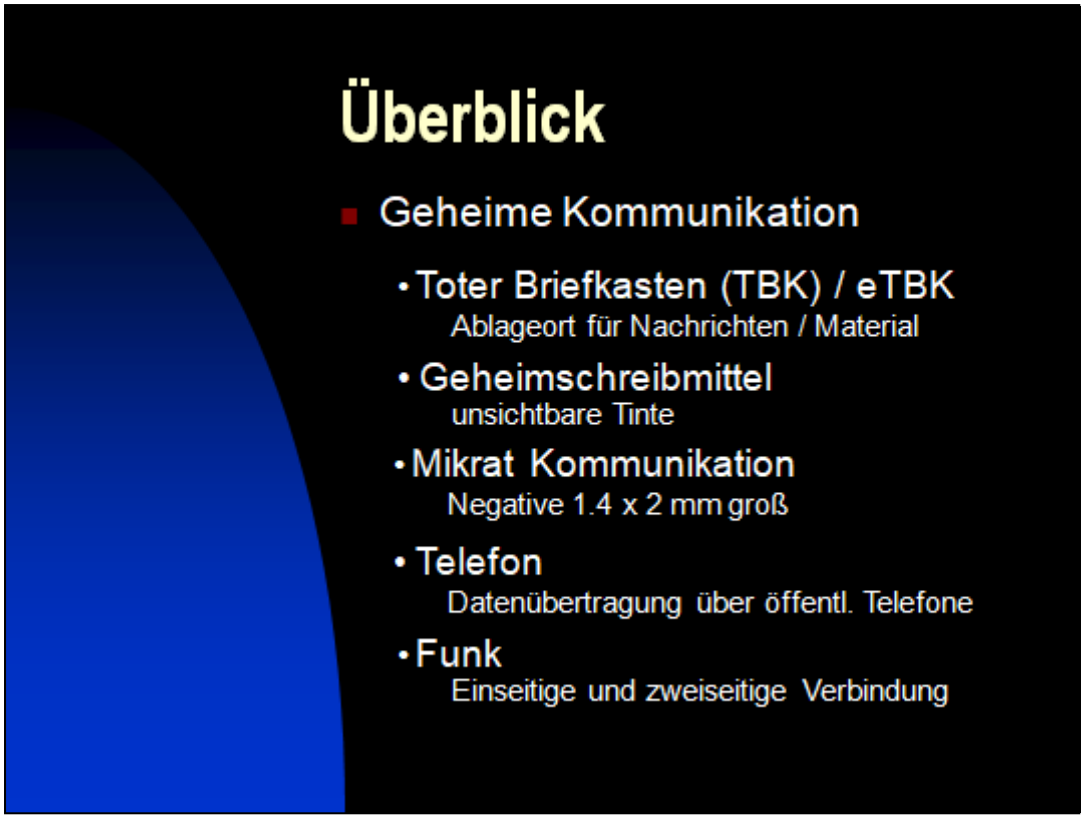
Guten Tag, meine sehr verehrten Damen und Herren,

Mein Namen ist Detlev Vreisleben und ich möchte über die geheime Kommunikation und Kryptografie in Deutschland während des Kalten Krieges sprechen.

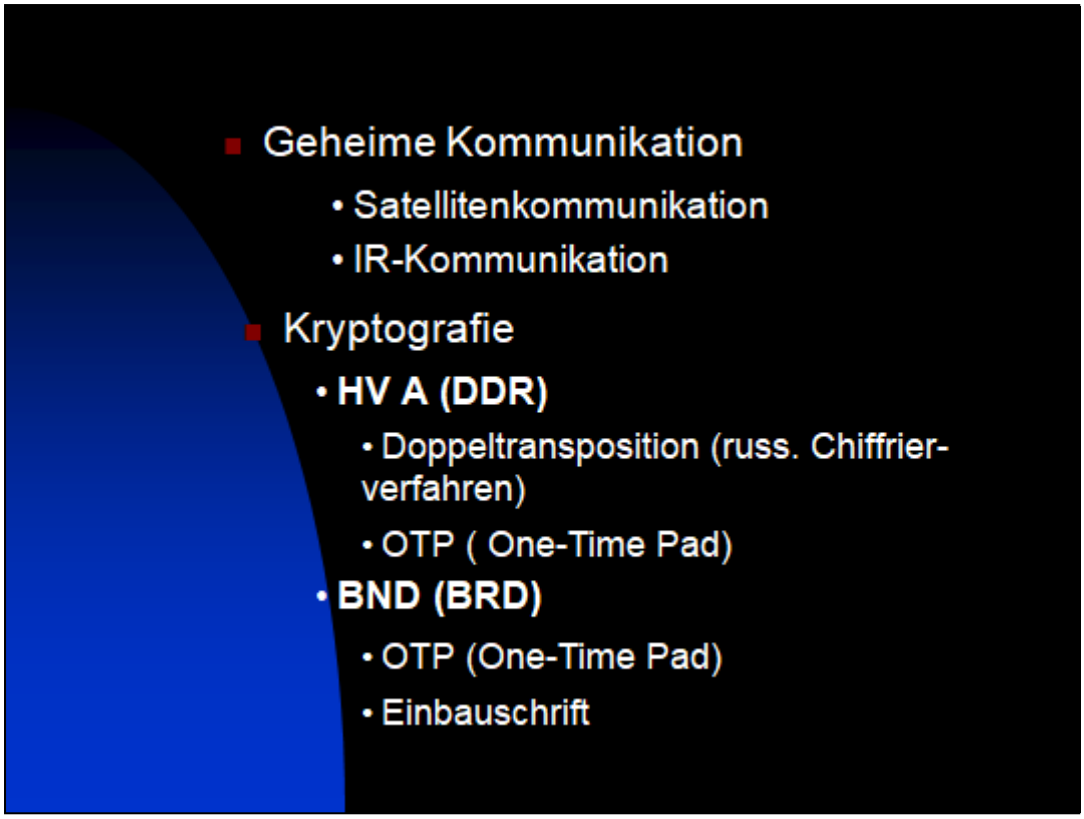
Hier sehen Sie Markus Wolf, den Leiter der HV A, der Auslandsspionage der DDR, dargestellt als Luchs. Er zeigt die Verwendung von Geheimschreibmitteln wie unsichtbare Tinte. Dieses Cartoon ist vom DDR Cartoonisten Erich Schmitt zum 60, Geburtstag von Markus Wolf im Jahr 1983 gezeichnet worden.

Der Luchs genießt im Fabelwesen ein besseres Ansehen als der Wolf, der ja Rotkäppchens Großmutter gefressen hat.



Ich möchte Ihnen hier die vielfältigen Möglichkeiten der geheimen Kommunikation zeigen.

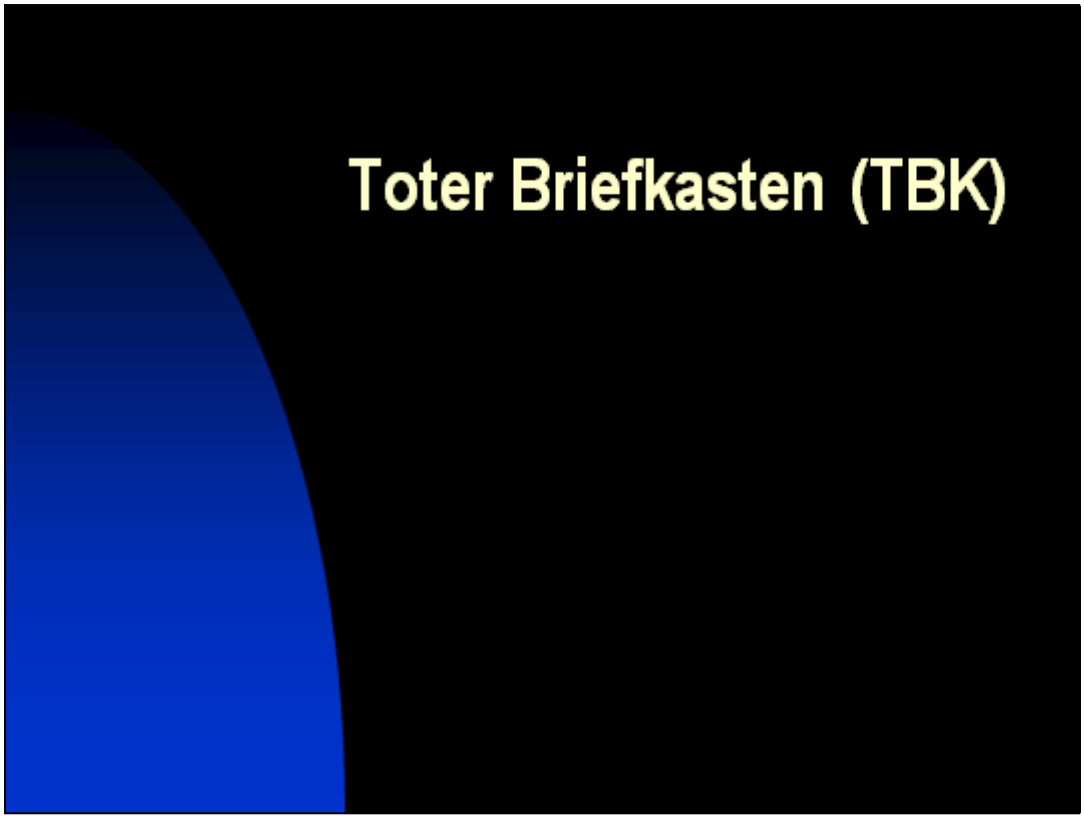
Ein Mikrat ist ein größeres Negativ als ein Mikropunkt, häufig 1,4 x 2 mm groß.



Die Satellitenkommunikation hat immer mehr an Bedeutung gewonnen.

Die IR-Kommunikation hat eine lange Geschichte, das Photophon wurde bereits 1880 von Graham Bell erfunden.

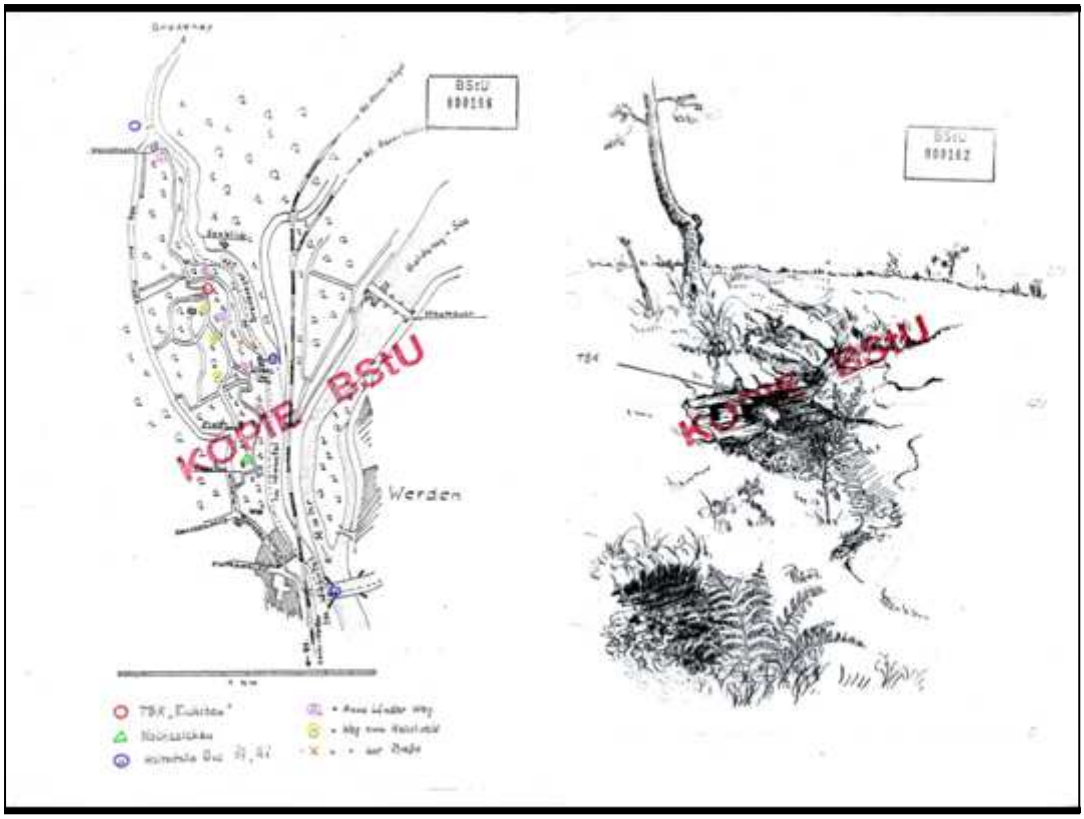
Im zweiten Teil gehe ich auf die Kryptografie ein, die von der HV A und dem BND verwendet worden ist.



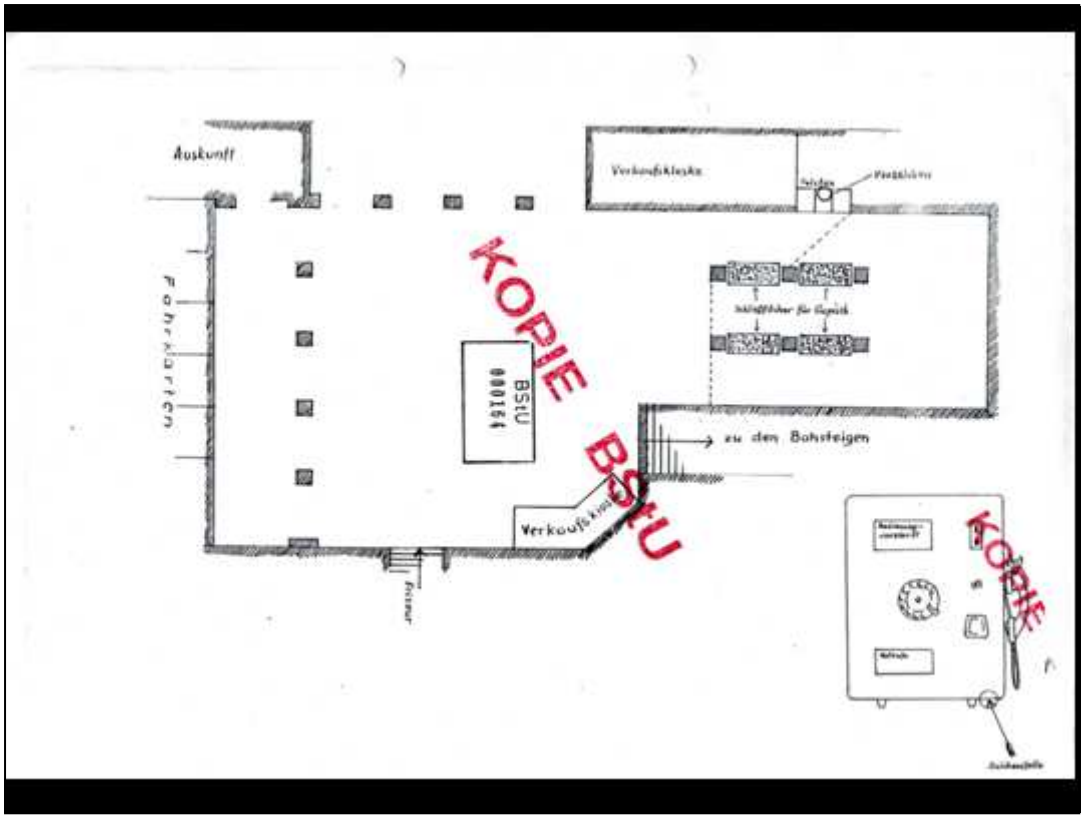
Ein Toter Briefkasten ist ein verabredeter Ort, wo Spione und Kuriere Informationen und Material ohne persönlichen Kontakt austauschen können.

Dies ist ein russischer Container, der als Toter Briefkasten benutzt worden ist, um Geld, Filme und Chiffrierunterlagen zu überbringen.

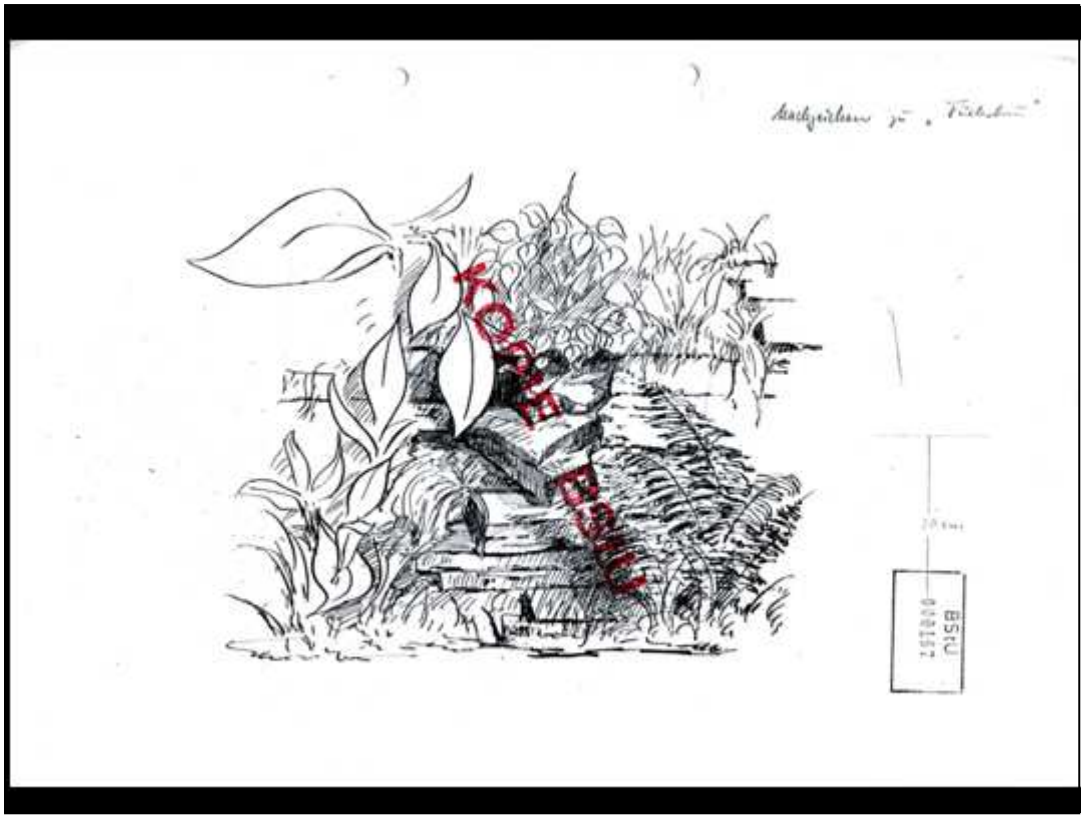
Ein TBK wird verwendet, um persönlichen Kontakt zu vermeiden, der zur Enttarnung führen könnte.



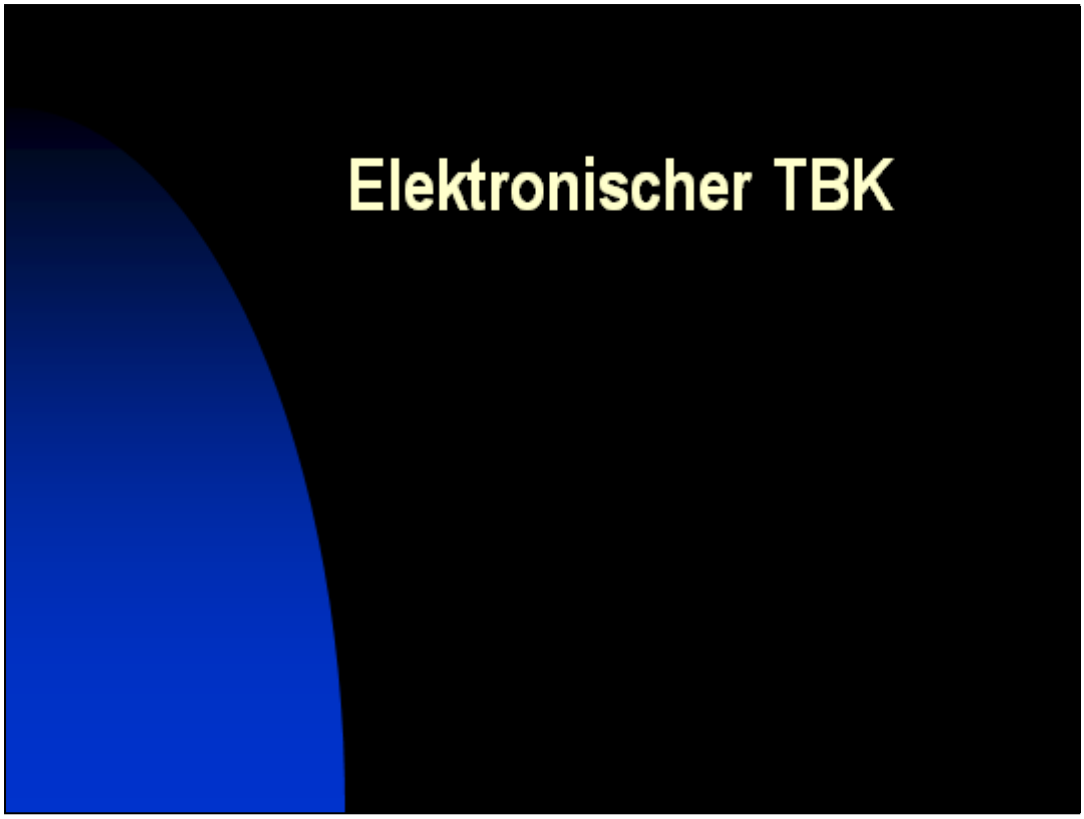
Ein Beispiel aus der DDR. Der Agent bekam Angaben, wo er den TBK finden kann.



Es gab ein Vorzeichen, wenn der TBK gefüllt war und geleert werden sollte. Am Telefon wurde rechts unten ein Kreidestrich angebracht, wenn der TBK zu leeren war.



Und ein Nachzeichen (Entleerungszeichen), wenn der TBK entleert worden ist: eine an dieser Stelle weggeworfene leere Ernte 23 Packung.



Der elektronische TBK heißt in Englisch SRAC, Short Range Agent Communication.

Diese Geräte speichern Informationen, die ein Agent im Vorbeigehen sendet und können von einem anderen ohne Kontakt zu dem Gerät abgerufen werden. Die Reichweite ist sehr begrenzt, einige 100 m.

Dar MfS begann in den 80er Jahren mit der Entwicklung solcher Geräte, drahtlos oder auch drahtgebunden über die Netzleitung z.B.

2006 entdeckte der FSB (russischer Inlandsgeheimdienst) zwei solcher Britischen SRACs in Moskau, die als Steine getarnt waren.

Stone Visitor
Каменный
гость
Russian TV documentary movie

Geheimschreibmittel

Geheimschrift, unsichtbare Tinte

Das ist eine Musterpostkarte für einen Agenten, wie er mit unsichtbarer Tinte zwischen die Textzeilen zu schreiben hat.

- 20 -

Bild 2 - Fotografische Dokumentation der entwickelten "Latenten Fotografie" auf der Bildseite der Ansichtskarte, die den Geheimtext an den Spion enthält.

(Der Geheimtext ist zusätzlich im gleichen Schriftbild abschriftlich oder als Vergrößerung beizulegen)

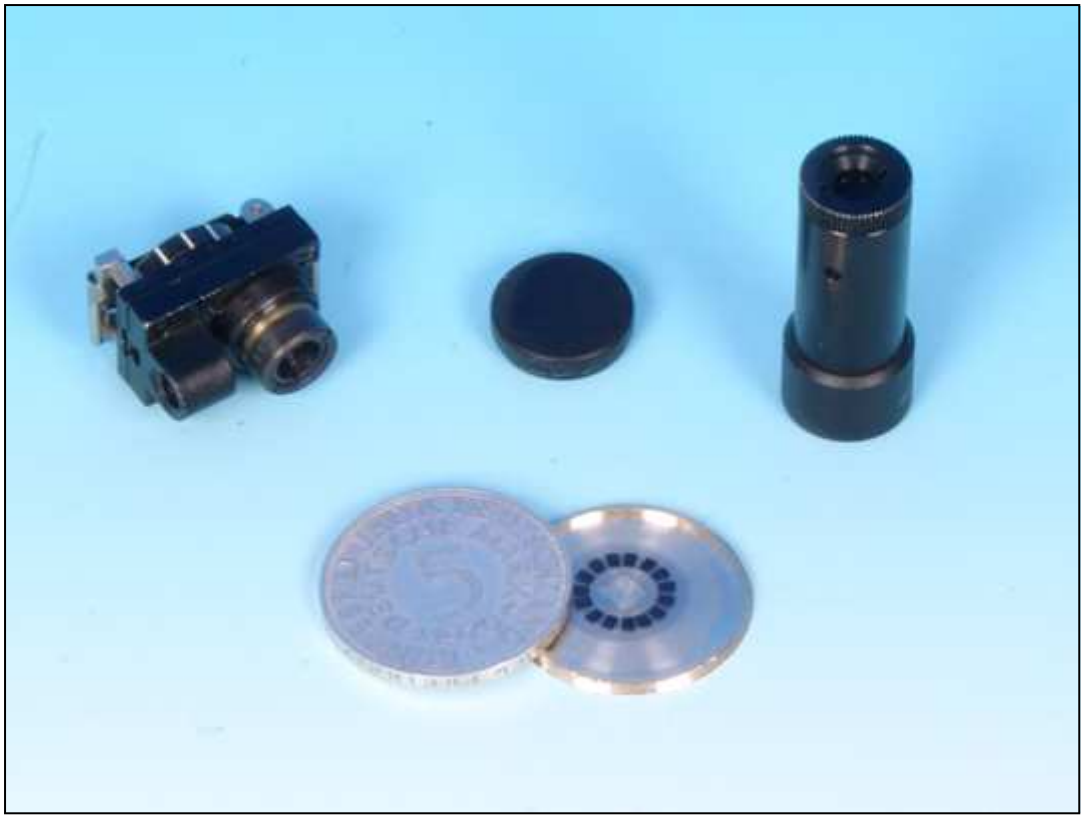
Eine Postkarte von der Zentrale an den Agenten, die einen versteckten, durch Entwicklung sichtbar gemachten Text im Bild der Postkarte enthält.

