

Imperial College London
Department of Computing

**Looking towards the future: the changing
nature of intrusive surveillance and technical
attacks against high-profile targets**

Jonathan Gudgeon

Supervised by Professor Chris Hankin

Submitted in part fulfilment of the requirements
for the degree of Doctor of Philosophy
November 2019

Abstract

In this thesis a novel Bayesian model is developed that is capable of predicting the probability of a range of eavesdropping techniques deployed, given an attacker's capability, opportunity and intent. Whilst limited attention by academia has focused on the cold war activities of Soviet bloc and Western allies' bugging of embassies, even less attention has been paid to the changing nature of the technology used for these eavesdropping events.

This thesis makes four contributions: through the analysis of technical eavesdropping events over the last century, technological innovation is shown to have enriched the eavesdropping opportunities for a range of capabilities. The entry barrier for effective eavesdropping is lowered, while for the well resourced eavesdropper, the requirement for close access has been replaced by remote access opportunities. A new way to consider eavesdropping methods is presented through the expert elicitation of capability and opportunity requirements for a range of present-day eavesdropping techniques. Eavesdropping technology is shown to have life-cycle stages with the technology exploited by different capabilities at different times. Three case studies illustrate that yesterday's secretive government method becomes today's commodity. The significance of the egress transmission path is considered too.

Finally, by using the expert elicitation information derived for capability, opportunity and life-cycle position, for a range of eavesdropping techniques, it is shown that it is possible to predict the probability of particular eavesdropping techniques being deployed. This novel Bayesian inferencing model enables scenarios with incomplete, uncertain or missing detail to be considered. The model is validated against the previously collated historic eavesdropping events. The development of this concept may be scaled with additional eavesdropping techniques to form the basis of a tool for security professionals or risk managers wishing to define eavesdropping threat advice or create eavesdropping policies based on the rigour of this technological study.

Acknowledgements

The completion of this study would not have been possible without the help and assistance of a number of people to whom I would like to express my sincere gratitude:

- To Professor Chris Hankin who has been my supervisor throughout the last five years of my part-time study. I am indebted to him for his unfailing support, understanding, constructive comments, advice and wise guidance, and without whom I would not have succeeded. I will be forever sincerely grateful;
- To Howard for his encouragement to begin this journey and the important introduction to my supervisor, and also Emeritus Professor Sir Peter Knight, for his support with this thesis;
- To David Parkins, at the UK National Authority for Counter-eavesdropping who sponsored my part-time research, and his office colleagues for dealing with practical matters;
- To all other individuals in the UK National Authority for Counter-eavesdropping. Without their participation, I could not have carried out this research and to whom I will remain ever grateful;
- To the Foreign & Commonwealth Office Services at Hanslope Park, particularly Rob Eason in Global Digital Technology. Thank you for your support and encouragement;
- I would like to thank and acknowledge BayesFusion, LLC for the academic licence granted for the use of GeNIe Modeler software used with this academic research;
- I feel truly honoured to have had the opportunity of being associated with Imperial College and the Institute for Security Science and Technology. As a part-time student, this university has made me feel very welcome. I would particularly like to mention Denise McGurk for her unfailing assistance and my fellow PhD student (now Dr) Helen Greenhough for her encouragement and always having the time to answer my questions;
- To my late parents Roy and Diana Gudgeon who will always live on in my heart;
- To my son Oliver, for his incredible and detailed proof reading;
- And finally, my utmost thanks to my wife Lisa for her love, unbelievable support and understanding over the last five years of this research (not to mention also proofreading this thesis). It was certainly not possible without you and I cannot fully express my gratitude to you.

Dedication

This thesis is dedicated to Lisa, Lewis and Oliver
who fill my life with joy

Copyright

The copyright of this thesis rests with the author. Unless otherwise indicated, its contents are licensed under a Creative Commons Attribution Non-Commercial No Derivatives licence (CC BY-NC-ND 4.0). Researchers are free to copy, distribute or transmit the thesis on the condition that they attribute it, that they do not use it for commercial purposes and that they do not alter, transform or build upon it. For any reuse or redistribution, researchers must make clear to others the licence terms of this work. Please seek permission from the copyright holder for uses of this work that are not included in this licence or permitted under UK Copyright Law.

Statement of Originality

I hereby declare that, except where specific reference is made to the work of others, the contents of this thesis are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This thesis is my own work unless referenced otherwise.

Furthermore, it should be noted that I am a serving officer of the Foreign & Commonwealth Office Services and that this thesis is written in my personal capacity.

Jonathan Gudgeon
November 2019

Contents

Abstract	i
Acknowledgements	iii
1 Introduction	1
1.1 Motivation and Objectives	1
1.2 Approach	2
1.3 Eavesdropping: an Historical Summary	3
2 Historical Technical Eavesdropping Events	8
2.1 Chapter Overview	8
2.2 Technical Eavesdropping Pre-Second World War	9
2.3 Technical Eavesdropping During the Cold War	17
2.4 Technical Eavesdropping - A Turning Point in Time	64
2.5 Chapter Discussion	86
3 Present-Day Intrusive Surveillance Techniques Research	92
3.1 Chapter Overview	92
3.2 Method	94

3.3	Results	95
3.4	Analysis	99
3.5	Chapter Discussion	126
4	Eavesdropping Technology Life Cycles	128
4.1	Chapter Overview	128
4.2	The Life Cycles of Eavesdropping Technologies	129
4.3	Eavesdropping Technologies Introduction Timeline	139
4.4	Eavesdropping Technology Evolution Case Studies	148
4.5	Chapter Discussion	159
5	Dealing with Uncertainty: Bayesian Predictive Model	162
5.1	Chapter Overview	162
5.2	Eavesdropping Technologies' Capability and Opportunity Requirements	168
5.3	Bayesian Modelling of Eavesdropping Capability, Opportunity and Intent	172
5.4	Chapter Discussion	187
6	The Changing Nature of Intrusive Surveillance and Summary	190
6.1	Chapter Overview	190
6.2	Macro-Environmental Factors	191
6.3	Contribution and Summary of Achievements	211
A	Copyrights	214

B Timeline of Eavesdropping Events 220

B.1 Events Derived from English Language Literature 220

B.2 Timeline of All Events Recorded 228

C Timelines and Technology Life Cycles 231

C.1 Timeline of Techniques First Seen 231

D Technology Life Cycles 239

D.1 Additional Technology Life Cycle Results 239

E Capability and Opportunity Plots 242

F Future Work 249

Bibliography 252

List of Tables

1.1	A short history of eavesdropping.	6
2.1	The long list of mobile telephone vulnerabilities.	70
2.2	Tailored Access Operations catalogue of technology attacks	71
3.1	Close access techniques identified by expert elicitation.	97
3.2	Remote access (stand-off) techniques identified by expert elicitation.	99
3.3	Types of product collected	100
3.4	Eavesdropping techniques identified matched to the category of users.	101
3.5	An analysis of all items entering and leaving a premises.	103
3.6	Eavesdropping techniques classified by access preparation.	104
3.7	Eavesdropping techniques classified by distance to target.	104
3.8	Eavesdropping techniques requiring insider access.	105
3.9	Eavesdropping techniques requiring adjacent property access.	106
3.10	Eavesdropping techniques requiring access less than a block away.	107
3.11	Eavesdropping techniques mountable remotely worldwide.	107
3.12	Distance to the listening post.	109
3.13	Eavesdropping egress paths by popularity.	112

3.14	Eavesdropping countermeasures employed.	113
3.15	Categorisation of eavesdropping countermeasures.	115
3.16	The eavesdropping techniques detectability.	116
3.17	The detection distance.	116
3.18	The eavesdropping techniques deniability.	117
3.19	Eavesdropping system complexity - group 1.	118
3.20	Eavesdropping system complexity - group 2.	119
3.21	Eavesdropping system complexity - group 3.	120
3.22	Eavesdropping system complexity - group 4.	120
3.23	Eavesdropping installation complexity.	121
3.24	Eavesdropping installation procurement.	121
3.25	Eavesdropping hardware or software.	122
3.26	Eavesdropping relative equipment cost.	122
3.27	Number of citizens affected.	123
3.28	Eavesdropping output collection.	124
3.29	Eavesdropping collection overview.	125
3.30	Eavesdropping collection processing.	125
4.1	Eavesdropping technology life cycle analysis.	134
4.2	Ordered life cycle timeline positions of eavesdropping technologies.	137
4.4	Year eavesdropping technology first seen.	141
4.5	Egress route considerations	145
4.6	Introduction year of major technologies.	146

4.7	The top ten daily uses of smartphones.	155
4.8	Mobile phone development and eavesdropping exploits.	157
5.1	Four Bayesian software packages considered.	168
5.2	The range values of egress methods	172
5.3	Node probability table prior indicators and values.	174
5.4	Types of eavesdropping techniques modelled.	176
5.5	Eavesdropping confusion matrix.	182
5.6	Bayesian model results table.	183
A.1	Images copyright of the author	214
A.2	Copyright permissions for images not produced by the author	216
B.1	SIGINT incidents in literature review.	220
B.2	Wired microphone incidents in literature review.	221
B.3	Radio microphone incidents in literature review.	222
B.4	Cypher incidents in literature review.	223
B.5	Photography incidents in literature review.	223
B.6	TEMPEST incidents in literature review.	224
B.7	Telephone incidents in literature review.	224
B.8	Covert entry incidents in literature review.	225
B.9	Tape recorder incidents in literature review.	225
B.10	Agent communications incidents in literature review.	225
B.11	Odd events worthy of mention from the literature review.	225

C.1	Eavesdropping year first seen 1900-1959.	235
C.2	Eavesdropping year first seen 1963-1984.	236
C.3	Eavesdropping year first seen 1985-2004.	237
C.4	Eavesdropping year first seen 2006-2014.	238
D.1	Timeline positions of eavesdropping technologies.	241
F.1	Eavesdropping techniques enabled by telephone line egress.	250
F.2	Eavesdropping techniques enabled by internet egress.	250
F.3	Eavesdropping techniques enabled by dedicated wiring egress.	250
F.4	Eavesdropping techniques enabled by physical access egress.	251
F.5	Eavesdropping techniques enabled by mobile telephony egress.	251
F.6	Eavesdropping techniques enabled by optical egress.	251
F.7	Eavesdropping techniques enabled by radio egress.	252
F.8	Eavesdropping techniques enabled by electromagnetic egress.	252

List of Figures

1.1	The Bayeux tapestry eavesdropper.	3
1.2	The former British Embassy in Moscow.	7
2.1	The Strowger 1891 rotary selector.	10
2.2	British Army portable telephone set D MkIII.	11
2.3	German WWI eavesdropping on telephones.	11
2.4	Mitrokhin's KGB archive.	13
2.5	View of the Moscow Kremlin from the former British Embassy in Moscow. . . .	17
2.6	The Great Seal cavity resonator.	19
2.7	Suspicious street lighting outside the Naval Attaché's office.	21
2.8	Floor plan of the Naval Attaché's office.	22
2.9	Northern European white tiled ceramic stove within the Naval Attaché's office. .	23
2.10	Three microphones discovered in 1959.	26
2.11	Close-up of the US embassy microphone discovered in 1964.	27
2.12	US embassy microphone discovered in 1964.	28
2.13	KGB "HEIIA" microphone used in the 1960s.	28
2.14	Microphone discovered in the late 1950s.	29

2.15 Lock-picking tools used by the Stasi.	35
2.16 The aerial in the chimney discovery.	36
2.17 Hidden electronics in Gunman.	37
2.18 An early commercial radio microphone.	40
2.19 A Russian six-battery 1970s woodblock transmitter.	41
2.20 A Russian ten-battery 1970s woodblock transmitter.	41
2.21 Early electronic transistor example from 1952.	41
2.22 The 1969 Bucharest shoe transmitter.	42
2.23 A CIA cocktail transmitter stick.	44
2.24 Russian-style Stasi radio microphones.	44
2.25 Radio microphone used by the Stasi.	45
2.26 Audio eavesdropping device made in the USA.	46
2.27 Telephone switch-hooks modified.	46
2.28 Switch-hook relay bypass	47
2.29 Soviet F21 miniature camera.	48
2.30 Stasi robot vollautomat star II.	49
2.31 Stasi telephone recording in operation.	50
2.32 Hidden Stasi camera within a tie.	51
2.33 Hidden Stasi microphone within a pen.	51
2.34 A selection of Stasi microphones on display in Leipzig.	52
2.35 A selection of Stasi microphones on display in Leipzig.	52
2.36 The CIA's CD-501 agent communication equipment.	55

2.37	Investigative journalist's public programme showing of Zircon.	58
2.38	Menwith Hill - secret American global satellite monitoring.	59
2.39	1970s Veroboard transmitter bugs.	61
2.40	The KGB gap jumper.	63
2.41	Simple battery-powered bug kit.	65
2.42	Results from a low-cost software defined receiver.	67
2.43	Online purchased GSM audio bug.	75
2.44	Light-weight system for Wi-Fi interception.	80
2.45	Wi-Fi monitoring equipment used against OPCW.	81
2.46	A summary of all eavesdropping events.	86
2.47	Distinct phases of eavesdropping in history.	86
2.48	The growth of internet users.	90
2.49	The growth of the mobile telephone subscriptions.	91
3.1	Eavesdropping system components.	99
3.2	The hierarchy of eavesdropping equipment.	102
3.3	Systems engineering approach to target analysis.	103
3.4	Close and remote eavesdropping victim numbers.	108
3.5	The trend towards remote access.	108
3.6	Overview of the electromagnetic egress spectrum.	113
3.7	Eavesdropping relative cost distribution.	123
4.1	Technology or product life cycle stages.	129
4.2	Technology life cycle phases of re-invention.	130

4.3	Intrusive surveillance technology life cycle.	131
4.4	Technology life cycle template.	134
4.5	Life cycle histogram of distribution.	138
4.6	Timeline of eavesdropping technology introduction in decades.	142
4.7	Eavesdropping technologies introduced.	143
4.8	Eavesdropping technologies year first seen.	144
4.9	General overview of technology inventions.	147
4.10	Five examples of technology life cycle stages.	148
4.11	The life cycle of illumination.	150
4.12	The Sabre transponder development.	151
4.13	The life cycle of TEMPEST.	153
4.14	The perfect eavesdropping system.	156
4.15	Mobile telephone development.	158
4.16	Eavesdropping life cycle ‘Inform/Exploit’.	160
5.1	Bayesian belief network for capability, opportunity and intent.	167
5.2	The Swiss Cheese layers of events alignment.	167
5.3	Capability and opportunity technique elicitation.	170
5.4	Examples of eavesdropping techniques plotted for capability and opportunity. . .	171
5.5	Tangible and intangible capability assets.	173
5.6	Fifteen example eavesdropping techniques modelled.	176
5.7	Bayesian opportunity modelling.	178
5.8	Bayesian intent modelling.	178

5.9	Bayesian prediction modelling.	180
5.10	Egress route to technique mapping.	186
5.11	Prediction when passive techniques are considered.	186
5.12	Prediction when active techniques are considered.	187
6.1	The sources of intelligence.	191
6.2	Urgency of requirement.	192
6.3	Examples of social media applications.	195
6.4	Data never sleeps.	196
6.5	Capability against year of introduction.	201
6.6	Capability against year of introduction.	202
6.7	Capability against year of introduction.	203
6.8	Indoor cellphone coverage in a rural area of the UK.	205
6.9	Worldwide GSM coverage map.	205
A.1	Permission to use copyright image	216
A.2	Permission to use copyright image	217
A.3	Permission to use copyright image	218
A.4	Permission to use copyright image	218
A.5	Permission to use copyright image	219
A.6	Request to use Fig. 6.1 on page 192 Credit (Gill and Phythian 2013).	219
B.1	Statistics from the literature review.	227
B.2	Eavesdropping events from circa 1900 to 1945.	228

B.3	Eavesdropping events from circa 1945 to 1995.	228
B.4	Eavesdropping events from circa 1995 to 2011.	229
B.5	Eavesdropping events from circa 2011 to 2019.	230
C.1	Eavesdropping technologies introduced.	231
C.2	Timeline of eavesdropping technology introduction.	233
C.3	Timeline cellphone development.	234
E.1	Capability against opportunity plots.	243
E.2	Capability against opportunity plots.	244
E.3	Capability against opportunity plots.	245
E.4	Capability against opportunity plots.	246
E.5	Capability against opportunity plots.	247
E.6	Capability against opportunity plots.	248

Chapter 1

Introduction

The changing nature of the technical threat to Information Assurance is such that high-profile organisations and their representational staff, while overseas, enjoy very little privacy and will continue to do so, so long as they employ security methods designed for the protection of paper assets.

Anecdotal evidence from exhibits from public spy museums (such as those in Washington, Berlin, Leipzig and Moscow), private museums and other similar collections, suggests that intrusive surveillance and technical attacks against the information of high-profile organisations and representational offices is likely to continue to change in nature due to a step change in surveillance techniques and technology.

1.1 Motivation and Objectives

Academic study of surveillance and the rise in ‘big data’ continues to be of interest to both academics and citizens alike. One category of citizen where surveillance is not just perceived, but is routinely experienced, is those of high-profile representatives whose activities are subject to monitoring and intense scrutiny. These representatives may be subjected to technical attacks which go way beyond those experienced by other citizens.

I am concerned that anecdotal analysis suggests a period of significant change in the nature of the technical threat to representatives overseas. There is a need to understand the evolving nature of technical threat in order to more scientifically define advice; which will in turn define policy, based on scientific and technological study.

This research sets out to understand the evolving nature of the technical threat. Understanding the changes that have taken place may suggest an improved security model in order to increase the Information Assurance of high-profile organisations and their representational staff into the future.

1.2 Approach

The approach is to research and analyse eavesdropping surveillance events available from literature and to research and analyse close and remote access eavesdropping technologies identified through expert elicitation.

The following research steps will form my approach:

- The analysis of past technical attacks often mounted against high-profile organisations and individuals for which data is available;
- The research of eavesdropping techniques and methodologies available to those with an aggressive stance towards high-profile organisations and their premises;
- The research of the changing nature of this technology and the life-cycles and building blocks of eavesdropping systems;
- The creation of an expert prediction system utilising a suitable computer modelling technique that is informed by capability and opportunity requirements derived from this research.

1.3 Eavesdropping: an Historical Summary

Intrusive Surveillance has a long history; the temptation and desire to eavesdrop is such a basic human instinct that we can safely presume it has been going on since the dawn of civilisation. The Persians, for instance, have a well known proverb *The walls have mice, and the mice have ears* and is said to date back to the third century BC. The Normans had a clear understanding of the value of intelligence in the run-up to their invasion of 1066: the Bayeux Tapestry depicts an eavesdropper listening behind a stylised stone column (See Figure 1.1). The term ‘eavesdropper’ itself appears first in the mid-fifteenth century, meaning someone who stood below the eaves of a building (protected from the ‘eaves drip’ of rain) in order to listen to what was being said within the walls. Eavesdropping was reportedly punishable by law as far back as Anglo-Saxon times, although the activity itself dates back to far older times.



Figure 1.1: The Normans had a clear understanding of the value of intelligence in the run-up to their invasion of 1066. Below the word LANT (in the heading) an eavesdropper is listening behind the stylised stone column.

Over the centuries the methods employed for eavesdropping have improved in their effectiveness, whenever new technologies have been devised. This is illustrated by examining Table 1.1.

Time	Event
Ancient history	The Greek tyrant Dionysius I of Syracuse (c. 432–367 BC) imprisoned his political opponents in a limestone cavern (called the ‘Ear of Dionysius’) that had perfect acoustics for overhearing them discussing plans and secrets.
11th century	The Bayeux Tapestry, which illustrates the events leading to the Norman invasion of Britain in 1066, includes an eavesdropper standing behind a stone column.
15th century	Liberton Tower, a stone-walled castle near Edinburgh, was built with a listening hole called a ‘luggie’ or ‘laird’s lug’ (‘lug’ is a dialect word for an ear). This small hole in the wall separating the hall from the north staircase was concealed by a hanging tapestry and enabled the laird to eavesdrop on his guests unobserved. Similar listening devices are to be found in several other Scottish castles of the period.
1930s	The Americans were aware that technical surveillance was being used by the Soviets at the U.S. Ambassador’s residence in Moscow. Guests were handed printed cards alerting them to the fact and warning them to be discreet with their conversations. Also, during the abdication crisis of King Edward VIII in 1936 the British Home Secretary gave instructions for monitoring the King’s telephone calls.
1940s	First discovery of an ‘illumination’ technique. In 1945 a delegation of Soviet Young Pioneers presented the American Ambassador in Moscow with a wooden replica of the Great Seal of the United States. In fact this decorative item was bugged with a microphone, one of the first devices to employ <i>passive resonant cavity</i> techniques to radiate signals. It was not discovered until 1952 when a Technical Security Countermeasures (TSCM) technician performing a radio sweep overheard conversations.

1950s	Relatively unsophisticated microphones were discovered in growing numbers in many diplomatic missions in eastern Europe. This coincided with the rapid escalation in the rhetoric and perceived threat of the Cold War.
1960s	Microphone attacks occur in many overseas residences and hotel rooms. The first detection techniques employed compasses to detect the large magnets used within the hidden microphones buried in the walls.
1970s	Improvements in transistor technology made the miniaturisation of radio transmitters feasible, leading to the widespread use of battery-powered hidden microphones.
1980s	The Americans were attacked in Moscow by trojan components installed virtually invisibly within IBM typewriters, which transmitted in bursts everything typed. The Americans codenamed this project Gunman. In the same decade analogue mobile telephone conversations were intercepted by hobbyists (an activity that achieved notoriety with the ‘Dianagate’ recordings of 1989).
1990s	Spy shops opened throughout the UK openly selling all manner of hidden radio transmitters placed within everyday objects. Several kit manufacturers produced ranges of items. This equipment was complemented by the widespread increase in radio scanner availability.
2000s	Russian-made equipment for decrypting GSM cellphone conversations became available to purchase on the open market. Hacking of mobile phone conversations was common. This later transpired to be the result of rogue journalists exploiting default pass-codes on mobile telephone-voicemail systems.
2010s	Wi-Fi tracking recording equipment is commonplace. Powerful hacking software permits vulnerabilities with Wi-Fi encryption to be monitored. Bluetooth systems in cars are exploited through poor configuration. Widespread availability of digital recorders enable the recording of audio and video in all manner of everyday items. Smartphone technology convergence has enabled a myriad of tracking, audio and video recording applications to become available.

2020s	ICT developments that make workers no longer desk-bound will simultaneously render users potentially more vulnerable to electronic eavesdropping, since this greater mobility will make it easier for cyber attackers to follow their targets wherever they may be. Micro-miniature bugging devices will be harder to detect, whilst equipment will become very vulnerable to ‘back door’ control by hostile interests.
-------	---

Table 1.1: A short history of eavesdropping over the centuries.

This work focuses on more modern times and eavesdropping by technological means. A rich source of early eavesdropping activity originates in literature spanning the Cold War against diplomatic missions and diplomatic staff posted behind the iron curtain. Diplomats overseas are often treated with suspicion and embassies act as intelligence bases and are often targets for local intelligence technical attacks (Herman 1998). It is widely reported that during the Cold War diplomatic embassies and their residences were bugged with microphones hidden in the walls and ceilings and the life of a diplomat would be under constant scrutiny from foreign intelligence services.

A posting to Moscow would be greeted with some trepidation; Sir Rodric Braithwaite, a past British Ambassador to Moscow summarised this well “When people ask us about life in Moscow, then and later, they always began with the same question: *“what was it like to be continuously observed and overheard by the KGB”*? It was indeed a constant part of our everyday life” (Braithwaite 2002).

My own first-hand experience too, obtained from a diplomatic posting to Moscow between 1988 to 1991, at the end of the Cold War, remains memorable. We assumed that our assigned diplomatic accommodation in Kutuzovsky Prospekt had been bugged and that our every movement in Moscow was monitored.

As Richard Aldrich states “bugging and other kinds of secret listening has the capacity to induce paranoia” (R. Aldrich 2011, p.3). And so it did; in early 1964 before his removal from

power, even Khrushchev himself had his telephone bugged by the KGB (Khrushchev 1988).

The former British Embassy, which remains today as the Ambassador's residence, is located in the Kharitononko Mansion located directly opposite the Kremlin on the other side of the Moskva river at 14 Sofiyskaya Naberezhnaya. The mansion celebrated its centenary with the publishing of a book dedicated to its history (Berton 1991). The mansion became the British Embassy in 1929 and the author, Kathleen Burton, writes "At the end of 1946 relations began to cool, reaching a very low point with the Berlin Blockade in 1948... Apart from occasional Foreign Ministry officials like Andrei Gromyko, Russians rarely came to the Embassy" (Berton 1991). They didn't need to; they knew almost every word that was spoken within the embassy (see Figure 1.2).

This sets the tone for early eavesdropping by technological means in unfriendly environments. Technology has however changed a great deal since these early microphone installations. The changing nature of the intrusive surveillance technology has provided constant challenges for privacy and information assurance. With the Edward Snowden leaks and revelations in 2013, the technology used for intrusive surveillance purposes appears to have reached new levels of sophistication and reach.



Figure 1.2: A night-time view of the former British Embassy in Moscow which was first bugged when vacated during the Second World War.

Chapter 2

Historical Technical Eavesdropping Events

2.1 Chapter Overview

This chapter researches intrusive surveillance events since the creation of electronic eavesdropping (which may better be referred to in the early days as more electrical than electronic) and some of the enabling technology trends behind these eavesdropping events.

In this chapter:

- Incidents are researched from early telephone monitoring, radio interception and wired microphone attacks against diplomatic targets, relating to the period 1891 to 1939;
- The proliferation of eavesdropping events and technology through the Second World War and the Cold War, from Soviet bloc and Western allies' microphone attacks, the transition to eavesdropping on communications equipment, and whole city populations, covering the period 1940 to 1990;
- The proliferation of eavesdropping events and the period of change from 1991 to 2019 when information technology becomes commonplace and highly portable;

- A conclusion and analysis of past technical attacks against high-profile organisations and individuals for which data is available.

This chapter is intended to consider the changing nature of intrusive surveillance technologies widely available and actively used against citizens by state security, investigative journalists, the commercial sector and enthusiastic hobbyists alike.

2.2 Technical Eavesdropping Pre-Second World War

This section relates to the period 1891 to 1939.

Non-technical surveillance occurred in 1906 within the British Foreign Mission to St.Petersburg (the Russian capital before the Bolshevik October 1917 revolution). The mission secretary Cecil Spring reported “For some time papers have been extracted from this embassy... The porter and other persons in connection with the embassy are in the pay of the police department and are also paid on delivery of papers” (Andrew and Gordievsky 1991, pp.28-29). The embassy safe and lockable filing cabinets’ principal purpose of protecting British information was completely negated when the British staff allowed the Russian embassy staff access to the keys. Copies of the keys were made in seconds when the opportunity arose by pressing the keys into soft wax which left a perfect impression. The impression facilitated the fabrication of a copy of the keys. Armed with their own set of keys the Russian staff were able to remove all the documents at night in order to be photographically copied.

2.2.1 Early Signals Intelligence

It would appear that we British were keeping a close eye on the new Soviet Government too. When the Soviets arrived in London in May 1920 for talks the British were the first to recognise this new Soviet Government. The British Government Code and Cypher School (GC&CS) were able to receive the wireless messages between Moscow and the Soviet Trade Delegation in Highgate, North London and decrypt most of the messages (Andrew 2009, p.144).

2.2.2 Strowger Telephone Switch

One of the earliest examples in the late nineteenth century of eavesdropping through technological means resulted in the invention of a key component of the automated telephone exchange. Almond Strowger was a Kansas City undertaker and was losing business to a rival. His rival's wife happened to be the town's manual telephone switchboard operator. As soon as a bereavement arose that required funeral services, the call was put through to her husband's parlour. Hubert states that as soon as commercial telephones were installed in Haven, Connecticut in 1878, individuals would eavesdrop to some extent (Hubert 1960). Manual switchboards provided no privacy and gave the opportunity for the operator to eavesdrop at will.

Strowger realised that by automating the telephone switchboard process it would enable people to call a business directly, cutting out the advantage of the other undertaker. Strowger's "rotary selector" was invented and formed the key component of an automated telephone exchange (Atherton 1988; Willder 1985). Strowger patented his rotary selector illustrated in Figure 2.1 in 1891 (Strowger 1891).

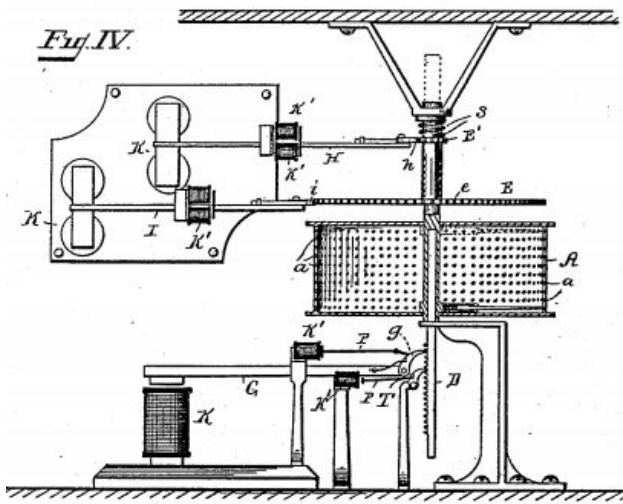


Figure 2.1: The Strowger 1891 patented rotary selector: the most important basic element of an automatic telephone exchange. Picture taken from the patent application.

2.2.3 First World War Trench Communication Intercepts

An early example of deliberate eavesdropping on telephone wires occurred during the First World War when telephone lines were laid out between front-line trenches. Both sides soon

discovered that the voice and morse code signals transmitted between trenches could be intercepted by laying out a long wire as close to the opposition as possible. These wires acted as an aerial that detected the poorly insulated signal which, through induction, could be detected as it leaked to earth.



Figure 2.2: British Army portable telephone set D MkIII. An example of the telephone the German soldiers could listen to on the front line in 1918, due to the compromising radiation from the telephone lines.

Figure 2.3 illustrates a rare photograph of German equipment in use in Bethincourt in France, at the time behind the German front line (The American Legion Monthly 1937).

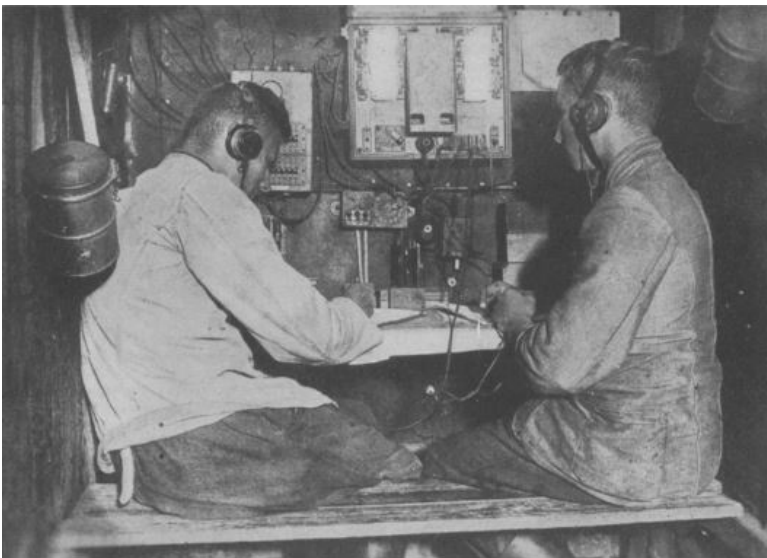


Figure 2.3: German soldiers listening into British Forces telephone conversations on the front line in 1918. Reprinted with permission of The American Legion Magazine, © March, 1937 www.legion.org.

British attempts were not at first as successful as those of the Germans. Matters improved modestly when in 1916 French listening sets were introduced, and four out of fifteen sets were intercepting German messages. The Signal Service historian reported that “...casualties suffered by their units were due to their own indiscreet use of the forward telephone” (Andrew 1985, p.138).

2.2.4 Telephone Tapping

In the 1930s the telephone lines of foreign embassies in London were being routinely monitored by a branch within MI6 called Section X. Professor Keith Jeffery, who was commissioned to write an authorised history of MI6, wrote that before the outbreak of the Second World War the embassies monitored included Germany, Spain, Italy, Japan and the USSR. “By 1938 the work had expanded so much that a P (or Press) Section was established to distribute the product” (Jeffery 2010, p.317). This was complemented by a secret department within the British Post Office who were having some success opening the diplomatic bags of the Italians, Japanese and Balkan embassies (Andrew 1985, p.384).

The British diplomat Henry Higman, who was posted to Chile in July 1941, felt that combining covert work with conventional diplomatic duties to be extremely risky and compromised the security of the embassy. In one case in 1941 in our embassy in Santiago “an elaborate telephone tapping operation was actually located in the British Embassy itself” (Jeffery 2010, p.463). Post-war MI6 used intercepted telegrams and telephone calls. The advantage stated “that we get from them the actual correspondence of foreign governments or their representatives” (Jeffery 2010, p.623).

Throughout the 1950s the Norwegian Intelligence Service tapped certain embassy telephone and telex lines from a bunker in the centre of Oslo and other offices with a focus on Soviet shipping agencies. Counter-espionage information was passed to the Security Police. Some interest was lost in the operation due to the hard work of transcribing all the tapes “in order to find out how many bottles of milk Ivanov should buy on his way home” (Riste 2014, p.31).

It is not difficult to imagine that British embassies were the subject of telephone tapping in many overseas capital cities, and likely remain so today.

2.2.5 Microphone Installations to the end of the Second World War

During a “Witness Seminar” entitled “The role of HM Embassy in Moscow” on the 8th March 1999 held in the Map Room at the Foreign and Commonwealth Office, London, the Russian defector Oleg Gordievsky reported “There were three attacks on the British Embassy: one was human, another technical (eavesdropping, observation, etc.) and the third - SIGINT (Soviet signals intelligence) - attack, the less successful one” (Staerck 2000).

Another Russian defector, Major Vasili Mitrokhin, was a KGB senior foreign intelligence archivist between 1972 and 1984. He defected to the UK in 1992 bringing with him his hand-written notes. With assistance from the MI5 historian, Professor Christopher Andrew, Mitrokhin produced two publications from his archive notes. In June 2000 his archive was the subject of a Parliamentary Intelligence and Security Committee Inquiry (Intelligence and Security Committee 2000) which stated that Mitrokhin’s archive led to 3,500 counter-intelligence reports which were passed to 36 countries. Mitrokhin’s archive is available on-line from Churchill College, Cambridge (Churchill Archive Centre 2016) and a page from the archive can be seen in Figure 2.4.



Figure 2.4: The late Major Vasiliy Mitrokhin and a page of his handwritten notes from his KGB archive. The archive is available to view at the Churchill Archives Centre, Cambridge University.

Mitrokhin’s archive is an important contribution to this Literature Review as it provides several examples of eavesdropping attacks, the majority of which are within his first publication “Sword

and the Shield” (Andrew and Mitrokhin 2000). Mitrokhin’s second publication “The KGB and the World” (Andrew and Mitrokhin 2006), provides fewer technical eavesdropping examples of interest.

An interesting report from Mitrokhin is that a wired microphone was installed by the KGB in a flat in Paris in 1931, using a French agent (Andrew and Mitrokhin 2000, p.98), a notable and unusual occurrence outside of the Soviet Union, as the wiring from the apartment would have required some degree of access.

The American State Department, Bureau of Diplomatic Security, report in a security history document some early incidents of eavesdropping attacks against their embassies in Moscow and Warsaw (US Department of State 2011). This recorded history begins in the early 1960s but the bugging of American diplomats began as soon as they established formal diplomatic relations with Russia in 1933. When the first American diplomats arrived in Moscow in 1934 and set up their Chancery in Spaso House, “they discovered that listening devices inside their offices and residences would be the way of life within the Soviet Union” (Wallace, Melton, and Schlesinger 2009, p.162).

Again in 1937 “when a bug was discovered directly over the Ambassador’s desk at the US Embassy in Moscow...Davies laughed it off. If the Soviets wanted to listen in, he told his incredulous staff, which included George Kennan, Charles Bolden, and other skilled State Department diplomats, they would only obtain proof of America’s sincere desire to cooperate with them.” (MacLean 1992) (Kahn 1998b). Wires were also found in the apartment of the Ambassador’s secretary (Kahn 2014, p.303).

In 1941 the German army began to approach Moscow resulting in Stalin ordering the Soviet Government and foreign embassy evacuation to the alternative capital Kuibyshev (Braithwaite 2010, p.242). Living conditions in Moscow deteriorated terribly between the years 1941 and 1943 but despite this, Stalin took advantage of the empty Western embassies by installing networks of microphone systems in many of them. Again, though the US and British being Russian allies, in 1943 the NKVD (the predecessor of the KGB) recorded the conversations of President Roosevelt and the British Prime Minister Winston Churchill while attending the

Tehran and Yalta Summit meetings. Roosevelt was persuaded to stay in the Russian compound for the Tehran Summit where the microphones used contained almost no metallic components, other than the diaphragm, so as to avoid detection by metal detectors. At the 1945 Yalta Summit, Roosevelt and Churchill's conversations were overheard with very little background noise from a distance of 50-100 metres away by using a directional microphone (Beria, Thom, and B. Pearce 2003).

In 1944 the activities of the Soviets during the Moscow evacuation years were finally uncovered when a very large network of microphones was discovered. "An FBI sweep of the American Embassy in Moscow the previous year (in 1944) had detected one hundred and twenty concealed microphones, and from time to time afterwards, new devices were found in furniture, wall plaster, and other inconspicuous places" (Kern 2008)(Andrew and Mitrokhin 2000, p.440).

The British Embassy evacuation was taken advantage of with the installation of a network of twenty six microphones built into the walls of the British Embassy discovered in 1944 (Drew 1946) and later in June 1948 the Norwegians too "found no less than thirteen microphones hidden in the walls" (Riste 2014, p.11).

While the Soviets were busy between 1941-1943 preparing for the Western embassy returns to Moscow, German prisoners of war camps between 1939 and 1942 were also being wired for audio. This was no ordinary bugging operation though. Masterminded by a brilliant spymaster, "Thomas Kendrick" from within MI-19, had the idea to install microphones in a large stately home and to then fill it with Generals and other high-ranking Nazi prisoners of war.

The "Type 88A" pressure microphones were provided by the American firm RCA and over a period of five months were carefully hidden in the fireplaces, skirting boards, ceiling roses, plant pots, billiard tables and even outside in park benches, trees and garden walls. Trent Park had twelve rooms bugged and the success of this operation led to two other Stately homes being bugged. Latimer House and Wilton Park each had thirty rooms bugged. The audio from the microphones were recorded using gramophone discs in seven minute sequences in what were called "M-rooms". An inventory of the equipment used in the operation exists (War Office 1939).

The high-ranking German officers were then subjected to faux interrogations. The British interrogators were often women too and this struck the Germans as being stupid and incompetent. Straight after the interrogation, the officers would return to their rooms and boast about all the things they had failed to reveal during the interrogation. This British Intelligence technique resulted in the production of 75,000 transcripts and a very rich source of military intelligence such as details of the V-2 rocket replacement, details that were thought to have contributed significantly to the success with the Battle of Britain, details of the “X-Gerät” system that used radio beams to pinpoint targets for German bombers and many other important intelligence information, considered to be on par with the intelligence produced by Bletchley Park (Fry 2012, 2019; Neitzel, Brooks, and Kershaw 2013).

Hubest reveals the extent of the consideration and effort required to mount an audio attack (Hubest 1960). Hubest also introduces the concept of “Hot Miking” which in the UK is known as a “Switch-hook Bypass”; a topic which is almost completely unmentioned in intrusive surveillance literature but was a common Eastern European attack method mounted against many diplomatic residences. Hubest credits the transistor and hearing aid development for creating improvements in the audio microphone technology, which continues at a pace today.

One of the most comprehensive articles on audio surveillance of Western Embassies during the Cold War period from 1945 to the late 1960s is written by Dr. David Easter from Kings College London (Easter 2016). This article reports that the bugging of diplomatic premises during the cold war was endemic.

2.3 Technical Eavesdropping During the Cold War

The Cold War spanned the period 1940 to 1990.

2.3.1 The 1947 LASER Microphone Invention

Léon Theremin (27 August 1896 - 3 November 1993) was born in St.Petersburg in Russia as Lev Sergeyevich Termen and was the inventor of the LASER microphone. In 1947 Theremin began work on the codename “BURAN” wireless surveillance device (Glinsky 2000a, pp.260-261). Theremin considered whether vibrations on windows might be caused through conversations within the room. Theremin devised a method of detecting these tiny vibrations at a distance using an infra-red beam directed at a particular point of a glass window, where the vibrations would be at the greatest amplitude for detection.



Figure 2.5: View of the Moscow Kremlin from the roof of the former British Embassy, illustrating the distance (approximately 300m) between the Kremlin and the British Embassy.

Theremin succeeded in producing a “hard to detect” bugging device that reflected infra-red light to a interferometer and a photo element to convert the reflected light received into a voice signal. The system was reported to work at a distance of sixteen hundred feet (487 metres). After some success against the American Embassy, Theremin turned it against the British and

French Embassies. Theoretically, at a distance of approximately 300m, the British Embassy was within the claimed range from the Kremlin (Glinsky 2000a, pp.260-261).

In theory it is plausible; in practice, the ability to locate the reflected light would have presented a significant challenge. The distance between the Kremlin and the former embassy is illustrated in Figure 2.5. Perhaps such a demanding technique became necessary after British Post Office technicians removed twenty six microphones from within the embassy the year before in 1946.

2.3.2 The 1952 Great Seal

The Great Seal (Codename LOSS or REINDEER by the Russian Technicians (Wallace, Melton, and Schlesinger 2009, p.165)) is one of the most famous bugging incidents of the twentieth century. Following the American loss of a U-2 spy plane shot down by the Russians in May 1960, the Great Seal was presented to the UN Security Council by the U.S. Ambassador to the United Nations, Henry Cabot Lodge, Jr. on the 26th May 1960. The Americans attempted to accuse the Russians of spying too, by revealing the Great Seal bug found earlier in 1952. Newsreel footage exists of this UN announcement (Universal International News 1960).

Copyrighted AP photographs exist on the internet of the U.S. State Department Director of Security, John Reilly inspecting the hidden transponder within the Great Seal with an unnamed American Security Agent (US State Department 2011, p.136).

Ahead of the UN Great Seal reveal, the CIA bugged the hotel rooms of many of the visiting Russian officials and the Russian TASS News agency official, attending the “Paris May 16 Summit” (Wallace, Melton, and Schlesinger 2009, p.182). That the Americans were bugging the Russian officials’ hotel rooms illustrates the aggressive nature of intrusive surveillance at the height of the Cold War.

The Great Seal incident began in 1945 when a delegation of Soviet boy scouts presented to the American Ambassador, Averell Harriman, a hand-carved wooden replica of the American Great Seal complete with a concealed Trojan-horse. The Trojan-horse device implanted within

the wooden carving was also the work of Léon Theremin (Glinsky 2000b). Harriman must have delighted the Soviets when he hung the Seal above his desk in the Spaso House residence study.

A wired microphone system could not be installed in Spaso House as egressing the microphone cables hidden out of sight from the residence presented problems; Theremin's challenge was to somehow overcome this problem. Theremin decided a wireless system was required so further developed a 1941 US Patent 223811 by Winfield Koch at RCA (Crypto Museum 2016b). Not that Theremin had a choice: his fear of failure may have resulted in a "return to Kolyma or worse" as Kolyma was a notorious region for Stalin's Gulag labour camps (Glinsky 2000b).

Eventually, in September 1952, the American technician Joseph Bezjian discovered the hidden passive resonator after intercepting a radio transmission containing the Ambassador's voice. An authoritative account is written by the US State Department (US State Department 2011) and the Ambassador present during the events of that evening when the device was discovered (Kennan 1983, pp.153-156) and many other writers too (Wise 1992), (Wallace, Melton, and Schlesinger 2009, p.162), (Andrew and Gordievsky 1991, p.452) and (Andrew and Mitrokhin 2000). An early sketch of the passive resonator was published in the *Amateur Scientist* in 1968 (Strong 1968) with the diagram illustrated in Figure 2.6 republished in 2002 in a popular spy book (Melton 2002a).

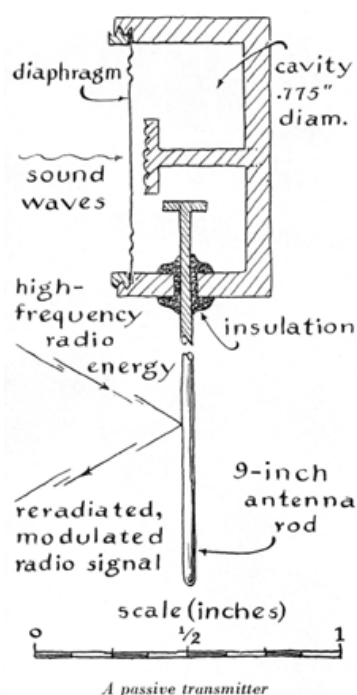


Figure 2.6: The Great Seal cavity resonator as depicted in the *Amateur Scientist* in 1968.

This was not the first time the cavity resonator technique had been used by the Russians. In 1950 routine security monitoring from within the Air attaché's office in the British Embassy detected a strong signal and the British Naval Attaché's voice could be heard while he was speaking within his office (Colville to Morrison 1952a,b). A Diplomatic Wireless Service engineer, Don Bailey, investigated the incident but results were inconclusive due to the technical apparatus deployed at that time (P. Wright 1987a, p.19). His directional aerial was cut to a considerably lower frequency than that used by the cavity resonator. What is conclusive is the fact that the Naval Attaché was subjected to an eavesdropping attack that appeared to be controlled externally. There was some interest in the recently Russian installed external street lighting outside the Naval Attaché's office (see Figure 2.7). This may have been the source of the illumination however the Russians had closer access to the most likely hiding place within the ceramic stove in the corner of the Naval Attaché's office, as this was close to the party wall feature (see Figure 2.9).

Photographs reference Figures 2.7, 2.8 and 2.9 have never been previously published. They were discovered by the author unannotated but have been verified to be from this incident (Bailey 1950).

Peter Wright's involvement with this British incident (P. Wright 1987a) and his later analysis of the American Great Seal device resulted in him completely understanding how the device worked. He used his practical radio skills background to estimate the frequency of operation of the device by assuming the length of the antenna acted as a half-wave dipole. This produced a frequency of operation around 600 MHz. The FBI's initial investigation suggested the antenna was 1.5 wavelengths long while the CIA detailed description of operation reported the antenna to be a half wavelength (Crypto Museum 2016b) supporting Peter Wright's initial findings. The Great Seal remains of interest to historians who have pieced together declassified sources of information to form a comprehensive timeline of events (Crypto Museum 2016b).

The US Naval Research Laboratories final FBI/NRL technical report on Theremin's resonant cavity microphone provides details of countermeasures equipment which became available within weeks after the discovery. Consequently this NRL report is one of the few documents yet

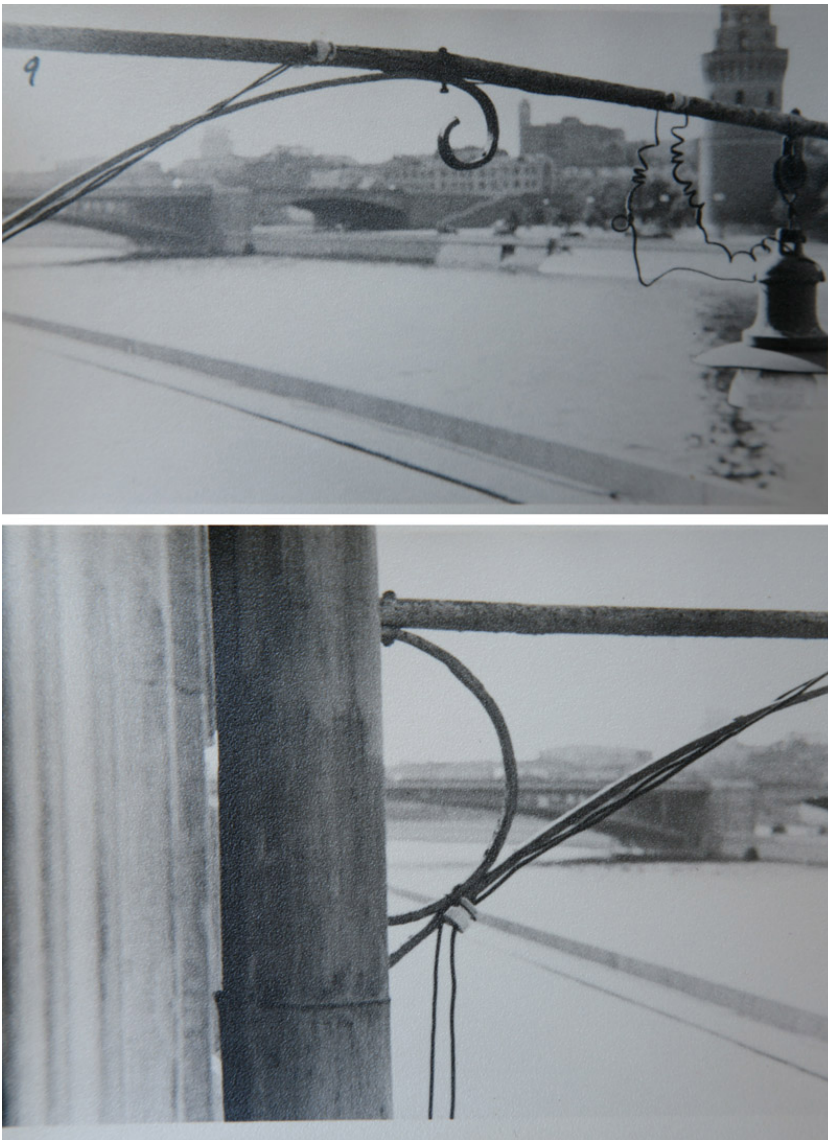


Figure 2.7: Suspicious street lighting outside the Naval Attaché's office which may have been a component of the technical attack. The Kremlin's Vodovzvodnaya Tower can be seen in the top-right of the picture. Credit FCO report R6/3.

to be declassified on this subject. Other work describes further analysis of the cavity resonator (Brooker and Gomez 2013).

The Great Seal device was reverse engineered by both the Americans and the British, although the American version was developed by the Dutch Radar Lab (Nederlands Radar Proefstation) in Noordwijk, in the Netherlands, under the code names Mark 2 and Mark 3 but given the CIA codename EASYCHAIR (Crypto Museum 2015). The British version SATYR (Crypto Museum 2016a) was developed by Peter Wright (P. Wright 1987a) who developed four prototype units ready for operation by July 1954 (TNA: PREM 11/760 1950). Wright went on to produce twelve sets for the Americans, who copied the design to make twenty more. SATYR was used by the British, Americans, Australians and Canadians. In 1957 Wright, aided by the

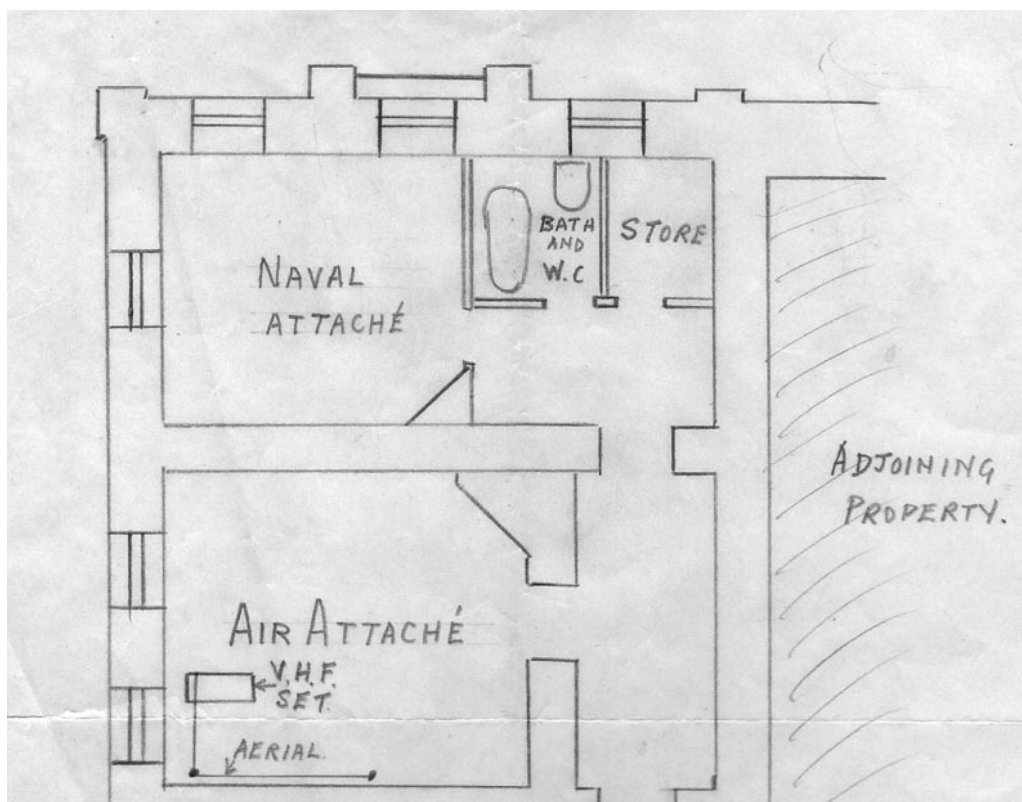


Figure 2.8: Floor plan of the Naval Attaché's East Wing office drawn during the investigation of the strange signal in 1950. The proximity of the adjoining property clearly illustrated. Credit FCO report R6/3.

Canadian RCMP, installed two SATYR devices against the Polish Consulate in Montreal but the operation failed as the Poles had been tipped off by the Russians. A further unsuccessful SATYR device, operation MOLE, occurred in Australia against the Russian Embassy in 1959 by a joint MI5 and Australian Intelligence Service (ASIO) operation. The SATYR device was installed in the sash window frame and although it technically functioned, it produced no intelligence (P. Wright 1987b, p.66).

Wise revealed that the KGB knew the Americans were developing a joint British-American research project to create a version of the Great Seal cavity resonator and the KGB were to be on the look out for any information (Wise 1992, p.15).

The discovery of both the Naval attaché event and the Great Seal caused considerable activity for years afterwards with priorities considered by an advisory panel for the newly created Foreign Service Technical Maintenance Section (F.S.T.M.S) sweep teams. In 1956 an extensive survey was conducted to establish revised threat assessments across the estates of the UK Government,



Figure 2.9: The Northern European white tiled ceramic stove within the Naval Attaché's office was a prime suspect for the location of the unknown listening device. Credit FCO report R6/3.

Commonwealth and Allied countries (Darlington 1956).

2.3.3 Wired Microphone Installations during the Cold War

In 1949 the Greek Ambassador, a bachelor, was in bed with his Russian housekeeper when the ceiling fell in revealing several microphones and the “ubiquitous eye of a camera”. The KGB transcribed what had taken place in the bedroom, together with some excellent photographs. The KGB attempted to blackmail the Ambassador but the Ambassador took the photographs from the KGB and showed them out. The Ambassador then, in high spirits, offered the photographs around of his antics at every diplomatic party he attended over a period of weeks. Not unsurprisingly, the KGB gave up on him (De Silva 1978, p.35).

In January 1952, just prior to the discovery of the Great Seal, a single microphone was found in the American Embassy in Moscow (Kennan 1983). Then later in 1953 inadequate physical

guarding of the American Embassy during its construction in Tchaikovsky Street, Moscow, led to the installation of microphones in the embassy (Andrew and Mitrokhin 2000). The Americans failed to learn lessons from the earlier 1944 bugging incident. “During its construction American security personnel stood guard each day to prevent the installation of listening devices, particularly on the two top floors which were to contain the CIA station, the Ambassador’s office and the cipher rooms. The day-long security vigil, however, served little purpose since the guards were withdrawn at night, thus allowing KGB personnel ample opportunity to bug the embassy” (Andrew and Mitrokhin 2000).

Fursend and Naftali revealed that “from April 1956 the Soviets had so thoroughly bugged the US Embassy in Moscow that the Kremlin could make copies of virtually every telegraphic message it sent and received” (Fursenko and Naftali 2010, p.92) (Wallace, Melton, and Schlesinger 2009, p.42). Afiani and Ivanov, two Soviet Archivists summarised classified reports retained by the Secretariat of the Communist Party of the Soviet Union. They suggested that some, not all, cables were distributed to the Soviet Presidium.

The American FBI in 1953 were bugging the Israeli intelligence service in New York in an operation first started in 1948 against the Arab League in New York (as cited in R.J. Aldrich 2006, p.406). Meanwhile their colleagues in the CIA were bugging a neutral country 7-man delegation in an Austrian Castle “Schloss Fuschl” on the Fuschlsee, 20 kilometres outside of Salzburg, who were preparing for a high-level strategic meeting soon to take place in Moscow. They placed a radio microphone in the pedestal of a table in the suite of the two leading team members. The radio microphones were then recorded by tape recorders left on the premises. The CIA did not bother to recover the radio microphone but predicted that in about six months’ time the batteries would “smell like dead fish” and would then be discovered, but they would be long gone and did not care (De Silva 1978, pp.89-91).

The CIA kept a close eye on the Soviet Embassy in Vienna too. Again in 1955 they noticed that the Soviet GRU and KGB staff often used a phone box located two blocks from the Soviet Embassy to make operational calls to set up meetings with their agents. The CIA technicians placed a radio microphone into the roof space of the phone box which could be easily retrieved

to change the batteries when required. Surveillance of this operation led the CIA to many KGB agents.

In another 1950s event the CIA station used their own home-made radio microphone housed within a nasal inhaler tube. After tests the device was installed by technicians who gained access to the target house. They used the radio microphone for a period of eight months against a Soviet target until the batteries finally went dead. The device was a “marvel of miniaturisation” but the maker of the device was rebuked by the CIA head office (De Silva 1978, pp. 115-117).

In 1956 US Sweep Teams also found microphones in the Ambassador’s office in Tel Aviv and Belgrade (as cited in R. Aldrich 2011, p.180). The Cold War increased the incidents of microphone installations but it was not only the Soviets installing microphones. The British too had a factory manufacturing eavesdropping microphones at Borehamwood, in Hertfordshire. “The build-up to the Suez Crisis had resulted in a high demand for bugs” (as cited in R. Aldrich 2011, p.181).

The audio from microphones was sometimes egressed from the target through mains wiring leaving a target location where the audio could be encrypted and masked to prevent discovery (Wallace, Melton, and Schlesinger 2009, p.197). A CIA manager reported that 5% of audio operations produced 95% of valuable information (Wallace, Melton, and Schlesinger 2009, p.231). Not all audio operations were complex. Aldrich released details of a private conversation with a former junior female British diplomat posted to Belgrade between 1961 and 1963. This young diplomat in her late twenties had a considerable linguistic ability; a crash course in Serbo-Croat at the School of Slavonic Studies at London University resulted in her translating for VIPs when their official interpreters were not at hand. One evening she was greeted by her elderly Yugoslav neighbour who was distraught as she was unable to operate the tape recorder attached to the microphones installed in her diplomatic residence. The secret police had failed to teach the old lady how to operate the tape recorder, so the young diplomat helped the elderly neighbour with extensive instruction (R.J. Aldrich 2006, p.408).

In January 1957 it was reported in a note about the expansion of the staffing arrangements

of the Foreign Service Technical Maintenance Service (FSTMS) that “Listening devices have been found in our Embassy in Spain, and there is evidence”, it was noted, “that devices may have been planted on us in Sweden” (Pumphrey and Skidmore 1957). Later in October 1959, Figure 2.10 illustrates the floor of the room where three microphones were found by FSTMS technicians in the British Embassy (*Reilly Papers* 1957). Two microphones were installed in the ceiling above the registry and a third above the cipher room. Analysis of the concrete revealed that they had likely been installed in 1942 (P. Wright 1987a, p. 292). Wright states the purpose of the microphone in the cipher room was to eavesdrop on the plaintext dictation of one-time pad enciphering. This therefore suggests that it was exploiting poor operational security rather than an acoustic TEMPEST technique being deployed.



Figure 2.10: Discovered in 1959, the floor of the British Ambassador's residence hiding the installation of three microphones attacking the rooms below. Not an easy task within such an ornate residence. It illustrates the achievement of a determined eavesdropper within a vacated premises.

In the early 1960s Dennis Amy, a British diplomat, claims that 200 microphones from staff flats in Moscow were recovered (British Diplomatic Oral History Programme 1998). Eventually, in

1960, the Foreign Office Security Department realised that tasking FSTMS “sweeping” of staff residences for eavesdropping devices was pointless due to the lack of security in these locations; bugs removed one day could be easily replaced the next. The Americans reported that they had found more than 100 devices in American diplomatic premises in countries behind the iron curtain (Kahn 1998a).

In 1964 the State Department discovered the bugging system first mentioned by Fursend and Naftali, who revealed that after a tip-off to the CIA by the Russian defector Nosenko, forty two microphones were honeycombed about the American Embassy (Fursenko and Naftali 2010). The Guardian newspaper reported that forty microphones had been discovered (The Guardian 1964), as did a later report (Cryptologic Spectrum 1972a). Christopher Andrew reports that the forty microphones were installed across two sensitive floors of the American Embassy and concealed in bamboo tubes hidden behind radiators in order to make them more difficult to discover with metal detectors (Andrew and Gordievsky 1991, p.453).



Figure 2.11: Close up of the US embassy microphone discovered in 1964.

The microphones “looked like wheels from a roller skate and were painted gun metal grey (See Figure 2.11). In the centre of each, a tube about the size of a drinking straw projected outwards to just behind the plaster to funnel the sound to the microphone. In some cases pin holes had been made to enhance the transmission of the sound” (Wise 1992, p.72).

Kessler provides further details (Kessler 1989, p.29), each of the microphones’ drinking straws were actually made from wood to prevent detection by metal detectors. Furthermore, the microphones were installed behind radiators so that they would likely remain undetected unless



Figure 2.12: US State Department's head of Security G. Marvin Gentile with one of the discovered microphones in 1964.

the inspection teams removed the radiators. This location also prevented decorators painting over the holes from the probe tubes. Kessler also reports that another 50 microphones were discovered in the adjoining diplomats' apartments.

In 1964 some difficulties were experienced by the KGB trying to bug a flat in Moscow as the residents rarely left the apartment. The KGB eventually gained access by befriending the occupants and making impressions of keys which then permitted later access (Andrew and Mitrokhin 2000, p.401).



Figure 2.13: KGB "HEPA" microphone (pronounced 'nirpa' in English) used in the 1960s.

Rustmann draws attention to the level of technical planning and detail given to a new target. Properties that joined any target were a priority to facilitate the possibility of drilling a probe tube into the area of interest from the neighbouring premises. When drilling into a property a

key requirement is to know when to stop in order to ensure that the last few millimetres are carried out with a very small diameter drill piece. This was achieved by using a CIA-developed back-scatter gauge which enabled the drilling to stop within half to three-eighths of an inch from the surface of the target room (Rustmann 2002, pp.62-63)(Wallace, Melton, and Schlesinger 2009, p.205).

The Back-Scatter gauge was complemented by a silent drilling technique that used grit to create a pin-hole in a plaster surface. The pin-hole could be made by eroding the surface quietly and when the surface was finally penetrated the change in pressure would be detected and the compressed air firing the grit would stop immediately (Wallace, Melton, and Schlesinger 2009). High speed silent drills were employed together with quick drying plaster with perfect colour matched new paintwork (Marchetti and Marks 1975, pp.188-189).

Marchetti and Marks describe in extensive detail the planning that goes into mounting a technical attack, such as where other residents will be and the location of security guards. Building plans will be studied including the colour and texture of any walls for the intended location of the microphones (Marchetti and Marks 1975, pp.188-189).

Rustmann also discusses the monitoring of an Asian embassy with an installation of eight separate microphones, the result of which produced hundreds of pages of documents. Every word spoken had to be transcribed and then translated consuming a great deal of the CIA services' resources.



Figure 2.14: Typical of the microphones being discovered in late 1950s in Warsaw, Poland.

Williams' book about the Czechoslovakia uprising between 1968-1970 (K. Williams 1997) states that:

Czechoslovakian Surveillance Technology: of seventy-eight listening devices planted in Western embassies and diplomatic suites, only half were in use; at the French Embassy only four of twenty were operating; none of the sixteen in the Austrian embassy worked; those in the American Embassy had been discovered in 1963. The British Embassy was impregnable.

This suggests that the British Embassy counter-eavesdropping defences in Prague were at that time effective. Microphone installations were installed for three purposes:

1. Listening to people's conversations: Many examples exist but one such example is that of monitoring the Russian Spy Oleg Penkovsky. When Penkovsky came under suspicion of the KGB, his apartment in Moscow was bugged from the apartment above. In addition to an audio monitoring post, a pin-hole camera also photographed his movements (Wallace, Melton, and Schlesinger 2009, pp.37-39);
2. Listening to typewriters in order to enable analysts to decode what was being typed from the noise of the keys being pressed either through timing patterns in the English language or tell-tail acoustic differences of each key pressed;
3. Listening to Cypher machines for acoustic TEMPEST: Peter Wright surmised that a microphone could be used to determine known core positions of a Hagelin cipher machine. If the settings of three or four of the wheels could be determined, this would enable the cipher to be broken. This technique was proved against the cipher machines of the Egyptian Embassy in London throughout the whole period of the Suez Crises (P. Wright 1987a, p.82).

2.3.4 Teleprinter Tampering

The historian David Kahn interviewed the KGB defector Victor Makarov, a Greek translator within the sixteenth directorate of the KGB. Makarov stated that "The Soviet Union seems to

have gained most of its communications intelligence, not from cryptanalysis, but from bugs and traitors” (Kahn 1998b, p.293). This statement was made after a meeting in June 1996 with the KGB General Andrei Nicolayevich Andreyev, who was a geologist rather than a mathematician or an electrical engineer.

Makarov’s access to documents reveals a two-page list of incidents of the KGB’s successful bugging of crypto targets. The Soviets bugged the German TX-20 teleprinter in Budapest, the Algerian Siemens T-1000 teleprinter, the Italian counter-intelligence’s and Switzerland’s Hagelin machine (and the Japanese too after 1983). The Indonesians used a secure cipher system, therefore, the Soviets had to bug them, rather than decrypt their communications. The Soviets read the messages of Syria, Iraq, Iran, the Palestine Liberation Army (from 1982), Portugal, low-grade Vatican cipher, China and North Korea one-time pad cipher as well as Zaïre (Kahn 2014, pp.296-298).

The bugging of the French Embassy’s six teleprinters in Moscow in 1977 egressed plain text for six years through the mains electricity supply to a nearby Soviet listening post. A large capacitor had been exchanged within each of the teleprinters that concealed additional circuitry. The capacitors were eventually spotted when it was noticed that the capacitor’s connector had four terminals rather than just two (Kahn 2014, p.304).

Makarov revealed that the Canadian Embassy was involved in a “bug-tug”. The Canadians had detected a microphone cable and just as the Russians were hastily retrieving the cable, the Canadians tugged the wire back (Kahn 2014, p.305). This is a little hard to believe and while there may be some element of truth in this story, it is hard to imagine that it involved a microphone cable, but rather some other form of technical attack associated with bugging.

2.3.5 TEMPEST Emissions Discovery

A declassified American document from 1972 (approved for release by the NSA in 2007) highlights “TEMPEST: A signal problem” (Cryptologic Spectrum 1972b). The “signal problem” was discovered by Bell Labs in 1943 when a researcher noticed that each time a 131-B2 Bell-

telephone mixing device stepped, an electromagnetic spike could be observed on an oscilloscope located at the other end of the lab.

This declassified document further revealed that the Soviets were ahead of the game by publishing in 1954 a “rather comprehensive set of standards for the suppression of radio frequency interference” (Cryptologic Spectrum 1972b). Furthermore, the article states “A disturbing discovery was that ordinary microphones, probably planted to pick up conversations in a cryptocenter, could detect machine sounds with enough fidelity to permit exploitation; such microphones were discovered in Prague, Budapest, Warsaw and, of course, Moscow”. A clear example of acoustic compromising emanations.

The BBC broadcasted a “Burke Special” on 15th June 1972 about the bugging of computers. Two techniques were discussed; the potential for unknown people to log into a computer via a Post Office telephone line using a modem and secondly, the ability to observe electromagnetic radiation received on a domestic television receiver highlighting to the public the possibility of the spatial radiation risk. Although at no point did they refer to this radiation risk as TEMPEST.

An article by Dutch Scientist Wim van Eck in 1985, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?” (Van-Eck 1985), discusses the realisation that electromagnetic “interference” signals from visual display units can be received with a standard television receiver and used for eavesdropping purposes. Van Eck demonstrated his discovery on the BBC2 programme “Tomorrow’s World” (BBC2 1985) with a follow up article in 1988 (Highland 1988).

Peter Wright proposed that without sufficient electromagnetic screening, any clear text input may be seen as an echo on the enciphered output; with the correct choice of an amplifier, it was thought possible to separate this “ghosting”. Wright claims these ENGULF experiments led to success against the French in 1960 in London against a high-grade cipher machines in operation STOCKADE for a period of almost three years (P. Wright 1987b, pp.109-110).

In 1988 Anderson and Kuhn (Kuhn and Anderson 1988) discuss using software to control TEMPEST emanations for both attack and defensive purposes. An interesting point is made that TEMPEST is becoming easier to investigate with the arrival of cheap software defined radio techniques which are lowering the TEMPEST investigation entry barrier. TEMPEST is no longer solely for Government or those with access to expensive equipment.

In 1990, Peter Smulders (Smulders 1990) concluded that “Data signals transmitted along an RS-232 cable connection may be vulnerable to interception at a distance”. Twelve years later, in 2002 a definition of the term TEMPEST (“unintentional intelligence-bearing signals”) is included within a declassified US National Security Agency’s Committee of National Security Systems document on Nonstop Evaluation Standards (US National Security Agency 2002). The term NONSTOP and HIJACK are defined in the reference (Institute 2016).

Markus Kuhn, a Senior Lecturer in Computer Science at the University of Cambridge Computer Laboratory (Kuhn 2016) highlighted a new information security risk in 2002 posed by cathode ray tube monitors and reflected light – so called Optical TEMPEST (Kuhn 2002). Kuhn continues his research and in 2003 discusses further eavesdropping experiments and compromising emanations from both cathode-ray tube and liquid-crystal monitors (Kuhn 2003), with further work in 2004 on flat panel displays (Kuhn 2004). Signal limits (Kuhn 2005b) and a real-time monitoring system in 2005 (Kuhn 2005a) were followed in 2006 by a practical demonstration of powerful field-programmable gate array based digital signal processing systems (Kuhn 2006). Kuhn published a further paper in 2013 reviewing compromising emanations from TV-Sets. He concluded that complications existed due to the variety of internal frequencies used within different LCD televisions.

TEMPEST emissions of electromagnetic radiation, acoustic or power supply fluctuation vulnerabilities may all provide an attacker with a passive way to receive plain language electromagnetic emanations from cipher machines. However just like the Great Seal transponder attack from 1952, it appears that the same illumination technique may be possible against susceptible cipher machines. Stannard called this an “interrogation attack” whereby the KGB could “direct a microwave or laser beam at the cipher room, reflecting back reverberations that might give

away the clear text of a message as it was typed on the keyboard” (as cited in R. Aldrich 2011, pp.216-217). To do this with a laser would require a direct line of sight to a cipher machine. An adjacent party wall seems more likely which may facilitate close access to the cipher machine of interest. A most interesting conclusion is drawn by Aldrich: “the exquisite dilemma of offence versus defence...[is] the conflicting demands of offensive SIGINT and defensive communications security” (R. Aldrich 2011, p.216).

2.3.6 Stealing Cypher Material and Bugging Typewriters

Sir Rodric Braithwaite recalled during an interview (Hutson 1998) that a fire was started by the KGB in the Autumn of 1964 in the British Embassy in Moscow.

There was a fire in the East Wing at the Embassy one evening. The Ambassador, Humphrey Trevelyan, was called out of a performance by the English Opera Group to go back and see what was going on. By the time I got there, which was after the opera was over, the place was surrounded by alleged Soviet firemen, directed by alleged senior firemen. It was pretty obvious that some of these people were not firemen at all. They wanted to get into that bit of the Embassy to see what was going on, so they set it on fire which was quite a good way. It did not succeed because they did not discover anything.

Victor Sheymov revealed that in 1977 the KGB used Low Energy Radio Frequency (LERF) technology which utilises relatively low energy spread over a wide frequency spectrum. This was used by the KGB to induce a fire in one of the equipment rooms in the US Embassy in Moscow. “A malfunction was forced on a piece of equipment, it caught fire, which spread over a sensitive area of the Embassy. The KGB tried to infiltrate its bugging technicians into the sensitive area under the cover of the firefighters who arrived immediately after the fire started. A similar event occurred at the British Embassy in Moscow several years earlier” (Sheymov 1978); presumably in the Autumn of 1964.



Figure 2.15: Lock-picking tools used by the East German Stasi secret police to gain entry to properties.

Mitrokhin reports the KGB in 1974 broke into seven missions in Prague, five in Sofia, two in Budapest and two in Warsaw, to steal cipher material (Andrew and Mitrokhin 2000, pp.458). In 1980 a French agent codenamed JOUR assisted bugging six French teleprinters installed in their Moscow Embassy between October 1976 and February 1977 (Andrew and Mitrokhin 2000, pp.609) (Kahn 2014, p.304). In Angola, an operation against the Brazilians produced photographs of the wiring of the Swiss made TS-803 cipher machine (Andrew and Mitrokhin 2006, p.96). By the 1980s the introduction of fibre optic cabling presented new challenges to the KGB.

The KGB used a portable x-ray generator to view the tumbler combination settings on the locks of safes to gain access into the safe without knowing the combination (Barron 1974, p.12). The high energy from these generators proved to be a health hazard for the operators who attracted the name *bezzubyie* – meaning “the guys with no teeth” (Wallace, Melton, and Schlesinger 2009, p.43).

