B. O. Evans.[56]

~~(TS//SI)~~ Unfortunately, just then, long-term goals had to be set aside, at least for a time. A cryptoemergency arose. In response, a very stripped-down version of Sled, with the appropriate name, Skate, was hurriedly produced and rushed to Washington in 1949 to try to unravel an intransigent [redacted] system.[57] After a relatively long shakedown cruise, Skate was put to work as a primitive electronic version of a numeric-only Slide-Run machine. It was soon followed by a more advanced copy, which cost twice as much as the first, over $500,000.[58]



~~(S)~~ Sled

P.L. 86-36
EO 3.3(h)(2)

~~(TS//SI)~~ The Skates were electronic advances, but costly ones in terms of dollars and manpower diverted from the Sled ideal. That upset one of the major figures in the agency who supported the Sled architecture, Albert Highley. He knew from first-hand experience of the need for a ubiquitous device on the machine room floor. His belief in a quickly convertible architecture was perhaps reinforced by the Skate experience: By the time the machine became fully operational, the original target had disappeared.

~~(TS)~~ Highley became worried that Sled would never be turned into hardware. As a result, he and his associate Ray Bowman began to apply new pressures on the company. Sled was finally born, but that was eight years after Leo Rosen had put forward the general outlines of such a machine and a year after the SIS and OP-20-G had been merged into the new organization, the National Security Agency.[59]

~~(TS//SI)~~ What finally arrived in Washington in the first half of 1953 were two copies of a custom-made machine whose basic design stood, for more than two decades, as a tempting alternative to the general-purpose computers. The Sleds did not achieve all that had been hoped for in 1945 when the "reconfigurable" design had first appeared, and they were more expensive than thought. But they were impressive.

~~(TS//SI)~~ The two copies cost a third more than Madame X, but that was not much more than the previous Skate "pilot" models had cost.[60] And they were inspirations to those who favored a special cryptanalytic architecture.

~~(TS//SI)~~ The Sleds depended upon high-speed electromechanical tabulator equipment for their input and output, but they were not retrogressions. The card reading and punching equipment was used because so much of the information that was to be processed was already in card form and because printers of the time were too slow to keep up with the electronics that had been developed.

~~(TS//SI)~~ The Sleds called upon the best large-scale memory technology of the era, magnetic drums. For the super-fast processes of offsetting messages, they used advanced delay-line systems.

~~(TS//SI)~~ The Sleds were built of hardwired function "boxes" with very advanced circuitry. Although they did not span the full range of cryptanalytic functions, those that were included gave Sled power over a wide range of cryptanalytic problems.[61] Critical to Sled was its type of "programs," a combination of plugboards and electronic matrices. They allowed instant switching and concurrent processing.

~~(TS//SI)~~ The hardwired functions, the fast memories, and the use of plugboard and electronic matrix programs were augmented by the ability to have much parallel processing. But with or without parallelism, Sled's speed was impressive. For example, it could make 30,000,000 comparisons a second if desired. In contrast, the mid-1940s NCR-Gray Comparators worked in the range of hundreds per second.

~~(TS//SI)~~ Sled could be used as an IC machine, a crib-dragger, a wired-wheel machine analyzer and analog, a statistical threshold tester, and much more. And it could be used for alphabetic as well as numeric data.

~~(TS//SI)~~ One reason for its wide abilities was its memory systems. Its magnetic drum held a significant amount of data for the time, 48,000 characters. Its delay lines and special circuits which could "precess" (offset) two messages made it a very fast comparator and crib-dragger. Sled also outdistanced the old Comparators because of its thirty-two counters and five accumulators.

~~(TS//SI)~~ Its electronic weighting circuits made it a very efficient version of a plaintext

recognition machine, and its circuits for statistical evaluation also helped in the several modes of IC analysis. Its "recognition unit" made it a fast slide-run machine, and it was a very, very rapid "locator." Its two large matrices aided it when it was used to decipher systems, including Enigma-like ones.

~~(TS//SI)~~ Although the Sleds were honored because of their slide-run "recognition" abilities, a clever engineer could make them perform a broad range of functions. One routine made the testing of the suspected reuse of key on a major system a routine matter.

~~(TS//SI)~~ For example, 3,000 ten-group portions of key had been recovered, and it was desired to see if any of them had been used on the messages that continued to flow in. To do that, all the groups had to be applied to the messages and the resulting text checked to see which, if any, of the keys produced a significant percentage of known code groups. Sled was able to test the 3,000 suspected keys against ten cipher groups in just fourteen seconds. [62]

~~(TS//SI)~~ "Programming" Sled was an art, with the programs looking more like engineering timing diagrams than the instructions for a digital computer.[63] Despite that, Sled gained so much loyalty that the first ones were cloned in a super-fast transistor version by the late 1950s. As we will see, a grand elaboration was proposed under the mid-1950s NSA Farmer program.[64]

(U) Faith and an Institution: the Chance to Begin an ERA

~~(TS//SI)~~ OP-20-G had its "reconfigurable" machine working some four years before the Sleds.[65] The reason for the earlier appearance was not because of more engineering genius within the navy; it was because of different postwar institutional arrangements.

(U) As the war was winding down, OP-20-G and the SIS knew they would be stripped of men and resources. The situation looked bleak. Rosen's "F" branch was in jeopardy, and Engstrom's "M" and the NCML faced extinction. The Bureau of Ships showed signs of tiring of the near autonomous NCML, and "M" had its own special problems because of navy personnel rules. Holding onto its many exceptional scientists and engineers was an especially difficult and pressing problem. Without them, little progress could be made on methods or machines. There were no cryptanalytic think tanks, and all the private computing machine contractors made no effort to hide that they were tired of government work. As threatening, in 1945 there was no electronic computer industry, and there was little indication that one would emerge.

(U) Friedman lobbied the army to maintain as many civilian slots as possible, and he tried to create a joint machine development center with OP-20-G, but he had to settle for a small group in the SIS that could direct and oversee established contractors.[66] Wenger sought much more. Rejecting the suggestions for a joint army-navy program, but later being forced to accept a joint board that sought to coordinate programs and targets, he began an independent search for a practical solution.[67]

(U) After some initial failures, things began to fall into place. The secretary of the navy took great pride in OP-20-G's achievements, and the Chief of Naval Operations had become an ally.[68] The Office of the Chief of Naval Operations helped overcome any objections from the bureau, and the NCML's life was extended, at least for a time. Some postwar funding seemed more than a possibility.

~~(TS//SI)~~ Wenger formed an in-house RAM panel to take advantage of that and to develop the technical arguments he would need to fend off any major threats to his automation program.[69]

(U) In late summer 1945 a $500,000, one-year development contract was awarded to NCML-NCR. It included funds to work on a new general-purpose Comparator. Wenger underscored the point that the United States could never again expect to have the time to make and correct fundamental mistakes as it had during World War II. He hammered at two other points: The traditional division between operational and bureau powers would ill serve a modern navy, and only a continuation of something like the cooperative relations between "M" group, NCR, and NCML could save naval cryptanalysis.[70]

(U) He was given assurances that OP-20-G would be allowed its own program and was told that navy money would be made available for continuous machine development. Then Wenger received the wonderful news of the establishment of Monogram, a long-term program to continue upgrading communications intelligence equipment and methods. Hooper's mid-1930s plan for naval communications and for linking science to the navy appeared to have finally been appreciated.

(U) Under project Monogram, every relevant research project was placed within one integrated program. Radio research, the mathematics of cryptanalysis, and even electronic explorations relevant to the gathering and analysis of signals were to be subject to its generosity. Millions of dollars, it was pledged, would be allocated for both research and advanced development projects.[71]

(U) More than money was promised. There was a strong hint of autonomy for "G." It would be allowed to direct its own work, free from the Office of Naval Research, the Naval Research Laboratory, the naval electronics laboratories and, to a very great degree, the Bureau of Ships. Although the other navy agencies continued the battle to control "G's" "turf," the naval Rapid Machine program had a future.[72]

(U) In late 1944 Wenger put Howard Engstrom, Ralph Meader, John Howard and another of the bright navy engineers, Bill Norris, to work on Hooper's suggestions.[73] They proposed what they thought was a way to permanently link science and innovation to the navy. It was a new version of Hooper's post-World War I RCA. In 1945 Wenger's men recommended creating the private, for-profit, National Electronics Laboratory. The company was to be staffed by the talented men from OP-20-G and the other advanced science agencies in the navy.[74]

(U) Wenger approved the idea, envisioning a firm that would devote itself to navy communications problems,[75] ranging from mathematical cryptanalysis to the physics of radio.

(U) The navy's legal experts gave the green light to "M's" officers, such as Engstrom and Norris, having an interest in the private company. Most of the "M" engineering team, including Howard, Coombs, and Steinhardt agreed to join, but those who had been IBM employees decided to return to their old company. Joe Desch and his men also opted to stay with their firm, NCR.[76]

(U) Soon, however, everything seemed to be falling apart. America's old scientific organizations rejected them. Rockefeller Foundation also thought America had enough research institutions. A sponsor could not be found, and the situation became critical. At the end of 1945 Wenger had his new research agenda and had promises of contracts, but he had no idea of where to find the men to build a full electronic Super Bombe, a new version of Mike, his grand "reconfigurable" Comparator, or even a viable punch for the old Comparators and the Copperheads.[77]

(U) A savior, at least a minimal version of one, finally appeared and turned Wenger's failing dream into the new company, Engineering Research Associates. But even the investment banker, entrepreneur, and old friend of the navy, John Parker, could not piece together truly ade-

quate funding. He could not even locate the new company near OP-20-G. The proposed research arm of "G" had to move to Minnesota.[78] Coming in contact with the Engstrom-Norris group through mutual friends in the military,[79] Parker was persuaded that a private version of the NCML-NCR could succeed. He agreed to gather minimal financing, to help with business matters, and to set the new company up in his old factory in St. Paul, Minnesota.

(U) ERA immediately gained the navy's approval, and it immediately won OP-20-G's big research contract.[80] In return "G" expected ERA to be a "captive" of the navy.

(U) It also won an important friend, OP-20's Louis Tordella. One of the young officers who decided to stay in "G" after the war, Tordella would become one of NSA's most dynamic leaders. In 1946 he began supervising the ERA contracts and acted as a general liaison with the company. Perhaps because of his interaction with the ERA engineers and mathematicians, Tordella became one of the future NSA's most energetic supporters of high technology as well as one of the most influential figures in the history of American intelligence gathering.[81]

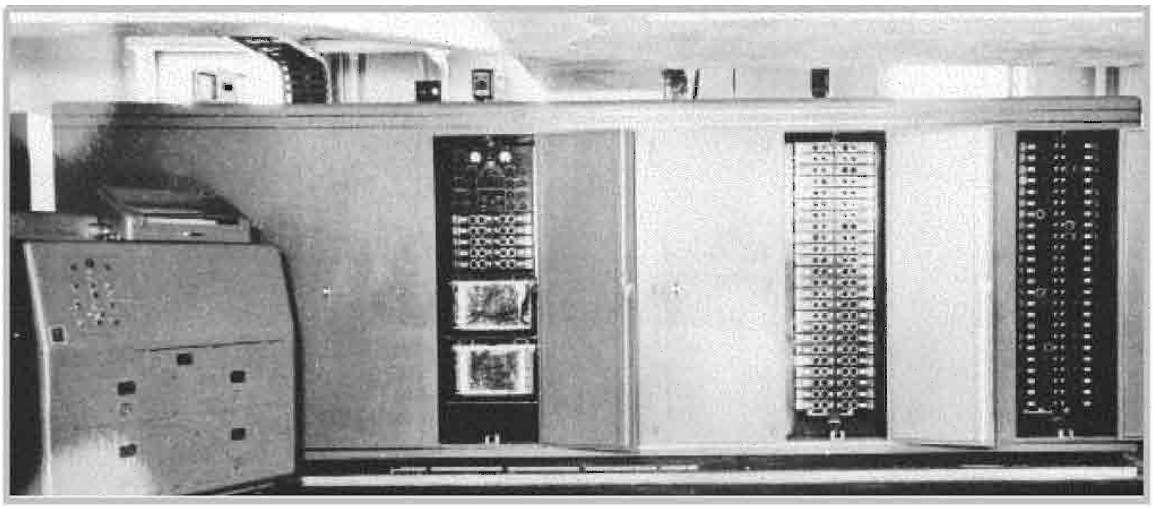
(U) A Bright Hope for Hooper's Dreams

(~~TS//SI~~) By mid-1946 ERA had a broad contract with "G," one that gave it the freedom Bush had sought in the 1930s. Its men were happy with competitive salaries, stock in the company, and the chance to do cutting edge work in computers, communications, and operations analysis. There were indications that ERA might also become a think tank and a center for advanced mathematical research.Those efforts, led by C. B. Tompkins, were coordinated with the research of several of "G's" alumni who had returned to teach at such prestigious institutions as Harvard and the University of Illinois. They did contract work on topics such as [redacted] and the behavior of binary systems.[82] Wenger had a small but effective cadre within OP-20-G to manage his technology program. Joseph Eachus, Howard Campaigne, and James T. Pendergrass were top-flight young scientists who appreciated the role of mathematics and computers in cryptanalysis. They helped Wenger set up a board to coordinate the RAM program with the needs of the cryptanalysts.[83]

(U) Most importantly, ERA was launched on the mission of creating a multipurpose cryptana-

(U) Louis Tordella

(U) Joe Eachus



(U) Goldberg

lytic computer.[84] But ERA did not start its career with a leap into fully digital electronic computing. It began with an attempt to build the navy's version of Sled.

(U) The Grand Machine of Its Time, the New Comparator

(U) The hopes for a single grand cryptanalytic machine had been boiling up at OP-20-G since 1944. But it took more than a year after Japan's surrender before the outlines of the machine called Goldberg got the financial nod from the Bureau of Ships.[85] Joe Eachus had explored possible technologies and sketched ideas which he passed on to his old friends who had joined ERA.[86] All types of memory media, including microfilm, were investigated, as were new tubes and circuit designs.

(U) At ERA the "reconfigurable" general-purpose Comparator Goldberg began as more of a research than a development project. Many of Goldberg's components were in advanced stages within its first year, but the machine was not delivered until late 1949, more than a year behind its production schedule, and two and one-half behind the hopes of its original planners.[87] Even more time was needed to smooth over its operations. ERA was not finished with the machine until 1951.[88] Goldberg ended up much more of a special-purpose machine than had been intended. It did not even become a fully reconfigurable computer. Operational needs pushed it to becoming an elaboration on the early Comparators, but one targeted at the new teletype-encryption devices.

(U) Goldberg took photoelectric sensing and paper tape scanning to new technical heights. Very fast tape drives were completed by 1947, allowing as many as four tapes to be run on top of each other. The drives ran the tapes at more than six times the speed of the older devices and were able to offset the tapes for IC testing without slowing the machine. A very complex and precise scanner was developed which included the photocells and circuits to sense each of the seven data and three control positions in each row on a tape.[89]

(U) Goldberg was also an example of how much electronics had matured since 1945 and how the emergence of new components could undermine investments in the development of

early technologies. Almost as soon as they were developed, the new tape systems were abandoned in favor of a series of emerging technologies.

(~~TS//SI~~) The first temptation that pulled attention away from tape or film was electrostatic storage. For a time it was thought that Goldberg was to have special television-like tubes and thus, a "random memory."[90] But when RCA and others were unable to make such systems operational, a "second best" technology was selected for Goldberg, the magnetic drum.

(U) Goldberg was treated to the slower but more tractable magnetic drum memory. The system included delay lines and sophisticated circuitry that allowed the tracks of information on the drums to be offset in the same way that Bush's earlier Comparators had slid one tape over another.[91]

(U) Goldberg was given one of the first magnetic drums in the world, and "firsts" always have problems. It took several years of effort to make the new technology behave. Even in mid-1949 there were problems with the huge drums on Goldberg.

(~~TS//SI~~) Much more than the drum was innovative. Goldberg's central cabinets were very impressive. They contained more than 7,000 tubes reflecting the complexity of its digital circuits. Going beyond the state of the art led Goldberg into trouble. At one point in its construction the majority of the tube sockets in the machine had to be replaced.[92]

(~~TS//SI~~) But once in operation, Goldberg was able to perform many different cryptanalytic functions through plugboard "programs." That helped fulfill some of its designer's hopes that it could be a "reconfigurable" machine.[93]

(~~S//SI~~) Goldberg could do anything that Mike or Copperhead or the old Comparator had done during the war and much, much more. It could perform so many standard functions that its "specialized" architecture seemed more suited to cryptanalytic needs than the proposed general-purpose programmed computers.

(~~S//SI~~) It performed frequency counts, IC tests, round robin searches, crib dragging, wheel stripping, roughness tests and, among other functions, weighted calculations. It had an advanced translation system for baud signals and an electronic 36 x 36 matrix that imitated, if desired, a wired wheel.[94] It also had a sophisticated threshold circuit that eliminated the "always print" feature of Bush's earlier machine, thus saving much run time and analyst's attention.

(~~S~~) And Goldberg was fast, although not as rapid as the later Sled. When Goldberg was in top shape, it made 20,000 serial comparisons a second. That was 250 times the rate of Bush's 70mm Comparator.[95]

(~~S//SI~~) Its thirty-six decimal (ring) counting circuits allowed deep statistical analysis. In addition, it had banks of rectifiers for short-term fast memory, which aided the special circuits used to calculate the IC statistics.

(~~S~~) The Goldberg work led to advances in the design and use of magnetic technology despite its drums sometimes being taken off to serve the emergency needs. Besides its contributions to the mechanics and electronics of drum memory, Goldberg incorporated a unique way of using its drums. They were used as "buffers." To speed processing, while one drum was providing data for calculations, the other was loaded with data from the tapes.[96]

(~~TS//SI~~) Although it was late in coming, Goldberg was the state-of-the-art "reconfigurable" Comparator. Contemporaries thought the more than $250,000 spent on it was a very wise investment, worthwhile enough to think of

replacing the slow and sometimes troublesome drums with a massive electronic memory.[97]

(~~U//FOUO~~) However, because of its long-delayed and sometimes painful delivery, it seemed best not to build any more of the "G" designed general-purpose "comparators." The contract for a second machine was canceled. The progress on the general-purpose computer, Atlas, and the old SIS group's faith in the Skate-Sled multipurpose machine project at IBM indicated that the Comparators had outstayed their welcome.[98]

(~~TS//SI~~) However, the engineers at ERA and NSA learned a great deal from its development and its perhaps four years of service. They transferred much of its technology to other machines, including a long line of limited comparator-like special-purpose devices that were begun in the late 1940s and early 1950s. The tape-based Robins and Connies and the ambitious delay-line Vivians and Dellas took much from Goldberg.[99]

(U) Meanwhile, a Last Chance for Microfilm

(~~TS//SI~~) Although the engineers at ERA had decided microfilm was inappropriate for Goldberg, there were many in "G" and the SIS who continued to have faith in the future of Bush's solution to the mass memory problem. While the navy had some engineers who saw Icky and Hypo as just the beginnings of a major postwar microfilm program, it was an army group that had the grandest postwar visions for film RAMs. Encouraged by the arrival of its microfilm plus electronic-counter machine in late 1944 and the about-to-be-completed 5202 Comparator for the Tunny problem, "F" wanted to order a whole series of machines from Eastman. Each would perform one of the major cryptanalytic functions.[100] The ideas were attractive because film continued to be a much higher volume memory than magnetic devices. Drive speeds did not erase the difference. In 1949 microfilm data could be read in at five times the speed of data on magnetic drums.[101]

(~~TS//SI~~) The postwar SIS was not allowed to launch the ambitious film RAM program, and it was unable to have Eastman-Kodak serve as an ongoing resource. But the SIS's film advocates did begin a project to do the necessary research and build an upgraded version of the ambitious 5202. Shortly after the war it hired several small electronics companies to explore all the possibilities. One, Hogan Laboratories, had a promising design. A contract was let, and the SIS would have a very advanced film Comparator before the end of the decade.[102]

(~~TS//SI~~) Those who continued to see the future of OP-20-G in terms of microfilm received some funding. With a rather handsome allocation in hand, they eventually convinced Eastman to do more than complete World War II's Ambers. In 1947 Eastman accepted a contract to begin to explore possibilities for a new Hypo and a new Icky. It would take quite a while for Eastman to deliver the new versions, but in 1947 film again seemed to have at least the possibility of a rebirth at "G."[103] There was even some thought of having the Eastman group under Tyler build a light-based bombe and a new electronic rotor bank. As promising was an exploration of a grand idea for a huge new comparator using large photographic plates or drums with as many as 10,000 tiny holes per square inch. As the plates could be aligned over each other in one-tenth of a second, a light-based machine to attack the new teletype encryption machines seemed within reach.[104]

(U) Finally, the Electronic Bombe

(~~TS//SI~~) In 1947 there was even more that gave indications that the cryptanalytic and technological triumphs of World War II would continue. Most important was the growing success against the high-level systems [redacted]. Enough had been learned about several of the [redacted] systems allowing the engineers at "G" and

the SIS to build new versions of the Purple machines. The [redacted] relay devices (now especially efficient because of a new IBM relay technology) were given the names of less intrusive colors, such as Tan and Pink.

(~~TS//SI~~) There was also a series of electro-mechanical analytic machines for the [redacted] problem. The small machines built by the in-house engineers were also given "softer" names than those used for similar machines of World War II. The Stork was one of many helpful devices used directly by the cryptanalysts.[105]

(~~TS//SI~~) Achievements against the [redacted] target went beyond tabletop relay boxes. Perhaps the first operating machine to use a magnetic drum was constructed as a crib-dragger to attack the very, very important on-line encryption device the [redacted] used for much of their top echelon traffic. Beginning work in early 1948, and using magnetic drums taken from Goldberg, ERA finished the first of several Demons in October. Although the Demons had many relays and plugboards, they had electronic components and the circuitry needed to search for high-frequency clear groups. Follow-on models were flexible enough to be used against several targets.

(~~TS//SI~~) The idea behind the Demon attack was clever. A large number of cribs were applied to one message of a pair determined to have to been produced by the same key through IC and similar analyses. The derived key from the first crib-plain match was applied to the other message. Then, to see if true key had been found, the result was looked up in the memory, which contained known high-frequency groups.[106]

(~~TS//SI~~) More thrilling for the machine builders was the chance to at last construct a full electronic Bombe. The explorations of the electronic matrices and the growing knowledge of the rotor-based, on-line [redacted] encryptor led to the appropriately named Hiawatha project.[107] It was one of ERA's great challenges because Hiawatha might cost $1,000,000 and call for 40,000 tubes and because ERA's engineers hoped they could construct and design it so that it could attack more than one teletype encryptor.

(~~TS//SI~~) Hiawatha was only a beginning. To cover the entire spectrum of [redacted] devices, "G" began the Ophis project. Its first goal was another electronic rotor, one for an attack on the mysterious Albatross machine. Albatross was thought to be like Germany's wired-rotor Green Enigma of World War II. The SIS and "G" hoped that Ophis' long-term result would be a general wired-wheel Bombe that would be more powerful than Hiawatha.[108]

(~~TS//SI~~) There were even greater and more exciting engineering challenges. By the time Hiawatha was conceived, both of the American cryptanalytic agencies were joining the race to complete the first modern "von Neumann" type of computer.

(U) Notes

1. (~~TS//SI~~) NSA CCH Series XII Z, "ANCIB Minutes, abstract of," 1955. This also states that the U.S. was much more technically advanced than the British. The only edge the British had, it stated, was in "collateral" information. (~~TS//SI~~) NSA CCH Series XII Z, draft copies of Michael L. Peterson, "The Bourbon Problem," indicates that early British successes against Russian cipher machines and their ability to intercept and process non-Morse transmissions were critical to convincing the American agencies to extend the World War II cooperation and formalize it in the BRUSA agreement. (~~TS//SI~~) NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April 1957.

2. (~~TS//SI~~) NSA CCH Series XII Z, "Procurement of Geheimeschreiber Equipment from British," J. N. Wenger, OP-20-G, 14 August 1945.

3. (~~TS~~) NSA AHA ACC 78098, "Monogram Report, Part IV, Field Research," is useful on multiplex needs.

4. (~~TS~~) On IBM's reluctance to take on any work after the war and even into 1947, (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949.

5. (U) By the 1950s the physics community would seek an alternative to the classic computer architecture as the demand for increased computing power escalated. But in the 1940s the codebreakers took the lead in seeking a different type of electronic computer.

6. (~~TS~~) NSA CCH Series XII MPRO, Box 1, "Machines in the Service of Cryptanalysis," 28 September 1954.

7. (~~TS//SI~~) NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April 1957.

8. (~~TS//SI~~) NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April 1957, 173.

9. (~~TS~~) The hopes of the army cryptanalysts were expressed in a long memorandum from Frank Rowlett to the commander at Arlington Hall in mid-1945, (~~TS~~) NSA AHA ACC 26373, Frank B. Rowlett, "RAM in Future Cryptanalysis," 3 May 1945. Note, however, that his vision was less far reaching than those expressed in Wenger's plans for RAMs at OP-20-G. For example, see (~~TS~~) NSA CCH Series XII Z, CNO to Chief Bureau of Ships, "Communications Intelligence: Research and Development," 21 December 1945, and, Wenger to Eachus, "Analytical Machinery Panel," 31 October 1946.

10. (~~TS//SI~~) NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April 1957.

11. (~~TS//SI~~) (~~TS~~) NSA CCH Series VI.1.8, "Martini," circa 1947. On Initram, (~~TS~~) NSA CCH Series XII Z, J. F. Beatty, "Martini (Longfellow)," OP-20, 1947. The old Japanese analogs, such as Python, contributed their parts to the anti-Soviet cause. See also the army's Tan analog of the Longfellow machine. Exciting sources on the progress against one of the Soviet's most sophisticated and important cipher machines are found in (~~TS//SI~~) NSA CCH Series XII Z, "Longfellow, History of," N-31 to 20-L, June 1948.

12. (~~TS//SI~~) (TS) NSA CCH Series XII Z, H. H. Campaigne, "Summary of War Diary September 1946," 7 October 1946. (~~TS//SI~~) NSA CCH Series XII Z, H. H. Campaigne to 20-34 L, "Longfellow, History of." June 1948. (~~TSC~~) NSA CCH Series V.I.1.20, "Longfellow, Machine Breaking, 1947." (~~TS//SI~~) NSA CCH Series XII Z, "OP-20-G, "History of Navy Attack on Longfellow," 14 December 1949.

13. (~~TS//SI~~) On the frustrations caused by the Soviet [redacted] (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings." One large set of comparators, the Robins, was built just for the problem but achieved little. (~~TS//SI~~) NSA CCH Series XII Z, AFSA-21 "Summary of the Early Operation of the Robin Machinery," 19 May 1951.

14. (~~TS//SI~~) When the world situation began to unravel in the late 1940s, not enough was known about some of the more important Soviet machines to allow a fast technological solution such as the Bombe program of World War II. The United States did not know enough about the wired-wheel Albatross machine, for example, to allow the construction of a massive analog-analytic machine like the Bombe. (~~TS//SI~~) NSA AHA ACC 18669, AFSA-02, "Request for establishment of Comparator Project (Albatross)," 6 June 1950.

15. (~~TS//SI~~) Oliver R. Kirby, "The Origins of the Soviet Problem: A Personal View," *Cryptologic Quarterly*, Vol. 11 #4 (Winter 1992), 51-58, gives an insight into the SIS' fears about being ordered not to pursue the Soviet problem. (~~TS//SI~~) The series of histories by CCH historian Michael L. Peterson published in *Cryptologic Quarterly*, 1994-95, shows the navy was working under the same fears.

16. (~~TS//SI~~) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948, provides a summary of the devices planned at the end of the war.

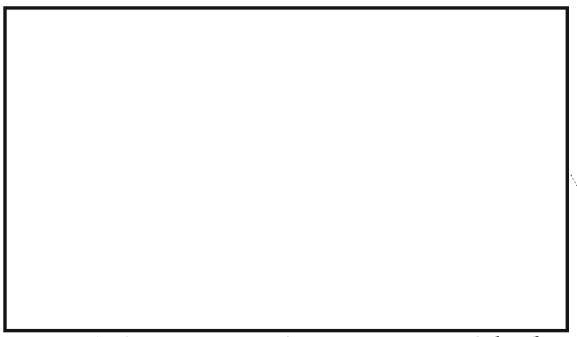
17. (~~TS//SI~~) OP-20-G invested much in the innovative Hecate machine, which was in the planning stage by the end of the war. It is described below as is a more general-purpose device, Alcatraz, which was at first targeted at [redacted]. (~~TS//SI~~) NSA CCH Series XII Z, AFSA-351B, "The Use of Hecate in [redacted] October 1950.

18. (~~TS//SI~~) On Hecate, (~~TS~~) NSA CCH Series XII MPRO, Box 1, "Machines in the Service of

Cryptanalysis," 28 September 1954. (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of Comint, Phase II," circa 1955. (~~TS~~) NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 198 (Hogan). And there seemed no need to rush its development and construction.

19. (~~TS//SI~~) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948, states that 32 Bombes, 2 Grandads and 4 Duennas were still available as of 1-31-49. The Autoscritcher was retired in 1945.

20. (U) A useful overview of the Hagelin enterprise and influence is Boris C. Hagelin, David Kahn (ed.), "The Story of the Hagelin Cryptos," *Cryptologia*, XVII # 3 (July 1994), 204-242.



22. (~~TS~~) NSA CCH Series XII Z, L. R. Steinhardt, "Digraph Counter, Improved, Conference On," 11 July 1945.

23. (~~TS//SI~~) Oliver R. Kirby, "The Origins of the Soviet Problem: A Personal View," *Cryptologic Quarterly*, Vol. 11 #4 (Winter 1992), 51-58. Note that in 1945 and 1946 even the president was unsure of the relationship between the United States and the Soviets and argued against reading their messages

24. (~~TS//SI~~) (~~TS~~) NSA CCH Series XII Z, L. R. Steinhardt, "Digraph Counter, Improved, Conference On," 11 July 1945, (TS//SI) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. (~~TS~~) NSA CCH Series XII Z, "The System [redacted] (Alcatraz)," AFSA-35lBm circa 1950. (S) NSA CCH Series XII Z, "ERA Task #7 Alcatraz," circa 1949. (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949. There is some confusion in the records over the production of a Baby Alcatraz. The best judgment seems to be that when the proposed size of machine was reduced, it was called, by some, "Baby," and that only one machine was built.

25. (~~C//SI~~) NSA CCH Series XII Z, Sam Snyder, "Draft Document, Pre-Computer Machines in Support of Cryptanalysis," circa 2 February 1978.

26. (~~S~~) NSA CCH Series XI K, Sam Snyder, Box 12, "Analytic Machinery Principles," September, 1949, 37. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley. "Cryptanalytic Machines in NSA," 30 May 1953. (U) Charles J. Bashe et al., *IBM's Early Computers*, (Cambridge: The MIT Press, 1986), 464.

27. (~~TS//SI~~) (~~S~~) NSA CCH Series XI K, Sam Snyder, Box 12, "Analytic Machinery Principles," September, 1949, 37. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 46. NSA's precursors acquired at least the next and more powerful version of the 603, the 604, and put it to use with tabulators stripping additives.

28. (~~S//SI~~) (U)) James W. Cortada, *Historical Dictionary of Data Processing: Technology* (New York: Greenwood Press, 1987), 366. See also the unpublished work on the early Remington-Rand machines by this author.

29. (~~TS//SI~~) NSA CCH Series XII Z, A. M. Gleason, "Inversion of Matrices with O'Malley," 1948.

30. (~~TS//SI~~) NSA CCH Series XII Z, "Use of HECATE [redacted] Message Placement," October 1950, and (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings."

31. (~~TS//SI~~) NSA CCH Series XII Z, NSA, "MPRO Technical Reports," circa 1956.

32. (~~TS//SI~~) NSA CCH Series XII Z, A. M. Gleason, "Inversion of Matrices with O'Malley," 1948.

33. (~~TS~~) NSA CCH Series XII MPRO, Box 1, "Machines in the Service of Cryptanalysis," 28 September 1954.

34. (~~TS//SI~~) (~~Laconic, Nocon~~) NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985. (TS//SI) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

35. (U) NSA CCH Series XII Z, NSA-OH-07-83, Oral History Interview with Beverly R. Chall, 2 May 1983.

36. (TS//SI) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase II,"circa 1955.

37. (TS) NSA CCH Series XII Z, ERA, Contract Number Nobsr-42001, "Preliminary Report and Proposal, Task: Project Warlock," 9 June 1948. (S) NSA CCH Series XII Z, ERA, "Warlock Progress Reports, ERA Task 18," 21 November 1947 to 10 April 1951.

38. (TS//SI) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

39. (TS//SI) (Laconic, Nocon) NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985. (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings." f[5134]. (TS//SI) NSA CCH Series XII Z, "Fifty Years of the Soviet Off-Line Machine Cipher," 10 January 1989.

40. (TS//SI) NSA CCH Series XII Z, ERA, Contract Number Nobsr-42001, "Preliminary Report and Proposal, Task: Project Warlock," 9 June 1948. Warlock borrowed from the Whirlwind Project at MIT. But it seems to have used a unique three-value logic for its weighing system to save tubes and processing time.

41. (TS//SI) Apparently, the rush of work in World War II led to the Americans not gaining enough skills to make independent attacks on the Tunny-like machines. (TS//SI) NSA CCH Series XII Z, S-2733, "Longfellow, History of," by Howard Campaigne, June 1948. (TS//SI) Oliver R. Kirby, "The Origins of the Soviet Problem: A Personal View," *Cryptologic Quarterly*, Vol. 11 #4 (Winter 1992), 51-58. A list of priorities from late 1947, after world events had put more pressure on the agencies, still reflect the faith in a general-purpose machine. (TS//SI) NSA CCH Series XI K, Sam Snyder, Box 17, "Long Range Cryptanalytic Program for Literal Systems," December 1947.

42. (TS//SI) The philosophy of "reconfigurable" machines and universal components underwent several modifications during the era, but the goal remained the same. For a later interpretation, (TS) NSA CCH Series XII X-MPRO, U.S. Cryptanalytic Research and Development Committee, "Joint Long Term Program for Research and Development in the Field of Cryptanalytic Equipment," 21 July 1948.

43. (TS//SI) NSA AHA 36746, Engineering Research Associates, Inc., "Proposal for An Electronic Rotor Program," 19 December 1946. On the continued search by the navy for high-speed components for the matrix, the Leo Project, which came to include the exploration of most basic technologies, including saturable cores, (S) NSA CCH Series XII Z, LEO: progress Report, ERA Task #11, 1 September 1947 – 1 October 1948. On the army's extensive basic electronic research during the late 1940s, (TS//SI) NSA CCH Series IV.C.2.14, ASA, "Annual Reports for the Fiscal Year 1949, Vol. II, Research and Development Division," Washington, 30 June 1949. The amounts invested in such research indicate that the SIGINT agencies must have played a significant role in pushing the development of tubes and transistor technology.

44. (TS//SI) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948, 9, shows that Sled became a joint army-navy project with the Bureau of Ships managing the contract. But the Sled concept seems to have originated at the SIS.

45. (TS//SI) On the army plans, Rosen (TSC) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings;" on the navy's (TS) NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986, (Hogan); and on the navy's participation in Sled (S) NSA CCH Series XII Z, J. H. Howard, "Conference on Slid(e)-Run Machine," 5 January 1946; (TS) NSA AHA 36746, Engineering Research Associates, Inc., "Proposal for An Electronic Rotor Program," 19 December 1946; (TS//SI) NSA CCH Series XII Z, "Joint Long Term Program (Old Planning Material, 1948-1949) compiled by Doug Hogan.

46. (TS//SI) Leo Rosen outlined his idea of a reconfigurable electronic machine in (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings."

47. (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," Joint Research And Development Board Memoranda.

48. (TS//SI) NSA CCH Series XH Z, "File Kept by Dr. Campaigne on Ram Panel Meetings.

49. (~~S//SI~~) NSA CCH Series XII Z, J. H. Howard, "Conference on Slid(e)-Run Machine," 5 January 1946.

50. (~~TS//SI~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949.

51. ~~(TS)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949.

52. (~~S~~) On the 604, ~~(S)~~ NSA AHA ACC 8544, "Memorandum for Members of RAM Panel, New I. B. M. Tabulator," circa 1948-9.

53. (U) NSA CCH Series XII Z, folder marked, Snyder, "Precomputer Comments," circa 1978, "Possible Item of Interest."

54. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948.

55. ~~(TS//SI)~~ NSA CCH Series XII Z, James L. Sapp, "The Analytic Machines," circa 1955. ~~(TS//SI)~~ NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953. ~~(TS)~~ NSA CCH Series XII Z, Sam Snyder, draft copy of, "Pre-Computer Machines in Support of Cryptanalysis," circa February 1978.

56. ~~(TS//SI)~~ NSA CCH Series XI K Snyder, Box 10, 10-27-77 Folder.

57. ~~(S)~~ J. J. Eachus, "SIGMAGE Threshold Control," 2 July 1946. ~~(S)~~ NSA CCH Series XII Z, BuShips, "Specifications Sled Navy Models CXOA and CXNQ Block Diagrams," 1 October 1948. (~~TS//SI~~) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948. ~~(TS)~~ NSA AHA ACC 10842, Ray L. Bowman," Engineering Diary,"circa 1945-1950.

58. (~~TS//SI~~) On the Skates (~~C~~) NSA CCH Series XII Z, Descriptions of NSA Early SPDs and Computers, as compiled from various NSA sources, and, ~~(C//CI)~~ NSA CCH Series XII Z, Herbert W. Worden, "EDP Machine History." Apparently both

[redacted]

in late 1948. See Michael L. Peterson, (~~TS//SI~~) "Beyond Bourbon," 1948, 4. The Skates were flexible enough, however, to be used on other problems.

59. ~~(TS//SI)~~ NSA AHA ACC 10842, Ray L. Bowman, "Engineering Diary," circa 1945-1950.

60. (~~TS//SI~~) NSA CCH Series XII Z, Samuel S. Snyder, "Pre-Computer Machines in Support of Cryptanalysis," draft, circa 16 February 1978, IV-25. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

61. ~~(TS//SI)~~ The Sled was constructed of two large interconnected cabinets; the term "boxes" is used for convenience.

62. ~~(TS)~~ NSA CCH Series XII MPRO, Box 1, "Machines in the Service of Cryptanalysis," 28 September 1954, 10.

63. ~~(TS//SI)~~ NSA CCH Series XII Z, James L. Sapp, "The Analytic Machines," circa 1955.

64. ~~(TS//SI)~~ NSA CCH Series XII Z, NSA, "MPRO Technical Reports," circa 1956. The price tag was not inconsequential. The transistor version cost approximately $2,000,000.

65. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. A pilot model of the proposed Sled, which was completed to help with the Soviet problem, was Skate. It arrived in late 1949; the version that was closer to the original grand intentions, Sled, was delivered in early 1953.

66. (U) Friedman sought a joint army-navy program, but the navy never accepted the idea. NARA RG457, SRMA-011, "Senior Staff Meeting Notes," April 3, 1945, "Friedman's joint work suggestion," 174, 231, 321. Samuel S. Snyder, "Abner: The ASA Computer, Part 1: Design," *NSA Technical Journal*, 25 (1980): 49. On turf battles among the services, Louis Kruh, "Army-Navy Collaboration for Cryptanalysis of Enemy Systems," *Cryptologia*, 16 (1992): 145-164.

67. (~~TS//SI~~) NSA CCH Series XII Z, "Joint Long Term Program (Old Planning Material, 1948-1949)" compiled by Doug Hogan.

68. (U) Robert William Love, Jr., *The Chiefs of Naval Operations* (Annapolis: Naval Institute Press, 1980), 137-192.

69. (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings."

70. (U) NSA RAM File: August 21, 1945, "Continuation and Development of Communication Intelligence"; Part II of Report to J. N. Wenger, Capt. USN, "Resume of the Dayton, Ohio Activity During World War II," December 21, 1945, CNO to BuShips,

"Continue to fund NCML"; and March 21, 1946, OP-20-G "History of Formation of ERA."

71. (U) NSA AHA ACC 40731A, SRMN-084, "The Evolution of the Navy's Cryptologic Organization." The importance and scope of Monogram for advancing intercept capabilities and mathematics in cryptanalysis is reflected in, ~~(TS)~~ NSA 40 AHA ACC 7808, "Monogram Report," 29 November 1949. ~~(TS)~~ NSA CCH Series XII Z, "Report of the Second Computer Study Group," as in *NSA Technical Journal*, XIX (Winter 1974), 21-61.

72. ~~(TS)~~ (U) NSA RAM File, December 20, 1945, "ERA postwar research plan," and July 20, 1946, Engstrom: BuShips,"Use Naval laboratories, not ERA." ON the Bureau of Electronics attempts to control OP-20-G's part in Monogram, ~~(TS)~~ NSA AHA ACC 7808, "Monogram Report," 29 November 1949.

73. (U) NARA RG457, SRH-267, "History of Engineering Research Associates." NSA RAM File, September 12, 1947, "Minutes of OP-20-2 Research Committee Meeting."

74. (U) NARA RG457, SRH-267, "History of Engineering Research Associates." NSA RAM File, January 2, 1945, Wenger OP-20-G to CNO, "Plan for ERA," and August 21, 1945, "Continuation and Development of Communication Intelligence [ERA]."