Einen unverschlüsselten Willkommensgruß für einen neuen Agenten!

Das Mikratverfahren ist ein zweiseitiges Verfahren, Anweisungen von der Zentrale zum Agenten und Dokumentenkopien vom Agenten zur Zentrale.

Ein Mikrat ist ein 1,4 x 2 mm großes Negativ. Es ist größer als ein Mikropunkt.

Wegen der geringen Abmessungen kann es unter einer Briefmarke, in Briefen, in aufgeschlitzten Postkarten oder in Paketen verschickt werden.



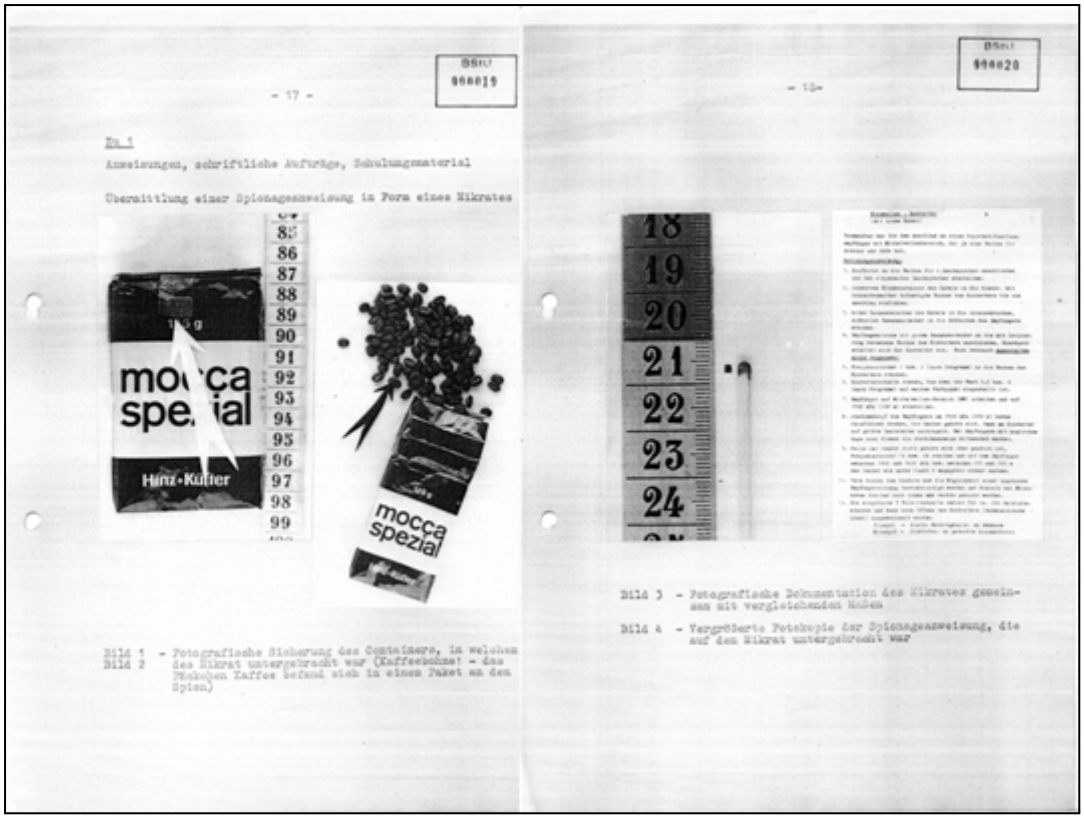
Links hinten eine Mikratkamera, die mit einem Klemmstativ an einer Tischplatte befestigt wird. Die abzufotografierenden Dokumente werden auf den Boden gelegt (Aufnahmeabstand 75 cm) und mit Fotolampen beleuchtet.

Hinten Mitte ein Filmdöschen, hinten rechts ein Mikroskop zur Überprüfung der entwickelten Mikrate.

Vorn in der Mitte ein Container zum Transport von Mikraten, ein hohles 5 DM Stück, das sich öffnen lässt , darin eine Filmscheibe mit 15 Mikrataufnahmen 1,4 x 2 mm, jeweils eine DIN A4 Seite.

Ein Mikratleser für Agenten.

Das Negativ kommt in den Schlitz auf der linken Seite, der Agent sieht in das Okular rechts und kann das Mikrat lesen.



- 17 -

Zu 1

Anweisungen, schriftliche Aufträge, Schulungsmaterial

Übermittlung einer Spionageanweisung in Form eines Mikrates

Bild 1 - Fotografische Sicherung des Containers, in welchen
Bild 2 des Mikrat untergebracht war (Kaffeebohne - das Mikrat im Kaffee befand sich in einem Paket an den Spion)

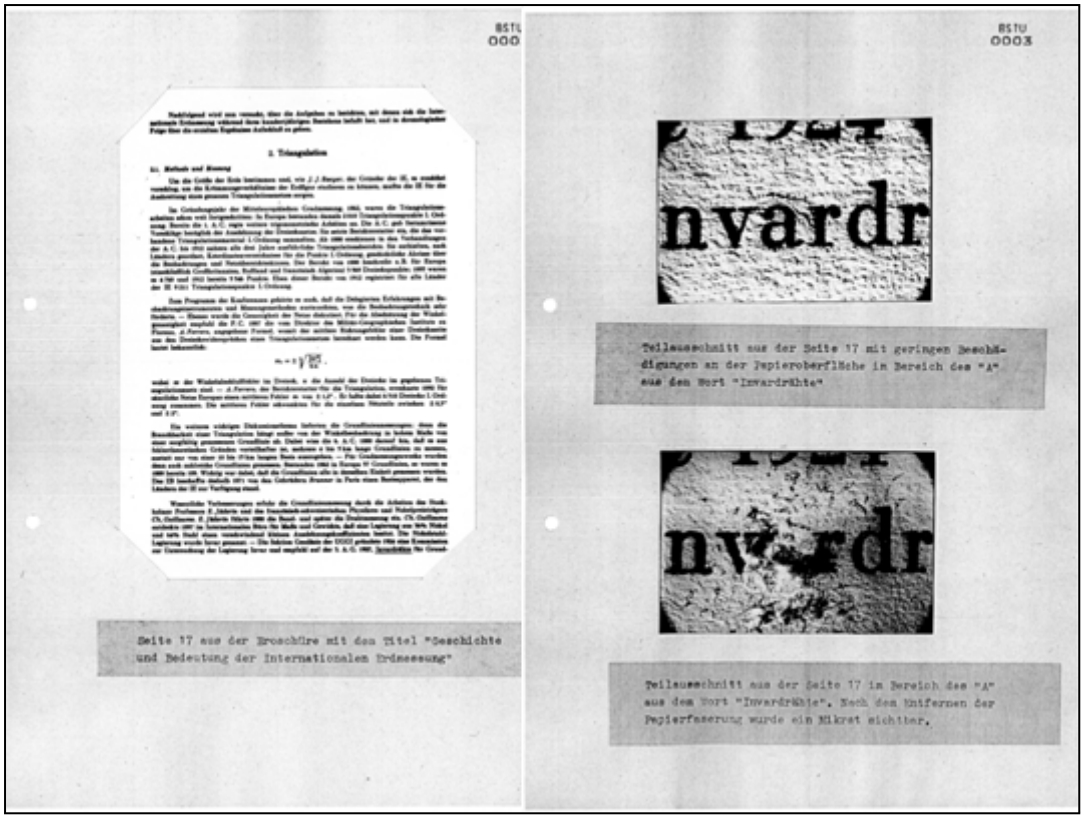
- 18 -

Bild 3 - Fotografische Dokumentation des Mikrates gemeinsam mit vergleichenden Mustern

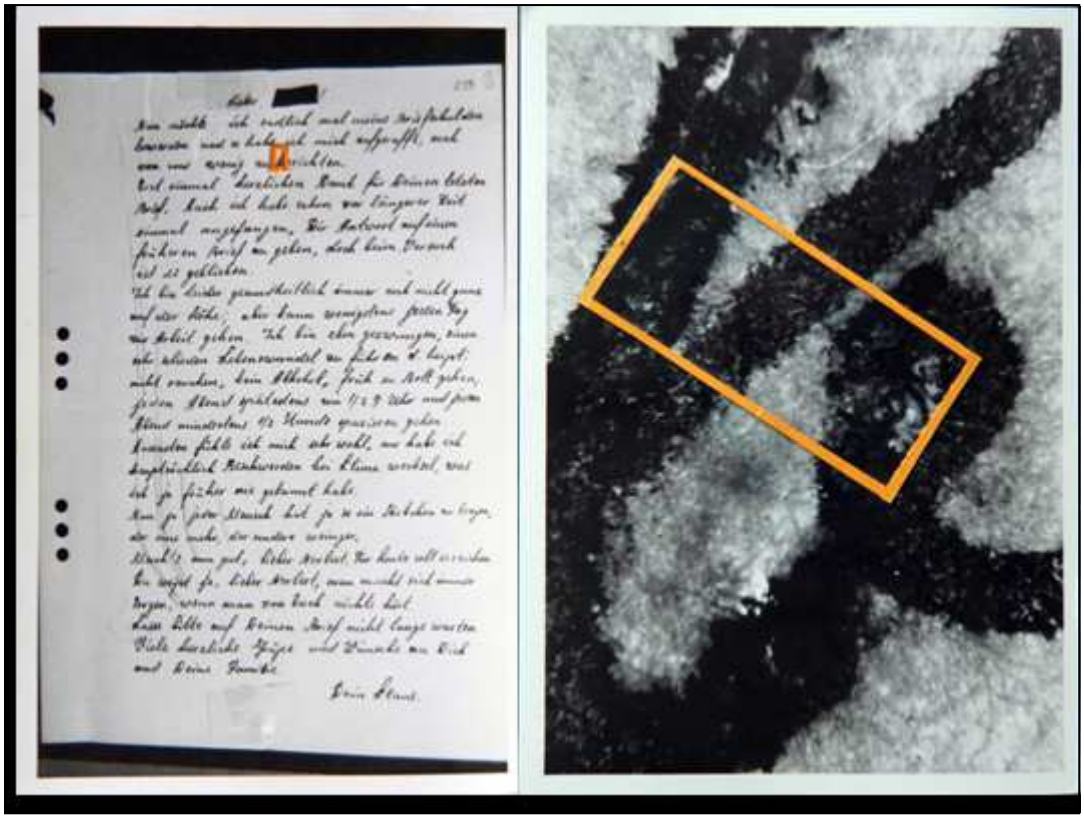
Bild 4 - Vergrößerte Fotokopie der Spionageanweisung, die auf dem Mikrat untergebracht war

Hier sehen Sie ein Mikrat versteckt in einer Kaffeebohne. Es enthält die Bedienungsanleitung für den KW-Konverter eines BND Agenten.

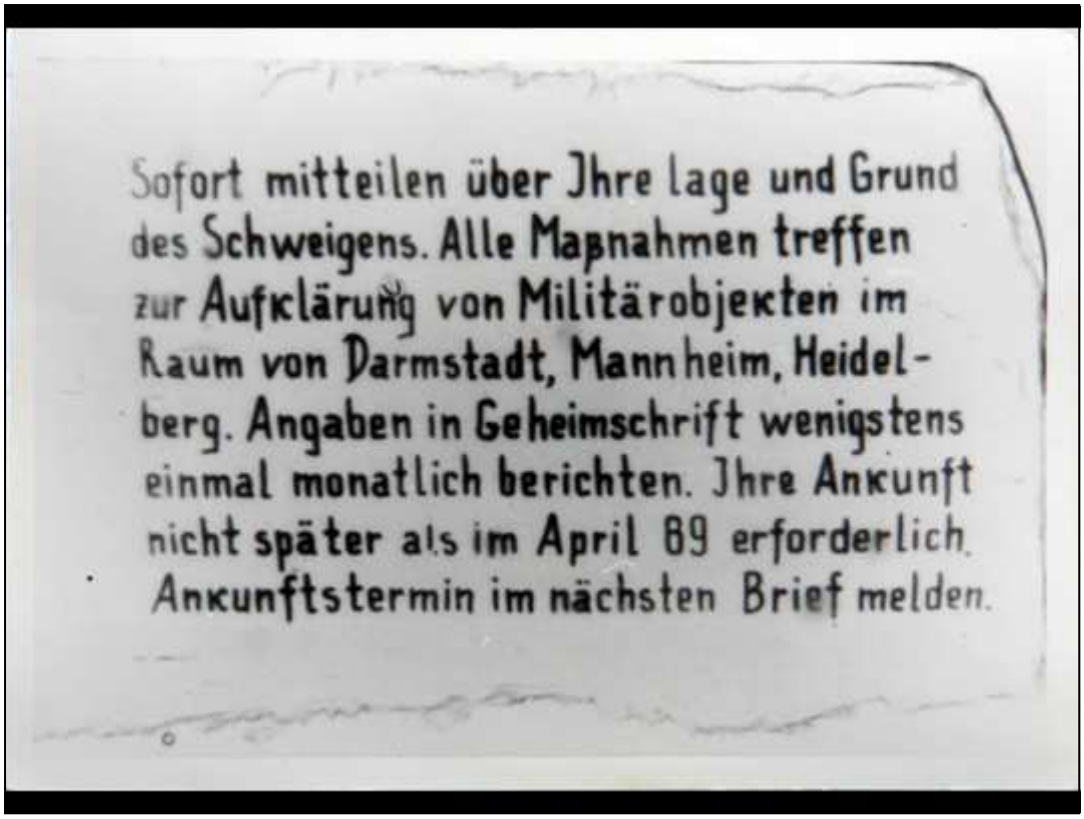
Am Paket war versteckt ein Hinweis auf das Mikrat, z. B. die Position in dem Inhaltsverzeichnis oder ein kleines Negativ, das im Packpapier an verabredeter Stelle verborgen war. Aber wie hat das MfS das herausgefunden? Möglicherweise weil mehrere gleich verpackte Pakete mit dem gleichen Inhalt gefunden worden sind.



Ein Mikropunkt versteckt in einer Broschüre. Er ist nur 0,6 x 0,9 mm groß.

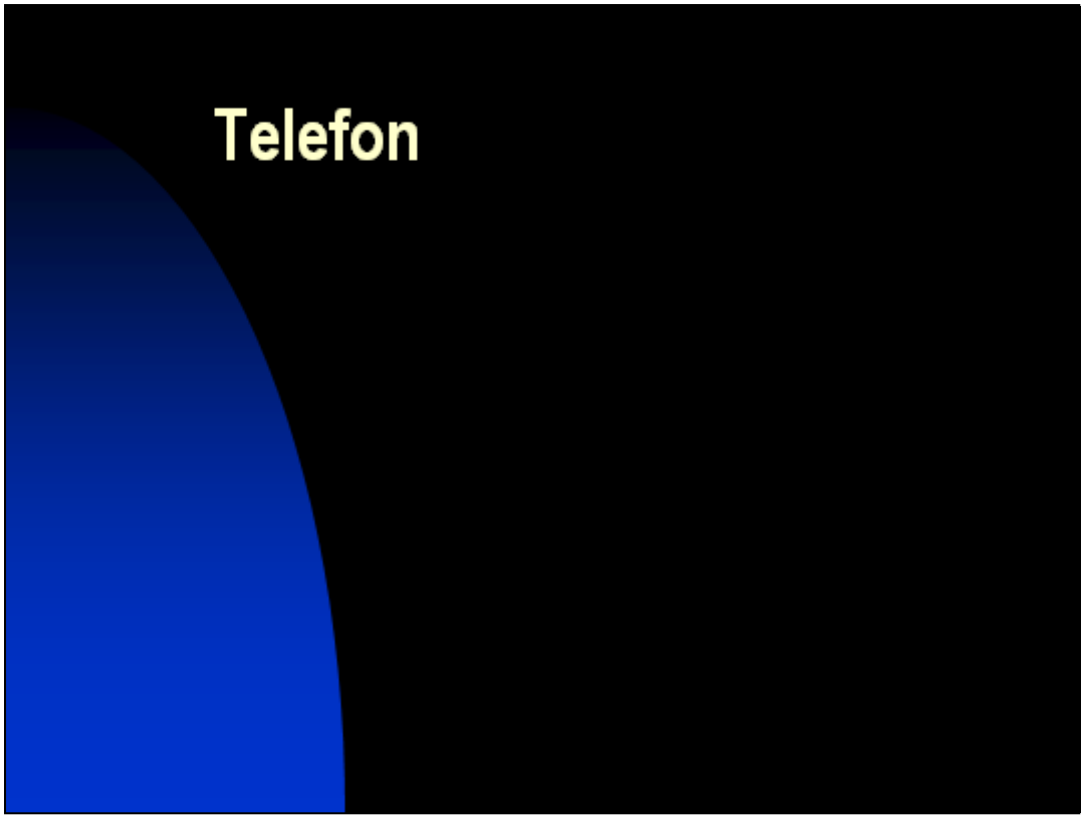


Die HV A hat dieses Verfahren noch 1989 verwendet. Der Agent war informiert, wo sich das Mikrat befand.



Sofort mitteilen über Ihre Lage und Grund des Schweigens. Alle Maßnahmen treffen zur Aufklärung von Militärobjekten im Raum von Darmstadt, Mannheim, Heidelberg. Angaben in Geheimschrift wenigstens einmal monatlich berichten. Ihre Ankunft nicht später als im April 89 erforderlich. Ankunftstermin im nächsten Brief melden.

Hier der vergrößerte Text



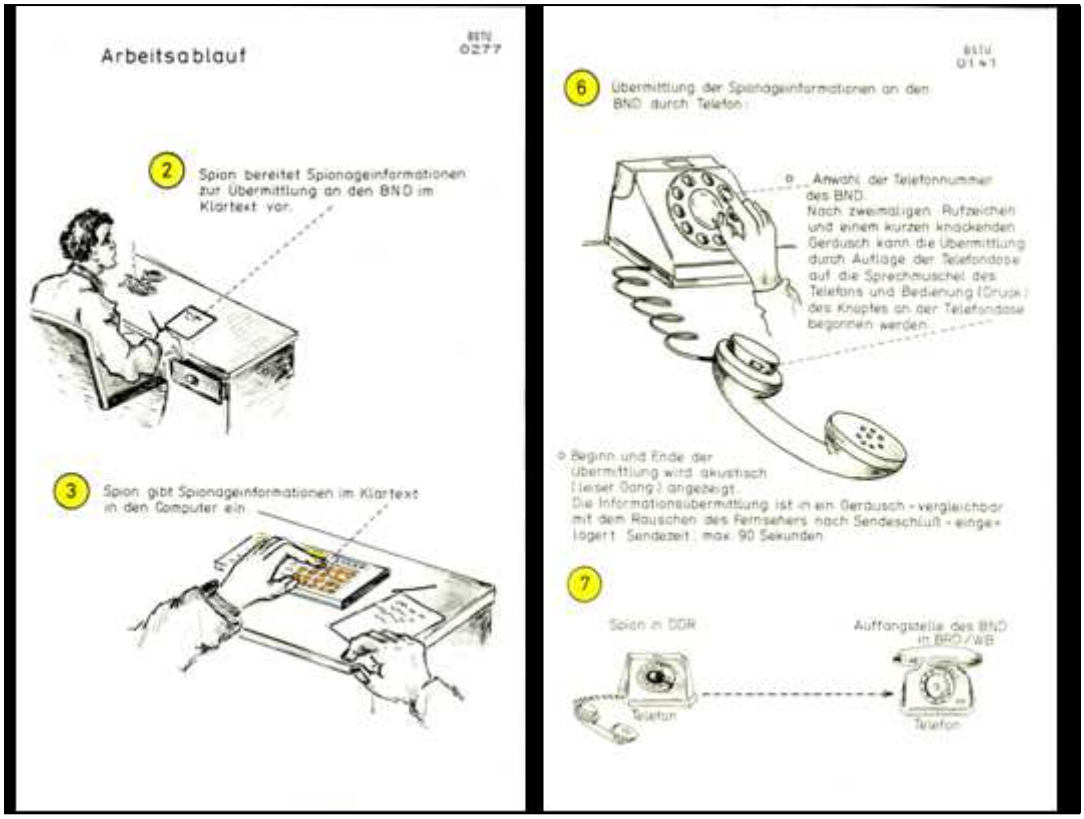
Über das öffentliche Telefonnetz können Daten übertragen werden.

Der Agent sendet vorher verschlüsselte Nachrichten, die im modifizierten Taschenrechner gespeichert sind, mit einem Akustikkoppler in einer öffentlichen Telefonzelle.

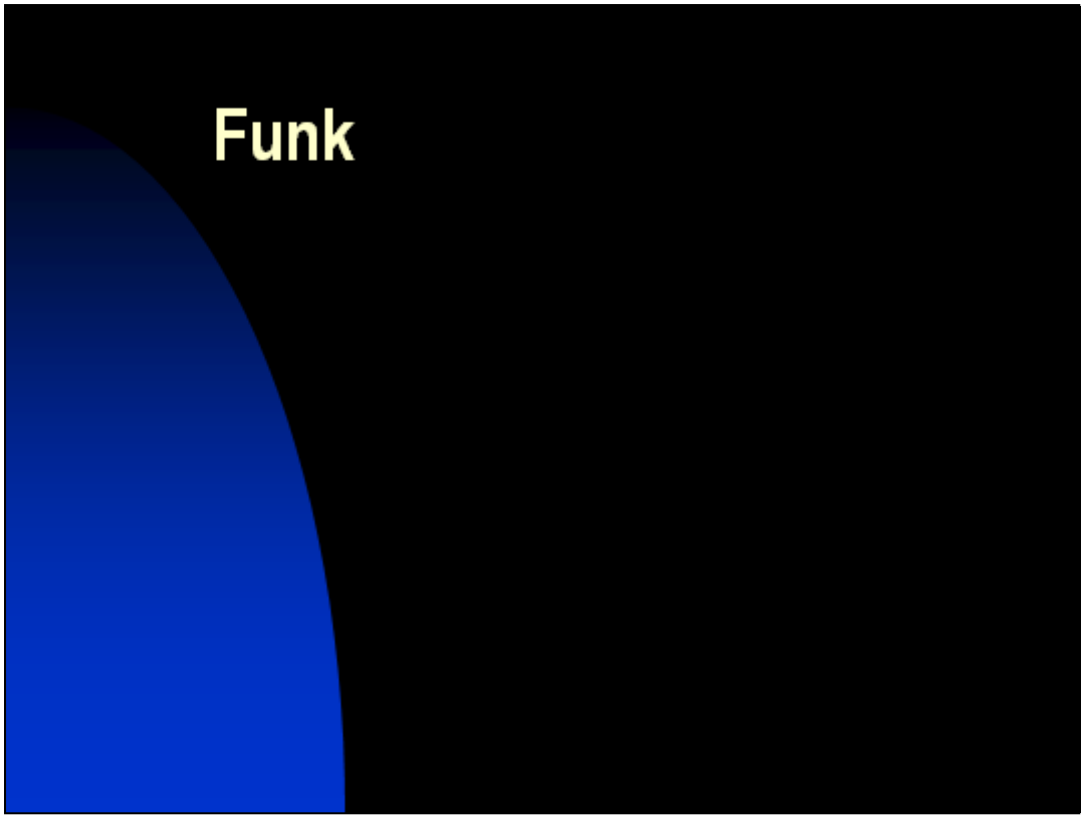
Links der Taschenrechner

Rechts der Computer TSG 7, mit dem in einer verabredeten Stelle die Nachricht empfangen und ausgedruckt wurde.