The Russian defector, Yuri Ivanovich Nosenko, also revealed the lengths that the KGB went to in the early 1960s in order to break into the Swedish Embassy in Moscow. The KGB first seduced the Embassy watchman, before befriending the ferocious guard dog through a period of feeding it choice cuts of meat. Then, when most of the Embassy staff were preoccupied with a party, they sent a team of locksmiths, photographers and other specialists to open the

Embassy safe, open sealed envelopes and photograph the contents (Barron 1974, pp.12-13).

Makarov told Kahn that the American consulate in Leningrad was penetrated “through a back door” meaning, acoustic microphones (Kahn 1998b, p.302)(Kahn 2014, p.302). A further clue to a possible technical attack arose after the discovery in 1978 of an aerial in a chimney shaft illustrated in Figure 2.16 in the American Embassy in Moscow (Hoskinson 1978). Its purpose could not be determined but from the antenna’s construction, clues about the radio frequencies used could be determined and that the embassy was under some form of technical attack that involved egress by radio.



Figure 2.16: An aerial in a chimney was discovered on the seventh floor of the American Embassy by a State Department technical inspector; a clue that a technical attack was underway.

The technical attack mystery was eventually solved and details were published in the NSA “Gunman Project” report (US National Security Agency 2007). The Makarov Leningrad penetration was likely to have been via a compromised typewriter.

All electronic equipment in use in the Embassy was returned to the NSA via diplomatic bag and systematically x-rayed. Eventually luck was on the Americans' side. One of the technical analysts stated:

I found that bug by luck. After looking at so many x-rays day after day for so many hours, I could easily have missed it. I'm glad that I saw it. I certainly was delighted with the \$5,000 cash award (US National Security Agency 2007, p.14)

The 1984 Gunman Project report provides details of sixteen compromised typewriters with implants comprising a combination of electrical and mechanical means. Thirteen typewriters were in use within the American Embassy in Moscow, with the remaining three located in the Leningrad Consulate. For a period believed to be eight years the Soviets were able to “receive copies of everything from routine administrative memos to highly classified documents” (US National Security Agency 2007, p.1).

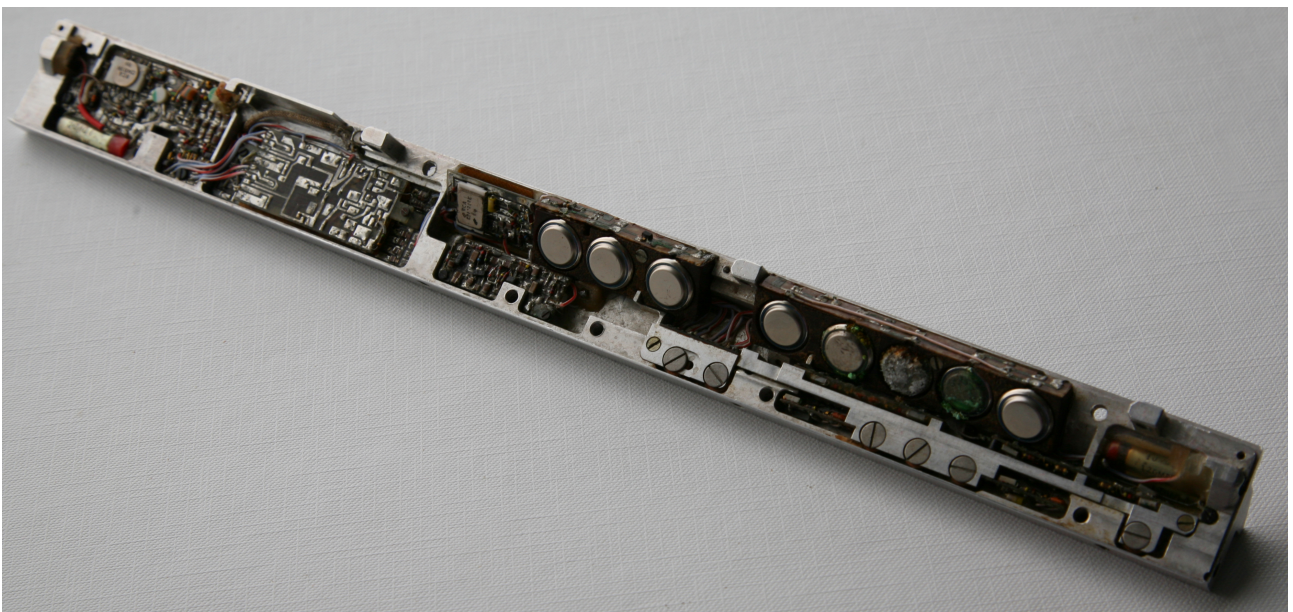


Figure 2.17: The advanced Russian electronics discovered by x-ray examination hidden in the components of the typewriter.

2.3.7 Audacious Communications Taps

In Vienna in 1948, Peter Lunn, the head of the SIS station in Vienna, dug a twenty-foot tunnel code-named “Conflict” in order to intercept a main Soviet telephone cable that was running under the British sector of the quartered city of Vienna. The Post Office research station at Dollis Hill provided an engineer to carry out the tap. The success was quickly followed by two more tunnels “Sugar” and “Lord” (Davies 2004, pp.214-216).

In the 1950s, in a joint operation by the British SIS (Codename Stopwatch) and American CIA (Codename Gold), it was realised that a crucial Soviet junction of telephone cables came within just a few metres of the American Sector in West Berlin. By 1955 a 450m tunnel had been dug to enable British equipment to tap the large number of unencrypted telephone and telex lines from 11th May 1955 until it was discovered by the Soviets in April the following year. The tunnel created an estimated three thousand tons of sand to move and “haunted the minds of the project team...Where do we put the dirt?” (CIA/DP 1968).

Statistics from the Berlin Tunnel Operation released by Clandestine Service History (CIA/DP n.d.) revealed that:

- Three cables were tapped containing 273 pairs and 1200 communications channels. 500 channels maximum in use at any one time;
- On average 28 telegraphic circuit and 121 voice circuits recorded continuously;
- Approximately 50,000 reels of magnetic tape were used (25 tons);
- The voice processing centre employed a peak of 317 people;
- 20,000 Soviet 2-hour voice reels containing 368,000 conversations, were fully transcribed;
- 13,500 German two-hour voice reels received and 5,500 reels containing 75,000 voice conversations were processed. 17,000 fully transcribed;
- The teletype centre employed 350 people at its peak. 18,000 six-hour Soviet teletype reels and 11,000 six-hour German reels were completely transcribed;
- Processing the back log of material continued until 30th September 1958.

The tunnel had its own heating system in order to cope with the cold Berlin winter. However,

the first time it snowed a path above the tunnel began to appear, so the heating system was quickly switched off (Dulles 2016, p.205).

There was no evidence that the Soviets attempted to feed deception material through the cables but the Soviets archive remains closed in order for this to be verified. However, it is widely believed that the British traitor, George Blake, informed the Soviets of the operation.

In September 1969 a German bug sweeper by the name of Horst Schwirkmann was sent to Moscow to find hidden microphones in the German Embassy. Whenever a microphone was discovered he had taken to injecting a very high voltage down the microphone cable (Barron 1974, p.8). This would have destroyed the electronics within any receiving apparatus at the listening post. Schwirkmann also discovered a listening device attached to the cipher machine which enabled the KGB to hear the plain text which, together with the enciphered output, enabled the encryption keys to be deduced. The KGB chose to administer some revenge on Schwirkmann for his high voltage injection and, while on a walk around Zagorsk Monastery (72 km North-East of Moscow), they shot him in the buttocks with nitrogen mustard gas causing Schwirkmann excruciating pain as the mustard gas ate away at his flesh. Schwirkmann survived but his recuperation was long and agonising.

In 1977 the CIA conceived an incredible attack against fibre optic cables running between Moscow and the closed to Westerners city of Troitsk. The information carried within these links was thought to be worth the high-risk technical attack codenamed CKTAW. The inductive tap weighing thirty-five pounds and at a development cost of twenty-million dollars was placed around the fibre cables one spring morning in 1981 by an American diplomat who had worked hard to convince the Russians he was of no interest to them. He developed a pattern of picnics with his family that led to no Russian surveillance thus enabling him to slip away on a bus from his family picnic and install the fibre tap in the manhole. Eventually the tap was discovered in the Spring of 1985 after a tip-off from the American defector Edward Lee Howard (Wallace, Melton, and Schlesinger 2009, pp.138-156).

2.3.8 The Radio Microphone Period from 1965

According to a politbureau report (Cold War International History Project Bulletin 1998) in 1967 alone, “the KGB carried out operations of clandestine pilfering of secret documents from intelligence services of the enemy. These and other measures resulted in obtaining the codes of seven capitalist countries and in implanting eavesdropping radio-devices at thirty six installations of interest for Soviet Intelligence”. The term “eavesdropping radio-devices” is interpreted as radio microphone attacks in thirty six different locations.

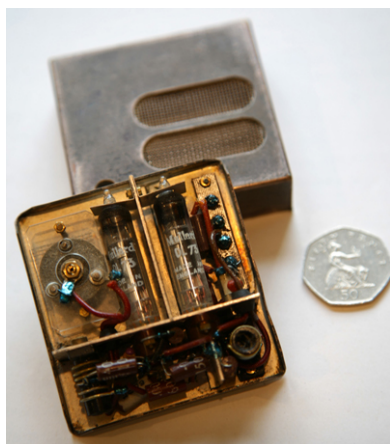


Figure 2.18: An early commercial two-valve Mullard DL-67 sub-micro pentode radio microphone.

Rustmann, a twenty four year senior-serving member of the CIA’s Intelligence Service who retired in 1990 discussed various early 1970s concealments important to successful audio bugging operations. Wood was a favourite material as it could blend in with the style of the furniture in the target location (See Figure 2.19). Rustmann had two favourite concealments, a ruler or a screw driver that can be easily hidden in a couch. Even more popular was the multiple AC wall plug adapter (Rustmann 2002).

Radio microphone attacks were responsible for several successes against the Americans and British in Third World countries where local agents could be recruited to plant bugs on behalf of the KGB (Andrew and Mitrokhin 2000, p.441). Such a case occurred with operation RUBIN in Beirut against the British Embassy SIS station. The operation began in 1967 and ran for three and a half years until it was discovered in 1971 (Andrew and Mitrokhin 2000, p.443).

David Wise reports that in a joint operation in 1959 by the FBI and the CIA, four Ford cars were “stripped down” and bugged. These cars were then delivered to the Soviet Embassy in



Figure 2.19: A Russian six-battery 1970s woodblock transmitter on display in the International Spy Museum from the personal collection of Prof. H.K. Melton.



Figure 2.20: A Russian ten-battery 1970s woodblock transmitter - This one found in Africa by the US State Department.

Mexico City but the bugs were found instantly (Wise 1992, p.92). The Russians had more success against the Americans. In 1965 a US CIA apartment was bugged in Conakry, capital of Guinea and in 1972 the American Embassy too. This bug was replaced in 1974 with a voice-operated switched bug. Mitrokhin states that this region was a priority for the KGB at this time. Russian radio microphone attacks were also mounted in 1969 against the UN, Secretariat of the UN Secretary General, and the Ghanaian mission to the UN (Andrew and Mitrokhin 2000, p.443) as well as the Senate Foreign Relations Committee. In 1973 the Senate Foreign Relations Committee bug was apparently found but continued to operate (Andrew and Mitrokhin 2000, p.449).

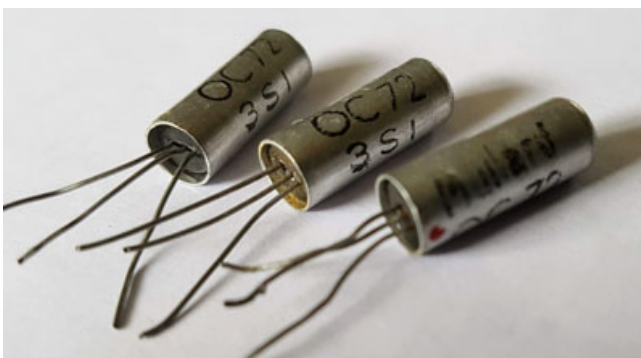


Figure 2.21: An example of an early Germanium transistor. This OC-72 example made by Philips in 1955. The transistor's power dissipation has been improved by covering the glass case with a metal sheath in order to provide greater heat transfer. This technology revolutionised the creation of miniature radio microphones.

A very well known bugging incident occurred in the US Embassy in Bucharest; the State Department Security Officer, Lou Grob, was routinely monitoring the radio spectrum during a conference meeting being held in the Embassy “bubble” (a safe speech room) when he came across a transmission which contained the voice of Harry G. Barnes, Jr., Deputy Chief of Mission in Bucharest. Lou Grob immediately informed the meeting of his findings and eventually after further investigation discovered the transmitter concealed in the heel of Barnes’ right shoe, implanted after being taken for repair locally in Bucharest (see Figure 2.22). A small pin inserted into the heel enabled his maid, earlier, to activate the transmitter (US Department of State 2011, p.178) (Barron 1974, p.7).



Figure 2.22: US diplomat bugged in Bucharest in 1969 by a transmitter concealed in the heel of a shoe. The photograph is a copy of the State Department find on display in the International Spy Museum in Washington.

A popular radio microphone system was developed by the CIA in the 1970s for use in restaurants housed within a pepper mill. Many other imaginative covert disguises were developed to hide audio transmitters such as table and desk lamps. A van was equipped with receiving equipment to receive output from these devices (Wallace, Melton, and Schlesinger 2009, p. 219).

Wise reports (Wise 1992, p.8) that the Soviet head man in Helsinki was suspicious that a cat which came through the ironwork bars of a window was somehow penetrating security. Wise reveals (and (Wallace, Melton, and Schlesinger 2009, p.200)) that the CIA had actually been experimenting with cats implanted with radio microphones in order to gain access to a target.

In 1959 the CIA were developing tiny transmitters to capture typed content from electric typewriters and also a tiny transmitter powered by self-contained batteries for use behind a car dashboard for tracking purposes. Marchetti and Marks describe some of the clandestine CIA

devices developed by the Technical Services Department: “a signal transmitter disguised as a tooth and a pencil for secret writing on special paper” (Marchetti and Marks 1975, pp.188-189). A microphone was also disguised as an olive in a cocktail, with the cocktail stick acting as the aerial (See Figure 2.23). In another device the audio transmitter was built into a tooth (Wise 1992, p.13). These gadgets are not credible and act as an odd propaganda better suited to the movies and television (Wallace, Melton, and Schlesinger 2009, p.407). These gadgets are more about the CIA exploiting the capability of the newly invented transistor and playing catchup with the Soviets after the Soviet “Great Seal” device stealing a lead for technological advancement (See section 2.3.2).

This was certainly a period of the CIA being imaginative. In 1976 the CIA were training pigeons, owls and ravens to carry small payloads such as photographic equipment. In one CIA report declassified in July 2019 a fascinating paragraph is included: “A clandestine operation was carried out some time in the past in Europe in which an audio eavesdropping device was delivered by a bird to a designated outside window sill. This operation was not successful because the audio device would not pick up a conversation from the desired target” (CIA 1976).

Marchetti and Marks further write about a report of audio operations in Latin America where bugs were placed in the homes and offices of key personnel and even ministers. They mention that these operations are used against less security-conscious targets such as those outside of communist countries, demonstrating some risk aversion. They also report that laser eavesdropping systems only worked in West Africa or in the United States (Marchetti and Marks 1975, pp.190-191).

Mitrokhin reported a very successful attack in 1980 against a private company in Arlington, Virginia, USA, by placing a battery-powered radio microphone under a conference room table. The receiver was located in a car with an antenna in the front wind-shield (Andrew and Mitrokhin 2000, p.456).

A failed CIA example illustrates the lengths that the CIA considered when they unsuccessfully developed a microphone and radio transmitter system that could be inserted into a .45 calibre



Figure 2.23: A 1966 CIA transmitter disguised as an olive in a glass of Martini; the cocktail stick acting as the antenna. This bug is more suited to the movies and television than reality. Reproduced from *Life Magazine* 20 May 1966 on an article about snooping.



Figure 2.24: Russian-style Stasi radio microphones on display in the Leipzig Stasi Museum (August 2016).

bullet. The bullet could be aimed at a tree near the target and fired from a rifle to place the microphone where required (Wallace, Melton, and Schlesinger 2009, pp.198-200). The Soviets and the Cubans considered the CIA's clandestine trade craft to be the best in the world (Fischer 2016, p.58). However, on one occasion the CIA's trade craft was not so good; a CIA officer bragged about his audio bugging operation in Bonn in such detail that the operation against a Russian GRU intelligence officer enabled the Soviets to find and remove the bug (Fischer 2016, p.61).

In 1971 the Russian Trade Mission in London had a network of bugs uncovered by the Soviets suspected to have been planted by MI5 in London. Graham, a double glazing contractor who

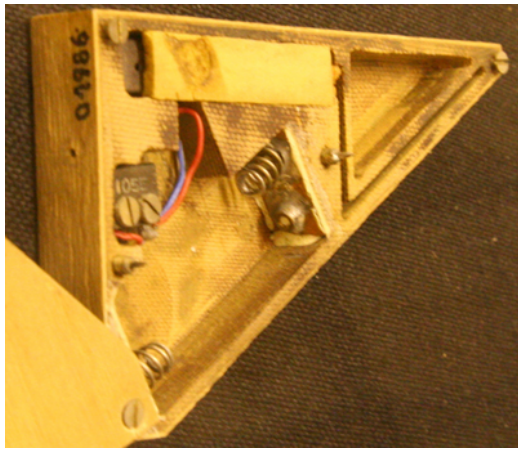


Figure 2.25: Radio microphone used by the Stasi. This one intended for mounting on a piece of furniture with the microphone below. Powered by two AA-sized batteries and switched on by inserting a pin through a small hole in the side of the wooden case. On display in the Leipzig Stasi Museum (August 2016).

worked at the Trade Delegation reported installing seven radio microphones in under an hour (Graham 1987, pp.68-70). The radio microphones were received in mobile “wagons” parked a mile away in Hampstead Heath.

However years later we learn that the bugging of the Trade Delegation proved to be rather more extensive than reported by Graham, extending to Soviet residential apartments too. In a similar way that the Americans revealed the Great Seal bug to the UN in 1960, the Soviets chose to hold an ITN news conference in June 1989 in an attempt to deflect blame for a diplomatic spying scandal by demonstrating to the world that they were the victim of a bugging scandal. The footage (ITN News 1989) shows the Russian Press Officer describing the extent of the network of microphones found and for the cameras two bugs were chiselled out of the wall of a Soviet apartment. The timing of the press release coincided with the expulsion of eight Soviet diplomats and three Soviet journalists for engaging in “activities incompatible with their status”, for attempting to re-establish a spy ring in London.

There was more to this 1971 Trade Delegation event that would later result in bugging incidents in Africa. In September of 1971, a Russian diplomat Oleg Lyalin also from the Trade Delegation was arrested on suspicion of drink-driving. Lyalin first sought political asylum but then defected. Lyalin revealed sabotage plans for London and other Western capitals. In addition, the Russians were trying to suborn politicians, scientists, businessmen and civil servants as well as trying to steal technological data (Barron 1974, p.28). This led to the expulsions of one hundred and five Russian GRU and KGB officers from London (Andrew and Gordievsky 1991, pp.522-523). BBC television coverage of the incident is also available (TV 1971). To plug the

intelligence gap these expelled officers were sent to UK Commonwealth countries such as Delhi, Colombo, Dar-Es-Salaam, Lagos and Lusaka (Andrew and Mitrokhin 2000, p.547).



Figure 2.26: 1990's vintage audio eavesdropping device made in the USA for the professional and commercial market.

2.3.9 Switch-hook Bypass Attack

Further switch-hook bypass attacks came to light in the conference room at the US Europe Command Headquarters. Fourteen rigged telephones were found. By 1960 more than one hundred had been found in US Diplomatic premises within Eastern bloc countries (Kahn 1998a).



Figure 2.27: Telephone switch-hooks modified to egress audio.



Figure 2.28: If the black relay at the bottom of the picture can be bypassed, the audio from the handset transmitter will egress audio to the telephone line even when the handset is placed on the cradle.

2.3.10 Photography

A brief mention of photography is made for training of a GCHQ spy in 1968 to use the Microdot technique and Minox camera (Andrew and Mitrokhin 2000, p.452). The KGB also successfully bugged the Syrian Embassy in Moscow. Of interest is not just the microphone installation in various offices but that they opened the Syrian Diplomatic Bag during transit back to Damascus which was never detected by the Syrians (Andrew and Mitrokhin 2006, p.202). Gordievsky reports that diplomatic couriers travelling on the night train between Petrograd (St.Petersburg) and Moscow would have their pouch contents opened and photographed while the couriers were asleep. In one case in 1921 the Russians even resorted to drugging a Finnish courier's tea to gain access to the pouch (Andrew and Gordievsky 1991, p.85).

Photography is an important tool for the copying of stolen documents. Barron reports that between 1957 and 1961, the KGB had a photographic lab in the back of a large black van that they parked close to the NATO Headquarters in order to photograph documents "on the spot" (Barron 1983, pp.376-418).



Figure 2.29: Soviet F21 miniature camera made in Krasnogorsk near Moscow from 1950 for the KGB. This model was used by the East German Stasi secret police too. This example is on display in the Berlin Stasi Museum (August 2016).

Orlov reports (Costello and Carev 1993) that the British cipher clerk, Ernest Holloway Oldham, was almost recruited in 1929 after walking into the Soviet Embassy in Paris when he offered to sell a British Cypher system for £2,000. Eventually Oldham was recruited in 1930 by the Soviet NKVD, the forerunner of the KGB. Oldham was said to have committed suicide in 1933. Orlov further reports that the Cambridge-ring spy Maclean from January 1936 “smuggled out an ever growing volume of documents. These were photographed overnight and handed back, to return the next morning...whenever possible, he should bring the documents out on a Friday night, to give the overworked photographer of the “illegal” station two days to work before the papers were returned on Monday morning”. With such operations in place, there would be little need for complex and time-consuming microphone eavesdropping systems.

Long-range photography was also used to monitor Oleg Penkovsky once suspected of being a spy by the KGB. The KGB set up telephoto lenses opposite Penkovsky’s apartment on the other side of the river. These lenses produced high-quality images which photographed Penkovsky’s spying activities (Wallace, Melton, and Schlesinger 2009).

The CIA developed their first ultra-miniature camera in 1970 called the T-100 specifically created for document copying. With a 4mm diameter lens it was capable of approximately 100 photographs on a 400mm film strip with each exposure producing a 4mm square negative (Melton 2002b, p.98). The second generation T-50 only provided half the exposure capacity of the T-100 but had improved reliability (Wallace, Melton, and Schlesinger 2009, pp.89-92).

MI6 also consider photography important. Tomlinson reveals “MI6 uses commercially available photographic equipment where possible because anything specially made could be compromis-



Figure 2.30: The East German Stasi used photography too: The “Robot Vollautomat Star II” was used to covertly photograph subjects with a remote shutter release. This particular camera was used within a compartment inside a watering can allowing covert photography through a small hole near the handle. The watering can continued to function as intended.

ing” (Tomlinson 2001a, p.69). Tomlinson also learnt how to covertly take photographs of the public using various still and video cameras mounted within briefcases or shoulder bags. The year of Tomlinson’s training is not mentioned but it was in the pre-digital era as he mentions “using the darkroom”.

2.3.11 The East German Stasi 1950 - 1990

No literature review of intrusive surveillance would be credible or complete without mention of the German Democratic Republic’s Ministry for State Security (MfS). Since the fall of the Berlin Wall, the MfS secret police force is largely known as the Stasi, abbreviated from the German word Staatssicherheit (State Security).

The Stasi operated for forty years between 1950 and 1990 with 91,105 full-time staff and about 176,000 informers shortly before its downfall. The Stasi’s dramatic ending, when outraged citizens occupied the Stasi offices in Berlin, secured documents not destroyed by the confused Stasi staff. This has provided historians and researchers the opportunity to study a totalitarian regime. An agency, Der Bundesbeauftragte für die Stasi-Unterlagen (BStU) (Der Bundesbeauftragte für die Stasi-Unterlagen 2016) known as “The Stasi Records Agency” was created in 1990 to preserve and protect the archives. The BStU continues to catalogue and release Stasi records and continuously updates its publication list (BStU 2016).

The Stasi Handbook, “Anatomy of State Security”, is available in German language only online in twenty eight separate parts. Two published sections “Hauptabteilung III: Funkaufklärung und Funkabwehr” (Department III: Radio Reconnaissance and Radio Defence) and “Hauptabteilung VIII: Beobachtung, Ermittlung, Durchsuchung, Festnahme (Department VIII: Observation, Investigation, Search, Arrest) provide insufficient technical detail for this study.

The Stasi department of interest to this research is the OTS: Operational Technological Sector, formed in 1960. It employed 1,131 people in 1989 under Dr. Wolfgang Schwanitz and was responsible for “Department twenty six which monitored telephone conversations and set up optical and acoustic equipment such as cameras and bugs”. In 1983, twenty five telephone monitoring stations located in East Berlin monitored twenty thousand telephone taps simultaneously (Dennis and P. Brown 2003).



Figure 2.31: Stasi telephone recording apparatus on display at the Stasi Museum in Berlin (August 2016).

The Stasi recognised the importance of the development of micro-electronics and opto-electronics but one official reacting to party propaganda remarked that “pretty soon they’ll just give us all microchips instead of something to eat” (Dennis and P. Brown 2003). However by the late 1980s Western technology was increasingly leaving the GDR behind, leaving the Stasi to turn to illegal embargoed imports of Western computing technology.

Kristie Macrakis has studied a small fraction of the ten thousand files of interest to this work. Her published book reports “More than eight thousand staff members at headquarters worked on providing James Bond-like technology to support espionage”(Macrakis 2014, pp.317-318). Macrakis believes that the technology used by the Stasi has been overlooked and underesti-



Figure 2.32: Hidden Stasi camera within a tie on display in the Stasi Museum in Berlin (August 2016).

mated because of the Stasi's prominence in human intelligence gathering. I am inclined to agree although note that Macrakis visited H. Keith Melton's private Museum in Boca Raton, Florida, and this will have informed her of the interest by Governments and technical individuals worldwide.

Macrakis' research reveals the size of the Stasi OTS, the Stasi Spy Tech University. Department thirty three, thirty five and "E" are the most interesting with relation to the creation of photographic and electronic surveillance technology. Macrakis discovered through researching Stasi yearly reports that in one year alone in the mid-seventies more than one hundred Mikrat cameras were made for agents (The Mikrat came into use in 1958) together with "infra-red cameras capable of photographing in the dark" and "1,216 containers (that housed concealments) were delivered, mostly made from leather". This was to meet a two hundred and ninety one percent increase in internal surveillance requirement and that "requests for eavesdropping devices increased sixfold in 1974".



Figure 2.33: Hidden Stasi microphone within a pen with the cable attached to a thin-wire recorder. Item on display in the Runde-Ecke Stasi Museum in Leipzig (August 2016).

Macrakis research provided other technical information: “In 1977 department E delivered fifty six small tape recorders with thirty concealments, and by 1980 a total of six hundred and forty three different types of tape recorders were in operational use, including four hundred and sixty seven small cassette recorders” and “The early seventies saw an increased use of infra-red and ultra shortwave radio technology. By 1979 decimetre radio communications had been phased out” (Macrakis 2014, pp.160-161). Note that Ultra-short-wave or UKW in German is known in the UK as the Very High Frequency band (VHF) between 30-300 MHz.

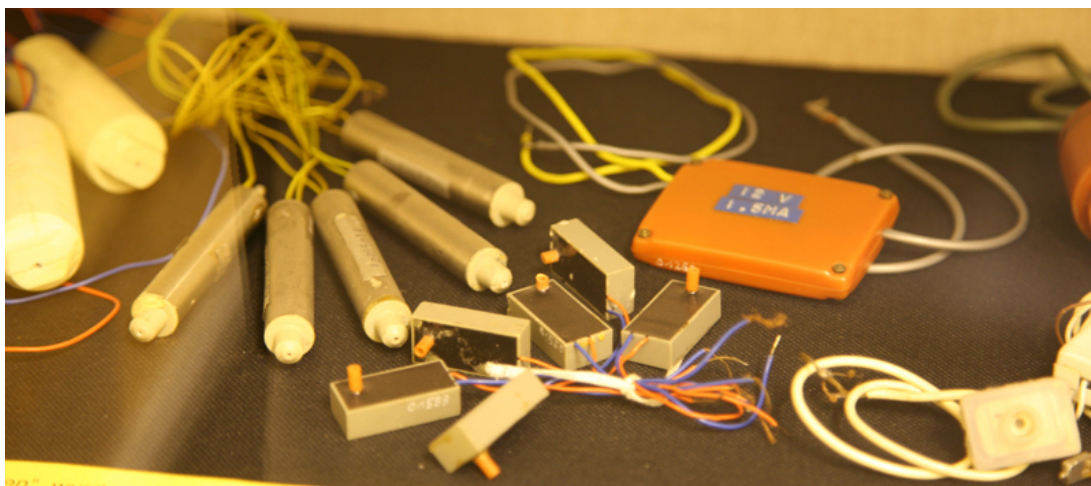


Figure 2.34: A collection of Stasi microphones on display in the Runde-Ecke Stasi Museum in Leipzig (August 2016).



Figure 2.35: A further display of Stasi microphones on display in the Runde-Ecke Stasi Museum in Leipzig (August 2016).

Macrakis illustrates the BEKO periscope camera designed in the 1970s to take photographs through a one millimetre aperture pin hole (Macrakis 2014, p.235). During the 1970s and 1980s more than forty thousand Western telephone lines were tapped. Internally, by the early 1980s, a database of between thirty thousand to forty thousand telephone numbers were routinely and

continuously targeted (Macrakis 2014, p.263). The tracking of foreign diplomats through the use of isotope laced pellets fired at diplomat's car tyres from up to twenty five metres away to enable tracking to be carried out for a hundred days. Real-world evidence of use is somewhat sketchy (Macrakis 2014, p.308). Anna Funder (Funder 2011, pp.191-192) describes the use of Stasi radioactive tags and pins sown into clothes and hand-pumped sprays to mark people in crowds to enable tracking, or a person of interest's floor impregnated with radiation to enable footprints to be tracked; the tracking provided by covertly worn Geiger counters with a vibrate function.

The Stasi collaborated with the KGB on a clandestine project against the CIA in East Berlin and used their extensive range of hidden cameras to do so (Fischer 2016, p.59) but the extreme intrusive surveillance system against the GDR's own citizens relied on a vast network of informants and technology. This was conveyed in 2006 through a German language drama film "The Lives of Others" (Florian Henckel von Donnersmarck 2006) a celebrated and Oscar-winning film that does not, however, provide a realistic portrayal (Ash 2007). Ash states that the film powerfully affects those who watch it, but is "all too highly coloured, romantic and even melodramatic". Anna Funder states this even stronger: "The film doesn't accurately portray the way totalitarian systems work" (Funder 2007). Funder's review is thought-provoking and she states "has an odd relationship to historical truth, a truth that is being bitterly fought now".

From my own observation too, the film contains technical inaccuracies; the surveillance monitoring team were unlikely to have been in the attic of the apartment under surveillance as they would have been quickly observed by the residents. The film also illustrates the use of a fine wire laying tool to quickly lay wires behind wall paper to a microphone hidden behind a light switch. This tool can be seen in a H.Keith Melton's book "the Ultimate Spy" (Melton 2002b), together with other Stasi photographic surveillance equipment.

Anna Funder writes further (Funder 2011) and although this book is devoid of technical details, it is a powerful collection of stories that remind the reader of the reality of this brutal regime that used technology to repress and control its population. Funder also states that at the time

of the book's publication in 2003 the Runde-Ecke Stasi Museum in Leipzig has three rooms housing Stasi artefacts (Funder 2011, p.7). A visit to the museum in August 2016 reveals the museum has grown in size with several rooms now devoted to technical surveillance equipment.

Despite the prominence of OTS, very little literature has been written about the technology that originated from the Stasi Spy Tech University. As the BStU continue to release documents, perhaps some details will emerge. The technology is limited to the period 1960 - 1989. There may be some pressure from other nations' security services to limit the record release of sensitive technologies created by BStU.

2.3.12 Short-Range Agent Communications Systems

In the early 1970s the first electronic short-range agent communications (SRAC) systems had been developed by the Americans. It was given the code name BUSTER and could fit in a coat pocket (Wallace, Melton, and Schlesinger 2009, pp.115-118).

The Americans invented burst radio communications devices at UHF via space-borne satellites for use with their agents in early 1970. One such device (a CDS-501 - See Figure 2.36) was given to the Cuban Security Agent Aurelio who infiltrated the CIA and returned with it to Cuba in November 1980 (Morera and Calcines 1988). The CDS-501 encrypted its messages and could transmit, up to a week later, 1,600 characters in 21 seconds to the MARISSA-3 satellite (Fischer 2016, pp.63-65). Another similar piece of equipment, the RS-804 was seized by the Russians in March 1983 while in use in a Moscow Park by the US Diplomat Richard Osborne. Osborne was later expelled from the Soviet Union for spying.

In a later computerised system Tomlinson (Tomlinson 2001b, p.69) provides an interesting update on the SRAC:

[The SRAC is]...only issued to long-established and highly trusted agents...the agent writes a message on a laptop, then downloads it to the SRAC transmitter, a small box the size of a cigarette packet. The receiver is usually mounted in the

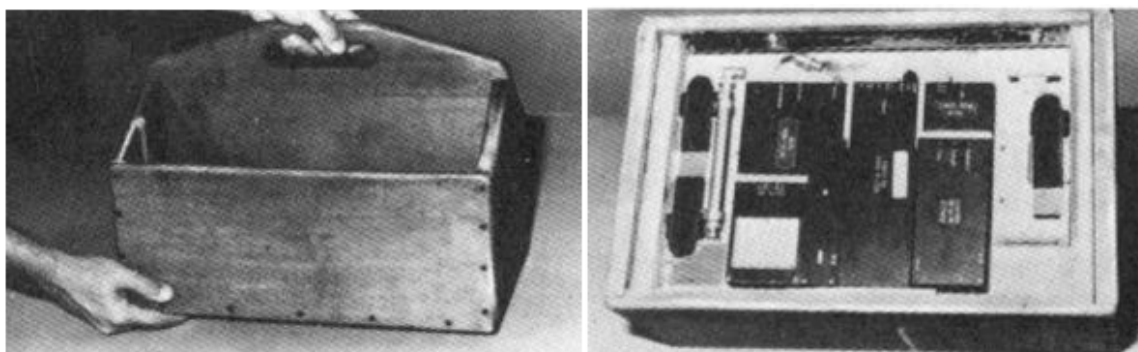


Figure 2.36: The CIA's agent communications equipment from the 1988 Cuban propaganda book "The CIA's War Against Cuba".

British Embassy and continually sends out a low-power interrogation signal. When the agent is close enough, in his car or on foot, his transmitter is triggered and transmits the message in a high-speed burst of VHF. The transmitter is disguised as an innocuous object and for many years "Garfield cat" stuffed animals were popular as their sucker feet allowed the agent to stick the transmitter on the side window of his car, giving an extra clear signal as he drove past the embassy.

2.3.13 Signals Intelligence (SIGINT) and Echelon

Signals Intelligence Operations date back to the First World War (see earlier section 2.2.3). The Second World War successes of Bletchley Park require no introduction and are the focus of many publications such as *Hut 6* (Welchman 1997) and *The Shadow Factory* (Bamford 2009).

Aldrich in his opening pages lists forty eight "Overseas British SIGINT stations and facilities" suggesting SIGINT is an important source of global intelligence (R. Aldrich 2011). The locations echoing the fortune of the British overseas estate. The map makes no mention of Berlin or Vienna British Embassy locations reported to be GCHQ sites by Campbell (D. Campbell 2015a).

In 1962 the British Prime Minister, Harold Wilson, was on holiday in the Isles of Scilly and was convinced that a Russian trawler was operating a SIGINT operation and listening to his

telephone calls (Andrew 2009, p.526). This may have been related to Wilson's paranoia but perhaps with good reason. In 1963 the KGB listened to the conversations of the US and the CIA in Mexico. By 1966 they were also monitoring in Washington and in New York in 1969 and by 1970 the KGB were carrying out SIGINT operations in fifteen cities (Andrew and Mitrokhin 2000, pp.447-451). The third largest SIGINT operation was located in Havana in Cuba, principally against the Americans where two hundred and sixty people were eavesdropping on nine hundred international calls a day (Andrew and Mitrokhin 2006, pp.92-93). While in the Middle-East, the KGB were producing most of their intelligence from SIGINT rather than HUMINT (Human Intelligence). In 1967 the KGB were decrypting the codes of one hundred and fifty two cipher systems used by seventy two different states (Andrew and Mitrokhin 2006, pp.139-140).

By 1975 the CIA were also increasingly turning to SIGINT with large scale collection operations employing long range sensors (Marchetti and Marks 1975, pp.190-191). As a result they claim that classical spies are becoming obsolete against the most important countries. Many of these remote sensors are placed in their US Embassies. There have been numerous stories from an outraged German Chancellor, Merkel, with stories in the Spiegel such as "No Longer in the Cold War": Merkel was infuriated by US Spying (Spiegel Staff 2013) when it came to light that the NSA had been listening into her telephone conversations. The British have come under the spotlight too by photographic analysis of the British Embassy roofs in both Berlin and Vienna by the British journalist Duncan Campbell (D. Campbell 2015a).

In the late 1980's HF Communications for British Diplomatic posts were coming to an end. However, eavesdropping on the Diplomatic Wireless Service of the British Foreign Office was not possible by the casual eavesdropper (Madsen 1988) since both encryption and the use of a multiple tone radio modem system called Piccolo (Robin et al. 1963) were used. Rustmann's introduction to the European Union's claims that the US, together with its Five-Eyes partners, were intercepting emails, faxes and telephone calls through a system called ECHELON (Rustmann 2002, p.126). The Echelon Global Spying System first became publicly known in 1976 following an "Eavesdroppers" article published in Time Out Magazine about GCHQ written by Duncan Campbell (D. Campbell 1976). The article resulted in the British Government attempting to prosecute Campbell for "unlawful receipt of information" and breaking the 1911

British Official Secrets Act in what became known as the “ABC trial” after the three defendants, Time Out reporter Crispin Aubrey, former Ministry of Defence employee, John Berry and Duncan Campbell (D. Campbell 1977).

Echelon was reported to be a system that “intercepts and decodes communications throughout the world” (D. Campbell 1976). The system was operated with the US National Security Agency and also had a base in the Cotswolds. In a further article in the New Statesman in 1988 (D. Campbell 1988) Campbell reports on the twelve hundred staff at Menwith Hills monitoring station (See Figure 2.38). Four systems were reported to be in operation in addition to ECHELON: SILKWORTH, a long-range radio monitoring system, MOONPENNY, a system for monitoring satellite communications, SIRE. RUNWAY was thought to be a monitoring system that operates an eavesdropping satellite called VORTEX. STEEPLEBUSH is thought to be a control centre for the biggest of the eavesdropping satellites code named MAGNUM.

The budget for the GCHQ involvement was hidden amongst other government department spending. Campbell wanted to reveal the GCHQ involvement as part of the BBC TV series “Secret Society” and the episode on the concealment to Parliament of “Zircon”, the British spy satellite. However the Strathclyde police seized both the master and backup tapes of the episodes, to prevent the BBC2 transmission (D. Campbell 1987). As a result, Campbell had a “special one-off showing” of the programs.

The conclusion of a report written on “the existence of a global system for the interception of private and commercial communications (ECHELON interception system)” by the European Parliament (Schmid 2001, pp.135-136) stated that the surveillance system depended, in particular, upon worldwide interception of satellite communications but that “capabilities of the system are probably not nearly as extensive as some sections of the media had assumed” (European Parliament 2001)(Piodi and Mombelli 2014).

An article for the Surveillance Society (S. Wright 2002) states “most US intelligence is gathered by signals intelligence using huge computers to trawl through the world’s telecommunications looking for selected key words using a complicated algorithm and dictionary system of key words...”. Keefe writes that despite Echelon, the spies with their SIGINT tools failed to predict



Figure 2.37: Investigative journalist Duncan Campbell's public programme showing of Zircon.

the four coordinated terrorist attacks by the Islamist terrorist group Al-Qaeda in September 2001 (Keefe 2006).

The existence and further details of Echelon resulted from Snowden's whistle-blowing and the release of Top Secret files to the internet (Gallagher and Greenwald 2014)(D. Campbell 2015b)(D. Campbell 2016).

2.3.14 The Watergate Scandal

In 1971 a team of five were caught breaking into the Watergate office complex in Washington, DC in order to bug the office of the Democratic National Committee headquarters. The fact that Richard Nixon's administration were involved created a political scandal that ultimately led to the resignation of Nixon as the President of the United States.

Of interest to this review is the bugging technology used within the Watergate offices. A website (Thomas Investigative Publications 1972) claims to show one of the three bugs, which, from the photograph, looks commercial in nature with an operating frequency of 154.815 MHz. The transmitter is remotely switchable by the use of two tones, one to activate the transmitter and



Figure 2.38: Menwith Hill - the location of the secret American global satellite monitoring station located in the UK. Photo Credit (CND 2011).

the other to de-activate it. The transmitter is modular in design and facilitates the connection to either a microphone or a telephone line. The device is operated on a single battery which suggests low transmit power and short range; the receiver would therefore likely have been close to the Watergate office. The 3,700 hours of secretly recorded audio from phone calls and meetings within the Watergate offices has been made available online (Nichter 2007).

2.3.15 Popular Bugging Books from the 1970s

J.K. Peterson's "Surveillance Technologies Handbook" 3rd edition (Petersen 2012) makes a contribution to this research. As the author Petersen states, "technology is changing faster than it can be documented". The author's credentials reveal her to be "a prolific writer in several venues" and an academic background interest in computer imagery, design and technology as a lecturer at the University of British Columbia (UBC) and Western Washington University in Canada. Petersen writes in Chapter One:

This book fills a significant gap in surveillance literature. There are thousands of books about spies, dozens of retail catalogues of spying devices and now, many

books that discuss loss of privacy. However, this is still the only foundation text that covers surveillance devices in a broader context so that readers can understand the origins and diversity of these devices, and how they are used in a wide range of fields (Petersen 2012).

The book is written in 18 chapters and while in theory every chapter is relevant to a study of intrusive surveillance, in practice this is not the case. Only chapters one and two: the general introduction and acoustics are of interest. Chapter 2 discusses the step change in technology in the 1990s, the concept of mobility and the freedom from the fixed land-line telephone representing key technology era changes. The section on Laser eavesdropping (Petersen 2012, p.162) is based on low-end amateur equipment and is not representative of the modern capability available in 2016 by high end commercial systems.

There are many books on the subject of bugging written for amateur hobbyist consumption (Palmer and Green 1977) (Melton 1993) (Wingfield 1984) (Bugman 1999) (Shannon 2000) (Brookes 2001) (Bergquist 2002); this list could be considerably longer. These books list popular commercial bugging frequencies and circuit diagrams of simple equipment for the amateur to construct. They are written by authors with past credentials in some security role capacity. Some books list bug detection equipment too and often mandate strict procedures to detect their presence. These instructions are written authoritatively as if following their strict guidance will result in complete assurance that all bugs will be found. These instructions relate more to entertainment than reality and are not suitable for hostile or aggressive espionage states. They are though representative of an era in time when bugging could be conducted by the average citizen as a hobby rather than the sole capability of a government security service.

2.3.16 Commoditised Eavesdropping - 1967 onwards

In 1967 a variety of consumer bugs were in reach of the amateur electronics enthusiast. In the USA, *The Electronic Invasion* (R. Brown 1967) illustrated several audio bugging techniques. The book reports that a new brand of automatic telephone transmitter was available on the

market every three weeks and provides lists of common frequencies used for bugging equipment.

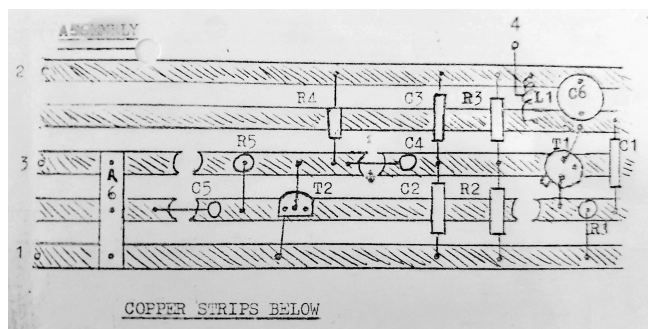


Figure 2.39: In the late 1970s mail-order transmitter bugs using Veroboard were available at pocket-money prices. There is no evidence to suggest these were used to bug people but rather, built by curious hobbyists for experimental purposes only.

In the UK in the late 1960s, a shop dedicated to bugging equipment opened in London's Mayfair district (Fitzgerald and Leopold 1987). In 1975 *The Times* published a photograph of a bug smaller than a two-pence piece (Christopher 1975) to further illustrate this new Swiss-made technology. The story was as a result of an earlier bug discovery in 1975 within the Communist Party Headquarters in London (*The Times* 1975). The two stories however are not related technologically; the two-pence piece bug story illustrated the advancement of technology in much the same way as the Martini Olive bug from the CIA, while the Communist Party Headquarters bug discovery has traits of professional installation similar to other wood block Soviet style transmitters found in Third World countries.

The Communist Party of Great Britain Headquarters (CPGB) in King Street, Covent Garden was the focus of eavesdropping attacks from 1942 onwards. As early as 1943, Blunt was warning the Soviets about the hidden microphones and the tapping of their telephones but despite the Soviets looking, they were never found (Andrew 2009, p.402). This eavesdropping at CPGB was still in operation in 1959 (Andrew 2009, p.409) and continued to 1984 when Arthur Scargill was involved with the CPGB and was categorised as “an unaffiliated subversive” with his telephone taps being attentively read by Margaret Thatcher (Andrew 2009, p.676).

2.3.17 Eavesdropping against a Terrorist Siege

In 1980 six armed terrorists called “The Group of the Martyr” who were fighting for autonomy of the Khuzestan Province in Iran, burst into the Iranian Embassy which is located close to Imperial College London in South Kensington. They took twenty-six hostages but after one of

the hostages was murdered and his body left on the embassy doorstep, the SAS moved in to end the siege; with the whole SAS operation appearing on live British television.

The SAS were very well informed before they entered the six floors of the Iranian Embassy as over fifty of the rooms had been bugged with elaborate listening devices. MI5 employed 35 of its technical staff with a further 16 staff from other intelligence organisations. Microphones were dropped down the chimneys in order to quickly gain audio intelligence from rooms. There was no time available to employ silent drilling techniques in this time critical situation, so a noise distraction was employed in the form of a British Gas road drill in an adjacent street in order to mask the sound of the walls being drilled by technicians next door. Audio in such instances, provided critical tactical intelligence (Andrew 2009, p.688).

2.3.18 The 1984 New American Embassy Build in Moscow

In 1979 the new American Embassy in Moscow became a very large KGB bugging operation. They produced a “system of sensors that could pick up virtually anything” (Andrew and Mitrokhin 2000, p.447). The system used reinforcing rods as antennas and a battery supply embedded in the walls within the concrete. Pre-fabricated columns had been prepared off-site (Kahn 2014, p. 304). The columns contained gap-jumpers illustrated in Figure 2.40.

Michael A. Boorstein reports “In August 1985, work was suspended in the new office building when the Soviet-implanted listening devices were discovered embedded into the structural shell of the building” (Boorstein 1998).

In 1987 the State Department released highlights from the appointed security consultant, James R. Schroedinger, on the new US Moscow Embassy build (Ottaway 1987). The report states “A Soviet attempt to plant electronic “bugs” in the building was “both foreseeable and foreseen. But as a nation, we have failed to anticipate the boldness, thoroughness and extent of the penetration”. The report goes on to say “for the past 15 years [the US] has “consistently underestimated” Soviet intelligence capabilities”. Boorstein reports that the Soviets handed over the complete plans of the bugging operations against the US new embassy build to the



Figure 2.40: The KGB gap-jumper so called as it jumped the gap between concrete support pillars placed end to end. This coupling egressed the extensive eavesdropping system built within the American Embassy during the construction stage.

American Ambassador to Moscow, Robert Strauss in early 1992. “Some Russians were horrified that the new government had taken this step, considering it an act of treason” (Boorstein 1998).

At the same time period Nosenko reported the use of a system codenamed “litra” to mark people’s post so that it could be tracked. The chemicals could also be dropped onto a target’s shoes enabling dogs to trace the path of the target (Wise 1992, p.76). This technique was the precursor of the later developed “spy dust” used to track Western diplomats and journalists in Moscow, which used the chemical nitrophenylpentadienal (NPPD).

2.4 Technical Eavesdropping - A Turning Point in Time

This section relates to the period 1991 to 2019.

2.4.1 The Rise of Surveillance Studies

Just as the personal computer becomes popular, with the rise of the internet via dial-up telephony Internet Service Providers and the increased networking of computer use in business, so too does the interest in possibilities that surveillance is occurring automatically via electronic means. As early as 1986 journalists such as Campbell wrote about the growing volume of information stored about British people and the threats this poses to privacy (D. Campbell and Connor 1986). The Australian David Clarke coined the phrase “Dataveillance” to describe the growing “Digital Persona” and its Application to Data Surveillance but which was also “potentially threatening, demeaning, and perhaps socially dangerous phenomenon” (Clarke 1994).

By 1994 Lyon writes “Of all the questions raised by new technologies, the one that strikes me as being most socially pervasive is the garnering of personal information to be stored, matched, retried, processed, marketed and circulated using powerful computer databases” (Lyon 1994, p.ix). These ideas are the beginning of the creation of the Surveillance Society. In 2001, just after the terrorist incidents against the World Trade Centre in New York and the Pentagon in Washington DC the Surveillance Society is created, dedicated to the study of surveillance. The society’s editorial within the first publication states “New technologies, above all the computer, facilitate surveillance in ways that Max Weber, Franz Kafka, or George Orwell never dreamed of” (Lyon 2002).

In September 2006 a report written for the UK’s Information Commissioner (Wood et al. 2006) discusses “A Week in the Life of the Surveillance Society in 2006” covering the everyday activities and surveillance story of the Jones family returning from a week’s holiday overseas. The report makes surveillance predictions for life in 2016, which we can today evaluate. Many

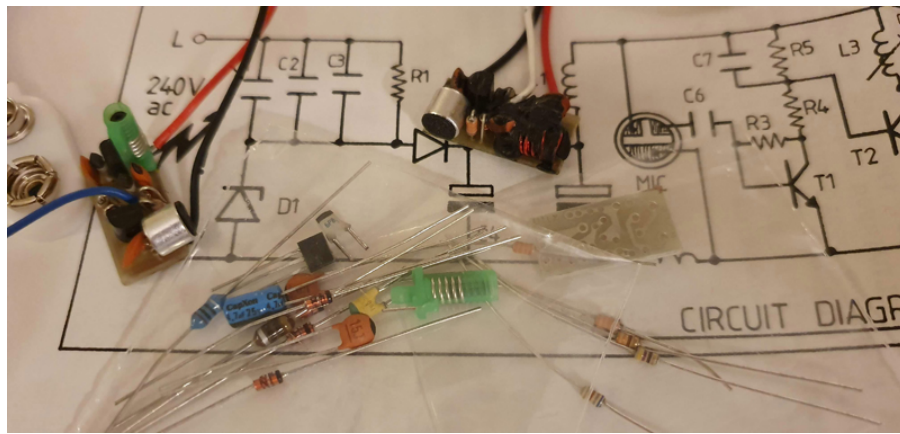


Figure 2.41: By the 1990s numerous simple battery or mains-powered VHF short-range bug kits became available from specialist mail order suppliers. The kits remained at pocket-money prices.

of the report's predictions were a little too futuristic; for example, we do not have implanted chips beneath our skin for cashless shopping.

Lyon and Ball write an authoritative handbook on the subject of surveillance studies in 2012 (Lyon, Ball, and Haggerty 2012) with an ever watchful eye on the balance required for increased government surveillance through legislation and customer privacy. People need to trust that their data is safe and secure but governments erode this trust. Mass surveillance by governments continues to erode a government's reputation.

2.4.2 Sousveillance

Sousveillance (“sous” meaning “under” and “veiller” meaning “to watch” translated from French) is “inverse” surveillance carried out by individuals with wearable technology, in order to survey the surveiller. It may be overt or covert in nature, with both methods provoking a different response by those in authority carrying out the surveillance. Interestingly, “The degree of objection to sousveillance varies with the amount of surveillance present” (Mann, Nolan, and Wellman 2002). Steve Mann carried out a series of experiments which “explores what happens when cameras move from lamp posts and ceilings down to eye level” (Mann 2004).

Jacquemard et al. (Jacquemard et al. 2014) takes sousveillance one step further with a discussion of “life logging”, cameras small enough to be permanently worn as “life logs” that are no bigger than postage stamps. The technological challenge of continuous personal surveillance raises ethical questions yet to be considered. There is no doubting the capability of the technology; small cameras with built-in digital recording capability powered by long-life batteries. If a “sousveillancer” wishes to record covertly, they are likely to remain unchallenged. The challenge to front of house security staff is both the initial detection and the likely confrontation in order to locate this body-worn technology. Such technology has the potential to record security equipment installed within a premises that may enable further vulnerabilities to be determined.

2.4.3 Phased Array Directional Microphone

Phased array directional microphone use is mentioned by Tomlinson (Tomlinson 2001a, p.183). Phased microphone arrays use electronics to control individual microphones in such a way that the whole array is able to focus in a specific direction and ignore others. It is a method of creating a highly directional beam-forming microphone system in disguises such as an A4-sized portfolio folder or what appears to be an iPad case. Tomlinson states the example of two salesman sat at a nearby table in a motorway service station with a microphone array mounted within a briefcase. On another occasion the briefcase was used against a target within a Dutch coffee shop (Tomlinson 2001a, p.186).

2.4.4 The Amateur TEMPEST Hacker Period

In 2015 projects and applications dedicated for the ubiquitous RTL-2832U cheap USB Software Defined Radio dongle (RTL-SDR.Com 2015) presented a practical demonstration and supporting software for a method of detecting electromagnetic radiation through a wall and covertly monitoring keyboard activity from a laptop. In 2016 Marinov (Marinov 2016a) provided a complete software toolkit to mount an attack against remote video using a selection of low-cost

SDR receivers. Figure 2.42 illustrates a screenshot of a SDR practical demonstration of the decoding of HDMI TEMPEST emanations from a monitor screen almost certainly aided by the cheap manufacturing techniques and low quality screening of the monitor and cables.

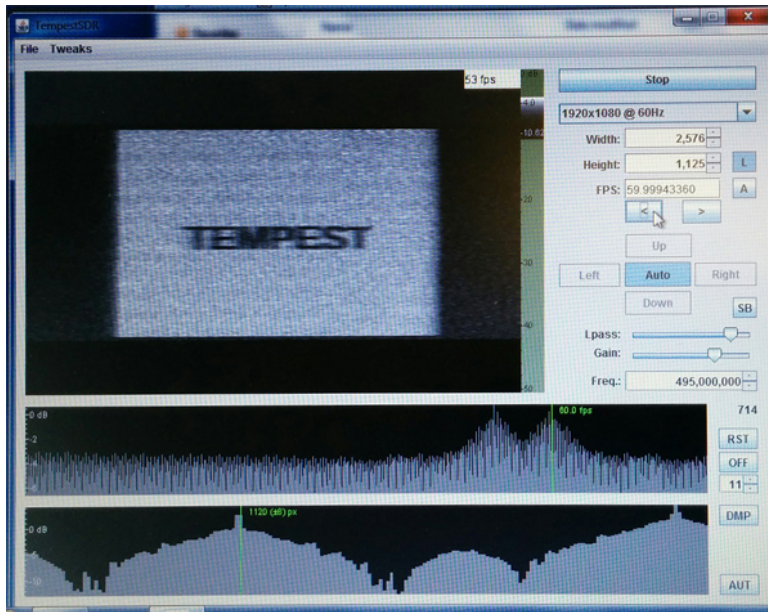


Figure 2.42: Impressive results from a low-cost software defined radio receiver.

Modern keyboards radiate compromising electromagnetic emanations (Vuagnoux and Pasini 2009) including radiation via the mains wiring, but other TEMPEST emissions have been studied by others: In 2008 Balzarot, Marco and Vigna (Balzarotti, Cova, and Vigna 2008) described their automated tool for long-term surveillance attacks that utilised a video camera analysing the finger movements above a keyboard to automate the reconstruction of typed input. Keyboards have been the subject of interest to many other researchers. In 2004 Asonov and Agrawal (Asonov and Agrawal 2004) described a way to recover 80% of typed text from keyboard input through audio analysis using neural networks. Further work in 2006 by Berger, Wool and Yeredor (Berger, Wool, and Yeredor 2006) used signal analysis and acoustic-based dictionary password cracker algorithm to increase the accuracy dependent upon the words used. In 2009 Zhuang, Zhou, and Tygar (Zhuang, Zhou, and Tygar 2009) continued the development with an improved accuracy. In 2014 further work by Tong, Qiang, Shanfeng and Yunhao (Zhu et al. 2014) deployed a different technique using acoustic emanations recorded from smartphone keyboards which determined the keys typed by estimating the keystrokes' physical positions based on the time-difference of arrival. This technique was also used earlier in 2011 by Marquardt, Verma, Carter and Traynor (Marquardt et al. 2011) who utilised

a smartphone's three-axis accelerometer by measuring the relative physical position and distance between each key input vibration with the typed input matched against a dictionary. This produced recovery accuracy of up to eighty percent. Keystrokes have also been detected by monitoring the reception of a local transmitter using multiple receiving antennas (Chen, Yenamandra, and Srinivasan 2015) placed within five metres of the keyboard.

Technology for TEMPEST continues to evolve; in 2004 the US Government invited bids for Automatic Data Processing Equipment - CESG TEMPEST Video Processor (governmentbids.com 2004) for use by the US State Department. Specialist receivers for TEMPEST reception use continue to fall in price with the development of Software Defined Radio (SDR). Amateur enthusiasts continue to develop TEMPEST applications for eavesdropping (Marinov 2016b).

2.4.5 Advanced Persistent Threat (APT)

In 2016 Advanced Persistent Threat is a serious pervasive threat to the security of Information Technology and network component systems. APTs represents the highest level of threat posed due to their sophistication, intent and unpredictable desired effect. They are created by aggressive state sponsored threat actors (Andress and Winterfeld 2013, p.28). "We should accept that people intent on breaking in to our large and complex IT systems, as part of their day job, will achieve it if they really want to" (Auty 2015). APTs may be carried out against a system over a period of years in order to achieve a particular objective.

"Intelligence-driven" defence is required (Hutchins, Cloppert, and Amin 2011) but defending against APTs is extremely difficult or perhaps simply not possible unless the IT system is effectively isolated. As lines of computer code continue to rise within systems, so too does the potential for the introduction vulnerabilities. Edsger Dijkstra commented as early as 1969 that "Program testing can be used to show the presence of bugs, but never to show their absence!" (Buxton and Randell 1970, p.16, p.66). The outcome or effect when instructions are received that are completely unpredicted or quite random may enable system exploitation. Exploitable bugs per thousand lines of code vary, but their discovery has created a commercial trade, with

exploits sold by private software companies and organisations, academics and students, all hoping to make a large sum of money quickly.

The American technology company Symantec reports that “More than 430 million new unique pieces of malware were identified in 2015. An increase of thirty six percent from the year before” and that there were fifty four zero-day vulnerabilities discovered in 2015; an average of one a week. This more than doubled the number found in the previous year (Symantec 2016).

The APT is also thought to be used in warfare too. The Cold War may be over but the new Cyber War era has begun. Russia allegedly used cyber techniques ahead of their attack in the Russian-Georgian War in August of 2008, with further similarities against Ukraine when Russia launched disruptive attacks on critical infrastructure (Babcock 2015).

Protecting information assets on networked IT systems is an enormous challenge. State sponsored threat actors have the advantage of never having to physically leave their country. The advantage may simply come down to the available “in-country” resources.

2.4.6 The Smartphone

Mobile telephones have introduced speech security vulnerabilities from the moment they were first introduced. Whether it was from a state’s legal intercept capability or from simple radio scanners monitoring analogue mobile telephone transmissions from the first generation of mobile handsets.

Smartphones have increased the vulnerability to eavesdropping through their ability to execute applications and the ever increasing array of sensors built into the devices. Eavesdroppers exploit these built-in sensors for purposes other than those for which they were originally intended. Other vulnerabilities are introduced within smartphones through the ability to execute applications without necessarily raising the attention of all but the most security conscious users.

A comparison of vulnerabilities introduced by using a smartphone can be seen in Table 2.1.

Mobile Telephone Handset Vulnerabilities		
Vulnerability	Older Handsets	Smart-phones
Taking control by means of trojan software	No	Yes
Taking control by means of trojan hardware	Yes	Yes
Legal eavesdropping by national authorities	Yes	Yes
Silent ring eavesdropping	Yes	Yes
Bluetooth eavesdropping	Yes	Yes
SIM card copiers	Yes	Yes
Transmitter concealed in mobile phone battery	Yes	Yes
Bluetooth device embedded in battery	Yes	Yes
Inappropriate disposal of mobile telephones	Yes	Yes
Voicemail password left on default setting	Yes	Yes
Real-time interception of calls	Yes	Yes
International mobile subscriber identity catching	Yes	Yes
Live tracking through network operator facilities	Yes	Yes
Live tracking through an application installed on the handset	No	Yes
Live tracking through an online application	No	Yes
Tracking by handset forensic analysis	No	Yes
Tracking by mobile device power analysis	No	Yes
Using bogus base stations for spoofing (“Man in the middle”)	Yes	Yes
Audio recording application software	No	Yes
Near field communications (NFC)	No	Yes
Optical communications via the screen	No	Yes
Gyrophone: recognizing speech from gyroscope signals	No	Yes
Acoustic eavesdropping through wireless vibrometry	No	Yes

Table 2.1: The long list of mobile telephone vulnerabilities.

2.4.7 The NSA ANT Catalogue

In 2013 Edward Snowden, an American computer specialist and former NSA contractor disclosed classified NSA documents to various media outlets worldwide. These documents revealed historical details of the US and Five-Eyes partners’ global technical surveillance activity. It is believed that Snowden may have leaked the NSA’s Advanced Network Technology (ANT) Division’s Tailored Access Operations catalogue which was published online by the German Spiegel magazine (Appelbaum, Horchert, and Stöcker 2008). The catalogue featured a broad range of NSA technical collection technologies in use up to the year 2008.

The catalogue lists 77 codewords relating to exploit technologies. The techniques listed used a mixture of hardware, software, SIGINT reception, Illumination and network exploitation.

Category	Occurrence	Codename
Room surveillance	5	CTX4000, LOUDAUTO, NIGHTWATCH, PHOTOANGLO, TAWDRYYARD
Computers exploit	9	GINSU, IRATEMONK, SWAP, WISTFULTOLL, HOWLERMONKEY, JUNIORMINT, MAESTRO-II, SOMBERKNAVE, TRINITY
Monitor surveillance	1	RAGEMASTER
Keyboard	1	SURLYSPAWN
USB Connector	4	COTTONMOUTH-I, COTTONMOUTH-II, COTTONMOUTH-III, FIREWALK
Wireless LAN	2	NIGHTSTAND, SPARROW II
Mobile phones	6	DROPOUTJEEP, GOPHERSET, MONKEYCALENDAR, TOTECHASER, TOTEHOSTLY, PICASSO
Mobile phone networks	9	CROSSBEAM, CANDYGRAM, CYCLONE-HX9, EBSR, ENTOURAGE, GENESIS, NEBULA, TY-PON HX, WATERWITCH
Firewalls	5	JETPLOW, HALLUXWATER, FEEDTROUGH, GOURMETTROUGH, SOUFFLETROUGH
Routers	4	HEADWATER, SCHOOLMONTANA, SIERRAMONTANA, STUCCOMONTANA
Servers	3	IRONCHEF, GODSURGE, DEITYBOUNCE

Table 2.2: The NSA's Advanced Network Technology Division's Tailored Access Operations catalogue of technology attack types and code names.

The techniques in Table 2.2 provide an insight into the access requirements for a target. Just as some of the early Russian exploits during the Cold War relied on interception during transit, so too do many of these exploits – for example, in network router firewall devices.

The use of illumination techniques also illustrates the continued development of the Great Seal illumination transponder technique from 1952. Illumination as a technique forms a case study in Chapter 4.4.1.

The ANT catalogue has attracted the interest of very capable electronic hobbyists who have created a community project to methodically work through the complete ANT catalogue collection in order to replicate the techniques, including the illumination technique (NSA Playset 2016).

2.4.8 Eavesdropping Events 1991 to 2019

Literature, academic papers and books, have made an excellent contribution revealing historical eavesdropping events, but less helpful revealing more recent events. The 1990s witnessed a period of significant internet growth with home computer ownership becoming commonplace. The introduction of Wi-Fi enabled greater use of portable equipment in the home too. Low-cost GSM telephone network provision, coupled with the smartphone introduction, changes the nature of information availability.

Although the internet enabled instant news, the technical details of eavesdropping events were often absent or reported incorrectly, requiring expert interpretation. The World Wide Web in its early evolution was dominated by the English language adding bias in reported incidents.

The internet today (late 2019) offers the ability via Google Translate to search for incidents in other languages. It is hard to be certain of the most popular languages on the internet; the most spoken languages in the world, based on population, may not necessarily be the most common language on the internet. The changing nature of internet penetration will continue to evolve, along with the languages used. From a survey conducted in November 2015, of 3,366,261,156 users, bias for both languages used on the internet and the internet user base

can be seen (Miniwatts Marketing Group 2015, 2018). The most common languages used on web pages are reported to be English, followed by Chinese, Spanish and Arabic. However Russian, German and Japanese are also frequently found. Since this research is focused on eavesdropping, Russian, German, Chinese, Spanish, Japanese and Arabic may serve to provide further coverage of eavesdropping incidents.

The following eavesdropping events within this period is almost certainly incomplete. However it provides an insight into the changing nature of eavesdropping.

Jealous Partners & Domestic Incidents

2006, May: The Malham village hall rose to fame with speculation about the WI and jam recipes. However, the focus of the bug placed inside a double 13A socket was a long-running dispute over rights of way across the village green had led to the parish council having to go into secret session when discussing the matter. The mains powered FM transmitter and microphone was discovered by an electrician (Stokes 2006).

2016, May: A girl in the later stages of primary school was at the centre of a family court dispute between her separated parents. Between November 2014 and March 2016 two bugs measuring no larger than 3 x 1.5 cm were bought on the internet and sewn into to a false bottom to the breast pocket of the girl's school blazer and raincoat just before she left for school to ensure the battery lasted all day. At the end of the day, the bug(s) would be removed from the clothing so the contents could be downloaded. The other devices used were an iPhone and an iPad left running in the breast pocket of the father or left in the partner's handbag in the room where the conversation was likely to occur. The father said "*This should hardly need saying, but nowadays it is all too easy for individuals to record other people without their knowledge. Advances in technology empower anyone with a mobile phone or a tablet to make recordings that would be the envy of yesterday's spies,*" (The Belfast Telegraph 2016).

2016, October: A man from Stoke-on-Trent attacked his girlfriend after a microphone he had planted in the television allowed him to monitor what his girlfriend was getting up to when he

was out (Daily Express 2016).

2017, March: In Scotland, a rugby star filmed an attack on his estranged wife's new partner after bugging her home to catch them together, a court heard. After the incident, the former world cup star's estranged wife drove home to find her estranged husband "pulling wires out of the hall" (Sabur 2017).

2017, May: In Greater Manchester, a jilted husband installed cameras and recording equipment around his matrimonial home in order to secretly tape his estranged wife's conversations for use in a custody battle for their four children. The wife discovered the device when a red light was spotted on top of her fridge (Burford 2017).

2018, February: In New York, a man was caught bugging his tobacco heiress' wife's phone during a bitter divorce case which the judge in Brooklyn has said that doing so will negate any claims of the family's wealth (Denney 2018).

2018, April: An American school in Maryland called Prince George's school found a video recording device in the school's administration office following several months of controversy due to a scandal involving graduation rates and the awarding of substantial pay raises to some officials (C. Williams 2018).

2018, April: A mother from Louisiana in the USA sent her severely autistic twelve-year-old son to school with a hidden voice recorder in his backpack after her son had started becoming aggressive, wetting his bed and had increased anxiety. The shocking recovered audio resulted in the firing of two school teachers (Knox 2018).

2018, September: A stalker in Bradford listened to two hidden audio and video cameras installed in mains socket adapters more than one thousand six hundred times over the course of fifteen days in order to provide a live feed of his ex-girlfriend's home. One of the devices was installed behind a TV in her bedroom (Perrie 2018).

2018, September: A Metropolitan Police Officer from Maidstone in Kent used a device he purchased from eBay to bug his ex-wife's bedroom (Bayliss 2018).



Figure 2.43: A Taiwanese-made GSM audio bug purchased online in the UK in August 2019 for less than a pint of beer in London. The insertion of a SIM card would make this operational. The single printed circuit board could be removed from the case and hidden in any other electronic equipment in order to provide access to a permanent power supply arrangement. The GSM network availability is the critical egress path.

2018, October: In Kuwait City, a Kuwaiti employee of the Ministry of Awqaf and Islamic Affairs informed Fahaheel Police Station that a recording device had been found in her SUV car by garage employees during a car service. The incident was reported to the police in the hope of discovering who had planted the recording device (Nayef and Al-Sanousi Al-Seyassah 2018).

2018, October: In Florida, USA, a couple were onboard the Carnival Fantasy for a three-day Caribbean cruise when they noticed the video camera and transmitter, hidden adjacent to other TV wires and was pointing at their bed. The device did not have a recording capability and must therefore have been received within close proximity of the couples cabin. Who carried out the attack is unknown (Inside Edition 2018).

2018, December: In Swansea in the UK a jealous husband bugged his estranged wife's house and car (Spillet 2018).

2019 January: In New Zealand a jealous husband tracked his wife's car (The Daily Mail 2019)

Political

1999, December: Mr Adams reported that a bug, two-foot-long with digital tracking capability, had been found built into the skin of his Ford Mondeo car used to transport himself and chief negotiator Martin McGuinness during the Mitchell Review. Later, in April 2003, The Times newspaper published what were said to be transcripts of secretly recorded telephone conversations between Mr McGuinness and senior government officials (Anon 2003; Mullin and White 1999).

1999, December: In Washington, Stanislav Borisovich Gusev, a KGB technical officer working under diplomatic cover, was filmed listening to a bug he had planted in the State Department. He had the bag next to him, one hand in the bag, and an earphone plug was in his ear with the wire snaking into the bag. The FBI named the whole operation “Sacred Ibis” and concluded that a listening device had been placed inside the State Department’s rear facade. Eventually the device was located on the seventh floor in a conference room concealed inside a chair rail moulding (Booth 2017; Leob and Vise 1999; Seper 1999).

2001, 5th October: Alastair Campbell’s diary reveals that Tony Blair’s bedroom was bugged. From the brief text within his diary “... at the hotel, our security service guys had found two bugs in TB’s bedroom and said they wouldn’t be able to move them without drilling the wall”. This suggests that the bugs were not radio transmitters but microphones mounted deep within the walls. It is surprising and unlikely that such microphones were found so quickly. This incident report should be treated with caution and lacks credible detail.

2003, March: Four bugs were found in the Justus Lipsius building within the headquarters of the Council of the European Union in Brussels. Five black boxes were discovered hidden in the concrete walls of the building. The telephone lines of the delegation rooms of France, Italy, Germany, the UK, Spain and Austria were tapped. They were thought to be in place to reveal the position of EU member states on the US and UK invasion of Iraq. An official enquiry in 2010 pointed to Israeli secret services as a potential culprit (Belgian Standing Intelligence Agencies Review Committee 2011; Black 2003; Clerix 2003).

2004: In Australia in East Timor, a huge spy scandal arose in 2004 when the Australian Secret Intelligence Service (ASIS) planted 200 covert listening devices in the Timor-Leste Cabinet Office at Dili (Allard 2006, 2014).

2004, September: Sinn Féin made public the “sophisticated bugging device” comprising a number of battery packs, along with a microphone and transmitter, and found by workmen in the living room ceiling of the home of a women who worked at the Sinn Féin’s party president’s constituency office. The discovery was ahead of political talks at Leeds Castle in Kent (BBC 2004).

2004, December: A “wood-stick” bugging device had been discovered in the Autumn behind wooden panels in the course of renovation work in the Salon Français, at the UN’s European headquarters in Geneva. An investigation failed to determine who planted the device however, the discovery echoed allegations by Clare Short, the former British cabinet minister, that Britain had bugged the office of the UN secretary-general, Kofi Annan, in 2003 during the run-up to the invasion of Iraq. Ms Short said she had seen transcripts of Mr Annan’s conversations (Whitaker 2004). The device created interest from experts who conducted detailed technical analyses (Atkinson 2004).

2009: In Ekaterinburg, Brothel; An American diplomat was caught on video in a Russian honeytrap. The diplomat was filmed with a prostitute in the brothel by a hidden camera placed at low skirting board level. The low quality and grainy black and white video footage was enough to cause considerable embarrassment when the footage was released onto the internet (Stewart 2009).

2011, May: In New Zeland, a listening device was discovered by Government Communication Security Bureau (GCSB) staff, ahead of the November election, at government ministers’ homes. At least one listening device was found but no further details are available. Electronic devices that are recovered are sent to the bureau’s “Black Museum” in Wellington (Marshall 2011).

2013, July: A bug was found in the Ecuadorian Embassy in London, the then home of Wikileaks founder Julian Assange, in a socket behind a light switch by technicians reviewing the wiring.

The bug was a GSM device crudely powered by the internal components of a USB power supply (BBC 2013).