75. (U) NARA RG457, SRMN-084, "The Evolution of the Navy's Cryptologic Organization," 15.

76. (U) Bright mathematicians and physicists also joined the new company. Hagley Museum and Library, Accession 2015, Unprocessed ERA Materials, ERA, Personnel Summaries, circa 1946, and Engstrom to Norris, September 11, 1946. The Staff of Engineering Research Associates, *High-Speed Computing Devices* (New York: McGraw-Hill, 1950). All departments of the navy were concerned about how to continue their advanced scientific work. U. S. Naval Administration in World War II, War History of the Naval Research Laboratory, Guide No. 134, and Harvey M. Sapolsky, *Science and the Navy: The History of the Office of Naval Research* (Princeton: Princeton University Press, 1990).

77. (U) Hagley Museum and Library, Accession 2015, Unprocessed ERA Materials, Engstrom to Norris, September 11, 1946. NSA RAM File, December 20, 1945, "ERA post war research plan," and December 21, 1945, CNO to BUShips, "Continue to fund NCML."

78. (U) The Charles Babbage Institute holds many informative interviews with ERA founders.

79. (U) Important was Nelson Talbott, the powerful Dayton business executive.

80. (U) Charles Babbage Institute, "An Interview With James Henry Wakelin, Jr.," OH 104, Conducted by Arthur Norberg, February 27, 1986. Hagley Museum and Library, Accession 2015, Unprocessed Remington Rand / ERA materials, ERA Minute books 1946. NARA RG457, SRH-267, "History of Engineering Research Associates," 6-7. NSA RAM File: March 8, 1946, John Parker to Secretary of the Navy, "Plan for ERA"; March 8, 1946, OP-20-G, "List of research projects and secret ERA contract of 12-21-45"; and March 21, 1946, OP-20-G "History of Formation of ERA."

81. (U) On the expectations that ERA would be a strictly navy firm, (U) NSA AHA ACC 40731A, SRMN-084, "The Evolution of the Navy's Cryptologic Organization."

82. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948. A somewhat later but very interesting project was concentrated on the mathematics of sorting. ~~(S)~~ NSA CCH Series XII Z, ERA A. E. Roberts, "An Experiment in the Rearrangement of Data (Sweater)," (Sorting, Nomad) 1 May 1950.

83. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948.

84. (U) NSA RAM File, December 20, 1945, "ERA postwar research plan." Hagley Museum and Library, Accession 1901, Yuter Papers, June 6, 1946 to July 28, 1946, ERA-NCML on "Orion-Goldberg Project," and August 4-8, November 1-9, 1946, ERA reports "Orion-Goldberg, binary and analog magnetic recording." Hagley Museum and Library, Accession 2015, Unprocessed Remington-Rand / ERA materials, August 17,1946. "ERA salaries." NSA RAM File: August 14, 1947, Bureau of Ships to ERANCML "Task contracts causing problems"; June 3, 1946, NCML to ERA, "have your work approved"; and July 22, 1946, CNO to Secretary of the Navy, "Project Monogram."

85. ~~(TS//SI)~~ NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings." OP-20-G had asked IBM to take on a long-term research contract in 1945 and again in 1946, but was refused.

86. (U) Hagley Museum and Library, Accession 1901, Yuter Papers, September 1946 November 1, 1946 reports "Orion-Goldberg, binary and analog magnetic recording."

87. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948."

88. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. ~~(S)~~ NSA CCH Series XII Z, "Goldberg Progress Reports," 30 December 1947 through 10 April 1951. (~~TSC~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings."

89. (U) Hagley Museum and Library, Accession 1901, Yuter Papers: Goldberg Reports July-August, 1946; January 1, 1947; and September 22, 1947.

90. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948.

91. ~~(TS)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949, gives the date of the commitment to magnetic drums as early 1947.

92. (~~TS//SI~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949.

93. (~~TS//SI~~) NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986.

94. ~~(S)~~ NSA CCH Series XI K, Sam Snyder, Box 12, "Analytic Machinery Principles," September 1949.

95. (~~S//SI~~) NSA CCH Series XII Z, "Symbols with their meanings for GOLDBERG programming," nd. On the speed of the 70mm Comparator, (~~TS~~) NSA CCH Series XII MPRO, Box 1, "Machines in the Service of Cryptanalysis," 28 September 1954.

96. ~~(S)~~ NSA CCH Series XI K, Sam Snyder, Box 12, "Analytic Machinery Principles," September 1941 43.

97. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. On the drum problems, ~~(S)~~ NSA CCH Series XII Z, "Goldberg Progress Reports," 30 December 1947 through 10 April 1951.

98. (U//~~FOUO~~) NSA CCH Series XII Z, Sam Snyder, "Draft Document, Pre-Computer Machines in Support of Cryptanalysis," circa 2 February 1978, IV-15.

99. (~~TS//SI~~) (U) Hagley Museum and Library, Accession 1901, Yuter Papers, ERA, Goldberg Reports, July 1946, September 1946, and January 1, 1947. On Vivians, (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. and their use v [redacted] (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase II," circa 1955.

100. (~~TS//SI~~) NSA CCH Series XII Z, "History of the Signal Security Agency, Volume Two, The General Cryptanalytic Problems." (~~TS~~) NSA CCH Series XII Z, "The Status of RAM," circa June 1945. ~~(S)~~ NSA AHA ACC 26373, SIS, "Technical Paper, RAM," circa June 1945. ~~(S)~~ NSA AHA ACC 29373, SIS Chief "F" Branch, "Request for RAM Equipment," 23 March 1945. ~~(S)~~ NSA CCH Series XII Z, OP-20-G, "SSA Proposal for 70mm Film I.C. Machine," 8 June 1945.

101. ~~(S)~~ NSA CCH Series XI K, Sam Snyder, Box 12, "Analytic Machinery Principles," September 1949.

102. ~~(TS//SI)~~ NSA CCH Series IV.C.2.14, ASA, "Annual Reports for the Fiscal Year 1949, Vol. II, Research and Development Division," Washington, 30 June 1949. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

103. ~~(TS//SI)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949. HYPO II was not delivered until 1952. There was also a project to explore the possibilities of computer output microfilm during the late 1940s. The Eastman contract was less than one tenth of what was allocated to ERA, but it was appreciable. ~~(TS)~~ NSA CCH Series XII X-MPRO, U.S. Cryptanalytic Research and Development Committee, "Joint Long Term Program for Research and Development in the Field of Cryptanalytic Equipment," 21 July 1948. ~~(C//SI)~~ NSA CCH Series XII Z, H. H. Campaigne, "Conference About Squinter," 15 November 1949. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948.

104. (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," and, ~~(C)~~ NSA CCH Series XII Z, H.H. Campaigne, "Conference About Squinter," 15 November 1949.

105. (~~TS//SI~~) NSA CCH Series XII Z, "Communications Supplementary Activities, RAM Report II," 21 December 1948, 19.

106. (~~TS//SI~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949, and,

~~(S)~~ NSA CCH Series XII Z, ERA, "Demon II Progress Reports," 15 July 1948 to April 1951.

107. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948," states that Hiawatha was begun on March 1, 1948, only to face the disappearance of Longfellow from the airwaves on April 11.

108. ~~(TS//SI)~~ NSA CCH Series XII Z, "Longfellow, History of," N-31 to 20-L, June 1948. ~~(TS)~~ NSA AHA ACC 8252, OP-20-G, "Communications Intelligence Research Plans, 1948," 7 April 1947. ~~(TS)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports," 1945-1949. ~~(TS//SI)~~ NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948.

This page intentionally left blank

Chapter 8

(U) Courage and Chaos: SIGINT and the Computer Revolution

(U) It Wasn't Safe at the Cutting Edge

(U) Well before the plans for Goldberg and Sled had matured, OP-20-G, joined a bit later by SIS, started a great adventure. They became part of what many see as one of the most important technological revolutions in history. The SIGINT agencies became active players in the attempt to make a technical fantasy come true – to build a universal machine. "G" and the SIS, along with several other military and civilian agencies, became prime movers in the early stages of the computer revolution. Establishing that historic foothold was not easy for either SIGINT group.

(U) An idea had emerged and became somewhat formalized outside of the intelligence community by 1945. It was going to be possible to have a high-speed electronic computer that could mimic any mathematical or logical process. With a rapidly changeable program, it had the potential to be a machine for every purpose, from calculation to machine control. The key to the machine's flexibility was its simplicity. It was to have very, very few hardwired functions, perhaps just the four basic arithmetic ones, and a few that allowed the movement of data between the input-output components, memory, and the single central processor. That and the organization of the machine around the binary system would, it was hoped, make it relatively inexpensive and allow it to become a mass-produced product. With one piece of hardware that could be made to imitate any machine through an inexpensive and easily changed set of instructions, the new computer had a great future. It would replace all other calculation and, perhaps, data processing devices.

(U) The ideas for the universal computer that began to take definite shape in England and the United States in 1946 were very appealing. As soon as they heard of them, mathematicians and engineers within "G" and the SIS pleaded with their superiors to make programmed computers part of the SIGINT arsenal. They were persuasive. By 1947 both agencies had committed themselves to acquiring general-purpose "computers."

(U) Neither agency realized what traumas they would have to go through to obtain them, however. Especially in the case of the SIS, the postwar experience was as anxiety-filled as the trials that Hooper and Wenger had gone through in the mid-1930s when they sought Vannevar Bush's help.

(U) Because Wenger had been able to set up a semicaptive engineering corporation in 1946, OP-20-G had an easier time than the army did. But even "G" and its Engineering Research Associates had some very tough moments trying to make the new computer come to life.

(U) That had not been foreseen in 1946. After learning of the possibilities of the new architecture, each agency had expected that outsiders would provide all that was needed. That was naive. The SIGINT agencies soon found it necessary to do much, much more than they anticipated. Because of the chaos that marked the development of the computer industry in the postwar era, both had to create their own machines.

(U) An Idea Differed

(U) In 1945 while the ambitious Goldberg's technology, if not its architecture, shifted with the appearance of technical innovations, and while machines like O'Malley were being constructed for immediate problems, another and more adventuresome project began at "G."[1]

(U) Duenna and the other "electronic" machines of the last two years of the war, combined with the knowledge of what other computer projects in the nation were attempting, gave the "M" group some ideas about a general-purpose computer. It was to be one much more flexible than Bush's older Rockefeller Analyzer or even his purely electronic Rapid Arithmetic Machine.

(U) When they had a few moments for reflection in 1944 and 1945, Engstrom and others in "M" speculated about what they could accomplish if they could find a large and fast memory, such as the vastly improved versions of the delay lines they were already experimenting with, to add to an electronic processor. While RCA's Jan Rachman's new idea for an all-electronic computer was rejected as almost "screwball," "M's" men kept thinking about the future. If a large memory with a speed that came close to that of the electronic processor could be found, then they thought a general-purpose computer was a possibility.

(U) But unless there was a high-speed memory, electronic processors would have to remain as special-purpose devices. Until the software could keep up with the speed of the processor, there was little need for electronics. If an electronic computer depended upon tape readers or the like for its directions, it could be no faster than the slow mechanical components.

(U) The input speeds of the best tape and card readers of the era were orders less than electronic processors. That limitation was compounded by the serial nature of both technologies. It was impractical to ask tape and card systems to back up to previous positions and repeat the reading of data or "instructions." A universal computer needed a memory that could support "go to" commands because tapes and cards could not fulfill that need.

~~(TS//SI)~~ The limitations imposed by the absence of high-speed memory were one of the reasons why the Sled architecture seemed so appealing. With special "boxes" hooked together through plugboard programs, processing was not dependent upon the nonexistent memory. The absence of memory was also one of the reasons why IBM and other business machines manufacturers confined their postwar electronic offerings to limited and special-purpose attachments, such as multipliers and dividers that hooked onto tabulators.[2]

(U) In 1945, any engineer who thought about moving further than the Aiken-IBM combination of motors, shafts, and tape readers, or the Moore School's set of ENIAC special-purpose boxes "programmed" through resetting huge electrical cables, had to have a great deal of faith. He had to believe that some technological hints would soon become viable and affordable hardware. There were some indications that such dreams might come true. But in 1945-6 they were just indications.

(U) Some thought that delay lines, tubes filled with chemicals, could be reengineered to serve as memories. The young experts at the University of Pennsylvania who were building the ENIAC felt they could convince delay lines from radar sets to behave well enough to hold programs as well as the data needed for immediate processing. That was a courageous commitment because those "acoustic" delay lines were very temperamental. It was very difficult to regulate the timing of the pulses that flowed through them. Slight changes in ambient temperature caused serious distortions. Also, it was difficult to monitor the behavior of the crystals that sensed the data "pulses" at each end of the tube. Even when all the technical difficulties were eliminated, a fundamental problem remained. The tubes could hold only a few "bits."

(U) There were some other memory possibilities being discussed at the end of the war. One

was to use a variation of the emerging television technology to store and recover "dots" of information on an oscilloscope-like screen. If it could be made to work, it would be an ultra-fast memory. A computer would not have to "wait" until the information it needed cycled past a sensing station. It would run at electronic speeds and would allow parallel data transmission.[3]

(U) There were more esoteric ideas for powerful memories, such as RCA's Selectron and the use of magnetics, but they were even less ready than the other alternatives.

~~(C)~~ Although the engineers at OP-20-G knew of the technological limits, they could not pass up a chance to at least survey universal computer options. John Howard formalized some of the ideas in a June 1945 memorandum; then, along with the "G" mathematician, C. B. Tompkins, toured all the East Coast computer projects looking for more ideas.[4] But little came of their trips. "G" was too busy to explore other than cryptanalytic machines. That remained true for several months after the war ended. Its workload even prevented "G" from sending a representative to one of the earliest postwar computer meetings.

(U) When Howard Engstrom received an invitation to participate in a major navy symposium on computers, he replied that "G" had done little of the type of work that was to be discussed and that he and his crew were too busy to attend.

(U) The urge to explore the possibilities of a general-purpose computer continued. But little could be achieved. "G" found it difficult to acquire connections to the outsiders, especially the academics, who seemed to be taking the first major steps towards creating the modern computer. "G's" old scholarly friend and go-between, Vannevar Bush, had stepped back from OP-20-G when the war broke out and did not try to reestablish the 1930s relationship. That left "G" without a prestigious outside scientist who could provide the critical endorsements speculative projects needed.

(U) Bush also decided not to return to MIT. He remained in Washington, acting as something of an academic elder statesman and high-level science policy maker until his retirement. Among his many contributions, he gave advice on the future of science in the military. In addition, Bush was frequently called upon to make recommendations concerning the integration of the nation's intelligence services. His role as a science advisor to President Eisenhower also played an important part in SIGINT mechanization in the 1950s.[5]

(U) Bush stayed at quite a distance from the computer developments of the postwar era. He also stayed away from OP-20-G, except for a few courtesy visits that Joseph Wenger arranged. One reason for Bush's arm's length relationship was a very heated argument with the Bureau of Ships about the Comparator. Soon after the war the bureau decided that it should be protected by patents. Bush was sent all the necessary paperwork to sign. He did so, but only after the deepest protests to the navy about revealing precious secrets and about imposing upon him.[6]

(U) OP-20-G had lost another friend. Stanford C. Hooper was in semiretirement. He was now old and ill, and he had to spend much time in Florida. He was acting as a consultant to several small electronics firms, including ERA, however. He still had the ear of many Washington influentials, but he could no longer aggressively fight to link OP-20-G, the scientific establishment, and the large corporations. In fact, he had become a bit soured on the corporations and academia. He had come to favor small private companies as the only guarantor of innovation and responsiveness.

(U) Meanwhile, the other part of OP-20-G's old university-computer connection, Bush's "boys," had migrated to the "captive" corporation, ERA. Howard, Coombs, and Steinhardt were

keeping up with computer developments, but ERA's first contracts and the imperative to develop a "cryptanalytic" machine kept them too busy to act as computer innovators. As a result, their 1945 general-purpose computer aspirations languished until mid-1946.

(U) Then, "G" developed a new and energetic computer champion. At the same time, it found someone with great enough scientific status to validate its request to acquire something which, in the mid-1940s, seemed more fanciful than Bush's 1930s machine.

(U) Goodbye Dr. Bush, Hello Professor von Neumann

(U) Just as the Goldberg project was launched in St. Paul and as Wenger's own research group was deciding whether or not to have someone build an electronic Super Bombe, one of "G's" mathematicians, James T. Pendergrass, enrolled in a summer institute on the programmable, digital electronic computer.[7]

(U) His inclusion in the Philadelphia meeting was almost an afterthought. Apparently "G" had not been asked to send someone until a few weeks before the Moore School Lectures began. Pendergrass had intended to spend much of the summer on vacation, but when his boss, Howard Campaigne, called him, he found it impossible to refuse the assignment. He rushed to the University of Pennsylvania and immediately began sending reports to Campaigne.

(U) Howard Campaigne was one of those bright young men who had been brought into "G" early in the war. Like his friend, Joe Eachus, he spent much time in England.[8] And like Eachus he became deeply involved with the RAM program. Deciding not to go to ERA, he became a civilian scientist within "G." He helped shape and direct "G's" postwar research agenda. By 1946 he was one of Joseph Wenger's right-hand men and was respected enough to be allowed to act as a representative of "G" to the outside world. That was what caused him to attend an important Navy Department conference in spring 1946.

(U) The conference was on the nature of large-scale computers. The major address was given by the man who would soon equal or exceed Vannevar Bush's status in the scientific-political realm, John von Neumann.[9]

(U) John von Neumann was perhaps the most famous of the new applied mathematicians. He had migrated from Europe in the 1930s to join the likes of Albert Einstein at America's only true research institute, a place where scholars set their own agendas. von Neumann became one of the "scientifically anointed" at the Institute for Advanced Study at Princeton.

(U) The first rumblings of war led the Institute and von Neumann to move far beyond their abstract academic origins. During World War II, von Neumann made important contributions to the atomic bomb project. As a result of that involvement, he became entangled in the ENIAC computer effort at the University of Pennsylvania.

(U) The University of Pennsylvania's World War II contract with Army Ordnance for the ENIAC had come almost by chance, just as the NDRC ended its computer program, and as firms such as RCA rejected pleas to turn their hard-pressed engineers to computer projects. Ordnance was in need of a way to speed the calculation of firing tables. With no other alternative, the army accepted the proposal of two young engineers at the Moore School. They promised to build an electronic version of Bush's great Differential Analyser. Fortunately for the history of computers, John Mauchly and Presper Eckert were given a great deal of freedom and time. Their much delayed postwar delivery of the relatively special-purpose ENIAC was not treated as a sign of failure, and their plan for a programmable

universal electronic computer was quickly funded.

(U) With the help of John von Neumann, they started the project (EDVAC) and began seminars that attracted the pre- and postwar generations of computer builders.[10] von Neumann's stature in the scientific and military communities had grown so much that his presence gave the Moore School's computer efforts the highest credibility. While working on the design of what is regarded as the first true universal computer, the EDVAC, the original leaders of the ENIAC project, Mauchly and Eckert, had become estranged from the university's administration and, to some degree, from John von Neumann.

(U) Von Neumann, whose importance increased in the postwar years, also became alienated from the University of Pennsylvania. He decided to found his own computer initiative. He was soon able to convince his old academic home, the Institute for Advanced Study (IAS) at Princeton, to accept several military and civilian grants and to create a center to house his attempt to design and build his own computer. His "IAS" machine was intended to serve the needs of applied mathematicians and physicists.

(U) Von Neumann did not confine himself to computer building. He became a major figure in Cold War science and policy. He advised all of the American leaders of the era, and he served on the most important science-related boards. He even became a good friend of OP-20-G and later NSA, serving on their expert panels. He gave them much technical and political advice throughout the 1940s and 1950s. His contributions included more than hints about new computer technologies. He frequently urged the SIGINT agencies to sponsor fundamental electronic research to be conducted by leading academics.[11]

(U) While von Neumann was forging his Cold War reputation, the Moore School had begun its own machine, the EDVAC. Sponsored by Army Ordnance, EDVAC was to have the simplest of architecture. Although it was intended to be an operational machine for the Aberdeen Proving Grounds, it was also something of a testbed. A central goal of the project was to prove that a universal machine could be made to work and to do it quickly. Therefore, EDVAC was designed as simply as possible.

(U) EDVAC was a binary machine that depended upon a serial acoustic delay-line memory. That memory was to hold both programs and data. The acoustic technology limited the machine to about 1,000 words of fast memory. Technological limits also dictated much of the EDVAC's internal organization. Trying to avoid the problems caused by the high failure rate of vacuum tubes, EDVAC's internal structure was made as sparse as possible. It had just one-third the number of tubes used in the ENIAC.

(U) To keep the number of components at an absolute minimum, the machine had only a few built-in instructions. That was a wise decision. Each "instruction" demanded dozens of tubes and hundreds of handwired connections. And each increased the computer's cost and multiplied the probability that it would experience a failure well before any significant computational task could be completed.

(U) In addition to keeping the number of components to a minimum, EDVAC's designers limited the machine to the serial transmission and processing of data (one bit at a time). Serial processing also reduced the amount of failure-prone electronics. But it carried the price of slower processing rates.

(U) EDVAC's designers made another trade-off that favored simplicity over speed. The machine's operations were based on "fixed clock" timing. That meant that no matter how little time one operation took, succeeding work had to wait until the next clock pulse.

(U) EDVAC's planners tried to keep their task manageable by concentrating on building a machine for mathematicians. EDVAC was not intended to be a data processor. The EDVAC engineers did not try to solve the many problems involved in making input and output rates approach electronic speeds. Slow tape and card readers gave the machine its data, and its even more primal cardpunches and teletypewriters displayed results. Although one of the first computer programs written by the ENIAC-EDVAC group was for sorting, EDVAC's builders never pretended that it could replace tabulator equipment.

(U) While the EDVAC's designs were being set, the ENIAC's parents, Eckert and Mauchly, left the University of Pennsylvania and attempted to found and keep afloat their own for-profit computer company. After more than six years of anxiety and tragedy, they completed the UNIVAC computer.

(U) The UNIVAC was also a delay-line, fixed-clock machine, but it went far beyond the EDVAC in terms of power and sophistication. One reason for that was the UNIVAC's attempt to become "the" new business machine, one to replace hundreds of tabulators. That called for the development of much-enhanced I/O technology. A new data processing capability was to some extent achieved through the creation of magnetic tape systems, a development that helps explain why the first UNIVAC did not appear until 1951.

(U) The goal of building a computer to replace the tabulators led to a very historic decision by Eckert and Mauchly. Because they wanted to maximize the speed of data processing, which typically demanded little calculation on a great deal of information, they deviated from a purely binary representation of numbers within the UNIVAC. It had what was called at the time a "decimal" representation. Although UNIVAC used binary circuits, a decimal format was imposed to speed the input-output functions.

(U) Eckert and Mauchly's commercial computer aspirations, as well as John von Neumann's academic ones, were just emerging when the University of Pennsylvania decided to host its historic summer 1946 Moore School conference. All those who had made contributions to computing during the war were invited to hear presentations by von Neumann and others who were outlining the computers of the future.

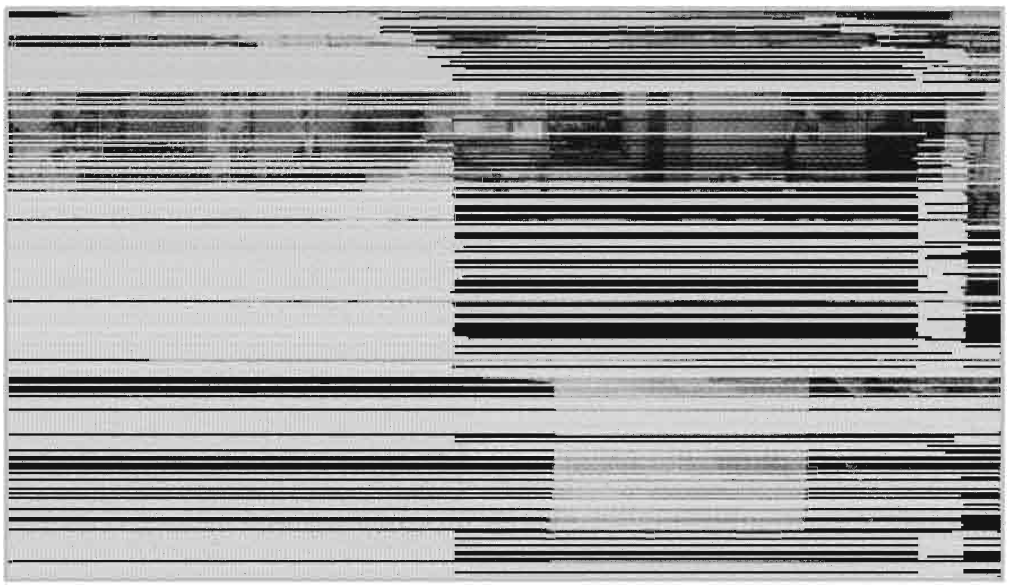
(U) A Summer in Philadelphia – an Exciting One

(U) It was probably Howard Campaigne's attendance at an earlier (May) navy symposium that made him aware of the Moore School conference. The Washington meeting was where he first made contact with von Neumann and where he realized that the general-purpose computer was going to be built, with or without OP-20-G. Campaigne decided that "G" should at least have a chance to be one of its sponsors.

(U) He hurriedly arranged for some funds and then called his assistant, James Pendergrass, asking him to attend the coming Philadelphia symposium. Campaigne was unable to tell him much about what was to take place in Philadelphia. As a result, much of what Pendergrass encountered surprised as well as thrilled him.

(U) During the Moore School's summer program, Pendergrass studied the designs of the ENIAC and those for the much more advanced EDVAC. He listened to the presentations of the other men who had begun to develop universal electronic machines.

(U) Coming from a physical sciences background and being an advocate for applied mathematics, Pendergrass was especially taken with John von Neumann's ideas, including his version of a programming language. When von Neumann outlined the concept for his new Institute for Advanced Study machine, Pendergrass became convinced that "G" had to have a von Neumann



(U) UNIVAC

type of computer. He thought the von Neumann design was the best, the one that would be the first to appear in hardware, and the one most likely to be cloned by a manufacturer. Well before the Philadelphia conference was concluded, Pendergrass convinced Howard Campaigne that OP-20-G should have one of the "new" computers, specifically one with a von Neumann architecture.

(U) Pendergrass was not the only one who believed in the IAS design. The mathematical and applied physics community took it as the model for computers for the 1940s and early 1950s. The emerging von Neumann architecture was especially attractive to mathematicians because it promised to provide a much faster and more precise computer than other designs of the era. It had the potential to be faster than the serial type of machines by factors in the hundreds. At least five IAS computers were copied in American universities and advanced research centers.

(U) The IAS machine was not going to send or process data bit by bit, nor was it going to make one operation wait for a "clock." It was going to send data simultaneously and would initiate an operation as soon as the previous one finished. As or more important, it was not going to be based on the limited delay-line memory. von Neumann bet that RCA would keep to its pledge and develop the very advanced Selectron tube within a few months. The Selectron promised to be a fast memory that would maximize the potentials of electronic speed and parallel data-transmission and processing.

(U) To many in the computer field, however, von Neumann seemed too far ahead of the technology. He also appeared to be naive about how much of the complexity of his proposed machine could be mastered by his handful of engineers. His critics thought the EDVAC group was taking a more sensible course: creating a minimal and reliable computer that had a possibility of being completed on time.

(U) Given the ambitious nature of von Neumann's computer, Pendergrass and Campaigne sensed that it was not going to be easy to persuade "G" that scarce resources should be devoted to a machine that was not yet fully designed, let alone built. No one, in fact, could

predict when any of the new computers would be completed.

(U) Despite von Neumann's reputation and the accolades that the atomic energy community was awarding to the IAS design, Pendergrass and Campaigne knew they would have to prove that "a" machine could compete with all the special-purpose devices that were in place at "G" as well as those that were being planned. And they would have to show, without insulting anyone, that the new computer would be as good as or better than Goldberg, the perhaps-universal comparator. Pendergrass and Campaigne were in a situation quite analogous to Hooper's in the early 1930s: How could they convince "operational" types that scientists had a better and practical grasp of the future?

(~~TS~~) Pendergrass got to work during the summer and continued on, with Howard Campaigne's enthusiastic help, through the remainder of the year. They composed two persuasive technical reports.[12]

(~~TS~~) The first was sent to "G's" higher-ups in October, the second in December. A great deal of effort had gone into both reports to ensure they would convince the cryptanalysts that, like the proposed Sled, the von Neumann machine would end the horror of having to wait two years while a requested special machine was constructed.[13] The reports did not refer to any particular experience, but Pendergrass knew that many in his audience had gone through the frustrations of World War II when almost all the RAMs (and the Bombes) had arrived too late.

(~~TS~~) In one of the classic statements in the history of computers, Pendergrass wrote: "It is not meant that a computer would replace all the machines in Building #4, nor is it meant that it could perform all the problems as fast as the existing special purpose machines. It is however, the author's contention that a computer could do everything that any analytic machine in Building #4 can, and do a good percentage of these problems more rapidly."[14]

(~~TS~~) The text of the report reflected both Pendergrass' orientation and the nature of mid-1940s computers. After explaining the logic of the von Neumann machine and admitting that it might be some time before any such computer would be available, he outlined what he thought was to be a standard programming language, one based on von Neumann's "one address" concept.[15]

(U) Von Neumann envisioned a machine that would be used for very precise calculation and little data processing. To speed calculating, it was to be a pure binary machine. To further improve performance, he had turned away from the original EDVAC idea of a four-address instruction. He had come to believe that the most efficient instruction format should include only one place to get or put data. That would allow, given the word size of the computer, more precise calculations without additional hardware.

(U) He argued that because his machine would be busy with much internal work, such as multiplication and division, it would be more efficient to have "get" and "place" addresses in separate statements. Only if a computer was to be used for much I/O and little calculation would a multi-address instruction be reasonable.

(U) Von Neumann also believed that his machine should have very few commands. The smaller the number of commands, the less internal circuitry that would be needed. Following his mandates, his engineers were able to reduce the number of components in the IAS machine. It had only two-thirds the number of tubes of the EDVAC. Von Neumann's mathematical focus also meant that he gave little thought to the I/O problem. What happened within the computer was more important to him than handling masses of data.

(~~TS//SI~~) Pendergrass agreed with all of von Neumann's ideas, but in his reports he suggested that a few additions be made to von Neumann's set of minimal instructions. They were to be ones which, like multiplication and mod 2 commands, would be needed to meet special cryptanalytic needs. Especially important to him were those which would speed the analysis of baudot traffic.

(~~TS~~) The politically important parts of the Pendergrass reports were the sections in which he and Campaigne presented computer programs for major cryptanalytic attacks. Demonstrating how the machine would perform the attacks was critical if "G" was to be persuaded to invest in a computer. Of course, the reports reflected an implicit faith that programming would be much, much less of a problem than building a special-purpose machine. No mention was made of how long it took to write the programs.

(~~TS//SI~~) The first report included software programs for a Generalized Copperhead problem, a Four-Wheel Enigma Grenade Problem, and a Hagelin attack. The December report was intended to impress any holdouts. It contained programs to imitate two of the grand achievements of World War I, the Duenna and the Mercury. As a concluding argument, the report showed how to end the great crypto-disappointments of the war years. There was a program that could imitate a cipher wheel. It showed that a general-purpose computer might act as an electronic Super Bombe.[16]

(U) Buy a Computer, Now

(~~S~~) The reports made their point, at least with farsighted men like Joseph Wenger. He took action even before the Pendergrass-Campaigne report of December was completed. To reinforce Pendergrass' arguments, he immediately arranged for ERA's John Howard to conduct a computer feasibility study and assigned Pendergrass to continue to survey the computer field.

(U) Pendergrass did not waste time. In November he informed "G" that many military and some civilian agencies were very interested in digital computers and that projects at the National Bureau of Standards and RCA (with the IAS) stood a good chance of producing machines by 1948. The IAS-RCA project, he thought, had the best design and best chance of success.[17]

(U) After attending another major computer conclave at Harvard in January, Pendergrass forwarded a new survey of America's and Britain's computer ambitions. He cited the emergence of more computer projects, most of which were supported by government agencies. The navy's Bureau of Ordnance and the ONR, he showed, had already established quite a foothold, as had Army Ordnance. Even the Census Bureau had become involved.[18] Among the six active projects[19] (the one under John V. Atanasoff had just been cancelled by the Naval Ordnance Laboratory), the IAS computer, Pendergrass reported, continued to be the best option. It remained much closer to completion than the proposed Whirlwind at MIT, and it was more suited to cryptanalytic work than the upcoming UNIVAC or the EDVAC.

(U) The only nonpositive things that Pendergrass had to say about the Princeton efforts were that he had discovered that RCA and Princeton did not have a formal agreement binding the corporation to build a computer and that its valuable Selectron was still in the "uncertain" category. Neither seemed critical to Pendergrass, however. He expected a working IAS machine by mid-1948. He assured "G" that if the Selectron were not perfected, an electrostatic memory, such as the one proposed by MIT's Jay Forrester, would serve as a fully acceptable substitute.

(~~S~~) Pendergrass' surveys were read by Howard Campaigne, then sent to Joseph Wenger. Wenger trusted Pendergrass, and he believed that OP-20-G should gain a foothold in computers before one of the other branches of the navy

established a monopoly. Without waiting for John Howard and C. B. Tompkins to submit their ERA report (it arrived in February 1947), Wenger made a commitment to acquire a von Neumann type of computer.[20]

(~~TS//SI~~) Even before a contract was let, plans were laid to use the new machine on major operational problems.[21] "G" even put aside the idea of building an electronic Super Bombe, at least until the potentials of the new universal computer were explored.

(U) In January Wenger was so enthusiastic that he ordered his men to establish project "Atlas," although he did not yet have the funds to design and acquire a machine.[22] The name "Atlas" was picked because a comic strip used it as a name for a "mental giant," but a reference to raw courage would have been as appropriate. Wenger still had to gain formal approval for the "G" computer.

(~~S~~) As Wenger struggled to find the money he needed, additional crypto-studies reinforced the initial enthusiasm, and went beyond it, perhaps raising expectation a bit too high: "This opens tremendous possibilities in the field of clinical attack by speeding this attack up to the point where large volumes of traffic may be so processed. With sufficient skill in preparing the logical control, it seems possible that the machine may be made to perform any cryptanalytic operation now done by hand, which does not require intuition."[23]

(~~S~~) Wenger did everything he could to make sure the "G" computer proposal would be funded. He had Pendergrass assigned as a liaison to the Office of Naval Research. It was exploring computers and was intensely committed to furthering applied mathematics. With Pendergrass in touch with ONR's experts, they would be unlikely to block the "G" request on technical grounds. Other mathematicians in the agency were sent to important computer seminars: Eachus, Campaigne, Blois, Tordella, and others met with the "greats" of computer history, such as Alan Turing and M. V. Wilkes.

(~~S~~) The contacts and investigations soon started to pay off. "G" was gaining a reputation as one of "the" centers of computer expertise. Other development projects, such as Whirlwind at MIT, gladly shared design information.

(U) At least in terms of computer architecture, "G" was well integrated with high science. "G" became committed to the atomic scientists' favored way of sending data within the machine: all the bits at one time in parallel, rather than one bit at a time (serial mode) as in the EDVAC. As important, "G" wanted Atlas to have a single memory, one to hold both data and instructions. That was in contrast to some architecture, such as those of Howard Aiken at Harvard, who thought separate memories, concurrent processing, and dozens of registers made for a more powerful computer.[24] Without any hesitation, "G" favored a pure binary system for its computer. The idea that became embodied in the UNIVAC, that some decimal representation was more efficient was rejected.

(U) While his research crew defined Atlas, Wenger worked on the politics of acquisition. He convinced the CNO of the need for Atlas, gained an extremely high priority rating for it,[25] and then sidestepped some serious objections from the Bureau of Ships.

(U) In response to hints there were already enough navy computer efforts and that long term research should be left to others, Wenger informed the bureau that "G" needed to acquire a "special analytical machine." The word "special" gave OP-20-G the opening it needed to avoid a worst-case situation in which it would be forced to wait for and accept a machine it might not want. It also gave "G" the chance to play a positive role in the emergence of the computer industry.[26]

(U) Well before authorization had been granted, "G" began a more detailed design and made evaluations of possible computer manufacturers. With all the other government agencies sponsoring research in the field and with the interest shown by several private companies, "G's" experts did not anticipate that a large investment would be required for the design or for the hardware. "G" still thought RCA would enter the market. The National Bureau of Standards also seemed ready to build a computer. Wenger expected to have Atlas at the Nebraska Avenue complex in approximately two years.[27]

(U) Whatever the options, Wenger wanted quick action. Even though a "special" machine had been approved and although Monogram funds were available, there was always the chance that the White House might decide that computers were a luxury. Even the $100,000 to $300,000 for the machine might be seen as too much for a peacetime intelligence agency.[28]

(U) Laying out the general specifications for Atlas was relatively painless. Pendergrass had done his technical homework, and his recommendations were only refined, not changed. Beginning in March 1947, when "G" decided to take more responsibility for designing its Atlas, Campaigne, Eachus, Pendergrass and many others at "G" began to meet to detail the functional characteristics of their newest "analytical machine." They even began to write programs. The enthusiasm was so great that many worked nights and weekends on their problems.[29]

~~(S)~~ "G" was to have a von Neumann computer, not a souped-up version of its older devices. Suggestions that Pendergrass' original sketches be altered by adding special-purpose attachments were adamantly rejected, as were those recommendations that the machine have control switches and plugboards. Software, driving elemental circuits, was to be the only control mechanism.[30]

~~(S)~~ But the number of commands built into the machine was to be expanded beyond von Neumann's original list, and Pendergrass' early recommendations. By 1947 close to forty commands were in the design. The expansion was aimed at easing cryptanalytic processing, as had been the alteration in the fundamental word size in the machine to six digits. That would allow letters as well as numbers to be analyzed.

~~(S)~~ The additional commands were at the fundamental level of the machine. There were no suggestions that complex sequences to imitate entire processes be wired into Atlas. A series of multiplication commands and a divide instruction were included, however, as were shift commands and noncarry arithmetic capabilities. Shifts were especially useful when rotor or wheel stepping was required, [redacted] Also, there were hopes that a random number generator could be devised.

(U) Campaigne, Eachus, and the others on the design team had bright hopes for Atlas. But there were limits to the aspirations. They accepted the fate that plagued the first computer generation: They did not attempt to write a compiler or a high-level language for the machine. The only treat the "G" group gave programmers was the luxury of writing in octal rather than binary notation. That provided some relief, but it did not allow a programmer to avoid specifying the location of memory addresses in "absolute" terms. There was no software to automatically keep track of where instructions or variables were located.

(U) Like the IAS computer, Atlas was to be centered about what the Princeton group considered "the" solution to the memory problem, the RCA Selectron tube. It would allow an electronic-speed mass memory, something needed to meet the potential of parallel data transmission and processing. Hopefully, the Selectrons would support a large memory. In 1990s terms, Atlas was to have 64K. In terms of the longer word size of the

Atlas, that was equal to 16,384 "cells." That was orders greater than what was planned for EDVAC.[31]

(U) The Selectron was under development at RCA's research laboratory. Rachman's tube promised to be much more powerful than the other types of binary electrostatic storage devices that were under development. And it was expected momentarily. Although some at OP-20-G had treated many of Rachman's ideas as more than fanciful, because of his advanced work during the war, he had become an ally of von Neumann, and his work demanded respect.[32]

(U) The Selectron was a complex device, but it had a great advantage; it was small and fast. Its size was one of its great attractions because other high-speed memories of the period, such as delay lines or the Wilkes electrostatic tube,[33] took a great amount of space. Unfortunately, the Selectron proved to be too complex.

(U) It was based upon the principle that "an insulated secondary-electron emitter can be made to 'float' at either of two stable positions..." Deceptively simple, the principle demanded much delicate hardware. Inside the three-by-seven-inch tubes was a dielectric target that was divided up by sixty-four metal bars and sixty-five circular metal rings. They created 4,096 "cells" that were the storage areas. When the four walls of a cell were all more positive than some particular voltage, a "bit" was registered.

(U) To von Neumann's and "G's" great disappointment, all that was too much, even for the great Jan Rachman.[34] By spring 1947 RCA had to admit that it might be some time before the Selectron was ready. That led to some technological soul searching in Princeton and Washington. The IAS put more effort into a television-like electrostatic memory and even explored the possibility of ultra-high-speed secondary memory based on magnetic wire wound on bicycle wheel drives.

(U) The news about the Selectron was only one indication that the computer revolution was going to take much longer than had been thought. RCA began to make it clear that it was pulling back from its hints of becoming a manufacturer, the National Bureau of Standards program had slowed to a crawl, and the probability that the ex-ENIAC team, Eckert and Mauchly, could deliver their promised computer to the Census Bureau in time for the 1950 census sank to near zero.

(U) By spring 1947 Atlas was on its own. If "G" were to have its computer, it would have to take even more responsibility, perhaps even for a very expensive failure. And it would have to make a critical technological choice.