Rainer Rupp (Topas) hat 1983 während des NATO-Manövers „Able Archer“ mit diesem Verfahren (HD) Nachrichten nach Ost-Berlin geschickt, dass er keine Angriffspläne der NATO sieht.



Der BND hat ein ähnliches Verfahren genutzt, hier Bilder der HA II, Spionageabwehr. Leider fehlt eine Information, ob auf dem Sharp Computer verschlüsselt worden ist.



Es gibt 2 Arten der Funkkommunikation.

Den einseitigen Funk von der Zentrale zum Agenten
und den zweiseitigen Funk, dort antwortet der Agent per Funk

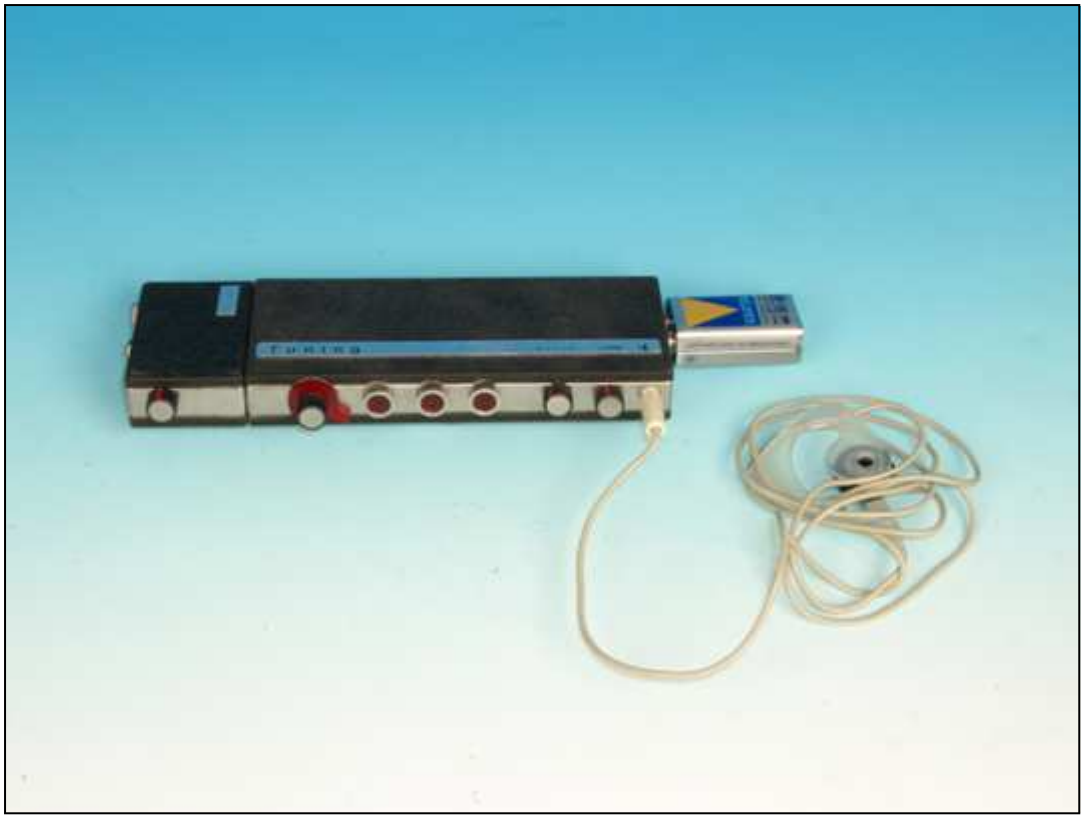
Funkkommunikation war weit verbreitet. Etwa 200 HV A Agenten empfingen ihre Anweisungen per Funk, aber nur 15 hätten im Spannungsfall per Funk antworten können.

Das ist der Sprach-Morse-Generator für verschlüsselte Nachrichten.
Sprache wurde in Europa übertragen, für Übersee Morsezeichen

Das Gesicht hinter der Stimme.

Normalerweise benutztendie Agenten handelsübliche Empfänger, um ihre Nachrichten zu empfangen.

Sie schalteten sie zur verabredeten Zeit auf der verabredeten Frequenz ein.



Für Sonderfälle hatte die HV A spezielle Empfänger

In der ersten Zeit rüstete der BND seine Agenten in der DDR mit einem Kurzwellenkonverter aus, weil die DDR Radios nicht die Frequenzen empfangen konnte, die der BND verwendete

Später wurden BND Agenten mit einem FE-10 Kurzwellenempfänger ausgestattet.

Die HV A Sendestelle war in Zeesen bei Berlin, die Empfangsstelle in Wernsdorf

Der BND nutzte 3 Sendestellen: München, Monschau und zusammen mit der CIA Frankfurt/Main

Ein Blick in die Sendestelle Zeesen. Verwendet wurden deutsche und russische 1 bis 20 kW Sender

Ein Blick auf die Antennen in Zeesen

So sieht das heute in Polen aus. Südwestlich von Warschau liegt dieses Gebäude mit ca. 15 Antennenmasten auf dem Freifeld. Dieses Bild stammt von Google Maps 2010, heute ist genau dieses Grundstück verpixelt.

Mit StreetView kann man die Antennen besser erkennen, das Schild „ BRAMA WJAZDOWA“ (Einfahrt freihalten) am Tor ist verpixelt!

Auf den Bildern von 2017 ist ein neues Schild zu sehen, was auf einen militärischen Bereich hinweist.

Links der Sender der HV A, rechts der des BND. Entstehende Ähnlichkeiten sind nicht zufällig.

BND Agenten haben zum letzten mal 1974 auf KW gesendet

Ein BND SP15 im Container, der Agent bekam 20 Quarze

Auch die CIA benutzte das SP 15 (FSS-7). Der Agent „JADUR“ hatte es im Emster Kanal bei Berlin versenkt.

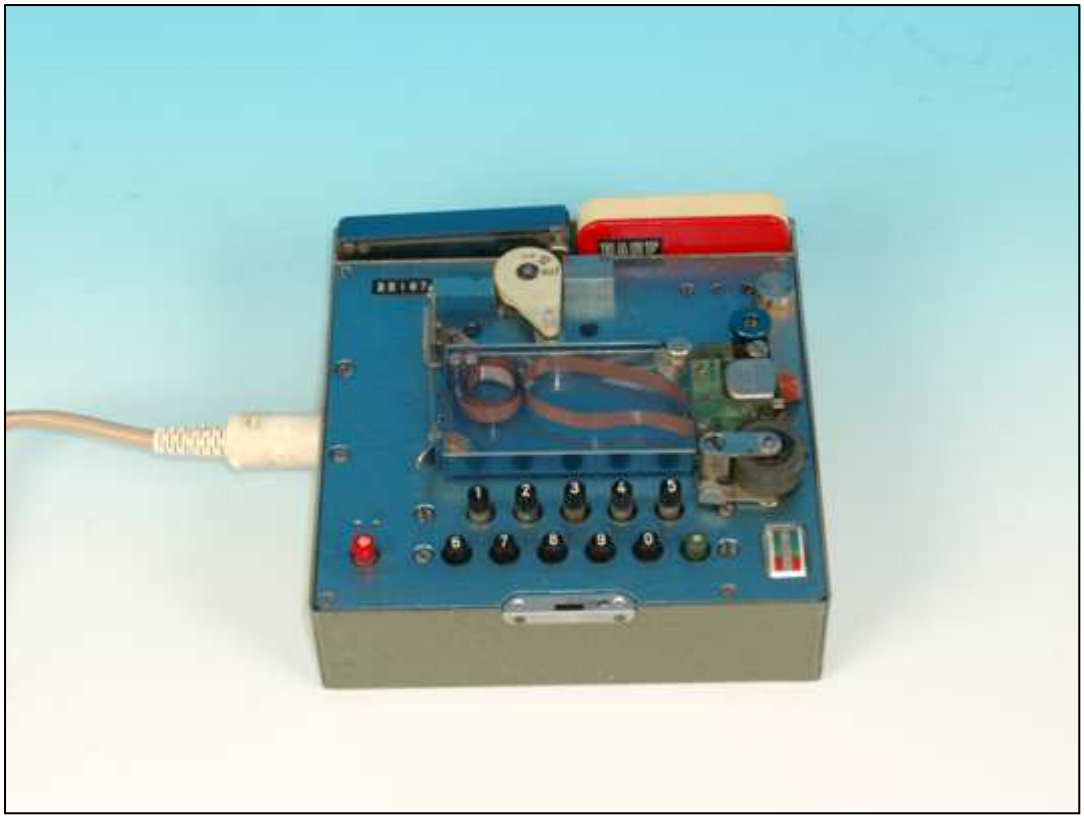
Hier der Schnellgeber KE 8, der an das FSS-7 angepasst worden ist.

Die CIA stellte JADUR 72 Quarze zur Verfügung!

Ende der 80er Jahre rüstete der BND seine Überrollagenten mit einem digitalen Gerät FS 5000 (Harpoon) aus, das von Telefunken entwickelt und gebaut worden ist.

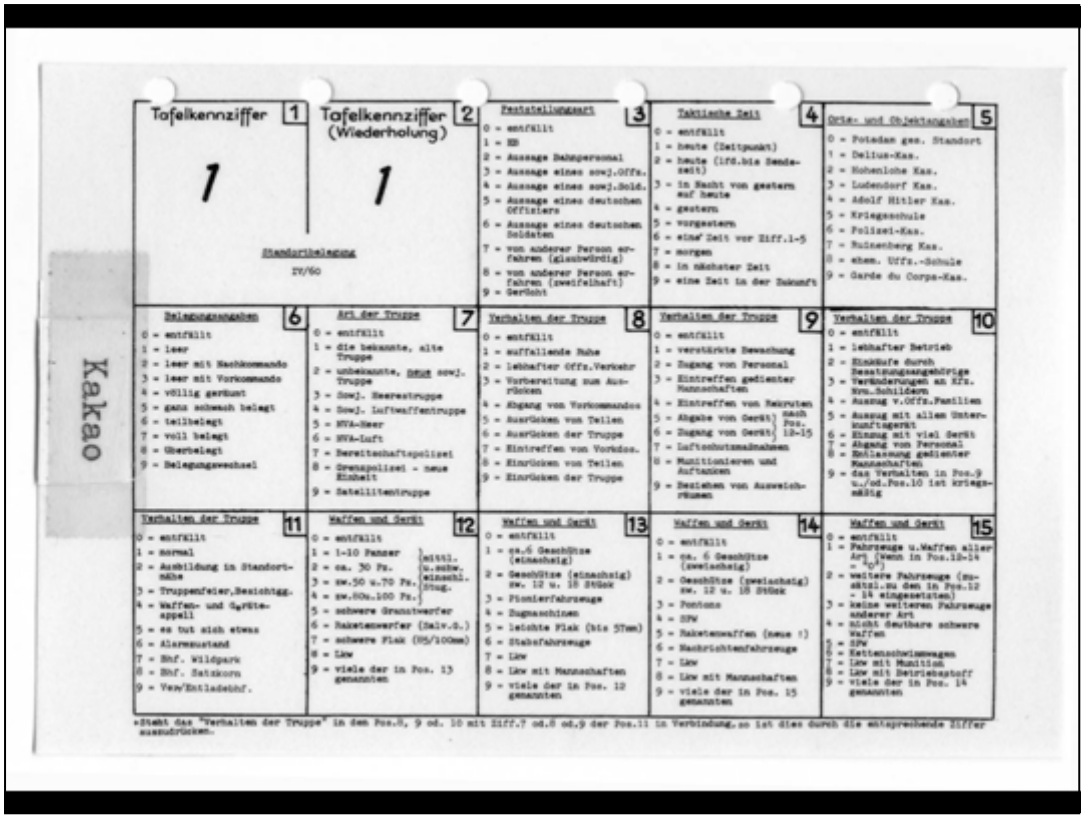
Das 3WU war das erste von der OG 1947 entwickelte Funkgerät. Es wurde in den USA gebaut. Der Namen bedeutet 3 Watt Universalgerät, weil es wie ein Vielfachmeßgerät aussehen sollte.

Der Nachfolger 12 WG (12 Watt Gerät) wurde von der OG gebaut, nicht von Wandel & Goltermann.



Um die Gefahr zu reduzieren, dass die Agenten beim Senden angepeilt werden konnten, verwendete man Schnellgeber, um die Sendezeit zu reduzieren. Hier ein Gerät der HV A, dass das Senden verschlüsselter Nachrichten gestattet.

Dieser BND Schnellgeber gestattet die Übertragung von 25 Zeichen. Was kann man denn damit übermitteln?



Tafelkennziffer 1

1

Tafelkennziffer (Wiederholung) 2

1

Standortbelegung

IV/60

Feststellungsart 3

0 = entfällt
1 = KB
2 = Aussage Bahnpersonal
3 = Aussage eines sowj.Offs.
4 = Aussage eines sowj.Sold.
5 = Aussage eines deutschen Offiziers
6 = Aussage eines deutschen Soldaten
7 = von anderer Person erfahren (glaubwürdig)
8 = von anderer Person erfahren (zweifelhaft)
9 = Gerücht

Taktische Zeit 4

0 = entfällt
1 = heute (Zeitpunkt)
2 = heute (lfd.bis Sendezeit)
3 = in Nacht von gestern auf heute
4 = gestern
5 = vorgestern
6 = einige Zeit vor Ziff.1-5
7 = morgen
8 = in nächster Zeit
9 = eine Zeit in der Zukunft

Orts- und Objektangaben 5

0 = Potsdam gen. Standort
1 = Dellus-Kas.
2 = Hohenlohe Kas.
3 = Ludendorf Kas.
4 = Adolf Hitler Kas.
5 = Kriegsschule
6 = Polizei-Kas.
7 = Ruhnenberg Kas.
8 = ehem. Offs.-Schule
9 = Garde du Corps-Kas.

Belegungsangaben 6

0 = entfällt
1 = leer
2 = leer mit Nachkommando
3 = leer mit Vorkommando
4 = völlig gerbunt
5 = ganz schwach belegt
6 = teilbelegt
7 = voll belegt
8 = Überbelegt
9 = Belegungswechsel

Art der Truppe 7

0 = entfällt
1 = die bekannte, alte Truppe
2 = unbekannte, neue sowj. Truppe
3 = Sowj. Heerestruppe
4 = Sowj. Luftwaffentruppe
5 = NVA-Heer
6 = NVA-Luft
7 = Bereitschaftspolizei
8 = Grenzpolizei - neue Einheit
9 = Satellitentruppe

Verhalten der Truppe 8

0 = entfällt
1 = auffallende Ruhe
2 = lebhafter Offz.Verkehr
3 = Vorbereitung zum Ausrücken
4 = Abgang von Vorkommandos
5 = Ausrücken von Teilen
6 = Ausrücken der Truppe
7 = Eintreffen von Vorkdos.
8 = Einrücken von Teilen
9 = Einrücken der Truppe

Verhalten der Truppe 9

0 = entfällt
1 = verstärkte Bewachung
2 = Zugang von Personal
3 = Eintreffen gedienter Mannschaften
4 = Eintreffen von Rekruten
5 = Abgabe von Gerät } nach Pos. 12-15
6 = Zugang von Gerät }
7 = Luftschutzmaßnahmen
8 = Munitionieren und Auftanken
9 = Bestehen von Ausweichräumen

Verhalten der Truppe 10

0 = entfällt
1 = lebhafter Betrieb
2 = Einsätze durch Besatzungsangehörige
3 = Veränderungen an Kfz. Nrn.Schildern
4 = Auszug v.Offs.Familien
5 = Auszug mit allem Unterkunftsgerät
6 = Einzug mit viel Gerät
7 = Abgang von Personal
8 = Entlassung gedienter Mannschaften
9 = das Verhalten in Pos.9 u./od.Pos.10 ist kriegsmäßig

Verhalten der Truppe 11

0 = entfällt
1 = normal
2 = Ausbildung in Standortnähe
3 = Truppenfeier,Besichtigg.
4 = Waffen- und G.prüfeappell
5 = es tut sich etwas
6 = Alarmzustand
7 = Bhf. Wildpark
8 = Bhf. Satzkorn
9 = Verw/Entladebhf.

Waffen und Gerät 12

0 = entfällt
1 = 1-10 Panzer } mittl. u.schw. einschl. Stug.
2 = ca. 30 Pz.
3 = zw.50 u.70 Pz.
4 = zw.60u.100 Pz.
5 = schwere Granatwerfer
6 = Raketenwerfer (Salv.G.)
7 = schwere Flak (85/100mm)
8 = LKW
9 = viele der in Pos. 13 genannten

Waffen und Gerät 13

0 = entfällt
1 = ca.6 Geschütze (einzelnstg)
2 = Geschütze (einzelnstg) zw. 12 u. 18 Stück
3 = Pionierfahrzeuge
4 = Zugmaschinen
5 = leichte Flak (bis 37mm)
6 = Stabsfahrzeuge
7 = LKW
8 = LKW mit Mannschaften
9 = viele der in Pos. 12 genannten

Waffen und Gerät 14

0 = entfällt
1 = ca. 6 Geschütze (zweizahnig)
2 = Geschütze (zweizahnig) zw. 12 u. 18 Stück
3 = Pontons
4 = SPW
5 = Raketenwaffen (neue !)
6 = Nachrichtenfahrzeuge
7 = LKW
8 = LKW mit Mannschaften
9 = viele der in Pos. 15 genannten

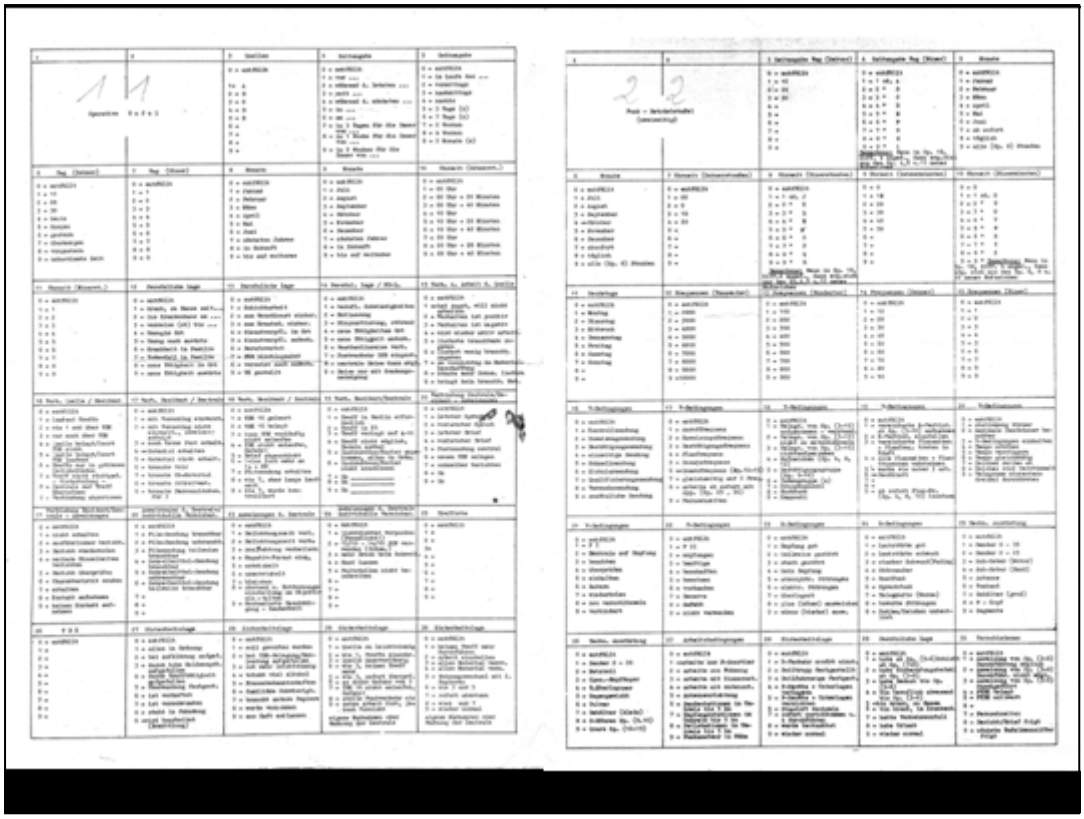
Waffen und Gerät 15

0 = entfällt
1 = Fahrzeuge u.Waffen aller Art (wenn in Pos.12-14 - Sp*)
2 = weitere Fahrzeuge (zusätzl.zu den in Pos.12 - 14 eingesetzten)
3 = keine weiteren Fahrzeuge anderer Art
4 = nicht deutbare schwere Waffen
5 = SPW
6 = Kettenschwimmwagen
7 = LKW mit Munition
8 = LKW mit Betriebsstoff
9 = viele der in Pos. 14 genannten

*Steht das "Verhalten der Truppe" in den Pos.8, 9 od. 10 mit Ziff.7 od.8 od.9 der Pos.11 in Verbindung, so ist dies durch die entsprechende Ziffer auszudrücken.

Kakao

Einen kompletten Lagebericht, es gab mehrere solcher Tafeln an die Bedürfnisse des Agenten angepasst. Auf dieser Tafel 1 aus 1960 wird noch die Adolf Hitler Kaserne aufgeführt!



Das sind die seltenen Tafeln für einen Residenten.

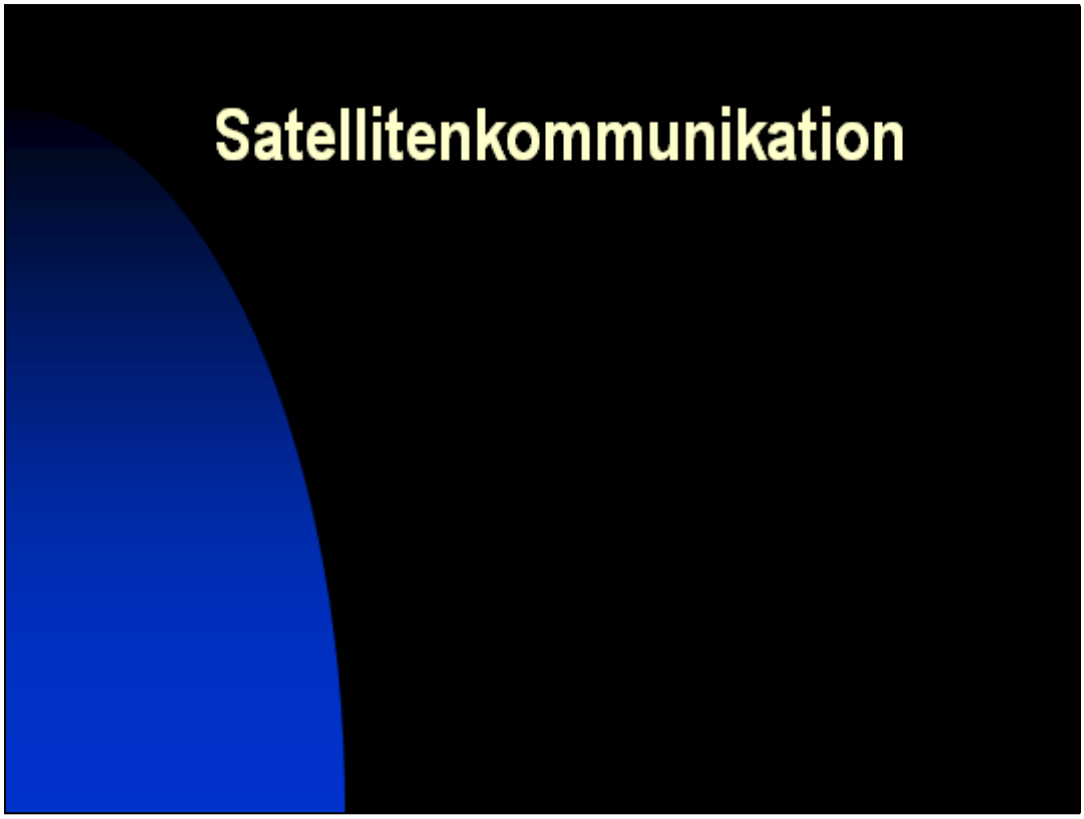
Der OTS war einfallsreich, hier eine Antenne, die aus zwei versilberten Regenschirmgestellen besteht, damit sie schnell z.B. in einem Hotel aufgebaut werden kann.

Es gab ein UKW Kommunikationssystem „Horizont“, das auf etwa 100 … 150 km von der DDR Grenze begrenzt war. Hier ist das Nachfolgesystem zu sehen, das nicht mehr in den Einsatz gekommen ist.

Links der erste Laptop von EPSON als Bediengerät, in der Mitte der Sender, rechts der Empfänger.

Etwa 17 HV A Agenten sind mit Horizont Sendern ausgerüstet gewesen, keines dieser Geräte ist gefunden worden.

Eine der Empfangsantennen stand auf dem Brocken im Harz nahe der Grenze.