2014, June: In Northern Ireland, a dissident republican from Lurgan, County Armagh, found what appeared to be battery packs and a transmitter hidden behind the rear bumper of his car and were believed to be attached to a listening device hidden somewhere in the vehicle. There was also a smaller device, believed to be a GPS locator that would have enabled those who planted it to track his movements (Kearney 2014).

2015, October: The dissident artist Ai Weiwei returned to Beijing, China after his first overseas trip in four years to discover listening devices hidden behind electrical sockets in his studio. The devices were discovered when the studio was being renovated and suggested that they may have been placed there four years ago. Weiwei shared the discoveries in a series of Instagram and Twitter posts, together with a video and pictures of the devices (Ryan 2015; Weiwei 2015).

2016, July: Council workers in Scotland used listening devices hidden in suitcases as well as covert cameras to snoop on blue badge cheats, nuisance neighbours and illegal money lenders (The Scotsman 2016).

2016, October: In Ottawa, Canada, workers preparing the former Nortel complex as the new home for the Department of National Defence were reported to have discovered electronic eavesdropping devices. Security officials informed journalists however that they had not discovered any bugs or listening devices. Privately, the journalists were informed that older spy devices might indeed have been discovered but were not functioning (Pugliese 2016).

2017, March: In Guantánamo, Cuba, a released report illustrated a “smoke detector” microphone that was found inside the US Navy base meeting room at the prison’s Camp Echo compound. The meeting room was used by attorneys when they met their captive clients for years at in Cuba. The Pentagon declined to comment (Rosenberg 2017).

2017, July: In South Africa police investigated claims of “covert” bugging at the office of South Africa’s Olympic sports body, Sascoc, and at the home of its chief executive. A technical investigation report revealed that active devices were transmitting and receiving over GSM and

Bluetooth. The signals were mainly from the second floor and that the executives office were the focal point for the surveillance (Bezuidenhout 2017).

2017, July: In Ghana, a minister at the forefront of the nation's fight against illegal mining, since he was appointed in January 2017, was bugged. An audiovisual recording device which included a camera, a storage unit and another device suspected to be a transmitter, was planted in a huge Coat of Arms plaque hanging in the Minister's office. The device was reported to be highly sensitive and could pick a whisper 35 feet away and was neatly housed in a black metal box and used batteries (Ghana Web 2017).

2017, December: In Dublin, the Garda National Surveillance Unit planted a sophisticated listening device in the snug of the Coachman's Inn on the Airport Road, which recorded the conversations between two Irish dissidents of a plot to carry out an operation involving explosives during the run-up of the State visit of Prince Charles in 2015 (MacDermott and Hickey 2017).

2018, January: In Vienna, the office of an Austrian far-right leader and vice chancellor was broken into shortly after bugging devices were discovered behind a mirrored wall by intelligence service specialists. They were reported as being discovered after a routine check when moving into a new office (Knolle 2018).

2018, January: In Addis Ababa, at the new headquarters of the African Union which was constructed by Chinese workers as a *Gift of China to friends of Africa* was allegedly targeted. The small African Union computer department became suspicious when its computer servers were found to be active with high volumes of data transfer between midnight and 2 am, despite the offices being completely dormant (Tilouine and Kadirir 2018).

2018, February: In Northern Ireland, an elaborate listening device was discovered in the home of a former senior republican and former IRA commander. The 'bug' was discovered by a young relative, who had been living in the west Belfast property for several years, and discovered the listening device concealed in a ceiling during recent renovations (Morris 2018).

2018, April: A Wi-Fi interception attack occurred against the Organisation for the Prohibition

of Chemical Weapons (OPCW). In-depth discussion of the methods used to hack into Wi-Fi system is best left for other authoritative experts and is covered extensively in other security journals. Equipment is readily available for the amateur enthusiast using the software suite such as BackTrack which first became available in 2006. BackTrack continued to be developed and was renamed Kali Linux in 2013 (Kali-Linux 2013) which provides a host of programs designed to eavesdrop on wireless networks. Many commercial systems exist that provide the ability to monitor Wi-Fi with small lightweight interception receiving equipment. The NSA's Tailored Access Operations group implant catalogue (United States National Security Agency (NSA) 2013) lists the lightweight product SPARROW II (See Figure 2.44).

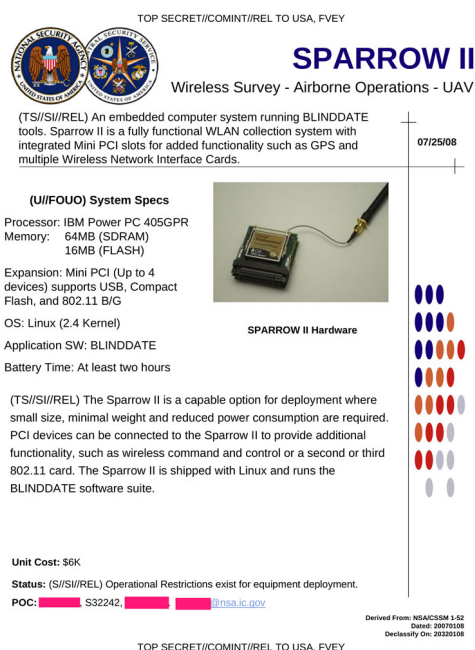


Figure 2.44: Light-weight aerial borne system for Wi-Fi interception.

Wi-Fi operates on one of two frequency bands; 2.4GHz or 5GHz. 5GHz suffers from attenuation by physical structures (walls and glass) to a greater degree than Wi-Fi systems that operate on 2.4GHz. The potential for eavesdropping thus decreases with 5GHz, as the coverage range will likely be reduced, but high-gain and directional aerials are available for either band, which will make an eavesdropper's task possible.

With the range of interception equipment available it is surprising that more evidence of Wi-Fi interception and eavesdropping do not become known. One such example of close access interception of Wi-Fi occurred in April 2018 when four GRU computer experts travelling under diplomatic passports were caught by the Dutch Security Services attempting to monitor the

Wi-Fi networks of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague in the Netherlands.



Figure 2.45: GRU Wi-Fi monitoring equipment mounted in the boot of a hire car used against the OPCW in 2018. The coat on the rear parcel shelf hides a Wi-Fi patch antenna. Below the shelf is the computer attached to a Wi-Fi dongle, large battery and power stabiliser and a GSM telephone that provides a remote data network connection.

Following the poisoning of a former Russian military officer Sergei Skripal, and his daughter Yulia Skripal, in Salisbury in early March 2018 by the Russian Novichok nerve agent, the Russian GRU were keen to establish any information available from the OPCW regarding the investigation into this incident of chemical weapon use.

The GRU deployed Wi-Fi interception equipment in the boot of a hire car (see Figure 2.45). The car was parked as close as possible to the OPCW building and a directional antenna, hidden on the back parcel shelf, provided antenna gain in the direction of the OPCW building. A cellphone connection into the equipment enabled the GRU to connect to the equipment from a safe distance.

2018, August: A tweet from a political reporter in Washington, Yashar Ali, stated that “several current and former White House/Trump campaign staffers ... are concerned that Omarosa

used a pen that has the capability of capturing audio to surreptitiously record meetings”. This was raised after the possibility that secret recordings had been made in the White House despite recording devices being prohibited (Hampton 2018).

2018, November: Secret listening devices have been discovered in the Kiev Central Synagogue on thirteen Shota Rustaveli Street. The bugs were found during a sweep inside the “House of God”. High-level law-enforcement officials in Ukraine were suspected of mounting the surveillance operation (JTA 2018a,b).

Sex Crimes

2018, May: In Boston, an employee of a Massachusetts daycare centre placed a recording device in a bathroom. The police later discovered a further three devices of the pen-like recording device (Germano 2018).

2018, October: In Cedar Rapids, Iowa, a basketball coach was charged with secretly recording his teenage players undressing (The Associated Press 2018).

2018, November: In Binghampton, in the USA, a man is accused of installing a video device in a residential bathroom (Borrelli 2018).

2018, November: An Iwowa Park Man, in Texas, was charged with inappropriate video recording after placing a camera on the bottom of a door in a bathroom (Garcia 2018).

Terrorist and Criminal

2009, September: Secret footage of terrorists planning an airline bombing has been revealed. Anti-terrorist police and MI5 concealed a camera and hidden listening devices inside a terrorist’s flat in the summer of 2006. The film was shot using a “fish-eye” lens from ankle height. A second camera, hidden across the street, captured the men arriving and leaving the flat. Grainy black-and-white footage from the camera was shown to jurors at Woolwich crown court (The Evening Standard 2009).

2013, September: Rogue routers were installed in Santander and Barclays Bank in two separate incidents by a bogus maintenance engineer. The router was connected to a keyboard video mouse (KVM) switch which enabled remote monitoring of bank clerks' terminal operation. Twelve men were arrested by Scotland Yard's E-Crime unit (Curtis 2013).

2015, August: In Johannesburg, South Africa, three men were found to be in possession of a cellphone intercept device purchased under false pretences when fraudulently acquired by a letter of authority from the South African government. The Israeli manufactured equipment was capable of cellphone-tapping, tracking and locating and is known as "The Grabber" (Maphumulo 2015).

2018, January: In Scotland, the head of Organised Crime and Counter Terrorism, revealed that criminals were using sophisticated commercially available car tracking devices, the size of packets of cigarettes, to stalk their underworld rivals and then commit violent assault. Trackers were also being used by the criminals to keep tabs on drug consignments (Silvester 2018).

2018, October 2nd: The shocking murder of the dissident Saudi journalist Jamal Khashoggi on the 2 October 2018, within the Saudi Consulate in İstanbul, Turkey, is of interest to this research for two reasons: (i) that his murder may have been the result of his WhatsApp messages being intercepted by the capable Pegasus spyware which may have been installed or targetted against Khashoggi's mobile telephone and (ii) the knowledge that audio recordings were made of Khashoggi's murder. In a BBC Panorama broadcast conversations take place with the very few people that have heard the audio recordings (Corbin 2019). The programme concerned the Consulate audio surveillance conducted by the Turkish National Intelligence Organization and that the installation was in place before Khashoggi entered the Consulate, as the tapes revealed the conversations of the preparation for Khashoggi's murder, suggesting that the installation was already in place. These facts end speculation that the audio was derived from Khashoggi's own mobile telephone using a feature of the Pegasus software and that the audio was from a professionally mounted microphone (or microphones) system installed by the Turkish National Intelligence Organization. No further details are known about the audio installation other than that the Turkish authorities were increasingly concerned with political instability.

One report from June 2004 reports that the Turkish authorities admitted to bugging the British Ambassador's telephone (Erdem 2004). Furthermore, a newspaper report from October 2013 announced that the Turkish National Intelligence Organization had a museum in Ankara of Cold War exhibits with later equipment unavailable for viewing (Hürriyet Daily News 2013).

Police Operations

2017, August: In Christchurch, New Zealand, an investigation into unauthorised bugging at Christchurch Men's Prison in relation to prison staff's use of covert listening devices to intercept private communications. The staff had bought eight covert listening devices from October 2014 to August 2016 and used them to intercept private communications. Covert cameras were used too outside the prison building perimeter and around the boundary fence, to identify where contraband was being dropped at night (New Zealand Herald 2017).

2013, April: In Derby, the police, under the Regulation of Investigatory Powers Act 2000, hid microphones at the hotel of suspects, the night before they were due to hold a press conference, as they were suspected of deliberately starting a house fire. The Assistant Chief Constable of Derby Police said that "The decision is never taken lightly and it is not a tactic we deploy regularly. We have to ask ourselves whether it is proportional, whether it is legal and whether it is necessary" (Britten 2013).

Financial and Industrial

1997, April: In Vienna, Austria, foreign agents are believed to have planted bugging devices in the walls of the Marriott hotel on Vienna's Imperial Ringstrasse. They were found during renovation in three rooms but it was impossible to say how long they had been installed and at whom they were targeted. The plush hotel has long been favoured by oil ministers and delegates of the Organization of the Petroleum Exporting Countries (OPEC) which is based in Vienna and ministers met there twice a year (Alexander's Gas & Oil Connections 1997). It is not the first time OPEC has been targeted. In the late 1970s, a meeting room at the

headquarters of OPEC was bugged with a small sophisticated covert listening device installed behind the wiring of the PA system (Museum 2016).

2013, September: In Glasgow, a tribunal heard how a director's office had been bugged with two devices amid fears that she was about to jump ship to her ex-husband's new company. The device recordings required tapes to be replaced (Callaghan 2013).

2014, July: In Michigan, USA, listening devices had reportedly been found in meeting rooms at Ford's US headquarters amid investigations into alleged industrial espionage by a sacked engineer. It was thought that the sacked employee was stealing trade secrets by hiding recording devices in meeting rooms. The employee admitted to hiding recording devices under tables to help her transcribe meetings (S. Campbell 2014).

2016, August: The All Blacks Rugby team hotel conference room was found to have a bug in a chair. The team's former security consultant Adrian Gard was thought to have placed the device in the chair's foam covering. Pulling back the foam revealed "what looked like a battery and some wires sitting in the foam of the chair and the wire running on top of the foam". This is an odd event clearly conducted by an amateur (Downs 2016).

2018, April: In Gibraltar, two crude listening devices had been found under tables in a Europort restaurant and are believed to be linked to similar bugs found in the Gibraltar Financial Services Commission in Atlantic Suites on Europort Avenue four years earlier (Reyes 2018).

2018, May: In the Central Bank of Curaçao and St. Maarten in the main building in Willemstad, eavesdroppers were detected within the bank after the bank's personnel reported a sense that they had been listened into. None of the devices were active when found and have since been removed (The Daily Herald 2018).

2018, August: In Port Talbot, South Wales, the police used a secret bugging device in the home of an amateur boxer to record the confession that he killed his girlfriend (Walford 2018).

2018, October: In Jamaica, an investigator at the Independent Commission of Investigations (INDECOM) admitted to supplying an accused murderer Constable Collis 'Chucky' Brown with a recording device to record his peers and superiors (Wilson 2018).

2.5 Chapter Discussion

This chapter provides a unique research focus on eavesdropping incidents over a period of one hundred and twenty years from the early twentieth century to present day. Figures 2.46 and 2.47 reveal a macro view and the changing nature of historical eavesdropping incidents.

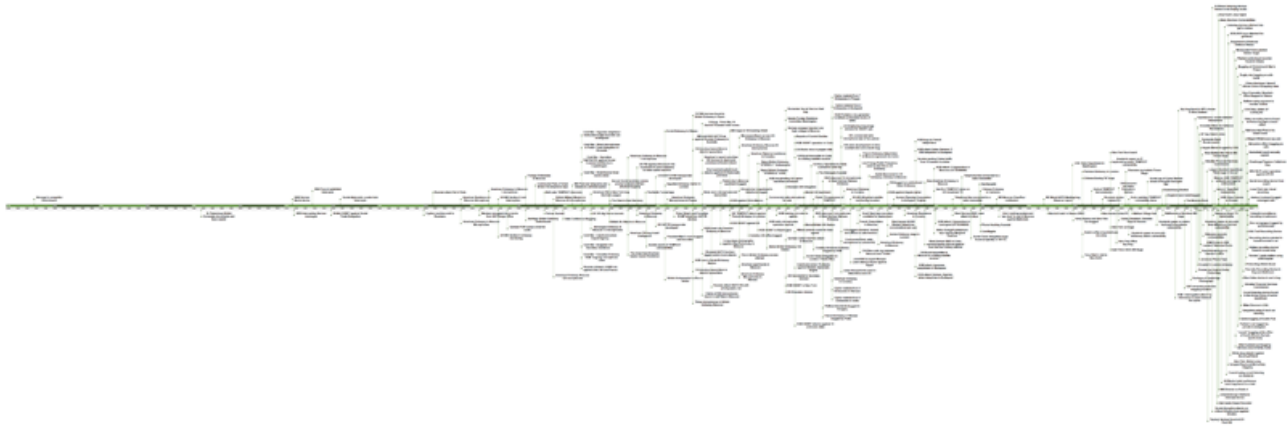


Figure 2.46: A summary of all known eavesdropping events from 1900 to 2019. The diagram illustrates the relative number of eavesdropping events across the decades. All events plotted are recorded within this thesis.

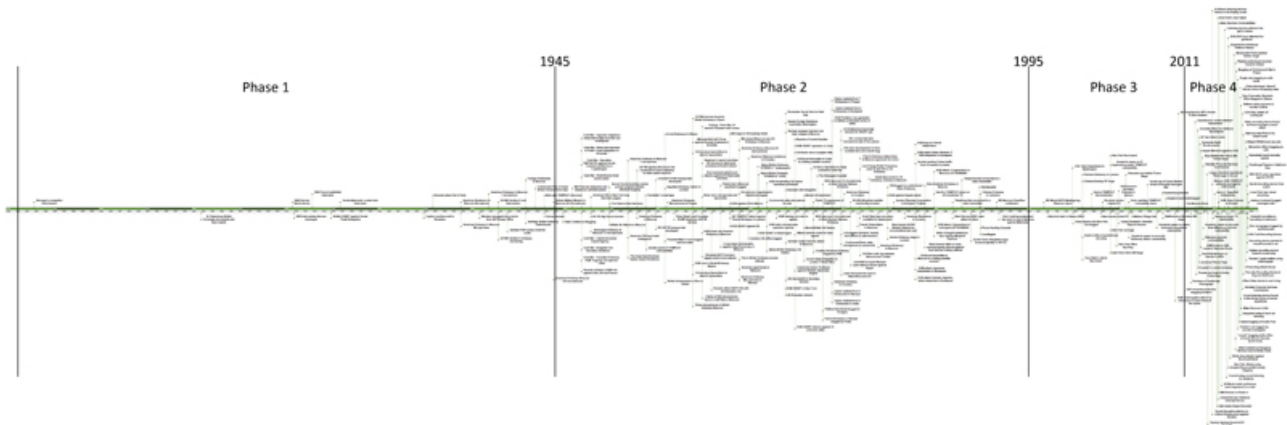


Figure 2.47: The four phases of distinct electronic eavesdropping in history: Circa 1900 to the end of the Second World War in 1945, from 1945 to the end of the Cold War in circa 1990, from 1990 with the rise of the internet to 2011 and from 2011 to 2019. The rise in eavesdropping incidents since 2011 are dramatic. Details of these incidents are available in Appendix B.2. These incidents are not cyber related.

Figure 2.46 illustrates on a timeline spanning one hundred and twenty years, all known eavesdropping incidents collated with the purpose of highlighting the macro patterns of activity, rather than the individual micro detail of each event.

When all eavesdropping activities are plotted, identifiable patterns of activity are exposed and

four phases of eavesdropping activity become visible: The periods 1891 to 1939, 1940 to 1990, 1990 to 2011, 2011 to present day 2019.

The incident in growth in 1945 is distinctive and the reason well documented but the decline in 1990 is also evident. The end of the Cold War is an obvious reason but my inclination is to suspect that the analogue mobile telephone became highly popular worldwide, as did the rise in internet usage and the home computer. This enabled eavesdropping to transition away from close access activities.

Further analysis of the four eras is as follows:

2.5.1 Phase 1: The period 1891 to 1939

This period illustrates the very beginning of electronic eavesdropping. A period reliant on agents with access, whether it is to a telephone switchboard or a trusted local employee with access to the key and locked documents within an embassy. Politics and war create immense distrust with greater risks taken to obtain information from any available source.

There are only a handful of incidents in this period. The 1920s Old Admiralty Building Room 40 SIGINT operations against the Soviets are a highlight within this period and there remain only a small number of wired microphone incidents known. Although some commentators mention that the Soviets were routinely listening into the conversations of diplomats living in Moscow, very little evidence has materialised. The shift in activity occurs at the end of this phase. Just when Hitler's army were an immediate threat to the citizens of Moscow and the battle for Moscow was underway, the Soviets were busy installing wired microphones into many Western embassies.

2.5.2 Phase 2: The period 1940 to 1990

The wired microphone dominates the eavesdropping activities of Soviet bloc and Western allies up until the point that the transistor was invented. This enabled a hidden transmitter to be

connected to a microphone and installed quickly by anyone with access to the target of interest. The radio microphone enjoyed a great deal of success by the agencies of the KGB/CIA/SIS in the activity hotspots of Beirut in the 1970s and the English-speaking African colonies vying for political supremacy over the emerging African independent states.

Eavesdropping becomes a despised tool through its use to control the people of the German Democratic Republic, which spied on its citizens until up until its collapse. The eavesdropping operations relied heavily on wired microphones installed in peoples homes; six thousand concurrent monitored microphones in Berlin alone.

Eavesdropping activity continued to be driven by political mistrust and the technology became smaller and ever more portable, created by capable government agencies. Audio was the predominant eavesdropping method but eavesdropping on communications equipment was always a focus of the more capable nation. If access could not be obtained to the target's communications equipment, SIGINT or TEMPEST techniques provided routes to access. The entry into space and the ability to eavesdrop over greater distances became a focus of the Americans and the UK.

It is interesting to note that there are no examples of radio microphone use in Moscow. The Soviet Security Services appear to have used radio microphones "overseas" but perhaps had no requirement to do so on home soil alluding to their wired microphone networks in place and the extent to which they controlled all aspects of their home environment.

2.5.3 Phase 3: The period 1991 to 2011

This period is an interesting point in time for electronic eavesdropping for three reasons: (i) The changing nature of the political landscape with former Soviet republics regaining their independence after the dissolution of the Soviet Union in December 1991, soon after the 1989 fall of the Berlin Wall, (ii) The change in networked computing and the take-up of the internet and the home computer and finally (iii) The growth of the unsecured analogue mobile telephone. The opportunities to eavesdrop increase considerably.

However, when the incidents are reviewed in this period they can be seen to relate predominantly to government eavesdropping operations. The Iraq War may be responsible for many of these events with governments taking risks desperately seeking the opinion of others, perhaps due to information unavailability from human, cyber or SIGINT sources. Other eavesdropping activities relate to Northern Ireland and the end of hostilities as political dialogue takes centre stage.

This period in time creates opportunities for governments to eavesdrop on unprotected emerging IT and analogue telephone networks leaving little or no evidence of any such eavesdropping activity.

2.5.4 Phase 4: The period 2011 to 2019

This phase is distinctive and relates to the continued rise in the internet, proliferation of very easy to obtain consumer eavesdropping equipment and smartphone software applications with features to track and monitor. Notable items are:

- The GSM bug for use in the home or the car. The very low consumer purchase price and low-cost ‘SIM card only’ consumer contracts combine to make a powerful eavesdropping capability;
- The MP3 voice recorder is housed in a myriad of disguises. The low-purchase price, low-power consumption and long solid state memory recording times combine to provide a powerful eavesdropping capability;
- The spy cameras, egressed over the internet or recorded onto low-cost solid state memory, and low-purchase cost, combine to make this a powerful eavesdropping tool;
- The myriad of software trojan applications that provide remote control and monitoring of all handset activity via an internet connection. Placed on the handsets remotely by governments or installed locally by partners with direct access to the handset;

- The myriad of apps installed by users of smartphones with little care or attention paid to the granting of access permissions of the applications installed. Data is backed up to cloud servers with unknown security protection.
- The reminder from the Istanbul 2018 event that Consulates or Embassies remain at risk from audio eavesdropping by aggressive National State Security operations.

The phases applied to Figure 2.46 may be compared to the growth of internet users in Figure 2.48 and the rise in mobile growth in Figure 2.49, in order to observe further correlation.

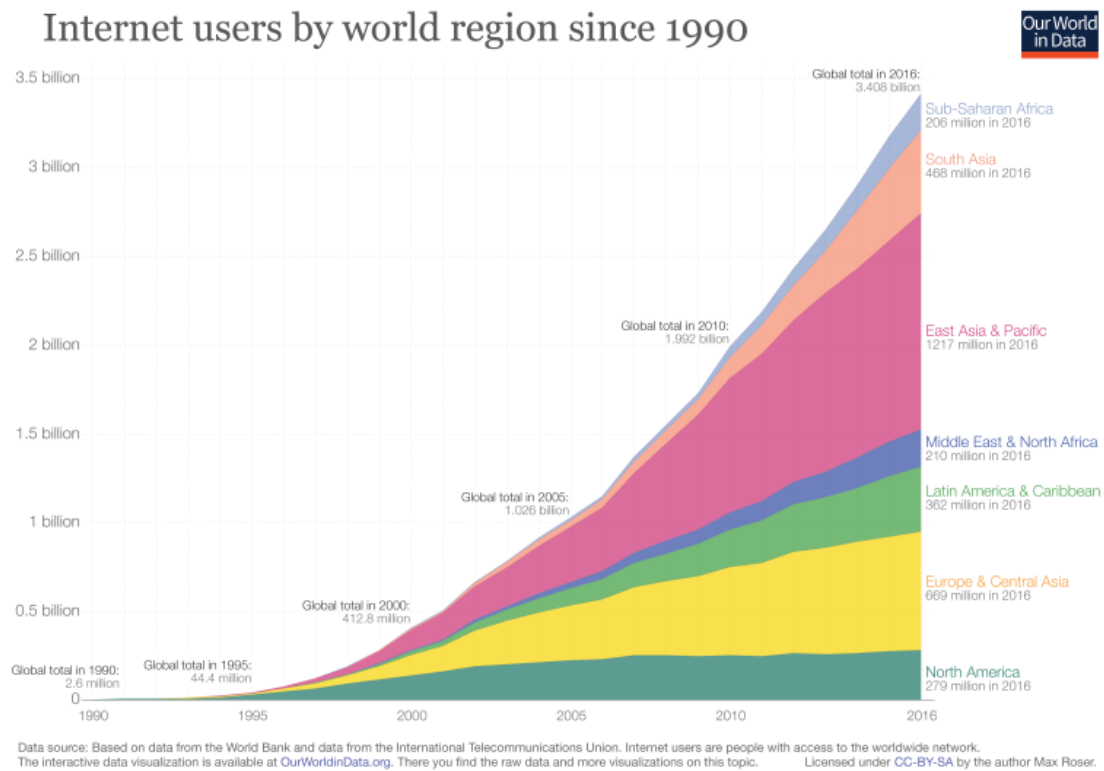


Figure 2.48: Growth of internet users worldwide since the 1990s (Murphy and Roser 2019)

Further detail of the timelines may be seen in Appendix B.2. A macro view of all events revealed from this research:

- Remote Access and bulk monitoring of the internet and mobile telephone networks has reduced instances of audio eavesdropping by governments. Close Access eavesdropping by governments is used for situations that call for immediate, tactical information;

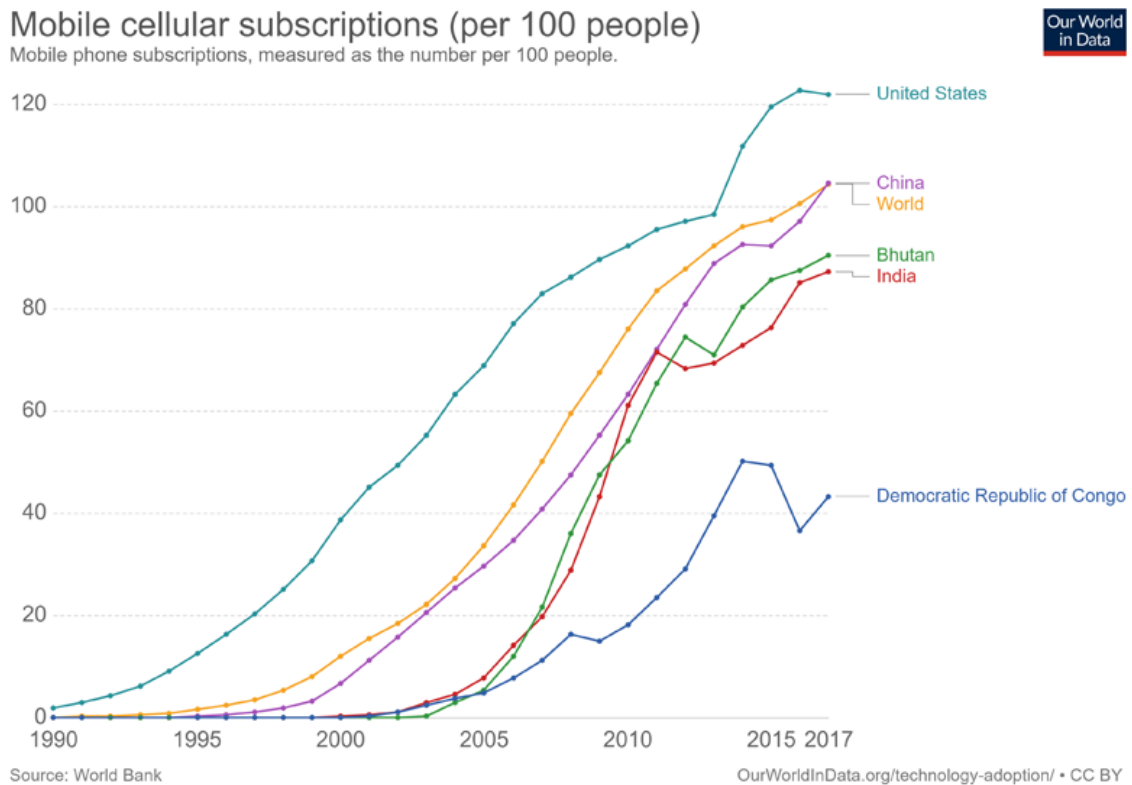


Figure 2.49: The growth of mobile telephone subscriptions worldwide since the 1990s (Murphy and Roser 2019)

- Close Access eavesdropping techniques have become commoditised, low cost and available to all;
- The citizen of today can mount effective eavesdropping attacks against targets so long as they have access to the target;
- GSM bugs and digital audio recorders are ubiquitous: consumer electronics provides a considerable capability to the amateur eavesdropper.

We began with the twentieth century of government espionage reliant on the wired microphone and home advantage. Radio developments and the transistor created ever greater egress opportunities. The twenty-first century has seen the addition of additional egress routes: the internet and the mobile telephone.

The conclusion from this chapter is that the two most critical factors for mounting an eavesdropping attack are access to the target and an egress route. Remove the egress route and you remove the opportunity to eavesdrop.

Chapter 3

Present-Day Intrusive Surveillance Techniques Research

3.1 Chapter Overview

The previous chapter provided a historical analysis of past eavesdropping events that became public knowledge. The focus of this chapter is on the actual technical eavesdropping techniques. The range of techniques available today, as suggested by the previous chapter, appears to have expanded considerably over time.

This chapter researches available eavesdropping techniques in order to understand the changing nature of this technology. The hypotheses are that:

1. The nature of technical eavesdropping attacks continues to evolve such that the technology is no longer solely the preserve of sophisticated and well-funded government agencies, with aggressive security services and an aptitude for technical surveillance;
2. Technology evolution and continuous innovation has lowered the entry barrier requirement for effective audio, data and video eavesdropping;
3. The trend for well resourced eavesdroppers is away from “Close Access” techniques, towards “Remote Access” techniques.

Computer hackers and hostile government spy agencies are reportedly stealing data from victims on a daily basis, but this is a relatively new route for information theft since the rise of the internet. However, eavesdropping by technical means has been in existence for well over 100 years (please see the previous Chapter 2) and is in continuous evolution; every time a new communications method or piece of technology is invented, an exploit will arise and likely be used by a capable eavesdropper.

Eavesdropping, as a topic, has received very little methodical research. It is a technology area shrouded in secrecy and often the subject of imaginative Hollywood scriptwriters rather than reliable facts. Books written on the subject are from the Cold War and relate to espionage activities such as ‘CIA Special Weapons & Equipment: Spy Devices of the Cold War’ (Melton 1993) or ‘The Ultimate Spy Book’ (Melton 2002a). Some too refer to the East German Stasi secret police as portrayed in the 2006 film ‘The Lives of Others’ (Florian Henckel von Donnersmarck 2006), and ‘Seduced by Secrets: Inside the Stasi’s Spy-Tech World’ (Macrakis 2014) which provides details of microphones used against the citizens of East Germany. Stasi publications focus on the repression of citizens rather than the technical details of the eavesdropping techniques. Books written for amateurs and hobbyists provide simple schematic diagrams to enable the would-be amateur spy to build their own equipment. Publications such as ‘A Complete Survey of Electronic Surveillance Today’ (Wingfield 1984), ‘Electronic Surveillance Devices’ (Brookes 2001) and ‘The Bug Book: Everything You Ever Wanted to Know about Electronic Eavesdropping but Were Afraid to Ask’ (Shannon 2000) are written for entertainment purposes and hobbyists with a passing interest in electronics.

A taxonomy of technical attacks is not available; therefore this research sets out to:

- Systematically understand the components of eavesdropping technology past and present;
- Understand in what way aspects of the technology repeat themselves through history;
- Understand what purpose different technologies address;
- Understand the changing capability that continuous innovation and evolution offers those who wish to use technology for eavesdropping purposes;

- Understand what technology is reserved exclusively for governments with technical expertise and large resources at their disposal and to contrast this with technology available to most citizens.

While politics and crime will always attract reporting of events that take advantage of eavesdropping technology, this chapter's focus is on the technology, not on the victims of the technology.

3.2 Method

In order to collate a comprehensive catalogue of techniques, subject area specialists were assembled to facilitate expert elicitation workshops. Access to a department of technical specialists dedicated to the protection of high threat establishments worldwide, created an opportunity for the identification and collation of technical attack methodologies and the codification of a department's knowledge on intrusive surveillance techniques spanning the early days of the Cold War to present day.

A structured brainstorming Nominal Group Technique workshop utilised within this group of experts codified their specialist knowledge across a broad range of access methods and technologies. The structured brainstorming Nominal Group Technique (Delbecq, Van de Ven, and Gustafson 1975) was selected for this group of experts because the anonymous generation of ideas, by writing down a single answer on a sticky note without discussion, ensured all attendees within the group assembled where able to freely contribute on an equal basis. Techniques and access methods were generated without being influenced by others in the group. The group assembled were keen to work together too as it was an opportunity for all attendees to demonstrate, in an almost competitive nature, their subject area knowledge.

As each eavesdropping technique was generated, the sticky notes were placed on a wall and grouped as unique and non-unique; duplicates were discarded but variants were retained. With a group of thirty experts present, the number of techniques generated increased quickly. After

the pace began to slow, the experts were asked to review the techniques identified and asked to add additional techniques that came to mind. This iterative process was an important step in adding further eavesdropping techniques and variants as memories were jogged by the growing list of techniques gathered.

The group assembled were asked two questions:

1. What ‘Close Access’ technical eavesdropping attack techniques might an attacker carry out, if access to the target were available?
2. What ‘Remote Access’ technical eavesdropping attack techniques might an attacker carry out, if close access to the target were not available?

3.3 Results

The complete collection of Close Access and Remote Access techniques generated by the workshop was collated and documented with the results shared amongst participants for final expert verification. The collection was evidenced based and supported by real-world examples where ever possible.

3.3.1 Close Access Techniques Identified

The techniques naturally grouped into themes around a particular variation relating to an egress route or situation. These themes are listed under the categories and subcategories.

Category	Subcategory
Wire Tapping for Audio and Data	Simple inductive taps
	Cabling infrastructure (tampering and patching)
	Concealed in walls - microphone attached to a sound tube
	Microphones egressed via very thin wires
Telephone Network Taps	Public switched telephone network (PSTN)
	Mobile telephone network operators taps
	Legal interception
Conference Room Facility Vulnerabilities	Projectors and projection systems
	Conference room radio microphone systems
	Podium microphones
	USB connecting leads to users' laptops
	Plugging memory sticks into unknown equipment
	Acoustically poor conference rooms
	Event staff - uncontrolled and non-vetted
Building Construction Opportunities	Wired microphones
	Optical fibre microphones
	Deep plant microphones built-in during construction
	Deep plant accelerometers built-in during construction
	Self-drilling microphone
	Gap jumpers egressing secure environments
	Concealed cabling within other building components
Disposal Chain	Paper assets
	Redundant computer equipment
IT Hardware Exploits	Personal computer hot-wired
	Video eavesdropping - non-TEMPEST equipment
	Video eavesdropping - external KVM switches
	Video eavesdropping - replaced video cables
	Audio eavesdropping - hardwired internal microphones
	Keyboard eavesdropping - hardware-based keyloggers (external)
	Keyboard eavesdropping - hardware-based keyloggers (internal)
	Keyboard eavesdropping - radar illuminated
	Eavesdropping through printer hardware-based additions
	Eavesdropping through modified USB ports
	Hardware eavesdropping on networks – via computer power lines
	Disguised equipment cases
IT Firmware/Software Exploits	Video eavesdropping - built-in applications
	Audio eavesdropping - built-in applications
	Eavesdropping through server bios exploitation
	Eavesdropping through poor printer configuration
	Eavesdropping through modified router software
	Eavesdropping through modified firewall software
	Eavesdropping through local software execution
Photography Opportunities	Document eavesdropping by photography
	Neckties with concealed cameras
	Buttons with concealed camera lens
Office Telephone System Exploits	PABX exchange exploits
	VoIP telephones
	Compromised analogue telephones
	Microphone created by switch-hook bypass in analogue telephone
	Modified telephone to become microphonic
	Microphone created by switch-hook bypass in an analogue telephone
	Microphones concealed in telephone Equipment
	Telephone line connected to a radio transmitter
	Telephone line egress of microphone audio through remote activation

Telephone line egress of microphone audio with low-frequency carrier	
Office Equipment Eavesdropping	Modified photocopiers
	Access to hard drive within photocopier
	Modified shredders
	Modified calculators
	Modified intercom systems
	Modified typewriters
	Modified teleprinters
	Modified printers
Consumer Portable Electronic Devices	Professional grade credit card recorder
	MP3 recorders
	iPods with built-in recording devices
	USB memory stick with audio recorders
	Watches with cameras and USB memory
	Pens with RF speech transmitters
	Pens with audio recorders
	Pens with digital video recorders
	Pens with video transmitters
	Pens with handwriting capture
	Cameras concealed inside everyday objects
	Smart glasses
	Tablets
	Smartphones with cameras, microphones, accelerometers and apps
	Analogue recorders using tape or wire
	GSM audio bug
	SIM card copiers
Li-Fi Data Egress over Light	Overt Li-Fi
	Covert Li-Fi
Radio Microphones	Digitally encrypted radio microphone
	Commercially available radio microphone
	Exchange and Mart radio microphone kits
	Broadcast radio (wirefree) microphone
Video Systems	Long-range video systems
	Very low-light systems
	Systems that operate in the dark
	Webcams
	Hidden spy cams
	Security cameras in the high street or protecting homes

Table 3.1: Close access techniques identified by expert elicitation.

3.3.2 Remote Access Techniques Identified

Category	Subcategory
Radio Transmission Emissions	Cordless telephone eavesdropping Analogue cordless telephones Digital cordless telephones In-house hand-held radios (security officers' radios) Baby monitor
TEMPEST Emissions	TEMPEST - radio frequency emanations TEMPEST - optical emanations TEMPEST - optical reflections from other objects TEMPEST - acoustic emanations TEMPEST NONSTOP and HIJACK
Wireless Network Interception	Wi-Fi interception systems Bluetooth interception
Infrared Communications Interception	Infrared headphones Infrared translation systems
Telephone Line Interception	Telephone speech interception Telephone fax interception Broadband data interception
Fibre Cabling Interception	Fibre or "fibre to the cabinet" interception Fibre optic eavesdropping
Point to point links	Microwave voice and data interception Laser free-space optical links
Magnetic Induction	Magnetic loop transmission systems
Mains Supply Interception	Mains egress data or audio systems Audio-video surveillance using a covert mains carrier system Mains socket bug HomePlug data sharing
Building fabric vibrations	Accelerometers attached to structural elements Contact microphones
Probe from adjacent premises	Probe microphones Long-range drilling Near-silent drilling Silent drilling
Acoustic Emissions	Directional microphones Shotgun or rifle microphone Phased array microphones Parabolic microphone Microphones created from loudspeakers
LASER Illumination Techniques	First generation laser microphone Second generation laser microphone Third generation laser microphone Fourth generation laser microphone
Radio Frequency Illumination Techniques	Radio frequency illumination for audio eavesdropping Radio frequency illumination for data eavesdropping
Photography Techniques	Photography - long-range with telephoto lens Long-range photography enabled lip reading Long-range photography enabled text analysis of keyboard entry Long-range photography enabled touchscreen snooping Long-range photography enabled by drones

Mobile Telephone Interception	Legal eavesdropping by national authorities Real-time interception of calls IMSI catching Using bogus base stations for spoofing ('Man in the middle' attacks) Near field communications (NFC) Optical communications via the screen Speech from smartphone gyroscope Acoustic eavesdropping through wireless vibrometry Audio recording application software Taking control by means of trojan software
Supply Chain Interception	Taking control by means of trojan Hardware Silent ring eavesdropping Bluetooth eavesdropping Transmitter concealed in cellphone battery Bluetooth device embedded in battery Voicemail password left on default setting
Waste management Interception	Inappropriate disposal of mobile telephones
Tracking of mobile telephones	Live tracking through the use of facilities provided by network operators Live tracking through the use of an application installed on the handset Live tracking through the use of an online application Tracking by handset forensic analysis Tracking by mobile device power analysis
Tracking	Bumper beacon systems

Table 3.2: Remote access (stand-off) techniques identified by expert elicitation.

3.4 Analysis

3.4.1 The Components of an Intrusive Surveillance System

From the analysis of the close and remote access techniques identified, key components of surveillance techniques were identified. The components grouped into the following building blocks of an end-to-end eavesdropping system (See Figure 3.1):

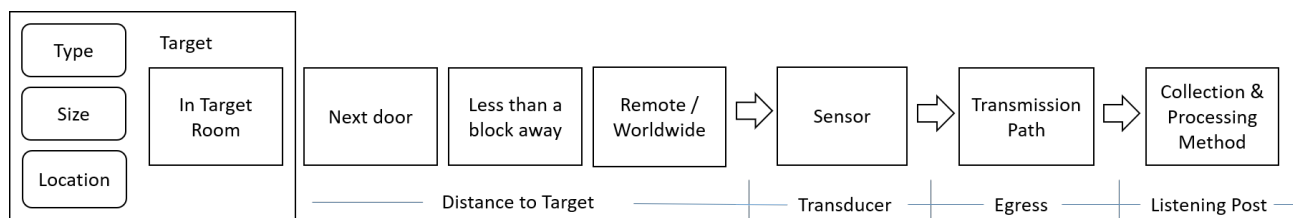


Figure 3.1: The component building blocks of an eavesdropping system.

The building block component details are as follows:

- The target type, size or location;
- How close the eavesdropper needed to be to mount the eavesdropping attack: within the target room, in an adjacent property, less than a block away or remote-worldwide;
- What was actually eavesdropped on (collected) and the type of sensor that was required for the technical collection;
- How the information from the sensor was transmitted (egressed) away from the target area;
- How the transmitted sensor information was collected, stored and processed.

3.4.2 Types of Sensor Output

Product Collected	Instances	% of Total	Description
Audio	88	44%	Room or environment audio - Speech or machine TEMPEST emanations
Data	59	29%	Computer or communications data
Video	39	19%	Static or motion pictures
Metadata	13	6%	Additional info such as 'Call set-up' information
Physical Media	3	1%	Paper files or photographs

Table 3.3: An analysis of the types of product collected from the eavesdropping techniques identified.

Of the one hundred and fifty-eight eavesdropping techniques collected and identified, audio was the most cited output type. There may be bias within these statistics in terms of the period under consideration and the particular expertise of the group that provided the list of eavesdropping techniques. It is interesting to note that the number of technique instances relates to the age of the technique: Audio being the oldest technique, then data followed by video techniques. Since cameras have been included in laptops and other consumer technology, video as a technique has become far more available for eavesdropping use. Physical collection (which is not electronic) is included as it relates to the very earliest methods conducted using photography to copy documents.

These statistics also reveal the 'follow the asset' approach of attackers. As soon as information was passed by electronic means, such as electronic tele-type equipment, attackers were gaining access to this equipment in order to read the traffic transmitted (and before encryption was applied). This trend continues with Information Technology today. If a computer is not networked and carries out some important function, a Close Access eavesdropping technique will be applied to facilitate the reading of information processed or stored on the computer. As soon as Information Technology becomes connected to networks, remote attack techniques become possible but this is not the focus of this research.

3.4.3 Eavesdropping Techniques by Type of User

Eavesdropper Categorisation	User Description	Instances	% of Total	Examples of Technology used
Government User	Hostile Intel. Service Operating Overseas	56	15.7%	IMSI catching, Wi-Fi interception
	Government with home advantage	99	27.8%	Legal Intercept, and TEMPEST
Commercial & Law Enforcement User	Investigative Journalist	33	8.9%	Internal keystroke logger
	Commercial or Criminal Espionage	48	13%	Cellphone Trojan software
	In country Law Enforcement	45	12.2%	Digitally encrypted Radio Microphone
Domestic User	Consumer	49	13.2%	GSM Bug, External key-logger
	Hobbyist	26	7%	Exchange & Mart kit, eBay kit

Table 3.4: Eavesdropping techniques identified matched to the category of users.

These categories of user largely relate to the budget available to the attacker, although it does not mean that the techniques identified are exclusively used by one particular user category, but rather, the user category identifies the most complex equipment available to that user group. Also, not all governments are alike; less well developed countries governments will be unable to deploy the most sophisticated techniques. An example in 2017 in Ghana illustrates this point, with commercial eavesdropping equipment being used against a Minister (Ghana Web 2017).

3.4.4 Access Requirement to Mount Eavesdropping Attacks

An eavesdropper with considerable intent will thoroughly investigate all access opportunities to mount an eavesdropping operation, through the production of a systematic survey of all possible

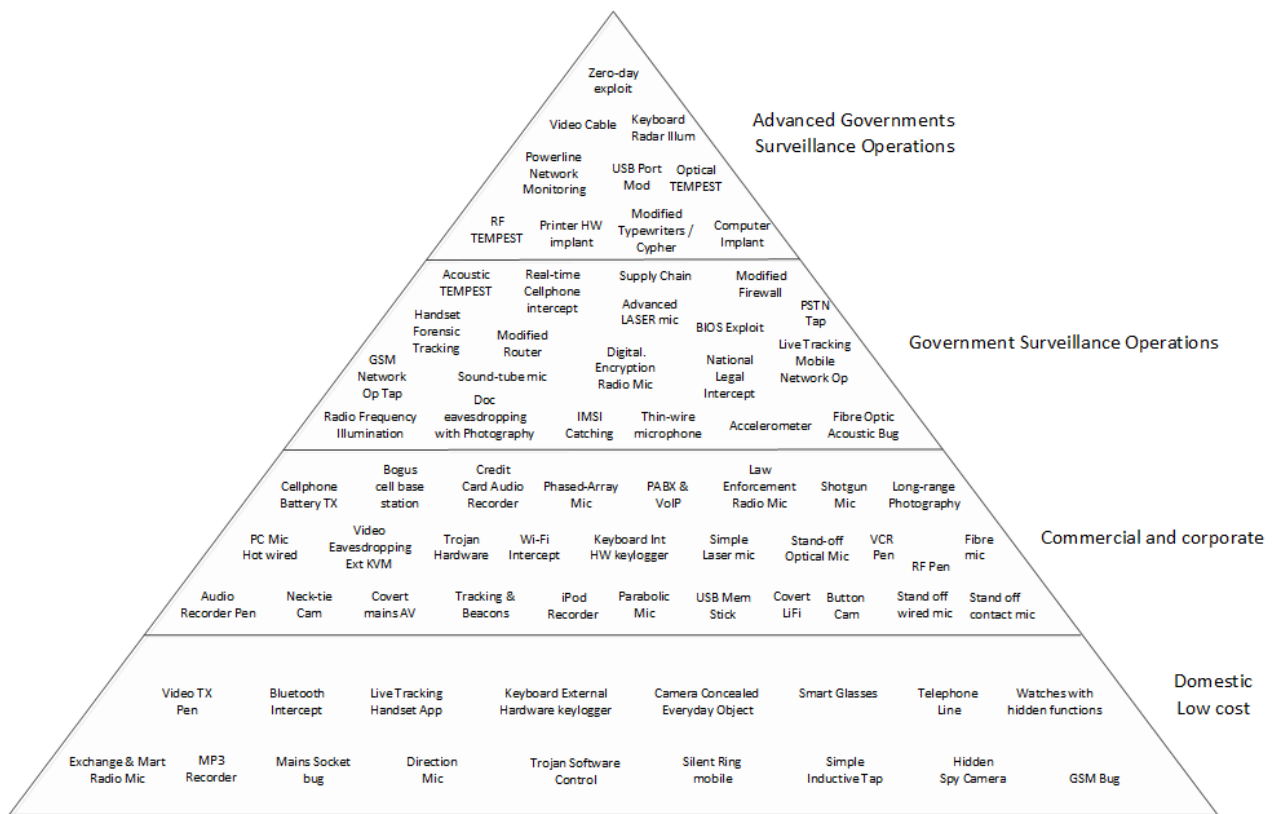


Figure 3.2: The hierarchy of eavesdropping equipment organised by type of user.

exploits available. Both technical and non-technical options will be considered, with nothing disregarded until proven to be unfeasible or ineffective, or the risk of discovery considered too great. The eavesdropping attack may well involve a multi-dimensional approach, with several stages required to align before the final eavesdropping attack is successful.

A Systems Engineering Approach to Access

A competent eavesdropper will likely adopt a complete ‘Systems Engineering’ approach, examining every input and output, the strength and weaknesses of security features present, the target’s ease of exploit, risk of detection, or cost of implementing the eavesdropping attack against the available timescale and consequential timeliness of the eavesdropped information.

A successful eavesdropping exploit implies having one or more egress channels at one’s disposal for extracting information away from the target’s premises. Having several different means or ‘attack surfaces’ is preferable, since a single method or channel might be discovered by the target and then disabled. Fortunately (for the would-be attacker), a large number of methods



Figure 3.3: Systems engineering approach to target analysis. Everything entering and leaving the premises will be considered in considerable detail in order to establish whether an opportunity exists that may facilitate eavesdropping.

can be exploited, either singly or in combination, all of which will be considered and evaluated as part of the systems engineering assessment.

Examples of items that leave a premises	Examples of items that enter a premises
TEMPEST Acoustic / optical / electromagnetic	Visitors Official / family
Ultrasonic	Employees
Optical emanations through the windows	Contractors
Physical vibrations	Maintenance staff
Radio communications	Emergency Services
Telephony	Catering staff and supplies
IT data circuits	Cleaners
Paper shreddings	Deliveries by post or courier
All waste / everything discarded	Anything purchased locally
The whole electromagnetic spectrum	Equipment suppliers e.g. photocopiers
Radio	Furniture suppliers
Microwave	Telecoms landlines
Infrared	Water / Gas / Electricity
Visible light	Cable services TV / Internet
Ultraviolet	Cellphone services
X-rays	Air conditioning / Ventilation / Lighting
Thermal signature	Stationery suppliers

Table 3.5: Examples of an analysis of all items entering and leaving a premises. The Bucharest shoe bug in 1969 is a good example of this type of analysis (see Figure 2.22 for further details of this event).

Access Preparation Required to Mount an Eavesdropping Attack

The techniques identified were analysed for the level of access preparation required. This ranged from quick plant techniques requiring very little preparation that could be instigated at a moment's notice, to the other extreme years of meticulous planning were required such as that required to mount the gap jumpers at the end of concrete columns within the comprehensive eavesdropping system mounted in the early 1980s against the American Embassy in Moscow (see chapter 2.3.18).

Access Preparation	Instances	% of Total	Examples
Low	43	27%	Consumer electronics devices, GSM bugs, covert photography
Medium	69	44%	Illumination or where something is hidden in a covert disguise
High	46	29%	Legal interception, deep-plant installations during construction

Table 3.6: The eavesdropping techniques classified by Low, Medium or High prior access preparation required to mount the attack.

Distance to the Target Required for an Eavesdropping Attack

An analysis of the eavesdropping techniques identified revealed two distinct points in time for an eavesdropping operation:

- The access requirements required to mount the attack;
- The access requirements required to operate the attack, once set-up.

Distance to Target to Mount Attack	Instances	% of Total	Examples
Within the target premises	80	50.3%	Consumer electronics devices
Adjacent to the target room	66	41.5%	TEMPEST, probe microphones
Within the target's city	7	4.4%	City telecoms interception
Anywhere Worldwide	6	3.6%	Zero-day IP exploits, IP networks, satellite interception

Table 3.7: An analysis of all eavesdropping techniques identified, classified by the distance to target required to mount an attack.

Four distinct distances from the target were noted within which a technical attack could be mounted:

1 - Eavesdropping Techniques requiring Access to the Target Room

Within Target Room	
(Person / Insider)	(IT Equipment)
Human individual	Keyboard eavesdropping - Hardware-based keyloggers (external)
Insider threat	Keyboard eavesdropping - Hardware-based keyloggers (internal)
Visitors wired with sound and vision	Eavesdropping through poor printer configuration
Perils of facilities management contracts	Eavesdropping through modified USB ports
Event staff	Disguised equipment cases
Tampering by IT and telecomms technicians	Plugging memory sticks into unknown equipment
	USB memory stick
(Audio)	Personal computer hot-wired
Self-drilling microphone	Optical communications via the screen
Audio eavesdropping - Hardwired internal microphones	

Professional grade credit card recorder	(Office equipment)
MP3 recorders	Modified photocopiers
iPods	modified shredders
Analogue recorders using tape or wire	Modified calculators
Audio-video surveillance using a covert mains carrier system	Modified intercom systems
Mains socket bug	Modified typewriters
Wired microphones	Modified teleprinters
Concealed in walls - Microphone attached to a sound tube	
Microphones Attached to Very Thin Wires	(Consumer)
Microphones created from loudspeakers	Watches with cameras and USB memory
Infrared communications systems	Pens with RF speech transmitters
Infrared headphones	Pens with audio recorders
Infrared translation systems	Pens with digital video recorders
Fibre microphones	Pens with video transmitters
	Pens with handwriting capture
(Telephony Related)	Cameras concealed inside everyday objects
Compromised analogue telephones	Smart glasses
Microphone created by switch-hook bypass in analogue telephone	Neck-ties with concealed cameras
Telephone line egress of mic audio with low frequency carrier	Buttons with concealed camera lens
Microphone created by switch-hook bypass in an analogue telephone	Tablets
Microphones concealed in telephone equipment	
	Beneath visible surface
(Cellphone Related)	Compromised entry and egress control
SIM Card Copiers	Paper Assets
Transmitter concealed in cellphone battery	Very low light systems
Bluetooth device embedded in battery	Systems that operate in the dark
Tracking by handset forensic analysis	
Tracking by Mobile Device Power Analysis	
Audio recording application software	
Near field communications (NFC)	

Table 3.8: An analysis of all eavesdropping techniques identified, classified by techniques that require access to the target room.

2 - Eavesdropping Techniques requiring Adjacent Property Access

Access 2 (Adjacent Property)	
(Person / Insider)	(Cellphone Related)
System failures and human weakness	Real-time interception of calls
Poor physical security	IMSI catching
Inadequate technical security	Using bogus base stations for spoofing ('Man in the middle' attacks)
Inappropriate disposal of mobile telephones	
(Audio)	(IT Equipment)
Airgap in target room	TEMPEST emanations
Acoustically poor conference rooms	TEMPEST - Radio frequency emanations
Contact microphones	TEMPEST - Optical emanations
Optical microphones	TEMPEST - Optical reflections from other objects
Probe microphones	TEMPEST - Acoustic emanations
Directional microphones	TEMPEST NONSTOP and HIJACK
Shotgun or rifle microphone	Video eavesdropping - Non-TEMPEST equipment
Phased array microphones	Video eavesdropping - external KVM switches
Parabolic microphone	Video eavesdropping - replaced video cables
	Keyboard eavesdropping - radar illuminated
	Wi-Fi or Bluetooth wireless systems
(Radio egress related)	Wi-Fi interception systems
Radio microphones	Bluetooth interception
Digitally encrypted radio microphone	
Commercially available radio microphone	(Optical related)
Exchange and Mart radio microphone kits	Overt Li-Fi
Broadcast radio (wire-free) microphone	Covert Li-Fi
Analogue cordless telephones	Projectors and projection systems
Digital cordless telephones	Laser microphones
In-house hand-held radios (Security Officers' radios)	First generation laser microphone
Radio frequency illumination	Second generation laser microphone
Radio frequency illumination for audio eavesdropping	Third generation laser microphone
Radio frequency illumination for data eavesdropping	Fourth generation laser microphone
Telephone line connected to a radio transmitter	
Magnetic loop transmission systems	(Access related)
Mains egress data or audio systems	Silent drilling
	Near Silent Drilling
(Telecomms infrastructure related)	Gap jumpers
Wire taps, cabling infrastructure (tampering and patching)	Deep plant devices built-in during construction
and exploiting cross-talk	Concealed cabling within other building components
Simple inductive taps	Accelerometers attached to structural elements
Telephone, broadband and FTTC lines interception	
Telephone lines	
Broadband and fibre to the cabinet	
Hardware eavesdropping on networks - via drop boxes	
Hardware eavesdropping on networks - via computer power lines	

Table 3.9: An analysis of all eavesdropping techniques identified, classified by techniques that require adjacent property access.

3 - Eavesdropping Techniques requiring Access Less than a Block Away

Less than a block away	
(Person / Insider)	(Optical related)
Agent communications	Photography - Long-range with telephoto lens
Disposal chain	Long-range photography enabled lip reading
Redundant computer equipment	Long-range photography enabled text analysis of keyboard entry
	Long-range photography enabled touchscreen snooping
(Access related)	Long-range photography enabled by drones
Long-range drilling	Document eavesdropping by photography
(Telecomms infrastructure related)	(Radio egress related)
Microwave links for voice or data	Tracking and beacon systems
Laser free-space optical links	
Fibre optic eavesdropping	

Table 3.10: An analysis of all eavesdropping techniques identified, classified by techniques that require access less than a block away.

4 - Eavesdropping Techniques Mounted Remotely from any Location

Remote attack techniques mounted from anywhere Worldwide	
(Access related)	(IT by remote access related)
Disguised receiving antennas (incl. satellite)	Video eavesdropping - built-in applications
	Audio eavesdropping - built in applications
(Supply chain related)	Eavesdropping through server bios exploitation
Intentionally compromised electronics (supply chain attacks)	Eavesdropping through printer hardware-based additions
Items compromised in transit	Eavesdropping through modified routers
Compromised IT hardware	Eavesdropping through modified firewalls
	Eavesdropping through modified computers
(Telecomms infrastructure related)	Eavesdropping through local software execution
Public switched telephone network taps	Taking control by means of trojan software
Mobile telephone network operators taps	Taking control by means of trojan hardware
PABX and VoIP telephones	Live tracking through the Use of an application installed on the handset
Telephone line egress of microphone audio through remote activation	Live tracking through the use of an online application
GSM Bug	
Exploiting building management system installations	(Optical related)
Legal eavesdropping by national authorities	Long-range video systems
Silent ring eavesdropping	Webcams
Voicemail password left on default setting	Hidden spy cams
Live tracking through the use of facilities provided by network operators	Security cameras in the high street or protecting homes

Table 3.11: An analysis of all eavesdropping techniques identified, classified by techniques that may be mounted remotely, worldwide.

Figure 3.4 illustrates a rather obvious point: the closer an attacker becomes to a particular target, the greater the likelihood that the target is very well defined and carefully selected to provide specific information. This does not preclude a specific target from being selected from the bulk monitoring of internet or cellphone traffic remotely. Simply that if an attacker is

carrying out a Close Access attack against a target, that this target is clearly the focus of the attacker. Also, the closer the attacker is to a particular target, the greater the ability of the attacker to confirm that the victim of the attack is the correct target. This simple fact is less likely to be established if the mounting of an eavesdropping operation is carried out remotely.

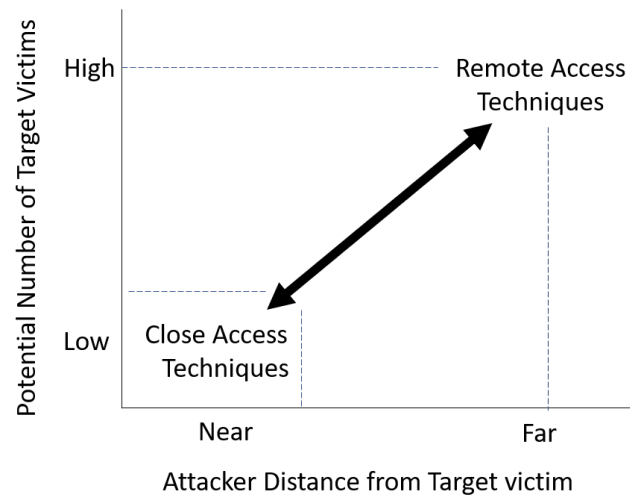


Figure 3.4: The number of potential eavesdropping victims when mounting Close Access or Remote Access eavesdropping operations.

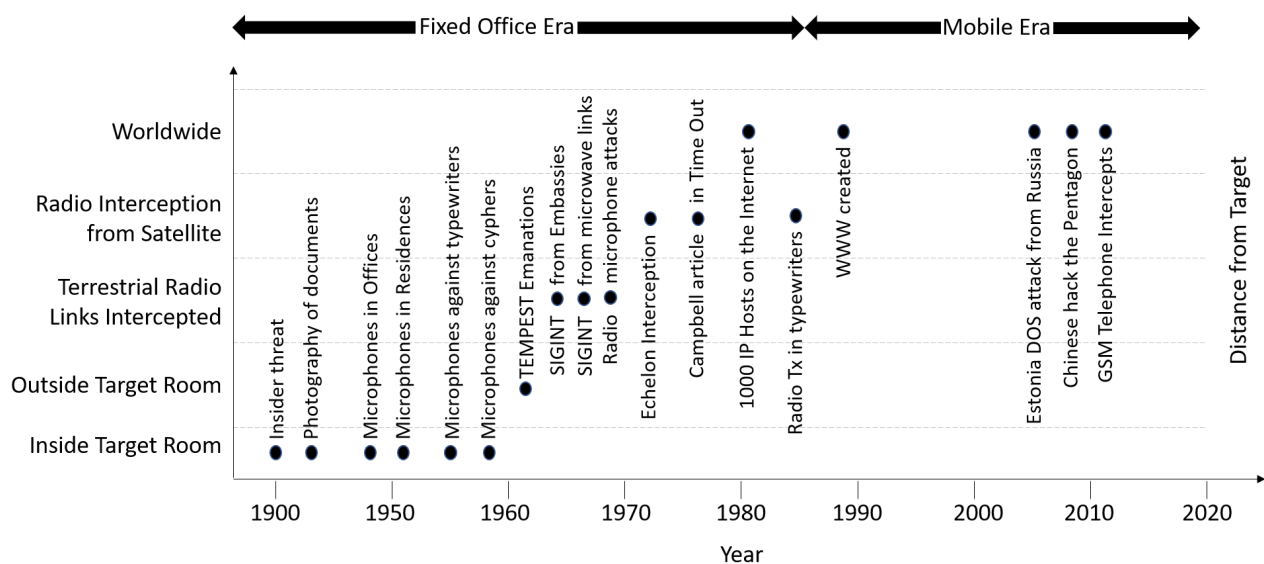


Figure 3.5: The trend towards remote access: technology has enabled remote access eavesdropping possibilities.

3.4.5 Access Requirement for Eavesdropping Operation

An analysis of the identified technical attack techniques revealed that the majority of attacks required the listening post to be close to the victim being attacked.

The advent of the internet will see these ratios change with ever increasing connectivity producing ever increasing remote access attack techniques.

Operation distance to LP	Instances	% of Total	Examples
In the target premises	19	11.8%	Most consumer electronics gadgets
Adjacent to the target room	103	64%	Illumination, probes, TEMPEST, Wi-fi interception
In the target's city	7	4.3%	City telecomms interception, local disposal
Anywhere Worldwide	32	19.9%	Software attacks via IP or telephony networks

Table 3.12: An analysis of all eavesdropping techniques identified, classified by the required distance to the listening post.

3.4.6 The Transmission Path

In order to operate an attack (with the exception of information collected within the target room for physical retrieval) an egress path will be required to transmit information away from the target, covertly, to a safe place where it can be monitored, stored or transmitted onwards away from an intermediate point to secure monitoring facilities.

The transmission path away from the target plays a vital role for all technical eavesdropping systems. Without an egress route, the attacker would require repeat and potentially frequent access to the target. The types of egress route vary considerably; attackers will use any means of egress route available in order to transfer information away from a target location.

To achieve a successful eavesdropping operation, attention must be given to minimise link detection and component detection. The transmission path link must remain undetected by the victim in order to operate a successful eavesdropping operation.

Within the eavesdropping attack techniques identified, it was noted that the egress opportunities have changed over time. As the range of eavesdropping methods has increased in line

with technical innovation and evolution, so too has the range of egress opportunities. From the oldest technique, progressing to the latest available:

- Direct acoustic listening by a person - the oldest of all techniques;
- Hidden wires direct from microphones capturing human voice and machine emanations;
- The exploitation of telephone lines, particularly from domestic settings as telephones become installed in homes. Eavesdropping acoustic output could be technically masked to make it less obvious to the telephone line owner that the line was being used for eavesdropping purposes;
- A low-frequency radio carrier superimposed onto a telephone line so that the eavesdropping audio remains inaudible to the telephone line user, but the room audio has the ability to be egressed a considerable distance from the target room, in much the same way as low-frequency carriers superimpose inaudible broadband services to telephone line subscribers;
- The exploitation of mains electricity wiring which leaves a target room for eventual connection to a power generator. The mains wiring listening post is located as close to the target as possible;
- By magnetic means. Hearing aid technologies provide short-range magnetic egress opportunities;
- The invention of the transistor enables miniature battery operated radio transmitters and the freedom to mount the microphone close to targets. Often these are remotely controlled to preserve battery life or to reduce the transmitter detection by technical means;
- Optical or visual sight methods either with a LASER to illuminate a compliant reflector within the target room or by lip reading via the direct optical visual path;
- Information Technology installations in offices provide structured cabling and network wiring egress opportunities;
- Permanent internet connectivity through the provision of broadband facilities over copper and fibre telephone lines;
- Mobile telephone developments: Initially analogue and unencrypted, and later through the GSM worldwide networks;

- Wireless options such as Wi-Fi and Bluetooth and the expansion of consumer electronics.

Egress paths can be either passive or active. Examples include inductive coupling taps on data cables, telephone and broadband lines, all of which exploit the ability to tap information outside the boundary of the target premises. Similarly TEMPEST emanations may be of sufficient strength that they can be detected and analysed at some distance from the premises using sensitive equipment.

Examples of active egress techniques include the Great Seal incident (Glinsky 2000b), Theremin's Buran LASER attacks (Glinsky 2000a) or the installation of hidden transmitters connected to microphones or typewriter components such as those found in American Embassy typewriters located in Moscow (See section 2.3.6).

The following egress methods identified in the techniques were listed by popularity:

Egress method	Instances	% of Total	Description
Radio to the LP	44	24%	Radio to the listening post (LP) provides flexibility for the attacker. Transmission frequency selection will dictate both the range and egress potential through building fabric. Higher frequencies also facilitate antennas with directionality to ensure transmission energy is directed towards the LP. It does however risk detection by capable defensive countermeasures.
Insider access	30	16%	Once a person has access to the target room the number of opportunities to carry out a technical attack multiply considerably.
Data to the LP	28	15%	With the rise in Information technology installations in both the home and office, wired Information Technology distribution cabling provides surplus conductors which are available for an attacker to exploit. Furthermore, egress via IP on data cabling provides the potential for worldwide egress paths to be established.
Cable to the LP	26	14%	This category includes wires direct from microphones and telephone wires as the principal transmission path away from a target.
Optical to the LP	25	13%	This technique is dependent on line-of-sight to the target from the attackers' LP. Considerable distances too are possible. This egress may be by active or passive means; passive through the transmission away from the attack area by visible or invisible light or through active illumination of a compliant target in order to gain some return.
Utility access	10	5%	Legitimate access to a target's telephone or IT network and equipment is an attractive option. Continuous access provides the ability to remove information recorded for later analysis (i.e. store and forward).
Direct audio	8	4%	The acoustic range is variable dependent upon many factors such as the noise within the surrounding environment and the noise in the target room.
Mains to the LP	6	3%	This method requires that the attacker can gain access to the correct mains phase, reducing the reliability of the mains as a suitable egress route. The mains is also likely to be a very noisy transmission path.
USB port	4	2%	The USB port is useful to the attacker since it includes a transmission path into and out of the device being attacked. It also provides power too enabling whatever is plugged into the interface to be powered and not reliant on battery life.
Electro-magnetic egress	3	2%	Physics dictates that this technique will only egress over a short distance. This being one reason magnetic induction is used for hearing aid technology, as the range can be controlled and confined to a single room.
Disposal interception	3	2%	An unreliable and unpredictable egress route. If access can be obtained to office waste then information may be gleaned, particularly if the victim is not security conscious. Electronic disposal provides the attacker the opportunity to conduct forensic analysis on equipment but the information gathered may be many years old.

Table 3.13: An analysis of all eavesdropping techniques identified, classified by the popularity of the egress route.

The spectrum of egress opportunities is illustrated in Figure 3.6 below. The construction techniques of buildings varies considerably. The transmission loss (i.e. the egress attenuation) through the fabric of the building will affect the likely choice of spectrum used to egress away an eavesdropper. Modern glass and steel construction offer considerably more potential for radio and optical egress than a traditional brick or stone built building. A casual observation

in any city of any Russian embassy will illustrate windows bricked up, presumably to reduce the potential for optical egress vulnerabilities.

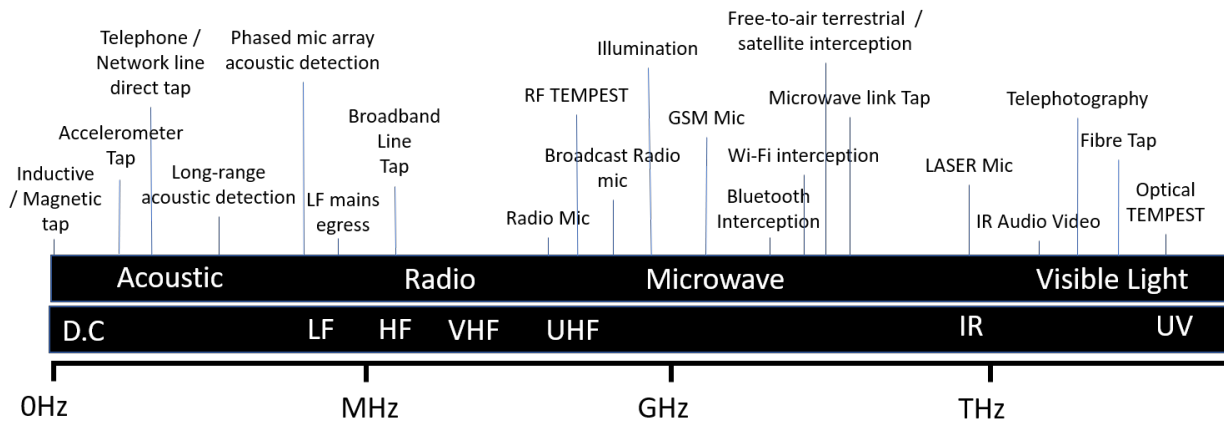


Figure 3.6: Overview of the electromagnetic spectrum used for egressing eavesdropping operations.

Figure 3.6 illustrates the wide variety of techniques and the broad frequency range exploited across the electromagnetic frequency spectrum.

3.4.7 Technical Eavesdropping Detection Avoidance

Of the one hundred and fifty-eight techniques identified the following detection avoidance countermeasures were noted:

Countermeasures Deployed	Instances	% of Total	Description
Yes	98	62%	Where the attacker had deliberately included anti-detection
No	60	38%	Where the attacker had not included countermeasures

Table 3.14: An analysis of all eavesdropping techniques identified, classified by those with detection countermeasures.

Approximately two-thirds of the attack techniques included some form of detection avoidance countermeasure. Table 3.15 groups the countermeasures by type.

Nature of countermeasure	Overview of countermeasure	Examples
Trojan horse concealed within a component of the equipment	Covert deep implant	Eavesdropping through modified USB ports
	Covert case	Microphones concealed in telephone equipment
	The case hides the implant	Eavesdropping through printer hardware-based additions
	Simple covert disguise	Modified calculators
	Specialist technical modification	Modified photocopiers Modified shredders Modified typewriters Modified teleprinters
Trojan horse concealed within software application	Deep plant covert software	Video eavesdropping - built-in applications
		Audio eavesdropping - built-in applications
		Eavesdropping through server bios exploitation
		Eavesdropping through poor printer configuration
		Eavesdropping through modified router software
		Eavesdropping through modified firewall software
		Audio recording application software Taking control by means of trojan software
Trojan horse concealed in everyday object	Simple covert disguise	Buttons with concealed camera lens
		Professional grade credit card recorder
		iPods with built in recording devices
		USB memory stick with audio recorders
		Cameras concealed inside everyday objects
		Hidden spy cams
		Pens with RF speech transmitters
		Pens with audio recorders
		Pens with digital video recorders
		Pens with video transmitters
		Pens with handwriting capture
		Transmitter concealed in cellphone battery
		Bluetooth device embedded in battery
		Neck-ties with concealed cameras Watches with cameras and USB memory
A way to securely egress from the target to a safe place for monitoring	Building fabric masking during install	Concealed cabling within other building components
	Privacy on egress transmission link	Gap jumper egress away from secure environment
		Digitally encrypted radio microphone
		Telephone line connected to a radio transmitter
		Telephone line egress of microphone audio through remote activation
	Specialist technical modification	Telephone line egress of microphone audio with low frequency carrier Modified intercom systems Smartphone spyware
Time shift of protection - Attack - mounted when less protection, for later activation	Building fabric masking of install	Self-drilling microphone
		Deep plant microphones built-in during construction
		Deep plant accelerometers built-in during construction
Electronic countermeasure - Non-linear junction detector detection avoidance	No metallic components to detect	Optical Fibre Microphones

Electronic countermeasure - Sound tube increases distance from target room	Building construction masking of install	Wired microphones
Speed of installation in wall paper for rapid and invisible egress	Stasi domestic technique to hide egress route	Microphones egressed via very thin wires
Staff under the control of the host nation	Covert activity of member of staff	Event Staff - uncontrolled and non-vetted
The exploit of a weakness or vulnerability for which the user has no knowledge.	User unaware of TEMPEST emanations	Video Eavesdropping - Non-TEMPEST Equipment
	Deep plant covert software	Eavesdropping through local software execution - zero day
	Specialist technical modification	Modified telephone to become microphonic
	The cable hides the implant	Video eavesdropping - replaced video cables
	Pico cell CM to enable specific area coverage	IMSI catching
	Invisible spot of light	Second generation laser microphone Third generation laser microphone Fourth generation laser microphone
Assumption that the victim does not notice additional implant at rear of desktop computer.	The case hides the implant	Keyboard eavesdropping - hardware-based keyloggers (internal)
Victim not aware for the need to protect against radio illumination	The radar is covert unless radio monitored	Keyboard eavesdropping - radar illuminated
	Localised radio transmission	Radio frequency illumination for audio eavesdropping Radio frequency illumination for data eavesdropping

Table 3.15: An analysis of all eavesdropping techniques identified, classified by the types of countermeasures.