(U) Little Thanks for That Memory

(U) In April 1947, after learning about the faltering industrial commitments and the Selectron's possible stillbirth, "G" made two very significant decisions. The first was to continue with the project and the acquisition of a computer despite the absence of an "industry" or even a university that seemed willing to build computers. The second decision was perhaps more dramatic.[35]

(~~TS//SI~~) When it was learned that the Selectron would not be available, there was a critical meeting at "G's" Nebraska Avenue headquarters. Some of those in attendance thought that without the high-speed memory it would be senseless to continue more than very general design work. What use would Atlas' electronic circuits be if the memory was a slow tape or similar device? Even looking for a manufacturer for Atlas did not make sense to them. There were a few suggestions that the entire project be put on hold.

(~~TS//SI~~) Howard Campaigne, perhaps worried that such a decision would end chances of funding, put up a stubborn fight. He won half his battle: The work was not canceled. But his victory seemed to open the door to some dangerous

possibilities. His recommendation to go with what had always been the "fall back" memory for Atlas and Goldberg,[36] a magnetic drum, stood the chance of making Atlas and "G" look rather foolish. It could make Atlas very slow and perhaps very dumb.

~~(TS//SI)~~ Drums were much faster than tapes or cards, but they delivered information at a rate of 1/400th or less of delay lines. Some estimates of the period gave the Selectron and electrostatic memories a 1,000-fold advantage.[37] If microfilm could have been made to be "rewritable," it could also have made a drum look antiquated. Seventy-millimeter microfilm held 12,000 bits per inch; drums had a density of from 100 to 200 bits.[38]

~~(TS)~~ Although "G's" RAM group realized that such a memory would slow the proposed machine manyfold, by a close vote its members decided that a drum would be acceptable. It seemed a much better choice than postponing the project and being left dependent on the whims of an almost nonexistent computer industry.

~~(TS)~~ Campaigne and his associates realized they were taking a chance. There were hosts of mechanical as well as magnetic-electronic challenges to overcome. Whether the "drums" were long bars or three-foot "wheels" covered with magnetic tape or sprayed with a magnetic coating, the problems of milling, sensing heads, and drive motors remained unsolved. Even ERA, with a head start on drum construction because of its connection to the earlier RAM projects, did not have a finished and sure technology in hand.[39]

~~(TS)~~ "G" decided to take the risk. While the IAS group waited for the Selectron's development or the appearance of another electrostatic memory, "G" started to work on revised designs for a drum machine. It also began a search for someone to build the newly defined Atlas.[40]

~~(TS)~~ No serious consideration seems to have been given to having, as would many atomic energy research groups, a university take charge of final design and manufacture. And "G" did not spend much time investigating the few companies that seemed willing to build computers. Thus, soon after the critical April 1947 meeting, ERA was chosen even though "G" knew how busy the young firm was with its first contracts.

~~(S)~~ There was some worry that Atlas might be a bit too much for the new company and that some emerging problems with magnetic drums might not be conquered.[41] But in August 1947 ERA was given a design contract. And it was informed that "G" wanted a machine soon. ERA was not to wait for the results of the several research projects OP-20-G and the SIS were sponsoring to develop multifunction and ultra-high-speed tubes and new circuits. And there was no thought of delaying Atlas just because there were not yet any high-speed printers suitable for an electronic computer.[42]

~~(TS)~~ There were a growing number of reasons why "G" wanted ERA to quickly prove the worth of a universal machine for cryptanalysis. Just as ERA was put to work on the final designs, the Sled project with its special architecture was being launched with much support from the Bureau of Ships. In addition to having some competition, Atlas had to face another possible trauma; there were well-grounded rumors that the Monogram budget was to be cut severely so.[41]

~~(TS)~~ With a great deal of help from "G's" research group in Washington, ERA was able to develop an acceptable design within a few months. As requested, it matched the von Neumann concepts and was aimed at avoiding manufacturing problems. Some rather useful ideas were sacrificed to the needs of the production schedule. A second processor, which would check results, was not included, and the suggestion to develop a partitioned memory was dropped. Having as many as eight active "accumulators" was also regarded as too much of a luxury.

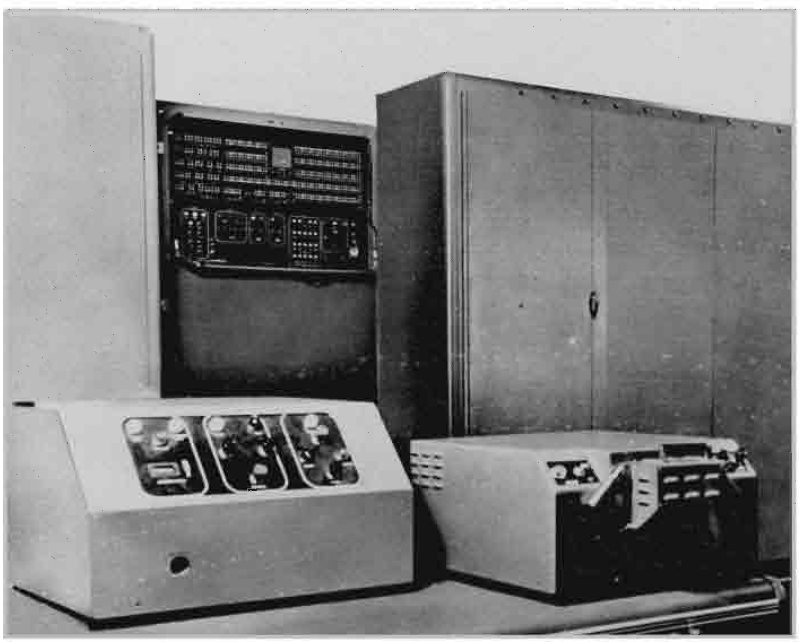
~~(TS)~~ In early spring 1948, in return for promises to use as much standard equipment as possible, ERA was awarded a construction contract. There was a caveat, however. ERA was more than encouraged to build Atlas in a way that would allow the substitution of electrostatic (Selectron) storage if and when it became available.

~~(TS//SI)~~ ERA and "G" were in a hurry. Atlas was given an AA priority, ERA borrowed much from MIT's Whirlwind project, and ERA gave Atlas as much attention as possible even when it had to rush to complete some special-purpose machines to attack Russian targets.[44]

~~(S)~~ While the engineers in St. Paul were working on Atlas, the mathematicians-turned-programmers in Washington built their own computer to prepare for Atlas' arrival. They wanted programs ready to help prove their electronic computer's operational value as soon as it was delivered. Constructed within four months out of relays and a small magnetic drum developed by ERA, their Abel computer was a logical clone of Atlas. It gave "G" more than a year's head start in training programmers and in writing some operational programs. Its drum was not large enough to perform all of Atlas' chores, and its relays were hundreds of times slower than ERA's circuits, but it came to be almost a "pet" of the research group.[45]

~~(C)~~ Meanwhile, despite the growing pressures on ERA, it was able to work something of a computer miracle: Atlas was delivered to the navy in early December 1950, fairly close to the anticipated delivery date. It had taken ERA less than two years to construct the machine, perhaps because so much time had been spent preparing for its production stage and because of ERA's experience building special-purpose machines, such as Goldberg. In fact, Atlas was the thirteenth project for "G."[46]

~~(C)~~ Most of the design goals were accomplished. That made Atlas one of the very first operational computers in the world. ERA also achieved another sort of computer first: Atlas worked and worked well for a decade after it was sent to Washington. A very efficient testing and maintenance schedule allowed replacement of tubes before they caused an unexpected failure. That contributed to an almost unheard of 90 percent "up-time" (availability), which made ERA very proud and very anxious to transfer its new computer skills to the commercial marketplace.[47] It was also proud that it could have built one of the most powerful of all the early computers using only 2,700 tubes and that its drum performed reliably.[48] As a result, ERA and its follow-



(U) Atlas 1

on companies became leaders in magnetic drum technology and gained a reputation as supercomputer builders.

(U) Saving a Reputation through Logic

~~(TS)~~ But all the original Atlas goals were not attained. The machine had cost perhaps three times the early postwar estimate; its delivery price was just short of $1,000,000. [49] More importantly, the drum held less than one-third the amount of information that had been hoped for in 1947. But ERA was able to rotate it at an extremely high speed. Partly by reducing its size from the dimensions of earlier drums (three feet in diameter) to twenty-five inches long and eight inches in diameter, Atlas' drum was ten times as fast as the one installed on Goldberg. [50] The increased speed helped, but it did not solve the memory access problem. The 1950 Atlas began its life as a very slow machine because the program, as well as data, had to be read from the drum. There did not seem to be a viable technical save. Replacing the drum with the still expensive and irritable electrostatic or delay-line memories seemed impractical.

~~(TS)~~ The programmers at OP-20-G were charged with finding the best solution they could. Perhaps to everyone's surprise, they came up with an answer that made Atlas competitive with other computers of the time.

~~(C)~~ The solution they devised was called "interlacing." Combined with very careful programming, it increased Atlas' speed by a factor of more than 300. That meant that the drum-based Atlas became approximately two-thirds as fast as a similar machine using the new magnetic core memory of the mid-1950s. In fact, Atlas came close to being a match for the IAS machine.[51] The increase in Atlas' speed came at a high cost to the early programmers, however.

~~(S)~~ The trick they had to pull off was to place instructions around the drum in such an order that rotation time until the next expected instruction was minimized. At first, a plugboard was used to accomplish the necessary scrambling of once-sequential locations. By 1951 an automatic "dial" system was installed that eliminated the need to replug a board for each program. Although the relocation of instructions was made automatic, programming was not. To utilize the "interlaced" instruction, programs had to be drafted on large sheets of paper. The two-by-three-foot sheets allowed the programmers to keep track of where the instructions were located and allowed them to perform timing miracles so that the call for the instruction came when the drum was in the correct positions.[52]

~~(TS)~~ Despite the near agony of Atlas programming, a wide range of statistical attacks was run on the machine. It proved Pendergrass' point about flexibility although writing Atlas' programs, took much, much longer than had been imagined by him in 1946. Such fondly remembered programs as Bootstraps for the identification of nonrandom distributions (roughness testing) and [redacted] analysis aids took enormous human effort.[53]

(U) The new programmers in Washington could not find any way to compensate for another of Atlas' failings, however. Atlas could not be coaxed into becoming a data processing computer. Its input-output capabilities were too limited. It brought data to its drum through a photoelectric papertape reader; an Electromatic typewriter and a tape punch handled its output. There were no pathways for punch card machines nor for the just emerging magnetic tape drives.

~~(TS)~~ A severe limitation with many ramifications was Atlas' inability to put the input tape-reader under program control. All the reader could do was load the drum. The paper tapes could not be used as a dynamic source of data.[54]

~~(S)~~ Atlas' sparse I/O was a result of conscious design judgments, ones which mixed technologi-

cal possibilities with operational needs and with a strong dose of "GM's" goal of fulfilling Wenger's dream of "mathematical" cryptanalysis.

~~(S)~~ When Atlas was being designed, the only new large-scale secondary memory media that seemed to have input potential was magnetic tape. But tape systems with the possibility of holding massive amounts of information remained in the development stage and were proving very stubborn. To wait for their maturation would have delayed Atlas' construction; to attempt to anticipate what circuitry Atlas needed to hook up to future systems would have been foolish.

~~(S)~~ Attaching Atlas to an IBM card reader might have seemed attractive at one point, but there may have been questions about using that company's equipment in a competitor's system.

~~(S)~~ In any case, "G" had decided by 1948 that energies would go to increasing Atlas' internal processing power by adding additional "instruction" circuits. The expansion of the number of hardwired instructions was intended to encourage the use of "mathematical"cryptanalysis. The many binary multiplication and shifting instructions and the divide circuitry made Atlas more expensive and harder to manufacture, but they speeded statistical testing by many factors.

~~(S)~~ Those features seemed so attractive that despite the severe I/O limitations, a second Atlas was ordered some six months before the first was shipped from St. Paul. Because the initial model absorbed the development cost, this Atlas was priced at one-third of the original. At the same time, a new design cycle was begun. The Atlas II, which in its civilian guise was called the 1103, was the machine that anchored the ERA group's computer building reputation, although its original price was $1,250,000.[55]

~~(TS//SI)~~ For a time, however, it was thought that Atlas III would be a data processor as well as a "number cruncher." But Atlas II could not overcome the earlier I/O limitations. When it was being designed, the Raytheon Company announced it was perfecting tape drives. ERA's engineers built a program-controlled I/O feature into the machine only to discover serious technical difficulties with the Raytheon magnetic tape systems. Despite a last-minute effort, eleven were delivered without a tape capability.[56] But its internal processing powers were much enhanced. Some electrostatic storage was added, the drum was improved, a two-address logic was introduced, the word size was increased, and several very useful basic instructions were added.

(U) All in all, "G" thought that its sometimes frustrating computer adventure had been worthwhile. The agency's advocates for general-purpose machines had made their point, and the work on Atlas helped to establish ERA as a computer company. The Atlas designs and designers would play an important part in the history of automation of communications intelligence.

(U) The relatively happy ending of the Atlas project was not quite matched in the army's attempts to establish its place in the computer world.

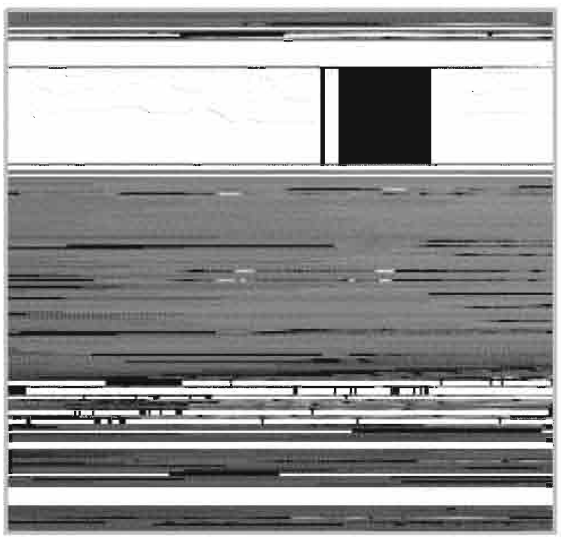
(U) The Army's Problem

~~(C)~~ The SIS lost many of its engineers after the war, and it was unable to create its own ERA. In response, it planned to do some machine design in-house, go to contractors for details and components, and, when necessary, assemble its secret special-purpose devices itself. That seemed quite efficient, but the SIS was unable to follow that approach when it began its quest for its first general-purpose computer, a machine that took its name from another newspaper cartoon character, "Abner." Although some have claimed the name was chosen because the modern computer without a program is a dumb machine, the selection of the name in 1949 may have been inspired by the nature of the search for a design and a

manufacturer. The army's codebreakers had gone through a bizarre and agonizing odyssey during the previous three years. The experience was almost cosmic.[57]

~~(S)~~ In 1945 there was a significant reduction in force at the SIS. But Solomon Kullback and Leo Rosen were able to retain enough personnel and funds to continue the old "F" branch – one with a fresh bureaucratic name and expanded powers.[58] One of their first and most important decisions was to appoint one of their young proteges to head a new subsection. In January 1946 Samuel S. Snyder, who later became a major figure in the computer and information world, was asked to survey the wartime computer developments and then to turn his new RAM research group into a dynamic force. The group was to keep the agency informed about all the computer developments in the world and to act as an advocate for further automation within the agency.

~~(C)~~ Snyder and his coworkers, Mary Roseboro and William May, began by gathering and rewriting all the documentation that remained on the World War II machines at SIS. Soon they decided to expand the survey to include the devices OP-20-G had obtained. That turned their project into creating what became the irreplaceable "Machine Aids to Cryptanalysis" series.[59]



(U) Samuel S. Snyder

~~(C)~~ Snyder did more than follow in-house developments. By mid-1947 he had visited the National Bureau of Standards and had made some contacts with those in academia and the commercial sector that had interests in computer development. But he got somewhat of a late start at his attempts to bring a computer to the agency.

~~(S//SI)~~ The SIS was at least a year or two behind OP-20-G's computer work. One reason was that someone like Snyder had not been selected to attend the Philadelphia computer symposium in mid-1946 that had so impressed Pendergrass. Instead, Kullback had sent a SIS engineer who had little or no mathematical or cryptanalytic experience. The man was not impressed with what he heard and did not report back to the SIS that a great technological and cryptanalytic opportunity had appeared. According to Snyder, the man did not even submit a report on the ENIAC and EDVAC designs.[60]

~~(S//SI)~~ Fortunately for the agency, Sam Snyder encountered Pendergrass' report. Inspired, he began contacting others who were developing what later became known as "computer science." Snyder became somewhat of a computer "trekkie." He attended all the meetings, such as the famous one at the Aberdeen Proving Grounds, of the just forming Eastern Association for Computing Machinery.[61] He learned of the vast data processing center at the Prudential Insurance Company (some 700 IBM machines) and the plans of one of its aggressive young executives to make the Prudential a center for electronic computer development and applications. That contact with E. C. Berkeley reinforced Snyder's rather philosophical view of the coming computer revolution. Berkeley was one of the first "futurists" in the computer field.[62]

~~(S//SI)~~ There was a much more practical side to Snyder's trips around the East Coast. By at least mid-1947 the SIS decided that it would not let OP-20-G be the only one with an electronic general-purpose computer. Snyder was sent to all the companies and academic institutions that had indicated they were going to take the risk of building a computer. The only centers Snyder did not seem to visit were ERA, Harvard, and Western Electric. He skipped ERA because he already knew about its computer design and, perhaps, because from the beginning, the SIS did not want just a clone of the navy's computer. Nor did it want to become dependent on the navy's captive corporation." He bypassed Harvard, where Howard Aiken continued to build ordnance computers, because the unique Harvard architecture did not seem right for cryptanalytic work. The Western Electric postwar devices also seemed to be a bit "old" in terms of design and hardware.

~~(S//SI)~~ Snyder's trips were exciting; he was becoming a pioneer. He was able to see all that the fledgling UNIVAC group in Philadelphia was doing. He even spent time with Grace Hopper, who was becoming a legend in the computer world for her contributions to programming. While in Philadelphia, he also made contact with the EDVAC team. Then he headed for Princeton and the Institute for Advanced Study where Julian Bigelow was leading the group that was slowly making John von Neumann's concept turn into hardware. The Institute and Bigelow were impressive, but Snyder continued his search. Soon he was in Boston, where he found what he thought was the most promising of all the computer projects in the country. It was the one within Vannevar Bush's old company, Raytheon. Bush, however, had nothing to do with the project. In fact, many of its bright engineers had come out of the World War II computer projects run by Howard Aiken at Harvard.

(U) Snyder thought that Raytheon's R. M. Bloch, R. V. D. Campbell, and M. Ellis were doing the most exciting work in the country and were the most likely to be able to construct the type of computer the SIS needed.[63] In addition to the design of its computer, Raytheon was attractive because it was the only large corporation in the country willing to subsidize computer development.

(U) The company was in a unique position. Raytheon had gone from a moderate size firm in the 1930s to become a major defense contractor during World War II. It was aggressively seeking new products and markets that would allow it to keep its position in the peacetime economy. That was in contrast, for example, to IBM, which was unwilling to endanger its major product lines by leaping into computers.

~~(TS//SI)~~ The small firms that were showing interest in computers were not viable alternatives for Snyder. Investing in them posed a risk for any purchaser. Even the one with the best reputation was showing signs that it was overreaching itself. UNIVAC's Eckert and Mauchly wanted the SIS's work, but could not commit to building a machine that would suit the needs of cryptanalysis within a reasonable time. In addition, there may already have been security problems at the company.[64]

~~(S)~~ That left Raytheon as almost the only option for the SIS. Then the proposed Raytheon machine received more acclaim. While Sam Snyder was making the rounds of the computer centers, his research group had been examining the designs of all the proposed computers and found that Raytheon's was to be a data processor, at least much more so than Atlas or any of the von Neumann machines, because it was a four-address device. In addition, although it was a serial processor, its speed would be more than adequate because it was to have a large and fast memory built of Selectrons. Although ERA had concluded that the Selectron might never appear and turned to the drums, the SIS bet that it would soon emerge from RCA's research laboratory.

~~(S)~~ Talks were begun with Raytheon's management, and by fall 1947 the SIS group thought an advanced computer was about to be built for them. The early plans included more than just a fast memory. Raytheon promised to make its computer more of a data processor than any other by developing revolutionary magnetic tape and wire systems. They were to provide high-speed bulk input, and there were even hopes of devising high-speed output mechanisms. Perhaps as important, the SIS thought that Raytheon might deliver a machine before Atlas could be sent to Washington.

~~(S)~~ It wasn't too long before those hopes were dashed. Raytheon let the SIS know that because it had obtained a contract for a computer from another navy agency (through the NBS), it would be at least three years before a SIS computer could be completed. Although the company offered an attractive price, $350,000, and indicated it would be able to provide the SIS with a machine that included their very promising plastic tape systems, they declared they would provide it on their schedule.

~~(S)~~ The SIS group hesitated before accepting the new offer, thinking that three years was much too long to wait. They had been very busy writing their own version of the Pendergrass report and had already written programs for the type of machine they desired. Those investments seemed too much to waste. But there was no alternative to Raytheon.

~~(TS)~~ When the SIS managers returned to the company, they were somewhat resigned to a long wait, although they planned to bargain over delivery schedules. As they started the negotiations, they received a shock. The company had reworked its estimate of the cost of a computer that met Snyder's needs. Raytheon now wanted so much more that the SIS turned the offer down without further bargaining.[65]

(U) Stratton's Dream Revisited

(U) In near desperation, Snyder went to the National Bureau of Standards. Standards had visions of becoming what Stratton had desired a generation before: the center for computer development in the nation. John Hamilton Curtiss, an applied mathematician with a Harvard degree and wartime navy experience, had been hired by the new crusading leader of the NBS, E. U. Condon, to accomplish that. By 1947 Condon had funds for computer development and was on the way to becoming an intermediary for all government agencies' computer purchases. With a group of energetic engineers and mathematicians, the NBS guided, for example, developments at UNIVAC and Raytheon. It was doing much more. It was encouraging and coordinating the work of many contractors who were developing computer components, and it was making suggestions to builders to improve computer architecture.[66]

(U) But contact with the NBS did not lead to any immediate relief for Snyder. The best the NBS said it could do was to allow Snyder's group to attend the computer lectures it was conducting and to provide leads to new companies that might be willing to build a computer.

(U) It was mid-1948 and the SIS still did not have a final design or a contractor.

~~(C)~~ The SIS went in circles for a time, then came back to an earlier contact, the Reeves Instrument Corporation, a New York firm that was a leader in the analog computer business. It had just completed a very useful and pathbreaking electronic differential analyzer, the REAC. It had also gained some digital experience by helping the University of Pennsylvania with its computer projects. More importantly, it had let it be known that it was going into the digital computer business. To do so it had hired one of the most unusual men in the early computer business,

Samuel Lubkin, to supervise the design and construction of its proposed REVAC.

~~(S)~~ Lubkin was an alumnus of the important University of Pennsylvania projects, and he wanted to build his own improved version of an EDVAC. His past experience and the preliminary design of the Reeves machine convinced the SIS's team to support Lubkin's design although he planned to use delay-line rather than faster Selectron memory. Abandoning the Selectron was difficult, but there was an attractive trade-off: Reeves was proposing to build its advanced version of the EDVAC within one year for a bargain price of $150,000. [68] Although the Reeves machine would be serial and clock-based, it was to use four addresses; most importantly, it would be at Arlington Hall before the end of the decade.[69]

~~(S)~~ Serious talks were begun with Reeves in early summer 1948 and Snyder and his team felt vindicated.

~~(TS)~~ Then chaos took hold again. Just as negotiations were begun, Reeves announced it was not going to branch out into digital computers.[70]

~~(S)~~ Lubkin immediately left the company. At first Snyder thought that all was not lost. There seemed a chance that Lubkin could become an SIS employee. At least the design for his machine could be finished. Talks were held: then Lubkin decided he wanted to found his own computer company. For a moment it appeared that the SIS might have its own version of ERA. That was a short-lived dream. Lubkin could not raise the necessary financing. Lubkin gave up and took a government job, but not with the SIS. He went with the National Bureau of Standards.

(U) There was no one left to build "Abner." For the SIS there was no American computer industry. Then there were a few moments of relief when the NBS gave some indications that it might arrange for a computer for the agency. As happened so many times before, the hopes were defeated. The contractors the NBS was depending upon for the computers to be used at its important applied mathematics centers could not meet their schedules. They got so far behind that the NBS decided to build a machine for itself. That eliminated any chance that the SIS could get a machine within the near future. The NBS would be too busy arranging for its "interim" computers. Its work force had to concentrate on a machine to save the NBS's numerical centers, and its needs would keep available subcontractors busy.[71]

~~(S)~~ Swallowing a great deal of pride, the SIS made another brief attempt to get Raytheon to reconsider. No deal could be struck. Then the SIS decided that it had only one alternative, unless it was to give up on the idea of being one of the first members of the world's "computer club." No matter what the risk, it had to build its own machine. Snyder reasoned that since the SIS now had an engineering staff of some sixty men who had already had much electronics experience (as a result of their work in radar and other military electronics), there was a chance of success.

~~(C)~~ But Snyder knew his group required help; it needed some experienced and skilled computer designers to flesh out the functional sketches being produced by the SIS engineers, such as Ray Bowman and Dwight Ashley. Again the SIS went to the National Bureau of Standards. Since Lubkin was there and since he had already put so much work into the design of the REVAC, it seemed reasonable to expect cooperation and a detail design within a short time. The NBS was reluctant to take on any more responsibilities, however. They had their own crisis to deal with. But after emphasizing that it was too busy to build a machine for the agency, in early fall 1948 the NBS offered to take on the design task for $150,000.[72] That seemed a bit too expensive. That was the amount that Reeves was to have charged for a delivered machine, but the SIS's options were limited. So, even though the NBS

was indicating that it was going to provide the SIS only with something close to a copy of the very simplified delay-line SEAC, it was rushing to build for itself, the offer was accepted.[73]

(S) To prepare for the arrival of the design, a team of engineers was formed and programming classes were begun. Snyder felt that his ordeal was finally over. The project seemed about ready to contribute operational results; there was great enthusiasm. The new programmers went beyond their lessons and began to write routines to attack [redacted]. Soon the mathematicians at the SIS were swept up in the excitement over the about-to-appear computer. Dick Liebler and Hugh Gingerich even devised a new class of attacks [redacted] ones that could be done only on a high-speed digital machine.[74]

(S) Unfortunately, the plans did not come from the National Bureau of Standards on schedule. Its crew was so busy with the bureau's own computer problems and those of the contractors it was supervising for other government agencies, that all Snyder got from them were promises to hurry. The situation got worse when Lubkin decided that Standards was not for him. That complicated an already difficult situation because those who took over his tasks favored a much simpler machine than the SIS was expecting.[75]

(S) There were meetings, but they were disappointing. The NBS was willing to promise a design for only a very bare bones device. And they could not guarantee when those plans would be ready for the engineers and programmers who waited for them at Arlington Hall.

(S//SI) Everyone at the SIS grew more frustrated. The frustration was compounded by growing ambitions. As the SIS engineers and programmers gained more experience, they thought of many ways to make "Abner" an effective cryptanalytic device.[76] But it would have to be a much more complex machine than the one proposed by the NBS and a more intricate one than Atlas. It was also clear that Abner was going to cost the agency much more than had been imagined.

(U) So Much for Simplicity

(TS//SI) With young men like Ray Bowman in the lead, ideas were put forward to change Abner into something more like a Sled than a simple EDVAC. He and others showed how basic cryptanalytic functions could be turned into circuits that, they thought, should become an integral part of Abner. Some fifteen special "instructions" were drawn as circuit diagrams and were shown to the few men at the NBS who had security clearances.[77] Their reaction was not positive; they felt they were being asked to do much more than was initially agreed upon. And even when a compromise was suggested, that the special functions such as a two-message offset instruction be put into a separate box that the SIS would design and build, agreements could not be reached. Even such a box, the NBS engineers argued, would demand too many complex circuits in the main computer.[78] There was a stand-off, a quiet one, but it was clear the two agencies had reached an impasse in late 1949.[79]

(U) Another critical decision had to be made. Should Abner be abandoned at least until the uncontrollable NBS decided to devote serious attention to it? Or, since the SIS and OP-20-G had been merged into the new Armed Forces Security Agency, should everyone be required to wait for the completion of the further advanced Atlas project? It did not take too long for the administrators to make a courageous decision. They allowed the Arlington Hall engineers to go ahead and design and build their own machine.

(U) That seemed a reasonable decision because so much agency effort had already gone into Abner and because the computer manufacturers, including IBM, continued to back away from taking contracts for machines. And the agency knew that smaller companies, such as Technitrol, could be counted on for components.

They were already helping with the special-purpose machines the agency was considering.

(U) Abner's Not Quite Best Friend

~~(S)~~ The decision to build Abner received an unexpected justification in mid-1950. During the first months of the Korean War, when the American military was unable to show that it could effectively police the world, it was at least suspected that the American navy's callsigns were inadequate. New ones had to be generated to protect the fleet and its messages. There was a critical need to run "involuntary matrices" to ensure randomness. That was a demanding job and one that Solomon Kullback, the agency's research director, had given the highest priority.

~~(S)~~ In summer 1950 a survey was made of the possibility of running the matrices on IBM tabulator equipment. The result was very disappointing. Then a suggestion was made that perhaps the relay analog of the soon-to-be-delivered Atlas could be used. Some of the mathematicians explored the possibility and then, perhaps prompted by Sam Snyder, looked at the possibility of using the NBS's new SEAC. It was the interim computer the NBS had decided to build on its own in 1948. Constructed in two years, it was a bare bones version of the EDVAC, but it worked.

~~(S)~~ Required to estimate whether or not it would be worthwhile to ask the NBS if SEAC could be used on the callsign problem, the SIS's programmers made pencil and paper calculations of the power of various alternatives.

~~(S)~~ Their estimates gave the following times for gaining a completed and satisfactory matrix.[80]

By Hand	By Relay	By Atlas (Drum)	By Seac (Delay)
5 hours	4.5 hours	3 minutes	20 seconds

~~(S)~~ The results seemed unambiguous. The electronic machines were undoubtedly faster than hand or relay process, and most importantly, the delay-line machines, such as SEAC, were orders faster than the ones with drum memory. That finding was support for Abner's cause and for the NBS's SEAC. As a result, Sam Snyder went to the National Bureau of Standards and gained permission to use the SEAC for the matrix problem.[81] Unfortunately, the first hands-on experience with an electronic computer was very disappointing. If there had not been so much invested in Abner, the experience with SEAC might have led to abandoning Abner.

~~(S)~~ A program for computing the matrices on SEAC was written in some two months, not an easy task in the early 1950s. Then in September some SEAC run time was allocated to the agency – but on weekends and nights and at $24.00 an hour, not an inconsiderable sum at the time. The expense had not been foreseen, nor had the SEAC's temper. SEAC soon taught the analysts that there was a vast difference between the theoretical internal speed of computers and their real operating time.

~~(S)~~ The first post-midnight session on SEAC took twelve very discouraging hours. Despite all the care that had been taken, the result had to be abandoned because of repeated machine errors. A few days later some 200 matrices were created, but then errors crept in again. After just two hours of successful runs, it was decided that a checking program should be written so that all results could be verified.

~~(S)~~ The frustrations continued. In mid-September, SEAC worked only four out of sixteen hours, and the results that were obtained were put into question because of the quirky behavior of the computer.

~~(S)~~ On September 19 SEAC did more than follow the laws of early computer technology (to rarely work); it committed a serious political blunder. The agency had reserved a precious twelve-hour chunk of time, between noon and

midnight, because some official had decided it was appropriate that the great secret of SEAC and the future Abner be revealed to the SIGINT community. Some twenty-five people were invited to watch the NBS's machine in action. Sam Snyder was in charge of running SEAC.

~~(S)~~ Much to Snyder's embarrassment, of the entire twelve hours "0 hours were productive." He was so angry that he wrote in a report, "In the future, when trouble with SEAC develops, no more attempts will be made by personnel of this Section to find the cause of the difficulty."[82]

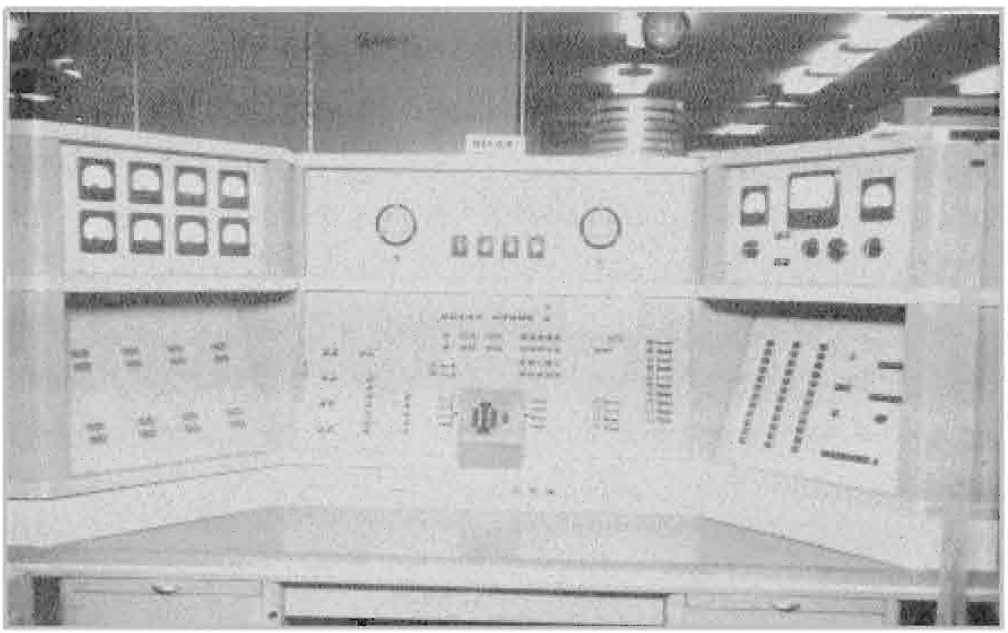
~~(S)~~ Despite the anger and the problems that continued to be encountered with SEAC runs, it was decided to keep the matrices that had been produced.

(U) Abner by Inertia

~~(C)~~ While SEAC was refusing to give its best, the crew at Arlington Hall got to work building Abner, not telling the NBS exactly what they were doing. They worked so quickly and quietly that when the NBS representatives finally appeared at Arlington Hall with some sketches, they were shown, with much ceremony, the completed SIS design.[83]

~~(C)~~ That design had become very ambitious, going far beyond the NBS's SEAC.[84] The basic EDVAC approach was maintained, but many special functions were included. Abner became much more of a crypto-computer than Atlas.

~~(S)~~ Three groups of special instructions were built into Abner. The first made encipher/decipher tasks easier. A programmer could call for addition without carrying and specify which number base, ranging from two to greater than thirty-two. Abner could very quickly run key against text, imitating many of the previous special-purpose machines. The second group of commands made Abner a more efficient processor of streams of data, allowing easy transfer of blocks of information and repetition of a series of instructions until a task was completed. The third



~~(U)~~ Abner

group contained instructions that made Abner a powerful "comparator." Using the one Swish instruction, a programmer could tell Abner to[85]

Pass two variable length streams of five-bit characters from memory to the control of the analytic unit of the machine;

Compare groups of varied sizes (one to sixty-three characters) for coincidences;

Store the count in a specified location;

Offset one data stream to prepare it for another round of coincidence testing.

~~(S)~~ As significant for the evolution of the computer, there were courageous attempts to give Abner what most other computers of the time did not have, a range of powerful input and output devices. A big gamble was taken: the new plastic magnetic tapes could be made to function. Connections for six of the Raytheon drives were installed. A punched tape reader was attached as well. Not as exciting, but more important from an operational standpoint, an IBM collator was to be used for card input and a modified IBM card punch for output.[86] There were many software developments. By the time Abner was completed in April 1952, the SIS programmers had written a wide range of operational routines.[87]

(U) Abner's Bad Temper

~~(S)~~ But it was some two years between the time the SIS engineers decided to detail their own Abner and its start-up as an operational machine. And its cost climbed to twice the original estimate of $300,000. Even then, it was just, as one engineer put it, an "experimental model."

~~(S)~~ And it was almost as temperamental as SEAC. Its special functions made it a bit too complicated to maintain (it had 1,500 tubes and 25,000 diodes), the PO devices and their interfaces had many troublesome moments, and the more than 100 delay lines needed constant fine-tuning.[88]

~~(S)~~ The limitations of the 1952 Abner were obvious. But its problems did not cause the SIS to abandon computers. A contract was let to have the Technitrol company in Philadelphia build a new version. It arrived in mid-1955, cost approximately $1,000,000, and like Abner I, had an operational price tag of almost the same amount.

~~(S)~~ It was known in the 1940s that operators, cooling systems and repairs would make computers very expensive to maintain. But there was another cost that was not anticipated: programming. Abner I needed $130,000 a year worth of programmer time plus additional amounts for special projects.[89]

~~(S//SI)~~ Abner had another expense: a clone. In 1950 it was decided that Abner should have the same kind of relay-circuit cousin that had been quickly built to train Atlas's programmers. When the construction of "Baker" began, no one expected it to take two years to complete, nor to become the size of a room. Nor did anyone foresee that the relay version of Abner would be much less reliable than the new electronic machine. Baker proved so difficult that it never kept its promise to be an inexpensive training and program-debugging aid to Abner.[90]

~~(S)~~ Despite Baker's failings, many innovative programs were written for Abner. They spanned all cryptanalytic attacks as well as data processing tasks. The list of programs is impressive, especially when it is realized they were written in an era when programming was something of a black art. For many years programs had to be written in the 0's and 1's the computer recognized, and even when "higher" level languages appeared, programming and debugging were energy-draining and emotion-laden exercises.

~~(TS)~~ Abner was used to "diarize" as well as to analyze wired rotor systems. But perhaps its most

useful program was Stethoscope. Written very early in the history of programming, it became a classic. Stethoscope very efficiently applied all the major statistical attacks against cipher text in unknown systems.[91] The routines proved so valuable, and the potentials of expanding Stethoscope seemed so great, that a very courageous step was taken by the SIS programmers. They decided to write one of the very first compilers. Bill Cherry played a key role in the LULU project to create software that would allow programmers to very easily compose and correct programs that called many subroutines. With the help of LULU and its follow-on, Stethoscope became the much more powerful general cryptanalytic program, Supersteth.

(U) And Then Came ...

(~~TS//SI~~) It had taken many years and millions of dollars to prove that a universal computer could be a valuable statistical tool, however. And there were some critical moments when it seemed that a special architecture would be the wisest choice for the SIGINT agencies. In fact, one of the gravest crises in the history of American cryptanalysis shifted attention to such alternatives and highlighted the weaknesses of the new general-purpose computers. "Black Friday" of 1948 saw a return to a faith in special-purpose devices; they seemed the only way to overcome Soviet systems that were making the Enigma and even Tunny look simple. But "Black Friday" also showed how far the computer had to go before it could replace the old reliable data processors, the tabulators.

Notes

1. (U) NSA, OP-20-G, J.T. Pendergrass, "Cryptanalytic Use of High-Speed Digital Computing Machines," 1946. NSA, Samuel S. Snyder "Influence of United States Cryptologic Organizations on the Digital Computer Industry," dates the beginning of Goldberg to 1947 perhaps on the basis of the contract for the machine rather than on the date of start of the explorations for a universal scanning machine.

2. (U) Interview with Philip J. Bochicchio, July 1994, On Rachman, (~~TS//SI~~) NSA CCH Series XII Z, and CCH Computer History Box, OP-20-G "War Diary Reports: March 1, 1943 - May 31, 1948," August 1945.

3. (U) Anthony Ralston (ed.), *Encyclopedia of Computer Science* (New York: Van Norstrand Reinhold, 1976), 482, 1459.

4. (~~C~~) NSA CCH Series XII Z and XI K, Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, I-2.

5. (U) On the postwar Selector project and its tie to Bush and "G's" ERA, see Colin Burke, *Information and Secrecy: Vannevar Bush, Ultra, and the Other Memex* (Metuchen, N. J.: The Scarecrow Press, 1994.) On Bush and Eisenhower, see Thomas Johnson, *American Cryptology during the Cold War: Book I*, Ft. George Meade, MD: NSA Center for Cryptologic History, 1995.

6. (U) Colin Burke, *Information and Secrecy: Vannevar Bush, Ultra, and the Other Memex*, (Metuchen, N. J.: The Scarecrow Press, 1994), Ch. 14.

7. (U) NSA, OP-20-G, J. T. Pendergrass, "Cryptanalytic Use of High-Speed Digital Computing Machines," 1946. (U) NSA, Samuel S. Snyder, "Influence of United States Cryptologic Organizations on the Digital Computer Industry" dates the beginning of Goldberg to 1947, perhaps on the basis of the date of the contract for the machine rather than on the date of the start of the explorations for a universal scanning machine.

8. (~~TS//SI~~) NSA CCH Series XII Z, H. H. Campaigne, "Reading TUNNY," *NSA Technical Journal*, (Fall 1962). (~~TS//SI~~) A fascinating source for the history of OP-20-G are Campaigne's War Diaries, 1943-1945.

9. (U) NSA CCH Series XI K, Snyder, Box 8, OP-20-G4, "Report on conference held at Navy Department 15 May 1946. "Survey of large scale automatic computing machines, given by J. von Neumann," Howard Campaigne, 16 May 1946.

10. (U) Martin Campbell-Kelly and Michael R, Williams (ed.), The Moore School Lectures: *Theory and Techniques for the Design of Electronic Digital Computers* (Cambridge, Mass.: MIT Press, 1985).