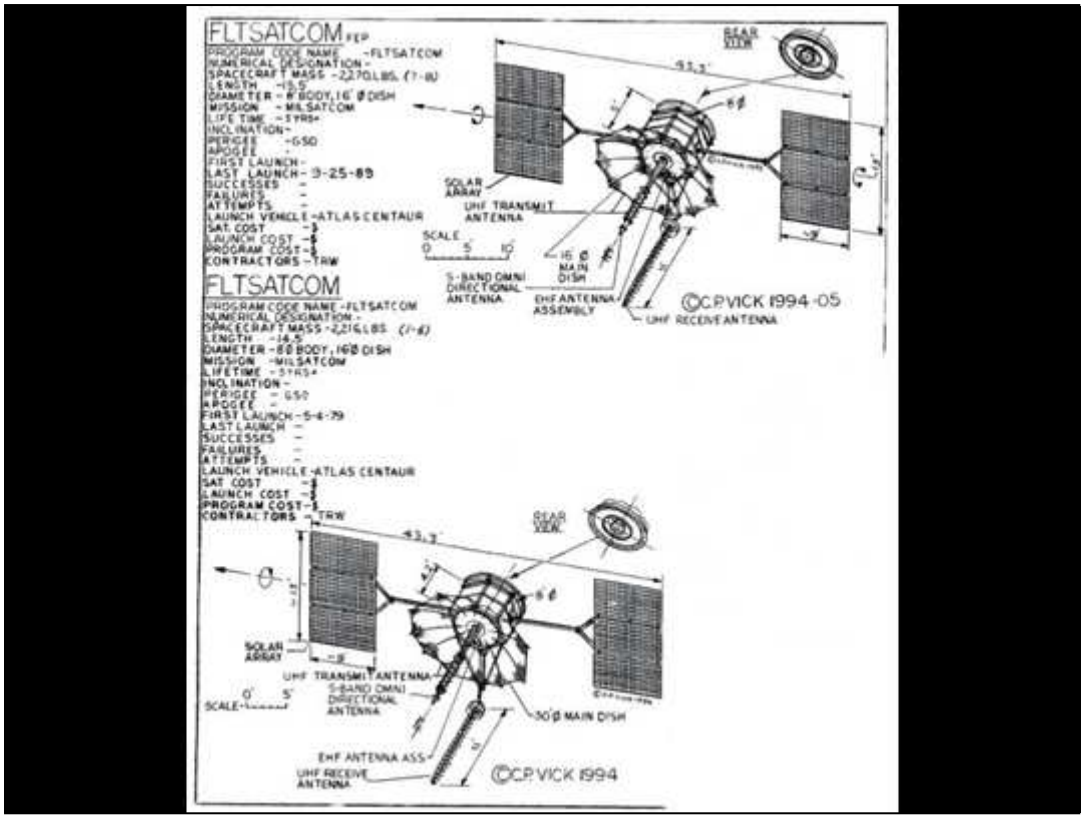


In den 80er Jahren begann die Satellitenkommunikation.

Der KGB beschlagnahmte 1983 in Moskau diesen Satellitensender bei einem Diplomaten. Heute hat die Satellitenkommunikation weitgehend den KW-Funk verdrängt.

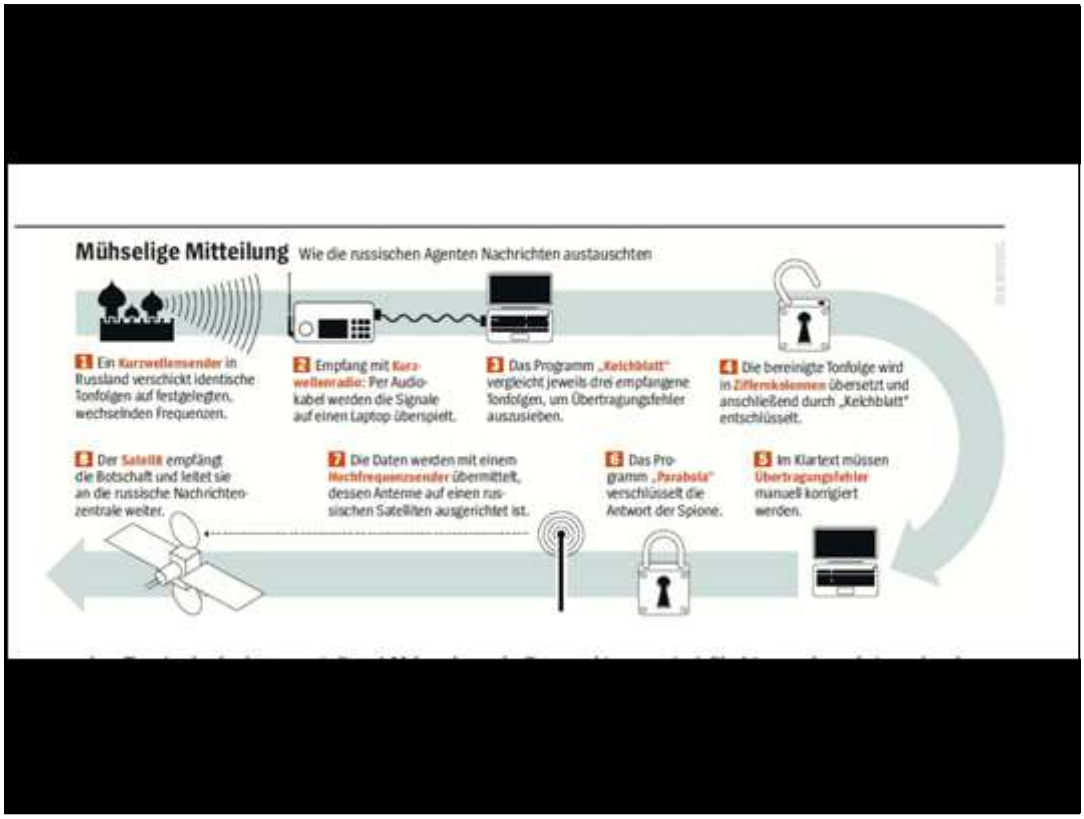
Das KGB-Foto zeigt den Sender RT-804, den Coder CK-42, das Batteriepack und Stromversorgung BS-804 sowie die Fernbedienung CPK-804. Der Sender arbeitete auf 311 MHz, das Projekt zum Aufspüren hatte den Decknamen „Pyramide“.

Quelle: BStU MfS HA II Nr. 44310



Die amerikanischen Fleet Sat Com Satelliten wurden zur Übertragung der Informationen genutzt, die von vergrabenen amerikanischen Sonden gesendet worden sind. Die Briten setzten S-Band Sonden ein, die wohl unentdeckt geblieben sind, aber auch Franzosen und Russen verwendeten Sonden.

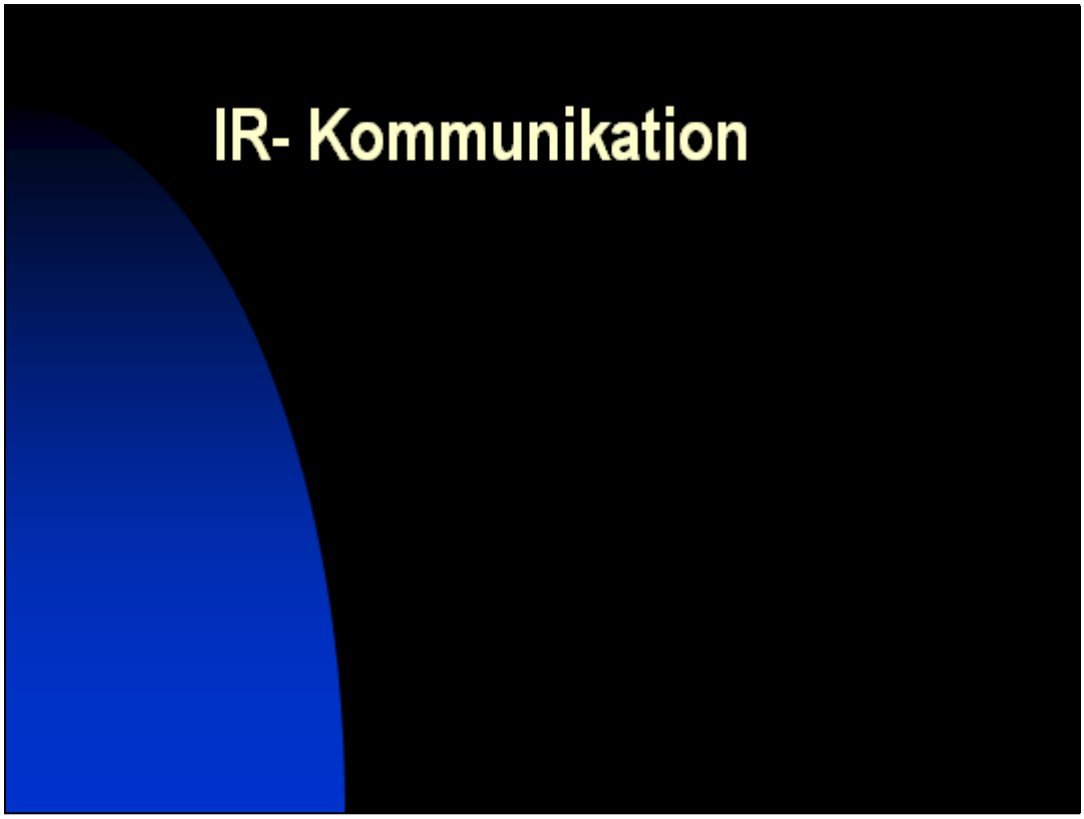
Die HV A wollte Agentenkommunikation über diese Satelliten betreiben, der OTS modifizierte dafür die Horizont-Sender.



Der SVR (Russischer Auslandsgeheimdienst) benutzt immer noch die KW-Kommunikation mit Agenten, heute werden aber keine Zahlen mehr gesprochen, sondern Töne übertragen.

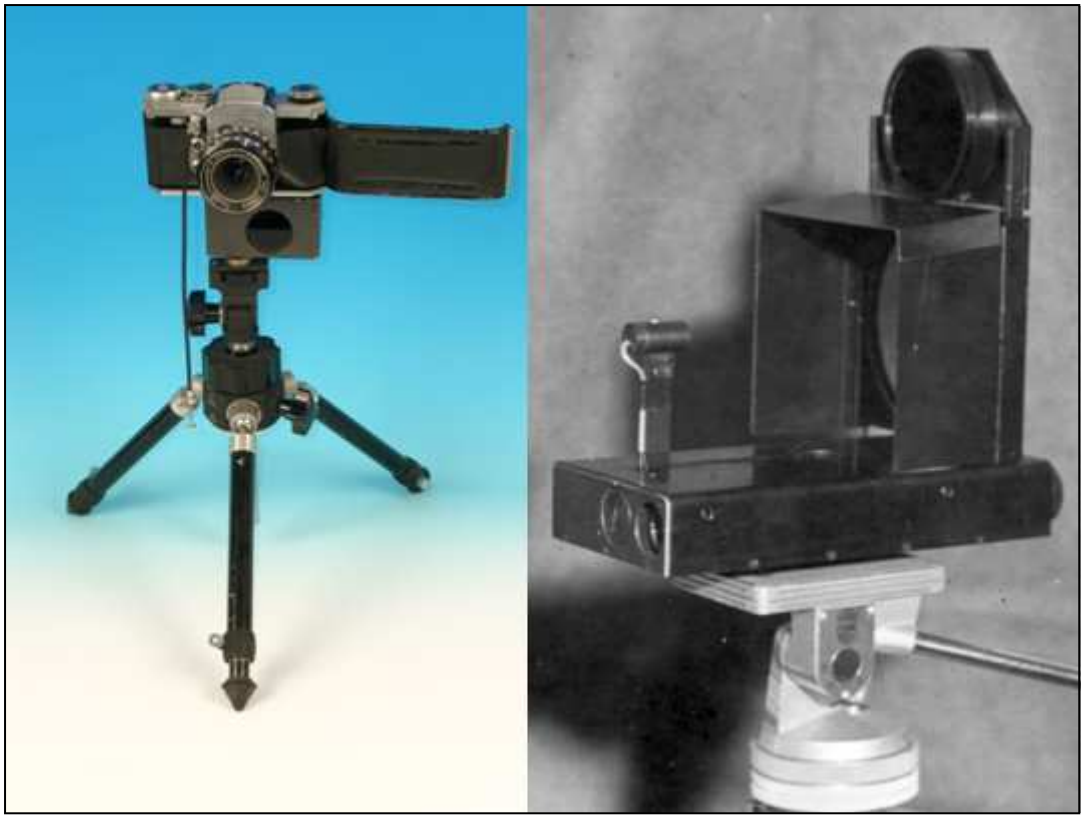
Oktober 2011 wurde ein Ehepaar namens “Anschlag” in Gießen verhaftet. Sie waren SVR Agenten und bekamen ihre Anweisungen über einen KW-Tonsender (XPA) und antworteten mit einem Satellitensender, der in einer Laptoptasche versteckt war.

Quelle: Der Spiegel



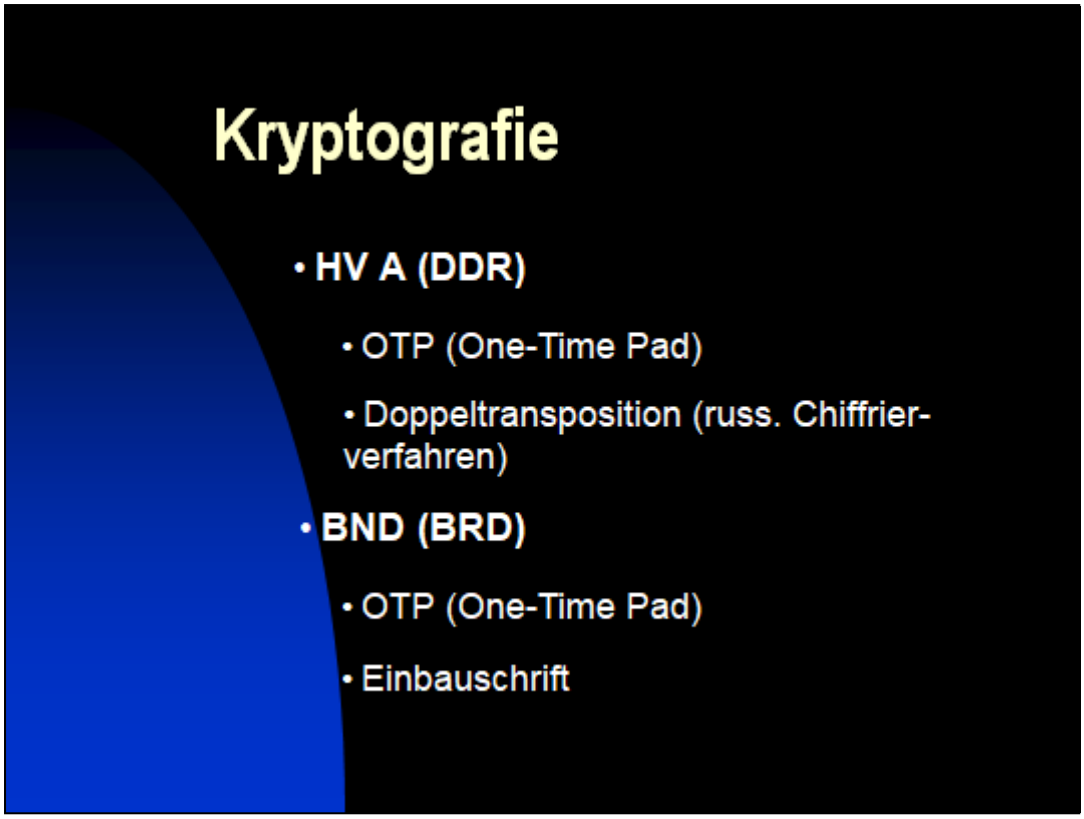
IR-Kommunikation ist eine ziemlich sichere Form der Kommunikation. IR ist Licht im Spektrum unterhalb des sichtbaren Bereichs.

Dieses amerikanische Lichtsprechgerät (Communication Set XE-2) wurde 1959 bei einer amerikanischen Agentin namens Gisela Gebhardt in Ost-Berlin gefunden.

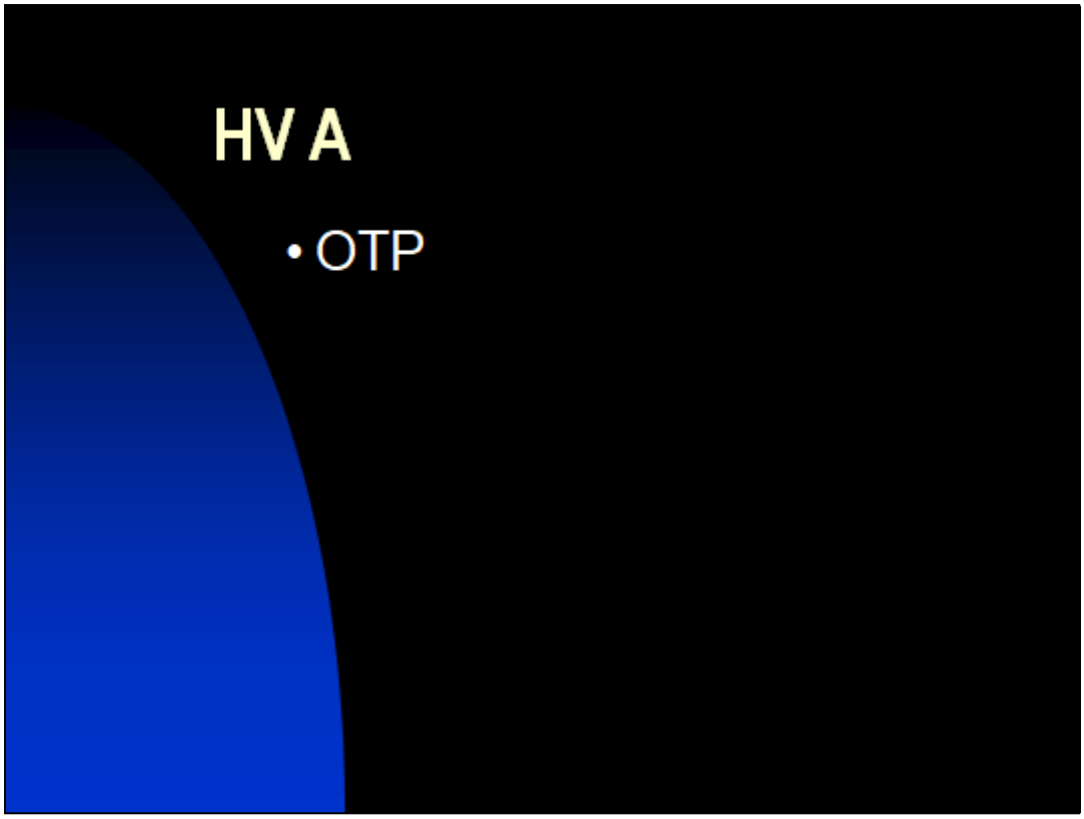


Das war der Auslöser für das MfS, ebenfalls IR-Lichtsprechgeräte zu entwickeln. Das erste MfS Gerät wurde 1963 in West-berlin gefunden. Der IR-Sender (modulierte Glühlampe) ist unter der Kamera, der Empfänger in der Kamera. Die Gegenstelle in der DDR war eine Dahme, ein Nachbau des amerikanischen Gerätes.

Das ist ein Überblick über die IR Geräte des MfS, vorn rechts das Gerät Finow, mit dem Telefongespräche über die Grenze möglich waren (ALD 3K)



Und nun der zweite Teil: Kryptografie



Die HV A (Hauptverwaltung Aufklärung) war der Auslandsspionagedienst der DDR und verwendete ab 1958 das OTP Verfahren. Das ältere Verfahren Granit erläutere ich im Anschluss.

Das OTP Verfahren ist sicher, wenn es richtig angewendet wird: One Time Pad nur einmal!

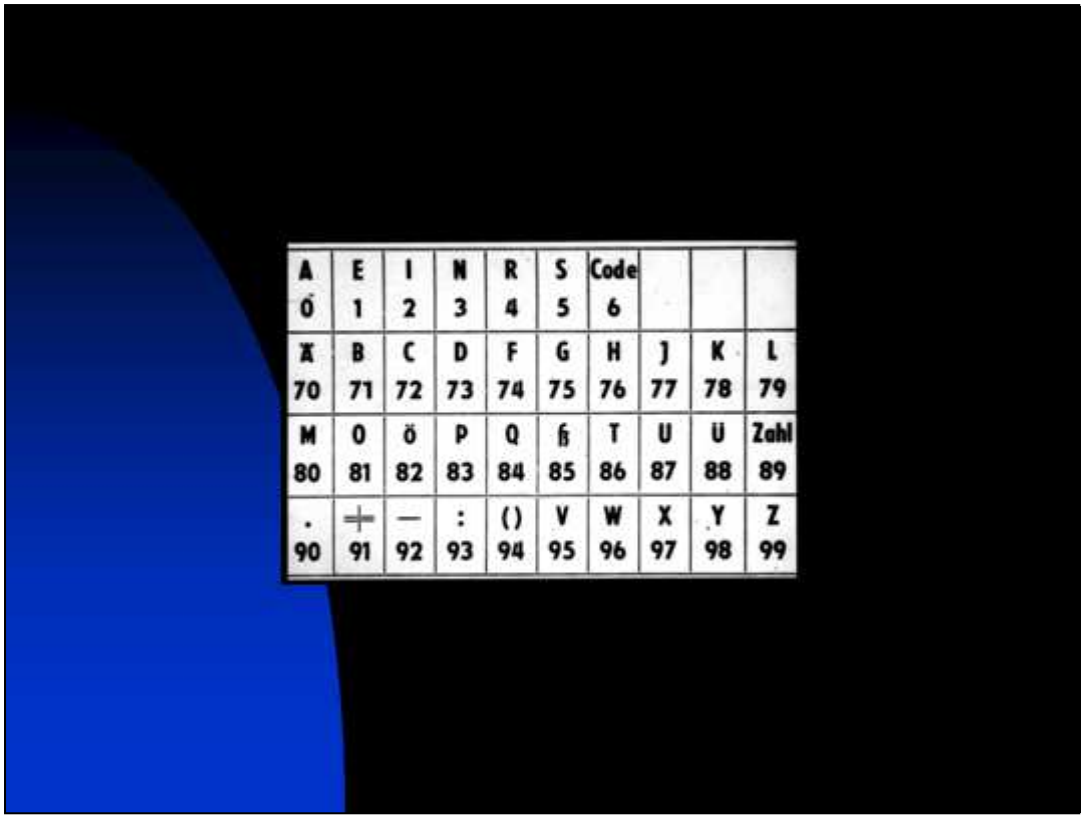
Empfangen	Achtung	71719	Trennung 09	Beginn der Sendung 9 min nach voller Stunde
dann	Achtung	71719	Trennung 06	Anzahl der Gruppen: 6

Empfangen	72927	67319	05875
- Schlüssel	68067	29703	56297
Ergebnis	14960	48616	59688
	ERWA	RTECode	NACHRICHT Ü

Empfangen	69829	99288	33334	Ende
- Schlüssel	98783	23505	25720	
Ergebnis	71146	76783	18614	
	BERCode	TBKP	ETER	

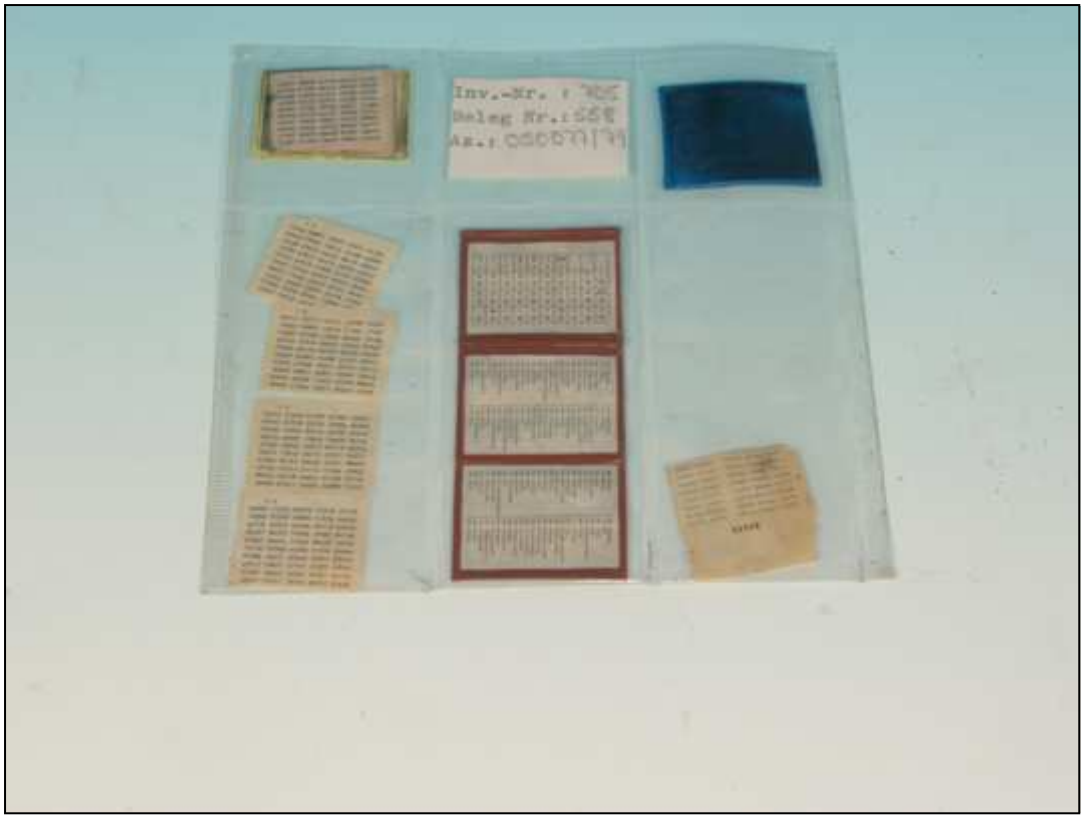
Gelb ist die vom Agenten empfangene Nachricht, darunter schreibt er die Zufallszahlen vom OTP und subtrahiert sie ohne Zehnerübertrag.