Table 3.15 illustrates the principal high-level groups of countermeasures deployed.

The first countermeasures, which stand out, are those whereby a component within an object is replaced by another component covertly, where the component forms an eavesdropping function. The techniques countermeasure relies on being hidden from visual inspection within some legitimate object that has a reason for being in the target room.

The second stand out countermeasure is almost identical to the first but software-based. A component of software within an object is replaced covertly in order to form an eavesdropping function. This software may be an application or firmware. The countermeasure relies on being hidden within a vast array of other software that makes it extremely difficult to identify its presence. Examples of this nature are illustrated with the concern over unknown software origin contained within communications equipment such as those posed by the Chinese telecoms giant Huawei and the security concerns of the American and other nation's governments.

A third stand out group is where an attacker has deliberately concealed components during the

construction of a building. Repeat access is not available to the installation and is consequently meticulously planned and literally buried under concrete structure to avoid detection. This group of countermeasures is aware of countermeasure detection techniques and adds additional anti-electronic detection prevention knowledge to reduce the potential of discovery.

A fourth group of countermeasures relates to the egress link avoiding detection either through encryption of the egressed information or the delayed transmission of the information at a time considered the least likely to be detected by the victim. This group includes illumination of either visible or electromagnetic energy. This group is also highly technical in nature and relies on the exploit of superior knowledge to that of the attacker.

Technical Detectability

Detectability minimisation is important if the attacker wishes to operate a covert eavesdropping operation and they believe the target may have the ability to identify that a technical attack is in operation. The detection ability will relate to the knowledge and skill-set, together with a belief that they may actually be a target. Of the one hundred and fifty-eight technical techniques:

Physical evidence detectable	Instances	% of Total	Description
Yes	94	59.5%	A physical aspect of the technical attack is present to the attacker
No	64	40.5%	No physical aspect is observable by the victim

Table 3.16: An analysis of all eavesdropping techniques identified, classified by detectability.

The distance with which a technique may be detected relates to the distance with which the attack is mounted. Of the attack methods identified, Table 3.17 indicates three groups of distances:

Detection distance	Instances	% of Total	Description
0-5m	60	38%	Likely to be within the target room or fabric of the target room
6m-50m	44	28%	Likely to be adjacent and external to the target room and surrounding environment
50m+	54	34%	Likely to be remote from the victim and extremely hard to detect

Table 3.17: An analysis of all eavesdropping techniques identified, classified by the detection range.

Plausible Deniability

Plausible deniability may be a consideration for a particular situation if the method of attack is risky in nature or has the potential for discovery. The many wired microphone attacks mounted against Western embassies in Moscow by the Russians after the Second World War had no plausible deniability but these attacks will have been considered in a risk balanced case; the long-term intelligence gathering against the risk of detection and the consequences of the detection.

Where information is required for more tactical reasons and time is not available for deep under cover installations, a quick plant technique may be required. Within plausible deniability there are two subgroups: (i) A technique that has been deployed that uses readily available consumer eavesdropping components that could have been purchased by absolutely anyone. Examples include the eavesdropping incident in the Ecuador embassy in London during the occupation by Julian Assange (BBC 2013) and (ii) A technical attack more sophisticated in nature that is clearly not available to the consumer but is the output of a highly capable technical manufacturer, such as the device found in the Salon Français of the UN's European headquarters in Geneva (Whitaker 2004) where according to analysis of the device (Atkinson 2004), provided few clues to its origin. Of the eavesdropping techniques identified:

Plausibly deniable	Instances	% of Total	Description
Yes	68	43%	Where the technique has the potential to be plausibly denied
No	90	57%	Where it is not possible to deny the attack origination

Table 3.18: The eavesdropping techniques deniability.

3.4.8 Technical Method Complexity

Each technique was analysed and placed within a technical hierarchy. Four distinct groups of complexity were identified:

- Group 1 (The High Threat Club): the highest technical ability required and will be limited to a small number of well funded and highly technical governments in the world;
- Group 2 (Government & Mass Surveillance): all other governments capable of monitoring their citizens and with good resources available;
- Group 3 (Commercial): commercial ability whereby technical methods may be purchased openly by anyone with sufficient funds to do so;
- Group 4 (Domestic and Low Cost): domestic techniques that are highly effective for very little cost, offering the consumer considerable capability but requiring minimal technical expertise to deploy.

Group 1 - The High Threat Club	
Concealed cabling within other building components	Concealed in walls - microphone attached to sound tube
Eavesdropping through local software execution - Zero Day	Eavesdropping through modified USB ports
Gap-jumpers egressing secure environments	Modified printers
modified teleprinters	Modified typewriters
Radio frequency illumination for data eavesdropping	Self-drilling microphone
Silent drilling	Speech from smartphone gyroscope
TEMPEST - optical emanations	TEMPEST - Radio frequency emanations
TEMPEST NONSTOP and HIJACK	Video eavesdropping - Replaced video cables

Table 3.19: An analysis of all eavesdropping techniques identified, classified by the most demanding techniques reserved for well-funded governments.

Group 2 - Government & Mass Surveillance	
Acoustic eavesdropping through wireless vibrometry	Acoustically poor conference rooms
Analogue recorders using tape or wire	Audio-video surveillance using a covert mains carrier system
Covert Li-Fi	Deep plant accelerometers built-in during construction
Deep plant microphones built-in during construction	Eavesdropping through modified firewall software
Eavesdropping through modified router software	Eavesdropping through printer hardware-based additions
Eavesdropping through server bios exploitation	Event staff - uncontrolled and non-vetted
Fibre optic eavesdropping	Fibre or “fibre to the cabinet” interception
Fourth generation laser microphone	Hardware eavesdropping on networks via computer power lines
IMSI catching	Infrared translation system interception
Laser free-space optical links	Legal eavesdropping by national authorities
Live tracking through the use of facilities provided by network operators	Long-range drilling
Long-range photography enabled by drones	Long-range photography enabled lip reading
Long-range photography enabled text analysis of keyboard entry	Long-range photography enabled touchscreen snooping
Microphone created by switch-hook bypass in analogue telephone	Microphones concealed in telephone equipment
Microphones created from loudspeakers	Microphones egressed via very thin wires
Microwave voice and data interception	Mobile telephone network operator taps
Modified intercom systems	Modified telephone to become microphonic
PABX exchange exploits	Public switched telephone network (PSTN)
Real-time interception of calls	Security cameras in the high street or protecting homes
Taking control by means of trojan hardware	TEMPEST - Acoustic emanations
TEMPEST - Optical reflections from other objects	The probe microphone
Third generation laser microphone	Tracking by mobile device power analysis
Wired microphones	

Table 3.20: An analysis of all eavesdropping techniques identified, classified by technical demands available in government.

Group 3 - Commercial	
Access to hard drive within photocopier	Analogue cordless telephones
Audio eavesdropping - built in IT applications	Audio eavesdropping - hardwired internal microphones
Audio recording application software	Bluetooth device embedded in battery
Bluetooth interception	Broadband data interception
Broadcast radio (wire-free) microphone	Bumper beacon systems
Buttons with concealed camera lens	Cabling infrastructure tampering and patching
Commercially available radio microphone	Conference room radio microphone systems
Contact microphones	Digital cordless telephones
Digitally encrypted radio microphone	Disguised equipment cases
Document eavesdropping by photography	Eavesdropping through poor printer configuration
HomePlug data sharing	Inappropriate disposal of mobile telephones
Infrared headphones	In-house hand-held radios (Security Officers' radios)
iPods with built-in recording devices	Keyboard eavesdropping - hardware-based keyloggers (internal)
Keyboard eavesdropping - Radar illuminated	Long-range video systems
Magnetic loop transmission systems	Modified calculators
Modified shredders	Near Field Communications (NFC)
Near silent drilling	Neck-ties with concealed cameras
Optical communications via the screen	Optical fibre microphones
Overt Li-Fi	Paper assets photographed
Parabolic microphone	Pens with digital video recorders
Pens with RF speech transmitters	Personal computer hot-wired
Phased array microphones	Photography - Long-range with telephoto lens
Plugging memory sticks into unknown equipment	Podium microphones
Professional grade credit card recorder	Projectors and projection systems
Radio frequency illumination for audio eavesdropping	Redundant computer equipment
Second generation laser microphone	Shotgun or rifle microphone
SIM card copiers	Smartphones with cameras, microphones, accelerometers and apps
Systems that operate in the dark	Telephone fax interception

Telephone line connected to a radio transmitter	Telephone line-egress of microphone audio through remote activation
Telephone line-egress of microphone audio with low-frequency carrier	Telephone speech interception
Tracking by handset forensic analysis	Transmitter concealed in cellphone battery
USB connecting leads to users' laptops	Using bogus base stations for spoofing ('Man in the middle' attacks)
Video eavesdropping - built-in applications	Video eavesdropping - external KVM switches
Video eavesdropping - Non-TEMPEST equipment	VoIP telephones
Wi-Fi interception systems	

Table 3.21: An analysis of all eavesdropping techniques identified, classified by technical demands available with commercial complexity.

Group 4 - Domestic and low cost	
Baby monitor	Bluetooth eavesdropping
Cameras concealed inside everyday objects	Directional microphones
Exchange and Mart radio microphone kits	First generation laser microphone
GSM bug	Hidden spy cams
Keyboard eavesdropping - hardware-based keyloggers (external)	Live tracking through the use of an application installed on the handset
Live tracking through the use of an online application	Mains socket bug
MP3 recorders	Pens with audio recorders
Pens with handwriting capture	Pens with video transmitters
Silent ring eavesdropping	Simple inductive taps
Smart glasses	Taking control by means of trojan software
USB memory stick with audio recorders	Voicemail password left on default setting
Watches with cameras and USB memory	Webcams

Table 3.22: An analysis of all eavesdropping techniques identified, classified by technical demands available to consumers.

It is interesting to observe the number of techniques that have become available to the domestic user. Particularly ubiquitous methods that have gained wide popularity such as the variants of the GSM audio bug that egress room audio from a target via a GSM telephone network. Another notable inclusion is that of trojan software applications that permit an attacker the ability to monitor all functions used by a victim's smartphone.

Installation Complexity

Within the techniques, there is an enormous range of installation complexity: from a simple consumer audio recorder that may be placed in the target room and collected at a later date, or stitched into a child's clothing, to the extreme example against the American Embassy in Moscow in the early 1980s, which required extensive planning and prior preparation and several years to implement in order to egress multiple microphone cables in a covert manner.

Of the one hundred and fifty-eight techniques identified:

Installation complexity	Instances	% of Total	Description
Simple	65	41.4%	Requiring very little or no technical experience. Quick to install and often consumer mass produced
Moderate	54	34.4%	Requiring specially trained staff in attack techniques, covert modifications to existing systems or optical/photographic systems operating at range
Complex	38	24.2%	Examples include technically demanding installations such as illumination or TEMPEST, or long planning requirements required against new building construction or complex national legal intercept systems.

Table 3.23: An analysis of all eavesdropping techniques identified, classified by installation complexity.

It is of interest to note that forty-one percent of the techniques are simple to install. This will likely continue to change over time. Technology continues to make what was virtually impossible to do yesterday simple to do today. This is researched in more detail in the next chapter.

Procurement Complexity

It is not surprising that procurement complexity is similar in nature to installation complexities, as illustrated in Table 3.24:

Procurement Category	Instances	% of Total	Description
Simple	60	38%	Easily obtained and available widely on internet shopping channels
Moderate	62	39%	More complex and specialist in nature requiring industry knowledge and specialist outlets Some outlets may restrict sales to some nations
Complex	38	23%	Not available commercially and requires sovereign or close allies manufacturing capability

Table 3.24: An analysis of all eavesdropping techniques identified, classified by procurement difficulty.

Hardware or Software-based Techniques

Of the one hundred and fifty-eight techniques identified:

Hardware or software	Instances	% of Total	Description
Hardware	127	78%	From the earliest photographic techniques and the use of hidden lenses in buttons, all manner of microphone developments across the twentieth century.
Software	35	22%	Techniques that grow in frequency after the 1990s and reach maturity in the new millennium. Relating to the introduction of IT into office spaces, and the mobile telephone, with the smartphone enabling software applications for tracking and monitoring to consumers

Table 3.25: An analysis of all eavesdropping techniques identified, classified by hardware or software deployment.

The transition of eavesdropping techniques exploiting software features of consumer electronics is considered in the next chapter.

Relative Cost

An analysis of the techniques identified was carried out for the relative cost of the technology in Table 3.26:

Relative cost	Instances	% of Total	Examples
Very Low	6	3.7%	GSM Bug, amateur kits and webcams
Low	43	26.7%	Keyloggers, calculators, Pens with recorders and transmitters
Medium	72	44.7%	Wired microphones, covert photography, audio recording credit cards
High	33	20.5%	Self drilling microphones, TEMPEST techniques, LASER and illumination techniques
Very High	7	4.4%	Telecoms Infrastructure taps, microwave interceptions, Legal Intercept

Table 3.26: An analysis of all eavesdropping techniques identified, classified by relative financial cost of the equipment.

The distribution of relative costs very much follows a normal ‘bell curve’ distribution.

3.4.9 Target Size

Some techniques are specifically aimed at an individual. The technique could only ever be employed in a particular scenario against the one individual target, while other techniques identified were capable of monitoring whole populations with a further ability to select a particular individual of interest within the mass of data available.

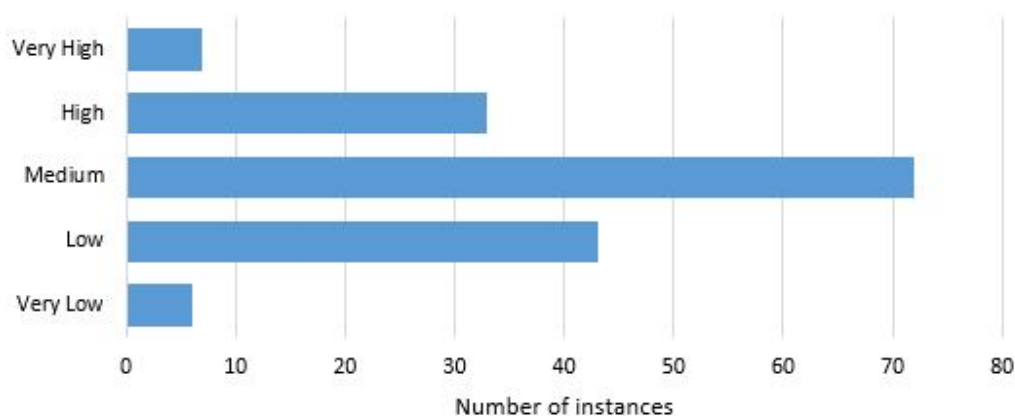


Figure 3.7: An analysis of all eavesdropping techniques identified, classified by distribution of relative financial cost of the equipment.

The Echelon project (see section 2.3.13) and the advent of international satellite communications created the ability to monitor whole country outputs. Satellite technology dedicated to spy operations are beyond the focus of this research but the very fact that the technology to launch satellites with this capability exists must be acknowledged.

Number of citizens affected in Table 3.27 relating to the techniques identified:

Citizens affected	Instances	% of Total	Description
An individual	132	63%	This list includes the vast majority of techniques
An organisation	72	34%	This group comprises shared office resources or building facilities
A population	5	3%	Largely confined to legal intercept on national communications infrastructure

Table 3.27: An analysis of all eavesdropping techniques identified, classified by the number of citizens affected.

The focus of this research is against high-profile targets. Two-thirds of the techniques identified were against individuals with approximately one third against an organisation. Examples of techniques capable of monitoring whole populations are highly likely to be exclusively available to governments. Examples of techniques included:

- Public switched telephone network monitoring (PSTN);
- Mobile telephone network operators taps;
- Microwave voice and data interception;
- Legal eavesdropping by national authorities;
- Security cameras in national road networks and high streets;
- Spy satellites such as Echelon in the 1980s (a technique not originally provided by expert elicitation).

3.4.10 Collection and Processing Requirements

Collection methods are very much dependent upon the type of attack. For a single microphone egressed with radio, the collection requirement will require a radio receiver within transmission range and some form of audio recording method for this single channel of activity.

The collection will serve a single point for a single microphone against a single target. The effort will require local infrastructure and dedicated human resource if listening to live broadcasts, or dedicated recording apparatus if the audio is to be recorded and analysed at a later point in time.

Collection method	Likely user	Example
Single point	Consumer and commercial users	Specific target monitoring
Radio spectrum monitoring	Government users only	Bulk collection e.g. microwave interception
Internet monitoring	Government users only	Bulk collection through national infrastructure

Table 3.28: An analysis of all eavesdropping techniques identified, classified by collection and processing requirements.

Table 3.28 highlights just three possibilities that collection may take. From a single point, from a single source, to the larger scale provided through radio spectrum monitoring in a particular area. The cost and complexity differences of collection and processing are dependent upon the technique and eavesdropping situation.

For example: the interception of the US government's radio traffic by the KGB from the Russian Embassy in Washington in the early 1960s (See section 2.3.13) required a well-funded and technically competent organisation with considerable resources to analyse the information recorded. Today, radio receiving equipment is available at very low cost and in reach of amateur enthusiasts such as the radio scanning enthusiast. One amateur enthusiast recorded the royal 'squidgate' telephone calls during the period that cellphone calls were analogue and unencrypted (See section 1.1).

Method	No. of Targets	Cost	Complexity	Automation Potential	Single Target Identifiable	Year Started	Proximity
Analogue line recording	Very Low	Very Low	Low	Very Low	By default	Early 1900s	Close to Target
Analogue radio frequency	Low	Medium	Medium	Very Low	By default	1950s	Same City
Bulk Analogue Radio Collection	High	High	High	Very Low	Yes	1950s	Same City
Bulk Digital Radio Collection	High	Very High	Very High	Very High	Yes	1992 in UK	Same City
Bulk Internet collection	Very High	Very high	Very High	Very High	Yes	Circa 1995	Worldwide

Table 3.29: An analysis of all eavesdropping techniques identified, classified by collection and processing overview.

The collection methods have changed over time. The internet and smartphone revolution has enabled the capability to bulk collect and analyse the activities of entire user populations. This will require considerable resources to do. The resources already exist commercially with organisations such as Google.

Software has even enabled consumers to contemplate advanced techniques such as TEMPEST. Any citizen in a high-density housing situation is capable of using software-defined radio techniques for the collection of TEMPEST emissions, unimaginable only five years ago.

In order for eavesdropping systems to convert their output from information into intelligence is beyond the scope of this thesis.

Processing Method
Intensive - Audio transcription required
Intensive - Visual interpretation required
Automated - From a script

Table 3.30: An analysis of all eavesdropping techniques identified, classified by collection processing.

Example: A microphone attack placed within a busy office environment within an embassy target will require considerable effort to listen, perhaps in real time, to the output of a single microphone. If multiple voices can be heard it may require a person to differentiate the voices, followed by transcribing all that is heard. Multiply this by 26 microphones (such as the attack against the British military establishment after the Second World War) and the resource required to mount such an attack becomes considerable in human resource effort.

A comparison of one user's mobile telephone metadata gathered electronically has the ability

to produce significant quantities of intelligence way beyond that gleaned from a single audio microphone.

3.5 Chapter Discussion

This chapter provides a collection of historical and present-day eavesdropping techniques derived through expert elicitation.

For the first time, analysis is presented in this thesis that reveals the component elements of a complete eavesdropping system and the changing nature of the techniques in use.

From the eavesdropping techniques identified, the following information is revealed:

- 44% of eavesdropping techniques capture audio content. Data, video and metadata are eavesdropped on too;
- There are three distinct user groups for eavesdropping equipment: Governments, commercial organisations and domestic consumers;
- 27% can be installed at a moment's notice, while 29% require meticulous planning;
- 50% require direct access to the target or target room, while 41.5% require access to adjacent or party features of the target and currently in late 2019, 3.6% can be mounted remotely;
- 64% (approximately two-thirds) require a listening post adjacent or close to the target while 19.9% may have their Listening Post anywhere in the world;
- 62% (approximately two-thirds) are covert in nature and have some form of anti-detection countermeasures by default;
- 59.5% are physically observable in nature, while 40.5% are not;
- In order to detect an eavesdropping attack one third of the techniques require detection to be within 5 metres of the attack, another third between 6m - 50m and the remaining third, greater than 50m;
- 43% of techniques are plausibly deniable, 57% are not;
- Complexity of eavesdropping systems falls into four distinct groups;

- The number of techniques available with low complexity relate to consumer electronics. Eavesdropping techniques can be simple, moderate or complex to both procure and install;
- Currently, in late 2019, 22% of the techniques are software-based;
- 63% of the techniques are targeted against a single victim or location. Five instances are able to eavesdrop on large populations;
- Software is permitting consumers to carry out highly effective techniques such as surveillance of mobile telephones through trojan app installation or TEMPEST monitoring through software-defined radio equipment.

Important points are identified as follows:

- ☐ The egress route is a critical component of an eavesdropping attack; the egress route provided by internet growth and availability adds a considerable capability to remote eavesdroppers worldwide;
- ☐ The internet and mobile telephone networks enable governments to eavesdrop through remote access techniques against large numbers of targets;
- ☐ That targets are no longer necessarily (or increasingly) fixed in one location or one office. Modern digital systems permit mobility via access to the internet through cable, Wi-Fi or telephony data networks;
- ☐ The availability of GSM mobile telephone networks and the low cost of network services adds a considerable capability to the consumer eavesdropper. The point at which 5G networks becomes low cost will enable a rise in eavesdropping capabilities that demand greater bandwidths such as real-time video monitoring with very high-quality video formats;
- ☐ That consumer eavesdropping capability against other individuals is significant; access to the target's home and car are often available and vulnerable to attack;
- ☐ That all eavesdropping techniques are likely to become software-based as targets use ever increasing numbers of digital systems, requiring different detection techniques to be developed.

Chapter 4

Eavesdropping Technology Life Cycles

4.1 Chapter Overview

The previous chapter provided a collation and analysis of the range of close and remote access eavesdropping technologies available. This chapter considers the life cycles of eavesdropping technologies.

In this chapter:

1. The life cycle position of eavesdropping technologies is identified, through expert elicitation;
2. The eavesdropping technologies' timeline is considered in relation to other major technological introductions;
3. The egress route of identified techniques is considered;
4. Three case studies are presented for the life cycles of three eavesdropping technologies;
5. A framework is presented to consider the life cycle position of eavesdropping technologies.

4.2 The Life Cycles of Eavesdropping Technologies

4.2.1 Product Life Cycles

A product life cycle is a popular business management tool used for the marketing of products. Each product goes through a series of stages from initial Invention, Growth, Maturity, Decline and eventually Extinction (See Figure 4.1). Some products may not make it past the introduction stage, while others may never reach the decline stage; some products continue to grow and others rise and fall away.

The same life cycle occurs for technology (the technology life cycle). For example, consider the electromechanical teleprinter which went through the introduction, growth, maturing and decline phases all within a few years. It would not be unreasonable to state that the teleprinter is now extinct; its utility has been replaced by more successful technologies.

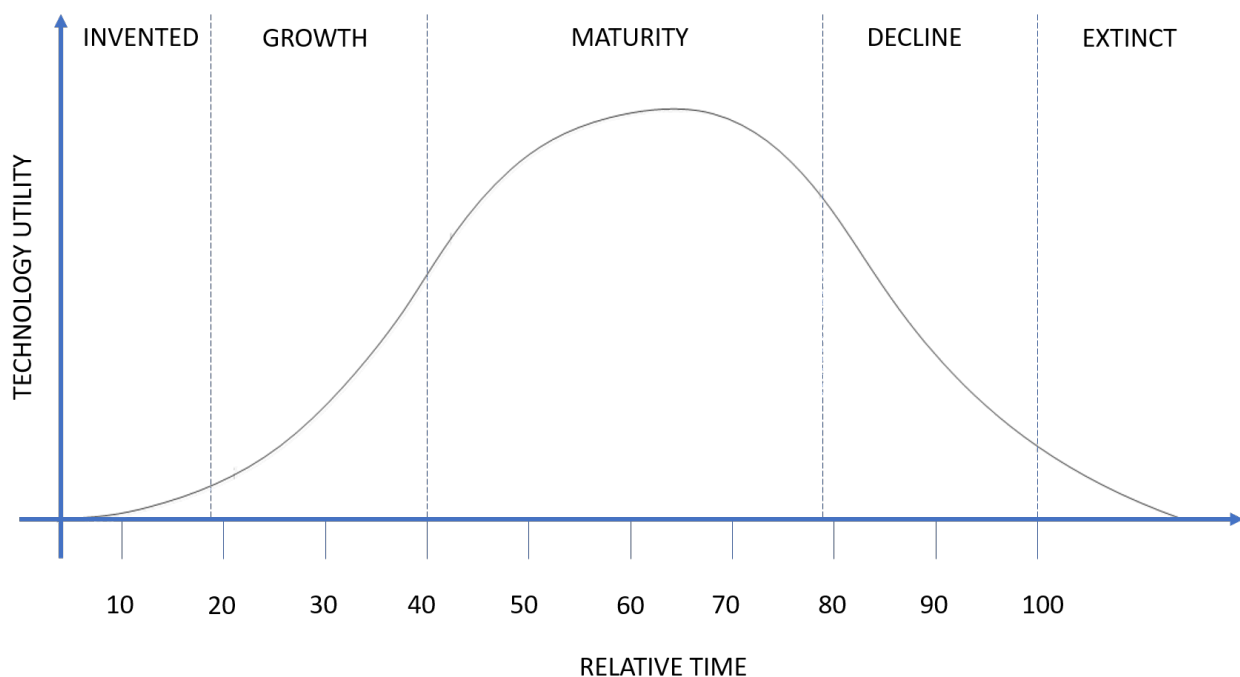


Figure 4.1: Technology or product life cycle stages.

Some technologies may experience very rapid periods of change, such as that experienced by the mobile telephone, while other technologies such as TEMPEST appear to change very little over many years. The mobile phone development is driven by a competitive sales environment

and the quest to include ever greater numbers of features in order to increase sales to large groups of consumers whereas TEMPEST life cycles are driven by government standards and thresholds required to protect information.

This is best illustrated by considering phases of life cycles. As the first cycle of a mobile telephone goes through the first stages of Introduction, Growth and Maturity, the manufacturers are already introducing the next model with the latest innovation and features.

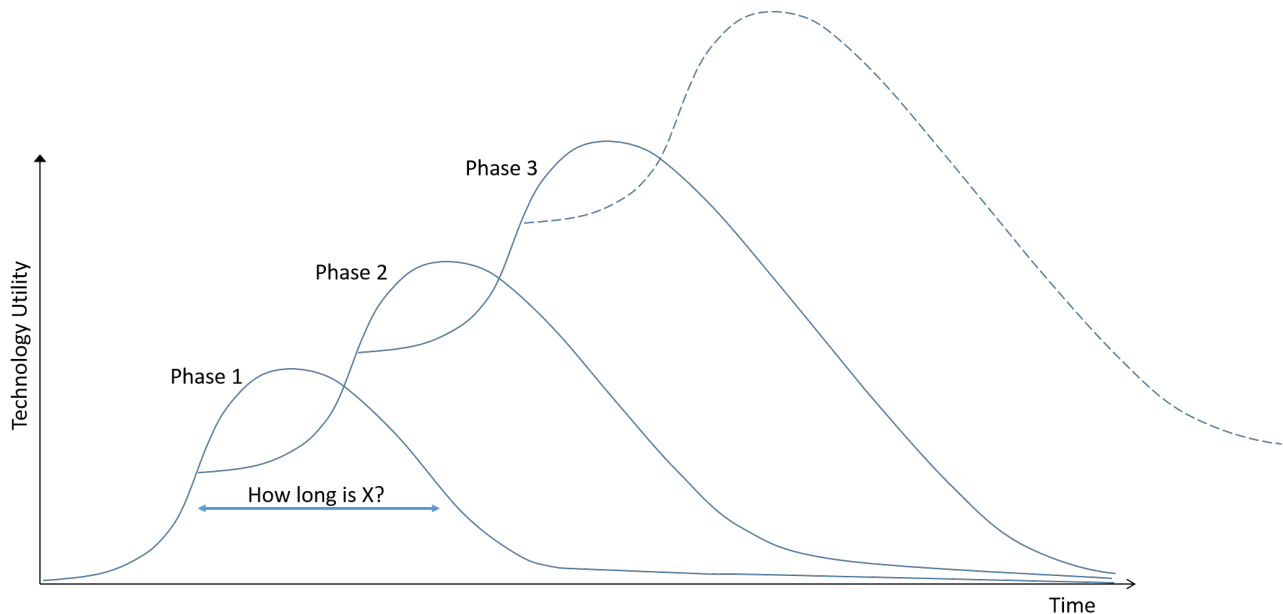


Figure 4.2: Technology life cycle phases of re-invention.

Figure 4.2 is generic and illustrates an ideal where technologies are invented and the next generation replaces the earlier technology through greater utility. The time taken for this evolution step, marked ‘x’ on the diagram, is of interest when considering future trends of a particular technology.

From observation of the surveillance technologies identified in earlier chapters of this thesis, the life cycle stage descriptions for eavesdropping technologies require a small adaption to better describe their life cycle stages.

Techniques begin their life on the design bench of the inventor. New techniques may be patented and the patent details are used by a nation with a novel new application for surveillance purposes (such as the technique developed by Theremin in Chapter 2.3.1). If the invention is by a nation’s

intelligence service, the technique will be deployed and exploited for as long as it can be kept secret. If another nation's intelligence service discovers the technique, they too will exploit it for as long as it possible (such as the illumination technique first created by Theremin in Chapter 2.3.2 and the subsequent CIA EASYCHAIR and British SATYR).

Eventually the technique appears to be leaked or discovered by either academics or those wishing to exploit the technique for commercial gain. Once capable academics review a technology, a paper may be written and disseminated, broadening the number of people that become aware of the technique. The greater the awareness, the less effective the technique becomes for collecting real intelligence. If the technique offers the potential for commercial gain, a commercial company will create the device and exploit, commercially, the device's features and benefits. Some commercial organisations that sell into government may restrict the sale and choose to only sell into government (but at a higher price to compensate) such as to the police services or other intelligence services, while others may care little and sell to anyone.

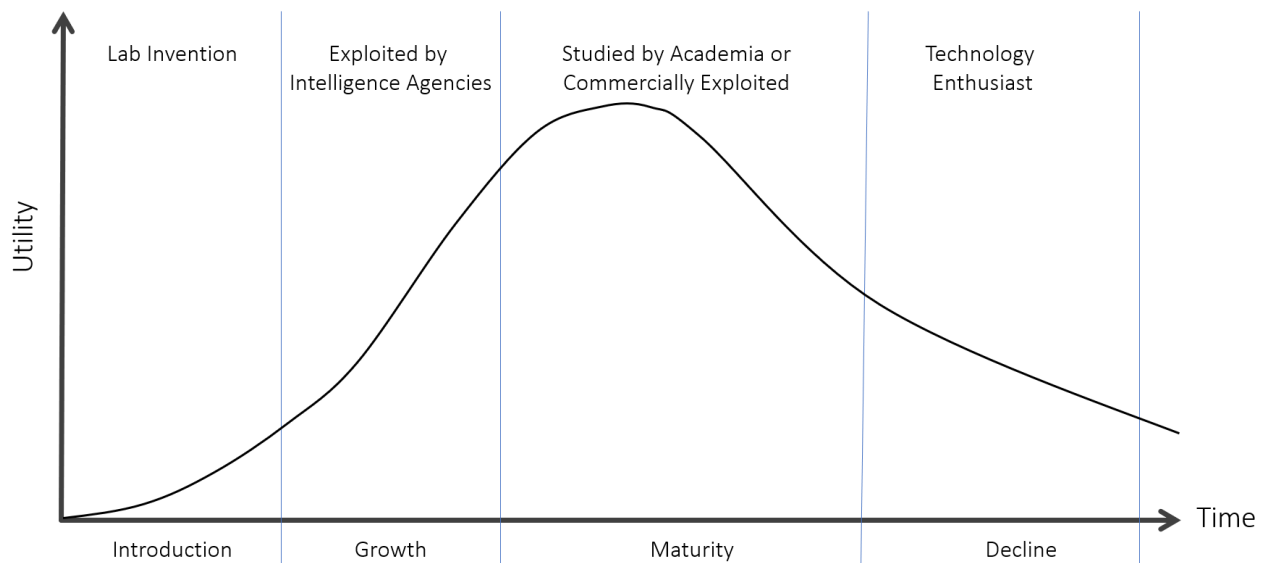


Figure 4.3: Intrusive surveillance technology life cycle.

Capable technology enthusiasts with small funds available may take an interest in a particular technique. The lack of funds may result in a novel or imaginative way of implementing a particular technique. The technique may become published on a website and attract the attention of other technology enthusiasts who may further develop the technique. The technique is likely not being developed for eavesdropping purposes, but rather for personal satisfaction, specialist

technical enthusiasm or educational knowledge.

This research uses a subset of the techniques established from earlier chapters in this thesis to define the life cycle position of these eavesdropping technologies based on the empirical review of experts.

4.2.2 Method

A group of ten subject specialists indicated the life cycle position of a range of technologies on a life cycle curve. To facilitate practical placement, the technologies were numbered and organised into sixteen groups of related technologies. Each of these groups of related technologies were mapped onto an individual life cycle curve. The technology groups, descriptions and technique identity number can be seen in Table 4.1.

No.	Technology Group	Group Description	ID Number and Technique
1	Covert Photography	Disguised photography	[59] Physical Covert Entry [32] Covert document photography [21] Neck-tie camera [29] Button camera [79] Long-range telephotography
2	Covert Video	Disguised video	[12] RF video transmitter pen [18] Video recording pen [34] Covert mains AV system [29] Button camera [13] Smart glasses for audio and video
3	Hard-wired microphones	Microphone such as those found during the cold war	[28] Probe microphone [26] Contact microphone [48] Accelerometer [33] Thin-wire egressed microphone [36] Fibre microphone [82] Self-drilling microphone [71] Magnetic induction loop audio transmitter
4	Modified Equipment for Egressed Audio	Examples include where loudspeakers have been used as microphones	[64] Rigged switch hooks [19] PC hot-wired microphone [24] Infra-red audio transmitters [25] Silent ring mobile phone [17] iPod recorder [61] Samsung TVs vulnerability
5	Radio Microphones for Room Audio	Any radio microphone	[44] Wood-block transmitters [11] RF audio transmitter pen [30] Law enforcement radio microphone [39] Broadcast radio microphone [37] Digitally encrypted radio microphone
6	Stand-off Audio	Not adjacent to a	[8] Shotgun - directional microphone

	Microphones	target property	[20] Parabolic microphone [27] Phased-array microphone [67] LASER microphone - optical lever technique [68] LASER microphone - against a retro reflector [69] LASER microphone - speckle interferometry [9] Bluetooth interception
7	Telephone Interception	Landline fixed or mobile telephone	[89] Host government legal intercept [78] PSTN tap [80] PABX exploits [5] Simple inductive telephone tap [77] GSM network operator tap [74] Real-time cellphone interception
8	Illumination Attacks	RADAR attack	[51] RF audio illumination passive (The Great Seal) [52] MI5 SATYR audio transponder [53] AudioTel SABRE audio transponder [54] NSA ANT playSet video transponder
9	SIGINT	Signals Intelligence eavesdropping on microwave distribution networks	[87] City microwave eavesdropping [88] Country-wide satellite eavesdropping [38] IMSI catching [72] Bogus cellphone base station [58] Wi-Fi interception
10	TEMPEST Emanations Exploits	Where a target is transmitting information unintentionally which an attacker exploits	[84] BELL labs TEMPEST discovery [50] RF TEMPEST [57] Optical TEMPEST [43] Video cable modified for enhanced egress [83] Marinov TEMPEST software for SDR Rx [42] Acoustic TEMPEST [86] Acoustic keyboard finger printing [35] Covert Li-Fi
11	Machine Attack	Teleprinter, Cypher machine or typewriter attack	[40] Modified typewriter attack [49] Modified teleprinter [73] Modified cypher machine
12	Computer Hardware Attack	Hardware attacked within either a desktop or laptop computer	[14] Keyboard keylogger using external hardware [15] Keyboard keylogger using internal hardware [23] Video eavesdropper by external KVM [41] USB port modification [45] Modified router or firewall [46] BIOS exploit [47] Keyboard illumination by radar
13	Software and Network Attacks	Rogue Software	[55] Trojan software Control [56] VoIP interception and exploits [65] IT network intrusion attack [66] Criminal credit card extraction [60] Personal data extraction or theft [81] Zero-day exploit
14	Store and Forward	Record in real-time and timeshift	[85] Mezon miniature wire tape recorder [63] Burst radio transmitter [70] Digital MP3 recorder [76] Credit card recorder
15	Consumer Electronics Eavesdropping Devices	Any eavesdropping device that a consumer or man in the street could purchase	[1] Exchange and Mart radio microphone kit [2] Mains two-way adapter bug [3] Audio recording pen [4] GSM audio SIM card bug [6] Hidden spy camera [10] Spy watch for audio or video

[16] USB memory stick audio bug			
16	Tracking methods	People of objects	
			[7] Tracking beacon
			[22] Live tracking with a smartphone app
			[31] Handset forensic tracking
			[62] Live tracking mobile network operator
			[75] Live tracking mobile through online function

Table 4.1: Sixteen groups of eavesdropping technologies with individual identity numbers subjected to life cycle analysis by subject area specialists.

After the ten subject specialists had indicated the life cycle position for all techniques on sixteen graphs (as illustrated in Figure 4.4), the value of the x-axis was recorded for each technology. Each technique's average was then calculated, weighted by the years of experience of each of the experts.

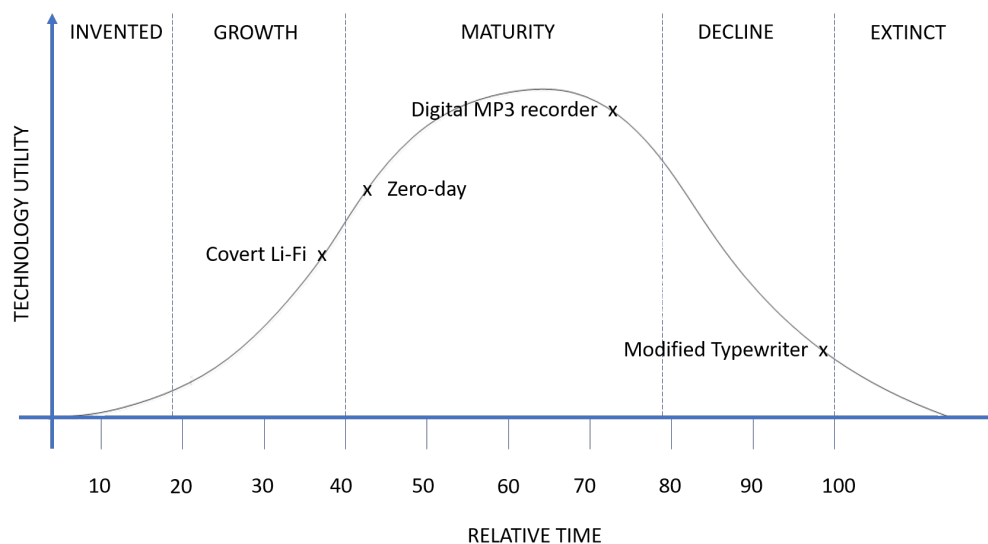


Figure 4.4: Example of the technology life cycle template used for expert elicitation.

Figure 4.4 illustrates four example eavesdropping technologies plotted onto the life cycle curve; Covert Li-Fi with an x-axis value recorded of 38.4, Zero-day with a value of 43.2, Digital MP3 recorder with a value of 73.4 and the modified typewriter with an x-axis value of 99.6.

4.2.3 Results

The results show the technique identity number and description, the average and the weighted average x-axis position for all ten subject experts, and finally the life cycle phase (growth, maturity or decline).

Unsurprisingly, none of the technologies plotted were recorded as being in the invented phase of the life cycle. Table 4.2 illustrates the results ordered by the lowest x-axis recorded position (representing the youngest life cycle phase) to the highest (representing the oldest life cycle phase).

Additional results are contained within Annex D.

Technique	Average	Weighted Average	Life cycle
[35] Covert Li-Fi	38	38.4	Growth
[81] Zero-day exploit	42.2	43.2	Maturity
[9] Bluetooth Interception	50.9	47.7	Maturity
[75] Live tracking through online function	49	49.4	Maturity
[65] IT Network intrusion attack	51.4	50.7	Maturity
[72] Bogus cell phone base station	52.4	50.9	Maturity
[54] NSA ANT PlaySet Video Transponder	54	51.6	Maturity
[74] Real-time Cell Phone Interception	52.1	51.7	Maturity
[43] Video Cable modified for enhanced egress	55.2	52.0	Maturity
[61] Samsung TVs vulnerability	54	52.1	Maturity
[60] Personal data extraction or theft	53.3	52.2	Maturity
[56] VoIP interception and exploits	52.2	52.7	Maturity
[55] Trojan Software Control	50.8	53.0	Maturity
[31] Handset Forensic Tracking	55	53.2	Maturity
[62] Live Tracking Mobile Network Operator	55.1	54.2	Maturity
[13] Smart Glasses for audio and video	54.7	54.2	Maturity
[46] BIOS Exploit	53.4	54.4	Maturity
[69] LASER Microphone - speckle interferometry	56.7	54.7	Maturity
[58] Wi-Fi Interception	53.7	54.9	Maturity
[41] USB Port Modification	56.2	55.2	Maturity
[45] Modified Router or Firewall	56.2	56.0	Maturity
[22] Live Tracking with a Smartphone App	56.9	56.3	Maturity
[79] Long-range telephotography	59.5	56.8	Maturity
[83] Marinov TEMPEST software for SDR Rx	57.2	57.0	Maturity
[66] Criminal credit card extraction	59.5	58.1	Maturity
[7] Tracking Beacon	60.2	58.4	Maturity
[89] Host Government Legal Intercept	60.2	58.7	Maturity
[38] IMSI Catching	59.4	59.5	Maturity
[86] Acoustic keyboard finger printing	62.4	60.5	Maturity
[77] GSM Network Operator Tap	60.8	60.5	Maturity
[34] Covert mains AV system	62.7	61.2	Maturity
[63] Burst radio transmitter	64	61.9	Maturity
[4] GSM Audio SIM Card Bug	62.1	62.2	Maturity
[37] Digitally Encrypted Radio Microphone	63.2	62.5	Maturity
[16] USB Memory Stick audio bug	62.8	62.6	Maturity
[76] Credit card recorder	62.6	62.8	Maturity
[25] Silent Ring mobile phone	64.9	62.8	Maturity
[36] Fibre microphone	64.4	62.9	Maturity
[27] Phased-Array Microphone	65.5	63.3	Maturity
[30] Law Enforcement Radio Microphone	63.8	63.5	Maturity
[88] Country-wide Satellite Eavesdropping	64.1	63.9	Maturity
[48] Accelerometer	66.6	64.2	Maturity
[68] LASER Microphone - against a retro reflector	65.5	64.3	Maturity
[42] Acoustic TEMPEST	66.8	64.4	Maturity
[59] Physical Covert Entry	66.6	64.6	Maturity
[71] Magnetic induction loop audio transmitter	67	65.4	Maturity
[57] Optical TEMPEST	70.1	65.6	Maturity
[6] Hidden Spy Camera	67.4	67.2	Maturity
[87] City Microwave Eavesdropping	69.5	68.0	Maturity
[23] Video Eavesdropper by External KVM	68.2	68.7	Maturity
[19] PC Hot-wired microphone	70.6	69.6	Maturity
[39] Broadcast radio microphone	69.2	69.7	Maturity
[15] Keyboard keylogger using Internal Hardware	69.9	69.7	Maturity
[18] Video recording Pen	71.6	70.2	Maturity
[26] Contact microphone	72.6	70.8	Maturity

[10] Spy Watch for audio or video	72.2	71.2	Maturity
[50] RF TEMPEST	73.3	71.4	Maturity
[47] Keyboard Illumination by Radar	73.8	71.5	Maturity
[17] iPod Recorder	72.9	71.9	Maturity
[12] RF Video Transmitter Pen	74.1	72.9	Maturity
[70] Digital MP3 recorder	73.4	73.1	Maturity
[28] Probe microphone	73.6	73.2	Maturity
[29] Button Camera	74.5	73.7	Maturity
[32] Covert Document Photography	76.5	73.8	Maturity
[67] LASER Microphone - optical lever technique	74	73.8	Maturity
[2] Mains two-way adapter bug	75.3	74.0	Maturity
[29] Button Camera	75.8	74.3	Maturity
[3] Audio Recording Pen	75.4	75.4	Maturity
[14] Keyboard keylogger using External Hardware	75.6	75.8	Maturity
[33] Thin-wire egressed microphone	77.2	76.3	Maturity
[53] AudioTel SABRE Audio Transponder	78.2	76.9	Maturity
[24] Infra-red audio transmitters	77.3	77.8	Maturity
[82] Self-Drilling Microphone	78.2	78.0	Maturity
[21] Neck-tie Camera	79.3	79.1	Decline
[1] Exchange & Mart Radio Microphone kit	82	80.8	Decline
[8] Shotgun - Directional Microphone	80.7	81.1	Decline
[78] PSTN Tap	81.3	81.2	Decline
[73] Modified Cypher machine	84	82.0	Decline
[20] Parabolic Microphone	83	82.7	Decline
[11] RF Audio Transmitter Pen	83.6	82.9	Decline
[80] PABX exploits	85.5	85.0	Decline
[52] MI5 SATYR Audio Transponder	88	88.0	Decline
[84] BELL Labs TEMPEST Discovery	89.8	88.7	Decline
[44] Wood-block transmitters	90.4	90.4	Decline
[64] Rigged Switch hooks	92	90.8	Decline
[5] Simple Inductive Telephone Tap	92	91.9	Decline
[85] Mezon miniature wire tape recorder	92	91.9	Decline
[51] RF Audio Illumination Passive (The Great Seal)	92.2	92.1	Decline
[40] Modified Typewriter attack	97.6	98.1	Decline
[49] Modified Teleprinter	99.6	99.5	Decline

Table 4.2: Ordered life cycle timeline positions of eavesdropping technologies with the youngest to oldest ordered timeline positions.

4.2.4 Discussion

Of the ninety techniques analysed only one technology was recorded within the Growth phase of the life cycle. Seventy two were recorded in the maturity phase and seventeen in the decline phase. Why technologies with an x-axis score over ninety were not recorded as Extinct is of interest; there was a reluctance within the group of experts to make a technology extinct when an old technique remained valid and could be used at some point in time, given a suitable context.

The distribution of frequencies from 38.4 to 99.5 is plotted as a histogram in Figure 4.5.

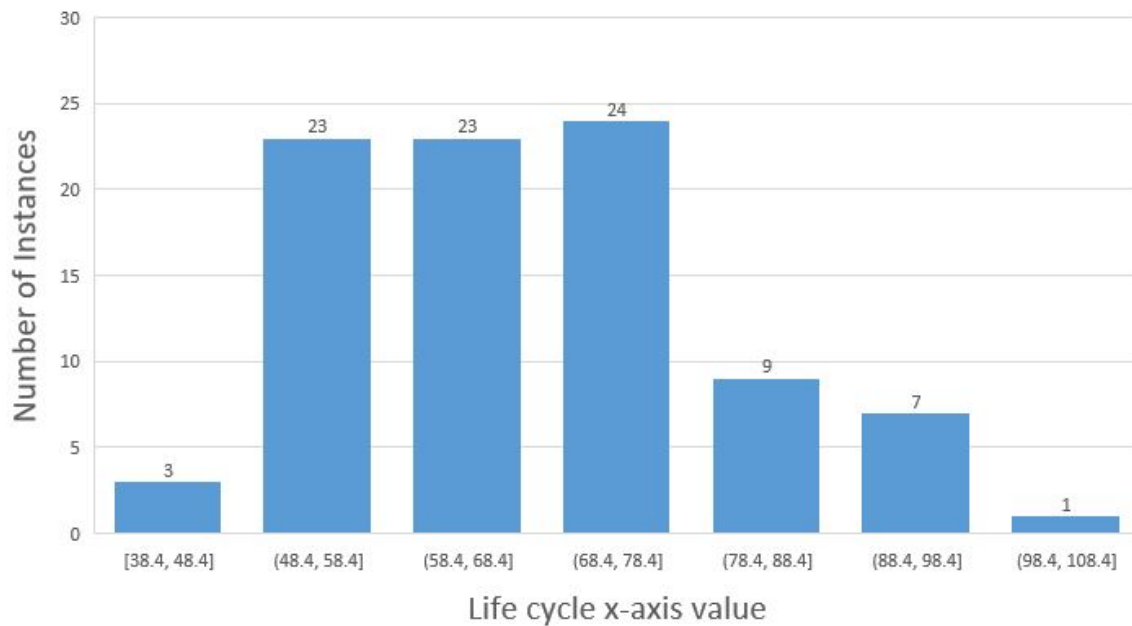


Figure 4.5: Histogram of the distribution of life cycle values of eavesdropping technologies.

Also illustrated are that three of the technologies are thought to be new techniques and are represented with x-axis values of 48.4 or lower. These three technologies are Covert Li-Fi, Zero-day exploits and Bluetooth interception.

The seventeen techniques with an x-axis value greater than 78.4 are historical in nature with many relating to techniques applicable to telephone lines, telephone exchanges and old 1970s cypher and communications techniques that are no longer in use today.

What is of interest is the seventy techniques within the mature eavesdropping life cycle phase; as of late 2019, these remain active and valid operational eavesdropping techniques.

It is interesting to consider the eavesdropping technology introduction dates. Is it not the case that techniques introduced many years ago are now becoming extinct and that new technologies that are in growth, are the most recent inventions. Figure 4.6 illustrates the distribution of these technologies over the decades. The Federal Security Service of the Russian Federation are allegedly continuing to use “extinct technology” such as manual typewriters and avoiding the introduction of newer technologies which they fear are more easily compromised by their adversaries.

4.3 Eavesdropping Technologies Introduction Timeline

In addition to the eavesdropping system model within the previous chapter in Figure 3.1 the date with which particular techniques were first introduced is listed in Table 4.4.

The Table contents have been produced from either known commercial market place introduction or from a date of an incident recorded within the literature review.

Year	Technology	Year	Technology
1878	Public telephone network	1975	Audio-video surveillance using a covert mains carrier system
1900	Acoustically poor conference rooms		Second generation laser microphone
	Event staff - uncontrolled and non-vetted	1976	Satellite interception
1900	Paper assets read	1977	Analogue recorders using tape or wire
1915	Simple inductive taps		Exchange and Mart radio microphone kits
	Telephone speech interception		Analogue cordless telephones
	Parabolic microphone		Fibre optic eavesdropping
1920	HF radio interception	1979	Microphones egressed via very thin wires
1931	Wired microphones		Deep plant microphones built-in during construction
1937	PABX exchange exploits		Deep plant accelerometers built-in during construction
	Baby monitor		Gap jumpers egressing secure environments
1940	Contact microphones	1980	Self-drilling microphone
1943	TEMPEST - radio frequency emanations		Pens with RF speech transmitters
1947	First generation laser microphone		Long-range video systems
1948	Cabling infrastructure (tampering and patching)		Infrared headphones
1949	Neckties with concealed cameras		Telephone fax interception
1950	Podium microphones		Mains socket bug
	Buttons with concealed camera lens	1984	Audio eavesdropping - Built-in applications
	Radio frequency illumination for audio eavesdropping	1985	Mobile telephone network operators taps
1953	TEMPEST NONSTOP and HIJACK		Legal interception
	Concealed in walls - microphone attached to a sound tube		Legal eavesdropping by national authorities
	The probe microphone		Real-time interception of calls - analogue
1957	Commercially available radio microphone	1990	Modified photocopiers
1959	Modified typewriters		Modified printers
	Directional microphones		Very low-light systems
	Shotgun or rifle microphone	1991	Optical fibre microphones
1960	Microphone created by switch-hook bypass in analogue telephone	1992	Projectors and projection systems
	Bumper beacon systems		
1962	Photography - Long-range with telephoto lens		Voicemail password left on default setting
			Live tracking through the use of facilities provided by network operators
1963	Comms interception	1994	Digital cordless telephones
1964	Security cameras in the high street or protecting homes	1995	Personal computer hot-wired
1965	Government manufactured		Audio eavesdropping - hardwired internal microphones
1966	Microwave voice and data interception		Keyboard eavesdropping - hardware-based keyloggers (external)
			Keyboard eavesdropping - hardware-based keyloggers (internal)
	Microwave interception		Digitally encrypted radio microphone
1968	Telephone line egress of microphone audio through remote activation		
1969	Modified teleprinters		Webcams
1970	Modified telephone to become microphonic		Microphones created from loudspeakers
	Microphones concealed in telephone equipment		Third generation laser microphone
	Telephone line connected to a radio transmitter		Taking control by means of trojan hardware
	Telephone line egress of microphone audio with low frequency carrier		Silent ring eavesdropping
	Long-range drilling		
	Silent drilling		Transmitter concealed in cellphone battery
1971	In-house hand-held radios (security officers' radios)		Inappropriate disposal of mobile telephones
1972	Video eavesdropping - Non-TEMPEST equipment	1997	Hardware eavesdropping on networks via computer power lines
1974	Magnetic loop transmission systems	1998	Eavesdropping through local software execution - zero day
	Phased array microphones	1998	Laser free-space optical links
1975	Conference room radio microphone systems	2000	Redundant computer equipment
	Concealed cabling within other building components		Infrared translation systems
	Modified calculators		Fibre or "fibre to the cabinet" interception
	Modified intercom systems	2001	MP3 recorders
			Wi-Fi interception systems

Year	Technology	Year	Technology
2001	HomePlug data sharing Real-time interception of calls - digital GSM IMSI catching	2008	Audio recording application software Taking control by means of trojan software Live tracking through the use of an application installed on the handset
2002	Access to hard drive within photocopier Fourth generation laser microphone TEMPEST - Optical emanations	2009	TEMPEST - Optical reflections from other objects Particulate flow detection microphone
2002	Broadband data interception	2009	Live tracking through the use of an online application
2003	iPods with built in recording devices	2010	Pens with digital video recorders Pens with video transmitters
2004	TEMPEST - acoustic emanations		Cameras concealed inside everyday objects
2005	Professional grade credit card recorder USB memory stick with audio recorders Pens with audio recorders Hidden spy cams Bluetooth interception Long-range photography enabled by drones		Tablets Bluetooth eavesdropping
2006	SIM card copiers	2011	Pens with handwriting capture Long-range photography enabled touchscreen snooping Near field communications (NFC)
2007	Video eavesdropping - Built-in applications Smartphones with cameras, microphones, accelerometers and Apps	2012	Using bogus base stations for spoofing ('man in the middle' attacks) Tracking by handset forensic analysis Tracking by mobile device power analysis
2008	USB connecting leads to users' laptops Plugging memory sticks into unknown equipment Video eavesdropping - replaced video cables Keyboard eavesdropping - radar illuminated Eavesdropping through printer hardware-based additions Eavesdropping through modified USB ports Eavesdropping through server bios exploitation Eavesdropping through modified router software Eavesdropping through modified firewall software Radio frequency illumination for data eavesdropping Long-range photography enabled text analysis of Keyboard entry	2013	Video eavesdropping - external KVM switches Watches with cameras and USB memory GSM bug Near-silent drilling Bluetooth device embedded in battery
		2014	Smart glasses Long-range photography enabled lip reading Optical communications via the screen Speech from smartphone gyroscope
		2015	Overt Li-Fi Covert Li-Fi Acoustic eavesdropping through wireless vibrometry

Table 4.4: The year that a particular eavesdropping technology was first introduced.

Figure 4.6 plots technologies on a timeline which illustrates that the number of eavesdropping surveillance technologies available over the period of the timeline has been increasing. This is contrary to the observation made for the general technology introduction in Figure 4.9. Figure 4.6 also illustrates that when the technologies are plotted on a timeline in decades one technology that has evolved over the last 20 years, has been responsible for much of the increase in eavesdropping incidents – the mobile telephone.

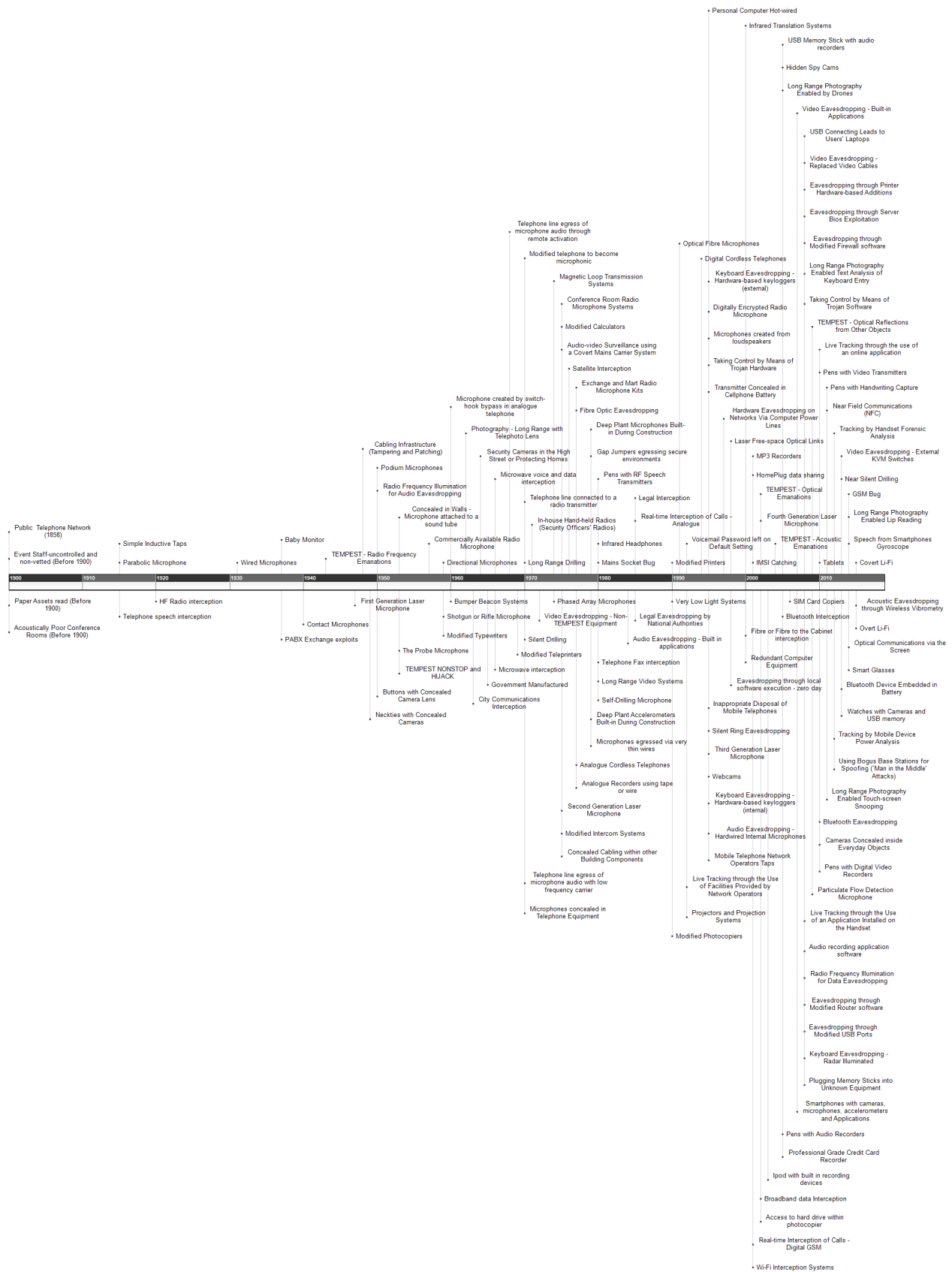


Figure 4.6: Timeline of eavesdropping technology introduction in the twelve decades between 1900 and present day.

Figure 4.7 illustrates the years in which a technology for eavesdropping was known to become available, either through commercial production, or through an eavesdropping incident. It should be noted that the timeline is not linear and that the rate of introductions between the years 1878 to 1969 witnessed 1, 2 or 3 new techniques for each year listed. After 1970, the situation changed; the frequency of new surveillance technology introductions should be considered to be evolutionary, rather than revolutionary. Two distinct spikes do occur and these may be attributed to the general take-up of the internet in 1995 and in 2008 the revelations revealed from leaked sources regarding technologies developed within the NSA ANT catalogue (United States National Security Agency (NSA) 2013).

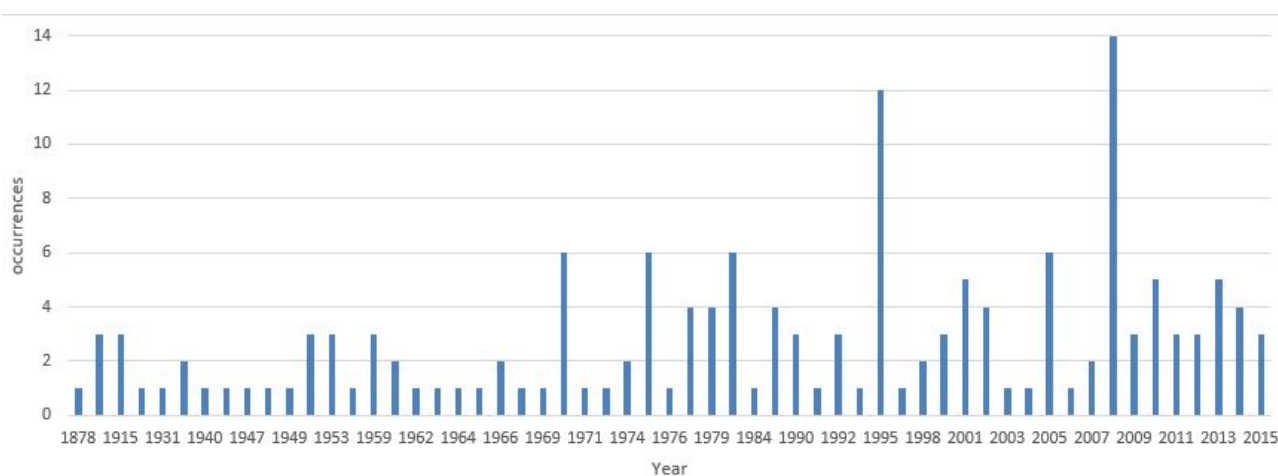


Figure 4.7: The number of eavesdropping technologies introduced by year.

The year that each technology was first seen was further analysed into seven broad groups by the method that the technique egressed its information away from the target. The seven broad egress methods considered were (i) enabled by a telephone line (ii) enabled by a physical placement and then later retrieval (iii) enabled by radio transmission (iv) enabled by some form of dedicated wiring away from the target (v) enabled by optical means (vi) enabled by the introduction of the internet or a computer network introduction and finally (vii) enabled by a mobile (analogue or digital wireless) telephone network. Further comments are available in Table 4.5.

Figure 4.8 illustrates the timeline of these seven broad groups of years first seen. The size of the bubble indicates the relative number of events that occurred in a particular year.

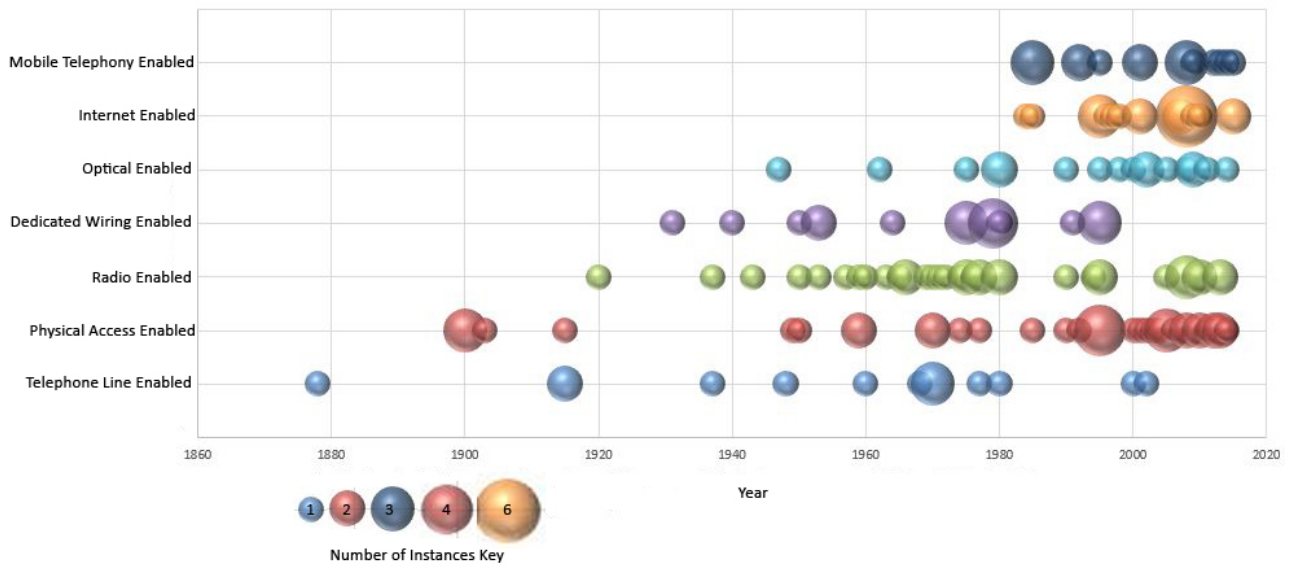


Figure 4.8: Eavesdropping egress route changes over time.

Egress Method	Listening Post Location	Setup Cost	Privacy	Detectable	Host Deniable	3rd-Party Possible	Flexibility
1: Telephone line	Anywhere between telephone handset and exchange	Medium	No	Yes	No	Unlikely	Need access to telephone line
Note: Once popular as it was often placed within a residence offering the potential to eavesdrop an unguarded moment							
2: Physical Access	Within target area or adjacent - a few metres	High	Yes	Potentially	No	Unlikely	Need physical access
Note: Physical placement & retrieval: From early document photography to the recent growth in consumer audio store and forward digital audio recorders							
3.1: Bluetooth	Tens of metres	Low	Yes	Yes	Yes	Yes	LP within wireless range
3.2: Wi-Fi	Tens of metres	Low	No	Yes	Yes	Yes	LP within wireless range
3.3: VHF	Perhaps up to 100m	Medium	If encrypted	Yes	Yes	Yes	LP within wireless range
3.4: Microwave Radio	Perhaps up to 100m	Medium	If encrypted	Yes	No	Unlikely	Line of sight to target required
Note: Enabled by the transistor and permitted portable battery-powered opportunities Recent Bluetooth and Wi-Fi techniques make this egress method a popular short-range technique							
4: Dedicated wiring	Tens of metres (If mains wiring then on same phase)	High	Yes	Yes	No	Unlikely	Need physical access
Note: A technique used for early wired microphones but increasingly less popular							
5.1: Optical (Photography)	Perhaps up to 100m	Medium	Yes	No	Yes	Yes	Line of sight to target required
5.2: Optical (LASER)	Tens of metres	High	Yes	Yes	Yes	Yes	Line of sight to target required
Note: The evolution of specialist photography techniques from the 1950s onwards to the explosion of high-quality consumer demand for video makes this technique hard to avoid in any situation							
6.1: Internet (Ethernet cable)	Within target area or adjacent - a few metres	Low	No	Yes	No	Unlikely	Need physical access
6.2: Internet (IP)	Worldwide	Low	No	Yes	Yes	Yes	Very flexible - LP could be anywhere
Note: Early networked office systems provided the first hard-wired egress opportunity The internet as an attack vector from the advent of the internet is the most significant development of all							
7.1: Mobile Telephony 2,3,4G	Worldwide	Low	No	Yes	Yes	Yes	Very flexible - LP could be anywhere
7.2: Mobile Telephony 5G	Worldwide	Low	No	Yes	Yes	Yes	Very flexible - LP could be anywhere
Note: The early analogue networks provided an easy eavesdropping opportunity but latter digital networks with low call costs make digital mobile-phone networks the choice egress method for consumer eavesdropping							

Table 4.5: An analysis of egress routes for eavesdropping purposes

4.3.1 Past Major Technological Inventions

In Figure 4.9, the linear nature of technology introduction can be compared against the introduction and availability of surveillance technology in Figures 4.6 and 4.7.

Intrusive Surveillance Technologies	Year Invented
X-rays discovered	1895
Marconi transatlantic radio signals	1901
Electronic television invented	1920
First Logie Baird televisual image	1925
Colour television pioneered	1930
RADAR developed	1930
BBC World Service starts broadcasting	1932
Typex British electro-mechanical cipher machine	1934
Rockex valve-based cipher machine	1943
Transistor Invented	1947
Gordon Gould coins the term "laser"	1950
Fibre optics pioneered	1954
Soviet Union launch Sputnik satellite	1957
Integrated Circuit developed	1958
Construction of the first laser	1958
Noreen cipher machine, developed in the UK	1960
CCD (charge-coupled device) invented	1969
ARPANET first deployed	1969
The IBM Selectric II Typewriter introduced	1971
First single-chip computer or microprocessor	1971
First hand-held cellphone developed	1973
Ethernet computer protocol invented	1973
VCR for consumers	1975
Introduction of the first mass-produced personal computers	1977
Teletext on TV available	1977
Sony Walkman developed	1980
Sinclair Zx80 launched	1980
Sony and Philips corporations Launch the Compact disc	1982
Cable TV roll-out	1983
AOL Launched	1983
Commercially available cellphone launched	1984
Astra 1A Satellite TV in UK	1988
Tim Berners-Lee invents the World Wide Web	1989
VoIP invented for sending telephone calls over the Internet	1994
Electronics companies agree to Wi-Fi worldwide standard	1997
Google.com	1997
Yahoo	1995
Apple unveils its iPod MP3 music player	2001
Apple introduces a touchscreen cellphone called the iPhone	2007
Apple releases its touchscreen tablet computer, the iPad	2010

Table 4.6: Introduction year of major technologies.

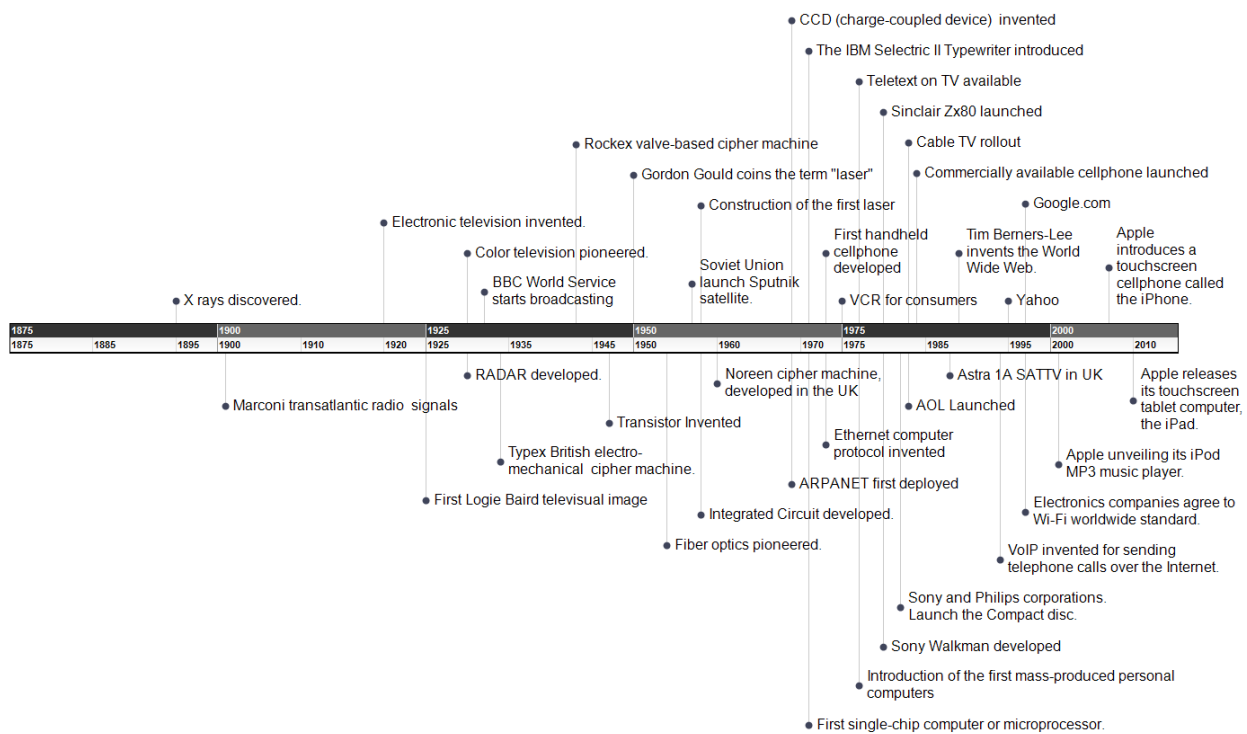


Figure 4.9: General overview of technology inventions.

Overall the trend is for cheaper computers, larger-capacity storage devices and expanding data bandwidths, all combined with ever-greater software products.