11. (~~TS~~) NSA CCH Series XII Z, NSASAB, "Historical Study, Lightning-Freehand," circa 1963.

(TS//SI) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase III: Third Addition," 1 November 1956. (U) "Remarks at the Dedication of John von Neumann Hall," *NSA Technical Journal*, VI (Winter 1961): 1. (TS) NSA CCH Series XII Z, Morris Pomerantz and Lawrence A. Sames, "Data Distribution Network for the TABLON Mass Storage System," circa 1970.

12. (TS) NSA CCH Series XII Z, Lt. Cdr. J.T. Pendergrass, "High Speed Digital Computing Machines, Cryptanalytic Uses of," 15 October, 1946. (TS//SI) NSA CCH Series XII Z, H. H. Campaigne and J.T. Pendergrass, "Second Report on Cryptanalytic Use of High Speed Digital Computing Machines," OP-20-L, 18 December 1946. Campaigne wrote one of the programs in the first report, but that has not been remembered. He was listed as the joint author in the second one.

13. (U) It is important to note that the reports did not claim that the machine was an efficient data processor. All of the many examples were cryptanalytic ones, and processing-heavy methods such as T/A were not mentioned.

14. (TS) NSA CCH Series XII Z, Lt. Cdr. J.T. Pendergrass, "High Speed Digital Computing Machines, Cryptanalytic Uses of," 15 October 1946, 1.

15. (U) von Neumann had, at first, favored a four-address system, then changed to the one-address idea because it would be better suited to mathematical machines. Pendergrass thought that the one-address was best for crypto-work. In contrast the SIS computer pioneers favored the four-address system.

16. (TS//SI) NSA CCH Series XII Z, H. H. Campaigne and J.T. Pendergrass, "Second Report on Cryptanalytic Use of High Speed Digital Computing Machines," OP-20-L, 18 December 1946. The available copy of this report did not contain the Mercury program, but it was cited as part of the report on page 1.

17. (S) NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," "Status of Digital Computers, November 1946."

18. (S) NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," "Status of Digital Computers, 20 January 1947."

19. (S) He included Alan Turing's work.

20. (S) NSA CCH Series XII Z, Ann M. Ford, "The Birth of Atlas 1, *NSA Technical Journal*, XVIII (Winter 1973): 53.

21. (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on RAM Panel Meetings," notes on the 13 November 1946 meeting clearly show that the digital computer was seen as a practical cryptanalytic tool, not just a research machine.

22. (S) NSA AHA ACC-32685, folder, "Atlas Computer Correspondence," "Memorandum for Research Division and Section Heads," 23 January 1947.

23. (S) NSA CCH Series XII Z, Ann M. Ford, "The Birth of Atlas I," *NSA Technical Journal*, XVIII (Winter 1973): 53.

24. (U) On the interesting Aiken designs, Michael R. Williams, *A History of Computing Technology*, (Englewood Cliffs, N.J: Prentice-Hall, 1985).

25. (S) NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," "Estimated Delivery to NCML," circa 1951. Atlas was given an AA priority; that was higher than Goldberg's, at least during the late 1940s.

26. (S) NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," CNO to Chief of Bureau of Ships, 23 May 1947."

27. (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," notes of meeting of 22 November 1946, page 2, shows "G" believed RCA and the NBS were soon going to build a computer.

28. (TS//SI) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948, 10. (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," report of 14 November 1946 meeting.

29. (C) NSA CCH XI K, Box 8, Snyder, "An Evaluation of NSA's Atlas I," Ann Ford H12, 8 November 1970. March seems to have been a critical month in Atlas history. "G" decided to build its own machine because no vendor seemed willing to do so.

30. (S) NSA AHA ACC 32685, folder,"Atlas Computer Correspondence," "Summary of Conference on Task 13 (Atlas)," 19 and 21 August 1947.

31. (S) NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," "Second Revision of

Military Characteristics of the Analytic Computer (ATLAS)," 6 July 1948.

32. (U) W. W. Stifler (ed.), *High-Speed Computing Devices*, (New York: McGraw-Hill Book Company, 1950), 370.

33. (U) Apparently, the proposed MIT tube was quite like Wilkes'.

34. (U) The result, a Selectron, was not available until the early 1950s. It was used in one von Neumann type of computer, but never afterward. One of the many leaps in computer technology had made it a technological dinosaur.

35. (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949," Meeting of April 15, 1947.

36. (~~TS//SI~~) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948. Electrostatic storage had also been planned for Goldberg.

37. (~~TS//SI~~) NSA AHA ACC 11112, "Interim Report on Computer Research," circa 1948.

38. (U) On microfilm, (~~S~~) NSA CCH Series XI K, Sam Snyder, Box 12, "Analytic Machinery Principles," September 1949. On Atlas' drum, (~~TS~~) NSA AHA ACC 13643 "Atlas I. "

39. (U) Philip J. Bochicchio has recounted his experiences with the earliest magnetic drums. He stated that in 1945, after gaining access to captured German equipment, he created a primitive drum that was taken by Joe Eachus to ERA. That inspired ERA, stated Mr. Bochicchio.

40. (~~TS~~) NSA CCH Series XII Z, "Report of the Second Computer Study Group," as in *NSA Technical Journal*, XIX (Winter 1974): 21-61. (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949."

41. (~~S~~) There were problems with the Goldberg drums, and they were run at a low 240 rpm. (S) NSA CCH Series XII Z, "Goldberg Progress Reports," 30 December 1947 through 10 April 1951.

42. (~~TS//SI~~) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948. (~~TS~~) NSA AHA 36746, Engineering Research Associates, Inc., "Proposal for An Electronic Rotor Program," 19 December 1946. (~~TS~~) NSA AHA ACC 8252, OP-20-G, "Communications Intelligence Research Plans, 1948," 7 April 1947. (~~TS//SI~~) NSA CCH Series XII Z, "Joint Long Term Program (Old Planning Material, 1948-1949) compiled by Doug Hogan. (~~S~~) NSA AHA ACC 32685 "Summary of Conference on Task 13 (Atlas)," 19 and 21 August 1947.

43. (~~S~~) J. J. Eachus, "SIGMAGE Threshold Control," 2 July 1946. (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949." Monogram's proposed allocations for computer research for 1949 were quite generous: $1,000,000 for general-purpose computer work and $1,000,000 for SPD and related electronic work. (~~S~~) NSA CCH Series XII Z, BuShips, "Specifications Sled Navy Models CXOA and CXNQ Block Diagrams," 1 October 1948, Monogram's 1948 budget was cut in half by the bureau, (~~TS~~) NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949," entry for 21 November 1947.

44. (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings," notes on 27 July 1948 meeting. (~~S~~) NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," "Estimated Delivery to NCML," circa 1951. (U) Hagley Museum and Library, Accession 1901, Yuter Papers, May 20, 1947, ERA Tompkins Report on Atlas, "shift Goldberg-Demon men to project." (U) Erwin Tomash, "The Start of an ERA: Engineering Research Associates, Inc., 1946-1955," in N. Metropolis, et al., (ed.), *A History of Computing in the Twentieth Century* (New York: Academic Press, 1980), 485-496.

45. (~~S~~) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 9.

46. (~~C~~) NSA CCH XI K, Box 8, Snyder, "An Evaluation of NSA's Atlas I," Ann Ford H12, 8 November 1970.

47. (~~C~~) NSA AHA ACC 32685 "First Endorsement on ERA. Inc..... 23 February 1951. (U) Samuel S. Snyder "Influence of United States Cryptologic Organizations on the Digital Computer Industry," *The Journal of Systems and Software*, 1 (1979): 90-91. (U) Hagley Museum and Library, Accession 1901, Yuter Papers: Engineering Research Associates, October 9, 1946, Meeting on NBS computer plans, "Summary of Computing Conferences"; Tompkins to

Norris, October 19, 1946, "Computing Business"; December 1946, "Reports on OP-20-G Projects and Atlas Computer"; and Goldberg Report, June 27, 1947.

48. ~~(S//SI)~~ NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 7. ~~(R)~~ NSA AHA ACC 32685, "Atlas I" circa 1952.

49. ~~(S//SI)~~ NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 7.

50. ~~(TS)~~ NSA AHA 6851 Atlas Analytic Computer, "Military Characteristics of the Analytic Computer (Atlas)," June 1947. NSA AHA ACC 13643, "Memoranda on Electronic Computers, Atlas I," circa 1952. ~~(S)~~ NSA AHA ACC 32685 "AFSA-351 Atlas Programming Bulletin No 1," February 1951.

51. ~~(C)~~ NSA CCH XI K, Box 8, Snyder, "An Evaluation of NSA's Atlas I," Ann Ford H12, 8 November 1970, 8.

52. ~~(S//SI)~~ NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 8.

53. ~~(TS)~~ NSA CCH Series XII Z, "Report of the Second Computer Study Group," as in *NSA Technical Journal* XIX (Winter 1974): 21-61. ~~(C)~~ NSA CCH XI K, Box 8, Snyder, "An Evaluation of NSA's Atlas I," Ann Ford H12, 8 November 1970.

54. ~~(S)~~ NSA AHA ACC 32685, folder, "Atlas Computer Correspondence," CNO to Chief of Bureau of Ships, 23 May 1947.

55. ~~(S)~~ NSA CCH Series XI K Box 8, Snyder, "Yearly Cost of Representative NSA Machines," May 1955.

56. ~~(S)~~ NSA Technical Literature Series Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 11. ~~(TS//SI)~~ NSA AHA ACC 30851, "Historical Notes on Computers at NSA," suggests that metallic tapes were planned.

57. (U) On the naming of the machine, ~~(S//SI)~~ NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982. The most complete survey of Abner is ~~(C)~~ NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979. See also, (U) Samuel S. Snyder, "Abner: The ASA Computer, Part I: Design," *NSA Technical Journal*, XXV No. 2 (Spring, 1980): 49. (U) Samuel S. Snyder, *History of NSA General Purpose Electronic Digital Computers*, 1964.

58. (U) The electronic group had some sixty employees in 1946.

59. ~~(C)~~ NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S, Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, I-6.

60. ~~(S//SI)~~ NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 70.

61. ~~(C)~~ NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, I-10. ~~(TS)~~ NSA CCH Series XI K, S. Snyder, Box 8, Mary Neely Roseboro, CSGAS-76c, "Commentary on the Pendergrass Report," 15 October 1947.

62. ~~(S//SI)~~ NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 121.

63. (U) See also, R. M. Bloch et al., "Logical Design of the Raytheon Computer," Mathematical Tables and Other Aids to Computation, 3 (October 1948): 286.

64. ~~(S//SI)~~ NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 121. The UNIVAC design had a serious shortcoming for cryptanalytic work. The standard UNIVAC had a decimal (BCD) organization. That meant it was not suited to handle many crypto-tasks. Especially important were the new targets of the crypto-groups, the baudot-based binary systems. The analysis of such systems demanded bit-by-bit testing, as did many of the older targets. ~~(S//SI)~~ NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 13.

65. ~~(TS)~~ NSA CCH Series XII X-MPRO, U.S. Cryptanalytic Research and Development Committee, "Joint Long Term Program for Research and Development in the Field of Cryptanalytic Equipment," 21 July 1948. (S) NSA CCH Series XI K

Box 8, Sam Snyder, "Evaluation of Computers as Crypt Aids," 7 September 1948.

66. (U) Mina Rees, "The Mathematical Sciences and World War II, *American Mathematical Monthly*, 87 (1980): 607-621. William Aspray and Michael Gunderloy, "Early Computing and Numerical Analysis at the National Bureau of Standards," *Annals of the History of Computing*, 11 (1989): 3-11. John Todd, "John Hamilton Curtiss, 1909-1977," *Annals of the History of Computing*, 2 (1980): 104-9. R. Cochrane, *Measures for Progress: A History of the National Bureau of Standards* (Washington: G. P. O., 1966). Samuel S. Snyder, "Abner: The ASA Computer, Part 1: Design," *NSA Technical Journal*, 25 (1980): 49.

67. (S//SI) NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 13. (C) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, I-13.

68. (C) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S, Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, I-13

69. (S//SI) NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 12. Raytheon also chose a more data-oriented design with four addresses for its RAYDAC.

70. (TS) NSA CCH Series XI, Snyder, Box 8, folder, "Snyder Computer Trips, 1947-1951." (C) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, I-14.

71. (U) James W. Cortada, *Historical Dictionary of Data Processing: Biographies* (New York: Greenwood Press, 1987), 64.

72. (U) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, 1-15.

73. (U) Samuel S. Snyder, "Abner: The ASA Computer, Part I: Design," *NSA Technical Journal*, 25 (1980): 49. Samuel S. Snyder, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 15. (C) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S, Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, II-3.

74. (S) NSA CCH Series XII Z, H. F. Gingerich, R. A. Leibler, "Hagelin Crib D Dragging on a High Speed Automatic Computing Machine," 26 August 1949. (S) NSA CCH Series XI K Box 8, Sam Snyder, "Evaluation of Computers as Crypt Aids," 7 September 1948.

75. (U) Samuel S. Snyder, "Influence of United States Cryptologic Organizations on the Digital Computer Industry," *The Journal of Systems and Software*, 1 (1979): 92.

76. (S//SI) NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers* by Samuel S. Snyder, 1964, 14.

77. (S//SI) NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 15, gives a full list of the special functions including the "Swish," which was "the logical equivalent of a complete high-speed comparator." The proposed special function of Abner found its way into the later Harvest machine.

78. (TS) NSA AHA ACC 10842, Ray L. Bowman, "Engineering Diary," circa 1945-1950. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982.

79. (C) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, II-15. The security clearance problem seems to have, again, complicated matters. It made communications difficult. The NBS faced severe problems because of "loyalty" questions in the early 1950s.

80. (S) NSA CCH Series XII Z, AFSA-32, Marvine Bass, "On Methods and Speed of Construction of Involuntary Matrices," August 1950.

81. (S) NSA CCH Series XI K, Snyder Box 10, "Extracts from AFSA-351D Weekly Reports re Seac Production."

82. (S) NSA CCH Series XI K, Snyder Box 10, "Extracts from AFSA-351D Weekly Reports re Seac Production."

83. (C) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, III-19.

84. (~~S~~) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, 1-2.

85. (~~S~~) NSA Technical Literature Series, Monograph No. 2, Samuel S. Snyder, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 16.

86. (~~S~~) A useful personal insight into Abner is Russell Chauvenet, "Early Days in NSA Computing," *Cryptolog*, August 1977: 8-10.

87. (~~S~~) NSA Technical Literature Series Monograph No. 2, Samuel S. Snyder, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 17. Abner was ready for its checkout phase in September 1951. All its instructions were accepted in April 1952.

88. (~~C~~) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, IV-14. (U) NSA CCH Series XII Z, to *Cryptolog* editor, by R. L. Bernard, "Comments on Abner," 18 January 1978.

89. (~~S~~) NSA CCH Series XI K Box 8, Snyder, "Yearly Cost of Representative NSA Machines," May 1955.

90. (~~S//SI~~) NSA CCH Series XII Z, NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, by Samuel S. Snyder, 1964, 18.

91. (~~C~~) NSA CCH Series XII Z and XI K Snyder, Box 9, Samuel S. Snyder, "And Then There Were Two, the Abner Story," Fourth Draft, December 1979, IV-8. (TS) NSA CCH Series XI K, Snyder, Box 16, List of Operational Abner Programs.

Chapter 9

(U) Wandering into Trouble

(U) A Cryptanalytic Future

~~(TS)~~ Although OP-20-G and the SIS were frustrated by the delays in their Atlas and Abner computer projects, 1948 began as a year of continued triumph for American communications intelligence. The cryptologic systems of the major powers were being read, and COMINT seemed about to supply America's leaders with the type of high-level information that had won "G" and the SIS so many accolades in World War II.

~~(TS)~~ Most of Stanford C. Hooper's dreams seemed to have been realized. The army and navy COMINT organizations had some professional mathematicians, they were starting vibrant new RAM programs, and they even had "scientific" advisory boards. The future of advanced cryptanalysis was bright, as was the future of American intelligence in general.

~~(TS)~~ Most important, the Cold War, it seemed, was to be a cryptanalytic one. A few foreign systems carrying high-level messages would yield to mathematics and computers and provide the kind of information needed to predict and, perhaps, counter the actions of the political and military leaders of all the important nations. There was even cryptanalytic progress against internal enemies. Old diplomatic messages were giving what was needed to find and break up Soviet espionage rings within the United States. There was hope that further works would lead to entries into all current Eastern bloc diplomatic and clandestine systems.

~~(TS)~~ Cryptanalytic success would not be expensive. Direction finding as well as the very labor-intensive traffic and plain language analyses would play secondary roles. America's COMINT agencies would not have to build a costly communications system to speed massive amounts of data to processing centers because high-level cryptanalysis provided lead time. Cracking important systems would give insight into the grand intentions of the world's political and military leaders, and that would give American policy makers time to formulate measured responses.

~~(TS)~~ The belief that cryptanalysis would be the heart of SIGINT's future was reflected in the kind of machines the army and navy developed during the immediate postwar years. They focused on general-purpose computers for cryptanalysis, not ones for massive data processing.

(U) The Worst of Times

~~(TS//SI)~~ Then the heroic cryptanalytic assumption was suddenly undermined! In spring 1948 the SIGINT agencies had to rethink their purpose and place in America's intelligence establishment. The Americans and their intelligence partner, the British, were being locked out of the world's most important code and cipher systems just as the Cold War became dangerous. Three years after the end of the war, the Soviets closed down their old high-level systems and replaced them with ciphers that could not be penetrated. Soon the Chinese revised their superencryptions, making them quite sturdy. Even the [redacted] strengthened their machines and procedures.

~~(TS//SI)~~ A series of very significant intelligence failures came after the cryptanalytic blackout. That put American SIGINT's future in jeopardy. The Soviets' A-Bomb, the Berlin Blockade, the forming of the satellite bloc in Eastern Europe, the fall of China, and the Korean War were not predicted.

(TS) As the Soviets increased their strategic military capabilities, the situation became critical. U.S. leaders demanded another Ultra and Magic. But the new organizations created to coordinate COMINT, the Armed Forces Security Agency (AFSA) and then the National Security Agency (NSA), were unable to replay World War II's COMINT history. Their cryptanalysts faced challenges much, much more difficult than Purple or the Enigma. The new code and cipher systems were so strong that it seemed that Hooper's faith in mathematics, science, and computers had been misplaced.

(TS//SI) The worth of SIGINT, especially cryptanalysis, came into question by the early 1950s. Many came to believe that cryptology had improved so much that cryptanalysis was a lost cause. The situation grew threatening: NSA was almost confined to performing menial intelligence tasks as the Central Intelligence Agency used a new techno-miracle, the U2 and its amazing cameras, to physically penetrate Soviet Russia.[1]

(TS//SI) Even those who continued to believe that another Ultra might emerge lost faith in the National Security Agency and its ability to develop its own techno-miracles. As a result, through much of the 1950s and 1960s, there were initiatives demanding the creation of an alternative relationship between science and SIGINT. America seemed poised to give a new generation of the likes of Vannevar Bush and John von Neumann enormous amounts of money and complete power over cryptanalytic research and policy. The United States came close to establishing a Manhattan Project for the cryptanalysis of Soviet systems, one which was to be staffed and led by academics, not professional codebreakers.[2]

(TS//SI) The intransigence of the Soviets' systems also had consequences for computer policy. On one hand, as NSA was forced to rely upon noncryptanalytic sources for its "intelligence," the Agency became as much or more a data processing center than a "cryptanalytic" center.[3] That caused NSA to search for high-speed substitutes for the best data processors of the era, tabulating equipment.

(TS//SI) Those who kept their faith in the powers of mathematical cryptanalysis sought a different type of computer, a super-number-cruncher. At the same time, more practical cryptanalysts began a search for special-purpose computers (SPDs), ones so fast that even brute force cryptanalytic attacks would allow identification of hoped-for weaknesses of the new machines of the Russians and their allies.

(TS//SI) The search for "busts" turned out to be a formidable challenge with a strange technological twist. Identifying "bust" conditions was demanding, but putting what was found to use was a greater and more complex chore. Because the "busts" did not produce statements of intentions, only a new type of automated intelligence "factory" could turn the chaos of millions of "small facts" into valuable information.

(S) Although the resulting emphasis on automated data processing brought NSA's computer needs closer to those of the private sector, the Agency could not rely upon the market place to supply what it needed. Whether the requirement was for analytic or data processing devices, NSA had to do much more than select hardware from the shelves of computer manufacturers.

(U) A computer industry had begun to emerge in the 1950s, and it matured in the next decade, but it was not meeting NSA's needs. Even the giant and wealthy IBM was unwilling to provide what NSA required without a great deal of coaxing. As a result, NSA had to "interfere" in the marketplace.

(U) No permanent and satisfactory relationship between the corporations and SIGINT was created, however. NSA functioned in an unpredictable and many times uncontrollable world.

The computer industry was so unstable that "G's" captive corporation, ERA, was saved only by the willingness of a larger corporation to absorb it. Then politics forced an end to the special relationship with it that Wenger had worked so hard to establish.

~~(S)~~ NSA was left adrift. It could not afford its own computer manufacturing facilities, and it did not have a cooperative and permanent corporate partner.

(~~TS//SI~~) That made it very difficult for the Agency during the mid-1950s when it attempted to overcome the technological advantage of Soviet cryptology. Based on an intense faith that new machines would work cryptanalytic and data processing miracles, NSA became involved in many projects to create new generations of computer technology.

~~(S)~~ Those projects were not always successful. Hopes were often far ahead of technology and of the organizational and research abilities in the computer industry. In several instances the incompatibility of NSA's technological needs and those of the market place led the Agency's contractors astray. Delays, cost overruns, and less than perfect machines became familiar. At least one involvement, NOMAD, was an embarrassing failure.

(~~TS//SI~~) But the Cold War was so dependent upon intelligence gathering that NSA and its allies were forgiven for most of the shortfalls. The need for information, combined with the memory of Ultra and Magic, led to more than absolution for not up-to-the-mark research and development projects. Despite some earlier developmental missteps, NSA was granted massive support for its efforts to reenter the Soviets' higher level cryptosystems. In the mid-1950s, NSA became entangled in one of the great techno-gambles in American history: it shunted tens of millions of dollars to computer companies hoping to develop machines so fast that its demanding attacks on Soviet cipher systems would become practical.

(~~TS//SI~~) The attempts led to advances in computer technology and to new generations of special-purpose, architecturally innovative RAMs. The new RAMs (SPDs) were arguably the most powerful computers in the world. But even without the challenge of the Soviet enciphering machines, NSA would have become one of the major users and sponsors of computers. By the early 1960s, NSA's "basement" became one of the world's great computer data processing centers. But the drive to find a cryptanalytic solution to meet the Soviet threat was the driving force behind the Agency's great commitments to advancing computer technology.

(U) The Magic Continues

(~~TS//SI~~) The World War II alliance of the United States, England, and Soviet Russia was based on convenience, not basic trust. As a result, in midwar America and England began intercepting Soviet radio traffic and diplomatic telegraph messages. The end of the war saw an increase in the attention paid to the Soviets. Great Britain and the United States signed the historic BRUSA agreement for SIGINT cooperation and intensified their joint work on Soviet and related systems.[4]

(~~TS//SI~~) There was some astounding cryptanalytic progress, and by late 1946 there were indications that four of the most important Soviet civil and military systems could be exploited. There were also indications that its one-time-pad diplomatic and clandestine systems might be breached.

(~~TS//SI~~) The reach of the BRUSA successes was astounding. The British and Americans were breaking into not just one, but several different types of enciphering machines and systems. While a team at the SIS began its three decades-long Venona project on Soviet diplomatic/clan-

destine messages, the British and then the American cryptanalysts attacked the Russian Longfellow [redacted] the Coleridge [redacted]

~~(TS//SI)~~ There was hope that the greatest prize of all, the [redacted] machine, might soon be penetrated. No one was sure if it was a cousin of an Enigma or a Soviet version of the American ECM, but it seemed clear that [redacted] carried the type of messages that had gained such glory for World War II's cryptanalysis.

~~(TS//SI)~~ Devoting almost one-half of "G's" and the SIS's resources to the Soviet problem was both inescapable and wise.[7] The Venona work began to pay off. It was discovered, through endless rounds of tabulator processing, that during the war the Soviets had reused some of their one-time pads. Finding [redacted] led to many readable messages. As the names of atomic and other spies appeared from the decrypts of the mid-1940s messages, there was hope that a similar effort would allow the postwar Soviet diplomatic communications to be read.

~~(TS//SI)~~ But the Venona victories were not complete; only a percentage of intercepted Soviet traffic was decrypted, and "scientific" cryptanalysis played a limited role. Many of the penetrations came as a result of information provided by prisoners of war and documents and devices retrieved from Germany.[8] Others were the result of something less than pure cryptanalysis; in the 1940s the Soviets had yet to perfect their cryptosecurity procedures. But traditional cryptanalysis did contribute, and by 1947 exploitation was more the result of machine analysis rather than operator errors and procedural weaknesses.[9]

~~(TS//SI)~~ There were more successes. The Americans joined the British codebreakers in profitable attacks on a host of Soviet hand ciphers and code systems. And the ciphers of most other nations were vulnerable, especially those generated by [redacted]

~~(TS//SI)~~ In 1947-8 GC&CS, "G," and the SIS appeared to be able to conquer any target.[10] The codes of both Chinas were opening and those of all the minor nations of the world were penetrable. In addition, the attack against the [redacted] cryptosystems gave the United States a great deal of information about the Third World. [redacted] for much of their traffic. Somewhat later, Japan's reintroduction of the Purple machine to generate one-time pads for its diplomats proved quite useful to America's SIGINT monitors. And the nations that continued to use the Enigma gave some of Joseph Desch's Bombes a productive second life.[11]

~~(TS//SI)~~ At the same time, England and America were tapping the surge of Soviet plain language transmissions, reading commercial codes and ciphers, and using undecryptable messages for traffic analysis. By 1948 OP-20-G alone was intercepting more than 1,000,000 Soviet plain-language messages a year. Some of that material was quite valuable because, for example, Soviet military production and deployments could be inferred from the communications concerning industrial orders and military logistics.[12]

~~(TS//SI)~~ Plaintext analysis contributed much, but cipher breaking was the hallmark of "G" and the SIS during the first postwar years.

(U) At Last, the Electronic Bombe – Perhaps

~~(TS//SI)~~ In early 1948 the emerging command over the Soviet cipher systems was so promising that the Americans decided to invest in two innovative and large-scale, special-purpose electronic computers. They would exploit the penetrations into the important Soviet Longfellow [redacted] Their com-

bined price tag equaled the cost of one-fourth of OP-20-G's World War II Bombes.

~~(S)~~ A third of a million dollars was committed to Pluto, an electronic machine built by Sylvania, the Boston electronics firm that was helping with the construction of MIT's Whirlwind computer. Pluto used twenty six-foot by twenty-foot frames crammed with vacuum tubes. Those walls of tubes and circuits were needed to test regular and [redacted] Longfellow and other [redacted] devices. Pluto ran through 1,000,000 settings a minute and was so precious that only a handful of the most trusted code-breakers were informed of its existence.[13]

~~(TS//SI)~~ Much more ambitious was Hiawatha. In late 1947 electronic potentials finally came together with a cryptanalytic opportunity to force the release of massive funding for the long-sought Electronic Super Bombe. The elusive electronic matrix finally seemed ready, and at the same time enough had been learned about Longfellow to think that a bombe would allow continuous reading of its messages. A huge amount for the time, $1,000,000, was promised, and it was made clear that more would come if the development of the new and aptly named "Hiawatha" machine demanded it.

~~(TS//SI)~~ OP-20-G ordered its favored contractor, ERA, to put its best men to work. In March 1948 a team was formed and the long-awaited machine was begun. The attack on Longfellow was thought to be just a prelude to reading the rest of Russia's most valuable communications. The Cold War, it seemed, was to have its own Ultra.

~~(TS//SI)~~ Then, on April 11, 1948, the Soviets took Hiawatha's target off the air. The reaction in America was immediate. The huge electronic Hiawatha project at ERA was cancelled.[14] A score of small relay analogs of Longfellow became useless. Sylvania was told to complete Pluto, but it was turned to analyzing the [redacted] of sometimes-friendly nations.[15]

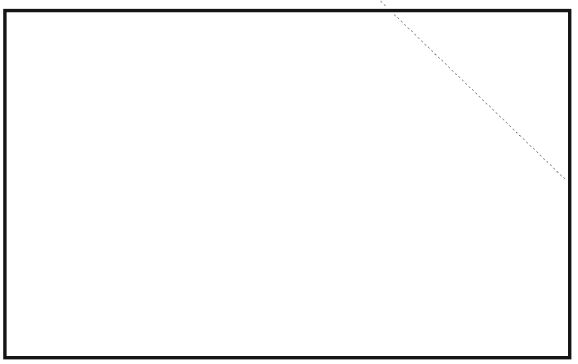
~~(TS//SI)~~ The bright young mathematician of World War II's OP-20-G who had remained on as one of the few civilians at "G," Howard Campaigne, was furious with the Americans as well as the Soviets. When he learned that ERA's electronic bombe project was terminated, he wrote:[16] "If we had complete coverage [of Longfellow] from the beginning [1943] we probably could have been reading their communications by 1945. If we had supported this by the analytic machinery recently planned, we could have broken out most of the available traffic. The entire story is one of 'too little too late'. This system was in use for five years, yet we were not ready to read it in quantity until it disappeared."

~~(TS//SI)~~ Campaigne would become distraught. Much, much worse was happening. Perhaps because of an American defector, by 1949 all of the four major Soviet cipher systems that the United States and England had penetrated were taken off the air.

~~(TS//SI~~) They were replaced by new machines, ones too fresh and too protected to be unraveled through operator errors or clandestine activities. There seemed little hope of a repeat of the 1930s when Japan sent messages on old and new systems at the same time or when a midnight visit to a consular office by the ONI could produce a code book or insights into highest level systems.

~~(TS//SI)~~ The Soviet problem was not the only frustration, nor the only danger to the survival of what became NSA. By late 1949 [redacted] began to tighten its cryptoprocedures, locking out the British and Americans. By 1952 [redacted] had done so much to protect its codes and ciphers that NSA worried that it would be permanently barred from some of the most important sources it had on developments in [redacted].[17] Even the Chinese Communists were replacing their simple additive and transposition codes. They began

borrowing much from the Soviets' rugged one-time-pad systems. The North Koreans soon followed their mentor's lead.[18]



(U) Without Magic and without Many Friends

~~(TS//SI)~~ The crypto crises of the late 1940s came when COMINT was losing many of its friends and its independence. Even before "Black Friday," when the Soviet systems were changed, there had been calls for reform, usually motivated by a search for efficiency. By the early 1950s NSA was alone, under scrutiny, and threatened.

~~(TS//SI)~~ Soon after World War II, the SIS and OP-20-G were ordered to cooperate on the allocation of targets and the design and purchase of machines. Then in a general cleansing of military inefficiencies, the army and navy SIGINT agencies were locked together in 1949 to become the Armed Forces Security Agency (AFSA). Unfortunately, the merger did not go well and caused many problems. Almost as soon as it was born, AFSA was criticized because it could not re-enter the high-level systems and, most significantly, because it missed predicting the outbreak of the Korean War! Combined with previous oversights, such as failing to spot the emergence of the Soviet atomic capability, the Korean oversight put centralized SIGINT in danger.

~~(TS//SI)~~ AFSA and American intelligence in general received a scathing review by the Brownell Committee as early as 1950. More than the organizational structure came under fire. Faith in cryptanalysis was plummeting, so much so that insiders later called the early 1950s the "Dark Ages of American Cryptanalysis."

~~(TS//SI)~~ The formation of the National Security Agency in 1952 did not reverse the cryptanalysts' fortunes. Results remained meager and SIGINT's reputation suffered. If there had been viable alternatives, such as penetration of Soviet systems by human agents, NSA might have become a minor player in the intelligence field. Necessity and a powerful director saved it. But the Agency was never secure in the 1950s.

~~(C)~~ Although NSA's tough and effective new leader, General Ralph Canine, hinted that NSA might soon be able to "listen into the conversations of the Polit Bureau," and was able to secure budgets that allocated $5,000,000 or more dollars a year for regular analytical equipment, NSA was not left to itself. [20]

~~(TS//SI)~~ A year after its birth, NSA was subjected to a series of threatening investigations by powerful review boards. As soon as one examination was concluded, another began. While some, such as the Hoover Commission, held that breaking the Soviet ciphers was of paramount importance, all the evaluations voiced a deep disappointment that an Ultra had not been re-created.

~~(TS//SI)~~ As a result, there were calls for a thorough overhaul of SIGINT. Even some of NSA's very best friends, such as William O. Baker, thought the Agency should be stripped of the responsibility of solving major cryptanalytic systems.

~~(TS//SI)~~ The SIGINTers had to prove their worth. Their only hope was for a technological and scientific "fix." Even if they had to continue to rely upon plaintext intercepts and T/A, new machines and methods were essential. Code and cipher breaking needed a technological revolu-

tion as well as mathematical breakthroughs. And NSA needed help to achieve both.

(U) Unfortunately, it had to pull itself up by its own bootstraps. The American computer industry was too immature to supply what was needed, and Big Science was paying little attention to cryptanalysis.

(U) The End of an ERA

(~~TS//SI~~) In the late 1940s, as the Soviets shut down their major systems and when American SIGINT critically needed technological and scientific help, one of "G's" most valuable allies, ERA, almost disappeared. Then, after ERA's rescue, it did not return to the role of the always ready and infinitely flexible partner that Hooper, Wenger, and Engstrom had envisioned.

(U) By as early as 1949, Engineering Research Associates (ERA) was experiencing internal problems and it was becoming a political target. The challenge of turning science into a business was difficult for the company. In St. Paul and Washington internal conflicts were developing. In addition, ERA's status as a favored captive corporation came under increasing fire as the Cold War began to turn computers and applied science into competitive industries.

(U) By 1950, Wenger's dream of having a devoted and responsive research and development firm, whose talents ranged from advanced mathematics to computer design, was lost. At a critical point, America's SIGINT organizations were left without their own "think tank" and without a computer company devoted to its needs.

(U) But in 1947, as ERA was taking shape, it seemed as if it would become a permanent multipurpose research and development arm of "G." It had some of the world's most skilled electronics engineers and even a leading mathematician cryptanalyst, C. B. Tompkins. Tompkins had a unique mission. He was intent upon creating a high-level mathematical research branch within the company. It would fill, he thought, the vacuum left when most of the mathematicians in "G" and the SIS returned to academia and noncryptologic investigations.

(U) Howard Engstrom had a longer agenda. He hoped that ERA would become the new embodiment of the Desch-NCML RAM-building combination that had been so creative and responsive during the war. But Tompkins and Engstrom realized that to survive, ERA had to take on more than what was offered by OP-20-G and, perhaps, the SIS.

(U) At the company's birth, that did not seem threatening. Joseph Wenger thought that ERA's special relationship with "G" would always induce the company to bow to SIGINT needs. But ERA's dual role quickly entangled it in a series of conflicts no one had foreseen. Then the creation of AFSA began to undermine the other side of the relationship – that ERA could always expect a steady flow of contracts from the SIGINT community.

(U) As the early Cold War's demands began to pile up on ERA, "G's" assignments and the company's private work came into open conflict. The conflicts with the Bureau of Ships and some internal frictions were not the result of avarice or greed. In large measure they came about because of lack of support for applied science before the Cold War created the science "industry" of the 1950s. ERA began its life on a financial shoestring. It had little working capital and, for a time, survived only because the Bureau agreed to pay it as stages of projects were completed.

(U) ERA also began with a fear that the navy's work would be unable to sustain it. Each of the founding members was urged to search for other projects. That search developed its own dynamic, and by the end of 1947 the navy's contracts

accounted for less than one-half of ERA's business.

(U) Although that share varied from year to year, ERA soon had a life of its own and developed many outside ties and obligations. It joined with the National Bureau of Standards in the search for a commercially viable electronic computer; it gained a prestige contract from the ONR to survey all computer logic and technology; it had contracts with the atomic energy agencies; it was developing civil air control systems; and one of its divisions was designing sanitary trucks for airports. ERA even signed an agreement to develop a magnetic drum computer for IBM.[21] ERA's financial guru, John Parker, had to sternly remind all the ERA men that "G's" work was and would remain the company's first priority.

(U) Throughout 1948 and 1949 the Bureau of Ships kept up the demands for an end to the special relationship between OP-20-G and ERA. The Bureau was ready to take further steps.[22]

(U) The pressures compounded the problems ERA faced as its managers tried to turn a group of ex-academics and very creative engineers into businessmen. There were internal disagreements about ERA's place in science and arguments also developed over which projects to support. ERA's founders began to drift apart. By late 1949 C. B. Tompkins departed for a more stable environment: the NBS's West Coast applied mathematics center. Almost as soon as he arrived he began lobbying for the creation of a special nonprofit mathematics "think tank" for cryptanalysis, one separate from ERA.

(U) He was not the only one to find ERA inhospitable. Key engineers were leaving to find positions in the emerging commercial electronic computer industry. One of the first men to go was John Howard. One of the reasons for his departure was ERA's rather ill-fated attempt to revive Bush's Rapid Selector.

(U) Howard was soon followed by other ERA founders. Even Laurance Safford, who retired and became a consultant on statistical work, stayed at ERA for only a few months. He found one of NSA's new friends, the MELPAR engineering company, more attractive.

(U) ERA's Traumas

(U) The grand hopes for ERA in 1946 had turned into frustration for its engineers, as well as for its managers by the late 1940s. They never imagined that defense and civilian work would come into conflict. ERA's attempt to build a new Rapid Selector became a technological, financial, and managerial nightmare. The engineers could not make military technology work in a practical civilian setting, they could not please their defense and academic customers at the same time, and the Selector project became an economic sinkhole for the company.

(U) The resulting tension was intolerable to many at ERA. John Howard decided to leave in the summer of 1948. His role in what had become a chaotic and perhaps hopelessly over-budget project made it difficult for him to stay. He drifted for a time, but became an important member of the team the Burroughs Corporation put together to lead it into the computer business. Ralph Meader left quite soon. John Coombs lasted a bit longer, then decided to join IBM's engineering staff.

(U) Financial pressures played a great role in the troubles at Engineering Research during the late 1940s. It became increasingly difficult for the ex-academics and scientists to keep their small company competitive as more firms began to compete in the expanding military and science-related computer markets.[23]

(U) In addition to the financial pressure, the drive for efficiency that came with the integration of the communications intelligence agencies also took its toll. Soon the AFSA demanded contrac-

tors who knew how to follow bureaucratic procedures and who could survive on low-margin government contracts. Although Joseph Wenger remained in the highest levels of AFSA and NSA and was influential in forming their technical and research policies, he could not protect ERA's old special relationship.[24]

(U) The technology politics of the Cold War also played a role. In 1950, just as ERA's leaders were searching for a financial sponsor to rescue them, they received a body blow from Drew Pearson. In his "Washington Merry-Go-Round" column,[25] his men exposed the special relationship between ERA and the navy. The criticism led the navy to take a harder look at the company and to tell the intelligence agencies to return to the bureaucratic way of doing business. The navy's auditors, angered over the special open-end contracts with ERA, paid such meticulous attention to ERA's internal accounts that bad feelings developed on both sides.

~~(TS//SI)~~ The navy threatened to terminate much of the vital secret work at ERA just as the Soviet crisis was calling for more, not less, cooperation. ERA's president, John Parker, let loose some verbal blasts that further eroded the necessary[26] trust between the navy and the company. Relations with the navy bureaus soured so much that Joseph Wenger was unable to arrange for either a ceremony for or a letter of special thanks to the ERA engineers who had designed and built the astounding Atlas computer. IBM's men did receive formal thanks for their new work, however.[27]

~~(TS~~) The reorganization of American SIGINT, leading to the creation of the AFSA in 1949, then the NSA in 1952, contributed to the demise of the special relationship between ERA and the codebreakers. The integration of the military agencies brought a shift in who made decisions about computer purchasing. Because of the personnel policies that had led the SIS to look to civilians while "G" favored the military, NSA inherited a "computer" staff predominantly composed of those from the army side of technical SIGINT. They had different ties and orientations than the few remaining old navy hands that worked at policy levels, such as Joe Eachus and James Pendergrass. Unlike them, the 1950s NSA computer group had grown up within the Agency, had a deep respect for IBM and its equipment, and were more "operational" than mathematical cryptanalysts. As a result, the new core NSA group did not protect when the special group that integrated Agency and ERA work was disbanded. The 1954 termination of the NCML in St. Paul went almost unnoticed.

(U) SIGINT Loses Another Friend

~~(TS//SI)~~ The impact of the frictions with the bureau and the disillusionment caused by "Black Friday" were not confined to Wenger and the crew at ERA. At the end of his life, Stanford C. Hooper was disappointed about what had happened to the company, to American COMINT, and to his fight for science and innovation. In particular, his relationship with Engineering Research Associates did not end happily. Because of his views on how the navy should organize research for the Cold War and his ties to ERA, the navy's bureaucracy turned on the man who had done so much to modernize naval communications and cryptanalysis.