Das Ergebnis wird mit der Substitutionstabelle auf dem nächsten Bild in Text umgesetzt



A Ö	E 1	I 2	N 3	R 4	S 5	Code 6			
Ä 70	B 71	C 72	D 73	F 74	G 75	H 76	J 77	K 78	L 79
M 80	O 81	Ö 82	P 83	Q 84	ß 85	T 86	U 87	Ü 88	Zahl 89
. 90	+ 91	— 92	: 93	() 94	V 95	W 96	X 97	Y 98	Z 99

Die Substitutionstabelle, mit der Buchstaben durch Zahlen und umgekehrt ersetzt (substituiert) werden. Die am häufigsten verwendeten Buchstaben werden durch nur eine Ziffer dargestellt, um die Nachricht so kurz wie möglich zu halten.



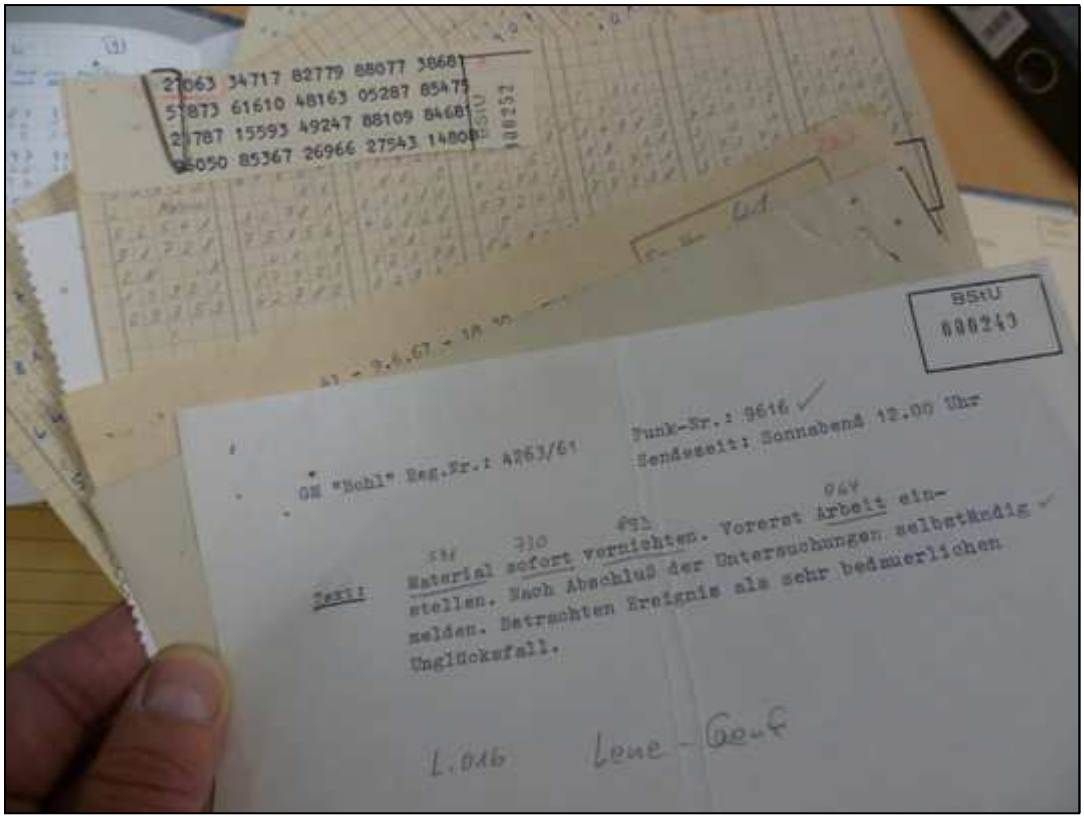
Diese Unterlagen hatte der Agent zum ver- und entschlüsseln.

Links die Entschlüsselungs-OTP, rechts die Verschlüsselungs-OTP mit Lücke zwischen der 2. und 3. Spalte.

In der Mitte die Substitutionstabelle und das Codeverzeichnis Titan/Z (GVS 4086/63)

In der Chiffrierstelle gab es eine ähnliches OTP, ein versiegeltes OTP für jeden Agenten

Es enthält die gleichen Zufallszahlen wie der Agent.



In den 60er Jahren wurden die Nachrichten in der Chiffrierstelle von Hand verschlüsselt.

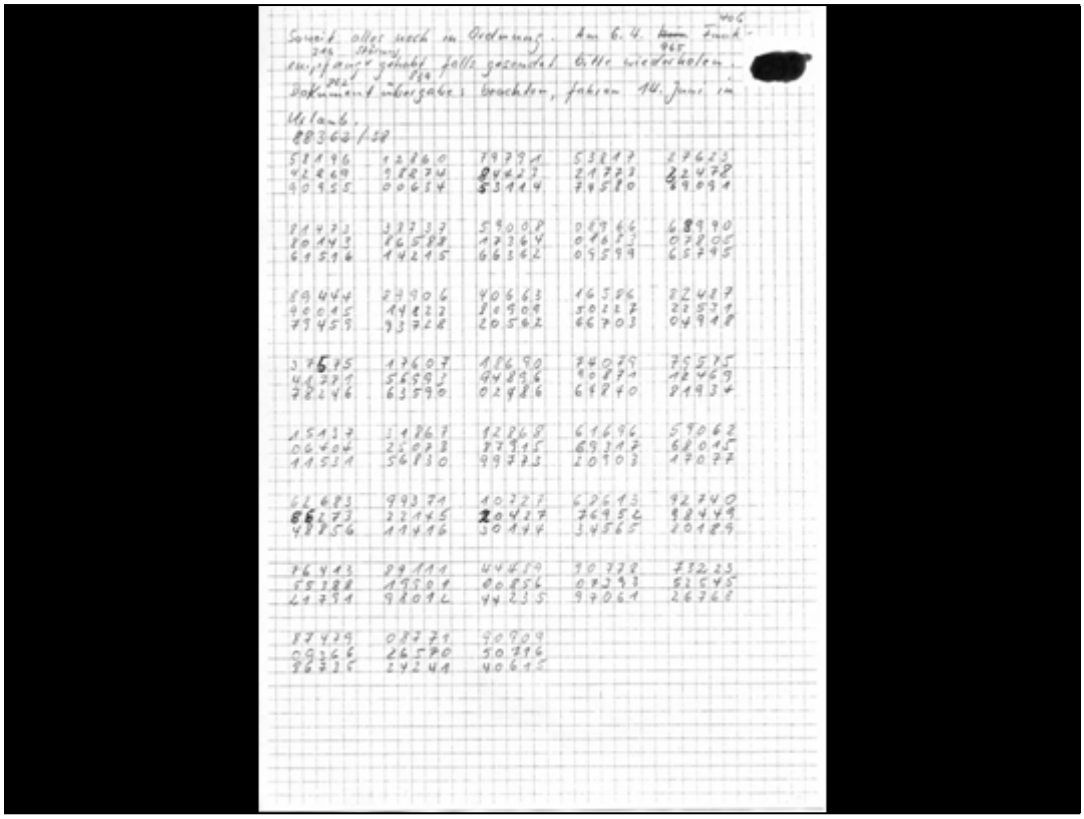
GM „Bohl“ ist Karl-Heinz Kurras, der westberliner Polizist, der am 2. Juni 1967 Benno Ohnesorg erschossen hat. Erst 2009 wurde entdeckt, dass er für das MfS gearbeitet hatte.

Seltsam, dass diese Nachrichten erhalten geblieben sind, normalerweise wurden Nachrichten vernichtet. Wollte das MfS eine falsche Fährte legen?

Copyright: BStU/Holger Kulick Akte BStU, MfS GH 2/70 GM "Otto Bohl

Später wurde elektronisch verschlüsselt.

Das Bild zeigt ein Gerät T-307/3



Hier kann man sehen, wie ein Agent seine Nachricht verschlüsselt hat:
Oben sein Klartext und dann Schritt für Schritt die Verschlüsselung.
Es gibt einen absichtlichen Fehler oben in der 5. Spalte, der Agent ist nicht entdeckt worden, sonst hätte er keinen Fehler gemacht.

Doppeltransposition

(russ. Chiffrierverfahren)

- Name: GRANIT E 160
- Beschreibung in http://scz.bplaced.net/index.html
- Wurde von der HV A bis 1958 verwendet
- Wurde vom „Verfassungsschutz“ geknackt
- Führte zur Enttarnung von Guillaume, einem Spitzenagenten und persönlichen Referenten des Bundeskanzlers Willy Brandt

		0	1	2	3	4	5	6	7	8	9
		R	H	E	I	N	A	S	T		
8		B	C	D	F	G	K	L	M	O	P
9		Q	U	V	W	X	Y	Z	zs	.	,

Das Verfahren benutzte eine Substitutionstabelle, die mit einem Schlüsselwort erzeugt worden ist. Zs bedeutet Zahl folgt. Zwei Sätze, die einem vereinbarten Buch entnommen worden sind, wurden zur Transponierung verwendet, Seitenzahl und Zeile wurden am Ende des Spruchs übertragen.

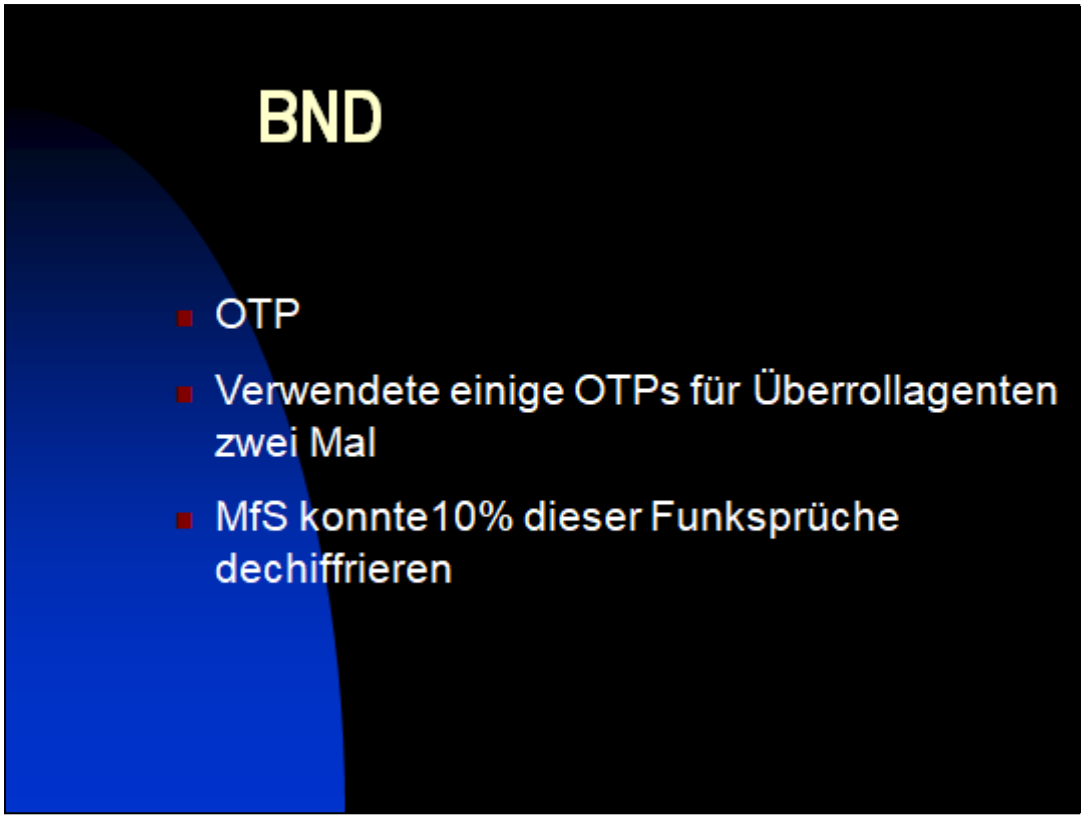
R	O	U	N	D	T	A	B	L	E
8	7	10	6	3	9	1	2	5	4
W	I	R	M	E	L	D	E	N	U
N	S	N	A	C	H	F	U	E	N
F	U	N	D	Z	W	A	N	Z	I
G	J	A	E	H	R	I	G	E	M
E	I	N	S	A	T	Z	Z	U	R
U	E	C	K	A	B	C	D	E	F

A	B	D	E	L	N	O	R	T	U
1	2	3	4	5	6	7	8	9	10
D	E	E	U	N	M	I	W	L	R
F	U	C	N	E	A	S	N	H	N
A	N	Z	I	Z	D	U	F	W	N
I	G	H	M	E	E	J	G	R	A
Z	Z	A	R	U	S	I	E	T	N
C	D	A	F	E	K	E	U	B	C

WIR MELDEN UNS NACH FUENFUNDZWANZIGJAEHRIGEM
EINSATZ ZURUECK ABCDEF
DEEUNMIWLRFUCNEASNHNANZIZDUFWNIGHMEEJGRAZZ
ARUSIETNCDAFEKEUBC

Beispiel für eine Transposition (Verwürfeln) mit Buchstaben.
Schlüsselwort Roundtable, Blender zum Auffüllen ABCDEF

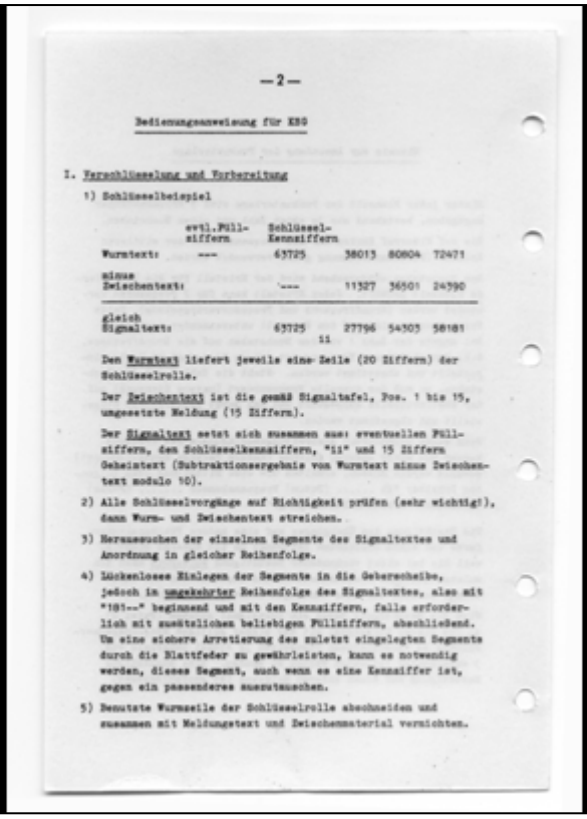
Der Kanzlerspion Guillaume bekam vor 1958 Geburtstagsgrüße und Gratulation zur Geburt eines Sohnes, die Jahre später entschlüsselt werden konnten und dann zur Enttarnung Guillaumes führten



Der BND verwendete ebenfalss das OTP-Verfahren

	0	1	2	3	4	5	6	7	8	9
	D	E	I	N			S	T	A	R
4	B	C	F	G	H	J	K	L	M	O
5	P	Q	U	V	W	X	Y	Z	.	,

Die Substitutionstabelle des BND, mit der Buchstaben durch Zahlen und umgekehrt ersetzt (substituiert) werden.



—2—

Bedienungsanweisung für KBG

I. Verschlüsselung und Vorbereitung

1) Schlüsselbeispiel

	evtl.Füll-ziffern	Schlüssel-Kennziffern			
Wurmtext:	---	65725	38013	80804	72471
minus Zwischentext:	---		11327	36501	24390
gleich Signaltext:		65725	27796	54303	58181
		11			

Den Wurmtext liefert jeweils eine Zeile (20 Ziffern) der Schlüsselrolle.

Der Zwischentext ist die gemäß Signaltafel, Pos. 1 bis 15, umgesetzte Meldung (15 Ziffern).

Der Signaltext setzt sich zusammen aus: eventuellen Füllziffern, den Schlüsselkennziffern, "11" und 15 Ziffern Geheimtext (Subtraktionsergebnis von Wurmtext minus Zwischentext modulo 10).

2) Alle Schlüsselvorgänge auf Richtigkeit prüfen (sehr wichtig!), dann Wurm- und Zwischentext streichen.

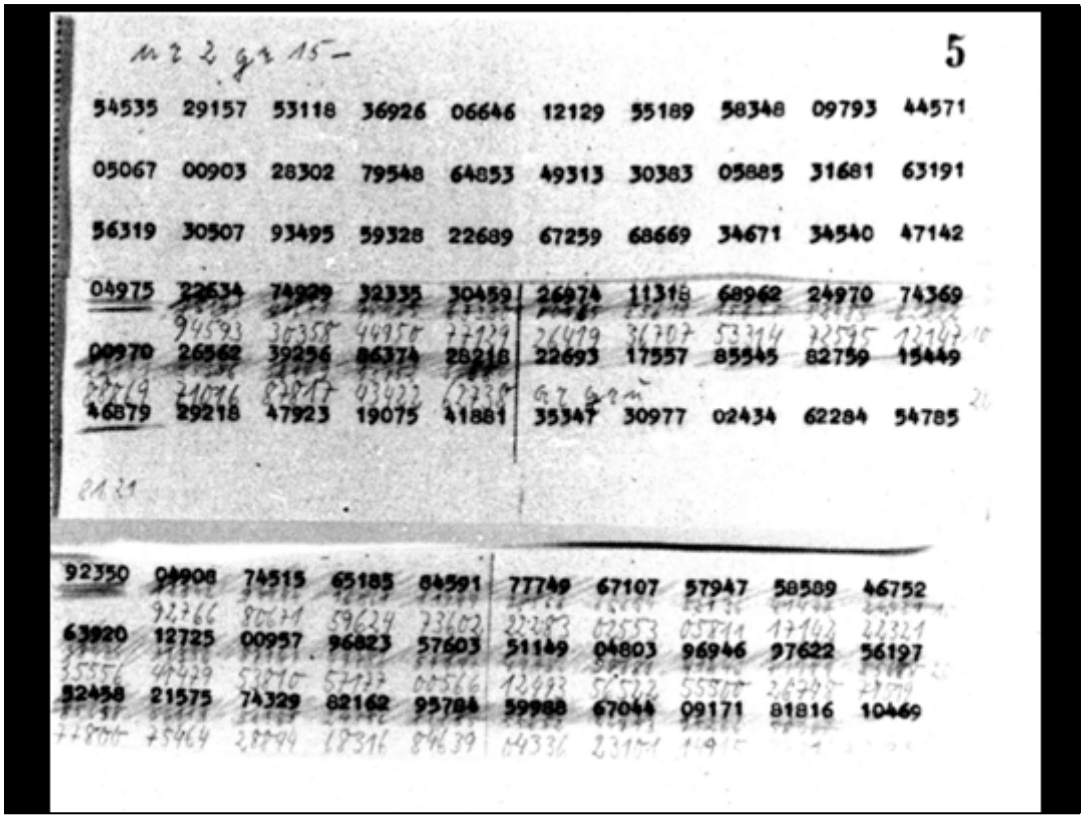
3) Herausuchen der einzelnen Segmente des Signaltextes und Anordnung in gleicher Reihenfolge.

4) Lückenloses Einlegen der Segmente in die Geberscheibe, jedoch in umgekehrter Reihenfolge des Signaltextes, also mit "181--" beginnend und mit den Kennziffern, falls erforderlich mit zusätzlichen beliebigen Füllziffern, abschließend. Um eine sichere Arretierung des zuletzt eingelegten Segments durch die Blattfeder zu gewährleisten, kann es notwendig werden, dieses Segment, auch wenn es eine Kennziffer ist, gegen ein passenderes auszutauschen.

5) Benutzte Wurmzeile der Schlüsselrolle abschneiden und zusammen mit Meldungstext und Zwischenmaterial vernichten.

Diese BND Anweisungen erläutern die Verschlüsselung, der Agent subtrahierte seinen in Zahlen umgesetzten Text vom OTP.

Zwischen HV A und BND Verschlüsselung gibt es einen kleinen Unterschied, bei der HV A wurde das OTP zum in Zahlen umgesetzten Text addiert und später subtrahiert, beim BND wurde zweimal vom OTP subtrahiert.



5

54535 29157 53118 36926 06646 12129 55189 58348 09793 44571

05067 00903 28302 79548 64853 49313 30383 05885 31681 63191

56319 30507 93495 59328 22689 67259 68669 34671 34540 47142

04975 22634 74929 32335 30459 26974 11318 68962 24970 74369

00970 26562 39256 86374 28218 22693 17557 85545 82759 15449

46879 29218 47923 19075 41881 35347 30977 02434 62284 54785

92350 04908 74515 65185 84591 77749 67107 57947 58589 46752

63920 12725 00957 96823 57603 51149 04803 96946 97622 56197

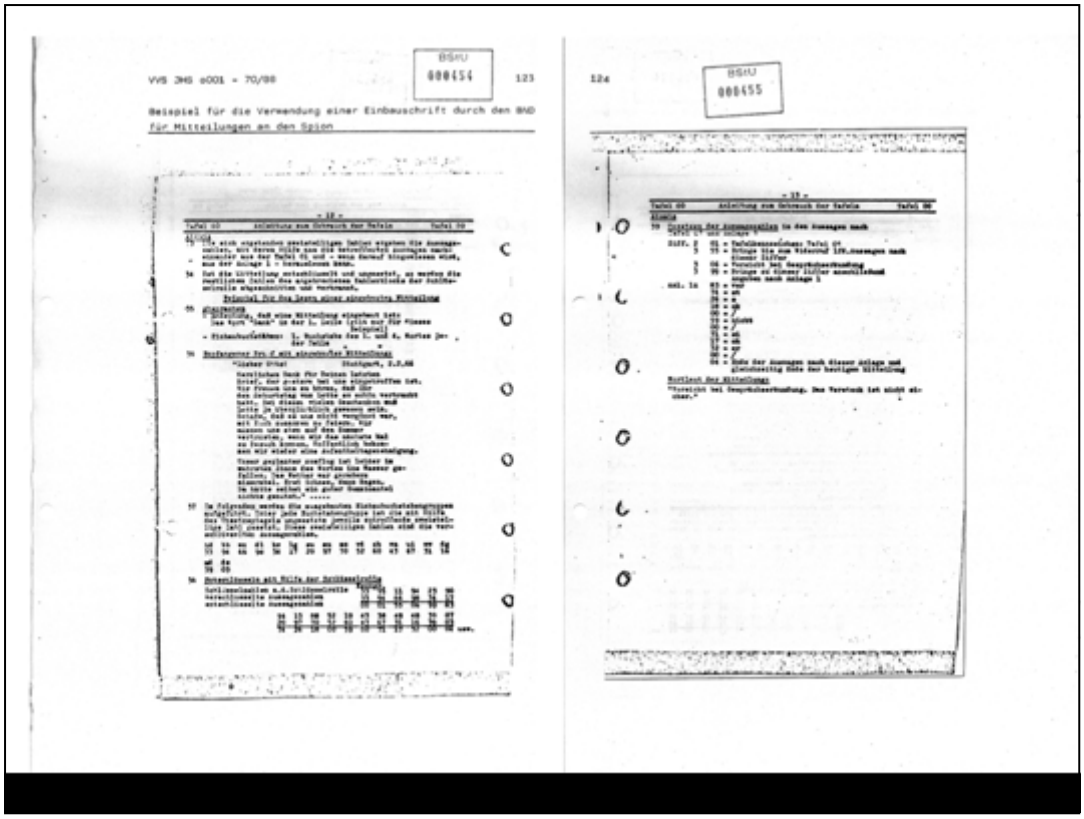
32458 21575 74329 82162 95784 59988 67044 09171 81816 10469

Hier hat der Agent zwei Funksprüche entschlüsselt. Der erste lautet: Naechster am 30.1. um 22 15 Uhr Gruss.