4.4 Eavesdropping Technology Evolution Case Studies

Figure 4.10 illustrates the eavesdropping technology life cycle stages for five eavesdropping techniques. These techniques show the phasing of technologies described in Figure 4.2:

1. Radio Frequency Illumination
2. Electromagnetic TEMPEST
3. The Mobile Telephone
4. The Audio Recorder
5. Acoustic TEMPEST

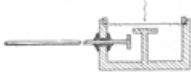












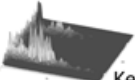
Life Cycle Stage					
Technique	Introduction (Lab Invention)	Growth (Exploited by Intelligence Agencies)	Maturity		Decline (Hobbyist Experimentation)
			(Studied by Academia)	(Commercially Exploited)	
1 - Illumination	 KGB Moscow 1940s	CIA - Mark 2 & 3 MI5 – SATYR 1955	? Evidence?	 Audiotel SABRE	 NSA Playset
2 - TEMPEST	TEMPEST: A Signal Problem <small>The story of the discovery of serious compromising radiations from communications and control equipment.</small> Bell Labs early 1940s	Peter Wright Revelations	 M.Khun's papers	 Numerous suppliers	 Marinov Thesis
3 - Mobile Telephone	EU Standards Specification 1987	Lawful Intercept RIPA 2000, CALEA, <u>Yarovaya Law</u>	GSM A5/1 A5/2 encryption studies		 Open BTS
4 - Audio Recorder	 Wax Recorder 1910s	 KGB Recorder 1950s	? Evidence?	 1980s Cassette recorder	 MP3 Recorder 2016
5 - Acoustic Intelligence Evolution	? Evidence?	 KGB Microphones	 Keyboard Acoustic Analysis	? Evidence?	? Evidence?

Figure 4.10: The life cycle stages for five eavesdropping technologies.

However, not all phases in the evolution are evidenced; the matrix prompts questions as techniques 1, 4 and 5 illustrated contain gaps in the detail of the life cycle stages. For example: the first illumination technique was invented by Theremin and then exploited by the Russian Security Services and quickly followed by the American and British Secret Services. The next phase steps over evidence of any academic interest straight into a commercial product and

final experimentation by amateurs. The life cycle prompts the question of how the technique transitioned to commercial interests.

Another example, Figure 4.10, raises questions in other phase gaps. The earlier chapter on historical eavesdropping events (Chapter 2) contains many examples of microphone installations in offices and cypher rooms. The academic phase and interest for decoding keyboards and keypad entries from acoustic TEMPEST emissions by utilising modern computer analysis techniques is known. This, together with the known placement of microphones adjacent to office typewriter and cypher machines, alludes to the likelihood that the microphones deployed were placed to detect acoustic TEMPEST vulnerabilities, rather than human speech.

This study technique of placing what is known into the life cycle stages for types of eavesdropping equipment generates questions regarding missing pieces of the jigsaw and also the prompt to consider not just the past but the future too.

The first three techniques, Illumination, Radio Frequency (Electromagnetic) TEMPEST and the mobile telephone life cycles are discussed in greater detail in the following case studies.

4.4.1 Case Study 1 - Illumination

Figure 4.11 illustrates the evolution of the illumination technique. The earliest known mention of this technique is from Theremin Buran Radar's (Glinsky 2000a) description of this experimental technique in secret early development under considerable pressure from the KGB. In 1951 an incident at the Naval Attaché's office (See Chapter 2.3.2) in the British Embassy Moscow was suspected of involving this illumination technique (P. Wright 1987a). A year later, the most famous of all eavesdropping devices had been discovered; the 1952 Great Seal (see Chapter 2.3.2) which hid the resonant cavity illumination device within its wooden carving while it hung above the American ambassador's desk in his official Moscow residence (Crypto Museum 2016b).

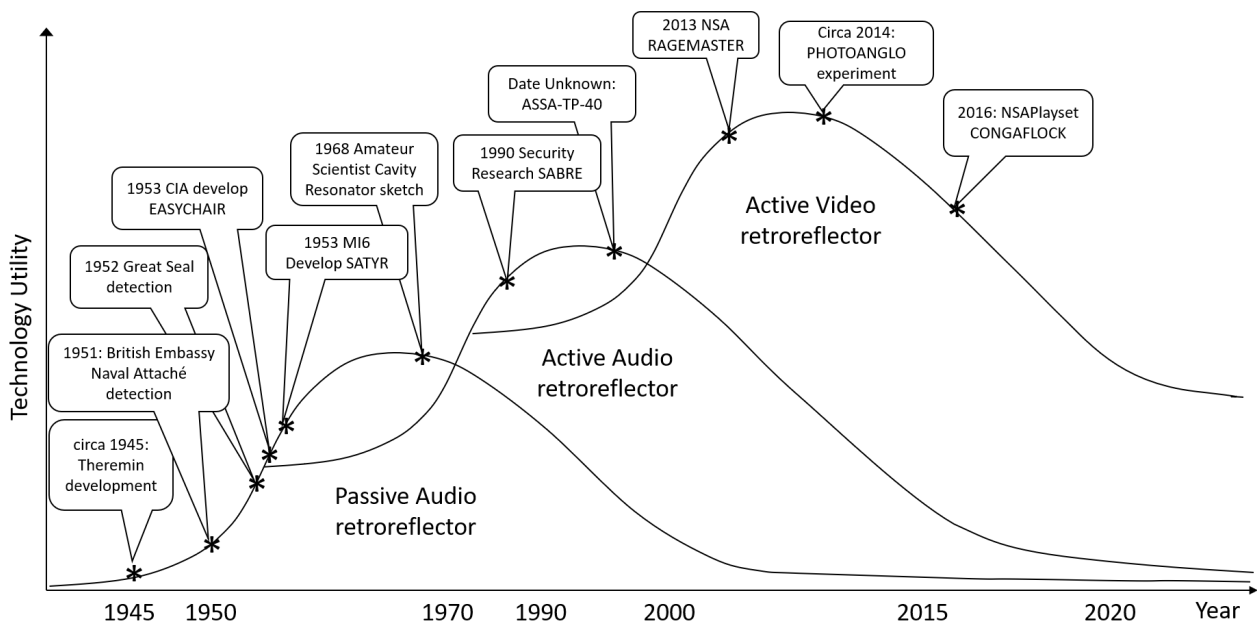


Figure 4.11: The three life cycle phases of innovation of the illumination eavesdropping technique from 1945 to 2019.

As reported by Peter Wright (P. Wright 1987a) the CIA and British soon reverse engineered the technique and produced their own versions. The Americans developed EASYCHAIR (Crypto Museum 2015) in 1954 with the help of the Dutch Security Service (BVD) and the Netherlands Radar Proefstation (NRP) in Noordwijk. The British developed SATYR (Crypto Museum 2016a). This technology, like the original Soviet device, was entirely passive; no power source was used in the devices in order to recover audio from the target.

The technique was made public in May 1960 by the Americans when they announced to the world at the United Nations that the Great Seal bug had been found earlier in 1952 (See 2.3.2).

An early sketch of the passive resonator was published in the *Amateur Scientist* in 1968 (Strong 1968) but this was never exploited commercially.

Life cycle phase 2 includes a considerable jump in the development of this technology in the form of a commercial product called SABRE (Security Research 2015) thirty-seven years later. Although this technology was also for the recovery of audio from the target, the construction used 1990 surface-mount electronic component construction. A critical difference too was the inclusion of a small battery power source that powered a small oscillator. The inclusion of a battery power source meant that the illumination ‘flooding’ energy requirement could be considerably reduced. The SABRE device was not the only commercial device offered to the marketplace and one other variant was produced by another commercial concern.

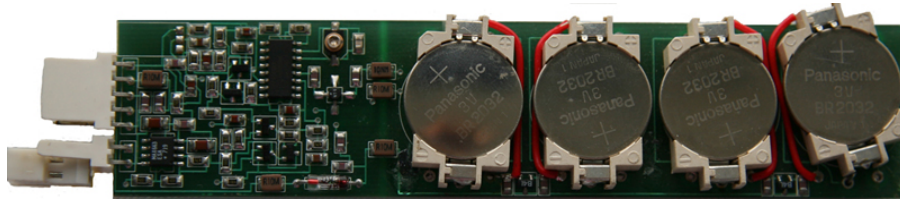


Figure 4.12: The Sabre device with battery support to enable a decrease in the illumination source power level.

The third life cycle phase, which became public knowledge in 2013, includes the development of the illumination technique against a composite video source rather than audio. This development codenamed RAGEMASTER was developed by the NSA and leaked in the ANT catalogue (United States National Security Agency (NSA) 2013).

The most noticeable and final development of this technique was made by the amateur enthusiasts who reverse engineered the NSA RAGEMASTER system in order to create an experimental NSA PLAYSET (NSA Playset 2016) and created their own version of the illumination technique.

This sequence of events illustrates the full life cycle to date: from its invention, some growth through the security services, the maturity and exploitation by commercial retailers, with the

final extinction and eventual experimentation by hobbyists and enthusiasts.

In summary:

- The first invention was by a Soviet government scientist (under considerable duress to succeed);
- Once one security service had invented the technique, two other security services quickly copied the technique;
- The technique's details remained closely held by governments;
- The technique became public knowledge in 1960 when announced at the United Nations;
- A drawing of the technical details was revealed in the *Amateur Scientist* in 1968 but was not commercially exploited at the time;
- Thirty-seven years later, the audio illumination technique was updated with active components by a specialist UK commercial supplier. In what way it was ever used operationally is unknown;
- At some time before 2013 the technique was updated to include the illumination of video by the NSA;
- In circa 2016, the technique was reverse engineered by enthusiastic hobbyists, following the very high-profile public awareness generated by WikiLeaks.

4.4.2 Case Study 2 - TEMPEST

Figure 4.13 illustrates the evolution of TEMPEST from the earliest discovery in the BELL Laboratory (Cryptologic Spectrum 1972a) in 1943. TEMPEST was reported to be a working technique by Peter Wright (P. Wright 1987a) when in the 1970s it was used against the French Embassy in London.

In 1972 the NSA released a paper (Cryptologic Spectrum 1972b) to the community in order to raise awareness of the vulnerability in order to enable organisations to implement appropriate countermeasures where required. With this awareness, commercial manufacturers provided

many expensive high-end specialist receiver and antenna test equipment together with TEMPEST standards for the safe levels of emissions required to be met by specialist computer manufacturers who certified this equipment as TEMPEST.

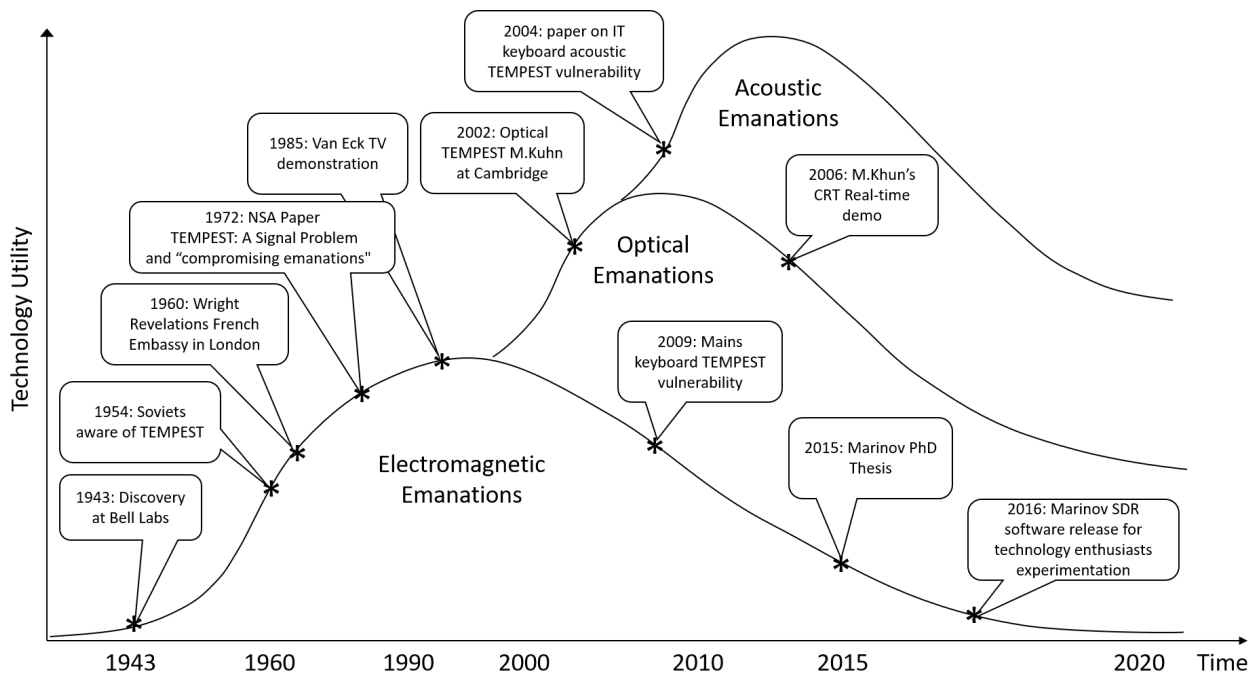


Figure 4.13: The life cycle phases of TEMPEST eavesdropping technologies.

Between 2002 and 2006 Markus Kuhn began to describe Optical TEMPEST in a series of academic papers (Kuhn 2002, 2003, 2004, 2005a,b, 2006) and he demonstrated his experiments on a working system that could decode the faint emission originating from a cathode ray tube computer display. In later work, Kuhn researched Optical TEMPEST from LCD displays (Kuhn 2013, 2016).

In a final phase of the TEMPEST life cycle, a tool was created as part of a PhD thesis (Marinov 2016b); academic interest by Marinov in TEMPEST has resulted in the creation of a software tool that is interfaced to a low-cost and high-performance software-defined radio receiver. This combination of low cost hardware together with software shared on an open-source basis has enabled TEMPEST experimentation by technology enthusiasts and electronic experimenters worldwide.

Access to Marinov's software programme is one step towards the ability to carry out a successful TEMPEST eavesdropping exercise. However the enthusiast would require considerable radio

knowledge in order to effectively receive sufficient radio energy, together with considerable knowledge of the characteristics of the items being eavesdropped upon.

There are three life cycle phases of TEMPEST identified: Electromagnetic emanations, Acoustic and Optical. The electromagnetic TEMPEST phases span from first invention in 1943 to the Software Defined Radio TEMPEST tool available in 2016. Although the optical phase appears before the acoustic phase, it is certain to have originated very much earlier than the academic paper written in 2004.

In summary:

- TEMPEST refers to emissions that occur naturally, not through some form of deliberate technical attack;
- TEMPEST emanations were discovered by accident in a government laboratory;
- Then exploited as an eavesdropping technique by governments for as long as possible;
- The commercial test equipment industry grows around servicing the defensive needs of governments;
- The public eventually gained awareness of TEMPEST through a TV Programme;
- Eventual academic interest in TEMPEST radio emissions by computer scientists;
- Eventual jump in academic imagination to consider other forms of TEMPEST;
- Optical TEMPEST from CRT screens vulnerability highlighted by academia;
- The starting point for the life cycle for acoustic and optical TEMPEST is unknown. If the pattern of life cycle sequencing is valid, governments have been aware of both acoustic and optical TEMPEST for decades;
- Exploitation of software-defined radio receivers published in a PhD thesis by a PhD student (Marinov 2016b);
- Interestingly, new phases of TEMPEST vulnerability are predicted. As data rates increase with increased network speeds, so too will TEMPEST vulnerabilities.

4.4.3 Case Study 3 - Mobile Telephone Eavesdropping

Figure 4.14 illustrates a fundamental point about the mobile telephone when compared to the ideal eavesdropping system. The perfect eavesdropping system has a range of sensors for audio, video together with tracking and position information. The ability to store data for a delayed transmission, the ability to program the device for a variety of situations all powered with a long battery life that also permits some ability to remote charge if a direct physical connection is not available. The radio transmission link must be reliable with a readily available listening post in range that will not attract attention. The choice of a radio frequency is important too; a frequency that doesn't stand out and is within a busy part of a radio spectrum, but equally, a frequency that will egress through buildings. The frequency wavelength should not require a long antenna to radiate effectively. The transmission link should be encrypted in order to provide link privacy. Ideally too, the technology should be low-cost and deniable.

The mobile telephone meets all of these requirements. Furthermore, it offers the eavesdropper a direct link to an individual. The mobile telephone is likely to be with the individual at all times, offering surveillance opportunity on all personal and professional activity if access to all applications installed on the phone are available.

A target's mobile telephone is almost certainly the single most important device to gain access to by any eavesdropper. Even as recently as 2017, the top ten uses of a smartphone did not include actually using the phone to speak to someone (mobiles.co.uk 2017).

The top ten daily uses of smartphones:

The top ten daily uses of smartphones	
1. Text - 88 per cent	6. Online shopping - 56 per cent
2. Email - 70 per cent	7. Checking the weather - 54 per cent
3. Facebook - 62 per cent	8. WhatsApp - 51 per cent
4. Camera - 61 per cent	9. Banking - 45 per cent
5. Reading news - 58 per cent	10. Watching YouTube videos- 42 per cent

Table 4.7: The top ten daily uses of smartphones in the UK. Note that making a telephone call does not feature in this list. Credit (mobiles.co.uk 2017).

What is not included is all of the additional metadata given away if the user’s geolocation facilities are shared for popular services such as mapping.

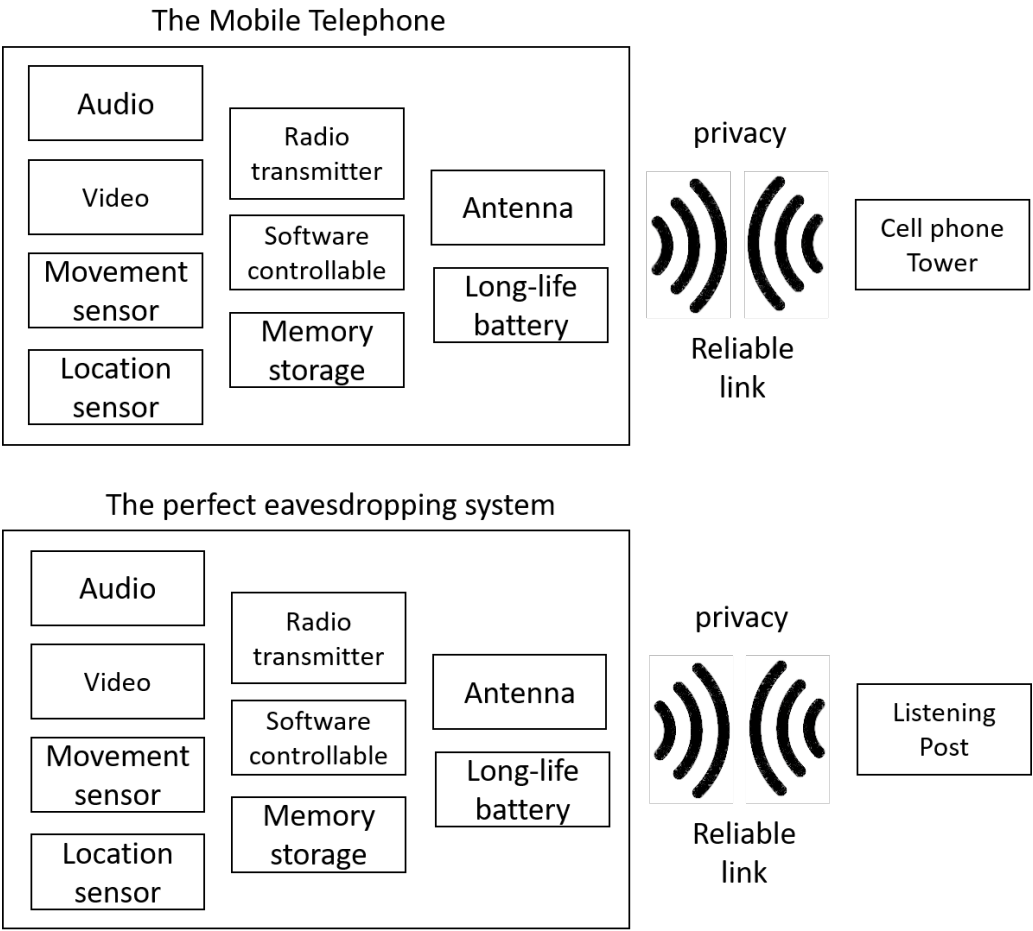


Figure 4.14: A comparison between the components of a mobile telephone system and the perfect eavesdropping system. The similarity should be noted.

Table 4.8 catalogues on the left-hand side the technological developments and small increments of continuous innovation for the most significant elements and features of mobile telephone technology. The right-hand column illustrates the year that a mobile telephone exploit was introduced.

Table 4.8 illustrates that for every new mobile telephone innovation development, after a small delay, an eavesdropping method became available to exploit in some way or another the new feature introduced. In the earliest days of the analogue mobile telephone, eavesdropping on the open radio networks between the handset and the cellphone tower was a trivial exercise. Proximity to the cellphone tower was the only requirement.

MOBILE TELEPHONE DEVELOPMENT	YEAR	MOBILE TELEPHONE EXPLOIT DEVELOPMENT	YEAR
1G UK Analogue Mobile phone roll-out	1985	Legal Eavesdropping by National Authorities	1980
2G GSM roll-out in UK	1992	Radio scanners tune into analogue calls	1986
SMS service introduced	1992	Time range-gate and antenna direction locating	1991
Voice mail introduced	1992	Live Tracking through Network Operator Facilities	1991
WAP Enabled handsets available in Europe	1999	Voicemail Password left on Default Setting	1992
First Watch Phone	1999	Silent Ring Eavesdropping software on mobile phone	1997
First Camera Phone	1999	Wi-Fi Interception Systems available commercially	1997
First GPS integrated receiver	1999	Bluetooth Device Embedded in battery	2000
BlueTooth available on mobile phone	2000	Transmitter Concealed in mobile phone battery	2001
First MP3 player on mobile phone	2000	SIM Card Copiers	2001
2.5G roll-out	2001	Real-time Interception of Calls A5/1	2001
GPRS Introduced	2001	IMSI Catching systems commercially available	2003
First email on a mobile phone	2001	Real-time Interception of Calls A5/2	2003
First Infrared port	2001	Children - Parental mobile phone tracking services	2005
First built-in FM radio	2001	Live Tracking through online application	2005
First full colour screen	2001	Live Tracking through application installed on mobile phone	2008
First long battery life phone	2002	Taking Control by Means of Trojan Software	2008
First Camera Phone	2002	Taking Control by Means of Trojan Hardware	2008
Wi-Fi available on mobile phone	2003	Near Field Communications (NFC) Exploits	2009
3G roll-out	2003	Audio recording application software	2010
1Megapixel camera	2004	Real-time Interception of Calls A5/3 (Kasumi)	2010
First dual processor phone	2006	Bogus Base Station Spoofing ('Man In The Middle Attacks')	2010
First mobile phone with a touch screen	2007	Software Defined Radio Base Station hack	2010
iPhone launched	2007	Tracking by Handset Forensic Analysis	2010
First 5 Megapixel camera phone	2007	Text Harvesting technology available commercially	2011
First Android OS on mobile phone	2008	Optical Communications via the mobile phone screen	2012
Handwriting recognition on mobile phone	2008	Tiny GSM modules available for throw-away bugging use	2012
Accelerometer built into mobile phone	2009	Spy software installed on mobile phone remotely	2013
First HD video camera built in	2010	Bluetooth Eavesdropping systems available	2013
Lithium batteries in mobile telephone	2011	Inappropriate Disposal of Mobile Telephones	2013
Near Field Communications added to cellphones	2010	Tracking by Mobile Device Power Analysis vulnerability	2012
4G roll-out	2013	US Government Survey Catalogue Leaked	2015

Table 4.8: Left-hand column: The major development stages of the mobile phone. Right-hand column: Consequential eavesdropping exploits introduced.

The introduction of GSM in 1995 added some privacy to the radio links between the handset and tower, but by 2001 decryption interception tools became available. Each mobile phone evolution has presented the intrusive surveillance eavesdropper a new challenge in order to ensure continued surveillance possibilities.

The timeline in Figure 4.15 illustrates, in five-year blocks, a dual timeline for the period 1980 to 2015. Events below the timeline represent the continuous innovation and introduction of new features for the mobile telephone technology, while those above the timeline illustrate the innovation and introduction of new eavesdropping exploits targeted against the mobile telephone.

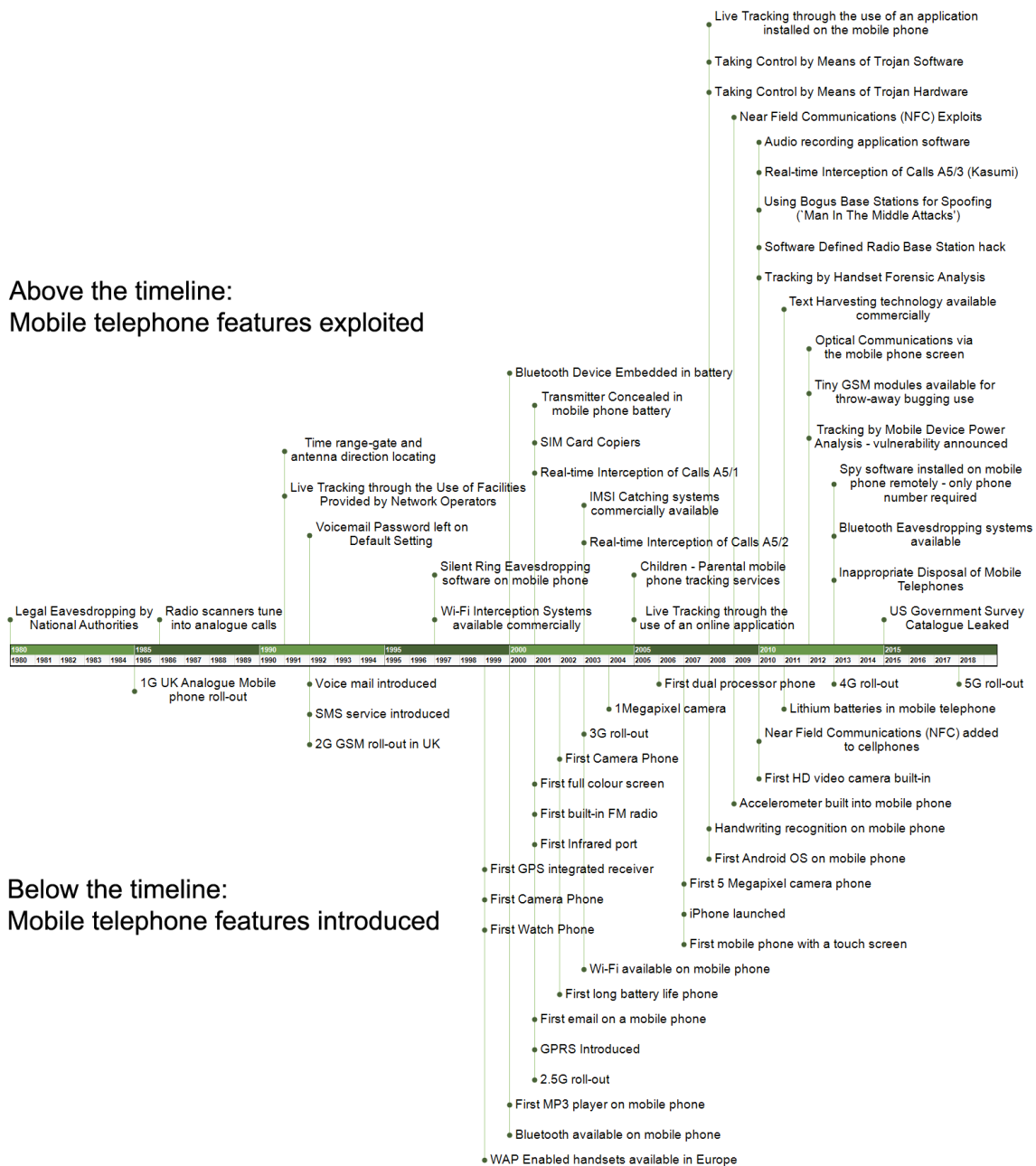


Figure 4.15: Mobile telephone development 1980 to present day. Annotation above the timeline: Mobile telephone exploit introduction years. Annotation below the timeline: Significant stages of mobile telephone technology development.

In summary:

- Eavesdropping on the first analogue systems was relatively simple and enabled by commercial low-cost radio scanners. Anyone in range of a base station could hear one side of the conversation. Anyone close enough to the mobile telephone handset could hear the handset conversation. With two receivers, both sides of the conversation could be heard

(if in range of the handset). Despite lack of privacy, mobile phone users remained either ignorant or did not care about the eavesdropping risk;

- With free-to-air transmissions, early analogue mobile phones required no modification to enable eavesdropping;
- GSM attempts to add privacy were quickly overcome. The internet became a source of propagating the decryption techniques;
- Commercial systems became available to decode the GSM privacy;
- Higher battery capacity enabled the powering of larger screens;
- Data availability on cellphones enabled email and applications to become available;
- Uncontrolled application installation on mobile telephones increased opportunities to eavesdrop;
- Increased memory and sensor types on smartphones and increased data bandwidths enabled ever more sophisticated eavesdropping systems on smartphones;
- Public awareness continues to show low concern for the eavesdropping potential;
- Social media usage by smartphone users reveal ever-greater information for every user;
- If you are concerned about the risk of being eavesdropped upon by a mobile telephone, the only effective prevention is to not use or own a mobile telephone;
- Mobile telephones will continue to provide governments and well resourced eavesdroppers with a powerful method of surveillance on individuals who own or use a mobile telephone;
- Ultimately, it is for the user to conduct a risk-balance case. Does the advantage of using the mobile phone outweigh the eavesdropping risk or concerns of an individuals right to privacy?

4.5 Chapter Discussion

This chapter highlights some important points about eavesdropping technology:

- Technology continuously evolves and reinvents itself, but the fundamental physics principles remain;

- Secret government techniques eventually become public knowledge. This may be from links with academia or commercial companies, insiders leaking information (so called whistle-blowers such as Snowden);
- The entry barriers for even advanced eavesdropping techniques are continuously lowered through technology evolution;
- Continuous horizon scanning is critical to successful countermeasures organisations with a requirement to operate on the Inform or Exploit life cycle edge.

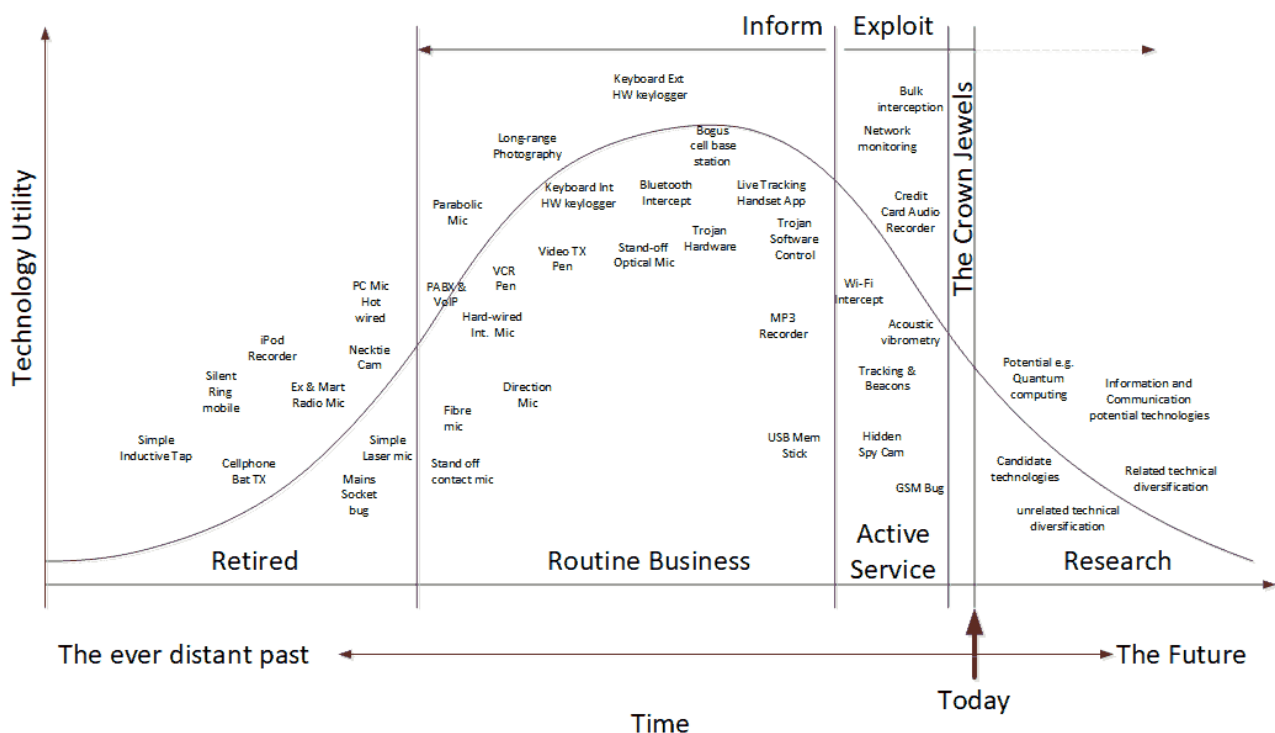


Figure 4.16: Eavesdropping life cycle ‘Inform/Exploit’ framework to consider the constant innovation of eavesdropping technologies.

Figure 4.16 illustrates eavesdropping life cycles in a single “reversed” life cycle diagram. The diagram provides a framework (with some technology examples plotted for illustrative purposes only) in which to consider the eavesdropping technologies that are no longer a threat, technologies that have become older tools but need to be remembered from a countermeasures point of view, eavesdropping technologies that are used in active service and finally those that remain closely guarded by governments wishing to gain an intelligence advantage.

Technologies at the end of life can be seen on the left-hand side of the diagram, with those currently only at the research stage, that will not become a threat until some time in the future, are on the far right-hand side. There is a large and ever-increasing variety of eavesdropping technologies all at a different point on their own unique life cycle path.

History teaches us that there will be a careful balance in existence between technologies with exploited vulnerabilities and technologies which require protection to protect our own defences against these same vulnerabilities. Those wishing to protect national interests will need to ensure they operate in the active service area and reach out to a wide range of research institutions to appreciate what is over the horizon and currently under development.

This framework looks to the future: it offers the eavesdropping countermeasures industry a mechanism by which to plot all known eavesdropping technologies in order to highlight the relevance of their own countermeasures strengths, weaknesses, opportunities and threats and to consider those that may arise in the near future. Any information gleaned from the world's intelligence services about the technologies active in the 'Crown Jewel' region will need to be mindful that these techniques may be in active use and form part of the 'Inform - Exploit' paradox.

Chapter 5

Dealing with Uncertainty: Bayesian Predictive Model

5.1 Chapter Overview

The preceding chapters have considered past and present eavesdropping technologies. This chapter considers, through the use of a suitable computer model, the potential to predict eavesdropping techniques deployed given a particular scenario.

Predicting eavesdropping technology deployment involves complexity and uncertainty in abundance. Experience may assist an expert but the introduction of a suitable model, where uncertainties are assigned probabilities, offers greater potential for prediction and therefore enhanced risk management.

An expert-led independent study on the UK computational modelling capability asserts that “Models can help to comprehend a complex world that is beyond immediate understanding” (Government Office for Science 2018, p.14) and that “The complexity of the system means that the risks and consequences of any choice cannot be anticipated on the basis of common sense or experience”. However, the combination of statistical judgement together with expert evidence will be researched in order to determine whether eavesdropping prediction is possible.

In this chapter:

1. Bayesian modelling for eavesdropping technology prediction is considered;
2. Expert elicitation is used to capture capability and opportunity requirements for a range of eavesdropping technologies identified in earlier chapters;
3. A complete Bayesian model for eavesdropping capability, opportunity and intent is developed;
4. The model performance results and validation are presented;
5. The potential for future work is identified.

5.1.1 Dealing with Uncertainty - Bayesian Overview

Bayes' rule was discovered by Thomas Bayes (1701-1761) and later, independently by Pierre-Simon Laplace (1749-1827). It has taken more than two centuries to emerge as a powerful tool. Bayes' rule is a rigorous method for interpreting evidence in the context of previous experience or knowledge (Stone 2013). One can think of Bayes' rule in terms of updating our belief about a hypothesis 'H' in the light of new evidence 'E'.

$$P(H|E) = \frac{P(E|H)}{P(E)}P(H)$$

Bayesian Belief Networks (BBN) are probabilistic graphical models that enable us to reason about uncertainty, with the uncertainty stored within an associated probability table. Each model comprises arcs and nodes. The arcs have a direction and represent causal relationships between variables while the nodes represent multiple states or values which can be discrete or continuous.

The probability of a state or value occurring at one of these nodes is termed a belief. The probability may be subjective (based on past experience, emotion or previous evidence) or objective (not influenced by emotions, opinions, or personal feelings and is quantifiable and measurable).

BBNs are an effective way of revising probabilities based on event observations (Beliefs); Beliefs are some form of body of knowledge. BBNs can be used for prediction (Inferencing) through knowledge gained from a machine learning process or gained through expert elicitation. Bayesian updating updates the model with evidence to further improve model performance.

Recent developments now permit the use of Bayesian techniques due to numerous software programs that efficiently implement algorithms which can use a reasonable number of variables.

BBNs provide the ability to:

- Explicitly model causal factors;
- Update beliefs in the model based on new evidence;
- Make predictions based on incomplete information from past events;
- Combine diverse types of evidence which may include subjective and objective data;
- Arrive at decisions based on visible and auditable (challengeable) reasoning.

The use of learning from BBNs may offer some potential; the output of the BBN could assist a Neural Network learning approach. However, eavesdropping events are rare and although a database of over 300 events has been created from open source material, this may be insufficient data for such an approach.

The key challenge for Bayesian modelling is the selection of available evidence for the creation of the network structure of the nodes and arcs. Professor Fenton's Software Metrics (Fenton and Bieman 2014) offers practical help to identify appropriate parameters to model.

There are few discussions of Bayesian modelling that do not discuss the sprinkler example written by the pre-eminent researcher, Judea Pearl (Pearl 2009, p. 15). The problem comprises five dependencies: Season, Sprinkler, Rain, Wet and Slippery. The model illustrates the probability of Slippery being caused by the Season, with which there is no direct link.

Using the causality principles of Bayesian modelling, with the ability to make predictions based on incomplete information, it may be possible to predict the likelihood of an eavesdropping event, together with the type of eavesdropping technology deployed.

5.1.2 Bayesian Belief Networks used for Threat Analysis

The use of BBN modelling for crime prediction may have many similarities to eavesdropping prediction, although many eavesdropping incidents remain undiscovered (or, in the opinion of the attacker, are successful), or even if the eavesdropping attack is discovered, it may remain unreported. Incidents whereby eavesdropping attacks are discovered or exposed by historians, political defectors, journalists or Technical Surveillance Countermeasure (TSCM) teams continue to provide a source of often incomplete and inaccurate information.

Olama (Olama et al. 2010) provides an example of a three-layer BBN model which ‘takes into consideration the relative threat of an attack against a particular asset’. The model also predicts the ‘individual psychology and motivations that would induce a person to either act alone or join a terrorist group and commit terrorist acts’.

The model assesses threats by combining information from disparate data sources, most of which involve uncertainties. The model also considers the likelihood and consequences of a threat and draws inferences about the risk of a terrorist attack. This would appear to be a very similar problem posed by the threat of an eavesdropping event. The challenge is to identify the disparate intrusive surveillance data sets, as with this example, into a coherent, analytically defensible and understandable manner.

Ronsivalle used a combined Artificial Neural Network with a BBN to assist with the modelling of bank robberies in Italy (Ronsivalle 2011). While the use of a Neural Network may or may not be helpful, Ronsivalle’s paper contains helpful guidance for the creation of the nodes and arcs required for the Bayesian network. The example of a ‘Robbery risk analysis model’ illustrates the challenge of codifying the problem into a Bayesian network.

The area of crime or burglary prediction contains similarities with the prediction of eavesdropping events, that is, random or rare, and largely unpredictable events that occur against a particular asset. Prakken et al. modelled crime scenarios with a BBN (Vlek et al. 2013), Baumgartner et al. used a BBN to profile criminal activity from limited data (Baumgartner, Ferrari, and Palermo 2008), and crime risk factors were analysed by (Boondao 2008).

A literature review of stochastic modelling identified specific modelling relating to risk assessment (Fenton and Neil 2012), (Stone 2013, 2015) and (Hopgood 2016). In particular, Fenton and Neil's papers on the use of Bayes on Causal Modelling in Decision Making, Uncertainty and Risk (Fenton and Neil 2011) and Managing Risk in the Modern World (Fenton and Neil 2007), together with the further publication (Trucco and Leva 2012, pp.97-104), have provided an overview of the potential for BBNs to model the combination of statistical judgement and expert evidence in order to predict the likelihood of a particular eavesdropping technology being used in some context.

There are many qualitative risk analysis methods, frameworks and techniques developed too. Examples include:

- The 'Operationally Critical Threat Assessment and Vulnerability Evaluation (OCTAVE) approach (Alberts et al. 1999), which considers risk impact through an impact evaluation criteria;
- A qualitative risk analysis which systematically evaluates tangible and intangible risks (Peltier 2005) in order to reduce these risks to a cost-effective level;
- Fan and Yu used BBN for risk reduction during the project management of software production (Fan and Yu 2004). This was based entirely on the experience of domain experts;
- Feng et al. created a risk analysis model that identified casual relationships within risk factors in order to model complexity and uncertainty of vulnerabilities. Their Security Risk Assessment Model used BBN to evaluate the most likely vulnerability (Feng, Wang, and Li 2014);
- Fenton and Neil have created a commercially available Bayesian analysis tool with a focus on the area of risk assessment and decision analysis (Fenton and Neil 2012).

The basis of many of the previous models is the determination of Capability, Opportunity and Intent and this basis (See Figure 5.1) is considered appropriate for the modelling of eavesdropping technology prediction.

Rare eavesdropping events are difficult to predict and prediction is further hindered due to

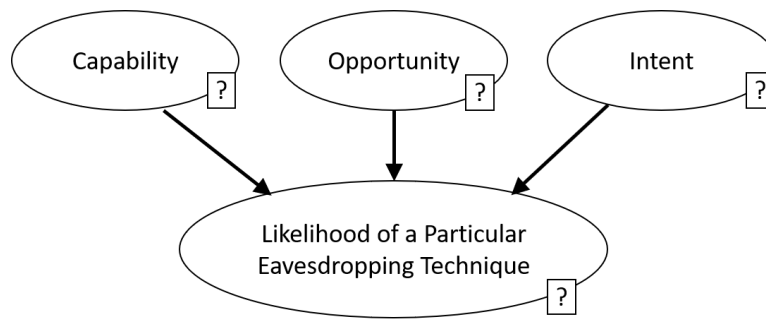


Figure 5.1: Capability, opportunity and intent nodes and arcs offer the potential for a Bayesian belief networks to highlight the likelihood of a particular eavesdropping technique being present.

insufficient information being available for modelling purposes. Reason (Reason 2016) describes an accident trajectory whereby a series of holes are required to line up in successive layers of defence. The events are rare as the holes rarely all align. Figure 5.2 illustrates the ‘accident trajectory’ when the ‘eyes’ in the Swiss cheese align and result in an accident. In this case, the metaphor of the holes in each of the layers represents an attacker’s Capabilities, Opportunities and Intentions to mount an electronic eavesdropping attack; whichever holes align, represents the particular target vulnerability and therefore the most appropriate eavesdropping technique to deploy. In some cases an attacker may have several holes that align. We can begin to reason the probability of a particular eavesdropping technique being deployed if we consider each of the layers individually.

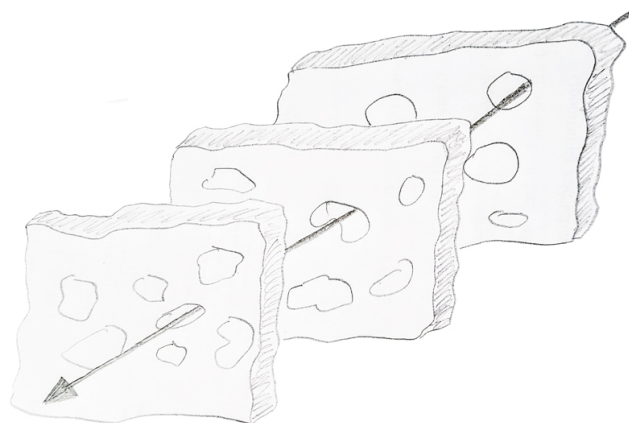


Figure 5.2: The Swiss Cheese alignment metaphor to illustrate the layers of capability, opportunity and intent and the ‘cheese eyes’ that must align in order for the rare eavesdropping event to materialise.

5.1.3 Bayesian Software Packages

Many commercial and free software packages are available for Bayesian analysis. This research requires a windows-based package with a graphical user interface to enable flexible and modular network experimentation. Of the many available, four packages were considered:

Package	Overview	Cost
BayesPy	Low-cost Python based but requires steep learning curve (See http://www.bayespy.org)	Free open-source initiative
AgenaRisk	Based on 30 years of research in computer science, AI, Bayesian probability, statistics and smart data (See www.agenarisk.com)	Subscription-based
Hugin	Flexible and user-friendly graphical user-interface and advanced HUGIN Decision Engine for application development (See www.hugin.com)	Subscription-based
BayesFusion GeNie	Graphical User Interface for BayesFusion SMILE Engine and allows for interactive model building and learning (See www.bayesfusion.com)	Free for academic use

Table 5.1: Four Bayesian software packages considered, with BayesFusion GeNie selected for this research.

BayesFusion GeNie was chosen for this research due to the availability of the academic licence and user-friendly graphical interface which facilitated network development.

5.2 Eavesdropping Technologies' Capability and Opportunity Requirements

In order to progress the Capability, Opportunity and Intent approach, it was necessary to establish whether technical eavesdropping techniques exhibit distinct capability and opportunity characteristics.

The following hypotheses will be tested:

1. An eavesdropping device's capability and opportunity characteristics are such that when plotted on a graph, the technique exhibits a distinctive *fingerprint* which may offer the potential for segmentation;
2. Expert judgement is capable of identifying the minimum capability and opportunity characteristics for each technical attack method presented to them.

5.2.1 Method

The following experiment was conducted utilising:

1. Twelve subject domain specialists with the knowledge required to classify a range of technical eavesdropping technologies;
2. The range of eavesdropping technologies identified within Figure 3.1 and Figure 3.2 in Chapter 3;
3. An x-y plot for each domain expert to record their subjective opinion for the position of each eavesdropping technique on the graph (see figure 5.3).

The plot in Figure 5.3 illustrates the graph provided to each expert. The x-axis provides a range of attackers' access opportunities from low to high. The y-axis provides a range of attackers' capabilities, from very low, such as those available within any domestic situation, to a very high capability, typical of those available from a well-resourced and funded government.

Following collation of the twelve expert opinions, the results were combined onto a graph for each eavesdropping technique. Each individual eavesdropping technique's graph contained three results:

- The domain experts' opinions of the capability and opportunity characteristics for each eavesdropping technique. Each expert's opinion is illustrated as a coloured dot;

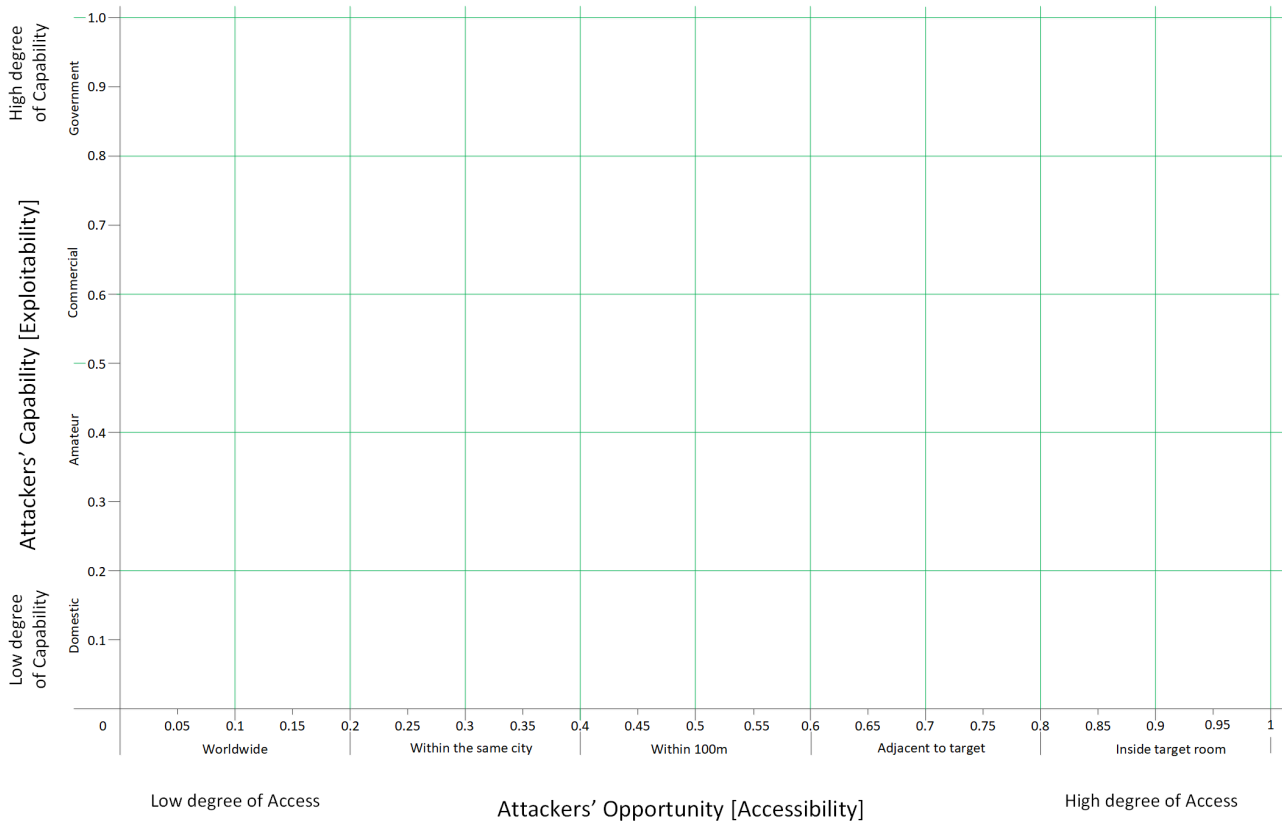


Figure 5.3: Expert elicitation template for determining eavesdropping techniques' capability and opportunity requirements.

- A weighted average centroid position, indicated as a triangle. The weighted average is applied in accordance with the domain experts' years of counter-eavesdropping experience. The higher the number of years of experience, the greater the weighting;
- Within the domain expert opinions, my own opinion is also recorded and indicated by a uniquely coloured dot.

5.2.2 Result

Eighty-nine eavesdropping techniques were plotted by the twelve domain experts. Figure 5.4 illustrates six of the eighty-nine plots. All results may be seen in the Appendix E.

Each graph comprises fourteen data points. The predominant round dots represent each of the expert's opinions. The triangle represents the weighted mean of all experts. The additional round dot represents my own personal opinion. The number in brackets indicates the technique

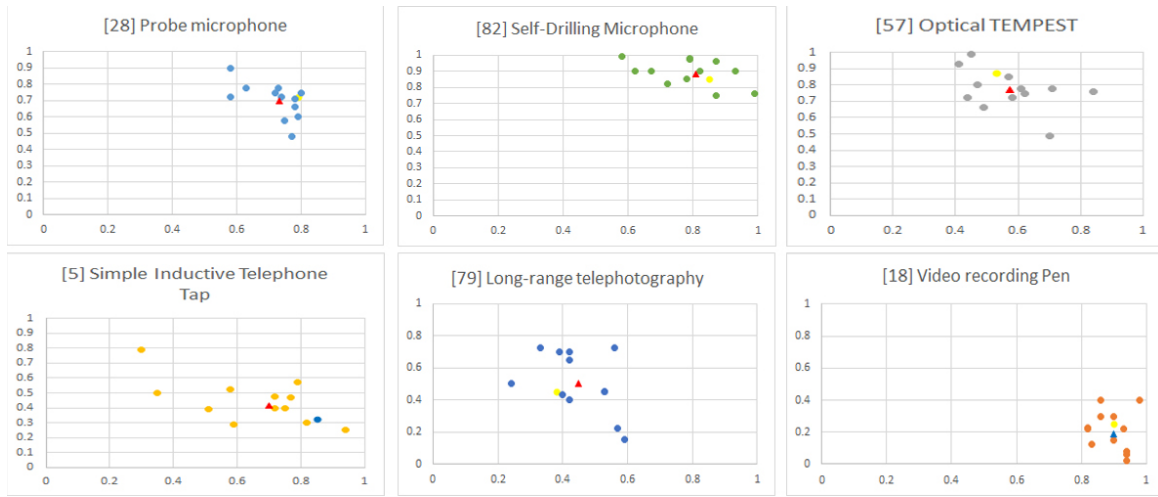


Figure 5.4: Six example results of eavesdropping techniques plotted for capability and opportunity.

number presented to the domain experts.

5.2.3 Discussion

Generally, the domain experts were in agreement with their opinions of the capability characteristics for each eavesdropping technique. It was noted that with the reviewed eavesdropping techniques, there were three broad groups of eavesdropping techniques:

- **Very expensive techniques** requiring considerable city-wide infrastructure available to a telecommunications provider or a government. The technique is capable of monitoring multiple targets (mass surveillance);
- **Very inexpensive techniques** widely available from the consumer market with very little skill required to mount or operate the technique. These techniques were generally focused on eavesdropping against a single target;
- **Technically complex techniques** that are not necessarily expensive but the technique required considerable expertise and know-how to mount and operate; potentially available to technical enthusiasts. These techniques were mostly against an individual or a small office or organisation.

The expert opinion for the opportunity characteristics produced less agreement. Later discus-

sions with the domain experts revealed that opportunity uncertainties were associated with the range of possibilities provided by a technique's egress method. Table 5.2 below illustrates egress methods and range variations.

Egress Method	The egress opportunity variability
Data network connection	From the end user terminal to the network boundary
Mobile telephone	From physical access to the handset to several metres away
Radio	From millimetres to kilometres from the target
Electromagnetic	Limited to close proximity within a few metres
Optical	Practically from a few metres to tens of metres
Telephone line	Anywhere between the telephone handset to the telephone exchange
Dedicated wiring	Practically from a few metres to tens of metres
Physical access	By definition - within touching distance of the target
Acoustic	Practically from a few metres to tens of metres

Table 5.2: The range values of egress methods

5.3 Bayesian Modelling of Eavesdropping Capability, Opportunity and Intent

The attackers ability to organise, coordinate and manage assets will determine their Capability and Opportunity for mounting eavesdropping attacks. While their Intent is somewhat different but critical in making a technical attack. Capability, Opportunity and Intent are considered individually in order to model each component of the predictive eavesdropping model.

5.3.1 Modelling Eavesdropping Capability

Grant's resource-based theory of competitive advantage (Grant 1991, 2016), although originally intended for business management, provides a basis for determining an attacker's eavesdropping capability. Grant's model considers tangible assets (financial and physical), intangible assets (technological, reputation and culture) and human resource assets (specialist skills and know how, communication and interactive abilities, motivation), all of which are important characteristics and suitable nodes for a Bayesian model.

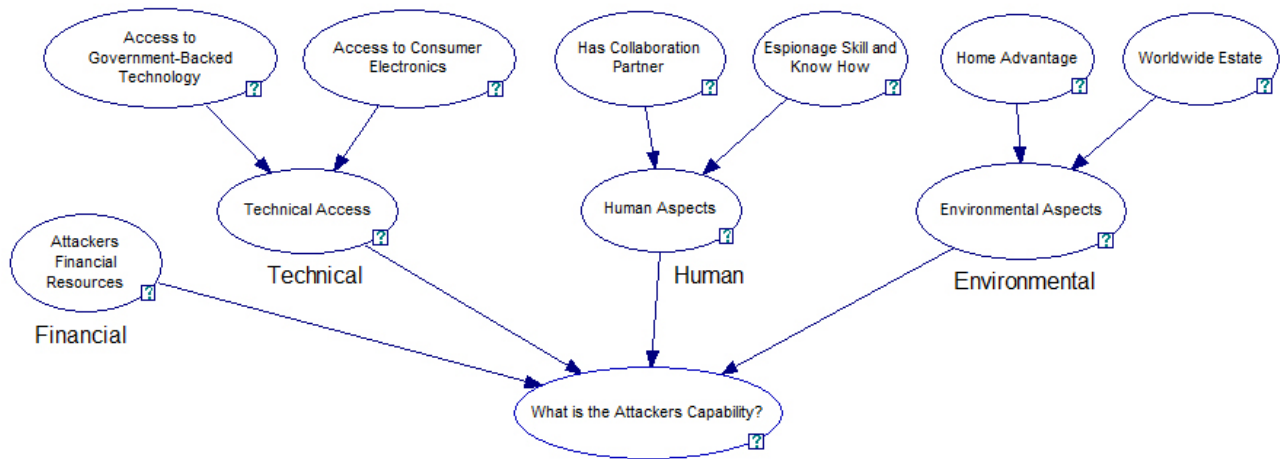


Figure 5.5: The tangible and intangible assets that contribute to an eavesdropping capability.

Node Probability Tables

The network was created with the following Node Probability Tables. The ranked nodes represent variables whose states are expressed alongside the node in the following table:

Node	Type	Value
Financial	Ranked	{High, Low, None}
Access to Government-Backed Technology	Ranked	{Formidable, Medium, Low}
Access to Consumer Electronics	Ranked	{Extensive, Some, None}
Technical Access	Ranked	{High, Medium, Low}
Has Collaboration Partner	Ranked	{Formidable, Minor, None}
Espionage Skill and Know How	Ranked	{Extensive, Amateur, No Skills}
Human Aspects	Ranked	{High, Medium, Low}
Home Advantage	Ranked	{Present, Absent}
Worldwide Estate	Ranked	{Present, Absent}
Environmental Aspects	Ranked	{Worldwide, Homebased, Not Applicable}
What is the Attacker's Capability?	Ranked	{Intel Service, Police Service, Domestic}
SIGINT Opportunity	Boolean	{Present, Absent}
IT Network Opportunity	Boolean	{Present, Absent}
Software Trojan Opportunity	Boolean	{Present, Absent}
Machine Compromise Opportunity	Boolean	{Present, Absent}
Laser Microphone Opportunity	Boolean	{Present, Absent}
WiFi Interception Opportunity	Boolean	{Present, Absent}
Radio Mic Opportunity	Boolean	{Present, Absent}
Photography Copy Stand Opportunity	Boolean	{Present, Absent}
Telephotography Opportunity	Boolean	{Present, Absent}
Wired Microphone Opportunity	Boolean	{Present, Absent}
Inductive Tap Opportunity	Boolean	{Present, Absent}
Telephone Landline Opportunity	Boolean	{Present, Absent}
GSM Audio Bug Opportunity	Boolean	{Present, Absent}
Consumer Video Opportunity	Boolean	{Present, Absent}
Digital Audio Recorder Opportunity	Boolean	{Present, Absent}
Attackers Access Opportunity	Ranked	{Vacant, Insider, Adjacent, City, Worldwide}
SIGINT Location	Boolean	{Present, Absent}
IT Network Location	Boolean	{Present, Absent}
Software Trojan Location	Boolean	{Present, Absent}

Machine Compromise Location	Boolean	{Present, Absent}
Laser Microphone Location	Boolean	{Present, Absent}
WiFi Interception Location	Boolean	{Present, Absent}
Radio Mic Location	Boolean	{Present, Absent}
Photography Copy Stand Location	Boolean	{Present, Absent}
Telephotography Location	Boolean	{Present, Absent}
Wired Microphone Location	Boolean	{Present, Absent}
Inductive Tap Location	Boolean	{Present, Absent}
Telephone Landline Location	Boolean	{Present, Absent}
GSM Audio Bug Location	Boolean	{Present, Absent}
Consumer Video Location	Boolean	{Present, Absent}
Digital Audio Recorder Location	Boolean	{Present, Absent}
Target Location Opportunity	Ranked	{Individual, Office, Residence, Transport, CityInfrastructure}
SIGINT Lifecycle	Boolean	{Present, Absent}
IT Network Lifecycle	Boolean	{Present, Absent}
Software Trojan Lifecycle	Boolean	{Present, Absent}
Machine Compromise Lifecycle	Boolean	{Present, Absent}
Laser Microphone Lifecycle	Boolean	{Present, Absent}
WiFi Interception Lifecycle	Boolean	{Present, Absent}
Radio Mic Location	Lifecycle	{Present, Absent}
Photography Copy Stand Lifecycle	Boolean	{Present, Absent}
Telephotography Location	Lifecycle	{Present, Absent}
Wired Microphone Location	Lifecycle	{Present, Absent}
Inductive Tap Lifecycle	Boolean	{Present, Absent}
Telephone Landline Lifecycle	Boolean	{Present, Absent}
GSM Audio Bug Lifecycle	Boolean	{Present, Absent}
Consumer Video Lifecycle	Boolean	{Present, Absent}
Digital Audio Recorder Lifecycle	Boolean	{Present, Absent}
Technology Lifecycle Opportunity	Ranked	{yr1901 to 2020}
SIGINT Attack	Boolean	{Present, Absent}
IT Network Attack	Boolean	{Present, Absent}
Software Trojan Attack	Boolean	{Present, Absent}
Machine Compromise Attack	Boolean	{Present, Absent}
Laser Microphone Attack	Boolean	{Present, Absent}
WiFi Interception Attack	Boolean	{Present, Absent}
Radio Mic Attack	Boolean	{Present, Absent}
Photography Copy Stand Attack	Boolean	{Present, Absent}
Telephotography Attack	Boolean	{Present, Absent}
Wired Microphone Attack	Boolean	{Present, Absent}
Inductive Tap Attack	Boolean	{Present, Absent}
Telephone Landline Attack	Boolean	{Present, Absent}
GSM Audio Bug Attack	Boolean	{Present, Absent}
Consumer Video Attack	Boolean	{Present, Absent}
Digital Audio Recorder Attack	Boolean	{Present, Absent}
Intent Trigger Event	Boolean	{Present, Absent}
Political Temperature	Ranked	{Immediate, Ongoing, Friendly}
Value of Intelligence	Ranked	{High, Low, Not Intelligence}
Past History	Ranked	{Significant, Minor, None}
Amplifier	Boolean	{Present, Absent}
Consequences if caught	Ranked	{Highly-Damaging, Some-Embarrassment, None}
Appetite for Risk	Ranked	{High, Medium, Low}
Countermeasures	Ranked	{Significant, Minor, None}
Plausible Deniability	Ranked	{Required, Some Requirement, None}
Restrainer	Ranked	{High, Medium, Low}
Intent Trigger Event	Boolean	{Present, Absent}

Table 5.3: Node probability table prior indicators and values.

Details for Capability Nodes:

- **Financial:** Financial resource availability assists greatly with the capability of the attacker. Governments generally have more financial resources at their disposal than commercial organisations, who in turn generally have more resources available than a single individual eavesdropper. Financial resources facilitate access to a range of technologies that may be either purchased or enable governments to manufacture their own bespoke technologies;
- **Technical - Access to Government Backed technology:** This capability enables the development of tailored access methods such as those available from the NSA ANT catalogue (United States National Security Agency (NSA) 2013) as well as large infrastructure projects for bulk surveillance programmes and on-line internet capabilities. The possibilities are endless if a government supports a technical goal and direction;
- **Technical - Access to consumer electronics:** provides a rich source of low-cost and easy-to-source eavesdropping equipment by anyone;
- **Technical - Has a collaboration partner:** which multiplies the resources available. Examples include the Five-Eyes collaboration partnership between the USA, UK, Australia, Canada and New Zealand. The sharing of resources and intelligence would provide a significant force multiplier;
- **Human - Espionage skill-set and know-how:** a core skill for successful eavesdropping implementation. Some countries have legendary skill-sets and know-how while others do not;
- **Physical - Home Advantage:** facilitates infrastructure capabilities such as Legal Intercept capabilities or even the ability to control all aspects of the environment to assist in mounting an eavesdropping attack;
- **Physical - Worldwide Estate:** Worldwide embassy access is one example that may create an opportunity for eavesdropping overseas such as SIGINT (D. Campbell 2015a; Spiegel Staff 2013) or the mid-20th century KGB eavesdropping incidents in the USA.

Remote Access or Close Access technical attacks are a combination of these capabilities.

5.3.2 Modelling Eavesdropping Opportunity

In order to create a proof of concept and to reduce the model complexity, a subset of fifteen of the most frequently used eavesdropping techniques (originating from Chapter 2) were modelled (See Figure 5.6). The particular techniques chosen required a range of attacker capabilities and opportunities (egress routes).

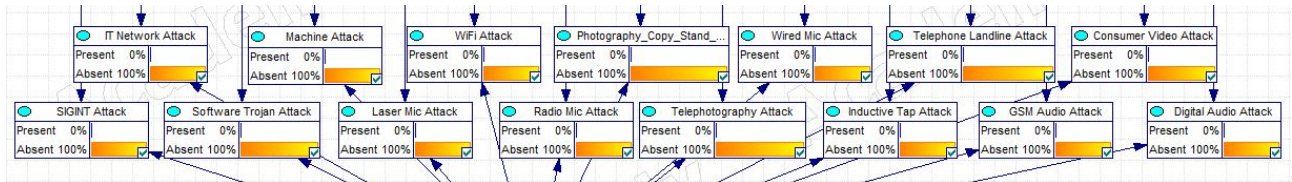


Figure 5.6: Fifteen of the most frequently used eavesdropping techniques selected to be modelled as a Bayesian Node. The probability of the technique being present will be a continuous probability range between present or absent.

These generic access opportunities were mapped against the following selected eavesdropping technologies:

No.	Eavesdropping Type	Examples
1	SIGINT	KGB against the USA, Martin Marinov TEMPEST
2	IT Network	Santander and Barclays Bank router incidents
3	Software Trojan	Pegasus software against mobile telephone
4	Machine Compromise	Against cypher machines in Moscow
5	LASER Microphone	BND in Germany, Theremin in Moscow
6	Wi-Fi Interception	GRU against OPCW in the Netherlands
7	Radio Microphone	Romanian Secret Service (Securitate) heel bug
8	Copy Photography	‘Cheka’ first secret police after the October Revolution
9	Telephotography	KGB against Khrushchev’s apartment in Moscow
10	Wired Microphone	Various iron curtain embassy attacks
11	Inductive Tap	Trench telephone intercepts on the front-line
12	Telephone Landline	‘Conflict’, ‘Sugar’ and ‘Lord’ taps in Vienna
13	GSM Audio	Various jealous partners, Ecuadorian Embassy in London
14	Consumer video	Ekateringburg brothel bugs against a diplomat
15	Digital Audio Recorder	Listening devices stitched into girl’s clothes

Table 5.4: The fifteen types of eavesdropping techniques modelled.

Further to Table 5.2 Access Opportunities are a key requirement that determine which eavesdropping technique may be used in a particular circumstance; the *How*, *Where* and *When* of an eavesdropping attack. In order to consider an attacker’s opportunity with regard to these fifteen technologies, three specific nodes have been considered:

- ***Attacker's Access Opportunities:*** For each eavesdropping technique, the probability that a technique will be deployed is considered in relation to the access available to the attacker. For example, an attacker with insider access has considerably more eavesdropping technique deployment opportunities available than a remote eavesdropper located thousands of miles away. The data for this node table is derived from the expert elicitation in Section 5.2;
- ***Target Location Opportunities:*** For each eavesdropping technique, five generic target locations were considered. The location of the target will dictate the potential for a particular technique to be used. For example, it is completely impractical for a LASER microphone or a wired microphone attack to be used against a moving transport system;
- ***Technology Life-cycle Opportunities:*** A primary requirement for this research is to understand the changing nature of eavesdropping technologies. The life cycle of each eavesdropping technique is fundamental to this model and research. For the fifteen eavesdropping techniques considered within this model (see Table 4.2), the probability of a technology being available within the twelve decades between 1900 to 2020 is considered. The data for this node table is derived from the expert elicitation in Section 4.

The probabilities of access, location and technology life-cycle ‘presence’ are concatenated to combine the likelihood of that particular eavesdropping technique being used with the context under consideration. The resultant modelling combinations for opportunity can be seen in Figure 5.7.

Technology life cycles within the model contribute a major component of this model. Constant incremental technological developments provide ever greater opportunities for technology to be used for eavesdropping purposes (such as those discussed earlier in Chapter 4 and the development of the mobile telephone and mobile telephone exploits in Table 4.8).

5.3.3 Modelling Eavesdropping Intent

The final component of the model is an attacker’s intent; this is by far the most difficult to predict.

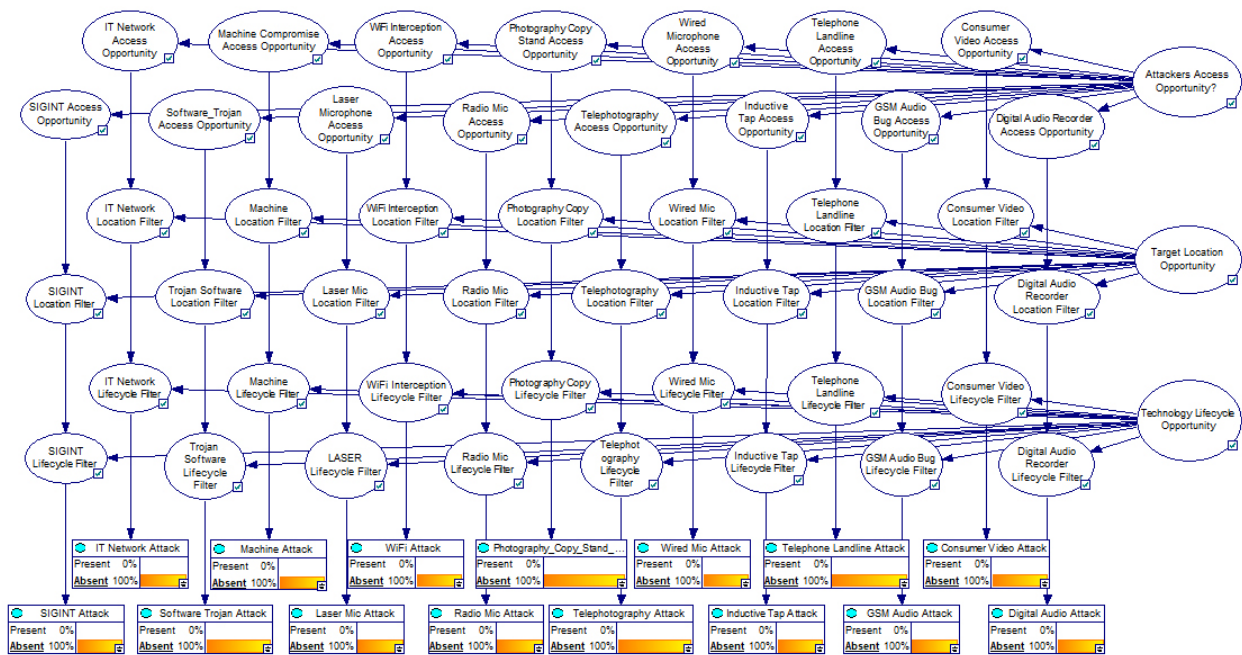


Figure 5.7: Access, location and life-cycle components that contribute to eavesdropping opportunities in the Bayesian model.

The creation of reliable intent prediction for such rare incidents would require an inordinately large number of considerations. The intent balance of *Amplifiers* and *Restrainers* provides the basis with which a model, with an eavesdropping focus, can be created.

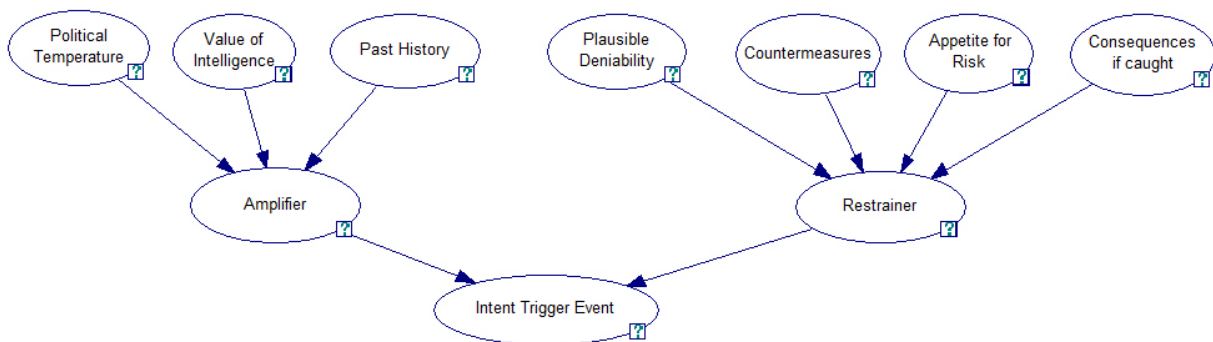


Figure 5.8: Nodes that contribute to ‘Amplifiers’ and ‘Restrainers’ for eavesdropping intent in the Bayesian model.

The nodes chosen to model intent are as follows:

- **Amplified:** For intent to be amplified, it must be that other sources of intelligence are unavailable. e.g. Human Intelligence (and all other) sources are absent and the only available source of the intelligence is by technical means;
- **Restrained:** For intent to be restrained, easier ways to obtain the information are available or that there are considerable obstacles to consider for a particular technical attack method, such as the requirement for the eavesdropping attack to remain covert;
- **Political Temperature:** Background of hostility, ongoing conflict or friendly relations may create urgency and demand;
- **Value of the Intelligence:** To an individual, organisation or government. If the value is high, the risk balance case changes;
- **Attacker's Past History:** The attacker's past eavesdropping track record. Some countries, e.g. the USA, UK or Russia have significant and undeniable history of mounting eavesdropping attacks;
- **Plausible Deniability:** Can someone else be plausibly implicated? If so, then this is a risk mitigation to consider;
- **Countermeasures:** Target awareness of the technical eavesdropping threat. Awareness levels change the potential for discovery;
- **Appetite for Risk:** Nationality or culture changes the risk appetite;
- **Consequences if caught:** Long- and short-term damage considerations are entirely context related. Being caught bugging by a jealous partner is likely to be handled very differently from being caught within an international diplomacy context;

'Consequences if caught' is an interesting node. There are instances where eavesdropping has been discovered but the victim has chosen to delay immediate rebuke and wait for some other political timing to reveal the incident for political gain. Examples include the Great Seal and the Russian trade delegation in London where both incidents were made public many years after initial discovery.