(U) Once retired, Hooper continued to serve on many science-related military boards, and his previous contributions to electronics led to more civilian accolades. At the same time, he began to act as a consultant to several small but important electronics firms.[28] He also remained in contact with the SIGINT agencies. As late as 1952 he was asked to serve on an important NSA advisory panel on communications.[29]

(U) Hooper became frightened of big business and discouraged by its attitude toward the needs of the military. He felt betrayed by those he and the navy and the nation had done so much for.

He was especially hurt by the actions of the company that he had helped to establish at the end of World War I, RCA.

(U) Hooper also worried that his old friends, the academics, would not serve the cause of SIGINT. He was alienated by their attempts to stake claims to a major share of military research funding and their demands for a vast and centralized postwar federal agency to mimic the NDRC.

(U) The military bureaucracy received even more barbed criticism from Hooper. Sadly, he received some in return. The navy's bureaus managed a direct slap at him. In the early 1950s, near the end of his life, he had to undergo a demeaning questioning of his integrity because of his relationship with ERA.[30]

(U) In 1947 Hooper's ties to ERA's operations became direct when he was asked to provide the kind of guidance he was giving to several other small electronics companies. His arms-length role in ERA was formalized in 1949 when the company agreed to pay him $3,000 a year to act as a "technical" consultant.

(U) The relationship pleased everyone until ERA was purchased by the giant Remington-Rand Corporation. Remington had decided to enter the computer business and to do so before it could be locked out by its competitor, IBM. In the early 1950s, Remington strengthened its old electronic research group, purchased the Eckert and Mauchly company and the rights to its UNIVAC business-oriented computer, and then bought ERA. Remington valued the cash-hungry ERA for its scientific computer designs and its patent rights on magnetic drums and other critical components. The ERA purchase made those who had retained ERA stock quite a profit, but Remington did not follow through on its chance to remain the world's leading computer manufacturer. Policy decisions, including ones holding back technological innovations, led many industry observers to characterize the firm as one that was able to "snatch defeat from the jaws of victory."

(U) Hooper had opposed the purchase of ERA by Remington Rand because he wanted ERA to remain flexible and focused on the needs of the intelligence community. Eventually, Hooper accepted the Remington purchase because there seemed no other financial alternative and because he thought that the link to Remington might have another important bonus. Being tied to Remington, he wrote, would ease the navy auditors' pressures on ERA. Sadly, with the takeover, the navy intensified its reviews of ERA, and it began to question Hooper's connection.

(U) Remington was ordered to show that Hooper had played a "technical" role. Remington could not muster the evidence necessary to show that Hooper had played a technical role. As a result, in 1954 Remington was notified that Hooper had not been and was not a legitimate employee of ERA. Therefore, declared the navy's attorneys, none of the payments to him could be charged to government contracts.[31] That decision came just a year before Hooper passed away.

(U) An Old Friend's Burdens

(U) As ERA and Stanford Hooper began to face their disappointments, another "G" old-timer was burdened with the responsibility of trying to rescue the fortunes of American cryptanalysis. The navy's Earl Stone, who had been a senior administrator in OP-20-G since World War II, was asked to head the new Armed Forces Security Agency. He accepted what became a very trying job. He had to supervise the bureaucratic merger of the two services, the SIS and "G," and, at the same time, rescue high-level SIGINT.

~~(TS//SI)~~ That was too much to ask. Despite the help of the "greats" of American codebreaking, such as Rowlett, Kullback, Sinkov, Rosen, Eachus, Campaigne, and even William Friedman, Stone ended his tenure in mid-1951 without

meeting the Soviet cryptanalytic challenge and without solving the problem of how to secure science's and industry's help in rescuing American codebreaking.

(U) Frank Powlett

(U) Dr. Abraham Sinkov

~~(TS)~~ But he had made some progress. With advice from Joseph Wenger who, although ill, continued to be a major figure in the SIGINT organizations,[32] Stone was able to do more than just fend off attacks on his agency. He convinced America's politicians that SIGINT funding should be increased and that previous levels of research and machine development be continued. And he encouraged the expansion of methodological and technical research branches in the agency. Before he left, ten percent of AFSA's workforce was engaged in some research activity, and the number of outside consultants, such as the mathematicians Marshall Hall and C. B. Tompkins, was increased.

(U) Stone was able to continue AFSA's role in exploring exciting, new technological frontiers. The agency invested in transistor development, and Stone encouraged the pathbreaking and very eliciting explorations by "G's" navy engineer, M. Scott Blois, into thin-film memory technologies. That work was a grandfather of microelectronics.

~~(TS)~~ The research climate under Stone was so open that the ideas of a young Korean War era sailor, Dudley Buck, were financed. AFSA began experiments on extremely low temperature and ultrafast "cryotron" circuits in its laboratories.[33]

~~(TS//SI)~~ Stone supported mathematical as well as technological research. As he was ending his reign, there was an attempt to build a formal program to attract the brightest and best of the nation's young mathematicians to the agency.[34] And Stone carried forward the "scientific" advisory groups that Joseph Wenger had begun after the war. Driven to find solutions to the Soviet problem, he established the Special Cryptologic Advisory Group (SCAG) and brought in men like Howard Engstrom and John von Neumann, who, he thought, would link AFSA to the cutting edge ideas in industry and academia. They were to serve another function. A friendly review board with a luminary such as William F. Friedman acting as liaison might protect the agency from those who thought AFSA should turn the Soviet problem over to an independent and "truly scientific" organization.[35]

~~(TS//SI)~~ Many of the members of the early advisory groups were recruited from the ranks of those who had served cryptanalysis then returned to industry, such as Joe Desch,[36] John Howard, Ralph Palmer, and IBM's John C. McPherson. Or they were old friends such as C. B. Tompkins and Marshall Hall, who had gone back to academic life. Although they were all agency connected, they had at least become "outsiders" with broader contacts than those within the agency.

~~(TS//SI)~~ And in the early 1950s, the ties of the science board to industry were acceptable. The direct link between industry and SIGINT provided by SCAG was seen as an invaluable benefit to the agency. Only later would questions of conflict of interest arise. That impelled NSA to seek more of its advisors, the likes of Claude Shannon and S. S. Cairns, from academia.[37]

~~(C)~~ Stone did more than forge a bridge to industry and science. He was able to secure budgets that gave the agency as much money each year for the purchase, rental, or development of computers and other analytic equipment as had been spent on all cryptomachines during the first two years of World War II.[38]

~~(TS//SI)~~ But Stone's years were marked by emergencies and cryptanalytic failures. Many of the ideas for advances in cryptanalytic computers had to be put aside as the agency desperately tried to reenter the Soviets' most important cryptosystems and to adjust to having to become one of the world's mightiest data collection and processing facilities.

(U) A Desperate Search for "Depth"

~~(TS//SI)~~ Before the Soviet blackout in 1948-49, the navy and army cryptanalytic groups had focused on the development of general-purpose cryptanalytic machines, such as Goldberg, Sled, Connie, and the 5202. The work on the electronic computers, Atlas and Abel, was an extension of the search for advanced and universal cryptanalytic engines. A few costly limited-purpose machines such as Warlock were designed, and there was some discussion of finding a replacement for the tabulators for data handling.[39] But until 1949 the army and navy engineers emphasized finding a way to automate the most sophisticated general cryptotechniques.

(U) Then priorities had to shift. Old development programs, such as those for Atlas and Abel, were allowed to continue, but dollars were shifted into creating simple but ultrafast comparators and into a tragic project to create a data machine as powerful as 400 tabulators.

~~(TS//SI)~~ In 1949 the emphasis was put on machines to "get the job done" rather than on creating elegant technological innovations. The central job of the early 1950s machines for the critical Soviet problem was to sift through millions of intercepts, hoping to find any hint as to how the cipher systems might possibly be attacked. The search for "depths" was the function of a new series of comparators.

~~(TS)~~ Machines were not required for complex mathematical analyses but to find errors in procedures or weaknesses in cipher equipment designs. The devices did not have to be very intelligent, nor did they have to be multipurpose. But they had to be fast – fast enough to perform massive searches.

~~(TS//SI)~~ No machine in AFSA or anywhere else was up to the challenges of 1949. To search through less than a single week's traffic from the one important Soviet system that had remained on the air, Albatross, would have called for 166,000 hours on the World War II 70mm Comparator. Even the advanced 5202 comparator was much too slow.[40] A new series of comparators had to be created, and quickly.

~~(TS//SI)~~ In early 1950 ERA was told to rush the design and manufacture of a machine that would be able to search a day's worth of Albatross

traffic in one week. The group in St. Paul put other projects on hold as it tried to meet the goal. Two machines were hurriedly put together in four months, then shipped to Washington. They were called Robins because they performed the round robin attack. Their speed was impressive although they reached only one-third of the rate that had been requested.

~~(TS//SI)~~ By looping two punched paper tapes, with one ten characters shorter than the other, and running them at thirty miles an hour past an improved photoelectric reader, 5,000 characters a second were read, and ten characters at a time were tested for simple IC coincidences. Because one tape loop was shorter than the other, the machine never had to stop or mechanically shift a tape. The improved electronic counters and circuits signaled when a threshold had been reached and punched an IBM card with identifications of the positions of the tapes without stopping the machine.

~~(TS//SI)~~ The first two Robins impressed the "cryppies." Solomon Kullback wanted forty of them, but financial constraints led to ERA being told to manufacture only a dozen copies, but as soon as possible. ERA worked some manufacturing miracles. Within a year fifteen Robins were running two shifts a day in Washington. That continued for half a decade as one million Albatross messages were run against each other. The result was tragic, however. Only 138 "busts" were located, and Albatross remained unexploitable.[41]

~~(TS//SI)~~ The Robins were only the first of a string of 1950s specialized comparators fast enough for the job of seeking the weaknesses in the tough cryptosystems. Every advanced technology was explored. When time allowed, some of the new machines were given complex architectures that provided flexibility. But speed was the goal. The 1950s comparators were, at the very minimum, three hundred times faster than the NCR-Gray Comparator of World War II. Several different companies contributed to this series of Comparator variations.

~~(TS//SI)~~ In fact, by the early 1950s, the comparator initiative shifted away from ERA and the old navy group within the agency. The army's cryptotechnicians and AFSA's contractors guided developments after the first Robins had been delivered.

~~(TS//SI)~~ But even before "Black Friday's" full impact, the army group had begun its own new comparator project. It called on its old friend Technitrol to put delay lines and magnetic tapes together to create the late 1940s generation of all-purpose comparators. But what had been planned as a long-term project for a series of ever more powerful machines turned into a rather hurried production of variations of more simple round-robin IC searchers. They were needed to meet the Soviet and new [redacted] The results were impressive, however. The Ciceros proved valuable for more than a decade and advanced the technology of magnetic tapes and their drive mechanisms. They also demonstrated how multiple memories could speed processing.[42]

~~(TS//SI)~~ Another high-speed, delay-line and tape depth searcher was Della. It could make 10,000,000 simple tests a second and compare 1,000 messages at all positions in seventeen hours.[43] Technitrol's Vivian series, which was designed to help on [redacted] was to include a machine with a magnetic core memory, one of the first uses of that technology, but that was abandoned as too time-consuming.

~~(TS//SI)~~ To rush delivery of a machine that could perform a parity bias attack, one of the Vivians was constructed by a new friend of the Agency, Denver Research. It was also asked to construct the important transistorized successors to Hecate, [redacted] crib machine. Those two Murdocks cost NSA three quarters of a million

EO 3.3(h)(2)
P.L. 86-36

dollars.[44] Another small company was called on in the 1950s for an ambitious project for a machine for locating and tallying group coincidences. An improved Connie that cost more than $650,000 was built by National Union Radio.[45]

~~(TS//SI)~~ Perhaps the most impressive of the new comparators was Duchess, another machine that was intended to be part of a long-term program. It was designed to tackle additive-pad problems to hopefully point to key reuse. It replaced the interim machines Countess, Mistress, and Consort. They had been too slow to re-create a new Venona-like triumph.[46]

~~(TS//SI)~~ Completed by IBM in the mid-1950s, Duchess contained several magnetic drums, helping it to perform as many as 1,000,000 subtractions, weightings, and threshold tests an hour. It cost over $700,000, but that seemed a bargain if it could conquer any of the frustrating one-time-pad systems used by the Soviets and their allies.

~~(TS//SI)~~ Unfortunately, the new comparators were not providing immediate solutions. The Soviet machine and high-level hand systems remained impenetrable, and the wisely used [redacted] proved as stubborn. Plain text and T/A and the tiny "facts" that came from lower level systems were what was yielding information to AFSA and NSA, but the agencies were becoming overwhelmed by all those disparate "facts."

(U) Earl Stone listened to the complaints of his machine staff, then gave them the signal to begin a project that had a very, very grand objective: to build one ultrafast data machine that would be more powerful than the hundreds of tabulators the agency was operating.

(U) His decision to launch the Nomad project led to "the" great defeat among NSA's early computer efforts. Millions of dollars went for nothing because of the chaos in the American computer industry and because of the cryptocrisis of the early 1950s.

(U) Wanderers and Nomads and Chaos

~~(TS//SI)~~ Vannevar Bush had not been alone in hoping for a machine to replace the electromechanical tabulator. As soon as World War II ended, OP-20-G used some Monogram funds to explore the logic of high-speed sorting, one of the most important functions in cryptanalysis and data handling.[47] Soon, an SIS team joined in to try to establish the logical basis for replacing the punch card.[48] Despite great hopes, it was realized that while the technology for mathematical machines such as Atlas was at the threshold, the hardware demanded by a data manipulation revolution was something for the future.

~~(S)~~ ERA's mathematicians continued their investigations of sorting, dispelling worries about losing data when it wandered around during sorts, but that was about all that was accomplished in the early stages of what came to be called the Nomad Project.[49]

~~(S)~~ The "memory" problem had defeated the first stages of Nomad. In 1948 file technologies, such as magnetic tapes, appeared to have too many problems to be overcome, even for IBM's team led by Ralph Palmer. Printers to keep up with electronic data machines were also in a distant and very expensive future.[50]

~~(S)~~ As a result, the early Nomad goal of a data computer 1,000 times more powerful than a tabulator or sorter was turned into nothing more than a rather speculative design project at ERA. Its engineers laid out a plan for an electronic computer that concentrated on sorting, collating, and other data handling tasks. Their Nomad was to have magnetic drums and some other high-speed memory to act as servers for a huge magnetic tape system, PIT. It was to hold the equivalent of 2,000,000 IBM cards. That PIT tape system was divided into four units, each of which

would deliver data to the computer's processor automatically. In addition to the data handling and sorting features, Nomad was to have a set of basic cryptanalytic orders and a special architecture to speed their execution.

~~(TS//SI)~~ Howard Campaigne and the others at "G" who were overseeing the project realized how speculative it was. They knew the Nomad concept was for the future. Even if they obtained the help of other government agencies, the machines' development would cost $5,000,000 and take seven years.[51] That was too much time and money, and Nomad began to wither. Some attempt was made to begin detail designs, but ERA became too busy with its emergency projects.

~~(TS//SI)~~ Then, another life for Nomad seemed possible. A preliminary research agreement was made with the NBS and the air force in mid-1949. A young navy engineer was sent to the NBS to work on the first stages of machine design.[52] Not much came of those explorations, however. The tapes and their drives continued to be stubborn and the cost of such a machine seemed prohibitive.[53]

(U) The idea seemed to be laid to a final rest, but in 1950 the crisis at AFSA led Earl Stone to agree to find the millions necessary to create a data processing revolution. If his staff, led by those from the SIS side of the agency, succeeded, AFSA would be the first in the world to have a massive data computer.

(U) The designs from ERA were dusted off and updated, and a request for a proposal was publicized in 1950. The proposal specified functions to be performed rather than hardware, but everyone knew that the mass memory demands would call for very advanced tape systems. After a year, a contract was signed. It was the largest single computer contract the SIGINT agencies had let since the Bombe project.

(U) The cost of the proposed machine was high but acceptable, especially to those who had lost faith in a heroic cryptanalytic future for SIGINT. The overwhelming processing demands that centralized noncryptanalytic "intelligence" would require could be met only with new and revolutionary input and file technologies.

~~(TS//SI)~~ There already was a need for such a technological revolution, and it was reaching a critical level. The amount of data reaching the Agency grew exponentially. By 1955 there was a torrent of "noninformation" flowing into NSA. The United States had more than 2,000 round-the-clock listening positions that were sending thirty-seven TONS of intercept material to NSA each month. In addition, some 30,000,000 words of intercept were sent by teletype.[54]

~~(TS//SI)~~ The data overload grew with every year and every Soviet challenge. NSA's posts were intercepting 2,000,000 messages a month from just one Soviet system, and the vast majority of that was plain text. And NSA's T/A section was processing more than 3,000,000,000 groups a year.[55] Within a short time, punching 1,000,000 IBM cards a month for just one problem was common. By the late 1950s the Soviet [redacted] problem alone was generating 15,000 magnetic tapes per month.

~~(TS//SI)~~ The other nations of the world were contributing their share. China generated 250,000 enciphered messages a year, matching the number of coded intercepts from the rest of the world. Plaintext numbers were much greater.[56]

(U) All that data had to be changed into a useful, if not standard, format, examined for relevance, sorted and merged, and routed to the analysts who attempted to turn the minute bits of data into intelligence. Even in the early 1950s the burden was becoming too much for hand and tabulator processing. NSA could not hire and train

P.L. 86-36
EO 3.3(h)(2)

enough people, and electromechanical machinery seemed unable to meet the challenge.[57]

(U) The risky gamble on Nomad seemed inescapable. The system was to cost at least as much as six or seven Atlas or Abner computers and would probably make the company that created it the world's leader in the manufacture of computers that were able to match the needs of business and bureaucracy. Although the Nomad design emphasized somewhat special-purpose sorting and data manipulation, the chance it provided to create new mass memory systems was very attractive.

(U) The Nomad contract was a great prize, and in some ways more important to the computer industry than the massive Sage early-warning computer project that IBM was taking on.[58]

(U) If You Can't Trust Someone from the Adams Family, Then ...

(U) Surprisingly, the late 1951 letter of intent for the huge data machine did not go to ERA, or even IBM, but to Raytheon, the company that had caused the army such frustration during the design and construction of Abner. Because of its earlier Nomad design work, ERA was the logical choice for the great project. But the emergence of AFSA's bureaucracy, the earlier political tussles that had weakened the special relationship with ERA, and its being in the process of total absorption into Remington-Rand made it a noncontender.

~~(TS//SI)~~ In fact, ERA was already being pushed to the side by its new owner and the SIGINT community. Only one major new AFSA or NSA computer contract was awarded to ERA until later in the decade.[59] Luckily, just after the Nomad award, the navy gave Remington-Rand/ERA a contract to develop a computer using the exciting and revolutionary new transistor in place of tubes. That would have a later impact on NSA's computer and communications capabilities.[60]

(U) The other likely winner of the contract, IBM, apparently did not make a serious attempt to take on Nomad. Although very worried by the UNIVAC computer, IBM's upper management was hesitant about putting too much effort into electronics. In addition, its own magnetic tape project faced continuing difficulties, and there were worries that government contracts would lead to the company's patents being threatened. IBM had a tradition of doing everything possible to protect itself.

(U) One tactic was to perform enough work on a technology before taking a contract to prevent developments financed by federal contracts from undermining patent claims. There may have been another reason. IBM had an overflowing plate. The computer advocates within the company had used the Korean crisis as leverage to convince Tom Watson to allow them to design and build the special NORC computer for the Naval Ordnance laboratory and, in a separate project, to create the Defense Calculator (IBM 701) to sell to agencies such as the AEC and NSA. All that taxed IBM's engineering staff and made the company's management quite worried about wasting men and money on additional speculative projects.[61]

(U) Raytheon was not awarded the Nomad contract by simple default, however.[62] The company had become well known and respected. And it was connected to New England's financial and industrial community. Its chief executive was of the famous presidential, intellectual Adams family. And its staff seemed worthy of the trust that had to go with a cost plus fixed-fee contract. The tape drives they had developed for Abner and the glowing reputation of its lead engineers made AFSA's team think they had selected the best firm. In addition, Raytheon's proposal was strong enough to allow a waiver of the usual requirement that a government agency accept the lowest bid.

~~(TS)~~ Raytheon's plan was very attractive. It met all the demands of the ERA's plans. Raytheon's machine was to have a large central memory. It was to provide fast access to 180,000,000 characters, about the amount of data that 2,300,000 IBM cards could hold. An innovative basic "stack" architecture was to speed data access by avoiding the need to determine and specify addresses. The central computer used vacuum tubes, but its speed was enhanced by having a thirty-six-bit word transferred and worked on in parallel.[63] Raytheon chose a three-address instruction to make memory fetches rapid. However, because of the special orientation of Nomad, the ultrafast main memory was limited to 1,024 words.

~~(TS)~~ Raytheon proposed to use glass delay lines for the main and fast buffer memories and a special three-inch tape for the PIT system. The tape system was very challenging. The vacuum column component that made stopping and starting tapes safe, as well as fast, and that would win so many sales for IBM, was yet to be invented.[64] Raytheon had experimented with many ways to reduce the start/stop time for the tapes and to minimize the debilitating strain on them. One pragmatic and unique part of their solution was a proposal to read and write on the tapes in both directions. Another was a special laminated tape that could handle stress and also serve as part of the tape drives' essential clutch system. The tapes had a layer of mylar, then a layer of metal, then a layer of mylar with oxide coating.[65]

~~(TS//SI)~~ The company promised to use innovative, pulse-position fast circuitry and to include a set of instructions tailored to AFSA's needs. They were to make sorting, collating, and modular arithmetic quite rapid and easy to program.[66] But Nomad was not to be a special cryptanalytic machine. Streaming units and the like were left to Sled and Abner.

(U) Work on Nomad began in late 1951 with generous expenditures of manpower and money. The AFSA stood ready to write a $1,000,000 check for the initial work and expected to send a similar amount to Waltham for each of the next three years or more. Although the agency knew Raytheon was working at the edge of computer technology, it thought its stable but innovative engineering team would conquer any problems.

(U) Very soon, however, AFSA's men sensed their expectations were not going to be met. They were correct. The Nomad project quickly became a demonstration of how little AFSA-NSA could depend on outsiders. Everything from management and technology to attitudes turned Nomad into a project nightmare.

(U) Some of the problems may have been due to the AFSA's shifting requirements and its acceptance of promises that major technological leaps could be achieved at minimal cost. Others were the result of the difficulty of attempting to do secret work in a corporate setting. But most of the problems were the price of the disorder in the computer industry of the 1950s.

~~(TS//SI)~~ Raytheon had begun to organize its project team and to explore its technological options well before the final contract for Nomad was signed in May 1952. Raytheon's best and brightest were assigned to the work. They received help from friends of SIGINT such as Dudley Buck and continuing advice from ERA. Unfortunately, ERA continued to refine and modify its designs, doing so into 1953.[67] The design changes made it difficult for Raytheon to begin the actual construction process and led to demands for increased payments for the machine.

(U) Some of the attempts to make Nomad a beyond-the-state-of-art machine created delays. The decision to use magnetic cores rather than delay-lines for the fast memories led to some dead-end explorations; the work on pulse-position circuitry ate up months; complex circuits to check and recheck the validity of data flows were

designed, then abandoned as too expensive; and then it began to be realized that the acronym "PIT" had become a much too accurate description of the magnetic tape development project.

(U) NSA had not closely supervised the Raytheon group, partially because the Agency was too short-handed to be able to assign a permanent overseer to Waltham. Thus, when hints of problems reached Washington during the project's first year, they did not cause alarm. By mid-1953 the technical and managerial difficulties were obvious, however. NSA teams began to visit the Raytheon site; then a rather typical Cold War problem almost brought the project to a complete halt.

(~~TS//SI~~) Naval security discovered that the wife of one of the lead Nomad engineers had relatives who were in powerful positions in the Chinese Communist Party, and the engineer still had close relatives living in China. His clearance was revoked.[68]

(~~TS//SI~~) At almost the same time, Raytheon encountered some financial problems. That led to a greater role for its accounting department in the Nomad project. The company could no longer afford to subsidize any part of the work. Then the accountants declared that Raytheon deserved much more than the government had expected to pay. The NSA's Nomad sponsors became outraged over that and the delays in the project. There was a diplomatic but very pointed request that Raytheon's "big brass" come to Washington for a review of the situation.

(~~TS//SI~~) Just as that was being arranged, the chief engineers at the company had a serious falling out. At the end of the year, several resigned, taking much of the talent in the company with them.[69] That truly worried those in NSA who were responsible for Nomad. The anxiety turned into anger when Raytheon requested prepayments to continue the work.

(~~TS//SI~~) The attempts by Raytheon's CEO, C. F. Adams, to calm NSA during his Washington visit, did not suffice. A formal review of the project was conducted, and a report was made to NSA's director. That report and the discussions among the Agency's computer experts led to a recommendation that an excuse be found to cancel the contract and bring the PIT work to Washington. In mid-1954 it was announced that Raytheon's Nomad had fallen too far below the technological curve to be worthwhile.[70]

(~~TS//SI~~) A prototype of PIT was shipped to NSA, and a large final check was sent to Massachusetts. A later accounting indicated that the prototype, the only lasting contribution of the Nomad project, had cost NSA $3,250,000.[71]

(U) Failure upon Failure

(~~TS//SI~~) In 1954 NSA was left without its grand "data" machine, and Raytheon went in search of an ally to underwrite its sagging computer effort.[72] The company found a sponsor, the Honeywell Corporation, but NSA was left adrift with a great deal of worry that the Nomad failure would make it impossible for the Agency to mount any more grand computer efforts. NSA was failing in its assault against its important target, and it had failed in its greatest computer effort.

(U) A great deal of faith in the Agency and in technology was needed.

Notes

1. (~~TS//SI~~) NSA CCH Series XII Z, "NSASAB Meeting," 19-20 May 1960.

2. (~~TS//SI~~) NSA AHA ACC 46406, "Recommendation for a Full-Scale Attack on Russian High Level Systems," 2 May 1956.

3. (~~S~~) NSA CCH Series XII Z, Ware on NSASAB Mathematics Panel, 9 January 1967.

4. (~~TS//SI~~) NSA CCH Series XII Z, draft copies of Michael L. Peterson, "The Bourbon Problem."

~~(TS//SI)~~ NSA CCH Series XII Z, S-2733, "Longfellow, History of," by Howard Campaigne, June 1948.

5. ~~(TS//SI)~~ NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April 1957. This source pictures the device as quite like the WWII German teletype machines, but other sources indicate [redacted] type attack was most useful.

6. ~~(TS//SI)~~ NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April, 1957, 106.

7. ~~(TS)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949."

8. ~~(TS)~~ NSA CCH Series IV W.1.5.12, "General History of OP-20-3-GYP," nd, 108.

9. ~~(TS//SI)~~ NSA CCH Series XII Z, draft copies of Michael L. Peterson, "The Bourbon Problem." ~~(TS//SI)~~ NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April 1957. ~~(TS)~~ NSA AHA ACC 7808, "Monogram Report," 29 November 1949. ~~(TS//SI)~~ NSA CCH Series XII Z, "Longfellow, History of," N-31 to 20-L, June 1948.

10. ~~(TS//SI)~~ NSA AHA ACC 1485, "Analytic Machine Aids Panel Meeting, 9 February 1949." ~~(TS//SI)~~ NSA CCH Series XII Z and CCH Computer History Box, OP-20-G "War Diary Reports: March 1, 1943-May 31, 1948," August 1945. ~~(TS//SI)~~ NSA CCH Series XII Z, "Processing of [redacted] Material By IBM Equipment," 7 May 1948.

11. ~~(TS)~~ NSA CCH Series XII Z, A. M. Gleason, "Inversion of Matrices with O'Malley," 1948. ~~(TS//SI)~~ NSA CCH Series XII Z, "Joint Long Term Program" (Old Planning Material, 1948-1949) compiled by Doug Hogan. ~~(TS//SI)~~ NSA AHA ACC 16093, "Rehabilitation of Bombe Equipments 1951-58."

12. ~~(TS//SI)~~ NSA CCH Series XII Z, Michael D. Peterson, "Bourbon to Black Friday: The Soviet COMINT Problem, 1945-1948."

13. ~~(S)~~ NSA CCH Series XI K Box 8, Snyder, "Yearly Cost of Representative NSA Machines," May 1955. The machine as constructed in 1948.

14. ~~(TS)~~ NSA CCH Series XII Z, "Report of the Second Computer Study Group," in *NSA Technical Journal*, XIX (Winter 1974), 21-61. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

15. ~~(TS)~~ NSA CCH Series XII Z, S-2733, "Longfellow, History of," by Howard Campaigne, June 1948. ~~(TS)~~ NSA CCH Series XIII Z, "Report of the Second Computer Study Group," as in, *NSA Technical Journal*, XIX (Winter 1974), 21-61. ~~(TS)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949." ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

16. ~~(TS)~~ NSA CCH Series XII Z, S-2733, "Longfellow, History of," by Howard Campaigne, June 1948.

17. ~~(TS)~~ NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986. ~~(S)~~ NSA CCH Series XII Z, NSA-314, "BISON," February 1955. ~~(TS//SI)~~ (~~Laconic, Noeon~~) NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985. ~~(TS//SI)~~ NSA CCH Series XII Z, NSA, [redacted] Modification," 4 March 1953. ~~(TS//SI)~~ NSA CCH Series XII Z, NSA-712, [redacted] 5 March 1953. ~~(TS//SI)~~ NSA CCH Series XII Z [redacted], "STURGEON," 15 February 1954. ~~(TS//SI)~~ NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase H," circa 1955.

18. ~~(TS//SI)~~ NSA CCH Series XII Z and AHA Series IV E.1.1, George Howe, "Historical Study of COMINT Production, 1946-1949," April, 1957.

19. ~~(TS)~~ NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986. (Hogan).

20. ~~(C)~~ NSA CCH Series XII Z, AFSA, "R&D Personnel Plan FY 1950-52," 13 October 1952.

21. (U) Hagley Museum and Library, Accession 2015, Unprocessed Remington Rand/ERA materials, ERA Minute books 1946-50, and Accession 1825, September 26, 1950, "Announcement of IBM Contract."

22. (U) NSA RAM File: July 20, 1946, Engstrom-BuShips, "Use Naval laboratories, not ERA"; August 12, 1946, BuShips-ERA "DC Office not legal, no plane allowed"; and July 26, 1948, BuShips to ERA, "All work to be done in St. Paul."

EO 3.3(h)(2)
P.L. 86-36

23. (U) Colin Burke, *Information and Secrecy: Vannevar Bush, Ultra and the Other Memex* (Metuchen, NJ: The Scarecrow Press, 1994).

24. ~~(S)~~ NSA CCH Personalities File, Joseph Wenger.

25. (U) *Washington Post*, August l6, 1950.

26. (U) Library of Congress, Papers of Stanford Caldwell Hooper, Box 23, "Page #211 attached to letter to Rumbles of Remington-Rand, August 25, 1952.

27. (U) The NCML in St. Paul was formally ended in 1954, putting a final stamp to the end of the special relationship. Apparently, ERA was not awarded any major contracts, except for the Bogart computers, from 1952 until late in the decade.

28. (U) Colin Burke, *Information and Secrecy*, 371-6.

29. ~~(TS)~~ NSA AHA ACC 28690, "Members of NSA Science, Electronic, and Mathematics Panels," circa 1953.

30. (U) Colin Burke, *Information and Secrecy*, 375.

31. (U) Hagley Museum and Library, Accession 2015, Unprocessed ERA materials, Remington-Rand General Counsel to ERA, St. Paul, February 16, 1954.

32. ~~(S)~~ NSA CCH Office Files, Personality Profiles.

33. ~~(TS)~~ NSA CCH Series XII Z, file folder, "Monogram and RAM Panel Reports, 1945-1949." (U) Emerson W. Pugh, Lyle R. Johnson, and John H. Palmer, *IBM's 360 and Early 370 Systems* (Cambridge: MIT Press, 1991), 451-2.

34. ~~(TS//SI)~~ Andy Gleason and Marshall Hall, called back into the Agency for the Korean conflict, began a Junior Mathematician program and began recruiting for it. Unfortunately, the program attracted only a few men and was not continued. ~~(TS//SI)~~ ~~(Laconic, Nocon)~~ NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985

35. ~~(S)~~ NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965. ~~(TS)~~ NSA AHA ACC 28690, "NSA SAB Members and Minutes," 27 April 1954. Note that C. B. Tompkins and Howard Engstrom were among those who were calling for such an independent "academic" organization. Stanford Hooper's ideas on such an extension of his early plea for science remain unknown. ~~(TS//SI)~~ NSA CCH Series XII Z, "Statement of Task priorities for SCAG," 12 September 1951. ~~(TS)~~ NSA CCH Series XII Z, "Abbreviated History of SCAG," February 1951-February 1952.

36. (U) Joe Desch was asked to become research director for "G" but declined the position. However, he continued to serve SIGINT for the rest of his career. He became head of NCR's military division and served on many advisory boards.

37. ~~(S)~~ NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965. ~~(TS//SI)~~ NSA CCH Series XII Z, "Statement of Task priorities for SCAG," 12 September 1951. ~~(S)~~ NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956. f[6071]. In 1953 SCAG's name was changed to "Scientific Advisory Board," and more academics were recruited.

38. ~~(C)~~ NSA CCH Series XII Z, AFSA "R&D Personnel Plan FY 1950-52," 13 October 1952.

39. (U) Like other organizations, the Agency did not replace its tabs until the 1960s when small computers such as the IBM 1401 were available. The 1401 was "the" computer substitute for the tabs because of its low cost, its ability to mimic tab procedures, and its high-speed printer. The Agency was one of the first to use the 1401s and had a dozen of them by 1962. NSA CCH Series XI H Box 12, Tordella, NSA General-Purpose Electronic Computers.

40. ~~(S)~~ NSA CCH Series XII Z, List of Machines and Targets.

41. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. ~~(TS//SI) (Laconic, Nocon)~~ NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985. ~~(C)~~ NSA CCH Series XII Z, ERA, "Robin Progress Reports," 1 August to 1 October 1952. ~~(TS//SI)~~ NSA CCH Series XII Z, AFSA21 "Summary of the Early Operation of the Robin Machinery," 19 May 1951.

42. ~~(TS//SI)~~ NSA CCH Series XII Z, James L. Sapp, "The Analytic Machines," circa 1955.

43. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

44. ~~(TS//SI)~~ ~~(Laconic Nocon)~~ NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985, 42 ~~(TS//SI)~~ NSA CCH

Series XII Z, "Office of Computers, List of Computers," nd.

45. (~~TS//SI~~) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. (C) NSA CCH Series XII Z, Herbert W. Worden," EDP Machine History."

46. (~~S~~) NSA CCH Series XI K Box 8, Snyder, "Yearly Cost of Representative NSA Machines," May 1955. (~~TS//SI~~) NSA CCH Series XII Z, James L. Sapp, "The Analytic Machines," circa 1955. (~~TS//SI~~) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. (~~TS~~) NSA CCH Series XII Z, Sam Snyder, draft copy of "Pre-Computer Machines in Support of Cryptanalysis," circa February 1978.

47. (~~TS~~) NSA AHA ACC 8252, OP-20-G, "Communications Intelligence Research Plans, 1948," 7 April 1947.

48. (~~TS//SI~~) NSA CCH Series XII Z, "Joint Long Term Program" (Old Planning Material, 1948-1949) compiled by Doug Hogan. (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings."

49. (U) The sorting explorations continued on for some time with work even being done at "G's" tab room. (~~S~~) NSA CCH Series XII Z, ERA A. E. Roberts, "An Experiment in the Rearrangment of Data (Sweater)," (Sorting, Nomad) 1 May 1950.

50. (U) Charles J. Bashe, et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), Chpt. 4.

51. (~~TS~~) NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986. (Hogan) (~~TS//SI~~) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings."

52. (~~TS//SI~~) NSA CCH Series XII Z, and, CCH Computer History Box, OP-20-G "War Diary Reports: March 1, 1943 -May 31, 1948."

53. (~~TS~~) The air force connection may have been part of the project later taken on by RCA in one of its first entries into the computer industry, its huge data processing tape machine, BIZMAC.

54. (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase II," circa 1955. (~~TS~~) NSA CCH Series XII Z, "General and Special Purpose Computers; A Historical Look and Some Lessons Learned," 23 May 1986. (Hogan)

55. (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase II," circa 1955.

56. (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase II," circa 1955.

57. (U) The electronic computers at NSA, such as Abner and Atlas did not displace the "tab." Hundreds of them were used in the Agency during the 1950s.

58. (U) IBM became involved in the Sage project in late 1952, and by 1953 it was a major effort within the firm leading to the production of almost fifty massive computer/communications systems. Charles J. Bashe, et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 244.

59. (U) The contract was for the very important Bogart computers for editing incoming information. The young Seymour Cray was the architect. ERA continued on with its 1103 deliveries to the Agency.

60. (~~TS//SI~~) The transistor contract of 1952 was NOBS 5750. NSA would return to Remington-Rand/ERA with the Bogart request and then with the emergency request to construct the Blueplate machine, an assignment that was extremely demanding. (~~TS//SI~~) NSA CCH Series XII Z, "The Shearman Complex: Part VII," Prepared by James L. Sapp, C425, circa 1960. (~~TS//SI~~) NSA CCH Series XII Z, NSA, "MPRO Technical Reports," circa 1956. Although it emerged in the laboratory shortly after World War II, and had been nurtured by giants such as Bell Labs and RCA, the transistor remained very expensive and unreliable. However, the emergence of the junction transistor and new production methods in the early 1950s signaled that it might soon replace the vacuum tube in computers.

61. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 132, 134, 135, 158.

62. (U) The final contract was signed May 1952.

63. (~~TS~~) NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986, (Hogan), 2-4.

64. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 209.

65. (~~TS~~) NSA CCH Series XII Z, "General and Special Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986, (Hogan) 2-6.

66. (~~TS//SI~~) NSA CCH Series XI K, Diaries of Samuel S. Snyder. (~~S~~) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 20.

67. (~~TS//SI~~) NSA CCH Series XI K, Diaries of Samuel S. Snyder, June 1953 and August 20, 1953.

68. (~~TS//SI~~) NSA CCH Series XI K, Diaries of Samuel S. Snyder, 31 July 1953.

69. (~~TS//SI~~) NSA CCH Series XI K, Diaries of Samuel S. Snyder, 16 January 1953.

70. (~~S//SI~~) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 73.

71. (~~S~~) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 20.

72. (U) Honeywell agreed to a joint program.

Chapter 10

(U) A Matter of Faith

(U) Would Science or an Old Tactician Save the Agency?

~~(TS//SI)~~ The Nomad debacle occurred as NSA was under siege. The Raytheon effort proved an embarrassing failure just as a round of threatening inquiries into NSA and the American intelligence community began.[1] NSA was under intense pressure because the Agency was letting America down. There were more than questions being raised about the Agency's Soviet effort.

~~(TS//SI)~~ Almost as threatening to NSA's future as the continued Soviet high-level blackout was what its critics thought was its inability to develop and employ science and high technology. The Cold War was a high-tech war, but NSA seemed incapable of achieving what Hooper had demanded in the 1930s, the integration of advanced science and technology into SIGINT.[2]

(U) NSA was almost confined to a very minor role in American intelligence. It came even closer to losing much of its independence. But it found a savior, the determined and politically savvy Ralph J. Canine, the new Agency's first director.[3] A regular army man in his mid-50s, Canine had an energetic and straightforward management style, but also a willingness to trust the judgments of his subordinates. Very important, he was an astute bureaucratic infighter; he blended the determination of a George Patton with the ability to relate to others. He knew how to deal with his superiors as well as his staff.

~~(TS)~~ As a result, in mid-1953, when the National Security Council began investigating the nation's strategic vulnerabilities, Canine was able to fend off its attempt to interfere in NSA's most secret internal affairs. To protect the Agency and its secrets, Canine formed his own review committee and filled it with NSA's good friends from the new version of SCAG, the NSA Scientific Advisory Board (SAB). Chaired by Dr. H. P. Robertson of the California Institute of Technology, the committee's findings were quite positive and, not surprisingly, fit with the plans and orientations of NSA's staff. Because of Robertson, NSA kept its independence and another chance at being a high technology innovator.

~~(TS)~~ Wisely, Robertson's report did not dwell on the high-level cryptanalytic failures; rather, it saluted NSA's plain language-T/A efforts. Robertson called for more of them and for the resources needed to extend its reach into voice intercept. But the recognition of the importance of the noncryptanalytic functions was not accompanied by cryptanalytic defeatism.

~~(TS)~~ Robertson saved the core of the Agency. He trusted NSA's "cryppies" and asked they be given what was needed for an all-out attack on the Soviet ciphers, especially the important Soviet [redacted] systems.[4]

~~(TS)~~ As Canine had planned, the report fit his policies, some of which were already being turned into hardware.

(U) Rushing "Bits," Not Even "Bytes," into the Agency

~~(TS//SI)~~ While Raytheon had been battling with the Nomad data processor, NSA's engineers were designing a series of much less ambitious but very important machines for the Agency's escalating data problem. They had to automate data collection. If the Agency was to provide intelligence based on low-level data, it had to modernize its collection systems.