Zweiter Spruch: Ein frohes 1956 wuenscht ihnen allen ZELOT. Naechster am 8. 1. um 15 Uhr Gruss

Einbauschrift

BND benutzte sie in den 60er Jahren

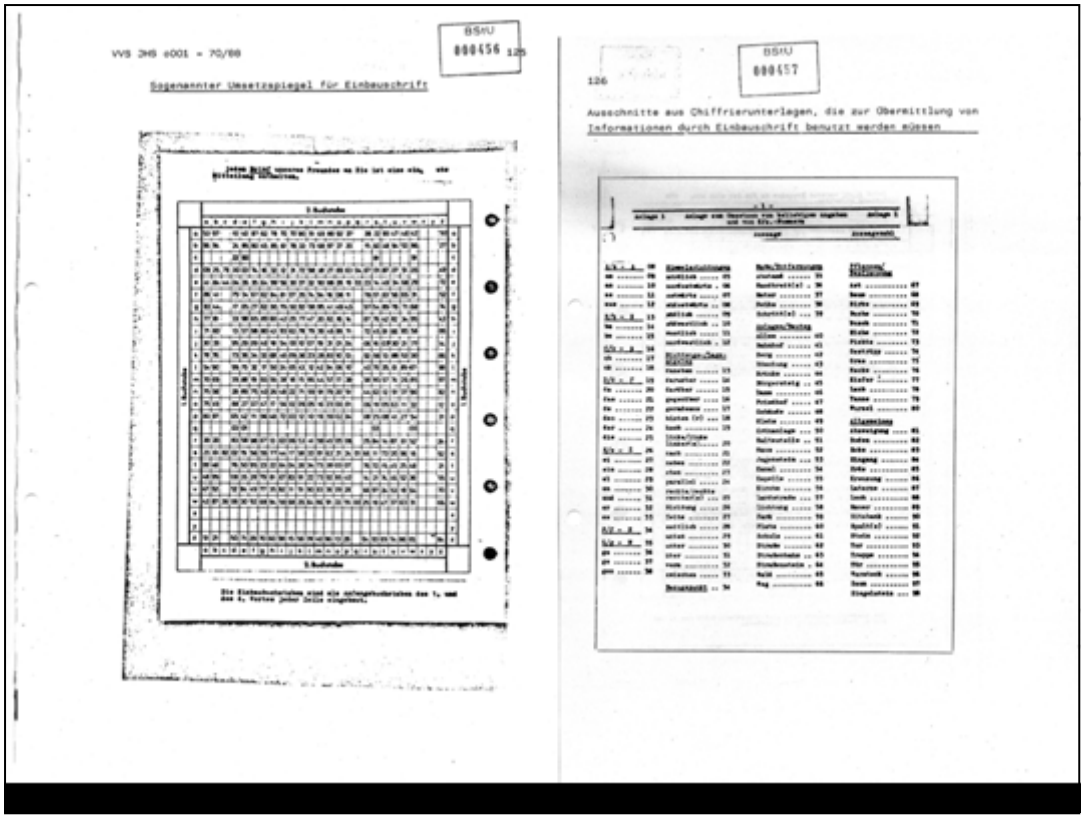


VVS 3HG 0001 - 70/80 BSrU 000454 123

Beispiel für die Verwendung einer Einbauschrift durch den BND für Mitteilungen an den Spion

124 BSrU 000455

"Einbauschrift" ist ein weitgehend unbekanntes Verfahren für verschlüsselte Kommunikation. In einem Text werden der erste Buchstaben des ersten und vierten Wortes mit Hilfe einer Tabelle in eine zweistellige Zahl umgewandelt. Diese Zahlen wurden vom OTP subtrahiert. Eine weitere Tabelle ordnete dem Ergebnis Begriffe zu.



Links die Tabelle, mit der die Anfangsbuchstaben in eine zweistellige Zahl umgewandelt werden, rechts die Tabelle, mit der Zahlen in Begriffe umgesetzt werden.

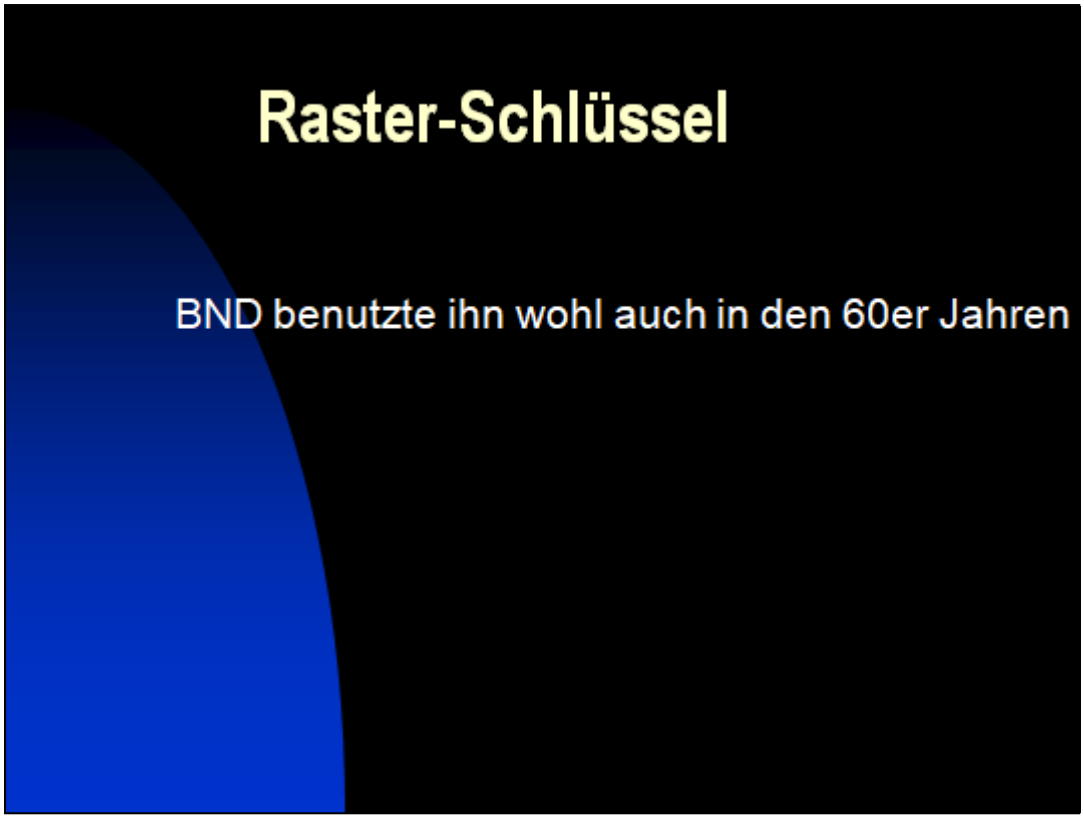
Leonard Nimoy, the sonorous, gaunt-faced actor who won a worshipful global following as Mr. Spock, the resolutely logical human-alien first officer of the Starship Enterprise in the television and movie juggernaut "Star Trek," died on Friday morning at his home in the Bel Air section of Los Angeles. He was 83.

His wife, Susan Bay Nimoy, confirmed his death, saying the cause was endstage chronic obstructive pulmonary disease.

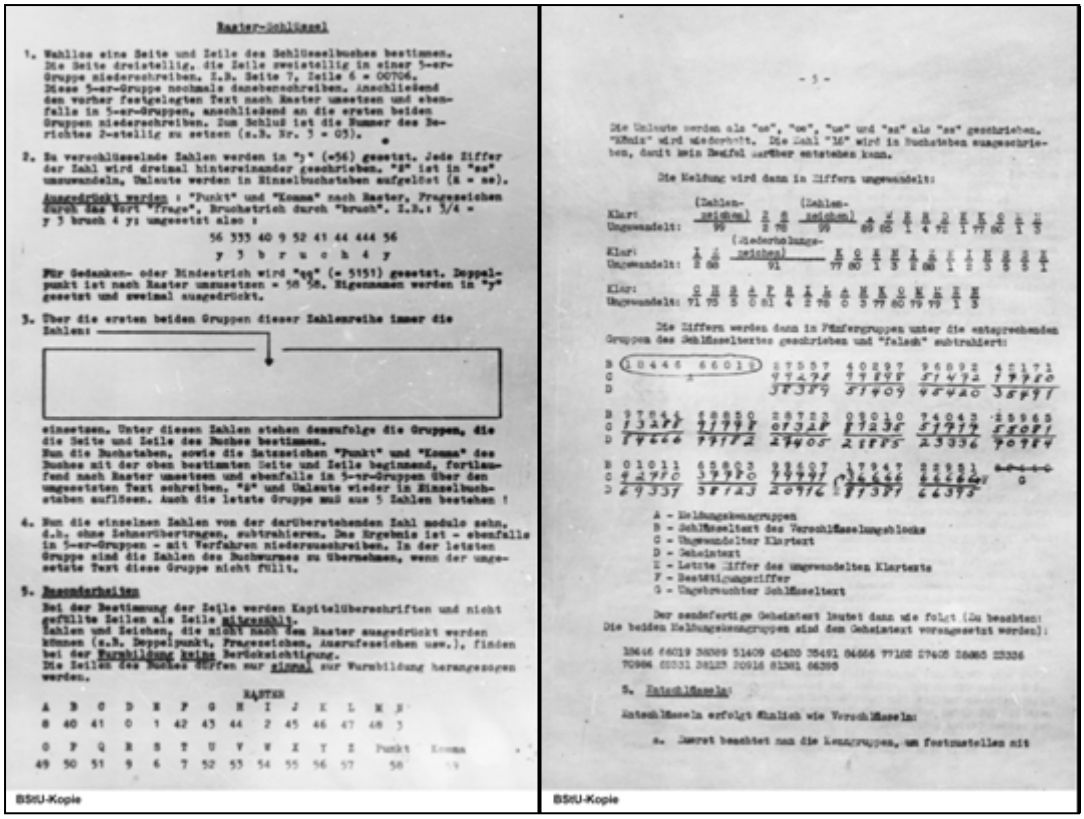
Mr. Nimoy announced that he had the disease. last year, attributing it to years of smoking, a habit he had given up three decades earlier. He had been hospitalized earlier in the week.

ls = 76 = Hecke (hedge)
fw = 31 = über (over)
fs = 57 = Landstraße (country road)
lf = 32 = vorn (ahead)
st = 73 = Fichte (...)
mt = 57 = ...
fh = 84 ...
sa = ...

Ein vereinfachtes Beispiel ohne Nutzung eines OTP.



Bilder aus D:\Eigene Dateien\MfS\Tgb.Nr.108461-13Z-2017b



Raster-Schlüssel

1. Wahllos eine Seite und Zeile des Schlüsselbuches bestimmen. Die Seite dreistellig, die Zeile zweistellig in einer 5-er-Gruppe niederschreiben. Z.B. Seite 7, Zeile 6 = 00706. Diese 5-er-Gruppe nochmals daneberschreiben. Anschließend den vorher festgelegten Text nach Raster umsetzen und ebenfalls in 5-er-Gruppen, anschließend an die ersten beiden Gruppen niederschreiben. Zum Schluß ist die Nummer des Berichtes 2-stellig zu setzen (z.B. Nr. 3 = 03).

2. Zu verschlüsselnde Zahlen werden in "y" (=56) gesetzt. Jede Ziffer der Zahl wird dreimal hintereinander geschrieben. "S" ist in "ss" umzuwandeln, Umlaute werden in Einzelbuchstaben aufgelöst (Ä = ae).
Ausgedrückt werden : "Punkt" und "Komma" nach Raster, Fragezeichen durch das Wort "Frage", Bruchstrich durch "bruch". Z.B.: 3/4 = y 3 bruch 4 y; umgesetzt also :
56 333 40 9 52 41 44 444 56
y 3 b r u c h 4 y
Für Gedanken- oder Bindestrich wird "qq" (= 5151) gesetzt. Doppelpunkt ist nach Raster umzusetzen = 58 58. Eigennamen werden in "y" gesetzt und zweimal ausgedrückt.

3. Über die ersten beiden Gruppen dieser Zahlenreihe immer die Zahlen:

einsetzen. Unter diesen Zahlen stehen demzufolge die Gruppen, die die Seite und Zeile des Buches bestimmen.
Nun die Buchstaben, sowie die Satzzeichen "Punkt" und "Komma" des Buches mit der oben bestimmten Seite und Zeile beginnend, fortlaufend nach Raster umsetzen und ebenfalls in 5-er-Gruppen über den umgesetzten Text schreiben. "S" und Umlaute wieder in Einzelbuchstaben auflösen. Auch die letzte Gruppe muß aus 5 Zahlen bestehen !

4. Nun die einzelnen Zahlen von der darüberstehenden Zahl modulo zehn, d.h. ohne Zehnerübertragen, subtrahieren. Das Ergebnis ist - ebenfalls in 5-er-Gruppen - mit Verfahren niederzuschreiben. In der letzten Gruppe sind die Zahlen des Buchwurmes zu übernehmen, wenn der umgesetzte Text diese Gruppe nicht füllt.

5. Besonderheiten
Bei der Bestimmung der Zeile werden Kapitelüberschriften und nicht gefüllte Zeilen als Zeile mitgezählt.
Zahlen und Zeichen, die nicht nach dem Raster ausgedrückt werden können (z.B. Doppelpunkt, Fragezeichen, Ausrufezeichen usw.), finden bei der Vorbildung keine Berücksichtigung.
Die Zeilen des Buches dürfen nur einmal zur Vorbildung herangezogen werden.

RASTER

A	B	C	D	E	F	G	H	I	J	K	L	M	N
8	40	41	0	1	42	43	44	2	45	46	47	48	3
O	P	Q	R	S	T	U	V	W	X	Y	Z	Punkt	Komma
49	50	51	9	6	7	52	53	54	55	56	57	58	[illegible]

BStU-Kopie

- 5 -

Die Umlaute werden als "ae", "oe", "ue" und "ss" als "ss" geschrieben. "Ähnlich" wird wiederholt. Die Zahl "16" wird in Buchstaben ausgeschrieben, damit kein Deafal [illegible] entstehen kann.

Die Meldung wird dann in Ziffern umgewandelt:

Klar: (Zahlen-zeichen) 2 8 (Zahlen-zeichen) A J E B J E K S L L
Umgewandelt: 99 2 70 99 69 00 1 4 70 1 77 00 1 3

Klar: 1 4 (Wiederholungs-zeichen) K O E N 1 2 1 1 N E S S
Umgewandelt: 2 00 91 77 00 1 3 2 00 1 2 3 5 5 1

Klar: G H S A F R 1 5 A K K O K K 2 N
Umgewandelt: 71 75 5 0 81 4 2 78 0 3 77 60 79 79 1 3

Die Ziffern werden dann in Fünfergruppen unter die entsprechenden Gruppen des Schlüsseltextes geschrieben und "falsch" subtrahiert:

B 10446 66012 27557 40297 96092 42171
C 97478 97898 51472 17950
D 38389 51909 48440 35491

B 97546 69850 28723 09010 74043 25965
C 13278 97798 07328 87235 51717 58091
D 79666 97172 27405 28775 23336 70784

B 01011 65863 93607 17947 22951 ~~[illegible]~~
C 42770 37770 79797 16646 ~~[illegible]~~ 0
D 69337 38123 20976 87397 66393

A - Meldungsbeginngruppen
B - Schlüsseltext des Verschlüsselungsblocks
C - Umgewandelter Klartext
D - Gehalntext
E - Letzte Ziffer des umgewandelten Klartextes
F - Bestätigungsziffer
G - Umgebrauchter Schlüsseltext

Der sendefertige Gehalntext lautet dann wie folgt (Zu beachten: Die beiden Meldungsbeginngruppen sind dem Gehalntext vorangesetzt worden):

33646 66019 38309 51409 45420 35491 84666 77102 27405 28865 23336
70984 00331 38123 20916 81381 66393

5. Entschlüsseln:

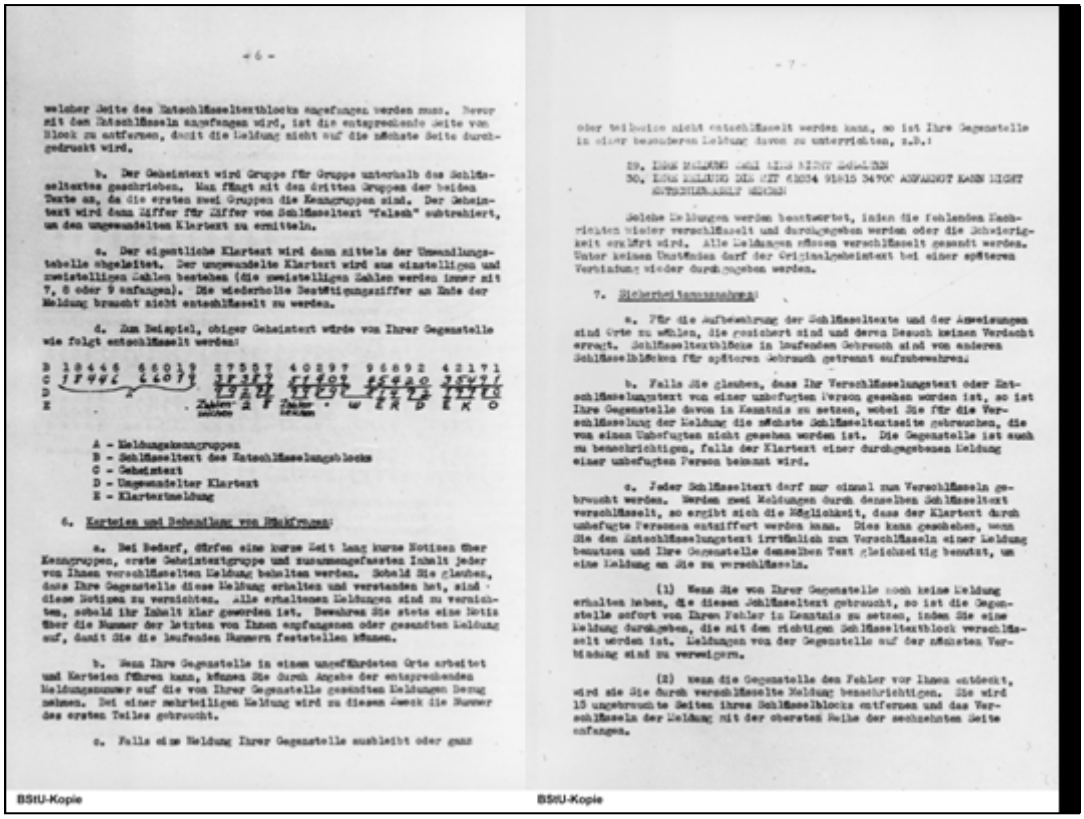
Entschlüsseln erfolgt ähnlich wie Verschlüsseln:

a. Zuerst beachtet man die Kennzeichen, um festzustellen mit

BStU-Kopie

Der "Rasterschlüssel" ist ebenfalls ein weitgehend unbekanntes Verfahren für verschlüsselte Kommunikation. Er verwendet ein Schlüsselbuch.

Leider fehlen einige Seiten der Anleitung



welcher Seite des Entschlüsselungsblocks angefangen werden muss. Bevor mit dem Entschlüsseln angefangen wird, ist die entsprechende Seite vom Block zu entfernen, damit die Meldung nicht auf die nächste Seite durchgedruckt wird.

b. Der Geheimtext wird Gruppe für Gruppe unterhalb des Schlüsseltextes geschrieben. Man fängt mit den dritten Gruppen der beiden Texte an, da die ersten zwei Gruppen die Kenngruppen sind. Der Geheimtext wird dann Ziffer für Ziffer von Schlüsseltext "Falsch" subtrahiert, um den umgewandelten Klartext zu ermitteln.

c. Der eigentliche Klartext wird dann mittels der Umwandlungstabelle abgeleitet. Der umgewandelte Klartext wird aus einstelligen und zweistelligen Zahlen bestehen (die zweistelligen Zahlen werden immer mit 7, 8 oder 9 anfangen). Die wiederholte Bestätigungsziffer am Ende der Meldung braucht nicht entschlüsselt zu werden.

d. Zum Beispiel, obiger Geheimtext würde von Ihrer Gegenstelle wie folgt entschlüsselt werden:

B 18446 66019 27557 40297 96892 42171
C 37996 66079 [illegible]
D [illegible]
E . Zahlen 2 F Zahlen . W E R D E K O

A - Meldungskenngruppen
B - Schlüsseltext des Entschlüsselungsblocks
C - Geheimtext
D - Umgewandelter Klartext
E - Klartextmeldung

6. Karteien und Behandlung von Mitschriften:

a. Bei Bedarf, dürfen eine kurze Zeit lang kurze Notizen über Kenngruppen, erste Geheimtextgruppe und zusammengefassten Inhalt jeder von Ihnen verschlüsselten Meldung behalten werden. Sobald Sie glauben, dass Ihre Gegenstelle diese Meldung erhalten und verstanden hat, sind diese Notizen zu vernichten. Alle erhaltenen Meldungen sind zu vernichten, sobald ihr Inhalt klar geworden ist. Bewahren Sie stets eine Notiz über die Nummer der letzten von Ihnen empfangenen oder gesandten Meldung auf, damit Sie die laufenden Nummern feststellen können.

b. Wenn Ihre Gegenstelle in einem ungefährdeten Orte arbeitet und Karteien führen kann, können Sie durch Angabe der entsprechenden Meldungsnummer auf die von Ihrer Gegenstelle gesandten Meldungen Bezug nehmen. Bei einer mehrteiligen Meldung wird zu diesem Zweck die Nummer des ersten Teiles gebraucht.

c. Falls eine Meldung Ihrer Gegenstelle ausbleibt oder ganz

BStU-Kopie

oder teilweise nicht entschlüsselt werden kann, so ist Ihre Gegenstelle in einer besonderen Meldung davon zu unterrichten, z.B.:

29. EINE MELDUNG [illegible] NICHT ENTSCHLÜSSELN
30. EINE MELDUNG DIE ZIF 61034 91815 34700 ANFANGT KANN NICHT ENTSCHLÜSSELT WERDEN

Solche Meldungen werden beantwortet, indem die fehlenden Nachrichten wieder verschlüsselt und durchgegeben werden oder die Schwierigkeit erklärt wird. Alle Meldungen müssen verschlüsselt gesandt werden. Unter keinen Umständen darf der Originalgeheimtext bei einer späteren Verhandlung wieder durchgegeben werden.

7. Sicherheitsmassnahmen:

a. Für die Aufbewahrung der Schlüsseltexte und der Anweisungen sind Orte zu wählen, die gesichert sind und deren Besuch keinen Verdacht erregt. Schlüsseltextblöcke in laufendem Gebrauch sind von anderen Schlüsselblöcken für späteren Gebrauch getrennt aufzubewahren.

b. Falls Sie glauben, dass Ihr Verschlüsselungstext oder Entschlüsselungstext von einer unbefugten Person gesehen worden ist, so ist Ihre Gegenstelle davon in Kenntnis zu setzen, wobei Sie für die Verschlüsselung der Meldung die nächste Schlüsseltextseite gebrauchen, die von einen Unbefugten nicht gesehen worden ist. Die Gegenstelle ist auch zu benachrichtigen, falls der Klartext einer durchgegebenen Meldung einer unbefugten Person bekannt wird.

c. Jeder Schlüsseltext darf nur einmal zum Verschlüsseln gebraucht werden. Werden zwei Meldungen durch denselben Schlüsseltext verschlüsselt, so ergibt sich die Möglichkeit, dass der Klartext durch unbefugte Personen entziffert werden kann. Dies kann geschehen, wenn Sie den Entschlüsselungstext irrtümlich zum Verschlüsseln einer Meldung benutzen und Ihre Gegenstelle denselben Text gleichzeitig benutzt, um eine Meldung an Sie zu verschlüsseln.

(1) Wenn Sie von Ihrer Gegenstelle noch keine Meldung erhalten haben, die diesen Schlüsseltext gebraucht, so ist die Gegenstelle sofort von Ihren Fehler in Kenntnis zu setzen, indem Sie eine Meldung durchgeben, die mit dem richtigen Schlüsseltextblock verschlüsselt worden ist. Meldungen von der Gegenstelle auf der nächsten Verbindung sind zu verweigern.

(2) Wenn die Gegenstelle den Fehler vor Ihnen entdeckt, wird sie Sie durch verschlüsselte Meldung benachrichtigen. Sie wird 15 ungebrauchte Seiten ihres Schlüsselblocks entfernen und das Verschlüsseln der Meldung mit der obersten Reihe der sechzehnten Seite anfangen.