When considering past event data, the incident has occurred and therefore the intent is clearly 100% present. This aspect of intent in the modelling is therefore of greater interest when trying to predict the presence of an eavesdropping attack.

5.3.4 The Complete Bayesian Model for Eavesdropping Prediction

Figure 5.9 illustrates the combined Capability, Opportunity and Intent nodes and arcs for the fifteen eavesdropping technologies modelled.

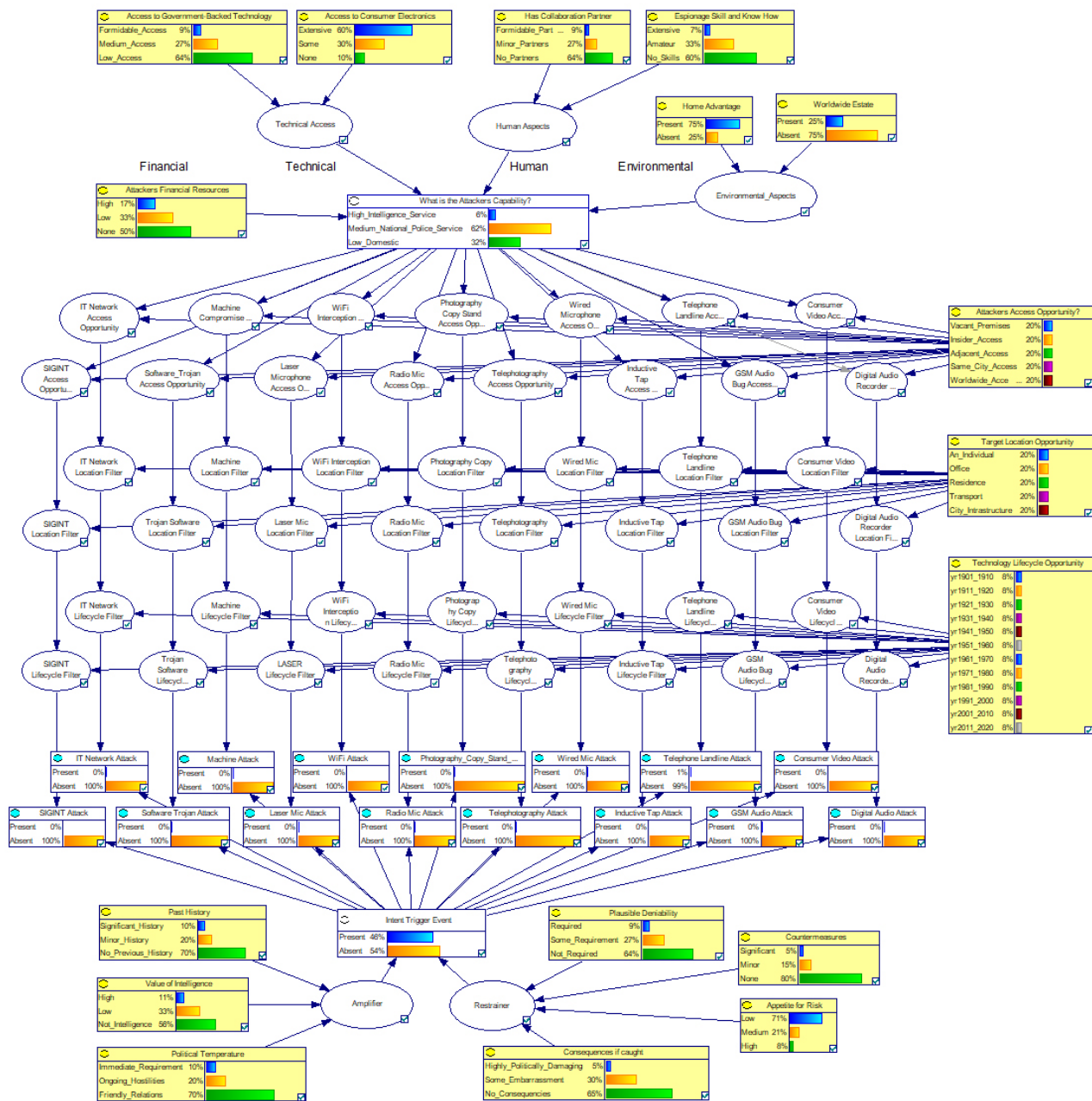


Figure 5.9: The complete eavesdropping Bayesian prediction model.

5.3.5 Validation

Model validation was achieved by comparing the model's performance against a sample of known past eavesdropping event data. The validation indicates the model's ability to predict the small subset of fifteen eavesdropping techniques against the techniques used within the historical data.

Validation methods for machine learning are not entirely appropriate for this Bayesian prediction model since the model predicts a series of probabilities for a range of eavesdropping techniques, whereby more than one technique may have been a viable answer.

The sample of known past events available does not provide all of the information required, which is precisely why Bayesian modelling was chosen as the prediction relies on the model's prior information for a particular node. Knowing who the attacker was in a given situation is a very powerful piece of information as it enables the model to consider the attacker's capability. This knowledge informs the probability towards a particular technique used, but the identity of the attacker is not always known, making prediction a challenge.

By using the confusion matrix details in Table 5.5 below, a methodology for validation is presented. The prediction will be considered valid if the actual test case technique is included within the model predictions.

A key consideration for this model is the inability to actually observe, by empirical means, the model's prediction accuracy when considering the future; observation is simply not possible and the accuracy of the model will not be known. Therefore, past event data alone will be used to point to the future.

	Predicted NO	Predicted YES
Actual NO	True Negative No eavesdropping event to predict	False Positive Model identifies a viable technique but not the actual technique used in the test cases
Actual YES	False Negative The model failed to predict the technique used	True Positive Model accurately predicts the eavesdropping technique

Table 5.5: Eavesdropping confusion matrix to establish the prediction performance of the Bayesian model.

Model Validation through Past-event Data

Event data collected in previous chapters provides access to a dataset of over 300 events (See Appendix B). For the model validation, 50 of these events were chosen across a time period from 1920 to 2018.

Test Case Number	Event Year	Digital Audio Recorder	GSM Audio Bug	Photography Copy-stand	Telephotography	Wired Microphone	Radio Microphone	Laser Microphone	Machine Attack	WiFi Interception	SIGINT Collection	IT Network Intrusion	Inductive Tel Tap	Software Trojan	Landline attack	Consumer Video	100% Correct	Technique predicted	Not predicted
1	1920	0%	0%	0%	0%	0%	0%	0%	0%	0%	11%	0%	1%	0%	8%	0%	1	0	0
2	1934	0%	0%	0%	0%	9%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0	1	0
3	1937	0%	0%	0%	0%	9%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0	1	0
4	1942	0%	0%	0%	0%	2%	0%	5%	0%	0%	8%	0%	1%	0%	6%	0%	0	1	0
5	1944	0%	0%	0%	0%	45%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1	0	0
6	1946	0%	0%	0%	0%	7%	4%	0%	0%	0%	0%	0%	0%	0%	11%	0%	0	1	0
7	1947	0%	0%	0%	0%	3%	0%	7%	0%	0%	10%	0%	1%	0%	8%	0%	0	1	0
8	1947	0%	0%	0%	0%	3%	0%	6%	0%	0%	9%	0%	1%	0%	7%	0%	0	1	0
9	1950	0%	0%	0%	0%	7%	3%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0	1	0
10	1953	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	1%	0%	9%	0%	0	1	0
11	1956	0%	0%	0%	0%	3%	0%	8%	0%	0%	9%	0%	1%	0%	8%	0%	1	0	0
12	1960	0%	0%	0%	0%	3%	0%	8%	0%	0%	0%	0%	1%	0%	9%	0%	0	1	0
13	1962	0%	0%	0%	7%	2%	0%	6%	0%	0%	0%	0%	1%	0%	6%	0%	0	1	0
14	1962	0%	0%	0%	7%	2%	0%	6%	0%	0%	0%	0%	1%	0%	6%	0%	1	0	0
15	1963	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	1%	0%	5%	0%	1	0	0
16	1964	0%	0%	0%	0%	5%	9%	0%	5%	0%	0%	0%	0%	0%	8%	0%	0	1	0
17	1965	0%	0%	0%	0%	4%	6%	0%	4%	0%	0%	0%	0%	0%	6%	0%	1	0	0
18	1967	0%	0%	0%	0%	4%	7%	0%	4%	0%	0%	0%	0%	0%	6%	0%	1	0	0
19	1969	0%	0%	0%	0%	4%	7%	0%	4%	0%	0%	0%	0%	0%	6%	0%	1	0	0
20	1971	0%	0%	8%	0%	17%	35%	0%	38%	0%	0%	0%	0%	0%	8%	0%	0	1	0
21	1971	0%	0%	0%	0%	4%	7%	0%	4%	0%	0%	0%	0%	0%	6%	0%	1	0	0
22	1972	0%	0%	0%	0%	2%	7%	0%	0%	0%	0%	0%	0%	0%	5%	0%	1	0	0
23	1974	0%	0%	0%	6%	2%	0%	6%	0%	0%	0%	0%	1%	0%	6%	0%	0	1	0
24	1974	0%	0%	8%	0%	17%	35%	0%	38%	0%	0%	0%	0%	0%	8%	0%	0	1	0
25	1976	0%	0%	0%	0%	2%	8%	0%	5%	0%	0%	0%	0%	0%	7%	0%	0	1	0
26	1981	0%	0%	0%	0%	5%	8%	0%	0%	0%	0%	0%	0%	0%	7%	0%	1	0	0
27	1983	0%	0%	9%	0%	14%	40%	0%	38%	0%	0%	6%	0%	0%	9%	0%	0	1	0
28	1984	0%	0%	0%	0%	5%	9%	0%	5%	0%	0%	0%	0%	0%	8%	0%	0	1	0
29	1984	0%	0%	0%	0%	5%	9%	0%	0%	0%	0%	0%	0%	0%	8%	0%	0	1	0
30	1987	0%	0%	0%	12%	10%	0%	5%	36%	0%	10%	5%	5%	0%	9%	0%	0	1	0
31	1990	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0	0	1
32	2004	1%	0%	0%	0%	0%	6%	0%	0%	0%	0%	6%	0%	0%	5%	0%	1	0	0
33	2006	1%	0%	0%	0%	0%	2%	0%	0%	0%	0%	2%	0%	0%	2%	0%	1	0	0
34	2012	0%	0%	0%	16%	0%	0%	0%	0%	24%	0%	16%	0%	4%	4%	0%	1	0	0
35	2013	1%	2%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%	2%	1%	1%	0	1	0
36	2013	1%	2%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	2%	2%	1%	1	0	0
37	2013	0%	0%	0%	0%	0%	0%	0%	0%	0%	45%	36%	0%	5%	8%	0%	1	0	0
38	2013	23%	20%	0%	0%	14%	15%	0%	0%	0%	0%	36%	0%	13%	9%	6%	0	1	0
39	2015	28%	31%	0%	0%	18%	0%	0%	0%	0%	0%	12%	0%	6%	4%	12%	0	1	0
40	2015	1%	1%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%	1%	0%	1%	0	1	0
41	2015	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	32%	0%	5%	7%	0%	1	0	0
42	2015	1%	2%	0%	0%	0%	4%	0%	0%	0%	0%	3%	0%	2%	2%	1%	1	0	0
43	2016	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	17%	0%	4%	5%	0%	1	0	0
44	2017	32%	36%	0%	0%	0%	21%	0%	0%	0%	0%	13%	0%	7%	4%	14%	0	1	0
45	2017	28%	31%	0%	0%	0%	18%	0%	0%	0%	0%	12%	0%	6%	4%	12%	1	0	0
46	2018	1%	2%	0%	0%	0%	2%	0%	0%	0%	0%	1%	0%	1%	1%	1%	1	0	0
47	2018	1%	2%	0%	0%	0%	3%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1	0	0
48	2018	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	3%	0%	0%	0%	1	0	0
49	2018	0%	0%	0%	16%	12%	0%	6%	0%	53%	12%	47%	2%	7%	11%	0%	1	0	0
50	2018	1%	0%	0%	0%	0%	2%	0%	0%	0%	0%	2%	0%	1%	1%	1%	0	1	0

Table 5.6: The Bayesian prediction of fifteen eavesdropping techniques against 50 past eavesdropping incidents.

Table 5.6 illustrates the fifty test cases, the year of the case and fifteen eavesdropping techniques. For each eavesdropping historical case, the eavesdropping technique is presented with

a percentage of probability that the technique was used in the test case under consideration.

The last three columns indicate whether the model accurately predicted the technique used or whether an alternative but viable technique was predicted. The final column indicates whether the mode failed to make a prediction.

Accuracy

The model's accuracy was considered: Accuracy is the ratio of correctly predicted eavesdropping techniques against the total number of test cases considered. In this case:

$$Accuracy = \frac{\text{Number of correct classifications (24)}}{\text{Total number of test cases (50)}} = 0.48$$

However, with this model, accuracy should be extended to include the correct prediction of viable techniques that may have been used in the cases considered. More than one eavesdropping technique could have been viable and dependent upon the target focus of the attacker.

$$Viable\ Technique\ Accuracy = \frac{\text{Number of potential techniques (49)}}{\text{Total number of test cases (50)}} = 0.98$$

If the number of techniques is extended in the model, the accuracy of the model is likely to change.

Precision, Recall and F1 Score

Precision states that: of all of them predicted by the model, how many techniques could have been used in the test cases.

$$Precision = \frac{\text{Number of true positives (24)}}{\text{True positives (24) + false positives (25)}} = 0.49$$

Recall states that: of all the accurate model predictions, how many of the accuracies were labelled? This is less useful for this model.

$$Recall = \frac{\text{Number of true positives (24)}}{\text{True positives (24) + false negatives (1)}} = 0.96$$

The F1 Score is the weighted average of both the Precision and Recall. Therefore, this score takes both false positives and false negatives into account.

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = 0.65$$

The most useful validation comparison for this model is the accuracy of that defined within the confusion matrix; the True Positives, False Positives and the False Negatives.

5.3.6 Future Work Identified

There are three areas where the model could be improved:

1. **Additional eavesdropping techniques:** The subset of techniques chosen represents less than 20% of the eavesdropping techniques identified in previous chapters. Additional techniques will increase the size and complexity of the model but will enable the broadest possible consideration of vulnerabilities;
2. **The addition of egress routes:** With the details of a particular scenario and period of time, it is possible to determine the range of available egress routes which will enable the creation of prior probabilities of particular eavesdropping techniques being present. Egress routes have been identified in Table 5.2 and form the basis of the additional modelling required. Figure 5.10 includes the most likely egress routes. Appendix F provides details of which eavesdropping techniques are associated with a particular egress route.

Looking to the future, it is important to consider new techniques that have yet to be

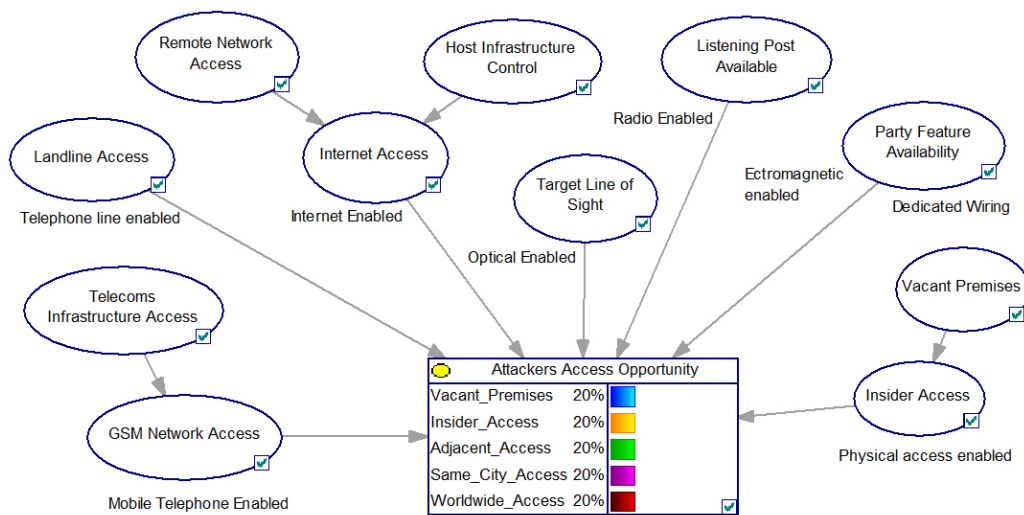


Figure 5.10: When egress routes are known, the ability to update Bayesian prior information is possible, increasing the prediction ability for known eavesdropping techniques.

deployed. Even unidentified eavesdropping techniques will require an egress route at some point within the spectrum. Figure 5.11 illustrates the potential to increase the egress route considerations.

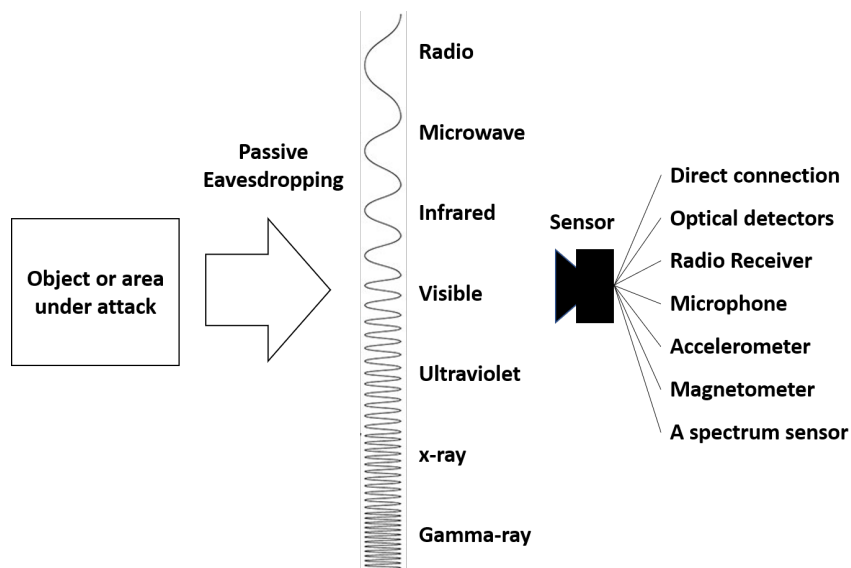


Figure 5.11: When egress routes are not known, the ability to update Bayesian prior information may be possible, by considering the likelihood of which portion of the spectrum may be used in a passive situation given a particular scenario.

3. **The addition of Active and Passive techniques consideration:** Figure 5.12 includes further consideration and builds on the previous broadening of the egress spectrum with the addition of active techniques. Within the techniques identified there are only

a handful of active methods included such as the radio illumination technique and the LASER eavesdropping technique which illuminates a target with an invisible light source. The returned acoustic vibrations would not do so without the optical illumination. The Wi-Fi acoustic vibration technique is similar in technique too, but illuminates the source with a radio frequency. If we consider the whole spectrum range linked to the known capability of an attacker, we may be able to extrapolate new previously unknown or unconsidered techniques.

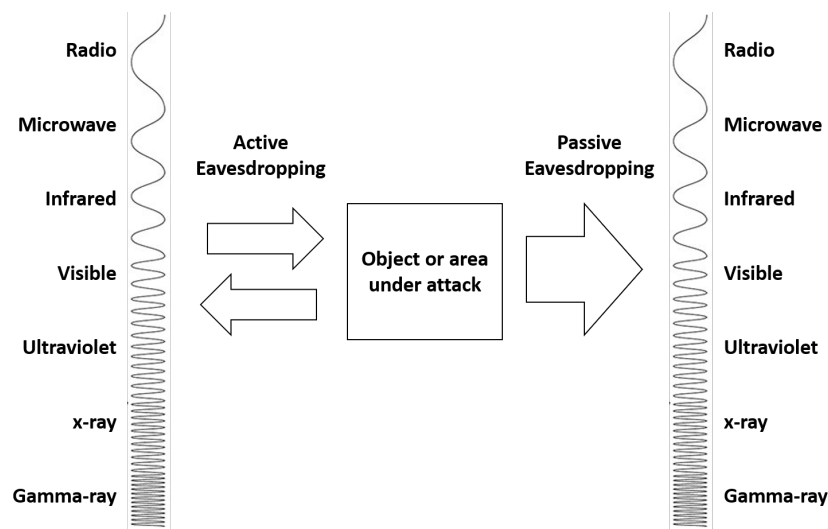


Figure 5.12: When egress routes are not known, the ability to update Bayesian prior information may be possible, by considering the likelihood of which portion of the spectrum may be used in an active situation given a particular scenario.

5.4 Chapter Discussion

This chapter set out to determine whether it was possible to predict the type of eavesdropping technology that might be deployed given a particular scenario. For the first time this model presents a novel methodology through the modelling of Capability, Opportunity and Intent, in order to predict the probability of a range of eavesdropping technologies that may be deployed in a given scenario.

There are two distinct uses of the model which highlight the importance and need for scenario and environment information:

- **To Test** the model against historical events when all of the historic environmental information may not be known and;
- **To Predict** eavesdropping attacks when situational knowledge is known.

It has been shown possible to use the known historical eavesdropping event information to compare the model's predicted probabilities. An important consideration with reviewing historical events is the extent to which information is simply not known. In many cases, the historical event details are minimal and incomplete and the model was required to rely on the prior probabilities. For example: not knowing the attacker's access available at the time of the event makes prediction very difficult, as the level of access is critical in determining the eavesdropping technique deployed.

Also, suppose we consider the Soviets who took advantage of Western embassy evacuations at the start of the Second World War. The model predicted that wired microphones would be present due to the level of access available. The model also provided the probability that the telephone lines were intercepted and monitored too, but we are unable to verify this probability as this information is unavailable. To validate this prediction would require the cooperation of the attacker or indeed attackers, if the target was of interest to more than one interested party.

The model's ability to predict an attacker's capability depends entirely on knowing who the attacker is in order to state their capability. This creates prediction difficulties if the attacker is not known. If however the technical attack technique is known, the model can be used in a back propagation mode. Setting the particular technique's probability value to be 100% 'present' cascades through the model creating node values that 'reverse engineer' all capability, opportunity and intent probabilities. Of course, when looking back at past events, it is not necessary to consider the attacker's intent: the eavesdropping event has occurred and the intent therefore is certain.

The model provides the ability for professional risk assessors to use evidenced-based risk assessment. With the technical risk assessor armed with information for each real-life scenario, the model is capable of augmenting the expert risk assessor's ability to contribute to risk assessment.

The Bayesian Inferencing model's prediction ability may be further improved through the use of expert updates. The ability to update prior information, when new information becomes available, is a powerful way of continuously augmenting expert opinion and contributing to enhanced prediction.

Risks from particular eavesdropping techniques may be mitigated with appropriate countermeasures when the attackers' capability and opportunity requirements are defined. For example: understanding the technical eavesdropping opportunities of particular egress routes enables mitigation measures. High-threat embassies in many cities worldwide illustrate bricked-up windows that deny all optical forms of technical vulnerability listed in Table F.

The selection of nodes that contribute to capability and opportunity is subject to further scrutiny as other combinations of available data may enhance the model's performance.

Chapter 6

The Changing Nature of Intrusive Surveillance and Summary

6.1 Chapter Overview

The previous chapters focused on past eavesdropping incidents, the technologies that enabled these incidents, the way in which these technologies have life cycles of innovation and whether it is possible to predict eavesdropping incidents.

In this chapter:

1. A macro environmental overview of eavesdropping is considered;
2. Emergent technologies and their impact to eavesdropping techniques are considered;
3. Final thoughts on the thesis are offered.

6.2 Macro-Environmental Factors

In order to provide a wider strategic analysis of eavesdropping in the year 2020 the following overview of macro-environmental factors affecting eavesdropping are considered:

6.2.1 Political Factors

The need for intelligence: The UK's Secret Intelligence Service states its mission publicly *'Our mission is to provide Her Majesty's Government with a global covert capability. We collect secret intelligence and mount operations overseas to prevent and detect serious crime, and promote and defend the national security and economic wellbeing of the United Kingdom... to help counter the increasing number of threats to the UK... to protect the country, its people and interests'* (SIS 2019).

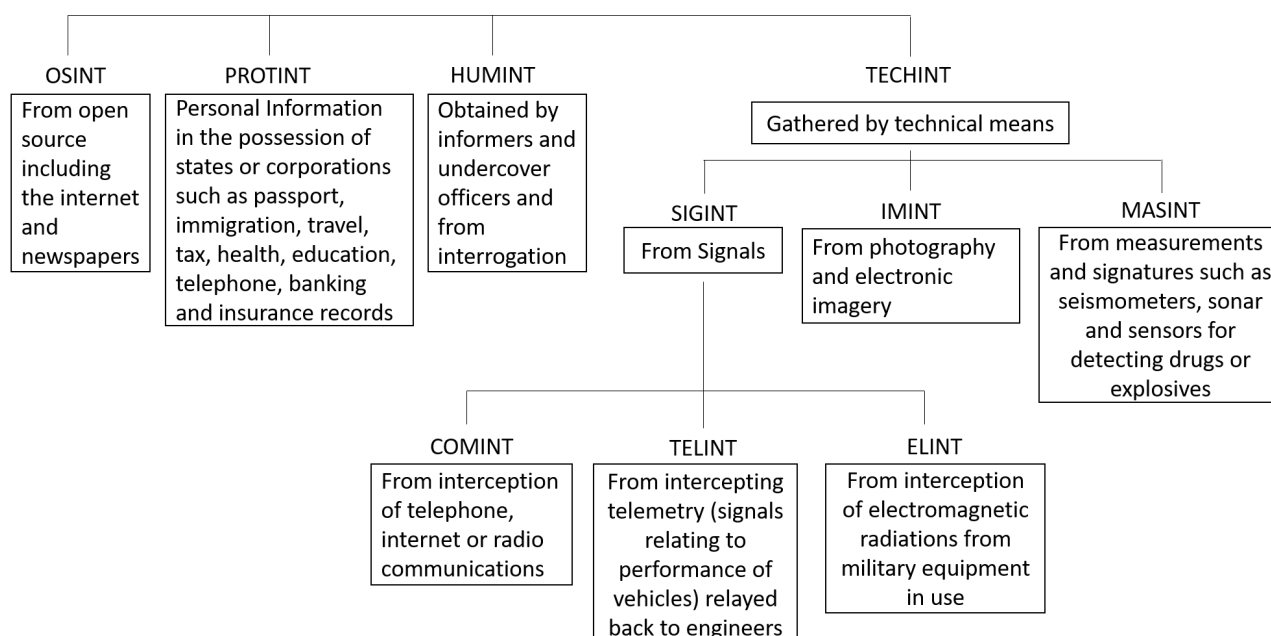


Figure 6.1: The sources of intelligence. Credit (Gill and Phythian 2013).

There will likely always be a requirement for intelligence; technical sources are one source of information and other sources exist too such as those illustrated by Gill and Phythian (Gill and Phythian 2013) in Figure 6.1. Technical intelligence (TECHINT) will always be expensive to develop and operate and is constantly becoming out of date. TECHINT is also unable to

provide important context. However, it will provide unbiased raw output with less of a risk to HUMINT sources.

The requirement for TECHINT will likely never diminish; it is just a question of the balance of sources of TECHINT, and for what purpose.

With the advent of computing and mobile telephone intercepts, it could be suggested that audio eavesdropping is no longer required. I propose that audio intelligence will always be required as it contributes a unique dimension to video, data and metadata in particular contexts. Consider the case of the Iranian Embassy siege in London in 1980 2.3.17, or the devices found in the Sinn Féin' car (BBC 2004). The first example demanded immediate situational intelligence and a microphone down a chimney provided a very rapid result. While the bugging of the car captured conversations and opinions that might not ever have been spoken on a telephone call. The immediacy of audio intelligence during a crisis or negotiations will always be highly valued. Furthermore, with the increased use of effective encryption on smartphones, interception of the pre-encrypted speech may again become more prevalent.

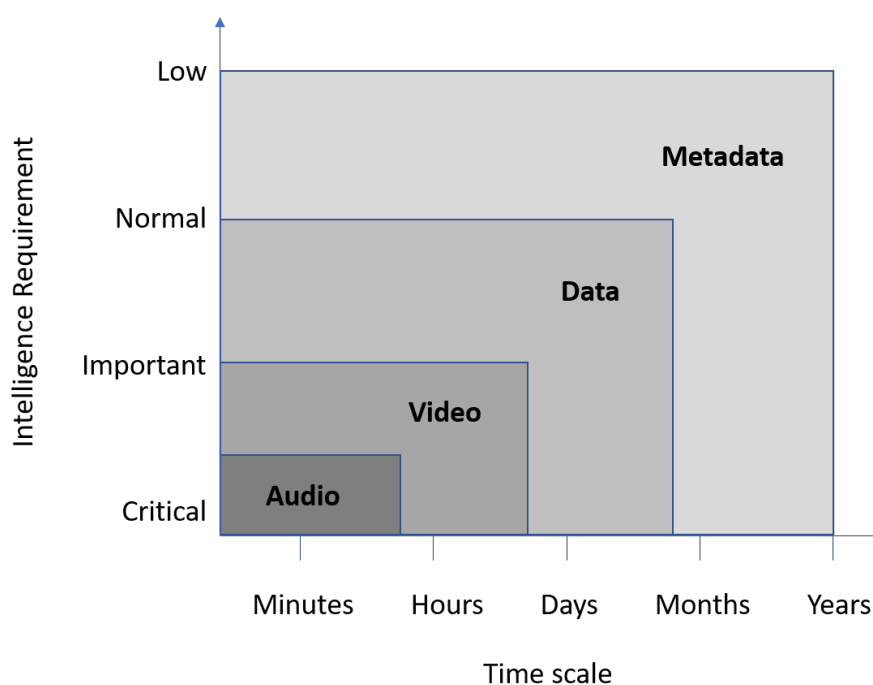


Figure 6.2: The urgency of requirement: Audio's immediacy during a crisis or negotiations will always be highly valued.

6.2.2 Economic Factors

Inflation, interest rates, unemployment rates, monetary or fiscal policies are all economic factors thought to have a very low impact to eavesdropping. However, some aspects of economics do affect the industry:

Fiscal policy: If a government wishes to pursue economic advantage by utilising theft of other countries' intellectual property, it may do so by the funding of appropriate resources with a remit to obtain or steal assets that would contribute to the country's growth. This is more likely to be by cyber intrusion rather than an intrusive surveillance incident.

Disposable income of buyers: There is anecdotal evidence that suggests that most eavesdropping items purchased from internet sites are not actually destined to be used, but purchased to satisfy the idle curiosity of the technically-minded or the curious hobbyists.

Credit accessibility: This factor is likely to have a low impact to eavesdropping. Low-cost internet purchases are of low value and will not require credit arrangements. High-cost items are likely to be purchased or manufactured by governments or very large organisations who will not be subject to credit restrictions, particularly if the eavesdropping equipment is used for national security purposes.

The foreign exchange rate: This factor will impact the cost of purchase of foreign made surveillance technologies. If purchased by governments, the impact will be negligible. If the cost of labour in a country is low due to foreign exchange rates, the low-cost of components will result in the low-cost of eavesdropping equipment. Conversely, should the rates increase, eavesdropping equipment may cease to become an impulse buy available to those with a disposable income.

Cost of telecommunications utilities: The cost of broadband provision within a country will impact the consequential availability of domestic Wi-Fi; the greater the number of broadband connections, the greater the number of Wi-Fi access points and the endpoints communicating with the Wi-Fi links. Low-cost broadband with permanent access to the internet will increase the ability for information technology attacks.

Changes to mobile phone services is also an economic factor: the increase in smartphones has increased mobile data usage. This has led to competition between service providers. Monthly low-cost SIM only contracts often provide unlimited voice minutes and text messaging, enabling the increased use of GSM audio bugs. Increased demand for mobile data usage has increased the GSM network as an egress route.

Internet Shopping and the rise in commoditised eavesdropping: The availability of eavesdropping equipment for audio-visual recording or live transmission purposes, available via online retailers is very high in the developed world. The cost of this equipment too is very low. While the price may be low, the capability of the equipment is high. The length of recording time available due to memory and battery capacity, together with miniaturisation has led to this technology being used imaginatively such as being stitched into clothing; a trait worthy of security services and stories of bugs being sown into coats when left at the theatre during the Cold War. Commoditised eavesdropping will continue to rise in line with in-country internet shopping availability.

6.2.3 Sociological Factors

Innovative technological platforms: This factor has impacted eavesdropping opportunities greater than any other factor and the question of privacy with social media is now at the forefront of people's minds. A data network connection at very low-cost and with a very high bandwidth is likely to be available almost anywhere; indeed we complain if it is not.

The convergence of voice, data and camera technologies built into a mobile smartphone has created social media platforms for a myriad of purposes (Johnson 2017). The regulation of social media sites and the user's inability to assure where and how their personal data is stored has led to users giving away information about themselves, far in excess of that gleaned from the post-second world war microphone eavesdropping attacks. Users are provided social media access for free not appreciating that the price they pay is high and their personal data has value and is exploited by commercial and government organisations alike. Facebook, created in 2004, has 2.27 billion monthly active users.



Figure 6.3: An example of the large number of social media applications available in 2018 (Solis 2019).

An example of the large number of social media sites is illustrated in Figure 6.3.

The cloud-based operating system ‘Domo’ has produced its seventh annual ‘Data Never Sleeps’ Infographic which examines what happens online in a single minute (Domo Inc. 2019). Domo informs us that as of July 2019, the internet reaches 56.1% of the world’s population (4.39 billion people) and that, because of ‘apps’, the number of emails sent per minute are reducing. The 2019 average of 188 million is down 8% from 2014. The way we are communicating is changing. Eavesdropping will ‘follow the asset’. The only difficulty will be to determine the asset to follow for each person or organisation of interest.

According to Ofcom (OFCOM 2018) a decade of change has occurred in the communications sector in the UK. In 2012 39% of adults owned a smartphone and by 2018 this rose to 78%

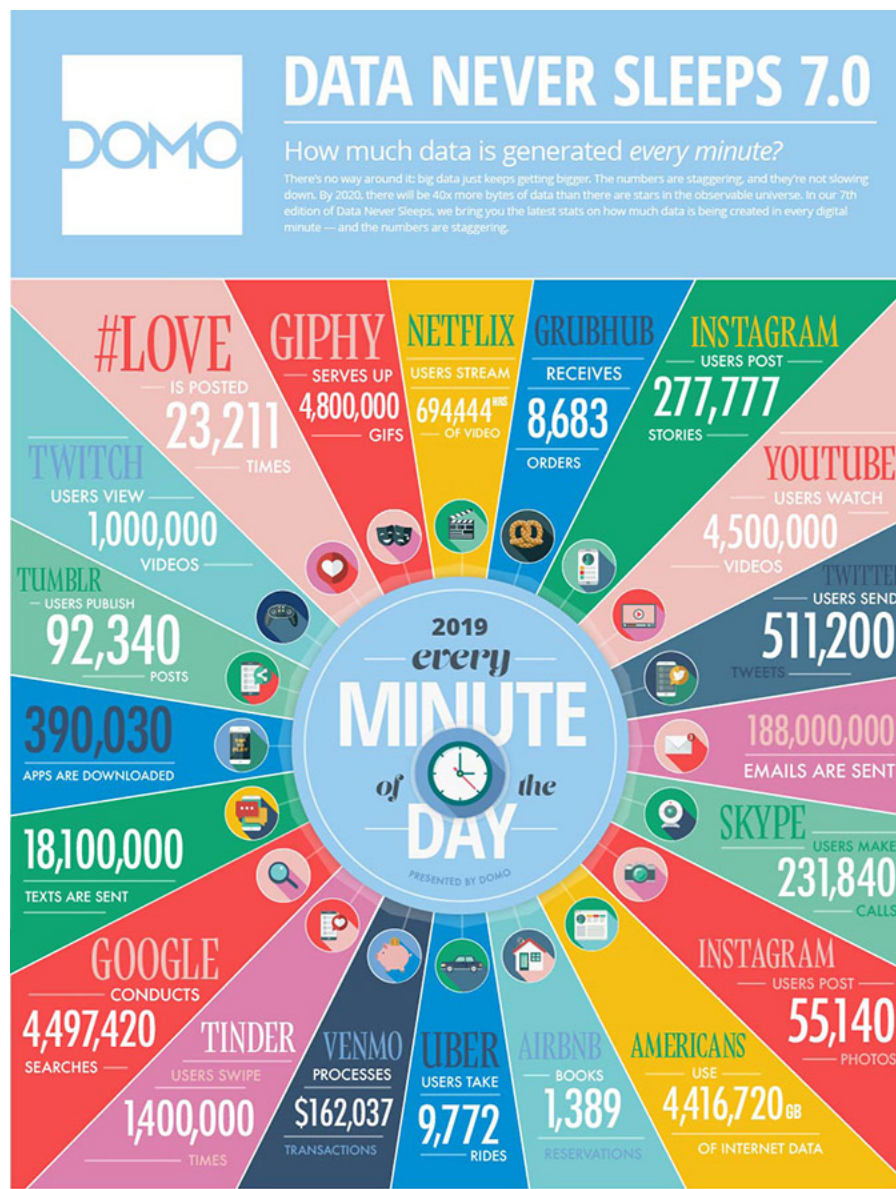


Figure 6.4: Data never sleeps: What is happening on the internet in a single minute. Reproduced with permission from (Domo Inc. 2019).

as well as becoming the most popular internet-connected device. The popularity of the fixed desktop computer, with it the requirement to be tethered to a location, is declining. In 2008 69% of people in the UK had a desktop PC in their home but by 2018 this had fallen to 28%. Furthermore, desktops were overtaken in popularity by laptops in 2011, and, in turn, laptops were overtaken by tablets in 2014. Although the popularity of tablets has stabilised over the last three years, smartphones have continued to rise.

In the UK we are a nation permanently connected to the internet too. The number of copper landline broadband connections was overtaken by fibre connections in 2017 (OFCOM 2018,

pp.12). The implication is that households are using mobile devices at home connected via Wi-Fi routers. The eavesdropping potential against an individual increases but is dependent upon an eavesdropper's ability to be within the range of the Wi-Fi signal.

Das et al. (Das, Borisov, and Caesar 2014) listed concerns regarding the ability to acoustically eavesdrop on internet-connected items. In February 2015 reports emerged that Samsung's internet-connected and voice-activated Smart TVs had the potential to capture customers' conversations (Goldman 2015; Samsung 2015). Despite this concern and a great deal of media coverage, in 2018 Smart speakers are present in 13% of UK homes. Although growth of these devices may yet be limited due to consumers beginning to realise the implications to their privacy (Price 2015).

Cultural implications: It is interesting to note that the overwhelming majority of past eavesdropping events relate to incidents with the USA, UK or Russia. Clearly, these past events are linked to the Cold War. It is interesting to note the emergent events that are now occurring from the indigenous people of African, India and South America. Events from China remain rare; a question arises therefore with the bias of event reporting and the use of the English language to capture these events. Events do occur within these continents suggesting that culturally, technological eavesdropping is not at odds with these people's ideas, customs or social behaviour.

Cultural dimension of uncertainty avoidance: Consideration was given to whether cultures with the greatest wish to avoid uncertainty may be more prone to aggressive eavesdropping activity. However, Geert Hofstede's cultural dimension of uncertainty avoidance evidence does not support this theory (Hofstede 1984, 2019).

6.2.4 Technological Factors

Emergent Intrusive Surveillance Technologies: Intrusive surveillance is heavily reliant on technology; and it is far from difficult to predict that surveillance technology will continue to evolve. The difficulties arise trying to predict future technology trends and this occupies the minds of governments and businesses worldwide.

The novel predictive model described in the previous chapter has been created to assist with prediction of eavesdropping technologies and with further development will highlight known eavesdropping techniques. Predicting unknown techniques is a challenge but even unknown techniques require an egress route. Again, the model is able to assist with the prediction of egress route possibilities.

The UK Centre for the Protection of National Infrastructure (CPNI) monitors technology developments that may impact the security of Critical National Infrastructure. CPNI commissioned two reports from industry which provide a forecast of twenty-eight technologies over the next three, five and ten-year time period (Dentons 2018; Qinetiq 2015). The UK Ministry of Defence have a continuous programme of trend research; the sixth version of their ‘Global Strategic Trends’ (Ministry of Defence 2018) study extends to 2050 and identifies 16 focus areas with the potential for profound change to humanity together with 40 strategic implications that will require attention.

Commercial and academic organisations produce trend analysis too. For the year 2019, ten breakthrough technologies are suggested by MIT (MIT Technology Review 2019) and Gartner (Gartner 2019) and six from Harvard Business Review (Salamone 2019). The Webbmedia Group Digital Strategy Trend report for 2016 (Webb 2016) suggests that eighty-one trends have been identified across a group of twelve themes, identified in order to help organisations make informed decisions. In another online resource Pearce from DIY Genius (K. Pearce 2013) considers thirty-five trends across seven themes for technology trends that will change our future.

Some technologies form the foundation for others to evolve. From the sources of trend information reviewed further work is required to understand which are the fundamental trends or the building blocks that will impact intrusive surveillance.

Advances linked to *Mesh Devices* or the *Internet of Things* are likely to aid egress. Once egressed the power of *Big Data* and *Advanced Analytics* of *Online Social Networking*, possibly aided by *Quantum Computing* may provide intrusive surveillance beyond imagination.

Moscella states that ‘Each major phase of information technology industry progress has been led by a new generation of firms’ (Moschella 2015, p.3). This makes the spotting of key progress changes a challenge. Moscella also considered the technology adoption time period between becoming available and being adopted by 50% of US homes. The research suggests that although the perception is for an ever-greater pace of technology change, this is not actually the case. Some technologies such as electricity or the telephone required considerable resources and the installation of a physical network in order to reach the consumer; Facebook required no such resources with the network already in place.

Rate of technological advance and obsolescence: In addition to Figure 6.5 above, Figure 4.15 illustrates that as each new mobile telephone advancement in technology is introduced, a vulnerability is discovered that is eventually, and often quickly, exploited for eavesdropping purposes.

Battery technology: The evolution of battery energy density and cost has revolutionised the smartphone industry, powering ever larger screens and software applications. This evolution has resulting in the growth of smartphones being used for eavesdropping purposes. The lithium-ion battery technology in smartphones is approaching its theoretical limit. However Berdichevsky (Gu et al. 2016) reports the new material Sila Nano technologies is to be available to manufacturers which could see a further increase of energy density by 20%.

Further advances in energy storage through the use of sodium, aluminium and zinc-based batteries has the potential to make a mini-grid feasible (Ministry of Defence 2018, pp.44) that could power very long-term remote collection equipment.

Graphene nanocoating could help improve battery efficiency together with flexible batteries spun from fibres and increases the likelihood that eavesdropping systems with storage capacity could become part of everyday items such as smart clothing or e-textiles. The ability to know whether a person within a secure situation is recording becomes increasingly difficult.

Underlying Technological Trends: Plotting the eavesdropping techniques' deployment capability requirements derived in Chapter 5.2 against the year of the technology's introduction in Chapter 4.3 highlights two observable trends: firstly that the capability requirement required for mounting an eavesdropping attack has reduced since the 1960s and secondly, the number of eavesdropping techniques also continues to increase (See Figures 6.5 and 6.7).

Figure 6.5 encapsulates the changing nature of eavesdropping in a single diagram (with Figure 6.7 further illustrating this point). There continues to be new methods of eavesdropping created for all capabilities.

Convergence: The convergence of technologies within a smartphone has particularly impacted and contributed to the decline of the electronic camera and electronic MP3 players. From an eavesdropping perspective, the built-in microphone, camera, battery and radio transmitter combine to create a natural eavesdropping system. In addition, the use of accelerometer sensors built into smartphones adds additional eavesdropping potential for acoustic or finger printing of adjacent keyboard typing should the phone be placed on the same surface.

Miniaturisation: This continues to make component detection within apparatus difficult. With multilayer printed circuit board in use, spotting additional trojan circuitry becomes increasingly impossible. Miniaturisation also creates the possibility of ever-greater functionality within smaller densities.

Memory capacity: Solid state memory continues to drive ever higher memory densities. With NAND non-volatile flash memory currently transitioning from planar to three-dimensional structures with multiple layers of flash memory cells, the evolution of ever higher memory density continues (Coughlin 2018).

This density increase, together with memory speed and reduced cost has enabled the develop-

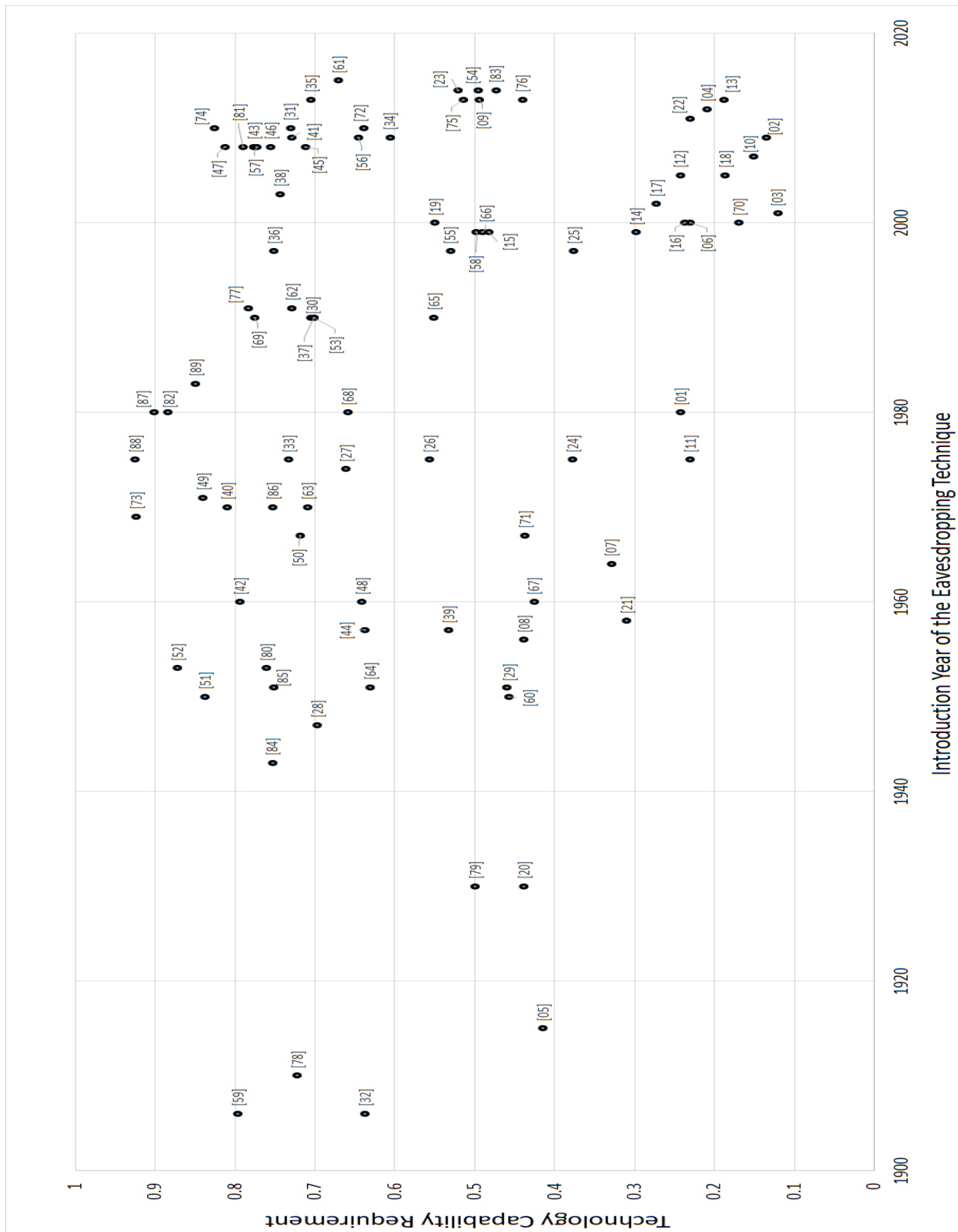
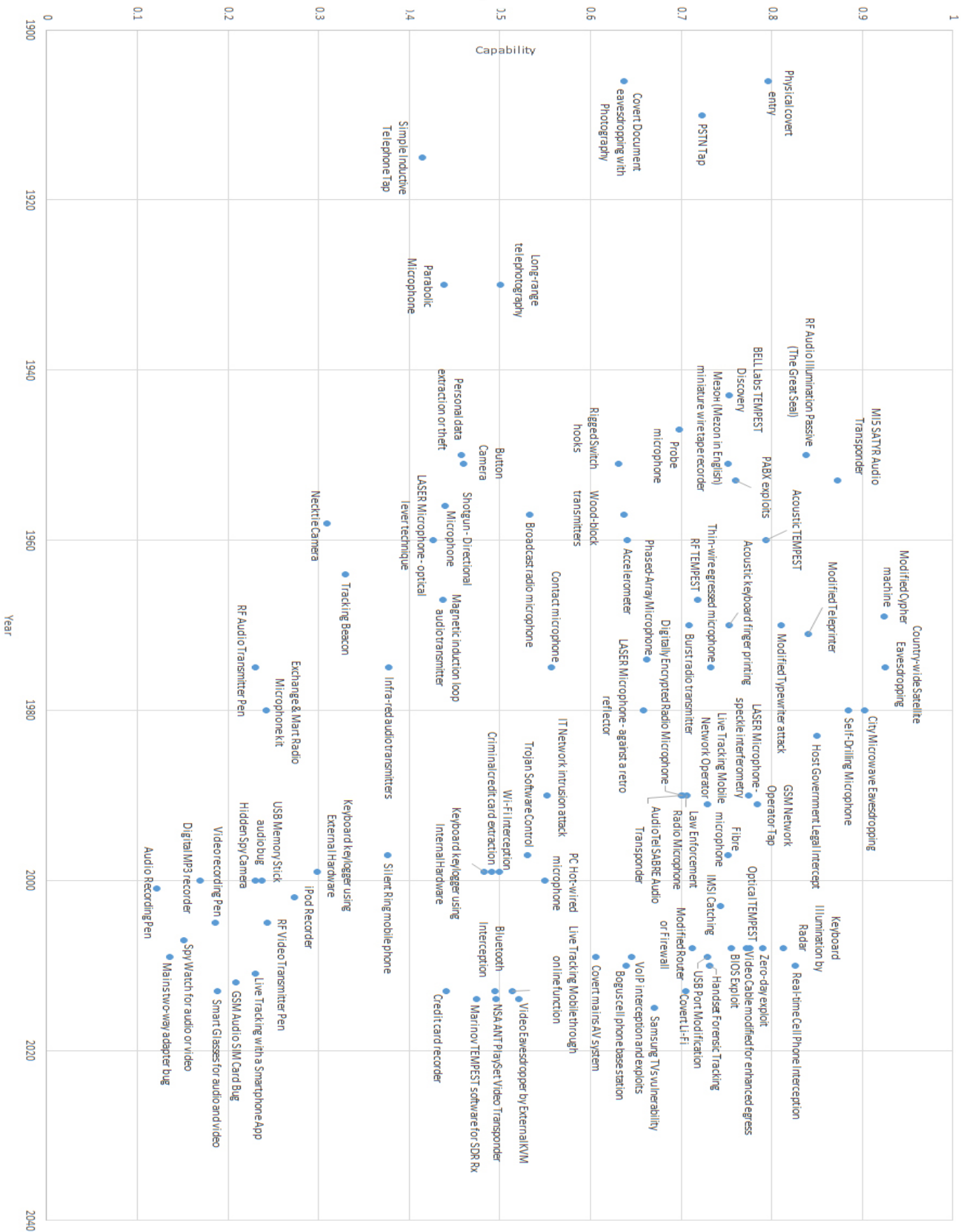


Figure 6.5: Eavesdropping techniques deployment capability requirements plotted against the year of the eavesdropping techniques introduction. The numbers identify the technique listed in Appendix E.



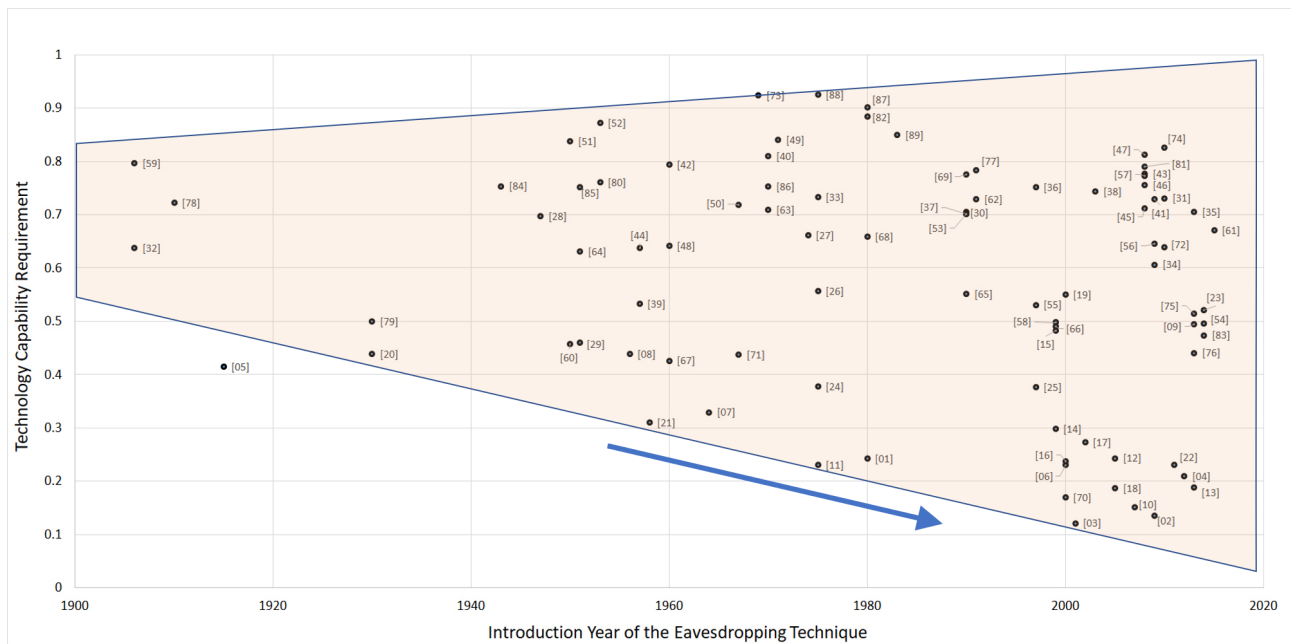


Figure 6.7: Eavesdropping techniques deployment capability requirements plotted against the year of the eavesdropping techniques introduction. The trend highlighted in pink is that technology innovation is driving the capability requirement down and the range of eavesdropping equipment available continues to increase. The numbers identify the technique listed in Appendix E.

ment of the 4K picture resolution that uses 8.3 million pixels to produce ultra-high audio-visual quality eavesdropping. High memory capacity also creates the possibility of recording sensors for considerable periods of time. Due to the higher capacities, eavesdropping systems may be deployed for greater periods of time before retrieval is necessary.

Internet growth: Section 2.48 highlights the incredible growth of the internet. Currently, in 2019, half of the world's population has access to the internet (Oxford Internet Institute 2019); a significant factor in the growth of eavesdropping egress over the internet.

It is interesting to note that the wealthiest countries are also the most open with their government's data ("Oxford Internet Institute" 2019). In research of countries' openness, 94 countries based on 1410 datasets concerning 15 different topics such as government spending, air quality and land ownership are recorded. With an openness of just 1% it could be concluded that Myanmar is a closed country and unlikely to be an egress route for eavesdropping incidents.

Estimates for worldwide internet usage in June 2018 (Miniwatts Marketing Group 2018) report by world continent usage: North America 95.0%, Europe 85.2%, Oceania and Australia 68.9%,

Latin America and the Caribbean 67.2%, Middle East 64.5%, Asia 49.0%, Africa 36.1%.

Internet-based cyber incidents are not the focus of this thesis, but the potential to use the internet as an egress route, whether for close or remote access, is now most probably dominant.

Wi-Fi growth: The global network Wi-Fi Fon report that since the introduction in 1999 of the 802.11 Wi-Fi standard, the demand for Wi-Fi has grown steadily. Internet Service Providers began to offer Wi-Fi routers in 2002 and soon after Wi-Fi enabled devices such as Portable Digital Assistants became available. With the advent of smartphones in 2007 demand for Wi-Fi grew exponentially. By 2011 Wi-Fi was being used by 1.2 billion users worldwide. By 2015 451 million householders had a Wi-Fi router in their home with a further 64.2 million public Wi-Fi hotspots available globally. It is thought that 24 billion devices will be connected to the Internet by 2020 (Fon 2015).

A new vulnerability has been identified that is introduced when Wi-Fi is installed in sensitive locations. In 2015 Wei.T et al. (Wei et al. 2015) described ‘Wireless Vibrometry’. A vulnerability that may create opportunities for eavesdropping on acoustic information adjacent to the Wi-Fi radio transmitter by monitoring signal level fluctuation.

Mobile telephone network growth: In addition to the growth of mobile telephone networks discussed in section Chapter 2.49, GSM network coverage across the UK for all four networks available is greater than 99%.

For an eavesdropping system using GSM an important aspect is the choice of frequency used. There are five frequency bands used for 2G, 3G and 4G cellphone coverage in the UK: 800MHz (Band 20), 900MHz (Band 8), 1800MHz (Band 3), 2100MHz (Band 1) and 2600MHz (Band 7). The new 5G spectrum is currently being finalised. At this moment in time, 5G will likely be centred around 3.5GHz and is thought to offer the best compromise between capacity and coverage.

Of all six bands available, 800MHz has the potential for the greatest range as this frequency is least attenuated by building materials. All four service providers use 800MHz for 4G services. It makes sense therefore for the most reliable GSM-based eavesdropping systems to be on 4G

services. Indoor coverage of mobile telephones is far from universal in many rural areas of the UK. A service predictor provided by OFCOM illustrates indoor coverage for a particular service provider (Ofcom 2019).

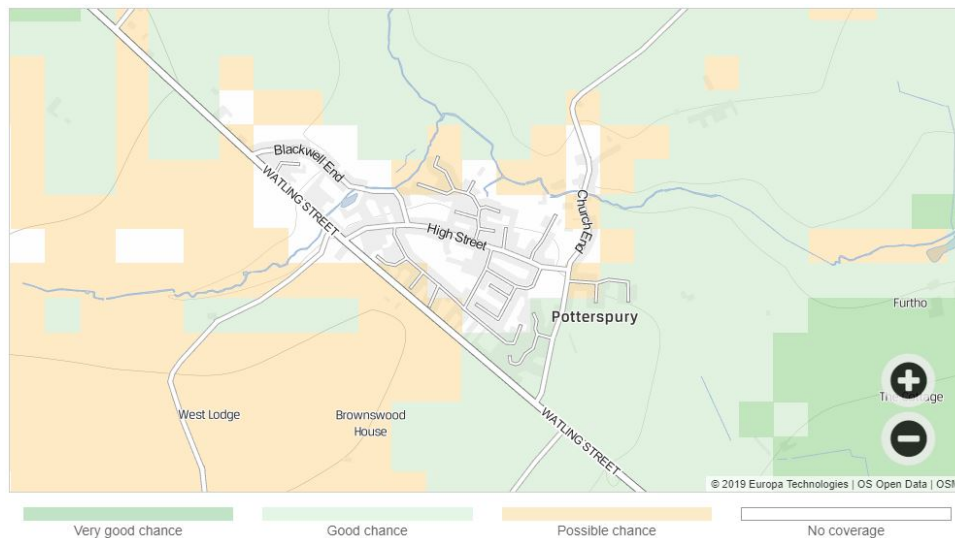


Figure 6.8: Indoor cellphone coverage in a rural area of the UK illustrating the poor or no coverage availability in a central rural UK village location (Ofcom 2019).

Worldwide usage of GSM makes GSM a universally potential egress route (WorldTimeZone.com 2019). Figure 6.9 illustrates the likely worldwide coverage. Two significant bands are used: 900/1800MHz or 850/1900MHz. One notable difference is that of Japan which employs additional frequencies.

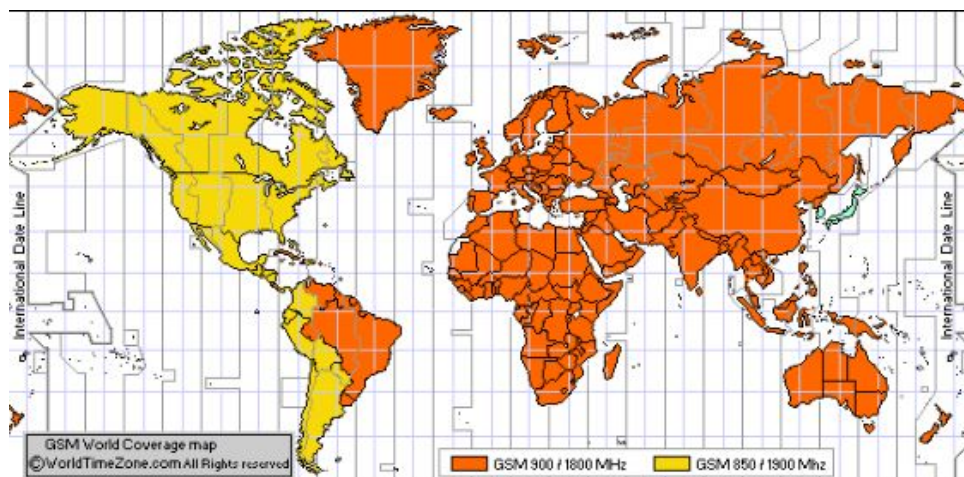


Figure 6.9: Worldwide GSM coverage and frequency bands used (WorldTimeZone.com 2019).

As with the detailed cellphone coverage illustrated in one example in the UK, the reliability of GSM will be on a country-by-country basis. Population areas in large cities offer the greatest

potential reliability for GSM eavesdropping egress.

An interesting development, if not alarming, was revealed by ITV's *Exposure* (Hardcash Productions 2019). The programme uncovered the use of China's government work with technology companies to control Uyghur Muslims through analysis of change in cellphone usage which challenges human freedom and liberal democracy.

Wearable Technologies: This has the potential to be a key technology threat for eavesdropping consideration. *Wearable Computing Devices*, possibly built using *Materials Science* advances or the capabilities of *Printed Electronics* and changes in *Battery Technology* capability. Grell et al. (Grell et al. 2019) have created a low-cost method for the metallisation of woven and non-woven fabrics. They have applications in eavesdropping technologies through their application in woven coil antennas for wireless energy harvesting or for Ag–Zn batteries for energy storage.

The increase in smart watches and wearable fitness technology has increased in adults over the age of eighteen from 2% in 2010 to 26% in 2018 (OFCOM 2018, pp.12). This technology is often worn 24/7, making it an attractive target for eavesdropping. The technology contains two key components: a battery and Bluetooth egress capability. The addition of a microphone to enable the recording or transmitting of conversations is quite possible. Confronting visitors who wear such devices when privacy issues are of concern is socially awkward and leads to a strong potential to overlook the threat.

The Internet of Things (IoT): This is an underlying enabling technology that is of considerable concern to those wishing to reduce eavesdropping vulnerabilities.

The low-cost electronic building blocks enable connection and information transmission from a sensor egressed to some remote location. For example, power derived from the air (Gollakota et al. 2014) has the potential to enable eavesdropping without a traditional power source. This may impact on where the sensor might be deployed and in a position not previously considered.

Internet televisions were an early adopter of internet integration. With this too were new vulnerabilities of voice commanded televisions connected to the internet.

Samsung was required to update their customers about the risks of their Smart TVs (Samsung 2015). The media were quick to pick up on the threat, with many online articles such as (Goldman 2015) and (Gibbs 2015) and then soon to decide the unsubstantiated conclusion that governments' security services must be behind such vulnerabilities (Whittaker 2017).

It is hard to imagine why anyone installing a smart speaker in their home does not consider the potential for eavesdropping. The very idea of connecting a microphone to the internet is inviting the likelihood of it being used for eavesdropping purposes. There are three main providers of this technology: Amazon Alexa, Google Home and Apple HomePod. All three have suffered problems with their first devices to market with the vulnerabilities highlighted below fixed.

Amazon's Alexa digital assistant has a line of Echo speakers; Xinyu Lei et al. identified several security vulnerabilities which included the Alexa device, service providers and third party service developers (Lei et al. 2017). The University of Indiana identified two major security vulnerabilities with Alexa which created new forms of cyber attack called 'voice squatting' (Spalding and Chow 2018). Amazon permitted third party developers to publish their own native Alexa applications and in doing so permitted the publication of malware which bears a name homophonous to other popular applications. Even more alarming, Day et al. reported that *'A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands'* (Day, Turner, and Drozdak 2019). The team of listeners occasionally hear clips that the owner of the Alexa device might prefer to stay private.

Russakovskii highlighted the vulnerability that Google's home smart speakers were spying on everything said. Google were quick to respond to this privacy issue with a fix (Russakovskii 2017).

Apple HomePod has fewer problems but then provides much less functionality than the Amazon or Google system. When it hears a request, Apple parses the request but does not associate the request with a user's account. Some problems exist in multi-user (multi-voice) homes, but are less of a security problem.

All three systems remain vulnerable to well-funded, focused and determined eavesdroppers who would likely exploit unpublished vulnerabilities to their advantage.

An IoT exploit demonstrated at Infosecurity Europe in 2015 was made against an iKettle that made it easier to hack Wi-Fi codes because it failed to verify the Wi-Fi access point by anything other than the SSID. Ken Munro, a security researcher at PenTestPartners detailed the hack and demonstrated the kettle's vulnerability (Munro 2015a,b,c).

The '*Internet of Things*' is often called '*The Internet of Vulnerabilities*'. There will be many theses and security papers written on this subject alone. The focus of this research is to consider the future of IoT and to be ever mindful of the potential for IoT to introduce eavesdropping vulnerabilities.

Embedded GPS Tracking: It is obvious when using a purpose-built car satellite navigation system that it has history features built-in for owner convenience. Google too permits the sharing of location details from an Android smartphone with chosen friends and family. There are other benefits to enabling location services with many apps offering feature rich benefits and instantly providing the user information about their surrounding environment or how to navigate to a new location with a mapping service.

However, in doing so, the user provides the service provider with information beyond that with which the user may initially realise. Google provide both a monthly and an annual report for the user tracked: '*Your timeline in Google Maps helps you curate the places you've been. Look back on the past month and reminisce about recent trips and past places.*' and all created entirely by automation from the recorded location history. In one user example the location services report for the year 2018 revealed the following information:

- The number of unique places, number of cities and countries visited;
- Where the user lived and worked;
- That groceries were purchased from the same supermarket and the number of visits;
- Where and how often the user went on holiday and the name of the hotels stayed in;
- The identity of the user's friends and where these friends lived too;

- Where and when the user ate out;
- The distance in miles/km travelled by the user (and how far that was around the world) and how many hours had been spent walking and the distance covered by these walks;
- That the user ran for a number of hours and the distance covered;
- How many hours the user spent in a car or a train and the distance covered;
- That the furthest travelled distance was to a named city.

The data would also have enabled Google to determine the user's socio-economic class, disposable income, employer's name, religion, interests, and even the individual's level of personal fitness. This rich list of intelligence, generated automatically by an algorithm from logged location history is significantly different to the past resources required and the information derived from monitoring a single wired microphone.

Sometimes though we would rather the ability to track our location was not available. Do we really want to give our home location away to everyone? Having GPS tracking built into smartphones is a known feature but care should be taken with other consumer devices where it may be less obvious.

Many cameras record location details. GeoTagging information for each photograph is embedded into the image but this is not always known and often forgotten by users. Care must be taken if sharing public photographs that the embedded location detail has been removed.

6.2.5 Legal Factors

The legality of eavesdropping is dependent upon in which country the eavesdropping is taking place and the specific activity conducted. If a radio transmission is used without a licence then this may be a crime against the Wireless Telegraphy Act. In many countries it is a specific crime to listen to telephone conversations. In the UK the tapping of telephones has received a great deal of attention after reporters from the News of the World were prosecuted for listening to voicemail. From a Data Protection Act angle, the UK Information Commissioner might take a view on the recording of conversations if they are recorded without consent.

However, the instances within this thesis are perpetrated by state actors worldwide. The legal status of eavesdropping will likely fall under national security and for the protection of the country's citizens. If legality is an issue, the obfuscation and deniability of an eavesdropping activity become more important.

Encryption will continue to play an important role in anti-eavesdropping of communications systems, with legality in some countries differing. In the context of the popular Facebook-owned WhatsApp communication tool it is interesting to note that although encryption is in place for point to point communication, if the conversations are backed up by a user, there is no encryption. This leaves open the potential for interested parties to gain access to historical communications. As more and more data is lost to hackers, legislation will continue to evolve. In the UK the General Data Protection Regulation (GDPR) was introduced on the 25th May 2018 with the aim of providing EU citizens with more control over their personal data. GDPR's implementation has been taken seriously; infringement can be enormous: administrative fines of up to 4% of annual global turnover or 20 million Euros, whichever is greater.

As the value of personal data becomes more apparent, there is growing concern with how this information is being gathered, stored and used. Privacy laws worldwide will continue to evolve and new legislation will be introduced as each country actively pursues more progressive privacy laws.

6.2.6 Environmental Factors

Environmental Factors may not initially seem worthy of consideration. However, the environment is an important aspect for eavesdropping consideration.

Geographical location: Increased transport costs and low-cost internet access has resulted in a rise in the use of teleconferencing systems and face to face applications from mobile telephones.

Mobility: The advent of low-cost portable computing and smartphone technology has:

- Reduced the requirement for an office, fixed landline telephone and desktop computer;

- Increased hot-desking in the office;
- Increased occurrences of home working and the consequential office documentation or IT equipment being left in the home unattended or available with reduced security access requirements.

The use of glass in buildings: Architects like using glass in modern buildings, they create nice places to work. However, when its dark outside, well lit internal offices create ideal conditions for overlooking with telephoto photography from surrounding external offices. Often, the external observing point will not be visible from the office.

Global warming: Global warming will drive instability and conflict. As the impact of global warming becomes ever more apparent, state stability and internal conflict will lead to state failure. Furthermore, the increase in impacts to the livelihoods of some commercial interests may also lead to complex security affecting situations. The rise in the lack of trust will lead to espionage and eavesdropping incidents between those with opposed interests.

Educational levels: A technical education is a prerequisite requirement for technical eavesdropping attacks. Countries with lower levels of technical education are less able to mount effective attacks.

6.3 Contribution and Summary of Achievements

This thesis is focused on the changing nature of eavesdropping technology. The contribution made by Chapter 2 is that of a technical study on an area that has seen little or no attention. Details of these eavesdropping events are dispersed throughout literature but have been collated into this single chapter which enables a new perspective to be observed.

The chapter reveals the way in which the industry began from early telephone intercepts, simple wired microphones against unprotected premises offering home nation advantages and the realisation by technically advanced nations that new techniques were required to outwit the opposition. As radio continued to develop through the invention of the transistor, methods

to attack high-profile targets in third party countries arose. With ever-greater mobility opportunities, radio techniques were created to illuminate microphones that required no power sources, or to exploit vulnerabilities in communications apparatus through signals interception and TEMPEST techniques.

As office life changed and ambassadors no longer dictated to their secretaries, eavesdropping technology changed focus too, following new assets. The communications hubs or early electrical mechanical communications and cypher systems were targeted. The rise of communication over telephone lines was soon replaced with communication via the internet. The convergence of mobile telephones and internet technologies create easier and more convenient ways to communicate, but create vulnerabilities that are also far easier and more convenient to exploit.

High-profile targets will continue to be a target for eavesdropping. This chapter however highlights that with lowered technical capability requirements for mounting an eavesdropping attack, anybody can be subjected to an eavesdropping attack, wherever or whoever, they may be.

The technology itself is the focus of Chapter 3 and the present-day intrusive surveillance techniques available. Through expert elicitation, comprehensive eavesdropping techniques have been collated in order to create a taxonomy of eavesdropping systems and methodologies. The components of a system are highlighted together with the critical transmission path needed to egress the information from the target.

Chapter 4 continues the contribution with the evaluation of eavesdropping system's life cycles. Technology makes what was impossible yesterday, possible today. Eavesdropping techniques are shown to have evolutions and these are illustrated through the research of three case studies; eavesdropping systems continue to innovate and the number of innovations is growing. Technical innovation is shown to enable the technically illiterate with powerful eavesdropping techniques. The framework provides a new and powerful methodology that will enable eavesdropping technology countermeasures to be considered.

The contribution made in Chapter 5 is to propose the concept of predicting whether a particular eavesdropping technology will be deployed given an attackers capability, opportunity and intent.

Dealing with uncertainty through the Bayesian Predictive Model reveals new insights in the probabilities and exploitabilities of techniques by differing capabilities.

This last chapter illustrates in Figure 6.5 the changing nature of eavesdropping technology and the trend of the capability requirement for deploying eavesdropping systems. It highlights graphically that the entry barrier requirement for effective eavesdropping has been lowered. The chapter also considers topics that are not normally considered but that are likely to have a growing impact in the future for eavesdropping technology.

Finally, I will make one prediction regarding eavesdropping that I can state with a high degree of certainty: that as long as people mistrust each other, eavesdropping will continue, but the way it is achieved technologically, will continue to change.