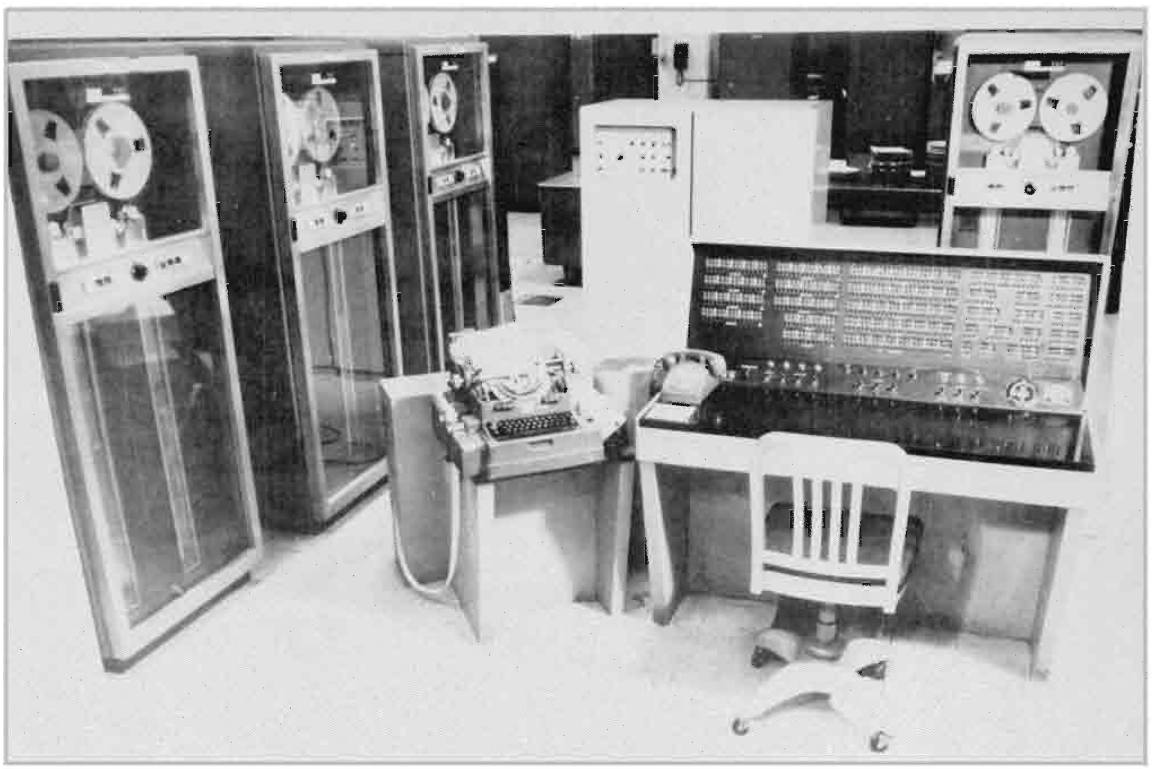
(~~TS//SI~~) After outlining their ideas, the engineers turned to several contractors. By the end of the 1950s, NSA's "basement" had almost two dozen special-purpose computers to convert complex analog signals to digital form, to reformat digital data for computer processing, to edit incoming messages, and even to scan the messages for "keywords."The new keyword programs eliminated messages of little interest, saving thousands of hours of analyst time.

(~~TS//SI~~) Audico, Buddy, Swallow, Neely, Tampa, Colt, Daytona and many other innovative special computers speeded the processing of all types of incoming data.[5] Of special importance were the Orlando and Bogart computers.

(~~TS//SI~~) The cost of the half dozen very specialized Orlandos was more than $2,500,000, but the role they played in converting Soviet [redacted] messages was invaluable. And their builder, the SIS's good friend Technitrol, of Philadelphia, made them to last. They ran constantly for eight years.[6] The Bogarts from ERA (Remington-Rand) served as long.

(~~S~~) Although the Bogarts were planned as straightforward machines to prepare data for Nomad, as it became evident that Raytheon's project was failing, their design shifted. The final Bogarts came close to being universal computers.[7] They were asked to fill in while the Agency searched for a true data machine.

(~~S~~) It took ERA more than three years to complete the first Bogart model in 1957. By the time the other four Bogarts were delivered, Remington-Rand had received almost $2,500,000 from the Agency, much more than originally intended. The money was well spent,



(~~U//FOUO~~) Bogart

however. Despite some "bugs" that delayed completion of the first model, the Bogarts were rugged and ubiquitous, partly because they used a valuable innovation. Their technology centered on what many thought would become the best alternative to vacuum tubes for the "logic" of a computer: magnetic cores similar to those appearing in the memories of advanced machines of the mid-1950s.[8]

~~(S)~~ That version of "solid-state" technology made the Bogarts very dependable. In addition, it allowed a powerful architecture, which led the Bogarts to play many different roles within the Agency. They even became a stopgap replacement for Nomad.

~~(S)~~ After it was accepted that Nomad was a failure, a Bogart was connected to a battery of tape drives. Using the IBM tape system that was evolving into the Agency's standard, that Bogart served as a useful cryptanalytic and data processing machine.

~~(TS//SI)~~ That and the other Bogarts became Agency favorites. They were called on for editing and scanning for keywords and even for testing for plain text through calculating the percentage of spaces in a message. They helped those who began designing circuits with computer programs; and the Bogarts were used for advanced statistical cryptanalysis.[9] The analysts who were researching the higher level Soviet systems asked for most of the Bogart capacity, but [redacted] erated messages received their share of machine time.[10]

~~(TS//SI)~~ The Bogarts did much more. With innovative additions, such as Meccano and Tune-Seek, which sampled analog (audio) inputs and converted them to various digital forms, the Bogarts became essential to the Agency's more advanced data collection systems.

~~(S)~~ One of the Bogarts became critical to an attempt to meet the demands of those frustrated by centralized computer systems. Cryptanalysts wanted computers closer to their work and to have control over their "runs." To answer that need, a Bogart served as the central computer for a remote job entry system at the Agency, Rob Roy. Rob Roy gave a hint of the future of computers within the Agency because it was a precursor of "distributed" processing.[11]

(U) Canine Guards the Fort

~~(TS//SI)~~ The Bogarts were an unqualified success, but they were not the kind of large-scale techno-victory that could prove NSA was worthy enough to guide its own future. When the Bogarts were still a sketch, Ralph Canine had to deal with another round of investigations and lobbying by outsiders. They were aimed at reducing the powers of NSA and exerting control over its operations. There was a real threat that if NSA did not show some astounding progress against the Communist targets, outsiders, such as DoD bureaucrats, would be given power over American cryptanalysis. Many critics wanted cryptanalysis turned over to academics.

~~(S)~~ Since the 1940s, when requests for a large number of supergrade personnel NSA needed to build a "science" cadre were refused, there were suggestions that a high-level and independent cryptanalytic think tank be established, one that could skirt the budget restrictions placed on the Agency. The "tank's" experts would deal with difficult problems without being distracted by day-to-day operational crises. Being outside of government had other advantages, it was claimed. In a sometimes-condescending way, it was asserted that an independent institution would be attractive to the "best" men because it could offer amenities barred to a federal agency. There would be competitive salaries and a "campus" atmosphere and routine; time cards and regulated hours would not be required.[12]

~~(TS//SI)~~ As NSA's Scientific Advisory Board's membership became more academic, the sugges-

tions to establish such a center increased, and they were accompanied by recommendations for an NSA program to support basic science/technology research.[13] Board members such as John von Neumann wanted the Agency to sponsor the development of an electronic circuit for computers that would be 1,000 times faster than current ones. Even nonacademics, such as Howard Engstrom, at times joined the chorus of voices that thought the best way to integrate science and cryptanalysis was to establish an independent "campus" research organization.[14]

(~~TS~~) Few within the Agency liked such ideas, however. They were taken as insults.[15] And they appeared to threaten the security of the Agency.

(~~TS~~) Ralph Canine led those who wanted to protect NSA from being torn apart. To do so, he had to fight many battles simultaneously. The military SIGINT groups wanted their freedom; the DoD desired to force "science" and scientific management on the Agency; "impractical" scientists demanded to take control of research; Congress wanted research and development to be contracted out to the corporations; and the CIA sought to establish its own cryptanalytic organizations.[16]

(U) Ralph Canine

(~~TS//SI~~) Canine was good at his job, but he could not overcome all the threats and challenges. He would have to give some ground to maintain the Agency's integrity.

(~~TS//SI~~) He did his best to build a viable research and development branch within the Agency. He finally secured a few supergrade slots and lobbied for an expanded engineering research group, one with enough men to build their own special computers and to adequately supervise contractors.[17] He tried to hire more mathematicians, in hopes that he could stave off the demands for that independent think tank. He sought a research director who could play the same political role. And he used all his political skills to delay being forced to create a new high administrative position, one for a "civilian" deputy director. He knew that would lead to DoD's interference within the Agency. The DoD wanted the power to appoint the deputy, and it was clear that he would be an "outsider."

(~~TS//SI~~) By the midyear of his tenure as NSA's director, Canine had done a great deal to protect the Agency and further its achievements. But he had not made up for the failure to penetrate the new Soviet systems; he had not been able to gain the resources needed to free the Agency from its dependence on contractors; and he had not solved the "science" problem. The Agency remained in trouble. Budgets were being questioned.

(~~TS//SI~~) Fortunately, Canine got some unanticipated help: the Hoover Commission of 1954. As a part of the mandate President Eisenhower had given to ex-president Herbert Hoover to review all of the executive branch, a subcommittee led by Mark Clark looked at, if not inside,

NSA. To Canine's relief, its many recommendations were almost all in favor of NSA.[18]

~~(TS)~~ When Clark's recommendations were echoed by those of a special Executive Office science board under James R. Killian (which had many contacts with NSA's Science Advisory group), Canine knew that if he had attractive programs the president would underwrite a massive "techno-fix" within the agency.[19]

~~(TS)~~ The only danger that Canine saw in the Clark-Killian recommendations was the reappearance of the idea that a captive but independent corporation be established to handle high-level cryptanalytic research.[20] But that threat was outweighed by the faith in NSA shown by the boards. In 1955 the news spread throughout the Agency that ideas that had been considered pipe dreams might be turned into projects.

~~(TS)~~ Several computer-related initiatives that had been discussed within the Agency and SAB were brought to Canine. By 1956 they were being formed into two historic projects that, it was hoped, would have a major impact on the computer industry's treatment of the Agency and reverse NSA's cryptanalytic fortunes.

~~(TS//SI)~~ One project was an attempt to define and build the perfect cryptanalytic computer. The other was a strange mixture of almost blind faith in practical cryptanalysis and in high science and technology.

~~(TS//SI)~~ Neither project went as expected, however. Although the Eisenhower administration granted NSA unprecedented amounts for the Harvest and Freehand Projects in 1962, a generation after Hooper had called for the integration of science and high technology into SIGINT, NSA remained unable to re-create an Ultra. It remained somewhat of a second-class citizen in the eyes of the computer industry.

(U) Enter Tom Watson and IBM

(U) Before the two great projects were more than speculations, it appeared that the Agency could rely upon the computer companies for much of what it needed, especially for data processing computers. Two major firms had emerged that were stable and willing to finance technological developments on their own. Remington-Rand (which included the old ERA) and IBM were upgrading their lines of computers and planning new advances. IBM, concentrating on data processing equipment, was finally catching up to Remington's sales.

~~(S)~~ Because of its long history of interaction with the SIGINT agencies, including the ongoing Sled and other RAM work, and with so many of its computer engineers having been part of the cryptanalytic efforts of World War II, IBM had a special view of NSA. It saw the Agency as in need of its help. IBM also saw NSA as an agency that could help IBM.

(U) IBM needed help. For IBM's computer advocates, who found it difficult to convince Tom Watson that electronics would become a sound business venture, contracts with government agencies were vital. They would provide needed research funds. Two old government friends of IBM's tabulators, NSA and AEC, seemed likely candidates to subsidize development.

(U) IBM engineers needed good friends. Tom Watson had taken a wait-and-see attitude towards electronic computers. After a rather costly and somewhat embarrassing venture, the creation of the SSEC computer, he resisted major computer investments. He financed several small research projects and supported the development and production of electronic add-ons for the tabs. But even emerging competition did not change his attitude. He was aware of the UNIVAC and of the work at ERA, but it was not until the increased pressures from his own engineers and the outbreak of the Korean War that he gave per-

mission to build a full-fledged electronic computer.[21] That permission came with some important qualifications, however.

(U) The firm's computer enthusiasts had to guarantee that IBM would not lose appreciable amounts on any computer development. Watson let it be known that enough customers had to have made promises to purchase any proposed computer before it went to the manufacturing stage. Someone besides IBM, he hoped, would underwrite development and initial production costs.

(U) An IBM research group associated with Columbia University was the first to take up the challenge. In late 1950 IBM agreed to a cost-plus, $1.00 fixed-fee arrangement for a one-of-a-kind special computer for Naval Ordnance. The NORC project launched IBM into computer development, but it did not satisfy many of the engineers who had been lobbying for a commercial product.

(U) Among them were many old friends of NSA. The head of IBM's electronics laboratory, Ralph Palmer (ex-OP-20-G), was constantly badgering the IBM hierarchy for more resources.[22] Having spent several years attempting to develop his Tape Processing Computer (TPM) and then becoming the overseer of the corporation's Poughkeepsie laboratory, he thought 1950 was a make-or-break year for the corporation's entry into the commercial computer market.

(U) His insistence, combined with Tom Watson's desire to show a contribution to the Korean War effort, led to high-level IBM managers being allowed to make the rounds of government and military agencies asking what type of machine was desired and what the agencies might be willing to pay. Of course, they visited NSA (AFSA at the time), where they learned of the need for a data processor. They also learned that NSA expected Atlas and Abner to be completed soon and that the Agency looked forward to buying more machines from ERA and Technitrol.

(U) The news about those purchases was worrisome, but it gave the IBM engineers some needed ammunition. When they returned home, they had good arguments for launching into a second IBM computer program. They pointed out that many government agencies had indicated they would buy a computer from the company. Of course, they emphasized the competitive angle. If IBM did not offer a machine quickly, it faced countless repetitions of what was happening at NSA.

(S) Computers were displacing tabs, and new companies were displacing IBM. NSA, the engineers reported, would soon have six of the largest and most advanced computers in the world, and none of them would be IBM's. They underscored another point: they could design a computer that would fit the needs of many types of users besides those already contacted. IBM could have a widely marketable machine. Thirty or more of them could be sold as soon as they were produced and additional orders were sure to arrive.

(U) After a push by young Tom Watson Jr. and a reassurance that patents would remain with the company, the engineers got a go-ahead from Tom senior to begin the Defense Calculator project. The engineers quickly decided on the nature of the computer that was later named the IBM 701.

(U) Their decision was one that showed that financial imperative, especially the need to develop a marketable, universal computer, had to outweigh sensitivity to NSA's special computing needs.

(U) After examining the requirements of the potential customers and balancing them against IBM's need to get an electronic machine on the market, it became clear that NSA would have to be treated as a stepsister. The new 701 computer

was to be a von Neumann-like number cruncher, a machine to satisfy missile developers, meteorologists, and ordnance agencies. The design made sense because the mathematically oriented agencies were the vast majority of expected customers. IBM decided to make some modifications to the design of the well-known IAS machine, however. They included magnetic tapes and enhanced I/O processing, but internal calculations remained the machine's forte. The 701 relied upon CRT-like fast memory and a slower magnetic drum.[23]

(U) IBM turned away from a design that was suited to NSA. The option to use the machine that Ralph Palmer had been working on, the TPM, was dropped because it was an "accounting" computer. Palmer, favoring a design that would allow a smooth transition from tabulator processing, focused on developing a machine that handled much input and output, but relatively little internal processing. Significantly, it was based on variable length internal "words," a feature essential to day-to-day cryptanalytic methods. It also used a Binary-Coded Decimal (BCD) representation of numbers which reduced the effort needed to translate characters.[24] All in all, his TPM was better for codebreaking work than the 701.[25]

(U) Unfortunately for NSA, there were problems with some of the TPM's essential elements, such as its tape drives. As a result, the TPM was kept in the laboratory as the 701 was rushed into production.

(U) With the 701's design specifications in hand, the IBM representatives returned to the government agencies seeking contracts. Unfortunately, they had to carry with them the news that the rental for the 701 might be twice as what had been mentioned during the earlier visits. The price increase was one of the reasons why NSA's computer group hesitated when IBM returned to Washington in mid-1952. The 701 was almost rejected, but it was given a second chance after a study group was formed. Joe Eachus led the evaluation, and William Friedman composed the summary reports.

(~~TS~~) IBM had some admirers who recommended that the Agency acquire two 701s. But the review panel's report, though positive, was cautious. The number-crunching nature of the machine was noted; there were complaints about the 701 being almost twice as expensive as an Atlas; and there were worries that IBM could not keep to its promised delivery schedule. The delivery issue was serious. Some at the Agency wanted a very severe financial penalty clause put in the contract; others demanded cancellation of the contract if the first machine was not in Washington by early spring 1953.

(~~TS~~) The group reached a consensus and recommended that two 701s with extra tape drives and memory be ordered. If the first was not delivered on time, both would be cancelled. It was expected that the two machines would cost the Agency $36,000 a month in rent.[26] The first machine arrived close to its promised date, but it was more expensive than thought. With operating charges included, it cost the agency $531,000 a year.[27] Disappointing to IBM's friends within the Agency, the 701 did not run as well as expected.

(~~S~~) Despite the 701's tantrums, it was put to productive use. The Agency reprogrammed many Atlas and Abner jobs for the 701 and even made it a replacement for Copperhead. But there were constant problems with the tapes and their drives; much time was wasted because cards had to be used as the 701's input. The 701 was replaced as soon as IBM completed its more reliable 704 in 1956.

(~~S~~) IBM's computer reputation within the Agency was saved by the arrival of the commercial version of Palmer's TPM, now called the 702. It arrived in early 1955, just after Nomad was canceled. In many ways, the 702 "saved the day." As would the Bogarts, it filled in part of the gap left

by the demise of Nomad. The 702 was a better high-volume data machine than the 701.

(S) Excited by the 702's data processing potential, the production group at the Agency began writing programs to replace the punch-card procedures for large volume jobs. The 702 did not include the hoped-for ability to perform I/O and other tasks concurrently, but its vastly improved tapes immediately showed their stuff.

(S) When the 702's 1956 upgrade, the 705, was announced, IBM's fortunes at the Agency were secure. Five 705s were ordered. The 705s became standbys in the Agency and benchmarks for its production processing.

(S) IBM's role in the life of the Agency increased. By 1957 IBM had manufactured about half of NSA's general-purpose computers. By 1961 the company had a lock on general-purpose computing. If the Bogarts, which were originally envisioned as special-purpose machines, and the experimental Alwac and LPG small computers are excluded, the only non-IBM general-purpose machine in the Agency in the early 1960s was an old Atlas II. And IBM remained as the vendor for the Agency's electromechanical machines.[28]

(U) A Machine for Us, Perhaps

(S) Although IBM began to offer machines such as the 702 and 705 to do much of what Nomad had been intended for, NSA's cryptanalysts and engineers were not satisfied. All the IBM machines were designed for others; NSA remained a poor relation in terms of computer architecture. The cryptanalysts and even the plaintext/TA handlers sought a truly "perfect" NSA machine, one that went beyond Sled in its originality and powers. It was difficult to achieve.

(TS) There were differences between the mathematically oriented, the operational cryptanalysts, and the data processors over the definition of an "NSA computer." In addition, the extraordinary cost of a large custom-made machine kept it as an ideal rather than a plan throughout the first half of the 1950s.

(TS) Only when the demand to conquer the Soviet problem and General Canine's political skills came together in 1956 was there an opportunity to create the great NSA computer. There were hints that enough money would be made available to allow the Agency to free itself from an architecture that was determined by the computer market place rather than by crypto-needs. There also seemed enough to make up for the Nomad tragedy. In response, old desires and ideas re-emerged.

(S) Concepts of a machine quite different from the commercial offerings, one far beyond a universal comparator or a Sled, had been discussed within the Agency (or its predecessors) since the late 1940s.

(S) Dissatisfaction with the von Neumann fundamentals had always been evident, especially among those involved with "production" rather than research. The type of programming an Atlas required seemed wasteful and illogical to those who had become used to calling upon separate special-function machines through commands plugged into high-speed boards. Supported by mandates to avoid building single-purpose computers, those who had grown up within the Agency, especially within the SIS, had led the crusades for the late 1940s alternatives: Sled and Abner's special hardwired features. Those were seen, however, as only a first step towards a true cryptoarchitecture.[29]

(TS//SI) Soon after the Abner and Sled projects were under way, explorations of great extensions of their special architecture began. One central NSA machine seemed to be the goal. By 1954, the explorations became formalized under the project name "Farmer." The technical/conceptual leader of Farmer was Ray Bowman, the old SIS hand who had been so important to Abner's spe-

cial crypto-features. In the mid-1950s, he was leading the Agency's analytic machine design group.[30] He received much help on Farmer from Samuel S. Snyder.

(~~TS//SI~~) In 1954 Bowman distributed a memorandum that was especially pleasing to the cryptoproduction groups. In it he outlined his architectural and procedural ideas. That first sketch gained wide circulation within the Agency.[31] It was followed by a series of papers that expanded the Farmer ideas.[32]

(~~TS//SI~~) Bowman's Farmer was to be a large, all-purpose cryptanalytic machine. At its center was to be a general-purpose computer that would act as a traffic director, taking the place of the old plugboards found on the tab-relay combinations and on Connie and Sled. That central computer was to be the "cop" that brought order to the electrical pathway (bus) that connected any number of special-purpose computers, each of which was to perform a particular crypto-function. Important to the goal of efficiency, the central computer would be smart enough to allow more than one job to be processed at a time.

(~~TS~~) Bowman was not asking for technology, but for more ideas. Knowing of the Agency's new long-term Dervish initiative to develop high-speed components, he thought it best that Farmer be a five-year design project. A follow-on effort starting in 1961 might lead to some construction. Bowman also thought it best that Farmer remain an Agency project, with all the design work to be done in-house. Only after the architecture had been refined, and when ten to twenty megacycle components were available, should outsiders be brought in.[33]

(~~TS//SI~~) Bowman's ideas and recommendations were widely circulated. Many engineers and cryptanalysts joined his study group. The group surveyed needs and methods within the Agency, leading to new suggestions. It worked so diligently that it was able to issue a report quite soon.

(~~TS//SI~~) The report contained a surprise. Another item had been added to Farmer's wish list. It changed the nature and, to a significant degree, Farmer's purpose. Now the Farmer project was to include a solution to the data processing problem. It was to take up where Nomad failed as well as be a super-Sled![34]

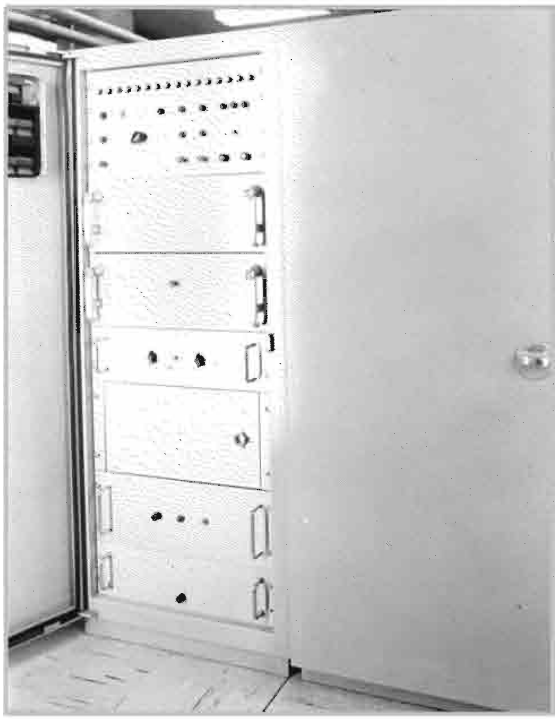
(U) One Big Machine Beats Out Many Little Ones

(~~TS//SI~~) Fortunately for Bowman and his overburdened aides, the report stated that this new version of Farmer was not to be turned into hardware until the technology to support it was developed.[35]

(~~TS~~) However, in 1955 there was growing pressure to turn ideas into machines immediately. That made it difficult for Bowman's group to keep Farmer a well-ordered design project. Criticism of the pace of the project arose. There were rumblings that Bowman and Snyder were taking on too much and that if a unique Agency machine were ever to appear, a special outside group would be needed.

~~(S)~~ There were more fundamental criticisms. Joseph Eachus did not like Farmer's architectural premises. He favored a type of machine that fit his view of the role of research and mathematics in cryptanalysis. He wanted computing brought close to and put under the control of users. That "distributed" processing contrasted with a large and centralized computing facility controlled by experts that "data processors" favored.

~~(S)~~ The distributed processing advocates were able to begin a project in 1954. As a result, two years later, the agency received the custom-designed Rogue system from Logistics Research of California. It had three "outstations" attached to its small Alwac general-purpose computer. A job could be submitted from any of the stations, saving users much time. Rogue proved so attractive that a much more powerful system, Rob Roy,



(U) Rob Roy

was ordered. Built around a Bogart, it had five outstations, and was in operation by early 1960.[36]

(~~TS~~) There were much, much more ambitious plans for distributed processing. In 1955 General Canine was convinced that what the Agency needed to meet the Soviet challenge was super-high-power mathematical machines close by each cryptanalytic group. To achieve that, he made a startling decision.

(~~TS~~) An order was cut to develop and manufacture a new version of the ERA 1103. Transistors were to replace tubes, thus allowing machines small enough to be put close to, even on the desks of, codebreakers. Canine looked forward to having forty of the new ERA devices within a short time. ERA's new parent, Remington-Rand, perhaps thought the old navy-ERA relationship was about to be reborn. Forty 1103s would cost at least $20,000,000.[37]

(~~S~~) But Remington did not get $20,000,000. The contract for the new 1103 did not go to ERA, nor did it lead to the forty machines. After six months of searching and negotiations, the Philco Corporation, which already had a reputation for manufacturing high-speed transistors, became the parent of the Solo project. Remington-Rand/ERA eventually gained a small part of the project; it was called on to manufacture the core memory for Solo.[38]

(~~S~~) Despite Philco's advanced technology, Solo's development bogged down. Cost and schedule overruns led to finger pointing among the contractors and a startling price tag of $1,000,000 for the first desk-size copy of Solo.[39] And it did not appear at the Agency until spring 1959. Not surprisingly, only one Solo was manufactured.

(~~S~~) There were other disappointments for those who favored distributed general-purpose computing. Computer technology of the 1950s did not favor small machines and remote computing of any type. A desk-size LPG-30 the Agency purchased in 1957, for example, did not perform well and had to be replaced.

(~~C~~) Meanwhile, Bowman's Farmer progress reports continued to circulate within the Agency. They received so much support that the criticisms by "mathematical" types such as Joe Eachus were ignored. One important reason for their dismissal was that Bowman's computer concepts received the blessing of a special NSA Scientific Advisory Board committee. It was charged with outlining a general-purpose flexible analytic machine program.

(~~C~~) After a year's study, in early 1955 the panel's chairman, John C. McPherson of IBM, issued a report containing the design for "the perfect cryptanalytic machine."[40]

(~~C~~) McPherson's logical-technical recommendations were much like those Ray Bowman had

suggested. That was because McPherson's panel was helped by one of his IBM colleagues, S. W. Dunwell. Dunwell, who had done so much for the SIS during World War II and who had become central to all of IBM's product planning, had spent the previous two years on a special IBM assignment. Stationed in Washington, D.C., he visited the major federal agencies seeking knowledge of their future computer needs. Among his visits were many to NSA where he "brushed up on the requirements being postulated by [its] staff members."[41]

(~~TS~~) Although McPherson's "perfect cryptanalytic" machine panel agreed with the architectural ideas in the Farmer proposals, its procedural ideas were very different. The NSA Scientific Advisory Board's panel recommended that the Agency stop dragging its feet and turn ideas into hardware. McPherson offered IBM's help.[43] It was not long before that "help" arrived; it came within a few weeks.

(U) An ERA by Any Other Name Is IBM

(U) Stephen Dunwell had been sent to Washington on a mission. He and other electronics advocates within IBM, such as Ralph Palmer, were again trying to sidestep corporate opposition to computers. Despite the success of the 700 series, management resisted investing in research or large-scale development projects. To men like Dunwell, IBM seemed doomed to take second place behind Remington-Rand. The corporation had increased its research expenditures and had a program for technology development, but it did not seem enough. Dunwell realized that the only hope to keep IBM at the competitive edge was, as in the early 1950s, to win government contracts for advanced computers.[44] Those contracts invariably included research subsidies.

(U) The need to win contracts to support IBM research grew intense in May 1955 when Remington-Rand triumphed over IBM and won the critical LARC competition for an AEC supercomputer. The LARC project would allow Remington to develop transistors and to move far beyond its UNIVAC and 1103 computers.[45] LARC also gave Remington's Philadelphia group under Presper Eckert the chance to redefine mainstream computer architecture.

(U) LARC was to be super-fast because of its multiple processors. One processor would control inputs and outputs; another would direct arithmetic operations. Extremely important, LARC was to be able to perform more than one task at a time. And it was to incorporate many new technology-based advances. It was to have, for example, ultra-fast memory fetches (0.5 microseconds).

(U) Once the LARC contract was announced, IBM searched for its own supercomputer contract. Its lead engineers were determined that their coveted development program of the mid-1950s would not die. To save it, a machine had to be constructed to prove that its ideas and technologies were viable. But IBM management did not want to risk a huge investment on a "demonstration" computer.

(U) As a result, an IBM representative appeared at NSA's headquarters just weeks after Remington won the LARC contract. He came with a very attractive offer.[46] IBM, he said, would build a super-speed machine tailored to the Agency's needs and have it in place by early 1959!

(U) As details of the offer for the special NSA machine were revealed, it seemed as if IBM had something the Agency could not refuse. For $2,500,000 NSA could have a computer with circuits two and one-half times faster than the current standard; for $3,500,000 it could have one with more advanced transistors and circuits, ones that would run at ten megacycles, or ten times the speed of the best components of 1955. Either version of the machine would have a revolutionary core memory that could bring information to the processors within 0.5 microseconds.

(U) There was more to the offer: IBM had, its representative said, a super-fast and high-capacity tape system. That system would be sold to the Agency, as would the computer, at a bargain basement price. The reason: IBM wanted a sophisticated user to test out its new components and architectural schemes.

(~~S~~) For the Agency's R/D group, the IBM offer seemed a gift from heaven. In mid-1955, Farmer's designers were terribly depressed. They were under pressures to produce, but the Agency was unable to allocate the people needed to continue the Farmer developments. Bowman and Snyder were among the most frustrated. They knew that the Agency needed a significant leap in computing technology to meet the Soviet crisis. But they could do little to answer the cries for help from cryptanalytic legends like Solomon Kullback.[47] The frustration level was so high that the R/D team seriously considered quitting the Agency to form a private company, one that could explore the new crypto-machine ideas. [48]

(~~TS~~) The IBM offer came at exactly the right moment for them. IBM, they thought, could take over the Farmer project.

(U) Is Half a Farmer Better Than...?

(~~TS~~) A follow-up visit by another IBM delegation, which included engineers who had been at SIS during the war, linked the Farmer goals more closely to IBM's offer.[49] That tipped the balance at the Agency. No time was lost. An inspection trip was made to the IBM plant by an NSA team in mid-July.Within a few days a letter contract was drawn up for the super-fast version of the IBM/NSA computer, one which, at a minimum, could serve as the central switching station for a Farmer machine.[50] IBM was beginning to call that computer "Stretch." NSA liked the name "Harvest" for its machine.

(~~TS~~) Then, the hope of rescuing Farmer encountered "outsiders." To please the DoD and the politicians, Canine had brought in an outside scientist to head a new research office. It had final say on large research and development projects. It reviewed the IBM proposal and to the shock of men like Sam Snyder, rejected it. The proposed arrangement with IBM was declared improper. A government agency was not to support development work within a corporation! Why should NSA pay for the development, for example, of special high-speed transistors that would become part of IBM's inventory?[51]

(~~TS~~) Just then, another block to implementing Farmer appeared. Joseph Eachus, frustrated over salaries, decided to leave the Agency and help the new Honeywell-Raytheon combination turn their Datamatic computer into a market contender. Snyder feared that even if the NSA research office relented, Datamatic would demand to bid on the "IBM" work, thus delaying any progress for so long that IBM might abandon its generous offer.[52]

(~~S//SI~~) Neither IBM nor NSA's R/D group could accept an end to the IBM-Farmer alliance. They were supported by Solomon Kullback.[53] While he was lobbying the research office, another prestigious IBM group rushed to the Agency in the summer of 1955 to argue for their "Stretch" proposal. Dunwell and the famous designer Gene Amdahl explained how pipelining, an interrupt system, "look-ahead," multiprocessing, interleaved memories, and automatic indexing would make the new NSA machine far ahead of its time. A multiprogramming ability, to run more than one program at a time, was more than hinted at.

(~~S//SI~~) The special IBM transistor and memory projects were described again, and their role in making the IBM machine perhaps one hundred times more powerful than existing computers, was explained.[54]

(~~TS~~) Sam Snyder's group presented new arguments to NSA's research office, explaining that NSA had frequently subsidized work within pri-

vate companies when it was to the benefit of the government.[55] Solomon Kullback was joined by Agency legends such as Abe Sinkov and Dale Marston in emphasizing how much the Agency needed a technological revolution.

(~~C~~) The pressure worked but not all the way. It was decided the Agency would support only a part of IBM's "Stretch" project. NSA agreed to give IBM $800,000 for eighteen months work on its high-speed core memory explorations. As something like insurance for the future of the special NSA computer, another $800,000 was promised to support an IBM team which was to design a computer that truly fit Agency needs, one following the ideas in the Farmer proposals.[56]

(U) St. Paul in Mohansic

(~~C~~) Somehow the flexibility in contractual relationships that had caused such furor when ERA was the favored company was becoming acceptable again. Apparently the late 1955 contracts for the Silo (memory) and Plantation (computer) projects were not put out to bid, and IBM was allowed to retain patent rights to much of what was to be developed.

(~~TS//SI~~) In fact, the Agency was creating a new version of an ERA, one within IBM's walls. While IBM's engineers began what became a very frustrating attempt to keep the promises about the high-speed memory and transistors, a special and highly secure Plantation area was set up within IBM's Mohansic laboratory. It was to be the new home of Farmer as well as a company-run NSA laboratory.

(~~TS//SI~~) The process of gaining high-level clearances for the Mohansic crew was begun. At the same time, Sam Snyder made the rounds of NSA's cryptanalytic and production groups requesting reports explaining their secret methods and procedures. The reports were shipped to Mohansic. IBM's laboratory soon had a library filled with NSA's most precious secrets.[57]

(~~TS//SI~~) The Plantation area became the Agency's computer think tank, but this time its powerful figures were not the academic types who had left "G" to found ERA.[58] Nor were they the new applied scientists who were making such a mark at centers such as Rand or Lincoln Labs.

(~~TS//SI~~) Those with practical orientations and those who had gained their cryptologic experience in the SIS were very influential. Stephen Dunwell, who had once led the SIS's machine room, directed IBM's Stretch project and had much to do with defining what the special NSA computer would be like. William Lawless, who had also been in charge of the Agency machine production facilities, played a more direct role within the "lab." Two other ex-Agency experts were hired to help sort through the crypto-procedures to identify common and essential cryptanalytic functions. Samuel Schmitt, a cryptanalyst/statistician, and the mathematician George Cramer, who had worked for ERA for some years, became invaluable. They gave much advice to the lead IBM engineers, Paul S. Herwitz, James Pomerene, and Fred Brooks.[59]

(U) But IBM's computer designers could not just attend to NSA's advice. The Stretch designers, it turned out, had to please other agencies and bow to the marketplace.

(U) Bucks Talk: the Favored Sister Gets the Attention

(U) Just as the Plantation group began to consider how to turn the Farmer ideas into hardware, IBM received some good news – at least it was good for the corporation. Determined to displace Remington-Rand, IBM had formalized its advanced work in late 1955, given it the name "Stretch," and scoured the country for more government contracts. What IBM had to offer was daring. They promised to make advances in

underlying technology and in architecture at the same time, something that would allow the company to leap frog Remington-Rand's LARC.

(U) For those with supercomputer needs, like physicists in the AEC, the Stretch program was enticing. They convinced the agency to pay IBM $4,300,000 for a super-calculating computer for Los Alamos. Soon, IBM had hopes that several other orders would follow for a similar machine.[60]

(U) The AEC Stretch became the focus of attention at IBM, and it was not long before a machine designed for physicists' number-crunching had an impact on what NSA's machine could be. Perhaps as early as 1956 and certainly by the time IBM and NSA were negotiating the contract for the construction of a machine in late 1957, IBM had decided that it would be too expensive to create a unique cryptanalytic computer. If NSA wanted a computer, a central part of it would have to be a clone of the Los Alamos design, including its high-speed and expensive floating-point arithmetic processor.

~~(TS)~~ NSA had become a stepsister again despite its original belief that IBM was to build "a machine designed primarily for Agency needs."[61] What NSA was calling "Harvest" was not going to be totally unique.

(U) A Data Factory

~~(S//SI)~~ Non-uniqueness also marked the NSA-IBM attempt to give Nomad a second life. NSA had its hopes raised in early 1955 when IBM representatives described the company's progress on its high-speed, high-density tapes[62] and an automated tape machine that would eliminate the need for human intervention in the selection and mounting of data. Exploration of such a system had been conducted as part of the corporation's AEC projects.

~~(S//SI)~~ When the special design group at Mohansic reaffirmed NSA's need for a mass data processing capability, the Agency's engineers argued that NSA should help IBM develop what would become known as the Tractor tape system. In response, the Agency gave IBM $300,000 for additional research, hoping the corporation's engineers would conquer the remaining problems.[63]

~~(S//SI)~~ If the hopes for Tractor were realized, the NSA Harvest computer could become the desired super data processor the Agency needed. The tape system would allow the creation of a centralized database to replace the thousands of separate magnetic tapes and tens of millions of IBM cards that were overwhelming the Agency. As significant, with Tractor, Harvest might well become a giant complex to replace all the Agency's tabulators and many of its special-purpose devices.

~~(TS//SI)~~ In fact, many hoped that Harvest would become NSA's data factory. Once in place, it would allow great efficiencies in the use of manpower and resources and make centralized management possible. Users would submit jobs and receive their output on a regular twenty-four hour basis.[64] The Agency was very concerned about information management, so much so that it held a pathbreaking conference in 1959 that helped define the emerging field of database management.[65]

~~(TS//SI)~~ The influence of those who saw NSA's future in terms of data processing reached into IBM's secret development laboratory. Their data processing demands were merged with IBM's decision to mold NSA's "perfect" computer to the corporation's need to minimize the costs of its Stretch computer program. All that was reflected in the Plantation report the Mohansic group issued in May 1957.

(U) Not a Farmer, a Nomad

(S) That first Harvest Manual accepted the AEC Stretch as the NSA system's centerpiece, it gave data processing a prominent place, and it recommended that implementing many of the architectural ideas of the 1955 Farmer proposals be deferred if not abandoned.[66]

(S) NSA's "special" computer had become a sophisticated appendage to a Stretch, rather than Stretch being a "traffic cop" for a cluster of separate special-purpose units linked through a data bus.[67]

(TS) The special cryptanalytic portion of Harvest, its attachment, or "bump," was to concentrate on a few general cryptanalytic tasks. It was not to be aimed at particular systems, such as the new Soviet [redacted] or the [redacted] Instead, IBM's team recommended that the "bump" be a very sophisticated and augmented version of the Streaming units in Abner.[68] The Streaming unit mimicked the logic of the older comparators.

(C) The Harvest "attachment" was to allow high-speed access to any "bit" or combination of bits in a stream of data, was to offset two streams, and was to perform the traditional counts and threshold tests used in statistical cryptanalysis. It was to be able to identify and perhaps correct garbles, to perform various types of modular arithmetic on the two data streams to produce a third stream, and it was to have a very advanced table lookup feature to facilitate language weighting. By a clever use of a base address and the characters encountered in a text, digraph or other language frequency weights could be referenced and applied without having to wait while a unique memory address was created.[69]

(C) Another special memory feature was recommended to help those involved with codebreaking rather than cipher work. By simplifying how a bit in memory was "filled" and located, frequency distributions and indicators of the existence or nonexistence of a group could be tallied at ultra-fast speeds. To facilitate all types of processing, the "attachment" was to have special ways of indexing – ways to address and access memory.[70]

(C) The mid-1957 Mohansic report admitted that the "attachment" demanded a special type of program, one that might have to be different from the one used on the main Stretch computer. In addition, the "attachment" would need a complex electronic version of the kind of plugboard program that controlled Sled and other special machines.

(C) The recommendations included some architectural possibilities. Multiprocessing/programming was one. It was thought it would be possible to have Stretch performing one or more tasks while the "attachment" was in operation and that the attachment itself might, as the Farmer outline had recommended, perform several jobs concurrently.[71]

(C) Despite the complexity of Harvest and its deviation from the original Farmer ideas, NSA's in-house evaluation group gave general approval to the design. But it asked for some additional information. When IBM submitted a revised plan later in 1957, it was accepted. Implicit in the acceptance was the idea that the Stretch with the attached NSA "bump" would be able to access a centralized database. Harvest was to be as much a Nomad as a Sled.

(C) The evaluation group's approval was needed because the IBM contract proposal was quite ambitious. It was no longer one for $3,500,000, but for more than $10,000,000.[72] That raised some questions within the Agency.