BStU-Kopie

Der “Rasterschlüssel” ist ebenfalls ein weitgehend unbekanntes Verfahren für verschlüsselte Kommunikation. Er verwendet ein Schlüsselbuch.

oder teilweise nicht entschlüsselt werden kann, so ist Ihre Gegenstelle in einer besonderen Meldung davon zu unterrichten, z.B.:

29. IHRE MELDUNG VOM [illegible] KONNTE NICHT ENTSCHLÜSSELT WERDEN
30. IHRE MELDUNG DIE ZIT 63034 91815 34700 ANWAENDT KANN NICHT ENTSCHLÜSSELT WERDEN

Solche Meldungen werden beantwortet, indem die fehlenden Nachrichten wieder verschlüsselt und durchgegeben werden oder die Schwierigkeit erklärt wird. Alle Meldungen müssen verschlüsselt gesandt werden. Unter keinen Umständen darf der Originalschlüsseltext bei einer späteren Verbindung wieder durchgegeben werden.

7. Sicherheitsmassnahmen:

a. Für die Aufbewahrung der Schlüsseltexte und der Anweisungen sind Orte zu wählen, die gesichert sind und deren Besuch keinen Verdacht erregt. Schlüsseltextblöcke in laufenden Gebrauch sind von anderen Schlüsselblöcken für späteren Gebrauch getrennt aufzubewahren.

b. Falls Sie glauben, dass Ihr Verschlüsselungstext oder Entschlüsselungstext von einer unbefugten Person gesehen worden ist, so ist Ihre Gegenstelle davon in Kenntnis zu setzen, wobei Sie für die Verschlüsselung der Meldung die nächste Schlüsseltextseite gebrauchen, die von einen Unbefugten nicht gesehen worden ist. Die Gegenstelle ist auch zu benachrichtigen, falls der Klartext einer durchgegebenen Meldung einer unbefugten Person bekannt wird.

c. Jeder Schlüsseltext darf nur einmal zum Verschlüsseln gebraucht werden. Werden zwei Meldungen durch denselben Schlüsseltext verschlüsselt, so ergibt sich die Möglichkeit, dass der Klartext durch unbefugte Personen entziffert werden kann. Dies kann geschehen, wenn Sie den Entschlüsselungstext irrtümlich zum Verschlüsseln einer Meldung benutzen und Ihre Gegenstelle denselben Text gleichzeitig benutzt, um eine Meldung an Sie zu verschlüsseln.

(1) Wenn Sie von Ihrer Gegenstelle noch keine Meldung erhalten haben, die diesen Schlüsseltext gebraucht, so ist die Gegenstelle sofort von Ihren Fehler in Kenntnis zu setzen, indem Sie eine Meldung durchgeben, die mit dem richtigen Schlüsseltextblock verschlüsselt worden ist. Meldungen von der Gegenstelle auf der nächsten Verbindung sind zu verweigern.

(2) Wenn die Gegenstelle den Fehler vor Ihnen entdeckt, wird sie Sie durch verschlüsselte Meldung benachrichtigen. Sie wird 15 ungebrauchte Seiten ihres Schlüsselblocks entfernen und das Verschlüsseln der Meldung mit der obersten Reihe der sechzehnten Seite anfangen.

d. Um Schreiben einer Meldung ist eine harte, ungewachste Oberfläche zu wählen, damit der Text nicht von der Unterlage abgelesen werden kann.

e. Alle Arbeitspapiere einschliesslich erhaltene Schlüsseltexte sind sofort zu vernichten, sobald die eine Meldung verschlüsselt bzw. entschlüsselt und das Resultat überprüft haben. Alle gebrauchten Schlüsseltexte einschliesslich des ungebrauchten Textes, der auf der letzten gebrauchten Seite übrig bleibt, sind zu vernichten. Bei Meldungen, die Sie senden, ist der Schlüsseltext sofort nach Bestätigung des Funkverkehrs zu vernichten.

(1) Zum Vernichten sind die Papiere zu zerreissen und die Asche zu zerreiben.

(2) In Notfall sind Ihre Materialien in folgender Reihenfolge zu vernichten:

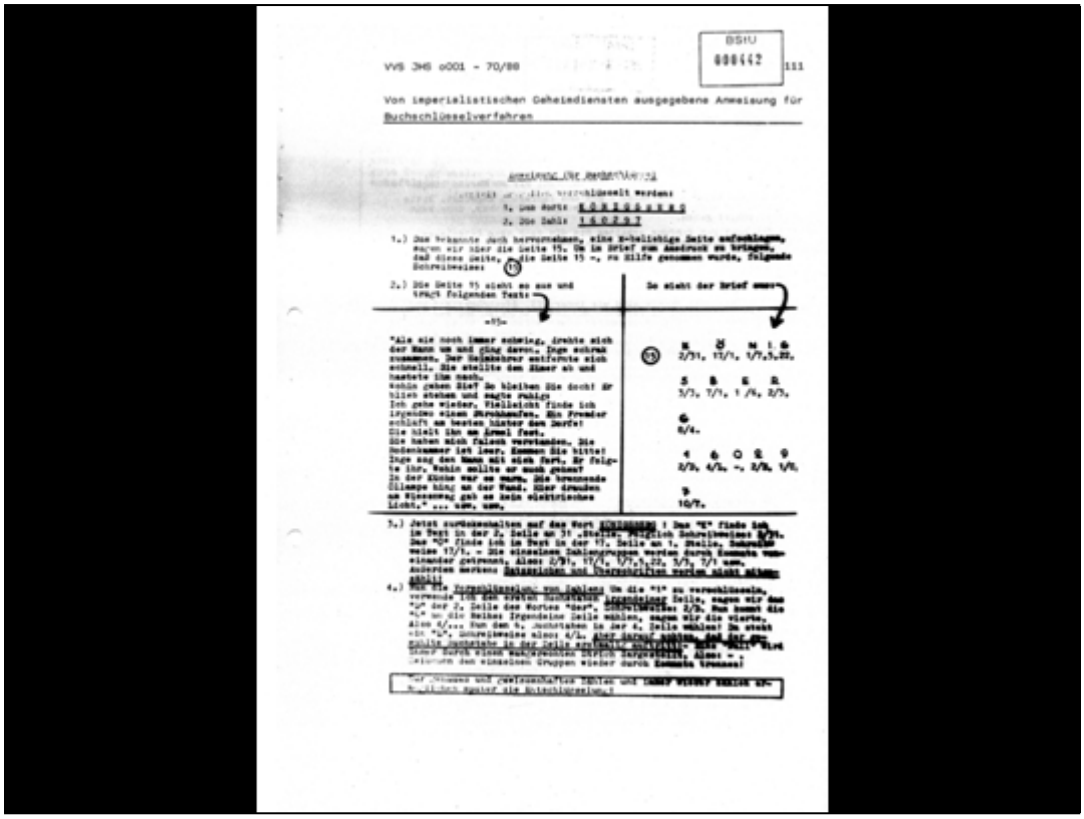
(a) Notizen über Meldungen
(b) Funkverkehrsprüfbuch und Anweisungen
(c) Verschlüsselte Meldungen
(d) Schlüsseltexte

BStU-Kopie
BStU-Kopie

Buchschlüsselverfahren

BND benutzte es wohl auch in den 60er Jahren

Bilder aus D:\Eigene Dateien\MfS\Scans/VVS



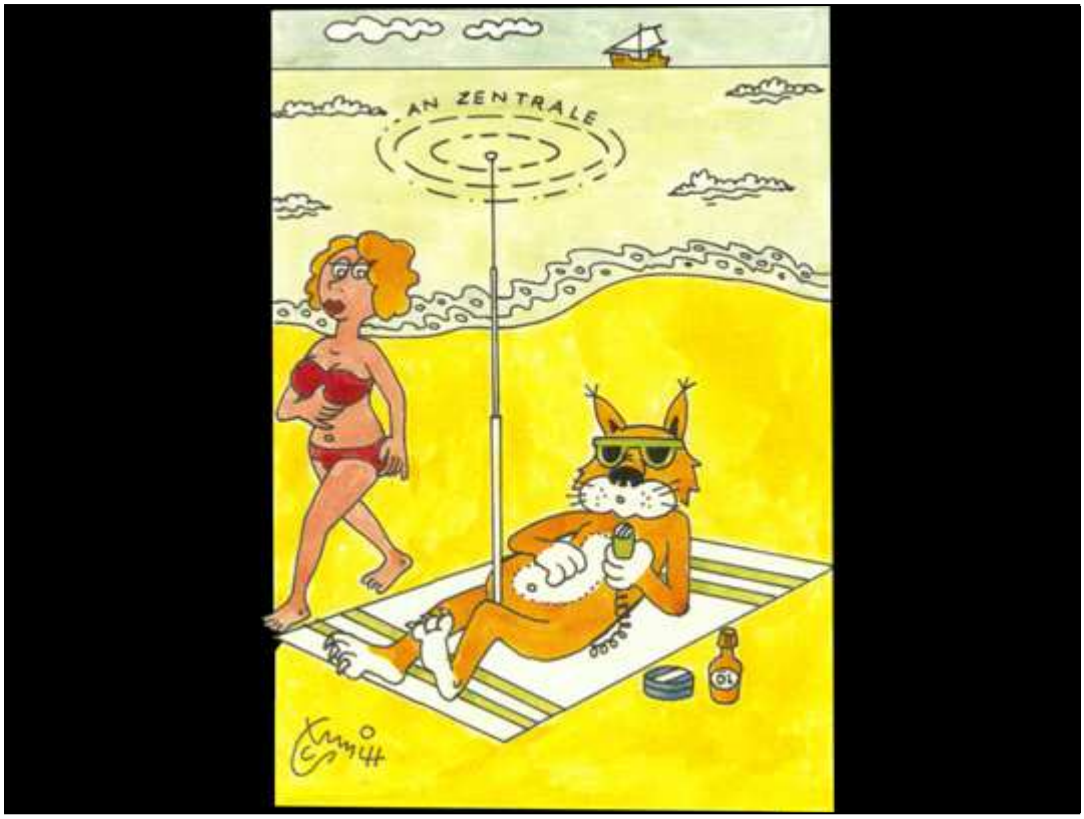
VVS JHS o001 - 70/80

BSIU 000442

111

Von imperialistischen Geheimdiensten ausgegebene Anweisung für Buchschlüsselverfahren

Diese Anweisungen erläutern die Verschlüsselung, der Agent setzt seinen Text in Zahlen um.



Ich beende meinen Vortrag mit einem weiteren beispiel der geheimen Kommunikation. Der Luchs sendet eine Nachricht an die Zentrale, dass er eine neue Agentin sucht.

MINISTERRAT
DER DEUTSCHEN DEMOKRATISCHEN REPUBLIK
Ministerium für Staatssicherheit
Hauptverwaltung A
1. Stellvertreter des Leiters

Berlin, 18. 10. 1988

Vertrauliche Verschlußsache
VVS-o015
MfS-Nr. A 27/88
45 Ausf. Bl. 1 bis XXI.

Beschluß
Generalleutnant

KOPIE BStU

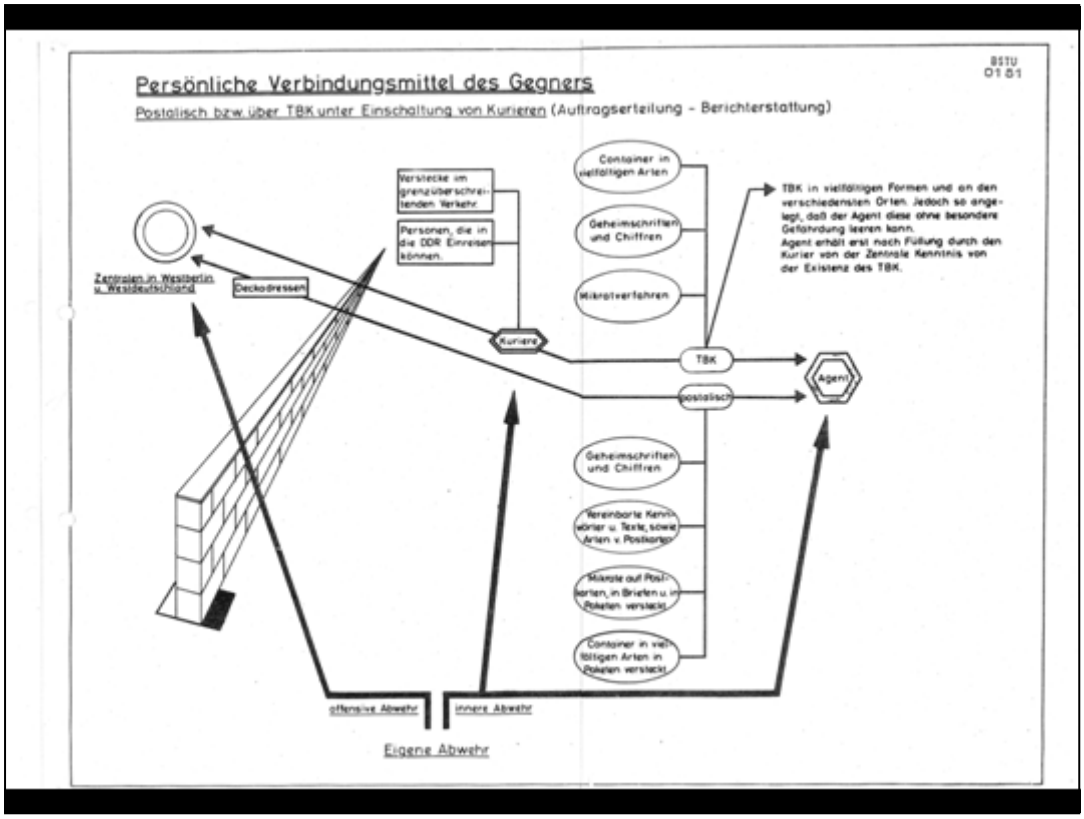
Ordnung Nr. 1/88 A
für die Arbeit mit operativen technischen
Mitteln der HV A

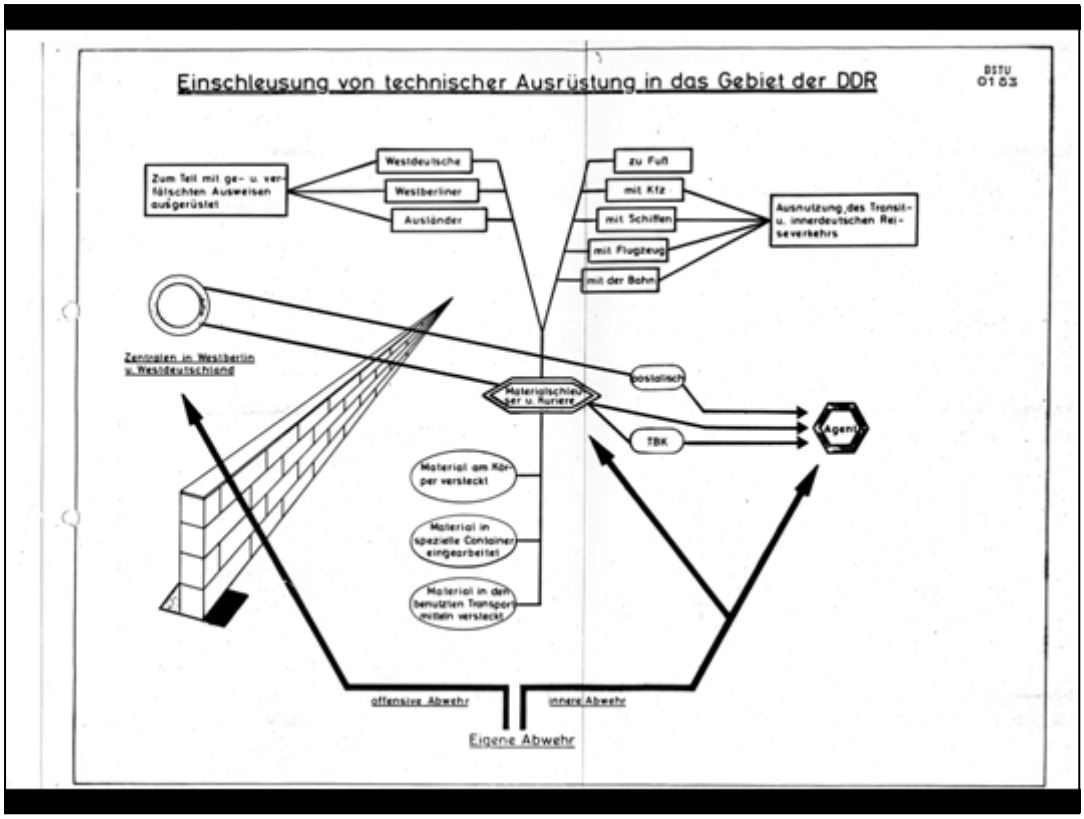
- ODM-Ordnung -

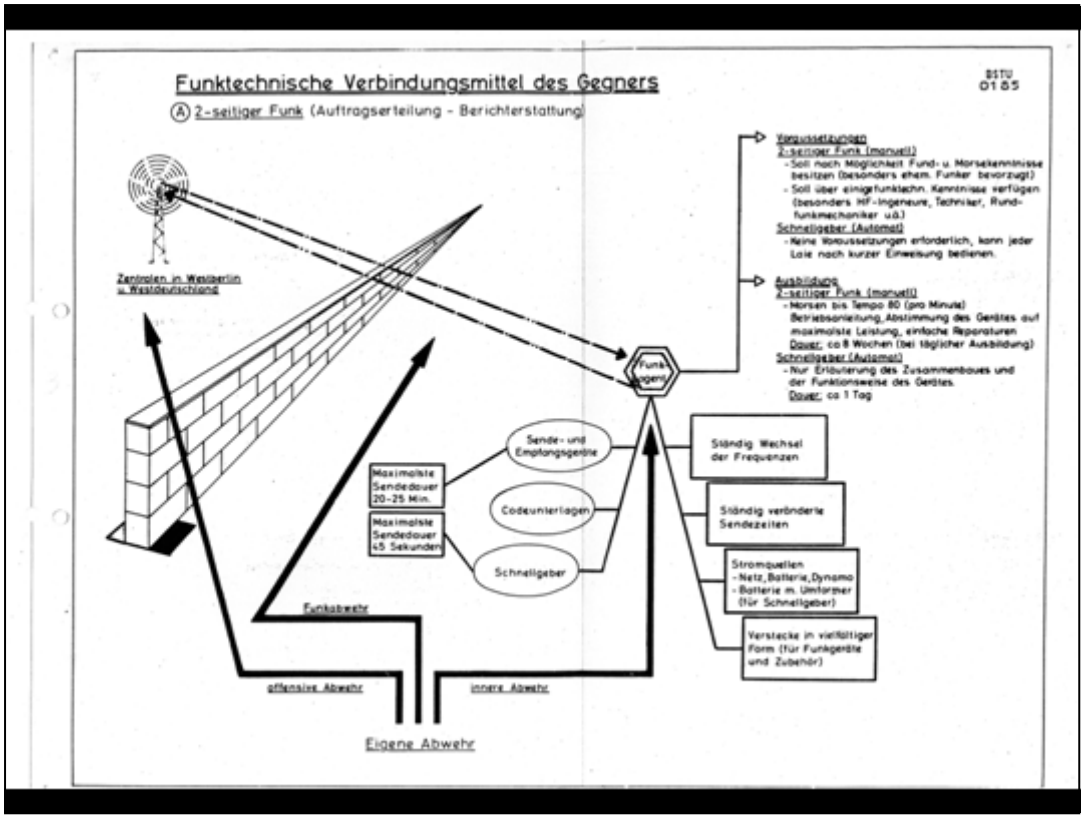
Tabelle 6/6: Verbindungsmittel (schließt Mehrfachnennungen ein)

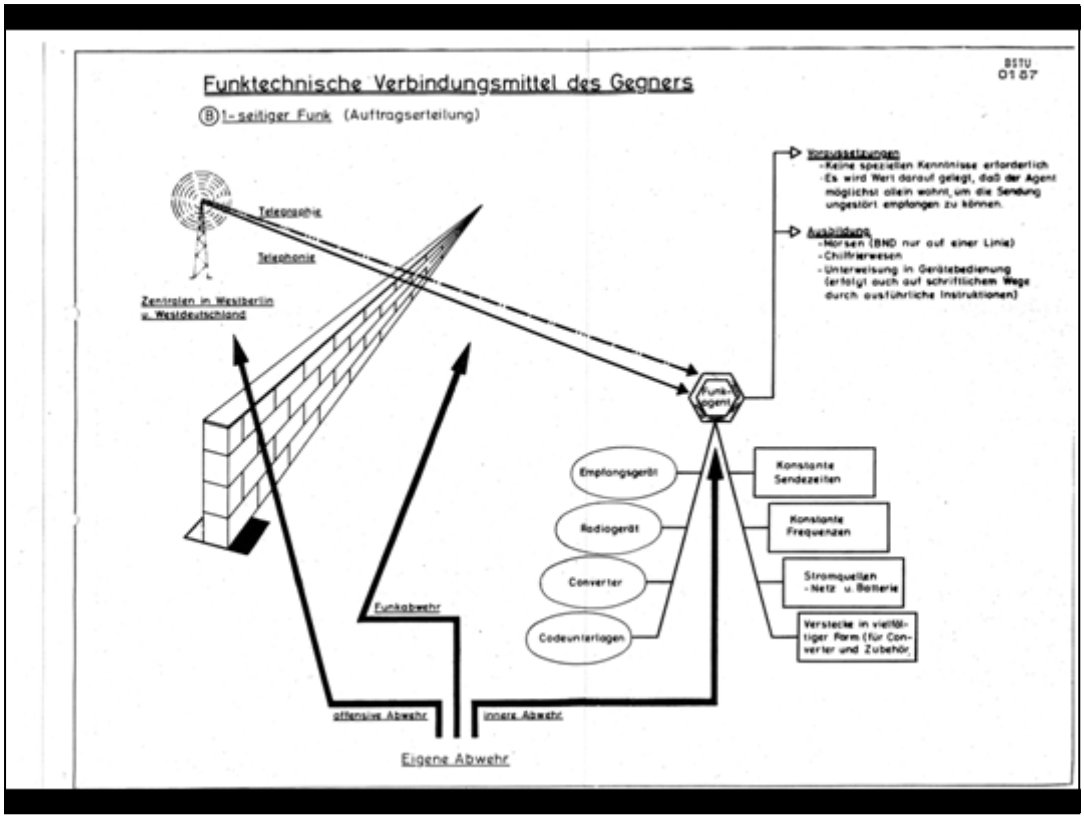
Verbindungsmittel	Anzahl
Deckadresse in der DDR	984
Instrukteurverbindung	786
Einseitiger KW-Funk	221
Chiffre	189
Geheimschreibmittel	148
Code	74
Persönliche Kurierverbindung	59
UKW-Signalsystem »Panorama«	43
Toter Briefkasten im Zug	42
Mikratfotografie	41
Toter Briefkasten	26
Verbindungsmittel »HD«	21
UKW-Funk »Horizont«	17
Zweiseitiger KW-Funk	15
Unpersönlicher Materialtransport	12
Deckadresse im »Operationsgebiet«	12

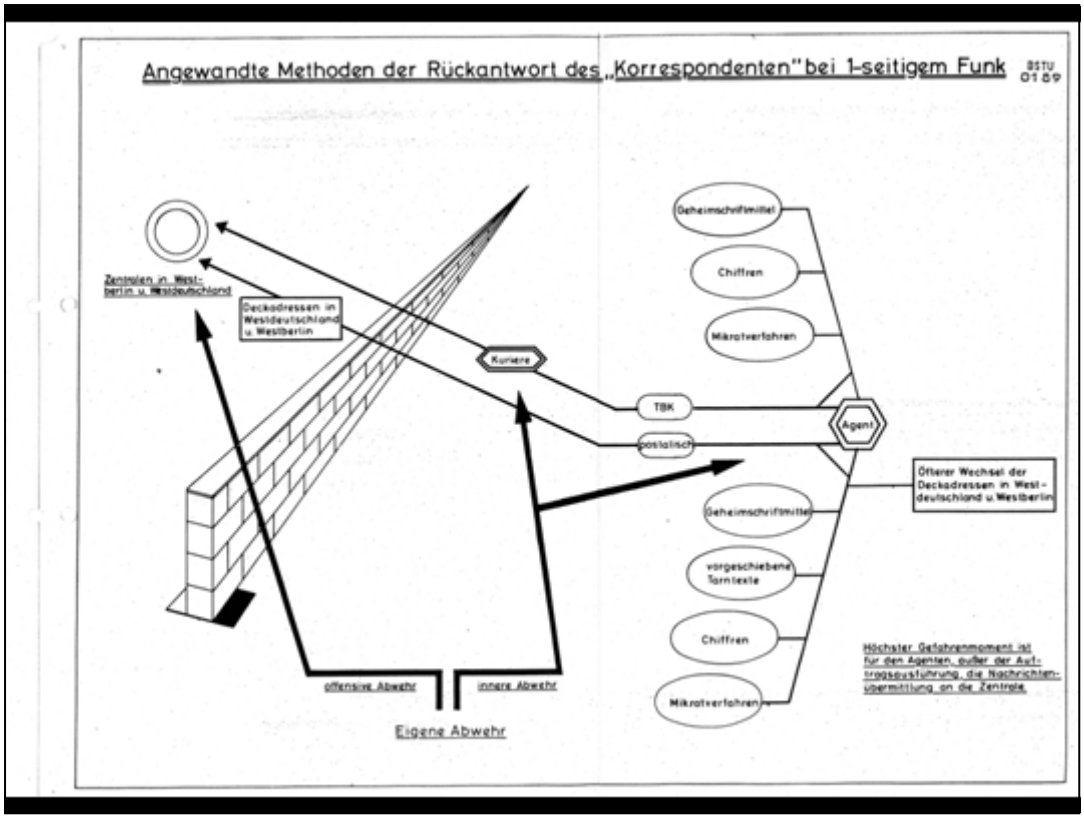
Communication system	Quantity
Cover address in the GDR	984
Instructor contact	786
One Way Shortwave Link	221
Chiffre	189
Secret Writing	148
Code	74
Personal Courier Contact	59
VHF-Signalling System »Panorama«	43
Dead Drop in Trains	42
Mikratphotography	41
Dead Drop	26
Telephone System »HD«	21
VHF-System »Horizont«	17
Two Way Shortwave Link	15
Unpersonal Materialtransport	12
Cover Address in BRD »Operationsgebiet«	12
(multiple mentions possible)	