Appendix A

Copyrights

The following figures are all copyright of the author:

Chapter	Figure Numbers
Chapter 1:	1.2
Chapter 2:	2.2, 2.5, 2.10, 2.11, 2.13, 2.14, 2.15, 2.17, 2.18, 2.19, 2.21, 2.22, 2.23, 2.24, 2.25, 2.26, 2.27, 2.28, 2.29, 2.30, 2.31, 2.32, 2.33, 2.34, 2.35, 2.37, 2.39, 2.41, 2.42, 2.43, 2.46, 2.47
Chapter 3:	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7
Chapter 4:	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.15
Chapter 5:	5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10
Chapter 6:	6.2, 6.5

Table A.1: Images copyright of the author

The following Table Ref. A.2 lists other copyright permissions

Figure	Page	Source	Copyright Holder
Fig. 1.1	3	http://www.hs-augsburg.de/~harsch/Chronologia/Lspost11/Bayeux/bay_tap1.jpg	Creative Commons Public Domain PD-Art
Fig. 2.1	10	https://patents.google.com/patent/US447918A/en	Public Domain
Fig. 2.3	11	Reprinted with permission of The American Legion Magazine, © March, 1937. www.legion.org	See email permission below
Fig. 2.4	13	https://www.chu.cam.ac.uk/news/2014/jul/7/mitrokhins-kgb-archive-opens/	See email permission below
Fig. 2.6	19	Reprinted with permission of Scientific America.	See email permission below
Fig. 2.7	21	Crown Copyright Report R6/3	Crown Copyright
Fig. 2.8	22	Crown Copyright Report R6/3	Crown Copyright
Fig. 2.9	23	Crown Copyright Report R6/3	Crown Copyright
Fig. 2.12	28	www.state.gov/wp-content/uploads/2019/05/176589.pdf	Public Domain State Dept.
Fig. 2.16	36	www.state.gov/wp-content/uploads/2019/05/176589.pdf	Public Domain State Dept.
Fig. 2.20	41	www.state.gov/wp-content/uploads/2019/05/176589.pdf	Public Domain State Dept.
Fig. 2.36	55	Cuban National Information Service	Public Domain
Fig. 2.38	59	https://www.flickr.com/photos/cnduk/6260000027	Creative Commons 2
Fig. 2.40	63	https://www.flickr.com/photos/ciagov/7190343303	Public Domain US NSA
Fig. 2.44	80	https://nsa.gov1.info/dni/nsa-ant-catalog/wireless-lan/index.html	Public Domain
Fig. 2.45	81	https://english.defensie.nl/binaries/defence/documents/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw/ppt+pressconference+ENGLISH+DEF.pdf	Creative Commons Zero (CC0) licence
Fig. 2.48	90	https://ourworldindata.org/internet	Attribution 4.0 International (CC BY 4.0)

Fig. 2.49	91	https://ourworldindata.org/internet	Attribution 4.0 International (CC BY 4.0)
Fig. 6.1	191	Credit (Gill and Phythian 2013)	Permission requested by email 16/09/2019
Fig. 6.3	195	https://www.flickr.com/photos/briansolis/35963831302	Creative Commons 2
Fig. 6.4	196	https://www.domo.com/learn/data-never-sleeps-7	See email permission below
Fig. 6.8	205	https://www.ofcom.org.uk/checker-app/about-the-checker	Public domain
Fig. 6.9	205	https://www.worldtimezone.com/gsm.html	See email permission below

Table A.2: Copyright permissions for images not produced by the author



Figure A.1: Permission to use Figure 2.3 on page 11.


Mitrokhin images



Director, Churchill Archives Centre <Director.Archive:

To: Gudgeon, Jonathan

Cc: Tom Davies

 Reply

 Reply All

 Forward



Mon 29/07/2019 12:03

Dear Jonathan,

Thank you for your email enquiry. I think it will be fine for you to use these images in your thesis as they have been widely published on the internet. But thank you for checking. The copyright is probably with the Mitrokhin estate. Unfortunately, they do not have anyone to answer such questions.

All best wishes,

Allen



Mr Allen Packwood

Director

Email: director.archives@chu.cam.ac.uk

Telephone: 01223 336175

Churchill Archives Centre

Churchill College

Cambridge, CB3 0DS

Registered Charity: No 1137476

Figure A.2: Permission to use Figure 2.4 on page 13.

Re: Request to use a figure from a book in a PhD thesis



Sciam randp <randp@sciam.com>
To: Gudgeon, Jonathan

Reply
 Reply All
 Forward

Thu 31/10/2019 22:53

Hello,

We do not object to your use of the images on pp. 132 and 133 for your thesis.

Best,
Rights and Permissions
Scientific American

From: Gudgeon, Jonathan
Sent: Friday, October 11, 2019 7:12 PM
To: Copyright Agent
Subject: Request to use a figure from a book in a PhD thesis

Dear Sir,

I am a research PhD student from Imperial College London and I would like permission to use a single figure from a 1968 publication in my soon to be submitted PhD thesis.

Your publication details and the citation I've created in my PhD thesis are as follows:

Strong, C.L. (1968). "The Amateur Scientist: Little radio transmitters for short-range telemetry".
In: Scientific American, Inc. Volume 218.Issue 3 (March), pp. 132-133.

I have attached the figure for your reference. Furthermore, the article is online at the university of Columbia, in New York See <http://www.apam.columbia.edu/courses/apph4903x/LittleRadio-SciAmer-1968.pdf>

I should be most grateful if you would consider my request. I will ensure full credit is given for the source of the diagram.

Yours gratefully,

Jonathan Gudgeon,
PhD Student, Imperial College London, United Kingdom.

Figure A.3: Permission to use Fig. 2.6 on page 19.

Re: WTZ-General enquiry



world time zone <wtz@worldtimezone.com>
To: Gudgeon, Jonathan

Reply
 Reply All
 Forward

Sun 15/09/2019 22:06

Feel free with credit.

thank you.

WorldTimeZone.com

Sent from my T-Mobile 4G LTE Device

Figure A.4: Permission to use Figure 6.9 on page 205.

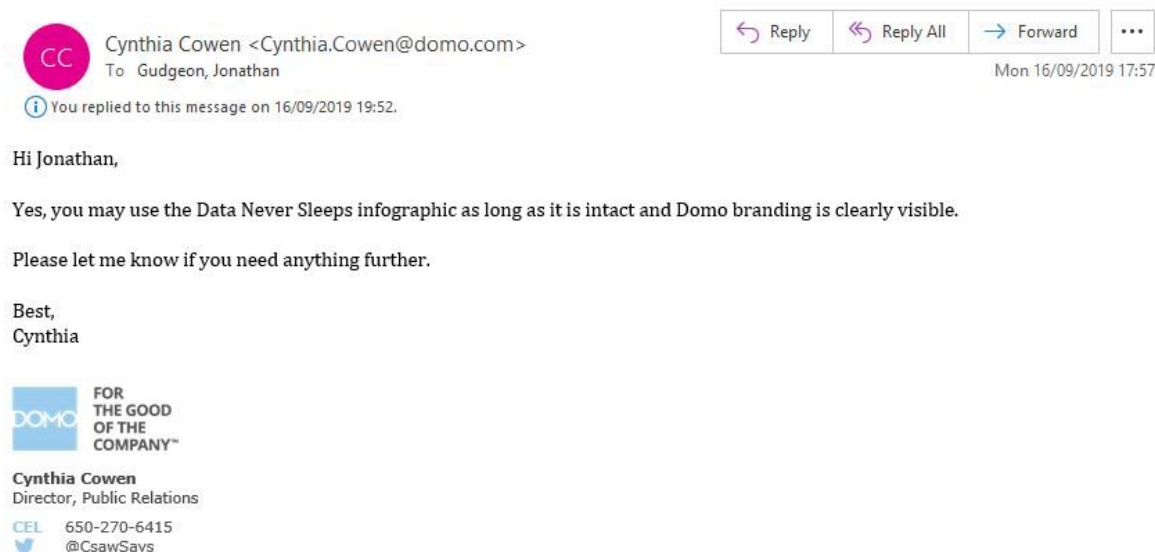


Figure A.5: Permission to use Figure 6.4 on page 196.

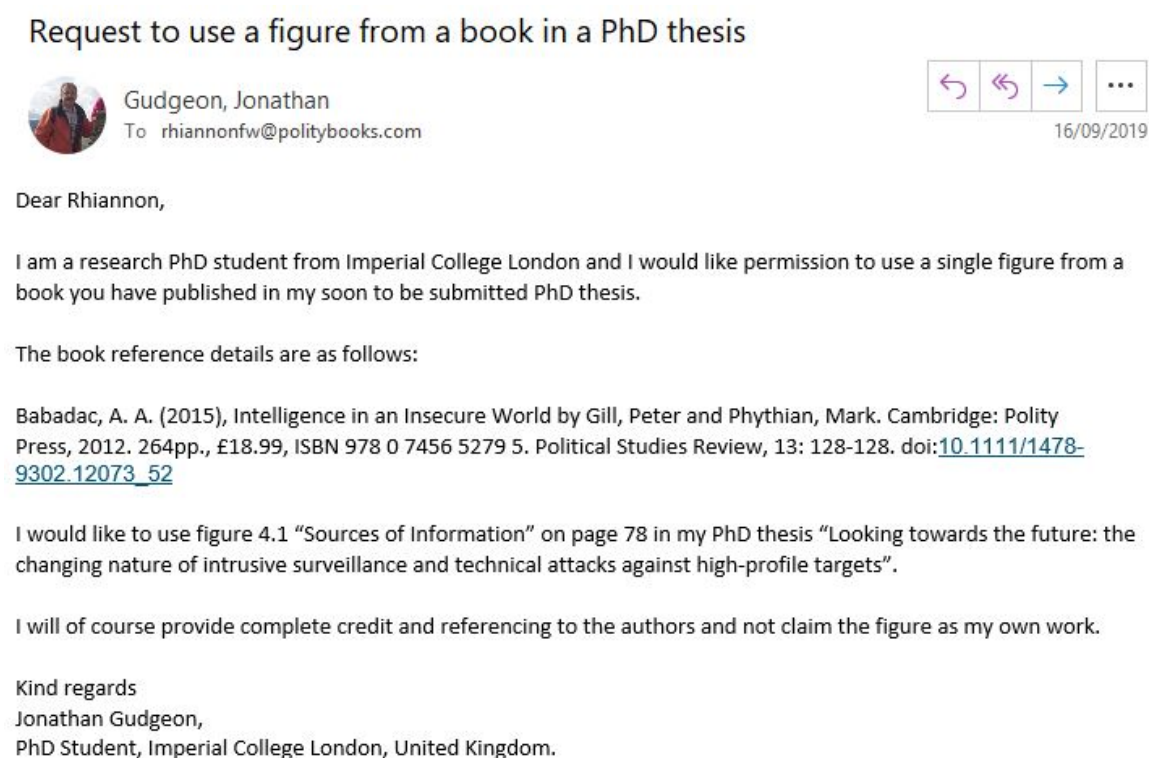


Figure A.6: Request to use Fig. 6.1 on page 191 Credit (Gill and Phythian 2013).

Appendix B

Timeline of Eavesdropping Events

B.1 Events Derived from English Language Literature

The following tables list the occurrences of incidents discovered through the literature research.

SIGINT			
Date	Count	Detail	Page
1920	1	SIGINT against Soviet Trade Delegation in Highgate	9
1963	1	KGB against US	56
1963	1	KGB against CIA In Mexico	56
1966	1	KGB SIGINT in Washington	56
1967	1	KGB deciphering 152 cipher machines worldwide	56
1969	1	KGB SIGINT in New York	56
1970	15	KGB against 15 cities (location not revealed)	56
c1970	1	KGB SIGINT operation in Cuba	56
1975	1	US Employing long-range sensors for SIGINT ops	56
1976	1	ECHELON global spying system first became publicly known	56
1976	1	ECHELON global satellite monitoring revealed	57
2013	1	US mobile telephone intercept against Germany in Berlin	56
2015	2	GCHQ SIGINT suspected in British Embassy Berlin and Vienna	55

Table B.1: SIGINT incidents in literature review.

Wired Microphones

Date	Office	Home	Detail	Page
1931		1	In Paris by the KGB	14
1934		1	American residence in Moscow	14
1937	1		American Embassy in Moscow	14
1939-42	72		UK Trent Park German POW camps wired for audio	15
1941	>1		Stalin bugged evacuated western embassies in Moscow	14
1943	Multiple		NKVD Tehran summit non-metallic microphones to avoid detection	15
1944	120		American Embassy find large microphone network	15
1944	26		British Military Mission in Moscow find 26 microphones	15
1945	1		NKVD recorded Roosevelt and Churchill conversations	15
1947	3		Infrared LASER mic against USA, UK and France	17
1948	13		Norwegian Embassy Moscow discovered 13 microphones	15
1948	1		American FBI in New York bug the Arab League	24
1949	>1		Several microphones discovered in collapsed ceiling of Greek ambassador's bedroom	23
1952	1		Single microphone discovered in the American Embassy in Moscow	23
1952	1		American FBI bugged the Israeli intelligence service in New York	24
1953	To Note		American Embassy in Moscow microphone installation	24
1956	To Note		American Embassy in Moscow continues to be bugged	24
1956	>1		Microphones found in Ambassador's office in Tel Aviv and Belgrade	25
1959	>1		FSTMS devices found in British Embassy in Spain	26
1959	1		FSTMS evidence in Sweden against British Embassy	26
1959	3		Three microphones found by FSTMS technicians in the British Embassy Moscow	26
1960		>1	CIA bugged Russian hotel rooms attending the 'Paris May 16 Summit'	18
1960		200	Claims of two hundred microphones found in staff flats in Moscow	26
1960	100+		American's report more than one hundred devices in diplomatic premises in Eastern block	27
1962		1	Penkovsky's Moscow apartment bugged from above	30
1964	42		American Embassy in Moscow microphone network	27
1964		50	American apartments in Moscow	28
1964		1	In Moscow flat by the KGB	28
1968-70	78		Czechoslovakian surveillance seventy-eight listening devices planted in Western embassies and diplomatic suites	30
1969	1		German sweeper injected very high voltage in Moscow	39
1975	2		Laser microphones used in West Africa and US	43
1979		6000	Stasi activity against own population	49
1979-84	>1		New American Embassy in Moscow	62
c.1980	8		CIA bugged an undisclosed Asian Embassy	29
1980	50+		Technical surveillance against Iranian Embassy in London under terrorist siege	62
1989	>1		Soviet Trade delegation bugs found (originally in 1971?)	45
2001		2	Bugs found in Tony Blair's hotel room in New Delhi	76
Unknown	1		Canadian Embassy KGB 'bug-tug' microphone cable	31

Table B.2: Wired microphone incidents in literature review.

Radio Microphones			
Date	Count	Detail	Page
1950	1	British Embassy Naval Attaché in Moscow	20
1952	1	The Great Seal - Spaso House US Residence in Moscow	18
c.1955	1	US EASYCHAIR transponder developed in the Netherlands	21
c.1955	1	UK SATYR transponder developed	21
1955	1	Phone box used by Soviet Embassy in Vienna	24
1955	1	CIA miniature unofficial device in Vienna residence	25
1957	2	Peter Wright and Canadian RCMP install two SATYR devices against the Polish Consulate in Montreal	22
1959	1	MI5 and ASIO SATYR op against Russian Embassy in Australia	22
1959		CIA develop transmitters in electric typewriters and self-contained batteries for use behind a car dashboard for tracking purposes	42
1959	1	CIA cat radio microphone development	42
1959	4	KGB cars in Soviet Embassy Mexico	40
1965	1	Conakry CIA office bugged	41
1967	36	KGB radio microphones in operation	40
1967-71	1	Beirut British SIS Station	40
1967	1	Commercial radio microphone for sale	60
1969	1	UN Secretariat to Secretary General	41
1969	1	Ghanaian UN Delegation	41
1969	1	Senate Foreign Relations Committee	41
1969	1	American Embassy diplomat's shoe bugged in Bucharest	42
c1970s	>1	CIA radio microphones hidden in pepper mills in restaurants	42
1971	>1	US Watergate and Nixon bugging scandal	58
1971	6	Highgate Russian Trade Mission	44
1972	1	Conakry American Embassy bugged by KGB	41
1974	1	Conakry American Embassy bugged by KGB	41
1975	1	UK commercial radio microphone size of two pence	61
1975	1	Communist Party radio microphone in London HQ	61
1975		CIA claim development of olive-cocktail stick and a tooth bug	43
1975		CIA bugged ministers' homes and offices in Latin America	43
1978	1	Aerial discovered in US Embassy chimney in Moscow	36
1980	1	Arlington private defence contractor KGB bug	43
c2001	2	Motorway service station and Dutch coffee shop briefcase mounted microphone array	66
2004	2	Sinn Féin floor board and car bugs	76
2004	1	UN Radio Microphone Bug in Geneva HQ	77
2006	1	Malham village hall incident	73
2011	?	KGB 'interrogation attack' by microwave or laser beam at the cipher room	34
2013	1	Equador Embassy in London bug	77
2015	1	Ai Weiwei listening devices hidden in his Beijing studio	78
2016	1	All Blacks hotel conference room bug found in a chair	85

Table B.3: Radio microphone incidents in literature review.

Cipher and Typewriters			
Date	Count	Detail	Page
1930	1	British cipher machine sold to OGPU (Soviet Intelligence)	48
1969	1	Germans discover attack against cipher machine in Moscow	39
1974	1	KGB steal cipher material from seven missions in Prague	35
1974	1	KGB steal cipher material from five missions in Sofia	35
1974	1	KGB steal cipher material from two missions in Budapest	35
1974	1	KGB steal cipher material from two missions in Warsaw	35
1976-83	1	KGB bug six French teleprinters	35
1977		French Embassy teleprinters in Moscow egressed via mains	31
1980	1	KGB attack Angola cipher	35
c.1983	1	KGB attack German teleprinter in Budapest	31
c.1983	1	KGB attack Algerian teleprinter in Budapest	31
c.1983	1	KGB attack Italian teleprinter in Budapest	31
c.1983	1	KGB attack Swiss Siemens T-1000 teleprinter in Budapest	31
c.1983	1	KGB attack Japanese teleprinters in Budapest	31
1983	10	Soviets reading cipher traffic from Indonesians, Syria, Iraq, Iran, the Palestine Liberation Army (from 1982), Portugal, low-grade Vatican cipher, China and North Korea one-time pad cipher and Zaïre	31
1984	3	KGB attack three typewriters in Leningrad (US GUNMAN)	37
1984	13	KGB attack thirteen typewriters in Moscow (US GUNMAN)	37
2008	1	Soviet use of cyber warfare ahead of Russian-Georgian War	69
2013	2	Santander and Barclays Bank router incidents	83
2013	1	Snowden revelations and leaks	70
2015	1	Soviet disruptive attacks on critical infrastructure against Ukraine	69

Table B.4: Cypher incidents in literature review.

Photography			
Date	Count	Detail	Page
1906	1	Documents copied in British Foreign Mission in St.Petersburg	9
1921	1	Against diplomatic couriers on Leningrad train	47
1936	1	Maclean smuggled out documents from UK Foreign Office	48
1949	1	Russian blackmail attempt against Greek ambassador in Moscow	23
1957-61	1	Against NATO HQ with van	47
1962	1	Long-range photography against Oleg Penkovsky in Moscow	48
1968	1	KGB training microdot to agents	47
1970s	100	Mikrat cameras made for Stasi agents	51
1970s	1	1mm aperture pin-hole camera available	52
2009	1	Ekaterinburg brothel bugs against a diplomat	77

Table B.5: Photography incidents in literature review.

TEMPEST

Date	Count	Detail	Page
1914-18	1	Trench telephone intercepts on the front-line	11
1916	4	Four out of fifteen sets were intercepting German messages	11
1943	1	Bell labs TEMPEST discovery	31
1954	1	Soviets aware of TEMPEST vulnerabilities	32
1956	1	Egyptian Embassy in London cipher machines bugged during the Suez crises	30
1960-63	1	UK TEMPEST attack against French Embassy in London	32
1972	1	Public TV awareness of TEMPEST	32
1985	1	Van Eck TEMPEST demo on UK broadcast TV	32
2002	1	Optical TEMPEST demo by Cambridge University Markus Kuhn	33
2004	1	Academic paper on IT keyboard acoustic TEMPEST vulnerability	67
2006	1	Academic paper on acoustic dictionary attack vulnerability	67
2006	1	Kuhn real-time TEMPEST vulnerability demo	33
2009	1	Academic paper on mains keyboard emanations vulnerability	67
2014	1	Academic paper on acoustic time difference of arrival vulnerability	67
2015	1	Miranov SDR TEMPEST software package for enthusiasts	67
2016	1	Software Defined Radio TEMPEST	68

Table B.6: TEMPEST incidents in literature review.

Telephone

Date	Count	Detail	Page
1878	>1	Haven, Connecticut Manual Switchboards' eavesdropping opportunity	10
1891	1	Strowger undertaker competitor eavesdropping	10
1938	5	UK MI5 monitoring embassies of Germany, Spain, Italy, Japan and the USSR	12
1941	1	Telephone tapping operation in Santiago "actually located in the British Embassy itself"	12
1942	>1	Communist Party of Great Britain HQ telephone taps	61
c1946	>1	MI6 Post-war telegrams and telephone call interception	12
1948	>3	UK SIS station in Vienna dug three tunnels code-named 'Conflict', 'Sugar' and 'Lord' to tap Soviet telephone and telex lines	38
1955	149	British operation 'Stopwatch and US operation 'Gold' tunnel tap against Soviets in Berlin	38
1960	14	Brussels NATO fourteen rigged switch-hook attacks against US Europe Command Headquarters	46
1960	>100	More than one hundred switch-hook attacks against US Diplomatic premises within Eastern bloc countries	46
1964	1	Khrushchev's apartment telephone bugged	7
1970-80	40000	Forty thousand tapped western telephone lines	53
1977	1	CIA fibre optic tap between Moscow and Troitsk	39
1983	20,000	Twenty thousand simultaneous telephone taps in East Berlin	50
1984	1	Arthur Scargill's telephone taps read by Margaret Thatcher	61
2003	4	Council of the European Union HQ, Brussels, bugs discovered	76

Table B.7: Telephone incidents in literature review.

Covert Entry

Date	Count	Detail	Page
1906	1	Keys copied in British Foreign Mission in St.Petersburg	9
1938	3	Post Office opening Italians, Japanese and Balkan embassies diplomatic bags	12
1960s	1	KGB break into Swedish Embassy in Moscow	35
1964	1	Low-energy radio frequency used to start fire in British Embassy Moscow	34
1974	1	KGB Portable x-ray generator to defeat combination locks of safes	35
1977	1	Low-energy radio frequency used to start fire in US Embassy	34

Table B.8: Covert entry incidents in literature review.

Tape Recorder

Date	Count	Detail	Page
1977	56	Small Stasi tape recorders available for deployment	52
1977	30	Stasi concealments available for deployment	52
1980	643	Types of Stasi tape recorder available for deployment	52
Cold War	1	Yugoslav neighbour instructed in tape recorder use in Belgrade	25

Table B.9: Tape recorder incidents in literature review.

Agent Comms

Date	Count	Detail	Page
1970	1	CIA burst transmitter in Cuba to orbiting satellite receiver	54
1983	1	CIA burst transmitter in Moscow to orbiting satellite receiver	54

Table B.10: Agent communications incidents in literature review.

Odd Events

Date	Count	Detail	Page
1971	105	Russians technical staff expelled from Trade Delegation in London end up in Delhi, Colombo, Dar-Es-Salaam, Lagos and Lusaka	46
1992	2	‘Litra’ marking system and ‘spy dust’ in use in Moscow against diplomats	63

Table B.11: Odd events worthy of mention from the literature review.

Figure B.1 illustrates the relative periods of technique employment. For example, the first occurrence of a wired microphone event occurred in 1931 with the last such event occurring within the literature review in 2001. The first radio microphone incidents occurred as illumination events in 1950 and 1952 with the next radio microphone event occurring in 1955. The most popular period of the radio microphone can be seen in the 1970s with its popularity ending in 1980. There is a resurgence of radio microphone use in 2004 as a result of Northern Ireland politics and the EU in 2004 is also an interesting Russian style wood-stick device. The Malham village hall incident in 2006 illustrates the commercialism of eavesdropping with technology available for anyone to purchase. The 2013 incident is interesting in that it uses new technology in the form of a GSM bug. Cheap telephone modules adapted for eavesdropping purposes enable worldwide egress via an available mobile telephone network.

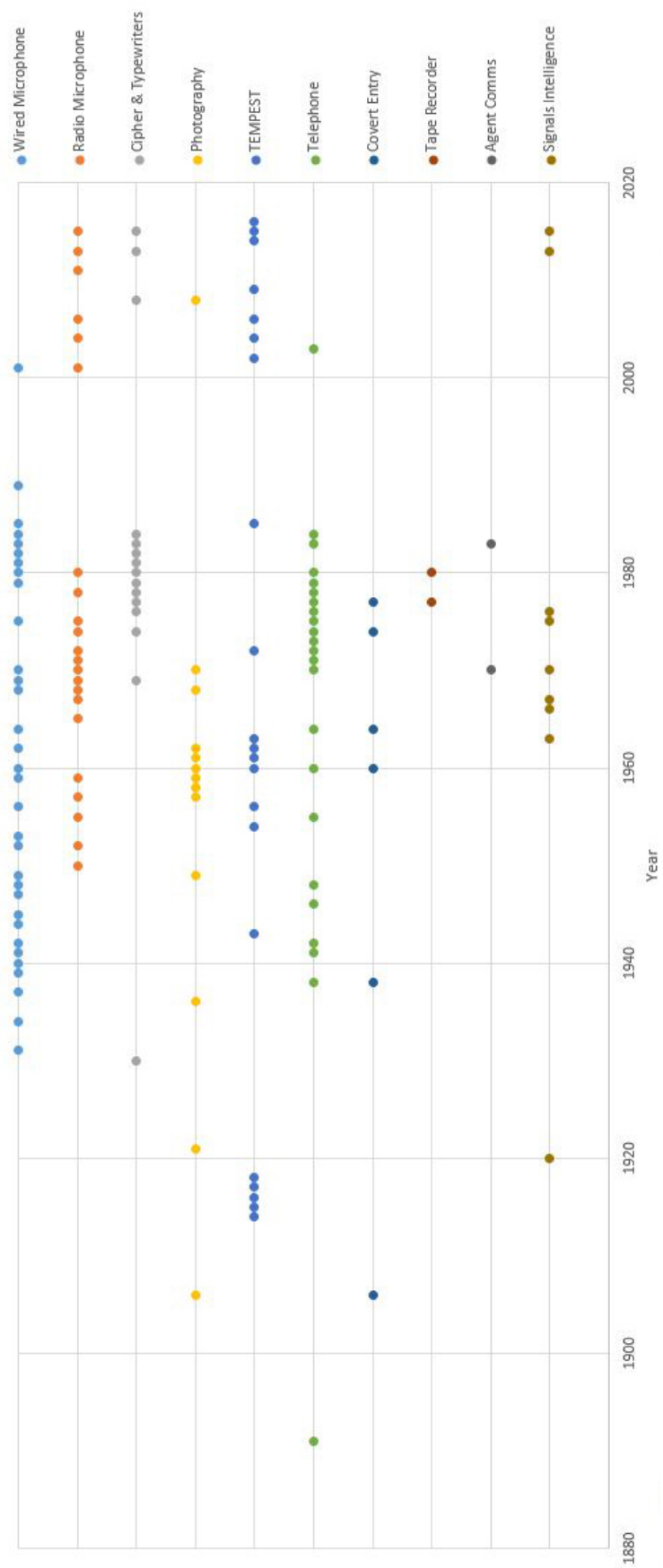


Figure B.1: Statistics from the literature review grouped into ten categories.

B.2 Timeline of All Events Recorded

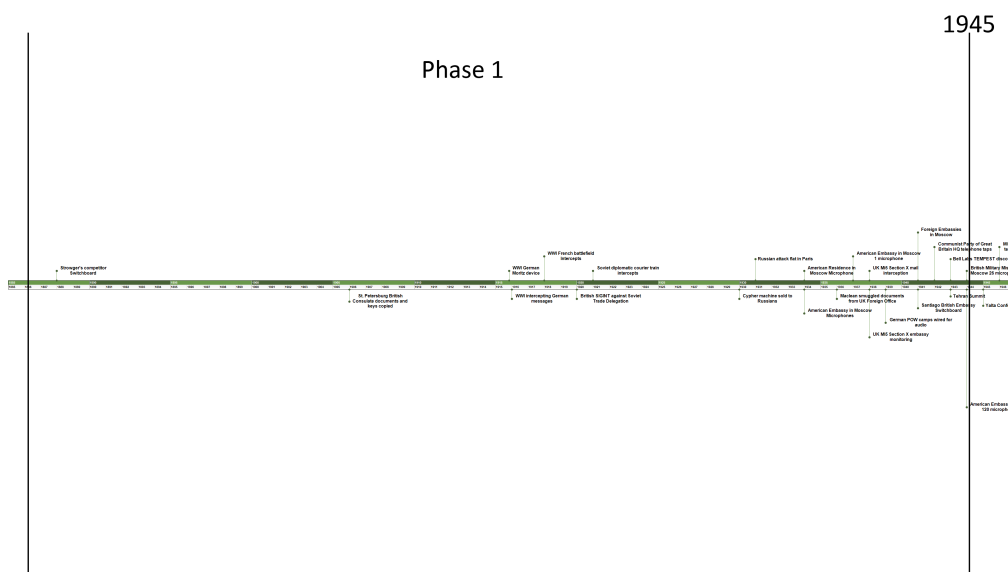


Figure B.2: Timeline of eavesdropping events from circa 1900 to 1945.

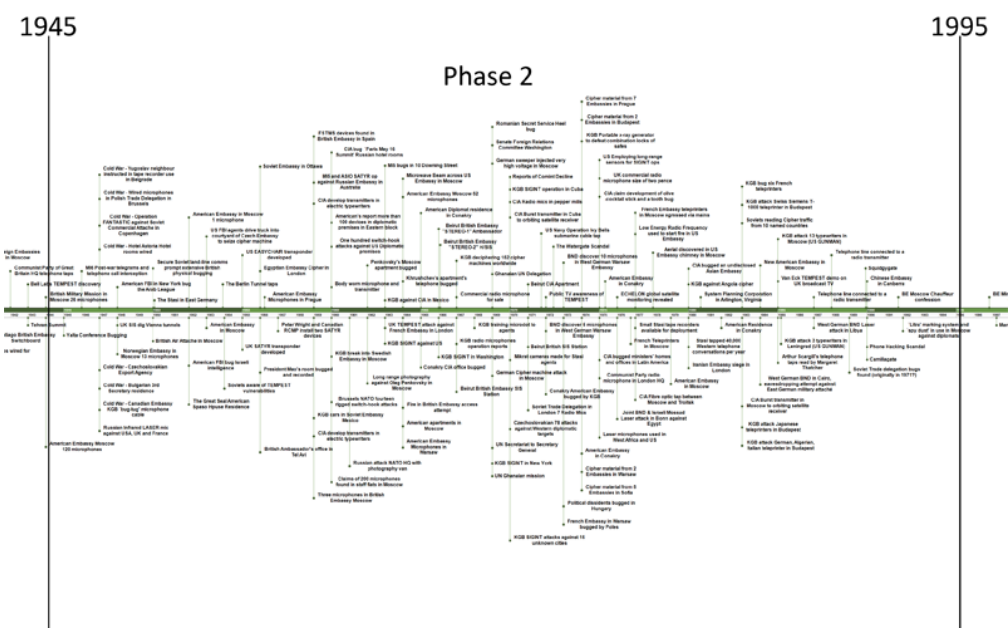


Figure B.3: Timeline of eavesdropping events from circa 1945 to 1995.

Phase 3

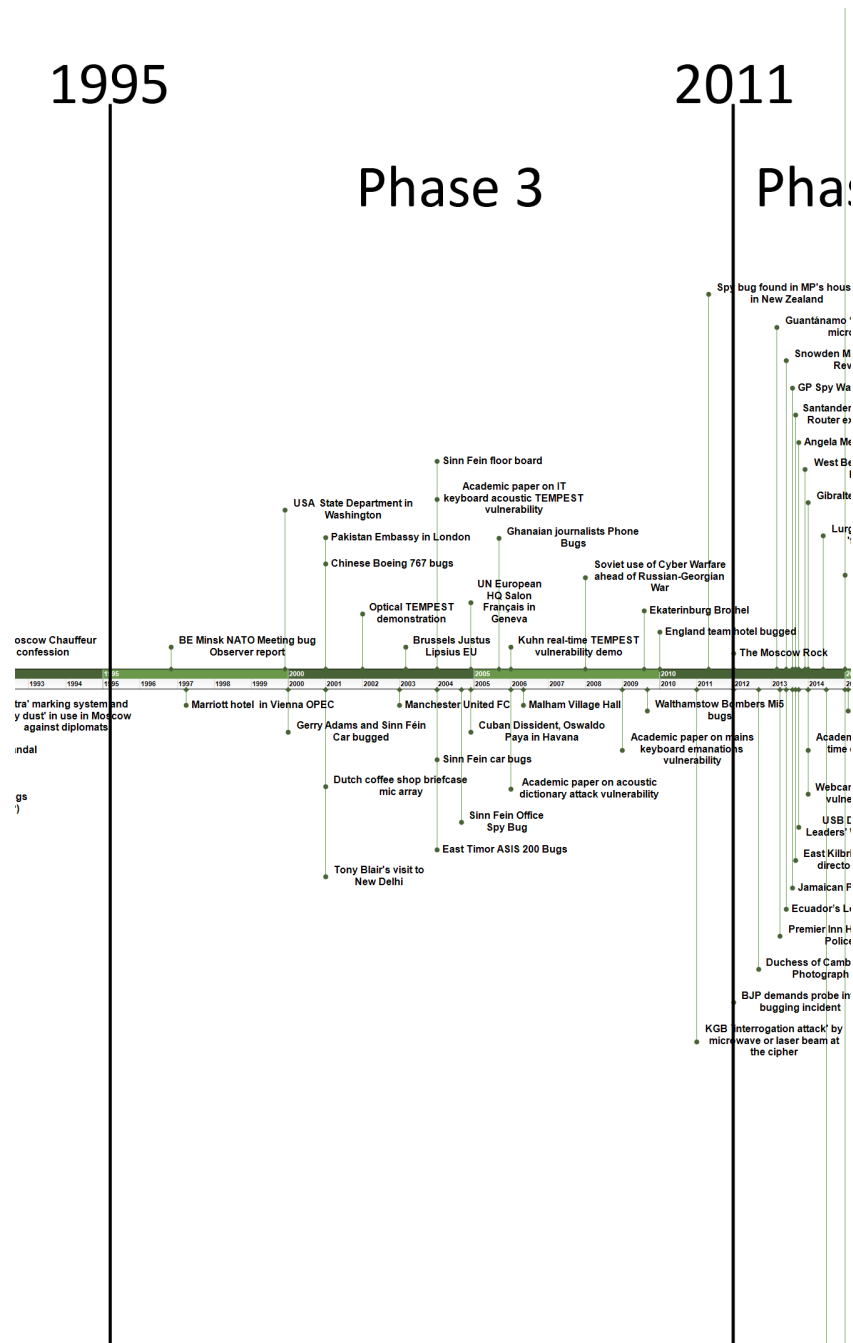


Figure B.4: Timeline of eavesdropping events from circa 1995 to 2011.

Phase 4

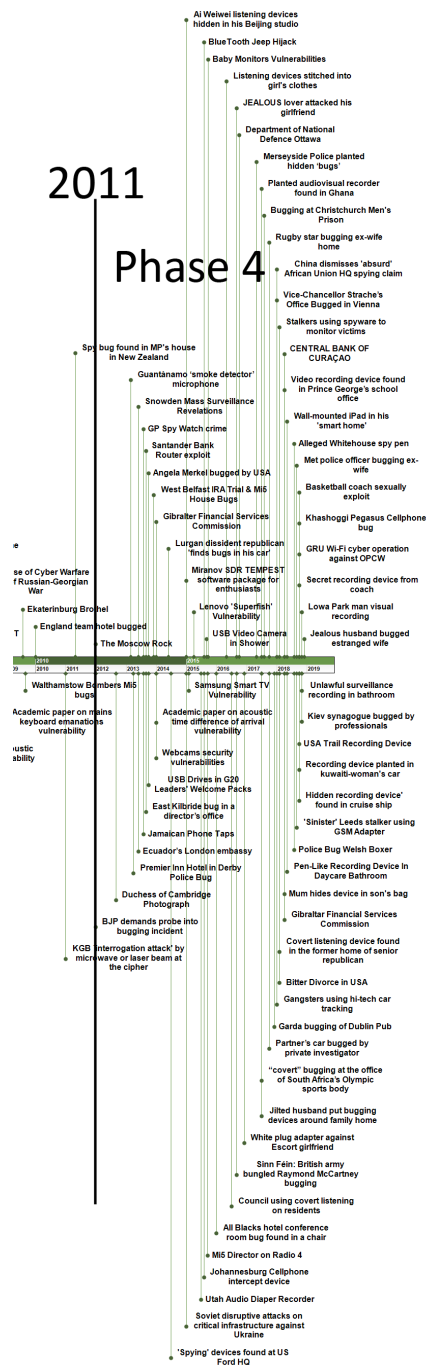


Figure B.5: Timeline of eavesdropping events from circa 2011 to 2019.

Appendix C

Timelines and Technology Life Cycles

C.1 Timeline of Techniques First Seen

In addition to the eavesdropping system model in Figure 3.1 an analysis of the year when a surveillance technique was first seen is plotted on a graph, Figure C.1 illustrates the number of surveillance technologies first seen between the years 1900 to 2015.

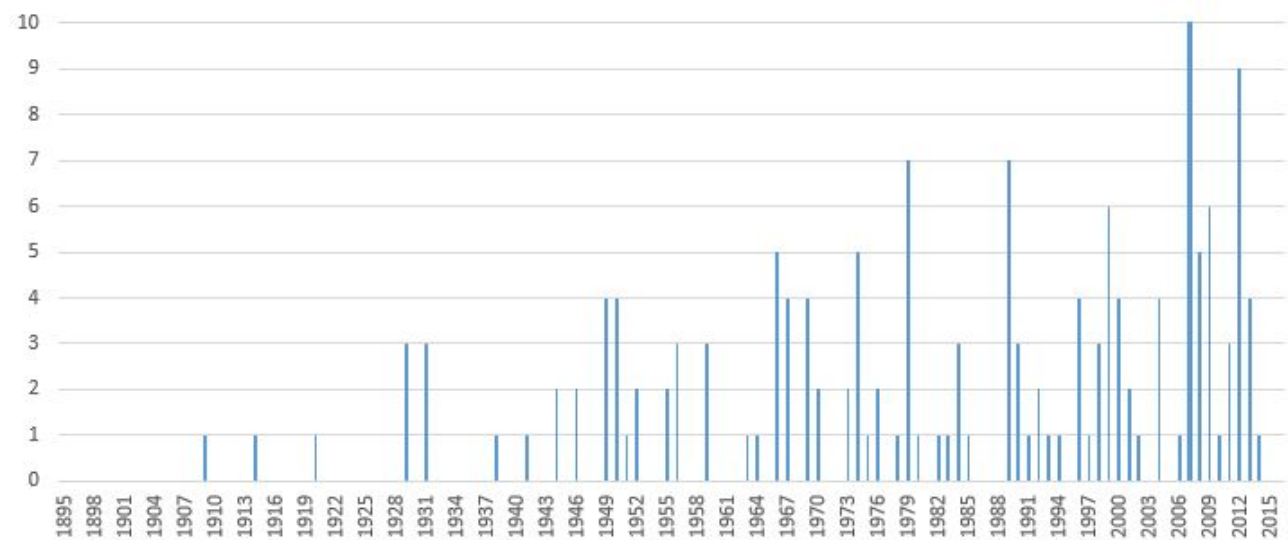


Figure C.1: Eavesdropping technologies introduced.

Figure C.2 plots technologies on a timeline which illustrates that the number of intrusive surveillance techniques available over the period has been increasing. This is contrary to the observation made for the general technology introduction in Figure 4.9.

One technology which has quickly evolved over the last 20 years is the mobile telephone. Each evolution has presented the intrusive surveillance industry with a new challenge in order to ensure continued surveillance possibilities. Figure C.3 illustrates on a timeline the evolutionary steps of mobile telephone technology development, while those below the timeline indicate the intrusive surveillance attack techniques that evolved to keep pace with these developments.



Figure C.2: Timeline of eavesdropping technology introduction.

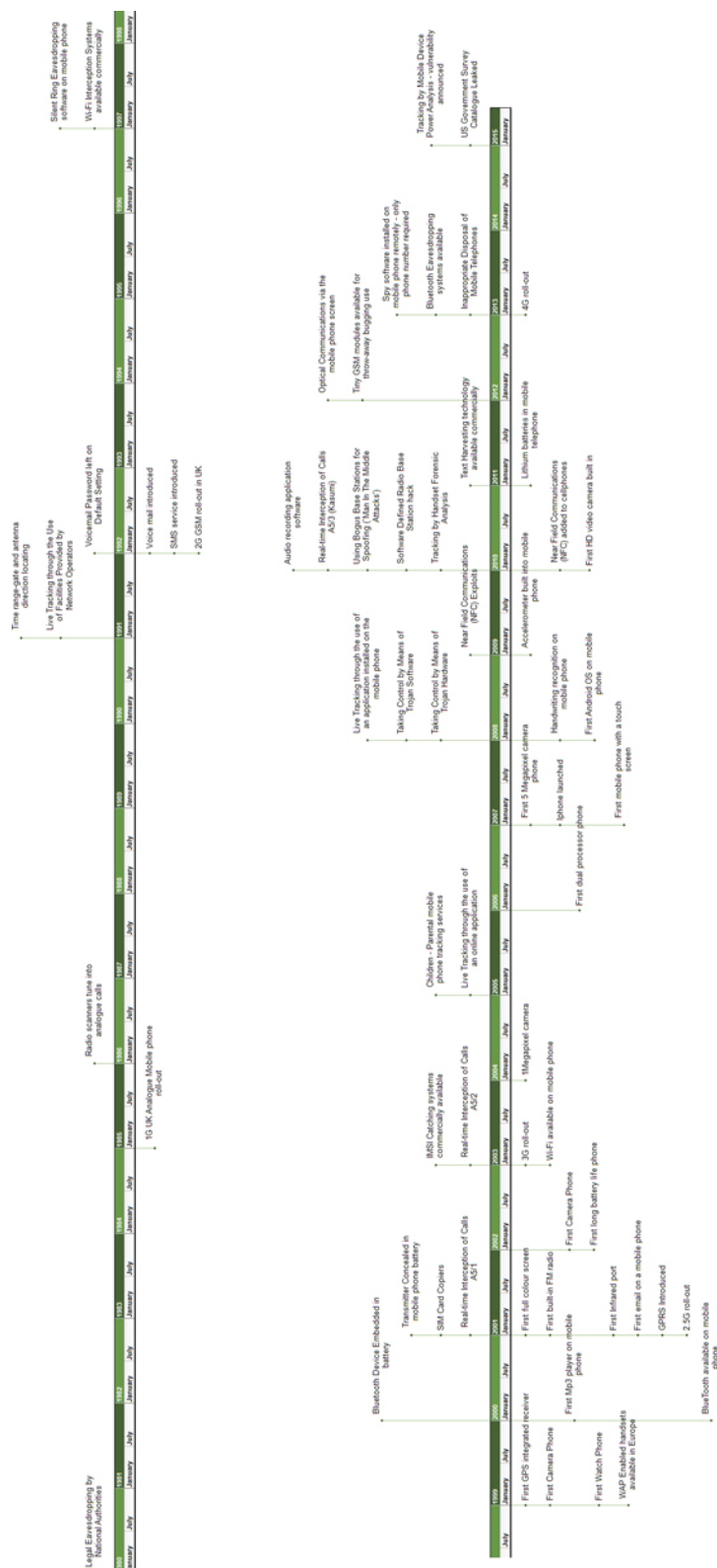


Figure C.3: Timeline cellphone development.

Eavesdropping Year First Seen 1900 - 1959

Year	Technology
1900	The insider threat
1900	Conference room facility vulnerabilities
1900	Acoustically poor conference rooms
1900	Event staff
1900	Paper assets
1900	Document eavesdropping by photography
1900	Agent communications
1909	Public switched telephone network taps
1914	Simple inductive taps
1920	Telephone lines
1929	Podium microphones
1929	Mains egress data or audio systems
1929	Parabolic microphone
1931	Deep plant devices built-in during construction
1931	Concealed microphones
1931	Wired microphones
1938	Disguised receiving antennas
1941	Security cameras in the high street or protecting homes
1944	Very low light systems
1944	Systems that operate in the dark
1946	Probe microphones
1946	Concealed in walls - microphone attached to a sound tube
1949	Buttons with concealed camera lens
1949	Long-range video systems
1949	Microphones created from loudspeakers
1949	Radio frequency illumination for audio eavesdropping
1950	Compromised analogue telephones
1950	Microphone created by switch-hook bypass in analogue telephone
1950	Analogue recorders using tape or wire
1950	Microphone created by switch-hook bypass in an analogue telephone
1951	Concealed cabling within other building components
1952	Conference room radio microphone systems
1952	PABX and VoIP telephones
1955	Microphones concealed in telephone equipment
1955	Shotgun or rifle microphone
1956	Radio microphones
1956	Commercially available radio microphone
1956	Broadcast radio (wirefree) microphone
1959	Visitors wired with sound and vision
1959	Accelerometers attached to structural elements
1959	First generation laser microphone

Table C.1: Eavesdropping year first seen 1900-1959.

Eavesdropping Year First Seen 1963-1984

Year	Technology
1963	Tracking and beacon systems
1964	Items compromised in transit
1966	Long-range drilling
1966	Projectors and projection systems
1966	Telephone line connected to a radio transmitter
1966	Magnetic loop transmission systems
1966	TEMPEST - Radio frequency emanations
1967	Telephone modified to become microphonic
1967	Telephone line egress of microphone audio with low frequency carrier
1967	Long-range photography enabled text analysis of keyboard entry
1967	Long-range photography enabled touchscreen snooping
1969	Modified typewriters
1969	In-house hand-held radios (Security Officers' radios)
1969	Second generation laser microphone
1969	Dragonfly insectothopter
1970	Modified intercom systems
1970	Modified teleprinters
1973	Telephone line egress of microphone audio through remote activation
1973	Phased array microphones
1974	Modified calculators
1974	Pens with RF speech transmitters
1974	Infrared communications systems
1974	Microphones attached to very thin wires
1974	Contact microphones
1975	Photography - Long-range with telephoto lens
1976	Cordless telephone eavesdropping
1976	Analogue cordless telephones
1978	Disposal chain
1979	Intentionally compromised electronics (supply chain attacks)
1979	Near silent drilling
1979	Self-drilling microphone
1979	Exchange and Mart radio microphone kits
1979	Microwave links for voice or data
1979	Baby monitor
1979	Third generation laser microphone
1980	Eavesdropping through local software execution
1982	Legal eavesdropping by national authorities
1983	Gap jumpers
1984	Exploiting building management system (BMS) installations
1984	Silent drilling
1984	Mobile telephone network operators taps

Table C.2: Eavesdropping year first seen 1963-1984.

Eavesdropping Year First Seen 1985-2004

Year	Technology
1985	Compromised IT hardware
1989	Redundant computer equipment
1989	Neckties with concealed cameras
1989	Taking control by means of trojan hardware
1989	Transmitter concealed in cellphone battery
1989	Voicemail password left on default setting
1989	Fourth generation laser microphone
1989	TEMPEST NONSTOP and HIJACK
1990	GSM in UK
1990	Webcams
1990	Live tracking through the use of facilities provided by network operators
1991	Modified photocopiers
1992	USB connecting leads to users' laptops
1992	Infrared headphones
1993	Digital cordless telephones
1994	Infrared translation systems
1996	Wi-Fi or Bluetooth wireless systems
1996	Taking control by means of trojan software
1996	Silent ring eavesdropping
1996	Fibre microphones
1997	Bluetooth
1998	Keyboard eavesdropping - Hardware-based keyloggers (external)
1998	Keyboard eavesdropping - Hardware-based keyloggers (internal)
1998	Wi-Fi interception systems
1999	Plugging memory sticks into unknown equipment
1999	Audio eavesdropping - Hardwired internal microphones
1999	MP3 recorders
1999	USB memory stick
1999	Hidden spy cams
1999	Personal computer hot-wired
2000	Pens with audio recorders
2000	Broadband and fibre to the cabinet
2000	Fibre optic eavesdropping
2000	SIM card copiers
2001	iPods
2001	TEMPEST - optical emanations
2002	IMSI catching
2004	Pens with digital video recorders
2004	Pens with video transmitters
2004	Bluetooth device embedded in battery
2004	Inappropriate disposal of mobile telephones

Table C.3: Eavesdropping year first seen 1985-2004.

Eavesdropping Year First Seen 2006-2014	
Year	Technology
2006	Watches with cameras and USB memory
2007	Video eavesdropping - replaced video cables
2007	Keyboard eavesdropping - Radar illuminated
2007	Eavesdropping through server bios exploitation
2007	Eavesdropping through modified routers
2007	Eavesdropping through modified firewalls
2007	Eavesdropping through modified computers
2007	Laser free-space optical links
2007	Audio recording application software
2007	Radio frequency illumination for data eavesdropping
2007	TEMPEST - optical reflections from other objects
2008	Eavesdropping through modified USB ports
2008	Mains egress data or audio systems
2008	Audio-video surveillance using a covert mains carrier system
2008	Mains socket bug
2008	HomePlug
2009	Tablets
2009	FTTC roll out
2009	Real-time interception of calls
2009	Tracking by handset forensic analysis
2009	Using bogus base stations for spoofing ('Man in the middle' attacks)
2009	Near field communications (NFC)
2010	Live tracking through the use of an application installed on the handset
2011	Digitally encrypted radio microphone
2011	GSM bug
2011	Optical communications via the screen
2012	Disguised equipment cases
2012	Professional grade credit card recorder
2012	Pens with handwriting capture
2012	Smart glasses
2012	Overt Li-Fi
2012	Covert Li-Fi
2012	Bluetooth interception
2012	Bluetooth eavesdropping
2012	Live tracking through the use of an online application
2013	Video eavesdropping - external KVM switches
2013	Optical microphones
2013	Long-range photography enabled by drones
2013	TEMPEST - acoustic emanations
2014	Tracking by mobile device power analysis

Table C.4: Eavesdropping year first seen 2006-2014.

Appendix D

Technology Life Cycles

D.1 Additional Technology Life Cycle Results

The results are presented in sixteen groups of similar technologies. The results show the technique identity number and description, the average and the weighted average x-axis position of all ten subject experts and the life-cycle phase (growth, maturity or decline). None of the technologies plotted were recorded as being in the invented or extinct phases of the life-cycle.

Technique	Average	Weighted Average	Life cycle
[59] Physical Covert Entry	66.6	64.6	Maturity
[32] Covert Document Photography	76.5	73.8	Maturity
[21] Necktie Camera	79.3	79.1	Decline
[29] Button Camera	75.8	74.3	Maturity
[79] Long-range telephotography	59.5	56.8	Maturity
[12] RF Video Transmitter Pen	74.1	72.9	Maturity
[18] Video recording Pen	71.6	70.2	Maturity
[34] Covert mains AV system	62.7	61.2	Maturity
[29] Button Camera	74.5	73.7	Maturity
[13] Smart Glasses for audio and video	54.7	54.2	Maturity
[28] Probe microphone	73.6	73.2	Maturity
[26] Contact microphone	72.6	70.8	Maturity
[48] Accelerometer	66.6	64.2	Maturity
[33] Thin-wire egressed microphone	77.2	76.3	Maturity
[36] Fibre microphone	64.4	62.9	Maturity
[82] Self-Drilling Microphone	78.2	78.0	Maturity
[71] Magnetic induction loop audio transmitter	67	65.4	Maturity
[64] Rigged Switch hooks	92	90.8	Decline

[19] PC Hot-wired microphone	70.6	69.6	Maturity
[24] Infra-red audio transmitters	77.3	77.8	Maturity
[25] Silent Ring mobile phone	64.9	62.8	Maturity
[17] iPod Recorder	72.9	71.9	Maturity
[61] Samsung TVs vulnerability	54	52.1	Maturity
[44] Wood-block transmitters	90.4	90.4	Decline
[11] RF Audio Transmitter Pen	83.6	82.9	Decline
[30] Law Enforcement Radio Microphone	63.8	63.5	Maturity
[39] Broadcast radio microphone	69.2	69.7	Maturity
[37] Digitally Encrypted Radio Microphone	63.2	62.5	Maturity
[8] Shotgun - Directional Microphone	80.7	81.1	Decline
[20] Parabolic Microphone	83	82.7	Decline
[27] Phased-Array Microphone	65.5	63.3	Maturity
[67] LASER Microphone - optical lever technique	74	73.8	Maturity
[68] LASER Microphone - against a retro reflector	65.5	64.3	Maturity
[69] LASER Microphone - speckle interferometry	56.7	54.7	Maturity
[9] Bluetooth Interception	50.9	47.7	Maturity
[89] Host Government Legal Intercept	60.2	58.7	Maturity
[78] PSTN Tap	81.3	81.2	Decline
[80] PABX exploits	85.5	85.0	Decline
[5] Simple Inductive Telephone Tap	92	91.9	Decline
[77] GSM Network Operator Tap	60.8	60.5	Maturity
[74] Real-time Cell Phone Interception	52.1	51.7	Maturity
[51] RF Audio Illumination Passive (The Great Seal)	92.2	92.1	Decline
[52] MI5 SATYR Audio Transponder	88	88.0	Decline
[53] AudioTel SABRE Audio Transponder	78.2	76.9	Maturity
[54] NSA ANT PlaySet Video Transponder	54	51.6	Maturity
[87] City Microwave Eavesdropping	69.5	68.0	Maturity
[88] Country-wide Satellite Eavesdropping	64.1	63.9	Maturity
[38] IMSI Catching	59.4	59.5	Maturity
[72] Bogus cell phone base station	52.4	50.9	Maturity
[58] Wi-Fi Interception	53.7	54.9	Maturity
[84] BELL Labs TEMPEST Discovery	89.8	88.7	Decline
[50] RF TEMPEST	73.3	71.4	Maturity
[57] Optical TEMPEST	70.1	65.6	Maturity
[43] Video Cable modified for enhanced egress	55.2	52.0	Maturity
[83] Marinov TEMPEST software for SDR Rx	57.2	57.0	Maturity
[42] Acoustic TEMPEST	66.8	64.4	Maturity
[86] Acoustic keyboard finger printing	62.4	60.5	Maturity
[35] Covert Li-Fi	38	38.4	Growth
[40] Modified Typewriter attack	97.6	98.1	Decline
[49] Modified Teleprinter	99.6	99.5	Decline
[73] Modified Cypher machine	84	82.0	Decline
[14] Keyboard keylogger using External Hardware	75.6	75.8	Maturity
[15] Keyboard keylogger using Internal Hardware	69.9	69.7	Maturity
[23] Video Eavesdropper by External KVM	68.2	68.7	Maturity
[41] USB Port Modification	56.2	55.2	Maturity
[45] Modified Router or Firewall	56.2	56.0	Maturity
[46] BIOS Exploit	53.4	54.4	Maturity
[47] Keyboard Illumination by Radar	73.8	71.5	Maturity
[55] Trojan Software Control	50.8	53.0	Maturity
[56] VoIP interception and exploits	52.2	52.7	Maturity
[65] IT Network intrusion attack	51.4	50.7	Maturity
[66] Criminal credit card extraction	59.5	58.1	Maturity
[60] Personal data extraction or theft	53.3	52.2	Maturity

[81] Zero-day exploit	42.2	43.2	Maturity
[85] Mezon miniature wire tape recorder	92	91.9	Decline
[63] Burst radio transmitter	64	61.9	Maturity
[70] Digital MP3 recorder	73.4	73.1	Maturity
[76] Credit card recorder	62.6	62.8	Maturity
[1] Exchange & Mart Radio Microphone kit	82	80.8	Decline
[2] Mains two-way adapter bug	75.3	74.0	Maturity
[3] Audio Recording Pen	75.4	75.4	Maturity
[4] GSM Audio SIM Card Bug	62.1	62.2	Maturity
[6] Hidden Spy Camera	67.4	67.2	Maturity
[10] Spy Watch for audio or video	72.2	71.2	Maturity
[16] USB Memory Stick audio bug	62.8	62.6	Maturity
[7] Tracking Beacon	60.2	58.4	Maturity
[22] Live Tracking with a Smartphone App	56.9	56.3	Maturity
[31] Handset Forensic Tracking	55	53.2	Maturity
[62] Live Tracking Mobile Network Operator	55.1	54.2	Maturity
[75] Live tracking through online function	49	49.4	Maturity

Table D.1: Weighted average timeline positions of 16 groups of eavesdropping technologies.

Table D.1 illustrates the results within the sixteen groups, together with the growth, maturity, decline label.

Appendix E

Capability and Opportunity Plots

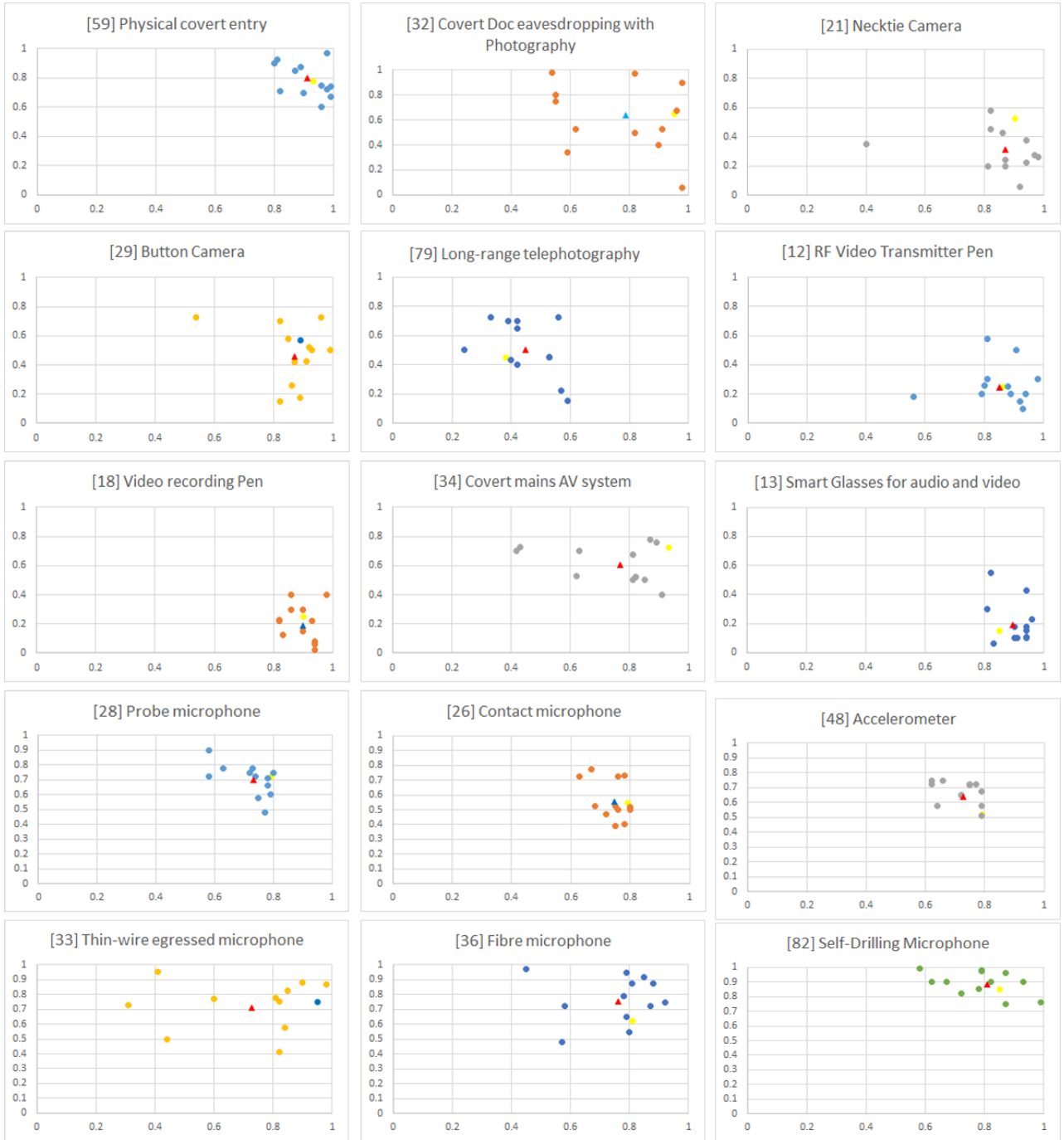


Figure E.1: Capability against opportunity plots.

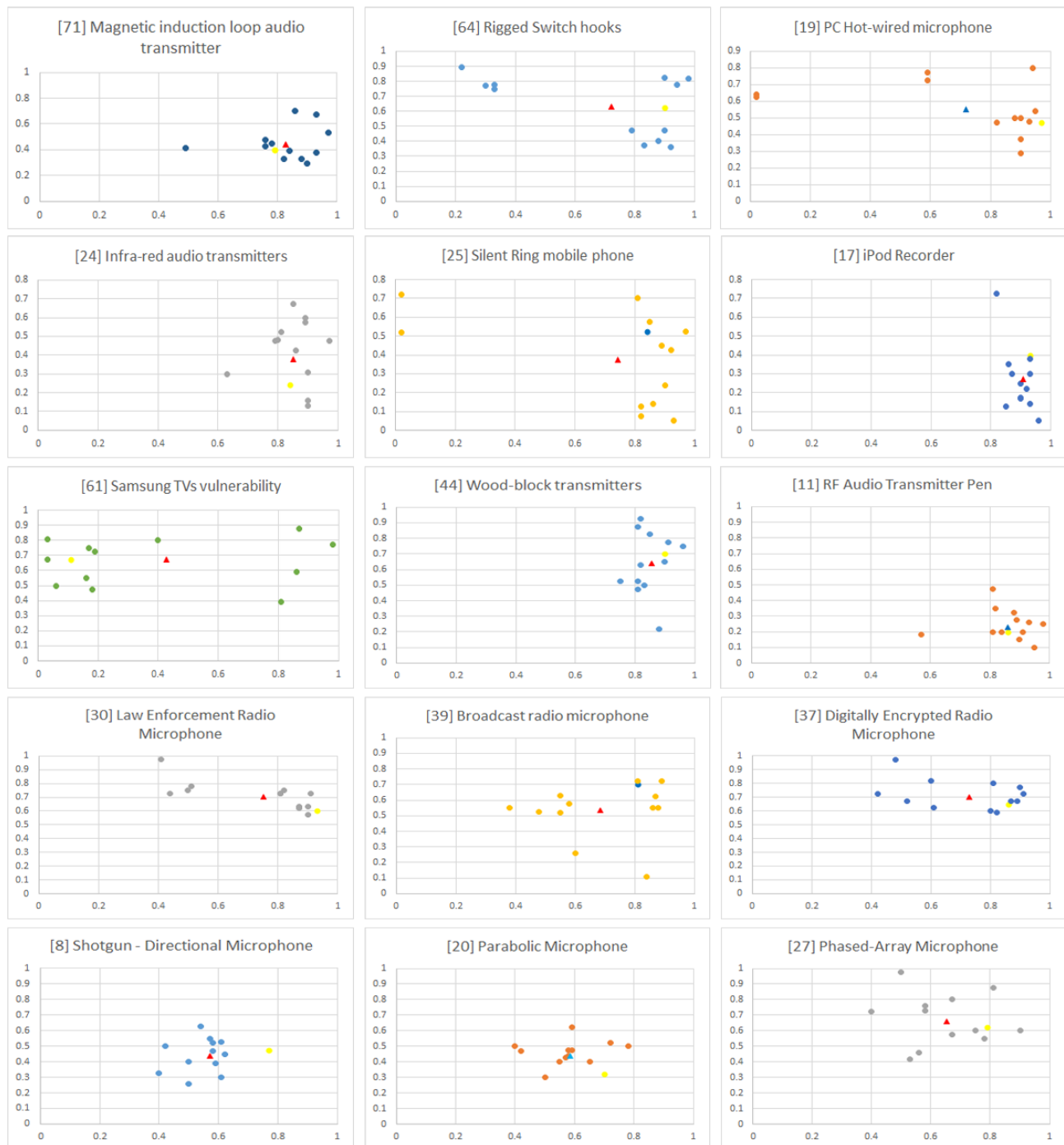


Figure E.2: Capability against opportunity plots.

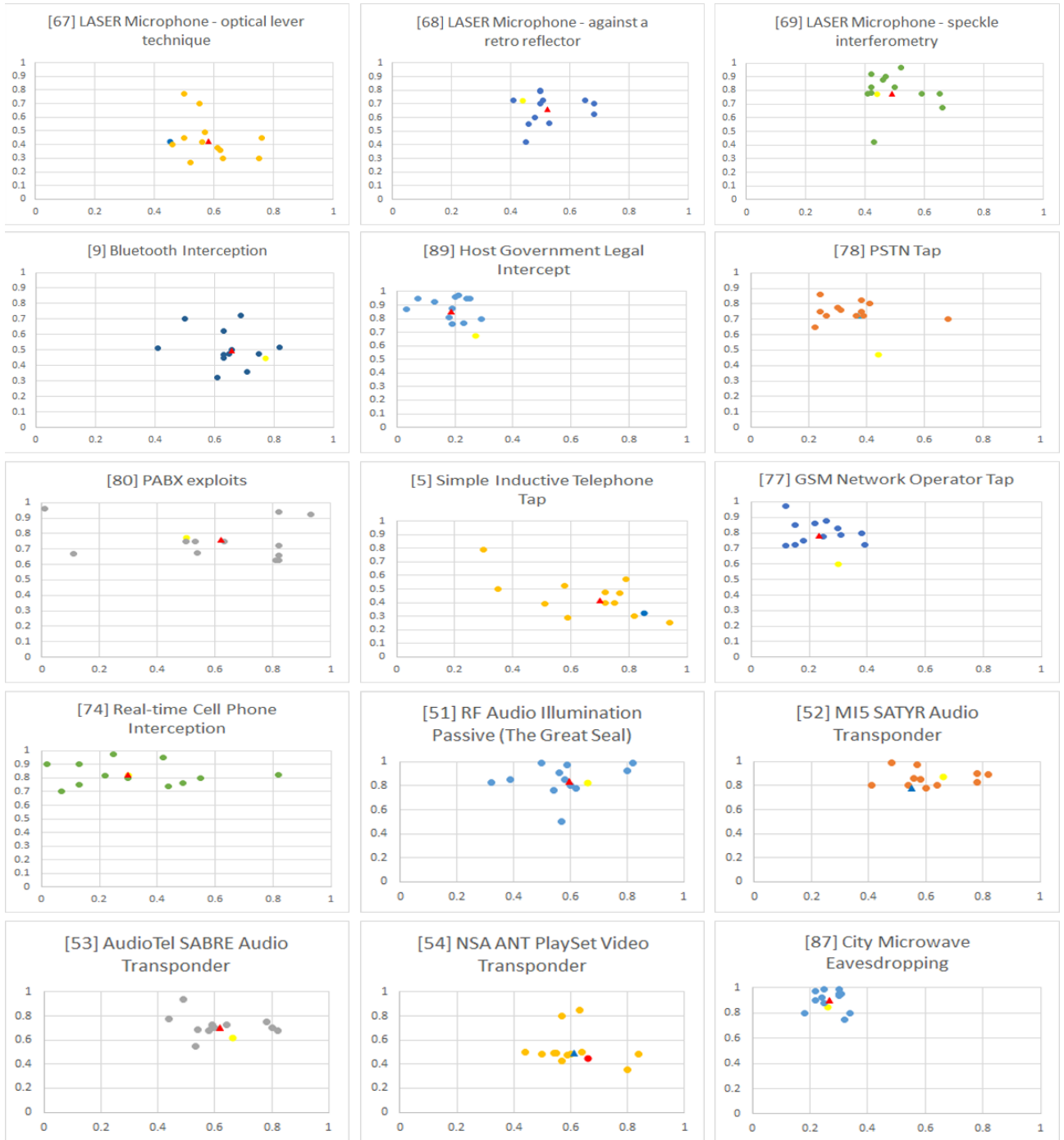


Figure E.3: Capability against opportunity plots.

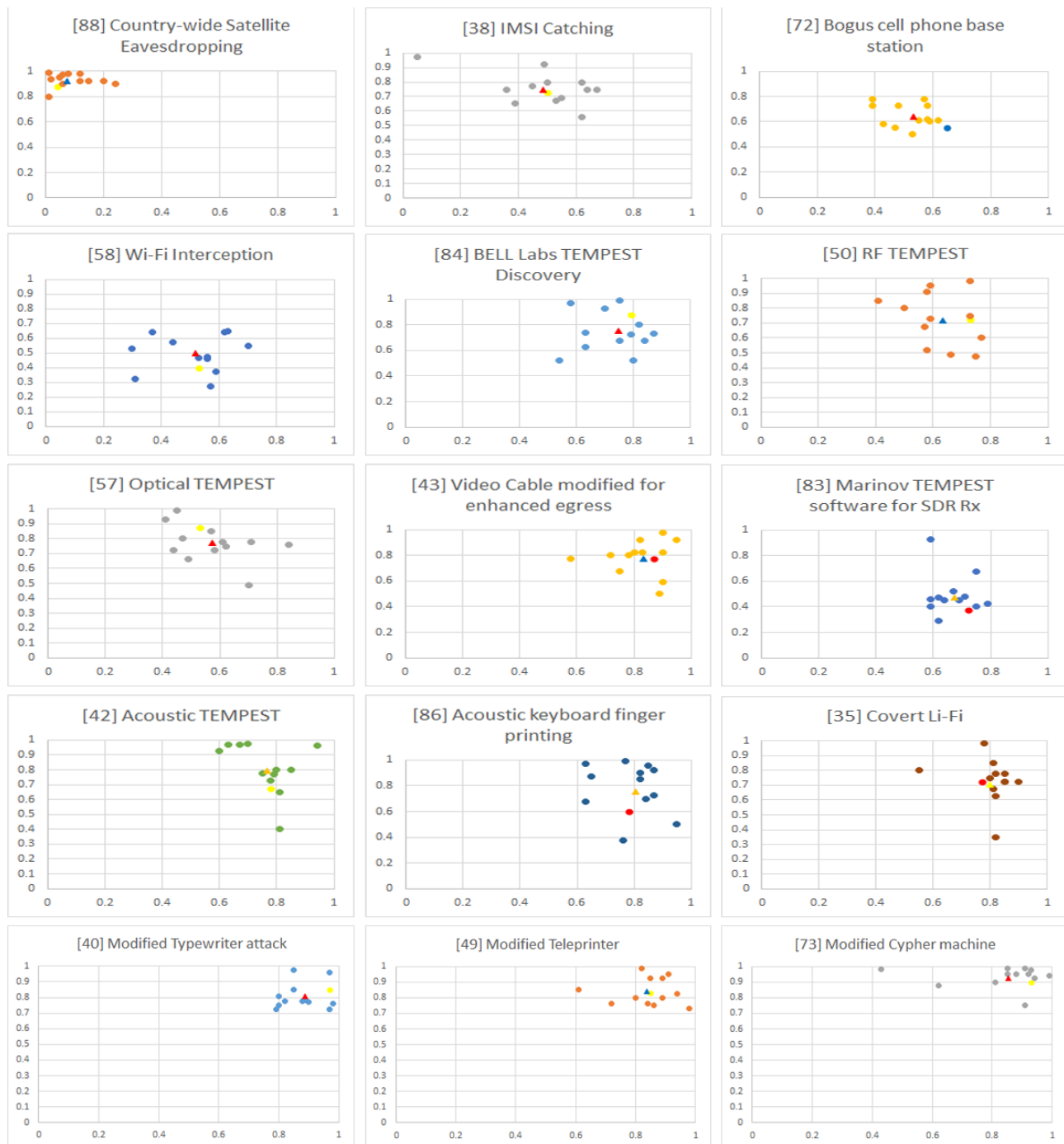


Figure E.4: Capability against opportunity plots.