(C) But concerns about Harvest were not limited to its increased price. And they began to be

voiced before the Plantation report had been formally released in 1957.[73]

(U) Engineering Is Not Science, at Least to the SAB

~~(TS)~~ To the embarrassment of its NSA parents, Harvest came under fire from the Agency's Science board and, later, from the godfathers of cryptanalytic automation, Joseph Wenger and Howard Engstrom. Their criticisms encouraged others. The Harvest debate became tied to more fundamental issues within the Agency. As a result, in the late 1950s there was a replay of the standoff between science types and operational cryptanalysts that had frustrated Hooper and Wenger in the 1930s. Harvest became a battleground for larger questions about SIGINT's future. Central to the debate was the issue of who should control NSA. The science boards and the "old-timers" had many disputes over technological and science policies.

~~(TS)~~ Joseph Wenger had not expected that when he established an advisory board (SCAG) for OP-20-G after World War II. In fact, he thought the board would prevent frictions. He purposely filled it with men who would be sensitive to day-to-day needs within the Agency. His appointees had direct experience with cryptanalysis and its technology.

~~(TS)~~ Such appointments continued after AFSA was created. That proved useful. When the Department of Defense, which had become enamored with the new applied scientists, pressured AFSA to give science an important voice in its work, the old SCAG group was used as a means of fending off unwanted outside influence.[74]

~~(TS)~~ When NSA was formed and SCAG was turned into the Science Advisory Board (SAB), its membership looked much like before. It played a crucial role in protecting the Agency during the first rounds of outside review.[75] As important, the first NSA boards refrained from interfering in Agency affairs. Its members saw their role as one of offering help when asked.[76]

~~(S)~~ But as the Agency failed to conquer the Soviet problem and as the Department of Defense increasingly called on scientists, the board changed. Its membership shifted towards relative outsiders, it was allowed to take independent action, and it was asked to perform some rather onerous tasks. By the mid-1950s, it and its host of new advisory subcommittees were directed to review Agency operations and to devise specific plans for technological advancement.

~~(S)~~ The board was frequently asked to preempt outside interference by conducting reviews of Agency programs and achievements.[77] Although the board continued to serve as a buffer against hostile outsiders, its new role led to resentment among the Agency's staff.[78] Agency personnel thought many SAB recommendations were unrealistic and, in some instances, insulting. In the mid-1950s, frictions between the board and the "insiders" intensified, rather than diminished, when the Agency was told to bring in new blood in the form of a civilian deputy director and a new deputy for research.

~~(S)~~ Following the directives of the DoD, instead of promoting one of the in-house group to the supergrade research directorship, an outsider was brought in. It was thought that someone with a range of scientific contacts, experience in designing long-term programs, and a bundle of fresh ideas would invigorate the Agency. As a result, Solomon Kullback, who had been the Technical Director of Research and Development since 1949, was assigned to a second-place slot in the revamped Agency research office.[79]

(U) The new research director, Alva B. Clark, seemed the ideal man from the ideal background. An electrical engineer/scientist, he had pulled himself through the ranks of AT&T to become a vice president at what was regarded as the premier research facility in the world, Bell

Laboratories. Bell Labs was unique because it conducted applied as well as abstract research, a blend that DoD's leaders thought was vital to meet NSA's challenges. Clark arrived at the Agency in early 1954, reviewed many programs, helped reshape the Scientific Advisory Board, and suggested new initiatives.

~~(C)~~ Many of his decisions did not fit with the ways of the Agency, however. One of them was his rejection of the proposed use of the Farmer project monies to support IBM's Stretch efforts. Alva Clark did not get to see the results of his decisions: he died just two months after he finally signed off on the Plantation and Silo projects.[80]

~~(C)~~ The Agency employees hoped the next director would not resist a full Harvest program and that he would be more willing to follow the advice of the cryptanalytic old hands on other matters. They lobbied to have an "insider" appointed.

(U) Howard Engstrom, the man who had directed OP-20-G's RAM projects and then became central to ERA, and who later had served on the Scientific Advisory Board throughout the 1950s, was contacted. In late 1956, although his health was failing, he agreed to leave his position as vice president of Remington-Rand (recently absorbed by the navy's good friend, the Sperry Corporation) and take over the Agency's research office.

(U) Howard Engstrom

~~(TS//SI)~~ Engstrom appeared to be an "insider" with an appreciation of the practical side of codebreaking, its technologies, and the need to keep high-level strategic cryptanalysis within NSA.[81] But Engstrom was more an "outside" scientist than had been thought; he remained committed to the belief that cryptanalytic problems could be conquered through scientific, mathematical research. For him, data processing, "busts," and crude statistical methods were expedients that had to be replaced, not something on which to base a nation's SIGINT future.[82] And he still believed in the possibility of a Soviet Ultra if something like "G's" World War II research branch, which had brought the nation's brightest and most energetic young academic mathematicians together, could be recreated.

~~(S)~~ That belief was shared by his old "G" colleagues and by many of the high science types on the SAB. Since the demise of the hopes that ERA would be a crypto think tank, "G's" alumni had made a series of recommendations for the creation of an independent research organization. In the early 1950s, Howard Campaigne lobbied for the establishment of a free-wheeling pure research branch within AFSA. Its members should, he argued, be free of any operational duties and be allowed to be self-directing.[83] C. B. Tompkins sought a totally independent organization which would attract academics. He suggested that it be a subdivision of California's Rand Corporation.

~~(TS//SI)~~ Similar ideas were discussed among the SAB's members. The ideas grew more specific as the board engaged more academics, such as the fathers of information science, Warren

Weaver and Claude Shannon, and brought in Cold War university managers like Jay Forrester and A. G. Hill of MIT's Sage Project and Lincoln Laboratory.[84]

(U) Forrester and Hill had forged new relationships between technology-based schools and the military. At the same time, others were creating the means to bring institutions specializing in more traditional academic subjects into the world of secret work. Among them was a close friend of NSA, John von Neumann.

(~~TS~~) Since his early days on NSA's advisory boards, von Neumann had argued for direct links to universities.[85] By the mid-1950s he recommended the emerging Institute for Defense Analysis as a model that NSA should follow if it wanted cryptanalysis to achieve intellectual respectability. He also wanted NSA to support fundamental research in fields of interest to SIGINT (and John von Neumann). He constantly argued that NSA had to step in and fill the research gap in computer technology and logic. He wanted NSA to fund expensive research into ultra-high-speed circuitry and computer design.[86]

(~~TS//SI~~) Such recommendations began to be turned into a program after the Hoover Commission's findings were released. The Hoover committee recommended an all-out effort against Russia's codes and ciphers and wanted it to be a scientifically based one. The commission could not be ignored. It and its friends on the SAB were powerful and had the ear of the nation's leaders.[87]

(~~TS//SI~~) The Hoover Commission's views fit with the predisposition of the research types in the Agency, especially those who had come to NSA from "G." They were poised and ready to take advantage of the potentials of the Hoover report.

(~~TS//SI~~) By June 1956, the "G" veteran Jack Holtwick and his team had completed the *Recommendations for A Full Scale Attack on the Russian High Level Systems*.[88] The report, with sections based on the contributions of other "G" alumni, such as mathematician Richard Liebler (another University of Illinois graduate), asked for millions of dollars for an intensified traditional NSA effort to find a pure solution. The emphasis was on the use of high science and, importantly, scientists. Although Holtwick, with the advice of the SIS legend Abe Sinkov, asked for $17,000,000 for new computers and an additional 900 people for an in-agency program; he requested even more for fundamental electronics research and for the creation of a cryptanalytic Los Alamos.[89] He wanted long-term research into super-fast computer components. Implicitly, Harvest was rejected.

(~~TS//SI~~) Importantly, Holtwick recommended that a parallel "outside" academic program be set up to tackle the Soviet problems. A simple expansion of the Mohansic laboratory was rejected. A Los Alamos type of program would call for a "campus" and an academic elite.

(~~TS//SI~~) There was no immediate action on Holtwick's proposal for a massive in-house program, but when Howard Engstrom took over the research office at NSA in late 1956, he became a determined advocate for the "outside" portions of Holtwick's plans. Sensing that the Eisenhower administration would provide needed support, Engstrom pushed for the Holtwick alternative to Harvest and the IBM-based crypto-research. The Agency began to refer to his program as "Freehand" as Engstrom lobbied the Defense Department for a huge special appropriation.

(U) You Can Take Science Out of the Agency, But Can You ....

(~~TS//SI~~) Freehand was not a complete plan in late 1956,[90] but Ralph Canine wanted it implemented before he was forced to retire. The CIA's

drive to at least share in the control of SIGINT, the failure to predict the Hungarian invasion, and the lack of progress against the Soviet ciphers threatened NSA.[91] More fundamental, the technological advances in all types of code and cipher-making seemed to have gone beyond the Agency's technical capabilities. Even the Larc and Stretch technologies seemed less than adequate to save NSA.[92]

(~~TS//SI~~) Canine needed action. He quickly began to muster the political backing the Agency required. He summoned the Scientific Board to an emergency meeting in Howard Engstrom's office on October 8, 1956. He informed them of his feeling that the need for intelligence was as critical as in World War II and that another Ultra had to be found. He requested the board to consider what had already been embedded in Project Freehand. He wanted something else. He asked its members to provide answers to questions from President Eisenhower's office as to what could be done about the Soviet high-level problem if the Agency "were not limited by money, people, etc."

(~~TS//SI~~) Canine had already gained the ear of Eisenhower's science advisors, including Vannevar Bush. They were supportive of the outside high-tech, high-science initiatives within Freehand, and Canine wanted to report back to them with a board-approved plan before they might change their minds.[93]

(~~TS//SI~~) NSA's Science Board listened to presentations on the "science" components in the initial Freehand wish list. There was to be an exploration of the possible contributions of mathematics and the probable impact of more and better mathematicians within the Agency. There would be an R&D technology program to create computers 1,000 times faster than the best of the mid-1950s and an outside parallel cryptanalytic effort against the Soviet cipher machines.[94]

(~~TS//SI~~) There was also something rather sad. The board learned that the crypto-technology tables had been turned. No longer was the United States a dependent waiting for the secrets of the British Bombe to be sent from GC&CS. Millions were to be spent to provide Britain with a new computer so that it could continue its anti- [redacted] research.

(~~TS//SI~~) The board was informed that the secretary of defense had already given his general approval for the parts of Freehand to be conducted outside of the Agency. Then they were told something rather ominous and certainly insulting to the old-timers in the Agency. The DoD was withholding its approval for the Holtwick/Sinkov request to vastly increase NSA's workforce and its stock of computers. The DoD wanted to see evidence that NSA's staff was making progress before it granted any more funds for a "business as usual" attack.[95]

(~~TS//SI~~) The board shared the DoD's views. They favored abstract "outside" work, not the application of more-of-the-same cryptanalysis. They were especially enthusiastic about the idea of a mathematical research program. They wanted a Big Science of cryptanalysis to be created. And they felt it could flourish only if it was outside the Agency! Although the most vocal science advocate, John von Neumann, was ill and could not join in the deliberations, the SAB went beyond what Canine and Engstrom had brought to them. While declaring that Engstrom's idea for a crypto-Manhattan project be immediately implemented, they wanted something more: commitment to abstract mathematical research free of any specific problems. Howard Engstrom also appreciated abstract research, but he and his supporters within the Agency wanted that cryptanalytic "Los Alamos" to be a massive applied project for the Soviet [redacted] problem.

(~~TS//SI~~) There were variations on the Los Alamos theme, and it received different names, such as "Project Parallel" or "Manhattan," but the

essentials remained constant. The Soviet threat, Engstrom argued, could be conquered if he had the right people working under the right conditions. With a call to duty by the White House, to the nation's leading scientists, with a budget of $5,000,000 a year for five years, with a re-creation of the atmosphere of the old "G" group and with the project's scientists free from bureaucratic control, a Soviet Ultra could, he thought, be created.

(~~TS//SI~~) Engstrom began to win converts on the board and, importantly, within the DoD.[96] He obtained a firm commitment to funding for the "outside" parts of Freehand. $25,000,000 for "Lightning," the hardware development task, was promised. It was to create a new generation of computer technologies: circuits 1,000 times faster than the computer industry was producing were central goals. The DoD promised that more money was to come when the plans for the "Los Alamos" research center were completed.

(U) Engstrom's next, and very difficult, task was to turn the Freehand dollars into programs.

(~~S~~) Although IBM's John C. McPherson resigned as chairman of SAB in late 1956, thus helping to avoid charges of conflict of interest, and although IBM had established a high-science program under the well-known Cold War scientist Emanuel Piore, little thought was given to placing the responsibility for Freehand in IBM's hands.[97] There was some mention of IBM as a possible site for circuit explorations, but McPherson's declaration that he thought the 1,000 megacycle goal unrealistic and the tensions over the Harvest program caused the Agency to look elsewhere.[98]

(~~S~~) The question of how to run the Freehand technology program was especially troublesome. There was much at stake. A repeat of Nomad would be a disaster. Howard Engstrom felt that NSA did not have the staff necessary to direct the $25,000,000 project, nor was it, he said, even capable of supervising contractors. He wanted the Lightning project turned over to an outside prime contractor who would handle all details. There were discussions of using MIT's Lincoln Laboratory, but its head and other SAB advisors, including Jay Forrester, indicated the lab would not accept the responsibility. Forrester suggested the Agency create a new university consortium. But when universities, such as MIT and Chicago, were called on, Lightning did not receive a friendly welcome.[99]

(~~S~~) No Lightning center could be created in 1956. The Los Alamos and longer term mathematical research projects seemed to have found a home, however.

(~~S~~) Through one of the SAB members, the Agency had already established a relationship with the General Electric Corporation. After some discussions, GE presented its plan to create and house at least the Los Alamos (Parallel) project for the Soviet [redacted] problems, if not the long-range mathematical program. The corporation wanted to have a workforce of 200 people. Eighty were to be highly qualified scientific researchers, and thirty of them were to be the most eminent of America's scholars. They were to be joined by a cadre from NSA's research group.[100]

(~~TS~~) General Electric's plans were attractive, but they were not turned into a contract in 1956. Despite Engstrom's enthusiasm, the NSA regulars resisted a commitment to any plan that would take its most important work "outside."[101] With Engstrom unable to create a captive corporation for the technological side of Freehand (Project Lightning), all Freehand was put on hold.

(~~TS~~) The halt came just as another threatening Agency review was to begin! The predictions about that 1957 Robertson investigation were not encouraging. It was known that one of the Robertson commission's mandates was to cut military and intelligence budgets. With so little to show in terms of results against its prime target,

with the Agency's super-advocate, Ralph Canine, retiring, and with so many threats to take high-level cryptanalysis out of NSA, 1957 looked bleak.

~~(TS)~~ Engstrom's office reconsidered Freehand and how to organize its work. At the same time, SAB began its own new look at the two main Freehand proposals and its own favorite, a pure mathematics think-tank. Within the Agency there was another attempt to establish how much NSA itself should be expanded. The need to hurry was clear.

(U) Almost in Science – Would Lightning Be the Other Harvest?

~~(TS//SI)~~ Engstrom eventually devised a way to organize the "1,000 megacycle" Lightning program. Because of the way he did it, he pushed NSA over a sensitive bureaucratic line in 1957. The Agency became a sponsor of basic research within industry.[102]

~~(TS//SI)~~ Lightning was a bold and expensive program, but out of it, Engstrom predicted, would come a machine 1,000 times more powerful than the current ones. It would be powerful enough to employ even the old unsophisticated exhaustive-trial crypto-techniques of the 1940s against the Soviet cipher machines.[103]

~~(TS)~~ Ralph Canine had laid much of the political groundwork for Lightning. He had turned President Eisenhower into a believer.[104] Ike lent his name to the project, allowing Engstrom to convince the DoD that NSA be given complete control over Lightning. NSA was able to dodge the DoD rules that fundamental research be administered by a central agency.[105]

~~(TS)~~ After a few months of rethinking how to organize the project, in June 1957, without waiting for the rest of Freehand to begin, Engstrom got Lightning under way. The project had been changed during the previous months. To reduce it to a manageable size, it was limited to the development of technology. The ambitious architectural and communications explorations that were part of the original Lightning plans were put off.

~~(TS)~~ Howard Campaigne was given overall Lightning responsibility.[106] Along with many others, he interpreted Lightning as a project aimed at the eventual "development of THE computer" NSA needed to meet the Hoover and Robertson commission's demands for results on the high-level Soviet problem. He hoped a machine would be in the planning stages no later than 1962.

~~(TS//SI)~~ Others, who were less accepting of the idea that an Agency project could lead to a revolution in electronics, thought that Lightning would always be more of a speculative research than a development project, at least for many years. They were certain that it would be impossible to deliver a machine 100 times more powerful than the proposed Harvest, and they were anxious about any hints that operational machines would come out of the project by the early or mid-1960s. They thought that a 1,000-megacycle computer was, at very best, a well-intentioned dream.[107]

~~(TS//SI)~~ Making too many promises about an NSA computer would, they thought, undermine the Agency's credibility. But Lightning began with a 1960s supercomputer as a goal. Because of that, the Agency wanted to keep control of all aspects of Lightning. That proved impossible, however. Engstrom was again unable to create a captive corporation, was unable to find a company to supervise the entire project, and was unable to hire enough people within NSA to run a tightly controlled program.[108] Lightning had to be parceled out among a number of contractors.[109]

~~(TS//SI)~~ But Engstrom devised a strategy to get as much as possible from an essentially unsupervised project. He decided to fund a few of the most advanced research projects on ultra-high-speed components in industrial and university research centers. He hoped the additional funds

would lead to the emergence of technologies by the 1960s. NSA's role would be confined to financing the intensified research.

(~~TS//SI~~) Many research centers were contacted before cooperative partners were found. After hopes that Bell Laboratories would play a role dwindled, IBM, RCA, and Sperry-Rand became Lightning's core. They were selected because they had already developed expertise in three of what NSA's engineers thought were the "technologies of tomorrow" (cryotron, thin film, and high-speed transistors) and because they were trusted to supervise their own work. MIT, Philco, Kansas State, and Ohio State agreed to take small projects.

(~~TS//SI~~) With the exception of a bit of work at MIT, all the contracts were for technological development. The design and construction of the Lightning computer was pushed into the background, and only the barest sketch of what it might be emerged within the Agency. But that sketch reflected the long-term ambitions of the in-house Freehand group: to develop and apply more science and mathematics to cryptanalysis. In general outline, the "1,000" had become a mathematical supercomputer. By September 1957 the Lightning computer was to be "a general-purpose machine" without special NSA circuits (which could be added later), and it would be built at an undetermined time after the research and development phases of Lightning were completed. That made IBM's Stretch something of a competitor to Lightning. Fortunately for the Harvest advocates within the Agency, a Lightning machine was, they thought, years away.[110]

(~~TS//SI~~) But the research phase of the Lightning project was progressing. Because the selected companies had already been working on the technologies, NSA's "research" began immediately. But as the implications of the goal of a 1,000,000,000 pulse-per-second circuit were confronted, there was worry that the program would implode.

(~~TS//SI~~) An oscilloscope that could measure pulses in ranges anywhere near the desired rate could not be found. Worse, to reach the 1,000-meg rate demanded that components be much smaller than first thought – submicroscopic in size. The basic laws of physics dictated it. That created more than a challenge in an era when "microelectronics" meant the ability to put the equivalent of a few transistors on a tiny glass plate. The expensive "solid state" circuits of the era held, at most, 100 components. It was to be more than a decade before a miniature memory circuit could hold sixty-four bits of information.[111] Large size meant slow speeds. It would be a generation before standard circuits ran at 100 megs.

(~~TS~~) Lightning's researchers looked at all the possibilities for microcircuitry. They even explored what became the world's solution to miniaturization, what we now call "chip" technology. They found no immediate solution; but after a few months on the first exploratory phases, they all reported that "the prospects of achieving the goal of a kilomegacycle operation in the not too distant future were good."[112] There were reports that a miniature circuit the size of a pinhead and with 1,000 components was possible.[113] Contracts were renewed. The researchers focused on the technologies most likely to produce results. Some of them seem strange given 1990's solid-state technology.

(~~TS~~) One contractor investigated the use of "resonant" circuits while RCA worked on the tunnel diode.[114] Meanwhile, IBM pursued a dream that NSA's Dudley Buck had explored and which other researchers worked on through to the 1980s, "cryotrons." Cryotrons were miniature elements operating at a temperature of absolute zero. Such "cold" circuits would take advantage of a fundamental physical property: With no heat, there is little or nor resistance in certain types of superconducting metal.

(~~S~~) Cryotrons demanded microcircuits, ones so small that if laid on a fingertip, they would not

be noticed. IBM's route to such circuits in the late 1950s was through the thin film process rather than through "chip" etching. Very, very fine layers of metal were plated on a tiny glass base until a circuit was "painted." The component was then submerged in liquid helium.[115]

(~~S~~) The other major Lightning contractor, Sperry-Rand, concentrated on a more mundane use of "thin film" technology. It was developing it for use in room temperature circuits. The company was already making thin film memories to replace magnetic cores. The new memories were 1,000 times faster than Bogart's and much cheaper to make because laying down thin film was automated. But Rand's circuits were very far from the 1,000 megacycle goal.[116]

(~~S~~) Sperry-Rand's work was continued by the Agency, but the research at some other Lightning contractors was terminated within a few years, perhaps too much hand wringing by the Agency. The research on ways to speed transistors and how to manufacture integrated circuits (chips) was dropped in 1959. NSA decided that since others might explore the chip and high-speed transistors, the Agency should sponsor only the cryotron, thin film, and resonant circuit research.

(~~TS//SI~~) By late 1959 there was so much faith in those three technologies that thoughts of applying them emerged. There was a resurgence in the hope for a Lightning computer. Despite the investment in Harvest, a group at NSA was given permission to create the $10,000,000 Redman project. It was to begin in 1961-2, was to evaluate Lightning's results and design, and was perhaps to build an Agency cryptanalytic supercomputer.[117]

(~~TS//SI~~) Redman was an indication that a significant group within NSA had maintained its faith in mathematical cryptanalysis. But there was not a consensus about the role of cryptanalysis. In 1957, just as Lightning began, some influential outsiders expressed a very different view of the future of cryptanalysis and NSA.

(U) What Kind of Friend Are You, Dr. Baker?

(~~TS//SI~~) The growing fears of Soviet capabilities and intentions and the apparent inability of SIGINT to penetrate the "Iron Curtain" led to the creation of yet another NSA review panel in 1956. It was perhaps the most powerful one that had ever been called on and the one most directly connected to the Cold War's scientific elite. William O. Baker, vice president of Bell Laboratories, who was one of the nation's "stars" of applied research, was asked to head the review. He consented, but only on the condition that President Eisenhower grant him extraordinary powers. The investigation was to be under the White House, and its reports were to go directly to the president, his science advisors, and the Presidential Foreign Intelligence Advisory Board.

(~~TS//SI~~) Baker's charge was broad, but it had a focus. He was to inform the president of NSA's and cryptanalysis' potential. Would a Soviet Ultra soon appear or should the nation put its faith in spy planes, satellite photoreconnaissance, and, if possible, covert actions by the CIA?[118]

(~~TS//SI~~) When the prestigious Baker panel was formed, both the research and operational types in the Agency thought they were to face a group of like-minded friends. Baker had a background in intelligence and was already well known to NSA's Science Advisory Board and the Agency's top-level administrators. Although he was not "told all" about the Agency's work, he was welcomed into NSA. But the assumption that the Baker panel would protect the Agency was wrong!

(~~TS//SI~~) Baker took Stanford Hooper's ideas about the relationship of academia to COMINT to the extreme. He even went beyond the Los Alamos and Parallel ideas.

(~~TS//SI~~) He recommended that NSA be stripped of its most important asset, scientific cryptanalysis. Baker and his advisors were committed to science and scientists, but they wanted them outside of and away from the control of NSA.

(~~TS//SI~~) That led to a vigorous protest by Agency insiders. In the early 1930s OP-20-G's cryptanalysts ignored Hooper's "computers"; in the late 1950s, after Baker's recommendations became known, there was much more than foot dragging.

(~~TS//SI~~) Well before Baker's Top Secret final report was formally released, word of what it contained reached down into the Agency. The most frightening part of the report was the conclusion that communications security, especially the Soviets', had far outdistanced cryptanalysis. There would be no more "great" intercepts. The report insisted that the Agency recognize the strength of the Soviet [redacted] systems and stop hoping that its cryptanalytic methods or its machines would ever unlock them. More-of-the-same cryptanalysis, Baker concluded, would never work. Nor would a more-of-the-same relationship between science and the Agency contribute much.[119] Baker declared that the age of heroic cryptanalysis had ended.

(~~TS//SI~~) Baker stated that NSA should focus on low-level systems and on integrating the fragments discovered in them. That was insulting to Agency regulars. It was unacceptable to NSA's "greats." Samuel Snyder, the man in charge of Harvest, reported that when the legendary William F. Friedman, "the man who broke Purple," heard of Baker's recommendation, he reacted emotionally and threatened to go to the White House. Like others, Friedman did not want the Agency to be confined to being just a data processor.[120] For Friedman, without cryptanalysis there could be no NSA.

(~~TS//SI~~) There was more to the Baker report, and it was not pleasant. Baker recommended that the Science Advisory Board be reorganized and its outsiders given a much more direct and regular voice in Agency policies. By implication, NSA's researchers had not done a good job.

(~~TS//SI~~) Even the Agency's attempt to join in the development of advanced computer technology was criticized. The Baker panel urged the Agency to drop Lightning and to end its role in Stretch. Let industry and other agencies deal with the general and fundamental problems, he said.

(~~TS//SI~~) Baker wanted the Agency involved in only two types of computer development. The most important was to continue the automation of signals gathering. He urged that the "front end" of SIGINT be automated immediately. After that was done, he wanted the Agency to concentrate on the creation of special-purpose computers to handle the torrent of "bits" the new front-end would provide. And that new NSA front-end was to include something that would truly make NSA as much or more of a data processing shop than a cryptanalytic agency. Baker wanted NSA to handle ELINT, the signals gathered from enemy radar and other electronic systems.[121]

(~~TS//SI~~) Worse for NSA's regulars was Baker's interpretation of what Howard Engstrom was promoting – the "Los Alamos" cryptanalytic project to work on the Soviet problems in parallel with the Agency analysts. Although the General Electric plan had withered, Engstrom continued to want a parallel effort.

(~~TS//SI~~) Baker's recommendation went much further, dangerously so. He sought to take advanced cryptanalysis completely out of NSA. The Agency was to turn over the Soviet and all other major unsolved systems. He wanted an applied mathematical center, one with very expanded powers. Filled with the best outsiders and some of the outstanding mathematicians from the Agency, it would have jurisdiction over

P.L. 86-36
EO 3.3(h)(2)

all the high-level problems, as well as the duty of exploring the frontiers of mathematical cryptanalysis. Based on the belief that even the best analysts were unable to concentrate on long-term challenges if they were within an operating agency, cryptanalysis, he said, should be removed to an independent campus."

~~(TS//SI)~~ That think tank was to have a wide reach. It should be the site for advanced computer work as well as codebreaking. Although emphasizing the proposed center's role in software development, hardware design was not excluded.

~~(TS//SI)~~ Agency representatives accepted the idea of a quasi-independent think tank – an extension of the older mathematics workshops that dealt with abstract problems.[122] But they argued that turning over the high-level problems to outsiders would be a tragic mistake. They warned, as Mrs. Driscoll had done in the 1930s, that much besides knowledge of the mathematics of a cryptosystem was needed to enter it. And, they said, sharing the high-level problems would be wasteful. It would be better to create more super-grade analyst positions within the Agency.

(~~TS//SI~~) The protests did not work! Baker and his panel were determined to establish an outside center. Armed with a presidential signature, Baker made sure that NSA set one up. With amazing speed, funds were allocated, a site was selected, and a cover name was created. Before the end of 1958, NSA had its think tank, one directly connected to the world of the sometimes-impractical academics. Within the Agency it was known as The Cryptanalytic Research Division of the Institute for Defense Analysis at Princeton University. Outsiders thought it was a communications research center within the Institute.[123]

(U) Dr. Baker's Half-an-Institute

~~(TS//SI)~~ The Institute for Defense Analysis was founded in 1956 as a means of creating a direct link between academics and the military. MIT, Stanford, and other research universities cooperated to set up the IDA for the exclusive purpose of serving the needs of the Department of Defense. Princeton, with its beautiful site, the Institute for Advanced Studies, and its proximity to Bell Laboratories, seemed the ideal "campus" setting. NSA agreed! But agreeing to establish the new institute was something different from doing all that the Baker panel had recommended.

~~(TS//SI)~~ The Agency was able to quietly avoid following many of the threatening recommendations. Only six NSA mathematicians were allowed in the new center because the Agency was determined to keep its own group working on the high-level problems.

(~~TS//SI~~) In addition, the Institute's mandate was unilaterally shifted to abstract research and to anticipating future systems, rather than "attacking solely current problems." Although its founders were told they would be responsible for advanced work on computer designs and software, there was no intention of taking all such responsibilities away from NSA's various research groups.[124]

~~(TS//SI)~~ And the work at the CRD got off to a slow start. It took some time to obtain rooms and then a separate building. More difficult was gathering a team of leading mathematicians willing to devote part of their academic careers to cryptanalytic problems. Running the old summer institute at Princeton helped attract some academics, but in its first years, 1959-1963, the CRD found it difficult to keep even its directors. Some great mathematicians served in that post, such as J. Barkley Rosser and A. Adrain Albert, but they did not stay on.[125]

~~(TS//SI)~~ But the main reason for the CRD's slow start was the Agency's decision to try to keep the Princeton group busy on abstract problems.

Materials on real targets were kept from the CRD's staff for several years.[126]

(~~TS//SI~~) The quiet changes to the Baker panel's recommendations about IDA were not the only ways the Agency defended itself during the late 1950s. Lightning, for example, was not canceled nor was Redman. More indicative of the power of the Agency was the reappearance of the Harvest project. After some rather sharp conflicts within NSA, in spring 1958 millions were committed to building IBM's version of an NSA computer.

(U) A Harvest of Overexpectations

(~~TS//SI~~) After a year of super-secret design work in its version of an ERA, the Mohansic Laboratories,[117] IBM returned to NSA in May 1957 with its design proposal for Harvest. Soon, there was a successful request for more Agency financing to develop the mass storage tape system, Tractor. But a formal agreement to begin Harvest had to wait another year, and the major financial commitment to it was delayed yet another half year. The delays were caused by more than quibbling over technical and financial details. There were substantive objections to IBM's design and procedures.[128]

(~~TS~~) The objections were voiced as early as 1957 when it became clear that IBM had decided that the heart of the NSA system was to be Stretch, the computer that had evolved into a super-speed number cruncher for customers such as the AEC. The proposed NSA Harvest computer was not going to follow the architectural specifications of Farmer.[129] The first "special" part of the proposed Harvest system was not going to be one of many "boxes" that would hook onto a databus, but an expanded version of Abner's Streaming unit that was hardwired into the Stretch.[130]

(~~S~~) The in-house NSA R&D evaluation group was not put off by the complaints nor by the deviations from the original Farmer ideas, however. They chose to ignore some mumbling against the Stretch component because they were so impressed with IBM's specifications. When the R&D group used the paper specifications IBM supplied to estimate Harvest's power, they were quite pleased. They calculated that major data processing tasks, such as mass sorting, would be 100 to 200 times faster than on their most trusted machine, the IBM 705. When IBM promised that it could build the Tractor mass memory system, it seemed sure that Harvest would be as much as five or ten years ahead of what the commercial computer market was producing. NSA, it appeared, was to have its super data-processing machine.[131]

(~~S~~) Tractor was appealing. Its design hinted that the Agency might have one great memory that would allow the use of advanced data management tools. Tractor's "data rate" was to be 100 times that of the best magnetic tape systems of the day. As important, it was to hold an enormous amount of information, so much so that it held out the promise of being able to automatically locate and deliver the backlogs of messages needed for "depth" searching. Each Tractor tape held the equivalent of eighty standard ones, and the system had 480 of them. Tractor would automate access to the equivalent of 39,000 regular tapes, perhaps enough to store all the Soviet messages.[132]

(~~S~~) Despite the encouraging news about Tractor, opposition to Harvest reemerged in late 1957. One reason for the new protests was the feeling that Harvest might undermine Lightning, but much was caused by dislike of the close relationship between IBM and the Agency.[133]

(~~S~~) While NSA's Harvest team worked on the various contract proposals IBM submitted, Howard Engstrom became a major and vocal critic. He made his position quite clear, even in the director's office.

(C) As head of NSA research, then as the Agency's deputy director, Engstrom was informed of the technical details of Harvest and IBM's contractual demands. He was not happy with either. He and others felt that IBM's technology was not really that far ahead of other vendors. He thought IBM had a lock on Agency business, and he was very upset by IBM's insistence that the Agency treat much of Harvest as "company confidential" information. As important to understanding his opposition to Harvest, he felt that the enormous cost of the Harvest would cripple other programs, including his creation, Freehand.[134]

(C) Engstrom wanted an end to the Harvest program or, at least, the negotiation of better terms. He took his views to the director's office, countering the pro-IBM arguments of the Agency's Harvest team. Engstrom was forceful, but the director knew NSA had already invested too much in Harvest to allow a real showdown. Lieutenant General Samford certainly did not want to be blamed for slowing the delivery of the AEC's machine by forcing IBM to reconfigure Harvest.[135]

(C) IBM and the Agency regulars won the day. Engstrom was overruled. And the Agency gave in on many Harvest contractual issues. IBM's refusal to provide rent-free equipment and to forego charges for other typically "free" items was accepted. Few penalties for late delivery were demanded.

(C) A final and very large contract was signed on 15 June 1959. The Agency had already invested $1,987,000 in IBM-conducted research and design studies; now it committed itself to an additional $11,400,000 for the Stretch computer, the Harvest "bump" and the Tractor tape system. Soon it added another $3,000,000 for additional high-speed memories.[136]

(C) That was not all, however. Within six months IBM returned to the Agency with the news that the corporation had underestimated the cost of the Harvest and Tractor components by approximately one hundred percent, or $5,500,000.[137] Then the Agency was informed that delivery would be postponed indefinitely. In addition, the Agency was told that many factors had led IBM to some "moderate degradation of some parts of the system hardware."

(C) The Agency was in too deep; there was little it could do. To withdraw from Harvest would cause another Nomad embarrassment. But the Agency took steps to protect itself; it negotiated a ceiling price for the Harvest component: The government was to pay no more than $9,300,000 for it.

(C) Then an unexpected expense had to be accepted. NSA would be one of the first to realize that Pendergrass had not been quite on the mark in the mid-1940s when he described the future of digital computing. He and everyone else had underestimated the difficulties and expense of programming. As computers increased in power and as users expected more from them, software development was taking as much or more time than hardware construction, and it was on a path that was making it as costly as the machines. Basic Harvest software, the Agency soon learned, was to cost more than the original price of Stretch.[138]

(C) Because IBM had not promised to supply much software, just what it had developed for and with the AEC group, NSA had to find the monies to create a powerful operating system and an applications programming language that would make the two types of computers in Harvest easy to use. Those were big chores in the late 1950s. The Agency spent more than $4,000,000 on the initial software for Harvest.[139]

(C) It took several years to develop the applications language, Transcrypt (later called Alpha), the HAP assembly program for expert programmers, and the operating system, HOPS. Pushed to

have them ready for the Harvest machine's delivery to NSA they, and the first applications, programs, were skeletons to be filled in over time.[140]

(~~C~~) The software was impressive, however. HOPS was one of the first sophisticated operating systems. Alpha was also ahead of its time. And the routines that gave easy access to the data in Tractor were innovative.

(~~TS~~) But the clever NSA software designers could not achieve one valued and expected goal for Harvest, multiprogramming. Harvest was unable to run more than one program at a time. Other frustrations arose when it was realized that Stretch could not run while the "bump" was in operation and that programming for the "bump" could not be turned over to nonspecialists.[141]

(~~TS~~) While the software project was being organized, Harvest's critics intensified their protests. Howard Engstrom and SAB members continued to be worried about IBM's ability to produce a functioning machine, but they were more upset by IBM's power to convince the Agency to allow the company to go its own way while it was working on NSA's problems. The stipulation that NSA approve the design changes was not always, perhaps rarely, followed. The Agency critics wondered if NSA would get an NSA computer, or one that suited the needs of IBM.[142]

(~~TS~~) The Harvest situation reached a crisis point in 1960. Since Harvest's beginnings, the SAB had been concerned that IBM would not follow its request to make Harvest, the special architecture Farmer computer. When the cost overrun and contractual problems aggravated an already tense relationship between the board and the operating cryptanalysts, when SAB was informed that Harvest's software would be sparse, and when it was told that the machine might have to be only a stopgap "transition to Lightning," the SAB became suspicious. When it learned of the details of IBM's program management, SAB decided to review the project.[143]

(~~TS~~) One source of SAB's concern may have been a young Agency engineer assigned to watch over Harvest's development in New York. He endangered his career by writing to the Agency in March 1959:[144]

"The situation here is now in a bit of an enigma. On the one hand the agency would like to make absolutely sure that the equipment which it requested will 1) accomplish the job desired, 2) work at the speed indicated, 3) make the most efficient use of components, 4) be as reliable as possible, 5) cost as little as possible, and 6) be delivered on the date indicated.

"On the other hand IBM desires chiefly that only item 6 and possibly item 5 be satisfied. Only as long as items 1,2,3, and 4 are consistent with these goals they [*sic*] will be considered.

"To guarantee any of items 1, 2, 3, 4 or 5, the agency must evaluate the design prior to construction. IBM cannot furnish information for this purpose. They cannot because their delivery date is predicated on designing while constructing.....

"IBM has so scheduled things and has kept its cards so close to its chest that it will be impossible to stem the tide. Any design evaluation will cause delay. Delay will cost the agency money and computing time out of all proportion to the savings. This is chiefly because the IBM machinery is going too fast to stop.... As usual the agency has a firm hold on the IBM leash and is being dragged down the street. It is this reporters [*sic*] view that if you want to control an R/D contract you should pick a company other than IBM. If you pick IBM sit back and wait to get something like the equipment you ordered at a premium price. Don't try to direct, you're only kidding yourself if you do."

~~(S)~~ The Scientific Advisory Board demanded an accounting. They created a special committee in 1960. The Harvest program was so important that the "greats" of American cryptanalysis, Joseph Wenger and William F. Friedman, were asked to head that blue ribbon panel.[145] Their selection reflects a search for balance. Wenger was noted for his sponsorship of "science" within the Agency; Friedman was the illustrious advocate of in-house cryptanalytic work. Although they had different perspectives, they agreed that Harvest was far short of expectations.[146]

~~(S)~~ The Wenger-Friedman report endangered NSA's research/development efforts. The report might not lead to Harvest's cancellation, but it could make additional large-scale projects unlikely. Samuel S. Snyder, who had been in charge of the Agency's Harvest group, was put in the uncomfortable position of having to rush to the defense of the machine and IBM. He met with the two "greats" and assured them of Harvest's potential to be a Farmer-architecture machine. He then insisted that IBM had done an adequate job of ensuring that Harvest would be reliable. Snyder cited the many internal error-checking systems in the machine and the effort that had gone into the quality control system for components.

(U) Snyder then asked the panel to reconsider its conclusion about the difference between initial promises of Harvest's speed and what was being reported in the late 1950s. He asked them to realize that until there had been enough time to develop sophisticated software, Harvest could not measure up to its true potential.[147]

(U) It was Snyder's persuasiveness, combined with the fact that the Agency had already invested too much to abandon IBM that led to a continuation of the existing Harvest program. There was another reason. In the context of the expenditures on the Cold War, Harvest's price was minute.

~~(TS//SI)~~ The radar early-warning computers IBM was building had a near $1,000,000,000 budget. A single B-52 bomber cost as much as the Stretch component of Harvest, and hundreds of them were being built.[148] Even the new NSA electronic communications systems, including CRITICOM to inform the president in emergency situations, were minor investments compared to the billions poured into the missile and space programs of the era.[149]

~~(TS//SI)~~ But there was something else that few knew about that may have allowed the Agency to go its own way and continue with Lightning, Harvest, and in-house work on the high-level Soviet problem. Something cloaked in the greatest secrecy was going on in the Agency. A hope with the name "Hairline" was shifting power back into the hands of the "insiders."

(U) ERA's and the Shop-floor Cryppies' Revenge

~~(TS//SI)~~ While SAB considered the merits of the high-tech and high-science aspects of Harvest and Freehand, Jack Holtwick was lobbying for $17,000,000 to purchase stock computers for the extension of the ongoing attack on the Soviet problem; five years of dogged work by NSA and British shop-floor cryptanalysts blossomed into what appeared to be a major coup.[150] In late 1956 the Agency "insiders" seemed vindicated.

~~(TS//SI)~~ By early 1957 the existence of two significant "bust" conditions [redacted] had been confirmed. There was a belief that their exploitation would yield much information and lead to a pure solution. Then the rest of the [redacted] machines would be penetrated.

~~(TS//SI)~~ Immediately an in-house oversight group was formed: Ray Bowman, Leo Lathrom, and Marge Haworth took charge. Then Dale Marston was asked to establish the managerial framework for a machine and processing complex for Hairline. Few others, especially outsiders,

were told of Hairline. It was a secret within a secret.