BSTU
01 01
Persönliche Verbindungsmittel des Gegners
Postalisch bzw. über TBK unter Einschaltung von Kurieren (Auftragserteilung - Berichterstattung)
Container in vielfältigen Arten
Verstecke im grenzüberschreitenden Verkehr
Personen, die in die DDR Einreisen können.
Geheimschriften und Chiffren
Mikroverfahren
TBK in vielfältigen Formen und an den verschiedensten Orten. Jedoch so angelegt, daß der Agent diese ohne besondere Gefährdung leeren kann.
Agent erhält erst nach Füllung durch den Kurier von der Zentrale Kenntnis von der Existenz des TBK.
Zentralen in Westberlin u. Westdeutschland
Deckadressen
Kuriere
TBK
postalisch
Agent
Geheimschriften und Chiffren
Vereinbarte Kennwörter u. Texte, sowie Arten v. Postkarten
Makrote auf Postkarten, in Briefen u. in Paketen versteckt
Container in vielfältigen Arten in Paketen versteckt
offensive Abwehr
innere Abwehr
Eigene Abwehr


Einschleusung von technischer Ausrüstung in das Gebiet der DDR
BSTU
01 03
Zum Teil mit ge- u. verfälschten Ausweisen ausgerüstet
Westdeutsche
Westberliner
Ausländer
zu Fuß
mit Kfz
mit Schiffen
mit Flugzeug
mit der Bahn
Ausnutzung des Transit- u. innerdeutschen Reiseverkehrs
Zentralen in Westberlin u. Westdeutschland
postalisch
Materialschleuser u. Kuriere
TBK
Agent
Material am Körper versteckt
Material in spezielle Container eingearbeitet
Material in den benutzten Transportmitteln versteckt
offensive Abwehr
innere Abwehr
Eigene Abwehr


Funktechnische Verbindungsmittel des Gegners
BSTU
01 85
Ⓐ 2-seitiger Funk (Auftragserteilung - Berichterstattung)
Zentralen in Westberlin u. Westdeutschland
Funk gegner
Voraussetzungen
2-seitiger Funk (manuell)
- Soll nach Möglichkeit Fund- u. Morsekenntnisse besitzen (besonders ehem. Funker bevorzugt)
- Soll über einige funktechn. Kenntnisse verfügen (besonders HF-Ingeneure, Techniker, Rundfunkmechaniker u.ä.)
Schnellgeber (Automat)
- Keine Voraussetzungen erforderlich, kann jeder Laie nach kurzer Einweisung bedienen.
Ausbildung
2-seitiger Funk (manuell)
- Morsen bis Tempo 80 (pro Minute)
Betriebsanleitung, Abstimmung des Gerätes auf maximalste Leistung, einfache Reparaturen
Dauer: ca 8 Wochen (bei täglicher Ausbildung)
Schnellgeber (Automat)
- Nur Erläuterung des Zusammenbaues und der Funktionsweise des Gerätes.
Dauer: ca 1 Tag
Sende- und Empfangsgeräte
Codeunterlagen
Schnellgeber
Maximalste Sendedauer 20-25 Min.
Maximalste Sendedauer 45 Sekunden
Ständig Wechsel der Frequenzen
Ständig verränderte Sendezeiten
Stromquellen
- Netz, Batterie, Dynamo
- Batterie m. Umformer (für Schnellgeber)
Verstecke in vielfältiger Form (für Funkgeräte und Zubehör)
Funkabwehr
offensive Abwehr
innere Abwehr
Eigene Abwehr


BSTU
01 87
Funktechnische Verbindungsmittel des Gegners
(B) 1-seitiger Funk (Auftragserteilung)
Telegrafie
Telephonie
Zentralen in Westberlin u. Westdeutschland
Funk-agent
Voraussetzungen
-Keine speziellen Kenntnisse erforderlich
-Es wird Wert darauf gelegt, daß der Agent möglichst allein wohnt, um die Sendung ungestört empfangen zu können.
Ausbildung
-Hörsen (BND nur auf einer Linie)
-Chiffrieren
-Unterweisung in Gerätebedienung (erfolgt auch auf schriftlichem Wege durch ausführliche Instruktionen)
Empfangsgerät
Radiogerät
Converter
Codeunterlagen
Konstante Sendezeiten
Konstante Frequenzen
Stromquellen -Netz u. Batterie
Verstecke in vielfältiger Form (für Converter und Zubehör)
Funkabwehr
offensive Abwehr
innere Abwehr
Eigene Abwehr


Angewandte Methoden der Rückantwort des „Korrespondenten" bei 1-seitigem Funk
BSTU
01 89
Zentralen in Westberlin u. Westdeutschland
Deckadressen in Westdeutschland u. Westberlin
Kuriere
TBK
postalisch
Agent
Geheimschriftmittel
Chiffren
Mikrotverfahren
Geheimschriftmittel
vorgeschiebene Tarntexte
Chiffren
Mikrotverfahren
Öfterer Wechsel der Deckadressen in Westdeutschland u. Westberlin
Höchster Gefahrenmoment ist für den Agenten, außer der Auftragsausführung, die Nachrichtenübermittlung an die Zentrale.
offensive Abwehr
innere Abwehr
Eigene Abwehr

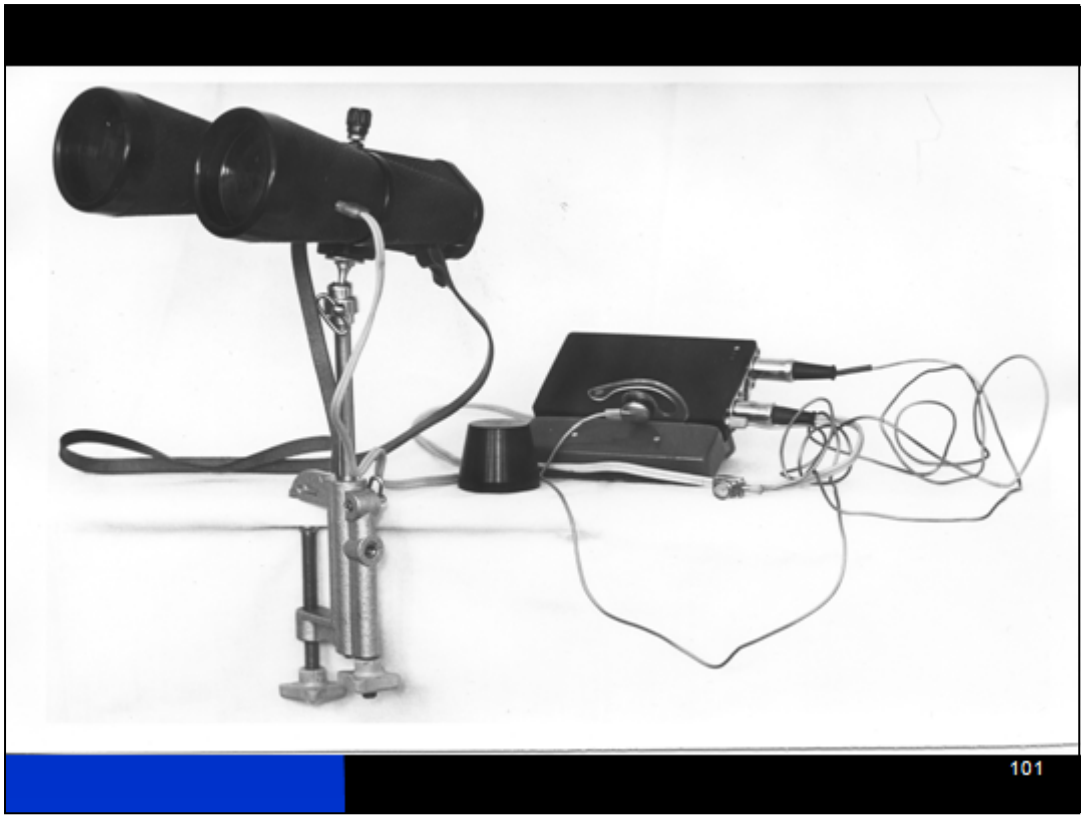
Das ist ein sehr alter DDR Agentenfunksender mit einem Schnellgeber, der ein gestanztes Tonband benutzt.

Ein DDR Sender der nächsten Generation. Links der Schnellgeber um die Sendedauer zu reduzieren, er nutzt eine Tonband-Endlosschleife. Rechts das Netzgerät, hinten das Kästchen mit Quarzen

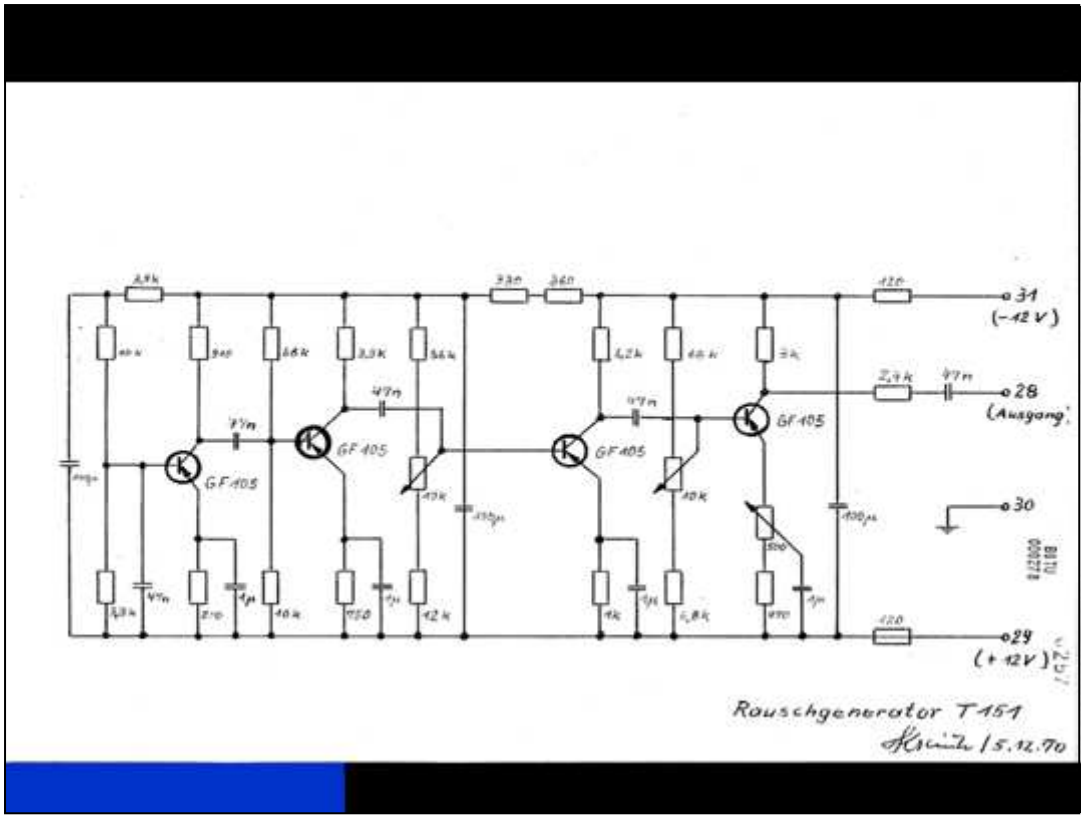
Der neuere HV A Sender WSA 1 (Weitverkehrssendeanlage)

Die letzte Sendegeneration WSA 6, die nicht mehr zum Einsatz gekommen ist.

Eine modulare Version des WSA 6 mit einem Taschenrechner als Bediengerät.



Ein Lichtsprechgerät der HV A, das in einem Fernglas getarnt war. Es ist von einem MfS-Überläufer verraten worden und nicht zum Einsatz gekommen.



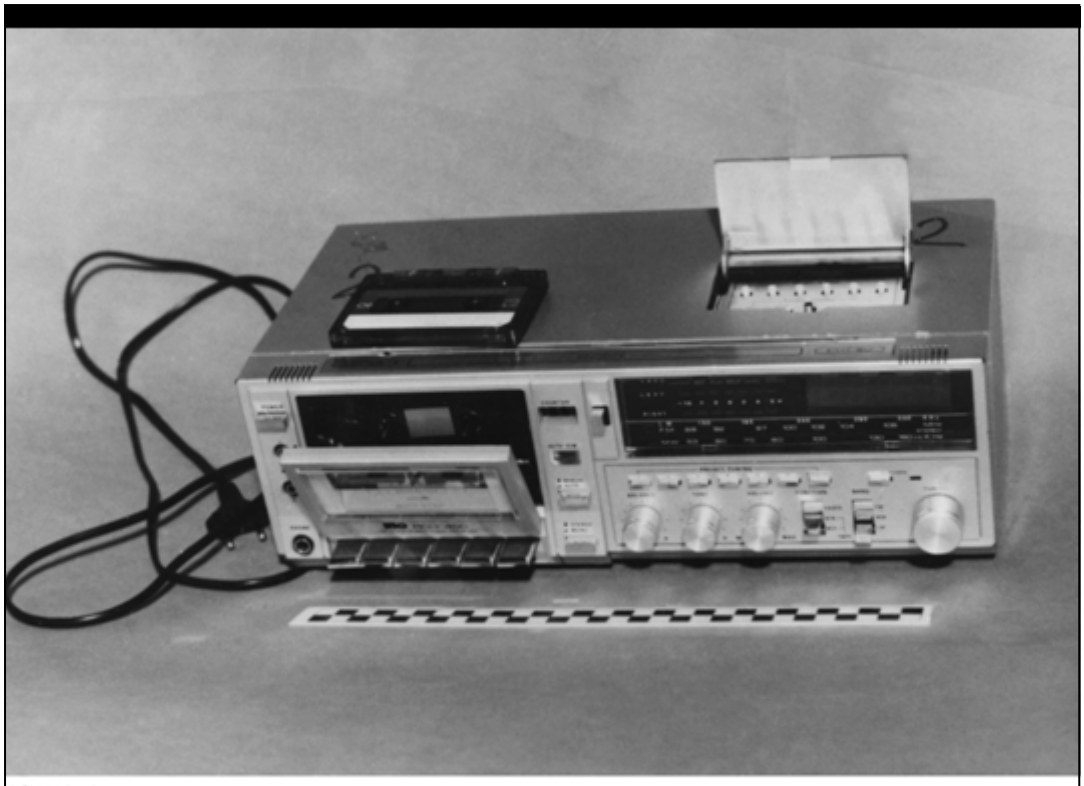
Das Schaltbild zeigt einen Rauschgenerator zum Erzeugen von Zufallszahlen.

5 solcher Generatoren wurden verwendet, um die 5 Löcher in Lochstreifen zu stanzen.

G	U	T	E	H	A	L	T	E	N	I	C	H	B	I	N	G	E	W	I	S	S
7	21	19	4	9	1	14	20	5	15	11	3	10	2	12	16	8	6	22	13	17	18

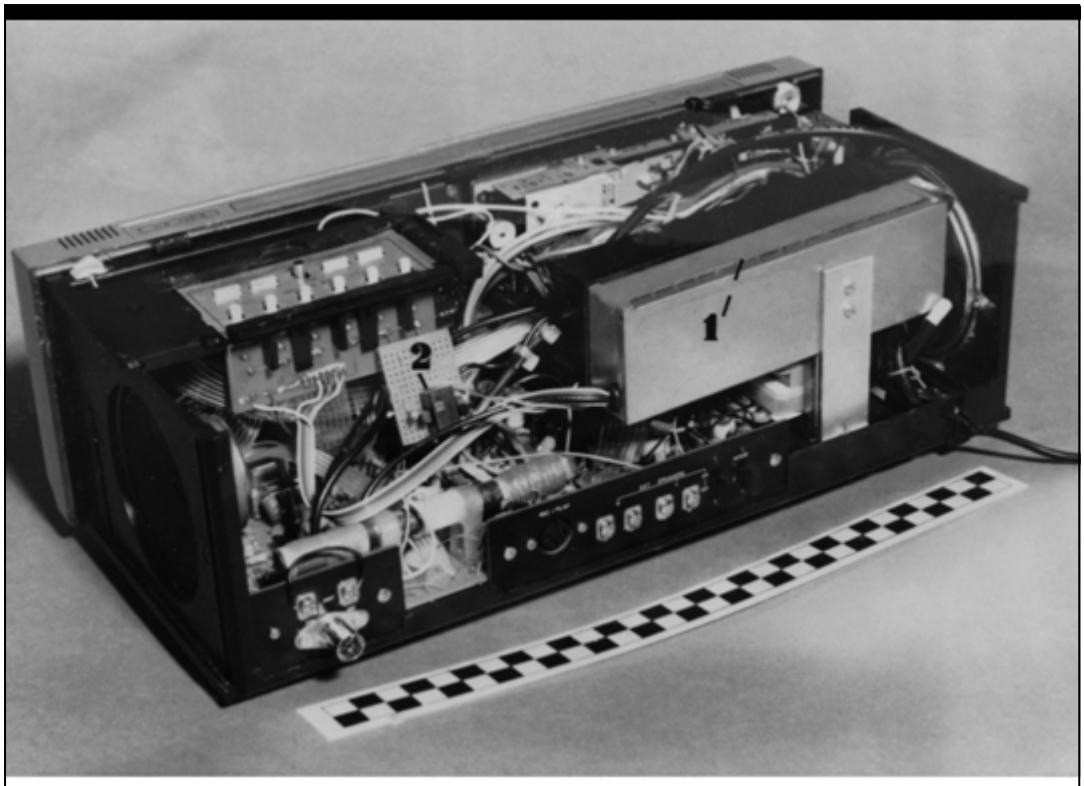
D	A	S	S	E	R	D	E	R	F	E	I	N	S	T	E	M	A	N	N		
3	1	17	18	5	15	4	6	16	9	7	10	12	19	20	8	11	2	13	14		

Dann wurden 2 Schlüsselsätze zum Verwürfeln verwendet.

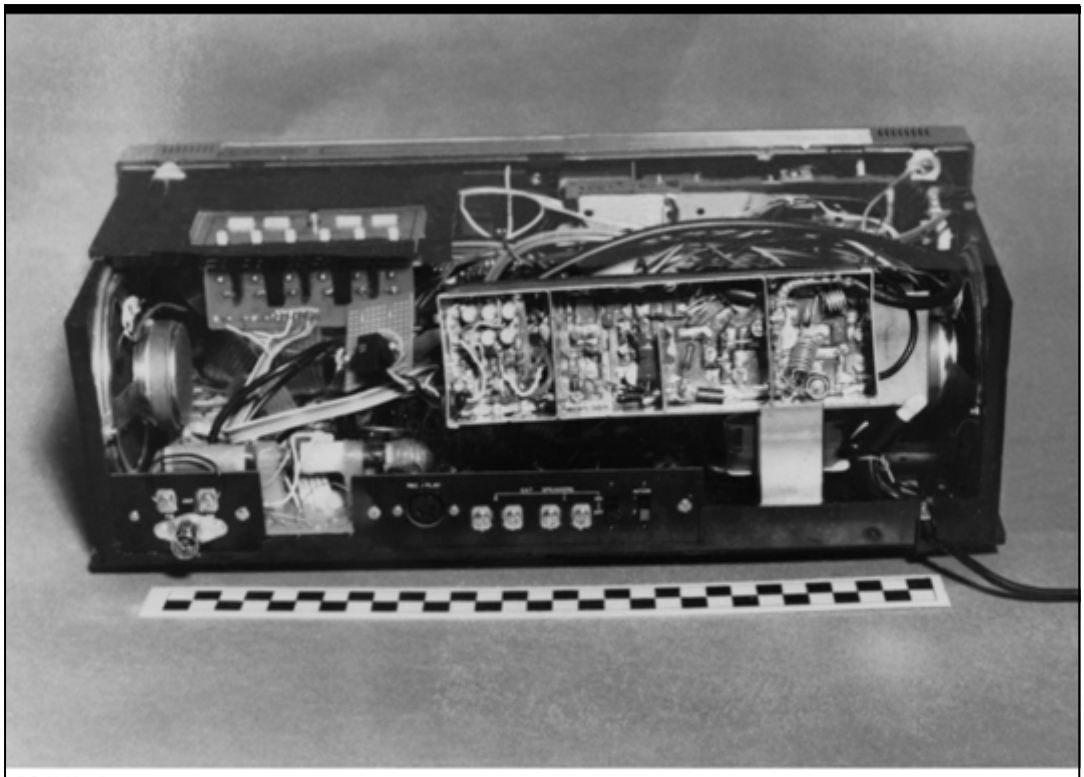


BStU-Kopie

Die folgenden Geräte wurden bei Westagenten gefunden. Es gibt leider keine weiteren Informationen.



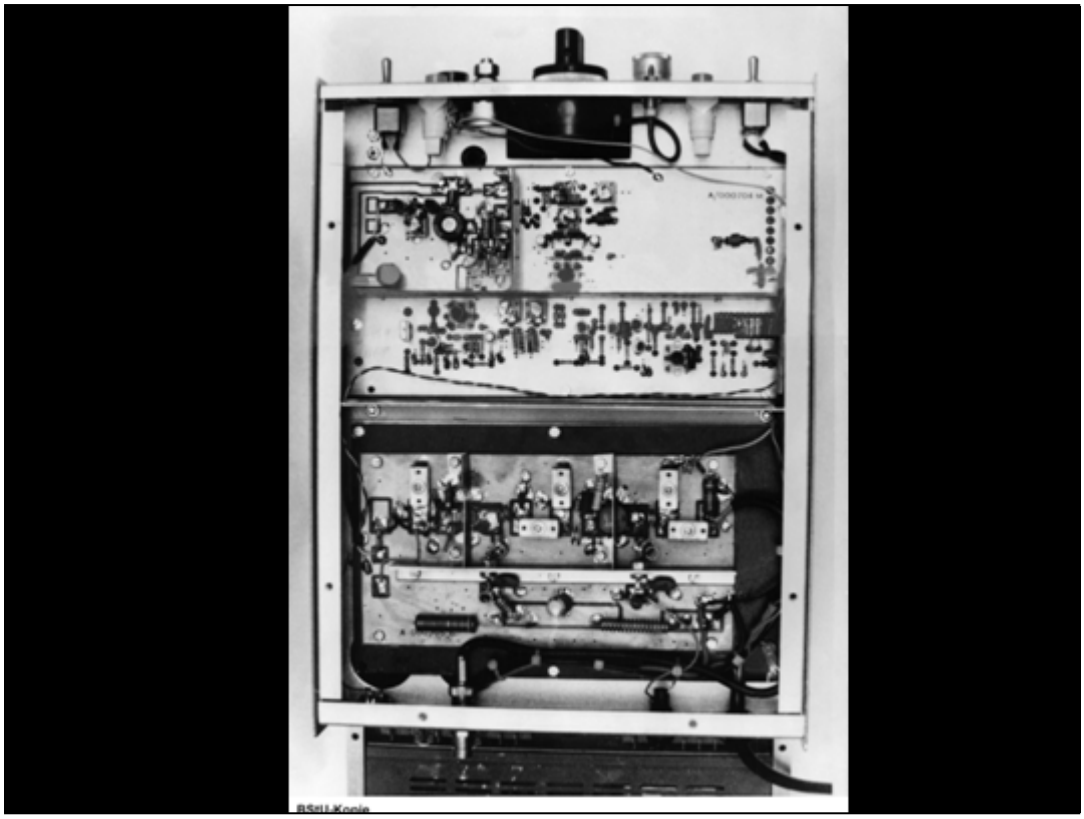
BStU-Kopie



BStU-Kopie

BStU-Kopie

Das Gerät ist in Polen gefunden worden.



Ein Beispiel für aktuelle Agentenkommunikation