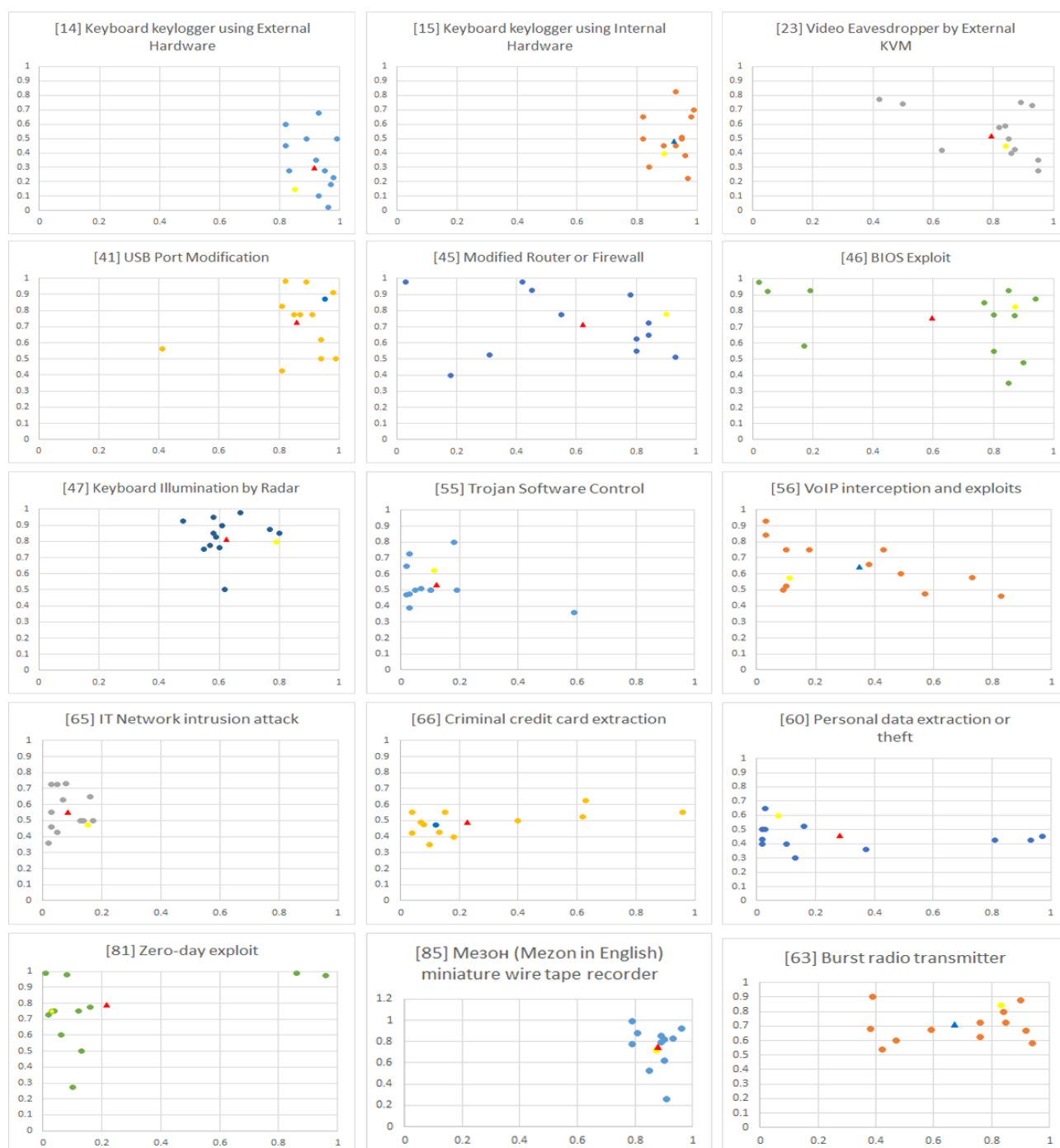


Figure E.5: Capability against opportunity plots.

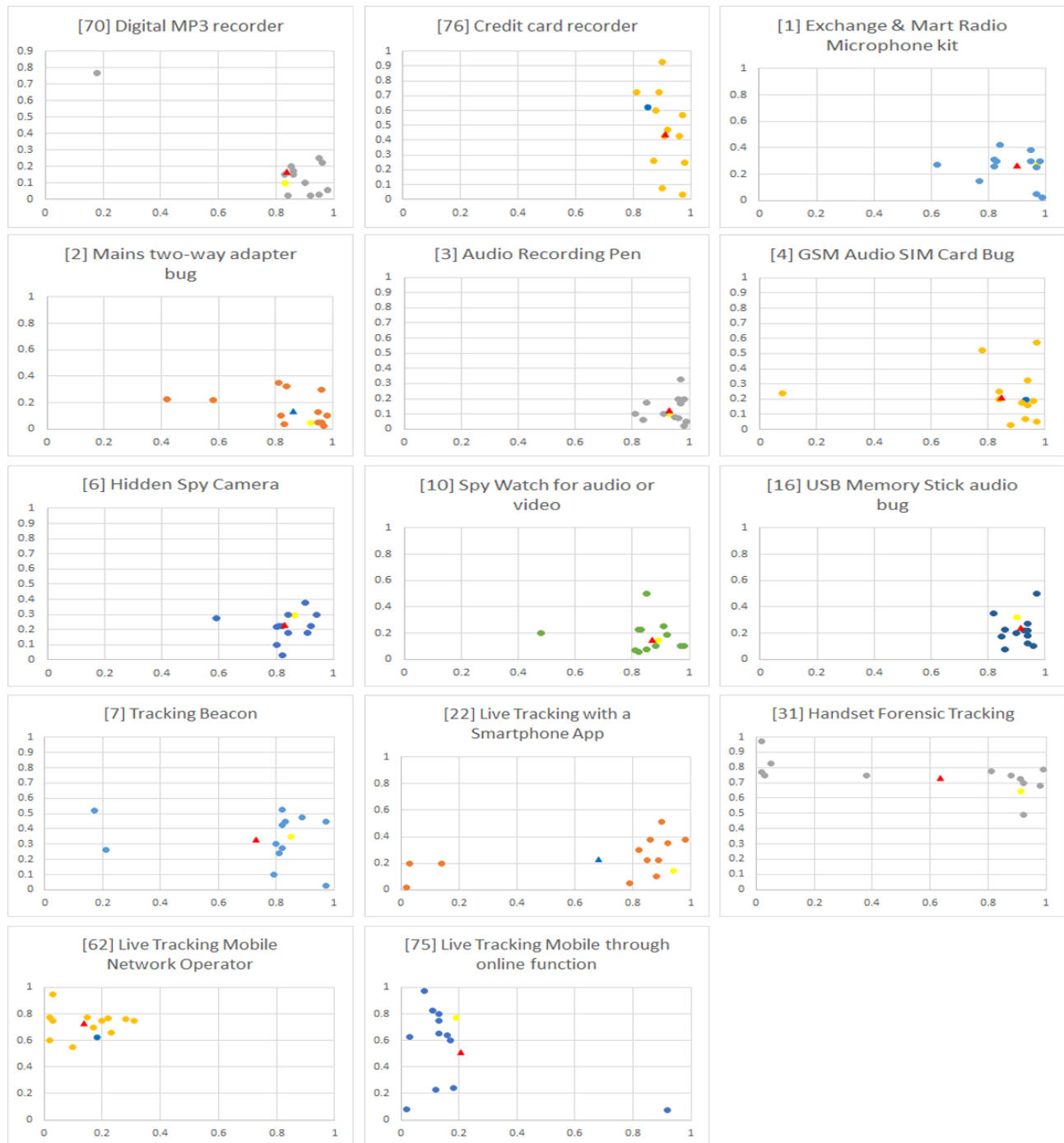


Figure E.6: Capability against opportunity plots.

Appendix F

Future Work

The following tables map the egress routes to eavesdropping techniques:

- Table F.1 - Telephone line enabled;
- Table F.2 - Internet enabled;
- Table F.3 - Dedicated wiring enabled;
- Table F.4 - Physical access enabled;
- Table F.5 - Mobile telephony enabled;
- Table F.6 - Optical enabled;
- Table F.7 - Radio enabled;
- Table F.8 - Electromagnetic enabled.

Telephone Line Enabled	
Simple inductive taps	Telephone line egress of microphone audio through remote activation
Cabling infrastructure (tampering and patching)	Telephone line egress of microphone audio with low-frequency carrier
Public telephone network	Telephone speech interception
PABX exchange exploits	Telephone fax interception
Microphone created by switch-hook bypass in analogue telephone	Broadband data interception
Modified telephone to become microphonic	Fibre or “fibre to the cabinet” interception
Microphones concealed in telephone equipment	Fibre optic eavesdropping

Table F.1: Eavesdropping techniques enabled by telephone line egress.

Internet Enabled	
Plugging memory sticks into unknown equipment	Tablets
Keyboard eavesdropping - Hardware-based keyloggers (internal)	Smartphones with cameras, microphones, accelerometers and apps
Eavesdropping through modified USB ports	Overt Li-Fi
Hardware eavesdropping on networks via computer power lines	Covert Li-Fi
Video eavesdropping - Built-in applications	Webcams
Audio eavesdropping - Built-in applications	Security cameras in the high street or protecting homes (digital)
Eavesdropping through server bios exploitation	Wi-Fi interception systems
Eavesdropping through modified router software	HomePlug data sharing
Eavesdropping through modified firewall software	Legal eavesdropping by national authorities
Eavesdropping through local software execution - zero day	Taking control by means of trojan software
VoIP telephones	Live tracking through the use of an online application

Table F.2: Eavesdropping techniques enabled by internet egress.

Dedicated Wiring Enabled	
Microphones egressed via very thin wires	Personal computer hot-wired
Podium microphones	Audio eavesdropping - hardwired internal microphones
Wired microphones	Modified intercom systems
Optical fibre microphones	Security cameras in the high street or protecting homes (analogue)
Deep-plant microphones built-in during construction	Audio-video surveillance using a covert mains carrier system
Deep-plant accelerometers built-in during construction	Contact microphones
Self-drilling microphone	Concealed in walls - Microphone attached to a sound tube
Gap jumpers egressing secure environments	The probe microphone
Concealed cabling within other building components	Microphones created from loudspeakers

Table F.3: Eavesdropping techniques enabled by dedicated wiring egress.

Physical Access Enabled	
Projectors and projection systems	Pens with audio recorders
USB connecting leads to users' laptops	Pens with digital video recorders
Acoustically poor conference rooms	Cameras concealed inside everyday objects
Event staff uncontrolled and non-vetted	Smartglasses
Paper assets	Analogue recorders using tape or wire
Redundant computer equipment	SIM card copiers
Keyboard - hardware-based keyloggers (external)	TEMPEST - acoustic emanations
Keyboard - hardware-based keyloggers (internal)	Long-range drilling
Eavesdropping through printer hardware-based additions	Near-silent drilling
Document eavesdropping by photography	Silent drilling
Neck-ties with concealed cameras	Directional microphones
Buttons with concealed camera lens	Shotgun or rifle microphone
Modified photocopiers	Phased-array microphones
Access to hard drive within photocopier	Parabolic microphone
Modified shredders	Near-Field communications (NFC)
Professional grade credit card recorder	Taking control by means of trojan hardware
MP3 recorders	Inappropriate disposal of mobile telephones
iPods with built-in recording devices	Tracking by handset forensic analysis
USB memory stick with audio recorders	Tracking by mobile device power analysis
Watches with cameras and USB memory	

Table F.4: Eavesdropping techniques enabled by physical access egress.

Mobile Telephony Enabled	
Mobile telephone network operators taps	Acoustic eavesdropping through wireless vibrometry
Legal interception	Audio recording application software
GSM Bug	Taking control by means of trojan software
Real-time interception of calls - analogue	Silent-ring eavesdropping
Real-time interception of calls - digital GSM	Voicemail password left on default setting
IMSI catching	Live tracking through the use of facilities provided by network operators
Using bogus base stations for spoofing ('man in the middle' attacks)	Live tracking through the use of an application installed on the handset
Speech from smartphone gyroscope	Live tracking through the use of an online application

Table F.5: Eavesdropping techniques enabled by mobile telephony egress.

Optical Enabled	
Long-range video systems	Infrared headphones
Very low-light systems	Infrared translation systems
TEMPEST - Optical emanations	Particulate flow detection microphone
TEMPEST - Optical reflections from other objects	Photography - long-range with telephoto lens
Laser free-space optical links	Long-range photography enabled lip reading
First generation laser microphone	Long-range photography enabled text analysis of keyboard entry
Second generation laser microphone	Long-range photography enabled touchscreen snooping
Third generation laser microphone	Long-range photography enabled by drones
Fourth generation laser microphone	

Table F.6: Eavesdropping techniques enabled by optical egress.

Radio Enabled	
Conference room radio microphone systems	In-house hand-held radios (security officers' radios)
Video eavesdropping - non-TEMPEST equipment	Baby monitor
Video eavesdropping - external KVM switches	TEMPEST - radio frequency emanations
Video eavesdropping - replaced video cables	TEMPEST NONSTOP and HIJACK
Keyboard eavesdropping - radar illuminated	Bluetooth interception
Telephone line connected to a radio transmitter	Microwave voice and data interception
Modified calculators	Magnetic-loop transmission systems
Modified typewriters	Mains socket bug
Modified teleprinters	Radio frequency illumination for audio eavesdropping
Modified printers	Radio frequency illumination for data eavesdropping
Pens with RF speech transmitters	Bluetooth eavesdropping
Pens with video transmitters	Transmitter concealed in cellphone battery
Government manufactured	Bluetooth device embedded in battery
Digitally encrypted radio microphone	Bumper beacon systems
Commercially available radio microphone	HF radio interception
Exchange and Mart radio microphone kits	Comms interception
Analogue cordless telephones	Satellite interception
Digital cordless telephones	Microwave interception

Table F.7: Eavesdropping techniques enabled by radio egress.

Electromagnetic Enabled	
Induction loops for t-coil hearing aids	Assisted hearing technology interception

Table F.8: Eavesdropping techniques enabled by electromagnetic egress.

Bibliography

- "Oxford Internet Institute" (2019). *Global Open Data Index Place Overview*. URL: <https://index.okfn.org/place/> (visited on 2019-09-03).
- Alberts, C. et al. (1999). *Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, Version 1.0*. Tech. rep. DTIC Document.
- Aldrich, R. (2011). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. HarperPress. ISBN: 9780007312665.
- Aldrich, R.J. (2006). *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*. G Duckworth. ISBN: 9780715636077.
- Alexander's Gas & Oil Connections (Apr. 14, 1997). "Eavesdropping on OPEC in Vienna hotel". In: *Alexander's Gas & Oil Connections*. URL: <http://www.gasandoil.com/news/europe/621afd571ca3076830a8f2952458a311> (visited on 2019-08-08).
- Allard, T. (Mar. 15, 2006). "ASIS chief Nick Warner slammed over East Timor spy scandal". In: *The Sydney Morning Herald*. URL: <https://www.smh.com.au/politics/federal/asis-chief-nick-warner-slammed-over-east-timor-spy-scandal-20160315-gnjpne.html> (visited on 2019-08-08).
- (Mar. 4, 2014). "Australia ordered to cease spying on East Timor by International Court of Justice". In: *The Sydney Morning Herald*. URL: <https://www.smh.com.au/politics/federal/australia-ordered-to-cease-spying-on-east-timor-by-international-court-of-justice-20140304-hvfya.html> (visited on 2019-08-08).
- Andress, J. and S. Winterfeld (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier Science. ISBN: 9780124166332.

- Andrew, C.M. (1985). *Secret service : the making of the British intelligence community*. London: Heinemann. ISBN: 9780434021109.
- (2009). *The Defence of the Realm: The Authorized History of MI5*. Allen Lane. ISBN: 9780713998856.
- Andrew, C.M. and O. Gordievsky (1991). *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*. HarperPerennial. ISBN: 9780060921095.
- Andrew, C.M. and V. Mitrokhin (2000). *The Mitrokhin Archive: The KGB in Europe and the West*. Basic Books. ISBN: 9780140284874.
- (2006). *The Mitrokhin Archive II: The KGB and the World*. Penguin. ISBN: 9780140284881.
- Anon (May 10, 2003). “Martin McGuinness wiretap transcripts.” In: *cryptome.org*. URL: <https://cryptome.org/mcguinness-taps.htm> (visited on 2019-08-08).
- Appelbaum, J., J. Horchert, and C. Stöcker (2008). “Shopping for Spy Gear: Catalog Advertises NSA Toolbox”. In: *Spiegel Online International*. URL: <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>.
- Ash, T.G. (2007). *The Stasi on our Minds*. URL: <http://www.nybooks.com/articles/2007/05/31/the-stasi-on-our-minds/> (visited on 2019-09-06).
- Asonov, D. and R. Agrawal (2004). “Keyboard acoustic emanations”. In: *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*, pp. 3–11. DOI: 10.1109/SECPRI.2004.1301311.
- Atherton, W. (1988). “Pioneers. Pt. 19: Almon Brown Strowger(1839-1902): inventor of the automatic telephone exchange”. In: *Electronics and Wireless World* 94, pp. 677–8.
- Atkinson, J. (Dec. 19, 2004). “Technical Analysis of the UN Bug”. In: URL: <https://cryptome.org/un-bug.htm> (visited on 2019-08-08).
- Auty, M. (2015). “Anatomy of an advanced persistent threat”. In: *Network Security* 2015.4, pp. 13–16. ISSN: 1353-4858. DOI: 10.1016/S1353-4858(15)30028-3.
- Babcock, C. (2015). “Preparing for the Cyber Battleground of the Future”. In: *Air & Space Power Journal* 29.6, pp. 61–73. ISSN: 1555385X.

- Bailey, D (1950). *R6/3: An eavesdropping incident at the Moscow embassy. Report of an investigation made 4th - 13th Sept 1950*. Four Photographs and partial floor plan.
- Balzarotti, D., M. Cova, and G. Vigna (2008). *ClearShot: Eavesdropping on Keyboard Input from Video*. Conference Paper. IEEE Symposium on Security and Privacy, pp. 170–183. DOI: 10.1109/SP.2008.28.
- Bamford, J. (2009). *The Shadow Factory: The Ultra-secret NSA from 9/11 to the Eavesdropping on America*. Anchor Books. ISBN: 9780307279392.
- Barron, J. (1974). *KGB: the secret work of Soviet secret agents*. Reader's Digest Press; distributed by E. P. Dutton. ISBN: 9780883490099.
- (1983). *KGB Today: The Hidden Hand*. Berkley. ISBN: 978-0883491645.
- Baumgartner, K, S Ferrari, and G Palermo (2008). “Constructing Bayesian networks for criminal profiling from limited data”. In: *Knowledge-Based Systems* 21.7, pp. 563–572.
- Bayliss, C (Sept. 18, 2018). “Met police officer, 57, faces jail after ‘keeping tabs’ on ex-wife by bugging her bedroom with listening devices during three-year stalking campaign”. In: *The Daily Mail*. URL: <https://www.dailymail.co.uk/news/article-6181647/Met-police-officer-faces-jail-bugging-ex-wives-home-three-year-stalking-campaign.html> (visited on 2019-08-07).
- BBC (Sept. 6, 2004). “Sinn Fein displays ‘bugging device’”. In: *BBC*. URL: http://news.bbc.co.uk/1/hi/northern_ireland/3631750.stm (visited on 2019-08-08).
- (July 4, 2013). “Ecuador asks UK for help on embassy bug”. In: *BBC*. URL: <https://www.bbc.co.uk/news/uk-23179431> (visited on 2019-08-08).
- BBC2 (1985). *Tomorrow's World*. URL: <https://www.youtube.com/watch?v=mcV6izFG3vQ> (visited on 2019-09-06).
- Belgian Standing Intelligence Agencies Review Committee (Jan. 11, 2011). “Investigation report on the way in which the Belgian intelligence services dealt with the phone-tapping incidents in the offices of delegations to the European Union Council in Brussels (2010)”. In: *Belgian Standing Intelligence Agencies Review Committee: Investigation Reports*. URL: http://www.comiteri.be/images/pdf/eigen_publicaties/2006.173%20f.pdf (visited on 2019-08-08).

- Berger, Y., A. Wool, and A. Yeredor (2006). "Dictionary Attacks Using Keyboard Acoustic Emanations". In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*. CCS '06. Alexandria, Virginia, USA: ACM, pp. 245–254. ISBN: 1-59593-518-5. DOI: 10.1145/1180405.1180436. URL: <http://doi.acm.org/10.1145/1180405.1180436>.
- Bergquist, C. (2002). *Guide to Electronic Surveillance Devices*. Thomson/Delmar. ISBN: 9780790612454.
- Beria, S., F. Thom, and B. Pearce (2003). *Beria My Father: Inside Stalin's Kremlin*. Duckworth. ISBN: 9780715630624.
- Berton, K. (1991). *The British Embassy Moscow : The Kharitonenko Mansion*. British Embassy Moscow: Butler & Tanner Ltd. Frome and London, p. 80.
- Bezuidenhout, J. (July 20, 2017). "Police probe bugging at Sascoc's Olympic House". In: *Mail & Guardian*. URL: <https://mg.co.za/article/2017-07-20-police-probe-bugging-at-sascocs-olympic-house> (visited on 2019-08-07).
- Black, I. (Mar. 20, 2003). "Bugging devices found in EU offices". In: *The Guardian*. URL: <https://www.theguardian.com/world/2003/mar/20/eu.politics> (visited on 2019-08-08).
- Boondao, R (2008). "Crime risk factors analysis". In: *Bayesian Networks: A Practical Guide to Applications*, pp. 73–85.
- Boorstein, M.A. (1998). "History of the Construction of the American Embassy in Moscow". In: *MoscowVeteran.org*, pp.12. URL: <http://www.moscowveteran.org/pg/embassy-construction> (visited on 2019-09-06).
- Booth, R.D. (Sept. 11, 2017). "How Russian Spies Bugged the State Department". In: *CNN*. URL: <https://edition.cnn.com/2017/08/23/us/spyhunter-russia-bug-us-state-department-declassified/index.html> (visited on 2019-08-08).
- Borrelli, A (Nov. 20, 2018). "Suspect accused of illegally video-recording people in the bathroom". In: *Binghamton Press & Sun-Bulletin*. URL: <https://eu.pressconnects.com/story/news/public-safety/2018/11/19/binghamton-unlawful-surveillance-broome-sheriff-video-spying/2056878002/> (visited on 2019-08-07).
- Braithwaite, R. (2002). *Across the Moscow River: The World Turned Upside Down*. Yale University Press, p. 60. ISBN: 9780300094961.
- (2010). *Moscow 1941: A City & Its People at War*. Profile Books. ISBN: 9781847650627.

- British Diplomatic Oral History Programme (1998). "An Interview with AMY, Dennis Oldrieve, CMG, OBE (b.1932)". In: *British Diplomatic Oral History Programme* DOHP 45 1 file. URL: <https://www.chu.cam.ac.uk/media/uploads/files/Amy.pdf> (visited on 2019-09-06).
- Britten, N. (Apr. 2, 2013). "Derby fire: police defend controversial use of bugging". In: *The Telegraph*. URL: <https://www.telegraph.co.uk/news/uknews/crime/9967246/Derby-fire-police-defend-controversial-use-of-bugging.html> (visited on 2019-08-08).
- Brooker, G. and J. Gomez (2013). "Lev Termen's Great Seal bug analyzed". In: *IEEE Aerospace and Electronic Systems Magazine* 28.11, pp. 4–11. ISSN: 0885-8985. DOI: 10.1109/MAES.2013.6678486.
- Brookes, P. (2001). *Electronic Surveillance Devices*. Newnes. ISBN: 9780750651998.
- Brown, R.M. (1967). *The Electronic Invasion*. J. F. Rider. ISBN: 9780810407794.
- BStU (2016). *Gesamtverzeichnis der Veröffentlichungen (Complete publications List)*. Report. BStU: The Federal Commissioner for the Stasi Records. URL: http://www.bstu.bund.de/EN/Home/home_node.html.
- Bugman, S. (1999). *The Basement Bugger's Bible: The Professional's Guide To Creating, Building, And Planting Custom Bugs And Wiretaps*. Paladin Press. ISBN: 9781581600223.
- Burford, R. (July 5, 2017). "Jilted husband put bugging devices around his family home to secretly tape his wife's conversations to use in a custody battle for their four children". In: *The Daily Mail*. URL: <https://www.dailymail.co.uk/news/article-4667352/Jilted-husband-bugging-devices-family-home.html> (visited on 2019-08-07).
- Buxton, J.N and B. Randell (1970). *Software Engineering Techniques: Report on a Conference Sponsored by the NATO Science Committee*. NATO Science Committee; available from Scientific Affairs Division, NATO.
- Callaghan, C. (Sept. 26, 2013). "Michelle Mone's firm bugged director's office amid fears he was about to jump ship to ex-husband's new company, tribunal hears". In: *Daily Record*. URL: <https://www.dailyrecord.co.uk/news/scottish-news/michelle-mones-firm-bugged-directors-2303455> (visited on 2019-08-08).
- Campbell, D. (1976). "The Eavesdroppers". In: *Time Out* May 21 - 27.

- Campbell, D. (1977). *ABC Case*. URL: <http://www.duncancampbell.org/content/abc-case> (visited on 2019-09-06).
- (1987). *How Zircon was launched*. URL: <http://www.duncancampbell.org/content/new-statesman-1987> (visited on 2019-09-06).
- (Aug. 12, 1988). “Somebody’s listening”. In: *New Statesman*, pp. 9–12.
- (2015a). *British Embassy Spying*. URL: <http://www.duncancampbell.org/british-embassy-spying> (visited on 2019-09-06).
- (2015b). *Global spy system ECHELON confirmed at last – by leaked Snowden files*. URL: https://www.theregister.co.uk/2015/08/03/gchq_duncan_campbell/ (visited on 2019-09-06).
- (2016). *Duncan Campbell.org*. Tech. rep. URL: <http://www.duncancampbell.org/content/biography#theeavesdroppers> (visited on 2019-09-06).
- Campbell, D. and S. Connor (1986). *On the record: surveillance, computers, and privacy : the inside story*. M. Joseph. ISBN: 9780718125769.
- Campbell, S. (July 25, 2014). “‘Spying’ devices found at Ford HQ”. In: *The Telegraph*. URL: <https://www.telegraph.co.uk/finance/newsbysector/industry/10991219/Spying-devices-found-at-Ford-HQ.html> (visited on 2019-08-07).
- Chen, B., V. Yenamandra, and K. Srinivasan (2015). *Tracking Keystrokes Using Wireless Signals*. Conference Paper. MobiSys ’15, pp. 31–44. DOI: 10.1145/2742647.2742673.
- Christopher, W. (1975). “Special Branch intensifies secret checks”. In: *The Times*, p. 3.
- Churchill Archive Centre (2016). *Mitrokhin’s KGB archive opens to public*. URL: <https://www.chu.cam.ac.uk/news/2014/jul/7/mitrokhins-kgb-archive-opens/> (visited on 2019-09-06).
- CIA (Sept. 7, 1976). “A program for providing high-resolution oblique photography over denied area. A program for providing H[15687573].pdf”. In: A program for providing high-resolution oblique photography over denied area: SPECIALCOLLECTION 06527331. Approved for Release: 2019/07/30 C06527331. URL: <https://www.cia.gov/library/readingroom/collection/animal-partners> (visited on 2019-09-19).

- CIA/DP (June 24, 1968). *Clandestine Service History: The Berlin Tunnel Operation, 1952–1956*. URL: <https://www.cia.gov/library/readingroom/document/5166d4f999326091c6a6081c> (visited on 2019-09-07).
- (n.d.). *Clandestine Service History: The Berlin Tunnel Operation, 1952–1956*. URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/on-the-front-lines-of-the-cold-war-documents-on-the-intelligence-war-in-berlin-1946-to-1961/5-7.pdf> (visited on 2019-09-08).
- Clarke, R. (1994). *The Digital Persona and its Application to Data Surveillance*. URL: <http://www.rogerclarke.com/DV/DigPersona.html#DV> (visited on 2019-09-06).
- Clerix, K. (Mar. 20, 2003). “Espionage in Belgium: recent cases”. In: *Euobserver*. URL: <https://euobserver.com/secret-ue/117564> (visited on 2019-08-08).
- CND (Oct. 16, 2011). *Menwith Hill day of action 2011 138*. URL: <https://www.flickr.com/photos/cnduk/6260000027> (visited on 2019-09-06).
- Cold War International History Project Bulletin (1998). “New Evidence on Soviet Intelligence: The KGB’s 1967 Annual Report. With Commentaries by Raymond Garthoff and Amy Knight”. In: *Cold War International History Project Bulletin No10 (1998)* Woodrow Wilson International Center for Scholars, Washington, D.C.10, pp. 212–217.
- Colville to Morrison (Oct. 9, 1952a). *Foreign Intelligence Activities. The National Archives*.
- (Oct. 13, 1952b). *MoD memo, 'Russian Eavesdropping'. The National Archives*.
- Corbin, J. (Sept. 30, 2019). *The Khashoggi Murder Tapes*. URL: <https://www.bbc.co.uk/iplayer/episode/m0008zf7/panorama-the-khashoggi-murder-tapes> (visited on 2019-09-30).
- Costello, J. and O.N. Carev (1993). *Deadly Illusions: The KGB secrets the British Government doesn't want you to read*. Crown Publishers Incorporated. ISBN: 9780517588505.
- Coughlin, T. (Jan. 2018). “A Solid-State Future [The Art of Storage]”. In: *IEEE Consumer Electronics Magazine* 7.1, pp. 113–116. ISSN: 2162-2248. DOI: 10.1109/MCE.2017.2755339.
- Crypto Museum (2015). *EASYCHAIR:Passive covert listening devices*. URL: <http://www.cryptomuseum.com/covert/bugs/ec/index.htm> (visited on 2019-09-06).

- Crypto Museum (2016a). *SATYR: Resonant cavity microphone*. URL: <http://www.cryptomuseum.com/covert/bugs/satyr/index.htm#ref> (visited on 2019-09-06).
- (2016b). *The Thing: Great Seal Bug*. URL: <http://www.cryptomuseum.com/covert/bugs/thing/index.htm> (visited on 2019-09-06).
- Cryptologic Spectrum (1972a). “TEMPEST: A Signal Problem”. In: *Cryptologic Spectrum* 2/2, pp.26–30.
- (1972b). “TEMPEST: A Signal Problem”. In: *Cryptologic Spectrum* 2/2, pp.26–30.
- Curtis, S. (Sept. 13, 2013). “Santander ‘hackers’ attempt to rob bank with £10 device”. In: *The Telegraph*. URL: <https://www.telegraph.co.uk/technology/news/10307586/Santander-hackers-attempt-to-rob-bank-with-10-device.html> (visited on 2019-08-08).
- Daily Express (Oct. 2, 2016). “Man attacks girlfriend after bugging her home and thinking she was being unfaithful”. In: *The Daily Express*. URL: <https://www.express.co.uk/news/uk/706587/man-attacks-girlfriend-bugging-home-unfaithful> (visited on 2019-08-07).
- Darlington, J.A.B. (Aug. 27, 1956). *Anti eavesdropping measures in United Kingdom Government, Commonwealth and allied countries*. The National Archives.
- Das, A, N Borisov, and M Caesar (2014). “Do You Hear What I Hear?: Fingerprinting Smart Devices Through Embedded Acoustic Components”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’14. Scottsdale, Arizona, USA: ACM, pp. 441–452. ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660325. URL: <http://doi.acm.org.iclibezp1.cc.ic.ac.uk/10.1145/2660267.2660325>.
- Davies, P. (2004). *MI6 and the Machinery of Spying: Structure and Process in Britain’s Secret Intelligence*. Studies in Intelligence. Taylor & Francis. ISBN: 9780203503720.
- Day, M., G. Turner, and N Drozdiak (Apr. 10, 2019). *Amazon Workers Are Listening to What You Tell Alexa*. URL: <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio> (visited on 2019-08-17).
- De Silva, P. (1978). *Sub rosa: the CIA and the uses of intelligence*. Times Books.

- Delbecq, Andre L, Andrew H Van de Ven, and David H Gustafson (1975). *Group techniques for program planning: A guide to nominal group and Delphi processes*. Scott Foresman.
- Denney, A (Feb. 16, 2018). “Judge Strikes Pleadings of Husband in Divorce Who Bugged Wife’s Phone”. In: *New York Law Journal*. URL: <https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2018/02/16/judge-strikes-pleadings-of-husband-in-divorce-who-bugged-wifes-phone/?kw=Judge+Strikes+Pleadings+of+Husband+in+Divorce+Who+Bugged+Wife%27s+Phone&slreturn=20190707132540> (visited on 2019-08-07).
- Dennis, M. and P. Brown (2003). *The Stasi: Myth and Reality*. Pearson/Longman. ISBN: 9780582414228.
- Dentons (2018). *New and Emerging Technologies - Key Considerations*. Report. Centre for the Protection of National Infrastructure (CPNI). URL: https://www.cpni.gov.uk/system/files/documents/d2/f3/CPNI_Dentons_New%20and%20emerging%20technologies.pdf. pdf (visited on 2019-09-06).
- Der Bundesbeauftragte für die Stasi-Unterlagen (2016). *Federal Commissioner for the Stasi Records, also known as The Stasi Records Agency*. URL: <http://www.bstu.bund.de> (visited on 2019-09-06).
- Domo Inc. (Aug. 17, 2019). *Data Never Sleeps 7.0*. URL: <https://www.domo.com/learn/data-never-sleeps-7> (visited on 2019-08-17).
- Downs, K. (Aug. 7, 2016). “All Blacks manager describes moment of ‘shock’ listening device was found in Sydney hotel last year”. In: *1NewsNow*. URL: <https://www.tvnz.co.nz/one-news/sport/rugby/all-blacks-manager-describes-moment-shock-listening-device-found-in-sydney-hotel-last-year> (visited on 2019-08-08).
- Drew (Feb. 25, 1946). “Security of offices and documents in the Colonies and foreign countries”. In: CAB 21/3946.
- Dulles, A. (2016). *The Craft of Intelligence: America’s Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*. Globe Pequot Press. ISBN: 9781493018796. URL: <https://books.google.co.uk/books?id=CmA-jgEACAAJ>.
- Easter, D. (2016). “Soviet Bloc and Western Bugging of Opponents’ Diplomatic Premises During the Early Cold War”. In: *Intelligence and National Security* 31.1, pp. 28–48.

- Erdem, S. (June 11, 2004). “Turkey admits bugging British Ambassador’s phone”. In: *The Times*. URL: <https://www.thetimes.co.uk/article/turkey-admits-bugging-british-ambassadors-phone-f6jktv9qzzl#> (visited on 2019-09-30).
- European Parliament (2001). *Interception Capabilities - Impact and Exploitation, Paper 1: Echelon and its role in COMINT*. URL: <http://www.duncancampbell.org/menu/surveillance/echelon/IC2001-Paper1.pdf> (visited on 2019-09-06).
- Fan, Chin-Feng and Yuan-Chang Yu (2004). “BBN-based software project risk management”. In: *Journal of Systems and Software* 73.2, pp. 193–203.
- Feng, N., H.J Wang, and M. Li (2014). “A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis”. In: *Information sciences* 256, pp. 57–73.
- Fenton, N. and J. Bieman (2014). *Software Metrics: A Rigorous and Practical Approach (3rd edition)*. CRC Press. ISBN: 9781439838228.
- Fenton, N. and M. Neil (2007). “Managing Risk in the Modern World”. In: *Application of Bayesian Networks*.
- (2011). “The use of Bayes and causal modelling in decision making, uncertainty and risk”. In: *CEPIS Upgrade* 12.5, pp. 10–21.
- (2012). *Risk Assessment and Decision Analysis with Bayesian Networks*. Taylor & Francis. ISBN: 9781439809105.
- Fischer, B.B. (2016). “Doubles Troubles: The CIA and Double Agents during the Cold War”. In: *International Journal of Intelligence and CounterIntelligence* 29.1, pp. 48–74. ISSN: 0885-0607. DOI: 10.1080/08850607.2015.1083313.
- Fitzgerald, P. and M. Leopold (1987). *Stranger on the Line: The Secret History of Phone Tapping*. Bodley Head. ISBN: 9780370307503.
- Florian Henckel von Donnersmarck (2006). *The Lives of Others (Das Leben der Anderen)*. Audiovisual Material.
- Fon (2015). *15 Years of Wi-Fi Evolution*. URL: <https://fon.com/fon-wifi-infographic/> (visited on 2019-09-06).

- Fry, H. (2012). *The M Room: Secret Listeners who Bugged the Nazis in WW2*. CreateSpace Independent Publishing Platform. ISBN: 9781481020084.
- (2019). Yale University Press. ISBN: 9780300238600.
- Funder, A. (May 5, 2007). “Tyranny of terror”. In: URL: <http://www.theguardian.com/books/2007/may/05/featuresreviews.guardianreview12> (visited on 2019-09-06).
- (2011). *Stasiland: Stories From Behind The Berlin Wall*. Granta Publications. ISBN: 9781847085085.
- Fursenko, A. and T. Naftali (2010). *Khrushchev’s Cold War: The Inside Story of an American Adversary*. W. W. Norton. ISBN: 9780393078336.
- Gallagher, R. and G. Greenwald (2014). “How the NSA Plans to Infect ‘Millions’ of computers with malware”. In: *The Intercept*. URL: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>.
- Garcia, K (Nov. 19, 2018). “Iowa Park man back in jail with new charge of improper visual recording”. In: *Texomashomepage.com*. URL: <https://www.texomashomepage.com/news/local-news/iowa-park-man-back-in-jail-with-new-charge-of-improper-visual-recording/amp/> (visited on 2019-08-07).
- Gartner (2019). “Gartner Top 10 Strategic Technology Trends for 2019”. In: *Gartner News Room* 13 March 2019. URL: <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>.
- Germano, B (May 23, 2018). “Man Charged With Placing Pen-Like Recording Device In Day-care Bathroom”. In: *CBS Boston*. URL: <https://boston.cbslocal.com/2018/05/23/learning-experience-foxboro-recording-device-darin-mcneil/> (visited on 2019-08-07).
- Ghana Web (July 10, 2017). “Planted audiovisual recorder found in ‘galamsey’ minister’s office”. In: *Ghana Web*. URL: <https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Planted-audiovisual-recorder-found-in-galamsey-minister-s-office-557196#> (visited on 2019-08-07).
- Gibbs, S. (Feb. 19, 2015). “Samsung smart TVs send unencrypted voice recognition data across internet”. In: *The Guardian*. URL: <https://www.theguardian.com/world/2003/mar/20/eu.politics> (visited on 2019-08-17).

- Gill, P. and M. Phythian (2013). *Intelligence in an Insecure World*. Wiley. ISBN: 9780745680897.
- Glinsky, A. (2000a). *Theremin: Ether Music and Espionage*. University of Illinois Press, p. 260. ISBN: 9780252025822.
- (2000b). *Theremin: Ether Music and Espionage*. University of Illinois Press, p. 259. ISBN: 9780252025822.
- Goldman, D (2015). *Your Samsung TV is eavesdropping on your private conversations*. URL: <https://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html> (visited on 2019-09-06).
- Gollakota, S. et al. (2014). “The Emergence of RF-Powered Computing”. In: *Computer* 47.1, pp. 32–39. ISSN: 0018-9162. DOI: 10.1109/MC.2013.404.
- Government Office for Science (Feb. 20, 2018). *Computational modelling: technological futures*, p. 124. URL: <https://www.gov.uk/government/publications/computational-modelling-blackett-review> (visited on 2019-09-06).
- governmentbids.com (2004). *70-CESG Tempest Video Processor System*. URL: <http://www.governmentbids.com/technology-bids/computers/70--CESG-Tempest-Video-Processor-System-en.jsa?id=545349> (visited on 2019-09-06).
- Graham, B. (1987). *Break-in: Inside the Soviet Trade Delegation*. Bodley Head. ISBN: 9780370310299.
- Grant, Robert M (1991). “The resource-based theory of competitive advantage: implications for strategy formulation”. In: *California management review* 33.3, pp. 114–135.
- (2016). *Contemporary strategy analysis: Text and cases edition*. John Wiley & Sons.
- Grell, Max et al. (Jan. 2019). “Autocatalytic Metallization of Fabrics Using Si Ink, for Biosensors, Batteries and Energy Harvesting”. In: *Advanced Functional Materials* 29.1. ISSN: 1616-301X. DOI: 10.1002/adfm.201804798. URL: <https://doi.org/10.1002/adfm.201804798> (visited on 2019-09-06).
- Gu, W et al. (Feb. 2016). “Lithium-Iron Fluoride Battery with In Situ Surface Protection”. In: *Advanced Functional Materials* 26, n/a–n/a. DOI: 10.1002/adfm.201504848.
- Hampton, R (Aug. 16, 2018). “It Is Remarkably Easy to Buy “Spy Pens” if You Were Inclined to Record Secret Conversations at the White House”. In: *Slate*. URL: <https://slate.com/>

- human-interest/2018/08/omarosas-alleged-spy-pen-use-is-easy-to-come-by-on-amazon.html (visited on 2019-08-07).
- Hardcash Productions (July 15, 2019). *Exposure : Undercover: Inside China's Digital Gulag*.
- Herman, M. (1998). "Diplomacy and intelligence". In: *Diplomacy & Statecraft* 9.2, pp. 1–22. ISSN: 0959-2296. DOI: 10.1080/09592299808406081.
- Highland, H.J. (1988). "Electromagnetic eavesdropping machines for christmas?" In: *Computers & Security* 7.4, pp. 341–341. ISSN: 0167-4048. DOI: 10.1016/0167-4048(88)90567-6.
- Hofstede, G. (1984). *Culture's Consequences: International Differences in Work-Related Values*. Cross Cultural Research and Methodology. SAGE Publications. ISBN: 9780803913066. URL: https://books.google.co.uk/books?id=Cayp%5C_Um409gC.
- (2019). *The 6-D model of national culture*. URL: <https://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/> (visited on 2019-09-06).
- Hopgood, A.A. (2016). *Intelligent Systems for Engineers and Scientists, Third Edition*. CRC Press. ISBN: 9781498783798.
- Hoskinson, S. (June 9, 1978). *Moscow Chimney Affairs*. URL: <https://history.state.gov/historicaldocuments/frus1977-80v06/d123> (visited on 2019-09-06).
- Hubest, A. (1960). "Audio Surveillance". In: *Studies in Intelligence* 4/3, pp.40–1.
- Hürriyet Daily News (Oct. 14, 2013). "Turkish intelligence's 'museum' revealed". In: *Hürriyet Daily News*. URL: <http://www.hurriyetdailynews.com/turkish-intelligences-museum-revealed-56190> (visited on 2019-09-30).
- Hutchins, E.M., M.J. Cloppert, and R.M. Amin (2011). "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains". In: *Leading Issues in Information Warfare & Security Research* 1, p. 80.
- Hutson, J. (Jan. 28, 1998). *Interview with Sir Rodric Braithwaite on 28 January 1998*. Interview. URL: <https://www.chu.cam.ac.uk/media/uploads/files/Braithwaite.pdf> (visited on 2019-09-06).
- Inside Edition (Oct. 26, 2018). "Couple Says They Found Hidden Camera Pointing at Their Bed in Carnival Cruise Room". In: *Inside Edition*. URL: <https://www.insideedition.com/>

couple-says-they-found-hidden-camera-pointing-their-bed-carnival-cruise-room-47948 (visited on 2019-08-07).

Institute, SANS (2016). *Introduction to TEMPEST*. Report. SANS Institute. URL: <https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981> (visited on 2019-09-06).

Intelligence and Security Committee (2000). *The Mitrokhin Inquiry Report*. URL: http://isc.independent.gov.uk/files/200006_ISC_Mitrokhin_Report.pdf (visited on 2019-09-06).

ITN News (June 3, 1989). *POLITICS: Soviet Embassy bug allegations*. URL: <https://www.gettyimages.co.uk/videos/politics-soviet-embassy-bug-allegations> (visited on 2016-07-30).

Jacquemard, T. et al. (2014). “Challenges and opportunities of lifelog technologies: A literature review and critical analysis”. In: *Science and engineering ethics* 20.2, pp. 379–409.

Jeffery, K. (2010). *MI6: The History of the Secret Intelligence Service, 1909-1949*. Bloomsbury. ISBN: 9781408813157.

Johnson, M.J. (2017). *The history of social media*. URL: <http://www.booksaresocial.com/timeline-social-media-2017/> (visited on 2019-09-06).

JTA (Nov. 1, 2018a). “Major Kiev Synagogue Bugged by Professionals, Ukraine’s Chief Rabbi Says”. In: *Haaretz*. URL: <https://www.haaretz.com/world-news/europe/major-kiev-synagogue-bugged-by-professionals-ukraine-s-chief-rabbi-says-1.6615103> (visited on 2019-08-09).

— (Nov. 1, 2018b). “Ukraine rabbi says a listening devices found at Kiev synagogue”. In: *The Jewish News*. URL: <https://jewishnews.timesofisrael.com/ukraines-rabbi-says-a-listening-devices-found-at-kiev-synagogue/> (visited on 2019-08-09).

Kahn, D. (1998a). “SOVIET COMINT IN THE COLD WAR”. In: *Cryptologia* 22.1, pp. 1–24. DOI: 10.1080/0161-119891886731. eprint: <https://doi.org/10.1080/0161-119891886731>. URL: <https://doi.org/10.1080/0161-119891886731>.

— (1998b). “Soviet COMINT in the Cold War”. In: *Cryptologia* 22.1, pp. 1–24. ISSN: 0161-1194. DOI: 10.1080/0161-119891886731.

- (2014). *How I Discovered World War II's Greatest Spy and Other Stories of Intelligence and Code*. Taylor & Francis. ISBN: 9781466561991.
- Kali-Linux (Mar. 13, 2013). *Kali Linux – Penetration Testing Distribution*. URL: <http://www.backtrack-linux.org/> (visited on 2019-08-07).
- Kearney, V. (June 12, 2014). “Lurgan dissident republican ‘finds bugs in his car’”. In: *BBC*. URL: <https://www.bbc.co.uk/news/uk-northern-ireland-27818441> (visited on 2019-08-08).
- Keefe, P.R. (2006). *Chatter: Uncovering the Echelon Surveillance Network and the Secret World of Global Eavesdropping*. Random House Publishing Group. ISBN: 9781588365330.
- Kennan, G.F. (1983). *Memoirs, 1950-1963*. George F. Kennan Memoirs. Pantheon Books. ISBN: 9780394716268.
- Kern, G. (2008). *How “Uncle Joe” Bugged FDR: The Lessons of History*. URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article02.html> (visited on 2019-09-06).
- Kessler, R. (1989). *Moscow Station: How the KGB Penetrated the American Embassy*. Scribner. ISBN: 9780684189819.
- Khrushchev, Sergei (1988). “My Father Nikita’s Downfall”. In: *Time* 132.20, p. 35. ISSN: 0040781X.
- Knolle, K (Jan. 25, 2018). “Austria investigating bugging, break-in at far-right leader’s office”. In: *Reuters*. URL: <https://www.reuters.com/article/us-austria-farright/austria-investigating-bugging-break-in-at-far-right-leaders-office-idUSKBN1FE2C0> (visited on 2019-08-07).
- Knox, F (Apr. 18, 2018). “Mum hides device in son’s bag, makes shocking discovery”. In: *Fraser Coast Chronicle*. URL: <https://www.frasercoastchronicle.com.au/news/mum-bugs-sons-bag-listens-horrifying-moment/3390079/> (visited on 2019-08-07).
- Kuhn, M.G. (2002). “Optical time-domain eavesdropping risks of CRT displays”. In: *Proceedings 2002 IEEE Symposium on Security and Privacy*, pp. 3–18. DOI: 10.1109/SECPRI.2002.1004358.

- Kuhn, M.G. (Dec. 2003). *Compromising emanations: eavesdropping risks of computer displays*. Tech. rep. UCAM-CL-TR-577. University of Cambridge, Computer Laboratory. URL: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf>.
- (2004). “Electromagnetic eavesdropping risks of flat-panel displays”. In: *Privacy Enhancing Technologies*. Springer, pp. 88–107.
- (2005a). *Real-time signal-processing platform for compromising video emanations*. Report.
- (2005b). “Security limits for compromising emanations”. In: *Cryptographic Hardware and Embedded Systems—CHES 2005*. Springer, pp. 265–279.
- (2006). “Eavesdropping attacks on computer displays”. In: *Information Security Summit*, pp. 24–25.
- (2013). “Compromising emanations of lcd tv sets”. In: *Electromagnetic Compatibility, IEEE Transactions on* 55.3, pp. 564–570. ISSN: 0018-9375.
- (2016). *Dr Markus Kuhn*. URL: <http://www.cl.cam.ac.uk/~mgk25/> (visited on 2019-09-06).
- Kuhn, M.G. and R.J. Anderson (1988). “Soft tempest: Hidden data transmission using electromagnetic emanations”. In: *Information hiding*. Springer, pp. 124–142. ISBN: 3540653864.
- Lei, Xinyu et al. (2017). “The Insecurity of Home Digital Voice Assistants - Amazon Alexa as a Case Study”. In: *CoRR* abs/1712.03327. arXiv: 1712.03327. URL: <http://arxiv.org/abs/1712.03327>.
- Leob, V. and D.A. Vise (Dec. 9, 1999). “Russian Diplomat Is Accused Of Spying”. In: *Washington Post*. URL: <https://www.washingtonpost.com/archive/politics/1999/12/09/russian-diplomat-is-accused-of-spying/8d646bf6-3fc5-4b81-9978-e08c7004e410/> (visited on 2019-08-08).
- Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press. ISBN: 9781452901732.
- (2002). “Surveillance studies: understanding visibility, mobility and the phenetic fix”. In: *Surveillance and society* 1.1. ISSN: 1477-7487.
- Lyon, D., K. Ball, and K.D. Haggerty (2012). *Routledge handbook of surveillance studies*. Routledge.

- MacDermott, D. and D. Hickey (Dec. 7, 2017). “How Garda bugging of Dublin pub led to downfall of ex-IRA man”. In: *The Irish Times*. URL: <https://www.irishtimes.com/news/crime-and-law/courts/how-garda-bugging-of-dublin-pub-led-to-downfall-of-ex-ira-man-1.3319075> (visited on 2019-08-07).
- MacLean, E.K. (1992). *Joseph E. Davies: Envoy to the Soviets*. Westport, CT: Praeger, p. 40.
- Macrakis, K. (2014). *Seduced by Secrets: Inside the Stasi’s Spy-Tech World*. Naval Institute Press. ISBN: 9781591141839.
- Madsen, C. W. (1988). “Hacking the airwaves”. In: *Security Technology, 1988. Crime Countermeasures, Proceedings. Institute of Electrical and Electronics Engineers 1988 International Carnahan Conference on*. IEEE, pp. 65–68.
- Mann, S. (2004). “Sousveillance: inverse surveillance in multimedia imaging”. In: *Proceedings of the 12th annual ACM international conference on Multimedia*. ACM, pp. 620–627.
- Mann, S., J. Nolan, and B. Wellman (2002). “Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments”. In: *Surveillance & Society* 1.3, pp. 331–355. ISSN: 1477-7487.
- Maphumulo, S. (Aug. 4, 2015). “Man in dock over R25m bugging device”. In: *The Star*. URL: <https://www.iol.co.za/news/man-in-dock-over-r25m-bugging-device-1895186> (visited on 2019-08-07).
- Marchetti, V. and J.D. Marks (1975). *The CIA and the cult of intelligence*. Dell.
- Marinov, M. (2016a). *Remote video eavesdropping using a software-defined radio platform*. URL: <https://github.com/martinmarinov/TempestSDR> (visited on 2019-09-06).
- (2016b). *Remote video eavesdropping using a software-defined radio platform*. URL: <https://github.com/martinmarinov/TempestSDR> (visited on 2019-09-06).
- Marquardt, P. et al. (2011). “(sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers”. In: *CCS ’11*, pp. 551–562. DOI: 10.1145/2046707.2046771.
- Marshall, J. (May 22, 2011). “Spy bug found in MP’s house”. In: *Stuff*. URL: <http://www.stuff.co.nz/national/politics/5037218/Spy-bug-found-in-MPs-house> (visited on 2019-08-08).

- Melton, H.K. (1993). *CIA Special Weapons & Equipment: Spy Devices of the Cold War*. Sterling Publishing Company. ISBN: 9780806987323.
- (2002a). *Ultimate Spy*. DK Pub. ISBN: 9780789489722.
- (2002b). *Ultimate Spy*. DK Pub., p. 82. ISBN: 9780789489722.
- Ministry of Defence, UK (2018). *Global Strategic Trends, The Future Starts Today*. URL: <https://www.gov.uk/government/publications/global-strategic-trends> (visited on 2019-09-06).
- Miniwatts Marketing Group (2015). *Top ten languages in the internet*. URL: <http://www.internetworldstats.com/stats7.htm> (visited on 2019-09-06).
- (2018). *Internet Users in the World by Region*. URL: <http://www.internetworldstats.com/stats.htm> (visited on 2019-09-06).
- MIT Technology Review (2019). *10 Breakthrough Technologies*. URL: <https://www.technologyreview.com/lists/technologies/2019/> (visited on 2019-09-26).
- mobiles.co.uk (May 25, 2017). “Top 10 Smartphone Uses”. In: *mobiles.co.uk*. URL: <https://www.mobiles.co.uk/blog/top-10-smartphone-uses/#fn1> (visited on 2019-08-14).
- Morera, J.L and R. Calcines (1988). *The CIA's War Against Cuba*. National Information Centre.
- Morris, A (Feb. 23, 2018). “Questions over listening device found at former home of senior republican”. In: *The Irish News*. URL: <https://www.irishnews.com/news/northernirelandnews/2018/02/23/news/questions-over-listening-device-found-at-former-home-of-senior-republican-1262171/> (visited on 2019-08-07).
- Moschella, David (2015). “The Pace of Technology Change is Not Accelerating”. In: *Leading Edge Forum* Monthly Research Commentary.
- Mullin, J. and M. White (Dec. 9, 1999). “Adams' fury at car bug”. In: *The Guardian*. URL: <https://www.theguardian.com/uk/1999/dec/09/northernireland.gerryadams> (visited on 2019-08-08).
- Munro, K (July 1, 2015a). *Finding wireless kettles with social networks*. URL: <https://www.pentestpartners.com/security-blog/finding-wireless-kettles-with-social-networks/> (visited on 2019-08-17).

- (June 8, 2015b). *Hacking kettles & extracting plain text WPA PSKs. Yes really!* URL: <https://www.pentestpartners.com/security-blog/hacking-kettles-extracting-plain-text-wpa-psks-yes-really/> (visited on 2019-08-17).
- (June 18, 2015c). *WiFi Kettle SSID Hack Demo*. URL: <https://youtu.be/GDy9Nvcw404> (visited on 2019-08-17).
- Murphy, J. and M. Roser (2019). “Internet”. In: *Our World in Data*. <https://ourworldindata.org/internet>.
- Museum, Crypto (Aug. 28, 2016). “OPEC bug”. In: *Crypto Museum*. URL: <https://www.cryptomuseum.com/covert/bugs/opec/index.htm> (visited on 2019-08-08).
- Nayef, M and M Al-Sanousi Al-Seyassah (Oct. 25, 2018). “Recording device planted in the car of a Kuwaiti woman”. In: *Arab Times*. URL: <https://www.arabtimesonline.com/news/recording-device-planted-in-the-car-of-a-kuwaiti-woman/> (visited on 2019-08-07).
- Neitzel, S., G. Brooks, and I. Kershaw (2013). *Tapping Hitler’s Generals: Transcripts of Secret Conversations 1942-45*. Pen & Sword Books Limited. ISBN: 9781848327153.
- New Zealand Herald (Aug. 25, 2017). “Bugging at Christchurch Men’s Prison to be referred to police”. In: *New Zealand Herald*. URL: https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11911401 (visited on 2019-08-07).
- Nichter, L.A (2007). *nixontapes.org*. URL: <http://nixontapes.org/index.html> (visited on 2019-09-06).
- NSA Playset (2016). *NSA Playset: CONGAFLOCK*. URL: <http://www.nsaplayset.org/congaflock> (visited on 2019-09-06).
- OFCOM (2018). *The Communications Market 2018: Narrative report*. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0022/117256/CMR-2018-narrative-report.pdf (visited on 2019-09-03).
- Ofcom (2019). *Mobile Availability*. URL: <https://checker.ofcom.org.uk/mobile-coverage> (visited on 2019-09-06).
- Olama, M.M et al. (2010). “A Bayesian belief network of threat anticipation and terrorist motivations”. In: *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, pp. 76660V–76660V.

- Ottaway, D. B. (1987). *Soviet ability to penetrate US embassy underestimated, Schlesinger report says*. (James R. Schlesinger).
- Oxford Internet Institute (2019). *Information Geographies*. URL: <https://geography.oxi.ox.ac.uk/#open-data-index> (visited on 2019-09-06).
- Palmer, R.E. and T. Green (1977). *The Making of a Spy*. Danbury Press. ISBN: 9780717281169.
- Pearce, K. (2013). *A Guide to the Technology Trends That Are Shaping Our Future*. URL: <https://www.diygenius.com/a-guide-to-the-technology-trends-that-are-shaping-our-future/> (visited on 2019-09-06).
- Pearl, J. (2009). *Causality*. Cambridge University Press. ISBN: 9781139643986.
- Peltier, T.R. (2005). *Information security risk analysis*. CRC press.
- Perrie, R. (Sept. 3, 2018). "STALKER HELL: Ex-boyfriend spied on lover by hiding secret cameras and listening devices in her home". In: *The Sun*. URL: <https://www.thesun.co.uk/news/7168023/ex-boyfriend-spied-on-lover-by-hiding-secret-cameras-and-listening-devices-in-her-home/> (visited on 2019-08-07).
- Petersen, J.K. (2012). *Handbook of Surveillance Technologies, Third Edition*. CRC Press. ISBN: 9781466554139.
- Piodi, F and I. Mombelli (2014). *The ECHELON Affair: The EP and the global interception system 1998 - 2002*. URL: http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf (visited on 2019-09-06).
- Price, D (2015). *5 Reasons to Avoid Smart Assistants If You Value Your Privacy*. URL: <https://www.makeuseof.com/tag/reasons-avoid-smart-assistants/> (visited on 2019-09-06).
- Pugliese, D. (Oct. 18, 2016). "The mystery of the listening devices at DND's Nortel Campus". In: *The Ottawa Citizen*. URL: <https://ottawacitizen.com/news/national/defence-watch/the-mystery-of-the-listening-devices-at-dnds-nortel-campus> (visited on 2019-08-07).
- Pumphrey and Skidmore (Jan. 3, 1957). *Diplomatic Wireless Service: expansion of the staffing arrangements of the Foreign Service Technical Maintenance Service*.
- Qinetiq (2015). *Emerging Technologies April 2015*. Report. Centre for the Protection of National Infrastructure (CPNI). URL: <https://www.cpni.gov.uk/documents/publications/>

2015/05-june-2015-emerging%20technologies%202015%20-%20v2_pv.pdf?epslanguage=en-gb (visited on 2016-07-09).

Reason, James (2016). *Managing the risks of organizational accidents*. Routledge.

Reilly Papers (1957). MS Eng. c.6922 vols. folio 57–58. Bodleian Library. URL: <http://www.bodley.ox.ac.uk/dept/scwmss/wmss/online/modern/reilly/reilly.html> (visited on 2019-09-06).

Reyes, B. (Apr. 13, 2018). “Europort ‘bugs’ may be linked to 2014 surveillance operation, police believe”. In: URL: <https://www.chronicle.gi/europort-bugs-may-be-linked-to-2014-surveillance-operation-police-believe/> (visited on 2019-08-07).

Riste, O. (2014). *The Norwegian Intelligence Service, 1945-1970*. Studies in Intelligence. Taylor & Francis. ISBN: 9781135230586.

Robin, H.K. et al. (1963). “Multitone signalling system employing quenched resonators for use on noisy radio-teleprinter circuits”. In: *Electrical Engineers, Proceedings of the Institution of* 110.9, pp. 1554–1568. ISSN: 0020-3270. DOI: 10.1049/piee.1963.0221.

Ronsivalle, G.B. (2011). *Neural and Bayesian Networks to Fight Crime: the NBNC Meta-Model of Risk Analysis*. INTECH Open Access Publisher.

Rosenberg, C (Mar. 8, 2017). “Pentagon: Microphone? What microphone?” In: *The Miami Herald*. URL: <https://www.miamiherald.com/news/nation-world/world/americas/guantanamo/article204120459.html> (visited on 2019-08-07).

RTL-SDR.Com (2015). *Spying on keyboard presses with Software Defined Radio*. URL: <http://www.rtl-sdr.com/spying-keyboard-presses-software-defined-radio/> (visited on 2019-09-06).

Russakovskii, A (Oct. 10, 2017). *Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7*. URL: <https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/> (visited on 2019-08-17).

Rustmann, F.W. (2002). *CIA, Inc: Espionage and the Craft of Business Intelligence*. Brassey’s. ISBN: 9781574883886.

- Ryan, F. (Oct. 4, 2015). "Ai Weiwei finds 'listening devices' hidden in Beijing studio". In: *The Guardian*. URL: <https://www.theguardian.com/artanddesign/2015/oct/04/ai-weiwei-finds-listening-devices-hidden-in-beijing-studio> (visited on 2019-08-07).
- Sabur, R. (Mar. 22, 2017). "Rugby star filmed attack on ex-wife's 'new partner' after bugging her home to catch them together, court hears". In: *The Telegraph*. URL: <https://www.telegraph.co.uk/news/2017/03/22/rugby-star-filmed-attack-ex-wifes-new-partner-bugging-home-catch/> (visited on 2019-08-07).
- Salamone, S. (2019). "6 Tech Trends for the Enterprise in 2019". In: *eWeek*, p. 1. URL: <https://www.networkcomputing.com/networking/6-tech-trends-enterprise-2019>.
- Samsung (2015). *Samsung Global Privacy Policy - SmartTV Supplement*. URL: <https://www.samsung.com/uk/info/privacy-SmartTV.html> (visited on 2019-09-07).
- Schmid, G. (July 11, 2001). *REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*. Report. European Parliament.
- Security Research (2015). *Sabre Microwave Flooding System*. URL: <http://67.225.133.110/~gbpprorg/mil/cavity/Sabre.pdf> (visited on 2019-09-07).
- Seper, J. (Dec. 10, 1999). "Russian bug heightens fears of spy activity". In: *The Washington Times*. URL: <https://www.washingtontimes.com/news/1999/dec/10/19991210-123422-8012r/> (visited on 2019-08-08).
- Shannon, M.L. (2000). *The Bug Book: Everything You Ever Wanted to Know about Electronic Eavesdropping—but Were Afraid to Ask*. Paladin Enterprises. ISBN: 9781581600650.
- Sheymov, V. (June 9, 1978). *The Low Energy Radio Frequency Weapons Threat to Critical Infrastructure*. URL: http://fas.org/irp/congress/1998_hr/sheymov.htm (visited on 2019-09-06).
- Silvester, N (Jan. 14, 2018). "Gangsters using hi-tech car tracking devices as part of menacing scheme to stalk and attack enemies". In: *The Daily Record*. URL: <https://www.dailyrecord.co.uk/news/scottish-news/gangsters-using-hi-tech-car-11846807> (visited on 2019-08-07).

- SIS (Aug. 17, 2019). *SIS: Our Mission*. URL: <https://www.sis.gov.uk/our-mission.html> (visited on 2019-08-17).
- Smulders, P. (1990). “The threat of information theft by reception of electromagnetic radiation from RS-232 cables”. In: *Computers & Security* 9.1, pp. 53–58. ISSN: 0167-4048. DOI: 10.1016/0167-4048(90)90157-0.
- Solis, B. (2019). *Conversation Prism v5*. URL: <https://www.flickr.com/photos/briansolis/35963831302> (visited on 2019-09-06).
- Spalding, Holt and Ming Chow (2018). “Investigation Of Amazon Alexa’s Explicit Invocation Policy”. In: URL: <http://www.cs.tufts.edu/comp/116/archive/fall2018/hspalding.pdf> (visited on 2020-01-09).
- Spiegel Staff (2013). *Embassy Espionage: The NSA’s Secret Spy Hub in Berlin*. URL: <http://www.spiegel.de/international/world/merkel-furious-at-us-spying-and-eu-to-check-offices-for-bugs-a-908859.html> (visited on 2019-09-06).
- Spillet, R (Dec. 17, 2018). “Jealous husband, 45, who secretly bugged his estranged wife’s house and car so he could listen in on her new life is slapped with a restraining order”. In: *The Mail Online*. URL: <https://www.dailymail.co.uk/news/article-6503803/Jealous-husband-secretly-bugged-estranged-wifes-house-car.html> (visited on 2019-08-07).
- Staerck, G. (2000). “The role of HM embassy in Moscow”. In: *Contemporary British History* 14.3, pp. 149–161. ISSN: 1361-9462. DOI: 10.1080/13619460008581598.
- Stewart, W. (Aug. 7, 2009). “U.S. diplomat ‘caught on video in a new Russian honeytrap’”. In: *Daily Mail*. URL: <https://www.dailymail.co.uk/news/article-1205043/U-S-diplomat-caught-video-new-Russian-honeytrap.html> (visited on 2019-08-08).
- Stokes, P (May 31, 2006). “Who is bugging the Malham WI?” In: *The Telegraph*. URL: <https://www.telegraph.co.uk/news/uknews/1519861/Who-is-bugging-the-Malham-WI.html> (visited on 2019-08-08).
- Stone, J.V. (2013). *Bayes’ Rule: A Tutorial Introduction to Bayesian Analysis*. Sebtel Press. ISBN: 9780956372840.
- (2015). *Information Theory: A Tutorial Introduction*. Tutorial Introductions. ISBN: 9780956372857.

- Strong, C.L. (1968). "The Amateur Scientist: Little radio transmitters for short-range telemetry". In: *Scientific American, Inc.* Volume 218.Issue 3 (March), pp. 132–133.
- Strowger, A.B. (1891). "A.B Strowger Automatic Telephone Exchange". In: *US Patent No.447,918*, p. 3. URL: <https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US447918.pdf>.
- Symantec (2016). "Internet Security Threat Report". In: VOLUME 21. URL: <https://www.symantec.com/security-center/threat-report>.
- The American Legion Monthly (1937). "Beyond No Man's Land". In: *The American Legion Monthly*, p. 37.
- The Associated Press (Oct. 4, 2018). "Judge upholds seizure of secret recording device from coach". In: *The Associated Press*. URL: <https://apnews.com/2928f30aabd24ef18a0b2b9a36e0bafd> (visited on 2019-08-07).
- The Belfast Telegraph (May 23, 2016). "Listening devices stitched into girl's clothes, court told". In: *The Belfast Telegraph*. URL: <https://www.belfasttelegraph.co.uk/news/uk/listening-devices-stitched-into-girls-clothes-court-told-34739374.html> (visited on 2019-08-07).
- The Daily Herald (May 2, 2018). "Eavesdropping devices found in Central Bank". In: *The Daily Herald*. URL: <https://www.thedailyherald.sx/islands/76213-eavesdropping-devices-found-in-central-bank> (visited on 2019-08-07).
- The Daily Mail (Jan. 9, 2019). "Jealous husband stalks estranged wife with car tracker". In: *The Daily Mail*. URL: <https://www.iol.co.za/lifestyle/love-sex/relationships/jealous-husband-stalks-estranged-wife-with-car-tracker-18750382> (visited on 2019-08-07).
- The Evening Standard (Sept. 8, 2009). "The Walthamstow flat where bomb plot was hatched". In: *The Evening Standard*. URL: <https://www.standard.co.uk/news/the-walthamstow-flat-where-bomb-plot-was-hatched-6762881.html> (visited on 2019-08-08).
- The Guardian (May 20, 1964). *Russians 'wired' US Embassy*. Newspaper Article.

- The Scotsman (July 11, 2016). "Council using covert listening devices to 'spy on residents'". In: *The Scotsman*. URL: <https://www.scotsman.com/news-2-15012/council-using-covert-listening-devices-to-spy-on-residents-1-4174509> (visited on 2019-08-07).
- The Times (1975). "Bugging device at the heart of Communism". In: *The Times*, p. 2.
- Thomas Investigative Publications (1972). *The Watergate Bug Exhibit*. Web Page. URL: <http://www.pimall.com/nais/pivintage/watergatebugclose.html>.
- Tilouine, J and G Kadiri (Jan. 26, 2018). "In Addis Ababa, the seat of the African Union spied by Beijing". In: *Le Monde Afrique*. URL: https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-ababa-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html (visited on 2019-08-07).
- TNA: PREM 11/760 (Oct. 25, 1950). "Soviet apparatus for listening to conversations in room without wire connections". In: 1952-54. Prime Minister's Office files (PREM) 11/760.
- Tomlinson, R. (2001a). *The Big Breach: From Top Secret to Maximum Security*. Cutting Edge. ISBN: 9781903813010.
- (2001b). *The Big Breach: From Top Secret to Maximum Security*. Cutting Edge. ISBN: 9781903813010.
- Trucco, P. and M.C. Leva (2012). *BN Applications in Operational Risk Analysis: Scope, Limitations and Methodological Requirements*. INTECH Open Access Publisher.
- TV, BBC, ed. (1971). *Bugger*. URL: <http://www.bbc.co.uk/blogs/adamcurtis/entries/3662a707-0af9-3149-963f-47bea720b460> (visited on 2019-09-06).
- United States National Security Agency (NSA) (Dec. 30, 2013). "Tailored Access Operations (TAO) by the ANT division. Der Spiegel". In: ed. by Christian Stöcker Jacob Appelbaum Judith Horchert. URL: <https://nsa.gov1.info/dni/nsa-ant-catalog/> (visited on 2019-09-06).
- Universal International News (1960). *UN Spy Debate: Reds 'Bugged' American Embassy Lodge Claims*. URL: <https://www.youtube.com/watch?v=yR1QZLuyiPM> (visited on 2019-09-06).
- US Department of State (2011). "History of the Bureau of Diplomatic Security of the United States Department of State". In: pp. 161–196. URL: <http://www.state.gov/documents/organization/176589.pdf> (visited on 2016-04-08).

- US National Security Agency (2002). “Nonstop Evaluation Standards”. In: *CNSS Advisory Standard TEMPEST* 01-02.
- (2007). “Learning from the Enemy: The Gunman Project”. In: *United States Cryptologic history* Series VI. Volume 13. URL: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-histories/Learning_from_the_Enemy.pdf (visited on 2019-09-06).
- US State Department (2011). “History of the Bureau of Diplomatic Security of the United States Department of State”. In: p. 136. URL: <https://www.state.gov/wp-content/uploads/2019/05/176589.pdf> (visited on 2019-09-06).
- Van-Eck, W. (1985). “Electromagnetic radiation from video display units: An eavesdropping risk?” In: *Computers & Security* 4.4, pp. 269–286.
- Vlek, C et al. (2013). “Modeling crime scenarios in a Bayesian network”. In: *Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law*. ACM, pp. 150–159.
- Vuagnoux, M. and S. Pasini (2009). “Compromising Electromagnetic Emanations of Wired and Wireless Keyboards.” In: *USENIX security symposium*, pp. 1–16.
- Walford, J (Aug. 20, 2018). “How a secret bugging device planted by police caught an amateur boxer confess to killing his girlfriend”. In: *Wales online*. (Visited on 2019-08-07).
- Wallace, R., H.K. Melton, and H.R. Schlesinger (2009). *Spycraft: The Secret History of the CIA’s Spytechs, from Communism to Al-Qaeda*. Plume. ISBN: 9780452295476.
- War Office (1939). *CSDIC: listening and recording equipment: Directorate of Military Operations and Intelligence, and Directorate of Military Intelligence*. The National Archives.
- Webb, A. (2016). *2016 Trend Report*. Report. Webbmedia Group Digital Strategy. URL: <http://futuretodayinstitute.com/2016-trends>.
- Wei, T. et al. (2015). “Acoustic Eavesdropping through Wireless Vibrometry”. In: *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, pp. 130–141.
- Weiwei, A (Oct. 4, 2015). “Aiww ‘Did you hear it’”. In: *Instagram*. URL: https://www.instagram.com/p/8ZsZy0qDz0/?utm_source=ig_embed (visited on 2019-08-07).

- Welchman, G. (1997). *The Hut Six Story: Breaking the Enigma Codes*. M & M Baldwin. ISBN: 9780947712341.
- Whitaker, B. (Dec. 18, 2004). "Bugging device found at UN offices". In: *The Guardian*. URL: <https://www.theguardian.com/world/2004/dec/18/iraq.iraq> (visited on 2019-08-08).
- Whittaker, Z. (Mar. 7, 2017). "CIA, MI5 hacked smart TVs to eavesdrop on private conversations". In: *ZDNet*. URL: <https://www.zdnet.com/article/how-cia-mi5-hacked-your-smart-tv-to-spy-on-you/> (visited on 2019-08-17).
- Willder, S. (1985). "Directing technological development—The role of the board". In: *Long Range Planning* 18.4, pp. 44–49. ISSN: 0024-6301. DOI: [http://dx.doi.org/10.1016/0024-6301\(85\)90083-4](http://dx.doi.org/10.1016/0024-6301(85)90083-4). URL: <http://www.sciencedirect.com/science/article/pii/0024630185900834>.
- Williams, C (Apr. 16, 2018). "Video recording device found in Prince George's school office, police say". In: *The Washington Post*. URL: https://www.washingtonpost.com/local/education/video-recording-device-found-in-prince-georges-school-office-police-say/2018/04/16/b5c54b62-41c9-11e8-bba2-0976a82b05a2_story.html (visited on 2019-08-07).
- Williams, K. (1997). *The Prague Spring and Its Aftermath: Czechoslovak Politics, 1968-1970*. Cambridge University Press. ISBN: 9780521588034.
- Wilson, N (Oct. 29, 2018). "'Chucky' Brown Trial — INDECOM Provided Accused With Recording Device". In: *The Gleaner*. URL: <http://jamaica-gleaner.com/article/news/20181029/chucky-brown-trial-indecom-provided-accused-recording-device> (visited on 2019-08-07).
- Wingfield, J. (1984). *Bugging, a complete survey of electronic surveillance today*. R. Hale.
- Wise, D. (1992). *Molehunt: the secret search for traitors that shattered the CIA*. Random House. ISBN: 9780394585147.
- Wood, D.M. et al. (2006). "A report on the surveillance society". In: *Surveillance Studies Network, UK*.
- WorldTimeZone.com (2019). *GSM World Coverage Map and GSM Country List*. URL: <https://www.worldtimezone.com/gsm.html> (visited on 2019-09-06).

- Wright, P. (1987a). *Spycatcher : the candid autobiography of a senior intelligence officer*. New York, N.Y., USA: Viking. ISBN: 9780670820559.
- (1987b). *Spycatcher : the candid autobiography of a senior intelligence officer*. New York, N.Y., USA: Viking, pp. 109–110. ISBN: 9780670820559.
- Wright, S. (2002). “The ECHELON trail: An illegal vision”. In: *Surveillance & Society* 3.2/3. ISSN: 1477-7487.
- Zhu, T. et al. (2014). “Context-free Attacks Using Keyboard Acoustic Emanations”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’14. Scottsdale, Arizona, USA: ACM, pp. 453–464. ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660296. URL: <http://doi.acm.org/10.1145/2660267.2660296>.
- Zhuang, L., F. Zhou, and J. D. Tygar (Nov. 2009). “Keyboard Acoustic Emanations Revisited”. In: *ACM Trans. Inf. Syst. Secur.* 13.1, 3:1–3:26. ISSN: 1094-9224. DOI: 10.1145/1609956.1609959. URL: <http://doi.acm.org/10.1145/1609956.1609959>.