(~~TS//SI~~) While the Freehand and Harvest projects waited, Hairline took off. Designers were set to work on six new and advanced special-purpose machines. They had to be advanced. Just one of the searches for the bust conditions called for 638,073,495,557,089,200 tests.[151] By mid-1957 three designs were ready. The machines were architecturally innovative. They had to be. Because the Hairline machines were needed immediately, they had to use existing technologies, slow ones. To compensate, the designers made imaginative uses of parallelism and multiple memories. Even analog circuits were employed to generate ultra-high-speed processing from old technologies.[152]

(~~TS//SI~~) The group turned to IBM to take over some of the detailing. There were thoughts of having IBM build all the Hairline machines. But as Hairline grew in size and importance, consultants from other companies were called in. John Howard, then an executive with Burroughs, helped, as did engineers from Sperry-Rand and Magnavox.[153] Then, when the original plan to have IBM construct the entire series of machines was dropped, the other firms were asked to do more than give technical advice.[154]

(~~TS//SI~~) By 1958 it seemed that the NSA was about to reenter the world of heroic cryptanalysis. The Agency and its crew needed such a belief because NSA failed to predict the launch of Sputnik in October. That Russian satellite, the world's first, did more than embarrass America's Big Science establishment. Sputnik proved that the Soviet Union could launch massively destructive missiles against the United States. America required high-level intelligence more than ever, and it needed it instantly.

(~~TS//SI~~) Perhaps that is why the November request to the Department of Defense for a special allocation of $20,000,000 for the first three years of the Hairline machine program received a quick and positive response. Told that "recent technical successes have resulted in the cryptanalytic reconstruction of a [redacted] machine cipher," which will make it "possible to read approximately 11,000,000 words per month," the Department of Defense could not resist. When it was informed that the CIA had agreed to help in the work, the project was even more attractive.[155]

(~~TS//SI~~) Hairline had to be made operational immediately. Luckily, NSA found a devoted industrial ally to help do that.[156] In a sense, it was a very old one, although it was a start-up company. Nineteen fifty-seven saw the rebirth of an "ERA" in St. Paul. One of the ex- "G" officers who had stayed on at the Minnesota plant after Remington-Rand bought ERA, William C. Norris, led a large contingent of frustrated engineers out of Sperry-Rand. They formed the Control Data Corporation. CDC was small but innovative and filled with men who had worked on military, even OP-20-G projects. They knew what cryptanalysts needed and how to conduct secret projects.

(~~TS//SI~~) The CDC group had been frustrated by the poor cousin treatment they had received from Sperry-Rand. Brilliant engineers like Seymour Cray had not been allowed to turn their advanced ideas into products. Unknown to IBM, they had developed, on a slim budget, a super-fast and rugged circuit design they wanted to use as the heart of a supercomputer. The circuit ran at 2.5 megahertz, a speed IBM was trying to attain through massive expenditures. Soon the CDC circuits ran at 10 meg.

(~~TS//SI~~) That circuit impressed the engineers at NSA who had been trying out an advanced twist on Farmer since the mid-1950s. The goal of their farsighted Dervish project was to create sets of functional circuits, each to be built using the latest miniaturized components. With the circuits being compatible, it was hoped that entire SPDs could be "assembled" rather than handwired.

That would allow NSA's own engineers to build Farmer machines in-house and to do so within months, not years. The Agency engineers achieved their goal in the 1960s. Using the CDC circuit as a model, they created their CADY cards and were able to build twenty-one very effective SPDs with them during the 1960s.[157]

(~~TS//SI~~) CDC's contributions went far, far beyond CADY. The computers they had in mind, what became the CDC 1604 and its grander follow-ons of the early 1960s, the 3000 and 6000 series, used very sophisticated architectural ideas. They led the company to become the world's leading supercomputer manufacturer of the 1960s and 1970s. Its smaller 160 also cut a path into what became the minicomputer market.

(~~S~~) CDC's achievements angered Tom Watson. How could a handful of engineers "and a janitor," he asked, be able to accomplish what IBM's teams of hundreds could not achieve? He may have been angered by something else: CDC became a favorite of the science-oriented men at NSA and a long-term partner of its special-purpose machine group, one which demanded and financed the development and use of cutting-edge technology and advanced architecture.[158]

(~~TS//SI~~) As in the days of ERA, CDC had its secret rooms where the world's most advanced computer work was done by engineers with the highest security clearances. The intimate NSA relationship with CDC lasted unbroken for a decade.

(~~TS~~) While it would supply NSA with its number-crunching supercomputers of the 1960s, the Hairline project was at the center of CDC's 1960s crypto-machine work. Some of the machines it created for the Soviet attack were works of engineering art. Welcher, Coiner, Pullman, Coleman, and Rudolph cost millions of dollars, but were worth it in terms of cryptanalytic power. Although some cost as much as one half the price of IBM's Stretch, they were twenty times as powerful.[159]

(~~TS~~) Using one of CDC's super-fast general-purpose computers, such as the 1604 or 3600, as the control and I/O for the special-purpose components, the Hairline machines remained in use and competitive with the latest commercial machines for more than a decade. NSA never got its modern Farmer, which could easily link any number of special-purpose machines, but the CDC creations came close.

(~~TS//SI~~) As important for the Agency, CDC's projects went smoothly. The company seemed as devoted to the Agency as to its commercial interests. It always kept the Agency informed of its progress, and it delivered machines on time.

(~~TS//SI~~) But the other major computer companies played an early and important role in Hairline. The first of the [redacted] computers, the $900,000 Blueplate, was shipped from Sperry-Rand's (previously Remington-Rand's) St. Paul factory to the Agency in October 1958.[160]

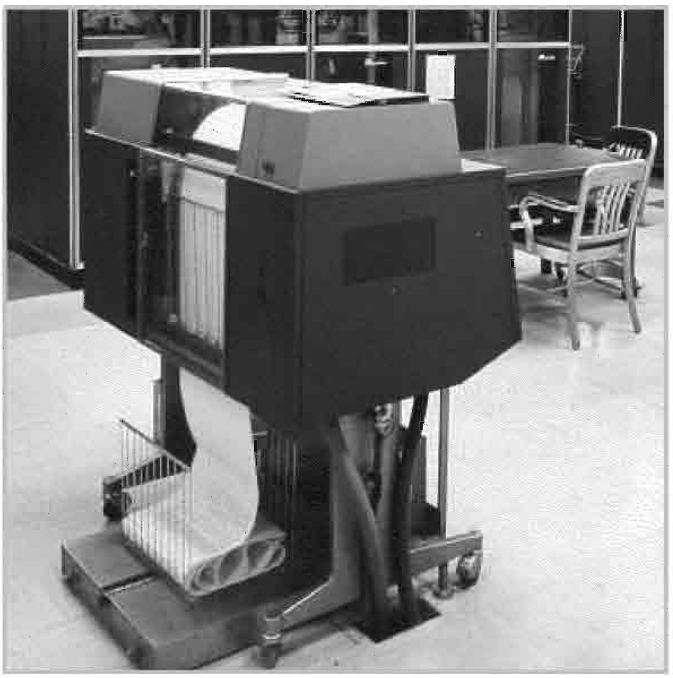
(~~TS//SI~~) Other machines followed. Sperry-Rand, CDC, and Burroughs built huge Hairline SPDS. One early Hairline machine, Haviland, cost almost $10,000,000. It and its sisters rivaled the supercomputers of the time in complexity and power and outpaced the best commercial computers of the 1960s and 1970s by factors of 1000.[161]

(~~TS//SI~~) IBM was asked to rejoin the special-purpose machine effort. In 1968 it delivered its impressive Aztek. Although only two-thirds the size of a Sperry-Rand SPD of 1965, its price tag reflected its power. It was the attempt to put Lightning's research to use.[162] Its high price brought great returns. Aztek did its particular job 2,400 times faster than IBM's commercial supercomputer of the era, the 7030 offshoot of Stretch.[163]

P.L. 86-36
EO 3.3(h)(2)

(U) Technology and Faith, 1962

(~~S~~) While Hairline was receiving its first set of machines, IBM delivered Harvest to NSA in February 1962 after its engineers overcame an unexpected and major problem. The critical special core memory for the machine had proven unworkable, and the Harvest project had almost come to a halt in mid-1960. It had taken additional millions and much creativity to find a substitute that could reach the speed IBM had promised.[164]



(U) Harvest

(~~TS//SI~~) Harvest's arrival meant that the mid-1950s faith in a technological solution could be tested. That faith had put the Agency's reputation on the line. NSA had convinced the government to invest more than $100,000,000 in special equipment and research to conquer the Soviet enciphering machines. That was twenty-five times what the World War II Bombes had cost. On top of those special investments, NSA had spent additional tens of millions of dollars on commercial computers. That included a copy of the startling CDC 1604 for IDA's mathematical explorations.

(~~TS//SI~~) More was going on. The IDA was beginning to lobby for access to real problems, and Britain was putting its Freehand machine to work against the Soviet ciphers. But no one was sure that the faith in technology and science would be sustained. Harvest's software had not had a chance to show its stuff, and Tractor had "bugs." Harvest's backers still had to prove that it would be the fastest and most powerful computer in the world.[165] The research portions of Freehand-Lightning showed promise, but also that some technological limits had been reached. Cryotrons proved stubborn, and thin-film technology, though still viable, was facing constraints. The IDA had not yet worked a methodological miracle and was just beginning to show how supercomputers could be integrated into day-to-day cryptanalysis.

(~~TS//SI~~) The Hairline system was yet to provide much. It was generating only a small percent of the traffic [redacted] While valuable, Silver's messages contained rather low-level information.

(~~TS//SI~~) There were some clear triumphs, however. NSA had continued its codebreaking victories over the codes and ciphers of nations other than those in the Communist bloc, reading at least [redacted] of the world's systems. And the Agency seemed to be creating valuable information on the Soviets through T/A, plain language, and ELINT.

P.L. 86-36
EO 3.3(h)(2)

~~(TS//SI)~~ But the high-level problem remained unsolved. The huge investments in Freehand, Hairline and Harvest had, as yet, failed to bring NSA into a new age of heroic cryptanalysis. Some results were badly needed if faith and investments in science and technology were to be maintained.

(U) Notes

1. (U) Thomas Johnson's *American Cryptology during the Cold War, 1945-1989* contains a valuable review of the numerous reviews and investigations of the Agency.

2. ~~(TS//SI)~~ Thomas Johnson's work is informative and ~~(TS)~~ NSA AHA ACC 28690, "NSA SAB Members and Minutes," 27 April 1954, is very useful.

3. (U) NSA CCH Series XII Z, Trish Gallagher, "Glimpse of a Man: The Life of Ralph J. Canine."

4. ~~(TS)~~ NSA CCH Series XII Z, DoD, Report of the Secretary's Ad Hoc Committee on COMINT/COMSEC, June 1958. (Robertson Report) The Robertson Report is housed in CCH Series VI.X.1.6.

5. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. (TS//SI) NSA CCH Series XII Z, BSA, "MPRO Tehnical Reports," circa 1956.

6. ~~(TS//SI)~~ NSA CCH Series XII Z, "Office of Computers, List of Computers," nd.

7. ~~(S)~~ NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964. The name Bogart was selected because it was the name of a well-known newspaper editor.

8. ~~(S)~~ NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964.

9. ~~(C)~~ NSA CCH Series XII Z, H. Campaigne, "Aristocrat: An Intelligence Test for Computers."

10. ~~(TS//SI)~~ NSA CCH Series XII Z, ADVA-13 "The HEXT 13ABS Diarization Program," 23 May 1960. ~~(TS)~~ NSA CCH Series XII Z, ADVA-13 Tech. Rpt, "The Devron-Pahala-Wyoming Mechanized Data Handling Complex," 23 May 1960. ~~(TS//SI)~~ NSA CCH Series XII Z, MPRO-11, "Reading Manual Morse on 13ABS Transmission Via Digital Computer, 16 December 1960.

11. ~~(S)~~ NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964.

12. ~~(S)~~ NSA CCH Series XII Z, SCAG Meeting of 6 December 1951.

13. ~~(TS)~~ NSA AHA ACC 28690, "Members of NSA Science, Electronic, and Mathematics Panels," circa 1953. ~~(TS)~~ NSA CCH Series XII Z, NSASAB, "Historical Study-Lightning-Freehand," circa 1963. ~~(C)~~ NSA AHA ACC 28690, "NSA SAB Members," April 1955.

14. ~~(TS//SI)~~ NSA AHA ACC 46406, "Recommendation for a Full-Scale Attack on Russian High Level Systems," 2 May 1956.

15. ~~(TS)~~ NSA CCH Series XI K, S. Snyder, Diary of Samuel S. Snyder, 29 October 1957.

16. (U) Canine had tried to build an SPD construction branch within the Agency that was large enough to do all of its own work, but Congress favored a system of contracting out to commercial manufacturers.

17. ~~(TS//SI)~~ NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase III: Third Addition," 1 November 1956.

18. (U) Thomas Johnson's *American Cryptology during the Cold War, 1945-1989* covers these points.

19. ~~(TS)~~ NSA AHA ACC 28690, "NSASAB Members and Minutes," 27 April 1954.

20. (U) The Hoover and Killian recommendations were, to a very great extent, affirmed in a third mid-1950s review of NSA by William H. Jackson, who was "keeping an eye on the Agency" for President Eisenhower. See Thomas Johnson's *American Cryptology during the Cold War, 1945-1989*.

21. (U) He had financed the successor to Howard Aiken's 1930s supercomputer in the mid-1940s. But that machine proved something of an embarrassment. His SSEC of 1948 had too many technological compromises and was soon regarded as a dinosaur. This experience may have led him to be wary of "machines before their time." Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 52.

22. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 132.

23. (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 45

24. (U) What is not explained in the documentation is why, after rejecting the UNIVAC machine in the late 1940s because it used "decimal" representation, the 702 was so well received at the Agency.

25. (TS) The NSA group knew of the TPM and found it attractive. When considering whether or not to acquire a 701, they were informed that the TPM development was lagging behind, and its production version (702) faced an indefinite birth date. (TS) NSA CCH Series XII Z, folder marked "Machine Reports 1951-1952." The 702 had an interesting feature, a bus architecture. With the bus acting as a transmission line, many separate units (ALUS) could be attached to the machine. Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 173. This architectural idea paralleled the "Farmer" concept that was developing within the Agency.

26. (TS) NSA CCH Series XII Z, folder marked, "Machine Reports 1951-1952."

27. (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964. (S) NSA CCH Series XI K Box 8, Snyder "Yearly Cost of Representative NSA Machines," May 1955.

28. (C) NSA CCH XI H, Box 12, NSA General-Purpose Computers, a list compiled by Samuel S. Snyder.

29. (TS) NSA CCH Series XII X-MPRO, U.S. Cryptanalytic Research and Development Committee, "Joint Long Term Program for Research and Development in the Field of Cryptanalytic Equipment," 21 July 1948. (TS//SI) NSA CCH Series XII Z, "File Kept by Dr. Campaigne on Ram Panel Meetings." (TS//SI) NSA CCH Series XII Z, "Communications Supplementary Activities, RAMP Report II," 21 December 1948." (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982. (TS//SI) NSA CCH Series XII Z, "Joint Long Term Program (Old Planning Material, 1948-1949)" compiled by Doug Hogan.

30. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982. (TS) NSA AHA ACC10842, Ray L. Bowman, "Engineering Diary," circa 1945-1950. Bowman's own ideas may have been reinforced after he learned of the [redacted] machine which, apparently, had an architecture quite like that advocated under the Farmer program. (S) NSA CCH Series XII Z, GCHQ, "List of Non-Hollerith X Department Machine Descriptions," 12 January 1953.

31. (S) NSA CCH Series XII Z, Ray Bowman, "Farmer," 5 April 1954. (TS//SI) (NOFORN) NSA AHA ACC 28690, "BSA SAB Minutes," April 1954. The project began in mid-1954

32. (U) Especially enlightening are (TS//SI) NSA CCH Series XII Z, "Report of Special Study Group on Analytic Requirements for Farmer-Nomad," 15 November 1954. (C) NSA CCH Series XII Z, "NSA SAB Subpanel on General Purpose Analytic Equipment," 7 March 1955. (TS//SI) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase III: Third Addition," 1 November 1956. (S) NSA CCH Series XII Z, "Farmer," S. Snyder 25 August 1955. (S) NSA CCH Series XII Z, "HARVEST as the Control Unit of the Farmer System." A fundamental difference between the typical computer and what NSA's men envisioned was its data flow. Most users had one data stream, but much of NSA's cryptanalytic work depended upon two streams. The old collator had proven so useful because it handled two flows, and the Abner streaming unit imitated many aspects of the collator.

33. (TS) NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. Dervish eventually led to the Cady building block components (which stemmed from the CDC work). On Bowman's plans. (S) NSA CCH Series XII Z, Ray Bowman, "Farmer," 5 April 1954. (S) NSA CCH Series XII Z, "General Plan for Farmer Program."

34. (TS//SI) NSA CCH Series XII Z, "Report of Special Study Group on Analytic Requirements for Farmer-Nomad," 15 November 1954.

35. (TS) NSA CCH Series XI K, S. Snyder, Diaries of Samuel S. Snyder, April 1954.

36. (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 73.

37. (TS) NSA CCH Series XI K, S. Snyder, Diaries of Samuel S. Snyder, April 1955.

38. (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 20.

39. (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 21.

40. (C) NSA AHA ACC 28690, "NSA SAB Members," April 1955. (TS//SI) (NOFORN) NSA AHA ACC 28690, "BSA SAB Minutes," April 1954.

41. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 418.

42. (U) The project began in mid-1954. NSA CCH Series XI K, S. Snyder, Diaries of Samuel S. Snyder, 2 March 1955 and 5 May 1955. (TS//SI//NF) NSA AHA ACC 28690, "BSA SAB Minutes," April 1954.

43. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 3 March 1955.

44. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 418, 424.

45. (U) James W. Cortada, *Historical Dictionary of Data Processing Technology* (New York: Greenwood Press, 1987), 246, 108.

46. (C) NSA CCH Series XI K, S. Snyder, "The Harvest Story," 5.

47. (S) Kullback wrote a long report outlining the critical processing needs at the Agency. (S) NSA CCH Series XII Z, S. Kullback, "The Increasing Complexity of the Analytic Equipment Program," 12 October 1955.

48. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 19 March 1955.

49. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, May 1955.

50. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 30 May 1955 and 22 August 1955.

51. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 7.

52. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 22 July 1955.

53. (S) NSA CCH Series XII Z, S. Kullback, "The Increasing Complexity of the Analytic Equipment Program," 12 October 1955.

54. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982. (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum, "Harvest Software," 19 June 1981. A useful article on Harvest is NSA CCH Series XI K, (U) Edward K. Yasaki, "Fastest in Its Time," (Stretch), Datamation, 28 (January 1982): 34-43.

55. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, August and September 1955. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 8.

56. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 10. On views of the "harvest" system, (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum, "Harvest Software," 19 June 1981.

57. (U) NSA CCH XI K Box 5 Samuel S. Snyder, folder, "Program Descriptions."

58. (U) George Cramer had been a navy mathematician, however.

59. (U) NSA CCH Personality File. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 12.

60. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 432.

61. (TS) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries 1 May 56. Kullback believed his directive to make it an Agency machine, rather than one to fit the commercial market, would be followed.

62. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February, 1982, 174.

63. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 183. (TS) NSA CCH Series XII Z, "Notes on Farmer." (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 15e.

64. (C) NSA CCH Series XII Z, "Farmer Plantation Definition and Objectives," 15 November 1956. At the same time that Tractor was being designed, the Agency was exploring the other mass memory devices of the era. Predating its acquisitions of automated microfilm and video mass memory systems, the microfilm Mini and Magnacard options were examined in the late 1950s. (S) NSA CCH Series XII Z, H. H. Campaigne, "Research at NSA," *NSA Technical Journal* (Spring 1968): 1. (S) NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965.

65. (TS//SI) NSA AHA ACC 36784, "Data Storage and Retrieval Symposium," 16-17 April 1959.

66. ~~(S)~~ NSA CCH Series XII Z, "HARVEST as the Control Unit of the Farmer System." ~~(S)~~ NSA CCH Series XII Z, Ray Bowman, "Farmer," 5 April 1954.

67. (~~S//SI~~) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982, 183. It is revealing to compare the 1955 Farmer outline by Samuel S. Snyder and the Harvest Report. ~~(S)~~ NSA CCH Series XII Z, "Farmer," S. Snyder 25 August 1955. The comparison shows that the Harvest group focused on a subset of the Farmer-recommended cryptanalytic tasks, the "scoring and testing" group.

68. (U) Note that later NSASAB panel reports, March 1955, did stress the ability to work on two sets of data at the character level. However, the report also emphasized the "ancillary units."

69. ~~(C)~~ NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 19.

70. ~~(C)~~ NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 19.

71. ~~(C)~~ NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 28.

72. ~~(C)~~ NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 30. (C) NSA CCH Series XII Z, "Harvest Farmer Costs."

73. (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum, "Harvest Software," 19 June 1981

74. ~~(S)~~ NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965. ~~(TS)~~ NSA CCH Series XII Z, "Abbreviated History of SCAG," February 1951-February 1952.

75. ~~(S)~~ NSA CCH Series XII Z, "Notes, Anne Brown Historical Study of NSASAB." ~~(TS)~~ NSA AHA ACC 28690, "Members of NSA Science, Electronic, and Mathematics Panels," circa 1953. ~~(S)~~ NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965.

76. ~~(S)~~ NSA CCH Series XII Z, "Notes, Anne Brown Historical Study of NSASAB."

77. ~~(C)~~ NSA CCH Series XII Z, "Some Recommendations for NSASAB Activities," 6 April 1961. ~~(S)~~ NSA CCH Series XII Z, "Notes, Anne Brown Historical Study of NSASAB." ~~(C)~~ NSA AHA ACC 36784, "Robertson Report," 31 May 1957.

78. (~~TS~~) NSA AHA ACC 28690, "NSA SAB Members and Minutes," 27 April 1954. (~~TS//SI~~) ~~(NOFORN)~~ NSA AHA ACC 28690, "BSA SAB Minutes," April 1954. ~~(C)~~ NSA AHA ACC 28690, "NSA SAB Members," April 1955. ~~(S)~~ NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956. (~~TS~~) NSA AHA ACC 28690, "Members of NSA Science, Electronic, and Mathematics Panels," circa 1953. (~~TS~~) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963.

79. (U) NSA CCH Personality file.

80. (~~TS~~) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 14 October 1857 shows other "science types" objected, as late as then, to giving IBM the Harvest contract. One reason was that it seemed to be turning Agency problems over to the corporation. Howard Engstrom pointed out in August that Harvest was so large that it threatened to eliminate many other projects in the Agency.

81. ~~(S)~~ NSA CCH Series XII Z, "Notes, Anne Brown Historical Study of NSASAB."

82. (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum, "Harvest Software," 19 June 1981.

83. ~~(S)~~ NSA CCH Series XII Z, H. Campaigne, "Lightning."

84. ~~(S)~~ NSA CCH Series XII Z, "SCAG Meeting of 6 December 1951." (~~TS~~) NSA CCH Series XIII Z, "Abbreviated History of SCAG," February 1951-February 1952. (~~TS//SI~~) NSA CCH Series XII Z, Notes from "First Annual Review of Group A Resources," 1962. (~~TS~~) NSA AHA ACC 28690, "Members of NSA Science, Electronic, and Mathematics Panels," circa 1953. (~~TS//SI~~) NSA AHA ACC 36784, "Data Storage and Retrieval Symposium," 16-17 April 1959. (~~TS~~) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963.

85. ~~(C)~~ NSA CCH Series XII Z, "NSA SAB Subpanel on General-Purpose Analytic Equipment," 7 March 1955. (~~TS//SI~~) NSA CCH Series XII Z, "The Accelerated Machine Program," 2 August 1955. (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of COMINT, Phase III - Third Addition," 1 November 1956.

86. (U) "Remarks at the Dedication of John von Neumann Hall," *NSA Technical Journal*, VI (Winter 1961): 1. (~~TS~~) NSA AHA ACC 42444, "Baker Panel: IDA established," 21 February 1958. (~~TS//SI~~) NSA CCH Series XII Z, "Mechanization in Support of

COMINT, Phase III - Third Addition," 1 November 1956.

87. (TS//SI) NSA AHA ACC 46406, "Recommendation for a Full Scale Attack on Russian High Level Systems," 2 May 1956.

88. (TS//SI) NSA CCH Series XII Z, "Lightning Research," nd.

89. (C) Holtwick's recommendation for the in-house initiative was oriented to a rather traditional search for a pure solution that included a subsidy of several million dollars for a computer for GC&CS. The machinery he asked for indicates that the Agency wanted a general solution and did not think the few busts they had found would ever provide valuable intelligence. For NSA he requested two 704s, three 705s, one Sled II, sixteen Audicos to convert incoming signals, eight Bogarts for editing, one special "Epicure," two high-speed Dervish machines, ninety small data conversion devices. (TS//SI) NSA AHA ACC 46406, "Recommendation for a Full-Scale Attack on Russian High Level Systems," 2 May 1956.

90. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956.

91. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956. NSA's "insiders," of course, had a role in formulating Freehand. OP-20-G's Jack Holtwick was central to the project. (TS//SI) NSA AHA ACC 46406, "Recommendation for a Full-Scale Attack on Russian High Level Systems," 2 May 1956. (TS//SI) NSA CCH Series XII Z, MPRO-03/4, "The Hairline Complex: Part 7, Coiner," Prepared by Richard W. Ader, 1 May 1960.

92. (TS) NSA AHA ACC 42444, "Lightning Program," 4 August 1958.

93. (TS//SI) NSA CCH Series XII Z, "Lightning Research," nd. Project Lightning gained their and the president's approval in early 1958 and in late 1957 Canine could state that the secretary of defense had already agreed to the proposals in principle. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956.

94. (TS//SI) NSA AHA ACC 46406, "Recommendation for a Full Scale Attack on Russian High Level Systems," 2 May 1956 shows how much the in-house group counted on the high-speed machine and how all of Freehand was shaped by the Soviet problem.

95. (TS) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963. On the details of the request for the in-house capability, see Holtwick, (TS//SI) NSA AHA ACC 46406, "Recommendation for a Full Scale Attack on Russian High Level Systems," 2 May 1956. He asked for some $17,000,000 in new computers, mainly to search for busts. He asked for 900 new workers. The list of computers Holtwick desired included many needed just to turn the complex intercepts of Soviet machines into forms useful in computer analysis.

Holtwick Requested:

2	704 or Atlas 2
3	705
1	Sled II
16	Audico
8	Bogart
1	Epicure
2	Dervish
90	Data Conversion ($300 each)

96. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956. (TS//SI) NSA AHA ACC 46406, "Recommendation for a Full Scale Attack on Russian High Level Systems," 2 May 1956. (TS) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963. There was a difference between the Manhattan-Parallel proposal, which was aimed specifically at the Soviet scrambler problem and the board's plan for a mathematical research center. See (TS) NSA AHA ACC 42444, "Baker Panel: IDA established," 21 February 1958. (C) NSA AHA ACC 36784, "Robertson Report," 31 May 1957.

97. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956.

98. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956.

99. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956.

100. (S) NSA AHA ACC 28690, "NSA Science Advisory Panel Minutes," October 1956.

101. (TS) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963. (TS) NSA CCH Series XII Z, DoD, Report of the

Secretary's Ad Hoc Committee on COMINT/COMSEC, June 1958. (Robertson Report)

102. ~~(C)~~ The office to centralize basic research, DARPA, was established in February 1958. Even before then the services discouraged subdivisions from subsidizing oftentimes-redundant investigations. The ONR's origins are connected to such motives.

103. ~~(TS//SI)~~ NSA CCH Series XII Z, "Lightning Research," nd. (~~TS//SI~~) NSA AHA ACC 46406, "Recommendation for a Full Scale Attack on Russian High Level Systems," 2 May 1956.

104. ~~(TS//SI)~~ NSA AHA ACC 46406, "Recommendation for a Full Scale Attack on Russian High Level Systems," 2 May 1956.

105. ~~(TS)~~ NSA AHA ACC 42444, "Lightning Program," 4 August 1958.

106. (~~TS//SI~~) NSA CCH Interview with Louis Tordella.

107. ~~(TS//SI)~~ NSA CCH Series XII Z, "Lightning Research," nd. Canine was informed that the five-years project would not yield a "1,000" machine, but he still aimed at major accomplishments. "...it is very important that everyone realize that the ultimate goal is a kilomegacycle computer, circuit limitations due to the speed of light notwithstanding."

108. ~~(TS//SI)~~ NSA CCH Series XII Z, "Lightning Research," nd.

109. (~~TS//SI~~) NSA CCH Series XII Z, "Lightning Research," nd., 19.

110. (~~TS//SI~~) NSA CCH Series XII Z, "Lightning Research," nd., 19. (S) NSA CCH Series XII Z, H. Campaigne, "Lightning," 54.

111. ~~(S)~~ NSA CCH Series XII Z, H. Campaigne, "Lightning." (U) Stan Augarten, *Bit by Bit: An Illustrated History of Computers* (New York: Ticknoir and Fields, 1984), 259.

112. ~~(TS)~~ NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963, 28.

113. (~~TS~~) NSA AHA ACC 42444, "HAIRLINE," 1958, 6.

114. ~~(TS)~~ A few years before and shortly after Lightning began, the Agency tried to combine cryotrons with the need for an "associative" memory, one that did not use formal addresses and that could test for near as well as exact matches. The projects at A. D. Little and General Electric were not operational successes. ~~(TS)~~ NSA CCH Series XII Z, "General and Special-Purpose Computers: A Historical Look and Some Lessons Learned," 23 May 1986. (Hogan)

115. ~~(S)~~ NSA CCH Series XII Z, H. Campaigne, "Lightning."

116. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 457. Points out that the Agency later supported very advanced thin film work at Texas Instruments.

117. ~~(TS//SI)~~ Leroy Wheatley "Content Addressed Memories," *NSA Technical Journal* IX (Winter 1964): 63. ~~(S)~~ NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965.

118. ~~(S)~~ NSA AHA ACC 36787, "A Summary of NSA Response to Recommendations of the 1957 Mathematics Panel Report," 18 February 1960, 119. ~~(S)~~ NSA CCH Series XII Z, "The Origins and Development of the NSASAB," 1 June 1965. ~~(TS)~~ NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963. ~~(TS)~~ NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 28 October 1957.

120. (~~TS~~) NSA CCH Series XI K, S. Snyder, Samuel S. Snyder Diaries, 26 October 1957.

121. ~~(S)~~ NSA CCH Series XII Z, "EDP Panel Minutes," September 1959-September 1965.

122. (~~TS~~) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963.

123. ~~(S)~~ NSA CCH Series XII Z, Cryptologic Milestones on, NSA-IDA, SIGINT Communications Systems, ACRP. (~~TS Laconic~~) "A History of IDA-CRD," by Richard Leibler.

124. (~~TS~~) NSA AHA ACC 42444, "Lightning and Hairline," 21 February 1958. The CRD would develop one of the first advanced operating systems for interactive computing. Its IDASYS was a result of its being the first to obtain a CDC supercomputer and to having a very creative programming expert as a visiting scholar.

125. (~~TS Laconic~~) "A History of IDA-CRD," by Richard Leibler. ~~(TS)~~ NSA AHA ACC 42444, "Baker Panel: IDA established," 21 February 1958. ~~(TS)~~ NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963. ~~(S)~~ NSA CCH Series XII Z, "Report of the NSASAB Committee on Item 12,"

4 February 1965. (U) NSA CCH Series XII Z, S. S. Snyder, "Memorandum for Dr. Kullback-Harvest," 30 November 1960. For an insight into the problems of the early years, (S) NSA AHA ACC 36787, "A Summary of NSA Response to Recommendations of the 1957 Mathematics Panel Report," 18 February 1960. In a December 1994 interview with Richard A. Leibler at the CCH, he stated that it was some years before the Agency agreed to send any real problems to the Princeton group. It took a major confrontation before the Agency released any [redacted] or Soviet problems to the CRD.

126. (U//FOUO) Interviews with Richard Liebler, at CCH, December 1994.

127. (U) IBM also maintained the old site in Vestal, New York, which was constructing advanced SPDs such as Sled II and Parson IV. The relationship of Vestal to Mohansic and why there were two NSA centers within the corporation remained unexplained. (TS//SI) NSA CCH Series XII Z, "Office of Computers, List of Computers," nd. Also important is Vestal's use of the Farmer approach of having building blocks of functional circuits as the basis for its mid-1950s devices.

128. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982.

129. (TS) NSA CCH Series XII Z, "Notes on Farmer." (TS//SI) NSA CCH Series XII Z, "Lightning Research," nd.

130. (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General Purpose Electronic Digital Computers*, 1964.

131. (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum, "Harvest Software," 19 June 1981, 10.

132. (U) In the late 1950s the Agency was in the forefront of exploring new database management ideas. See, for example, the NSA symposium held in 1959, (TS//SI) NSA AHA ACC 36784, "Data Storage and Retrieval Symposium," 16-17 April 1959. On Tractor designs, (S) NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964.

133. (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum, "Harvest Software," 19 June 1981, 14.

134. (U) Engstrom left one meeting in protest when the IBM representative declared that all that would be revealed would be "company confidential." Engstrom also argued against the major Harvest contract in a meeting with the director, General Samford. Others had similar feelings, (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 36.

135. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 32-3.

136. (U) NSA AHA CCH Series XI K, S. Snyder, Box 16, HARVEST Financial Summary.

137. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 33.

138. (U) NSA CCH Series XII Z, Interview with Dr. Joseph Blum,"Harvest Software," 19 June 1981.

139. NSA AHA CCH Series XI K, S. Snyder, Box 16, Harvest Financial Summary.

140. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story, Software."

141. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story, Software," 9. (S) NSA CCH Series XII Z, "EDP Panel Minutes," September 1959-September 1965. (TS) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963. (TS//SI) NSA CCH Series XII Z, "NSASAB Meeting," 19-20 May 1960.

142. (C) NSA CCH Series XI K, Sam Snyder, "The Harvest Story," 32.

143. (U) NSA CCH Series XII Z, S. S. Snyder, "Memorandum for Dr. Kullback–Harvest," 30 November 1960. (S) NSA CCH Series XII Z, "EDP Panel Minutes," September 1959-September 1965. (TS//SI) NSA CCH Series XII Z, "NSASAB Meeting," 19-20 May 1960.

144. (TS) AHA CCH Series XI K, S. Snyder, "Harvest Memo," Donald M. Rickerson to S. S. Snyder, 13 March 1959. (S//SI) NSA CCH Series XII Z, Oral History Interview OH 04-82 with Samuel S. Snyder, 24 February 1982.

145. (S) NSA CCH Series XII Z, Ware on NSASAB Mathematics Panel, 9 January 1967. (TS) NSA CCH Series XII Z, NSASAB, "Historical Study: Lightning-Freehand," circa 1963.

146. (U) NSA CCH Series XII Z, S. S. Snyder, "Memorandum for Dr. Kullback-Harvest," 30 November 1960.

147. (U) NSA CCH Series XII Z, S. S. Snyder, "Memorandum for Dr. Kullback-Harvest," 30 November 1960.

148. (U) Marcelle Size Knaack, *Encyclopedia of U.S. Air Force Aircraft and Missile Systems*, vol II, "Post-World War II Bombers 1945-1973" (Washington: Office of Air Force History, 1988).

149. ~~(S)~~ B. Peters and C. Palmer, "RYE, An Extended Capacity Remote Access System," *NSA Technical Journal* IX (May 1964): 77. ~~(TS//SI)~~ NSA CCH Series XII Z, ADVA-04, "Survey of Prod Analytic Requirements for Mechanizing Baud-Based Operations," 11 May 1961. ~~(S)~~ NSA CCH Series XII Z, NSA Historian P2217 Historical Study: NSA's Telecommunications Problems, 1952-1968, July 1969.

150. ~~(TS)~~ NSA CCH Series XII Z, Edward F. Miller, "Informal Note on Early Special Purpose Devices Built at Control Data Corporation," July 1993. Some three percent of the traffic of the [redacted] machine was being exploited by late 1957. ~~(TS Laconic)~~ "A History of IDA-CRD," by Richard Leibler.

151. ~~(TS//SI)~~ NSA CCH Series XII Z, MPRO-203, "The Hairline Complex: Part II, The Cipher Machine," Prepared by James L. Sapp, 17 May 1960.

152. ~~(TS//SI)~~ NSA CCH Series XII Z, "The Shearman Complex: Part VII," Prepared by James L. Sapp, C425, circa 1960. ~~(TS//SI)~~ NSA CCH Series XII Z, MPRO-03/4, "The Hairline Complex: Part 7, Coiner," Prepared by Richard W. Ader, 1 May 1960. ~~(TS//SI)~~ NSA CCH Series XII Z, MPRO-203, "The Hairline Complex: Part II, The Cipher Machine," Prepared by James L. Sapp, 17 May 1960. ~~(TS//SI)~~ NSA CCH Series XII Z MPRO-203, "The Hairline Complex: Part III Clip Pin," Prepared by James L Sapp, 17 May 1960.

153. ~~(TS//SI)~~ NSA AHA ACC 42444 "Special and Emergency Funding of NSA," (Russian high-level [redacted] circa November 1957.

154. ~~(TS//SI)~~ NSA CCH Series XII Z, Edward F. Miller, "Informal Note on Early Special Purpose Devices Built at Control Data Corporation," July 1993.

155. ~~(TS//SI)~~ NSA AHA ACC 42444 "Special and Emergency Funding of NSA," (Russian high-level [redacted] circa November 1957.

156. ~~(C)~~ NSA CCH Series XII Z, Herbert W. Worden, "EDP Machine History," suggests that CDC displaced Technitrol and other computer companies at this time for special-purpose orders. Orders from IBM for special-purpose machines declined, but it received a massive contract for the huge and very secret Aztek computer, the embodiment of much Lightning research. ~~(TS//SI) (Laconic, Nocon)~~ NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985.

157. ~~(TS//SI)~~ NSA CCH Series XII Z, LeRoy H. Wheatley, "Cryptanalytic Machines in NSA," 30 May 1953, and various years. ~~(TS//SI)~~ ~~(Laconic, Nocon)~~ NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985. ~~(TS//SI)~~ Leroy Wheatley "Content Addressed Memories," *NSA Technical Journal* IX (Winter 1964), 63. ~~(TS//SI)~~ NSA CCH Series XII Z, "Crossland." ~~(TS)~~ NSA CCH Series XII Z (Library s185024), "Hembree."

158. ~~(C)~~ Edward S. Miller of NSA kept a scroll listing all the larger Agency SPD projects. It shows how important CDC was to the Agency for more than two decades. See NSA CCH Series XII Z, "Miller Scroll."

159. ~~(TS)~~ NSA CCH Series XII Z, Edward F. Miller, "Informal Note on Early Special-Purpose Devices Built at Control Data Corporation," July 1993. (C) NSA CCH Series XII Z, Herbert W. Worden, "EDP Machine History."

160. ~~(TS//SI)~~ NSA CCH Series XII Z, "The Shearman Complex: Part VII," Prepared by James L. Sapp, C425, circa 1960. ~~(TS//SI)~~ NSA CCH Series XII Z, MPRO-03/4, "The Hairline Complex: Part 7, Coiner," Prepared by Richard W. Ader, 1 May 1960.

161. ~~(TS)~~ NSA AHA ACC 42444, "HAIRLINE, funding," 1 December 1960 shows the request for additional Hairline funds for $1,300,000 to complete the largest of the early machines, Haviland.

162. (U) Interview with Mr. Ray Miller of NSA, January 1994.

163. ~~(TS//SI) (Laconic, Nocon)~~ NSA CCH Series XII Z, Glenn F. Stahly, "Fifty Years of Mathematical Cryptanalysis," August 1985, 75-6.

164. ~~(S)~~ NSA Technical Literature Series, Monograph No. 2, *History of NSA General-Purpose Electronic Digital Computers*, 1964, 30.

P.L. 86-36
EO 3.3(h)(2)

165. (U) The direct commercial version of Stretch certainly did not meet its goals. It was only a bit more than one-half as powerful as expected. (U) Charles J. Bashe et al., *IBM's Early Computers* (Cambridge: The MIT Press, 1986), 373. Phillip Bochicchio remembers that Harvest's circuits were much slower than ten meg. Interview, December 1994.

~~(U//FOUO)~~ Colin Burke graduated from San Francisco State College. After spending almost twenty years as a professional musician, he obtained his Ph.D. in history from Washington University, St. Louis. For the last two decades he has been a professor at the University of Maryland, Baltimore County. He has published in the fields of American social and demographic history, the history of higher education, quantitative methods in history, the history of computers, and the history of information and cryptanalysis. He was lucky enough to be the senior Fulbright scholar in Poland during the year Communism fell. Dr. Burke served as Scholar in Residence in NSA's Center for Cryptologic History from 1991 to 1992.

~~(U//FOUO)~~ The Center for Cryptologic History would like to extend its deepest appreciation to Mr. James L. Boyle, who edited and "fine-tuned" Dr. Burke's manuscript. Mr. Boyle served as a contractor on detail to the CCH Publications Team from October 1998 to February 2000.

This page intentionally left blank

(U) Index

EO 3.3(h)(2)
P.L. 86-36

This page intentionally left blank