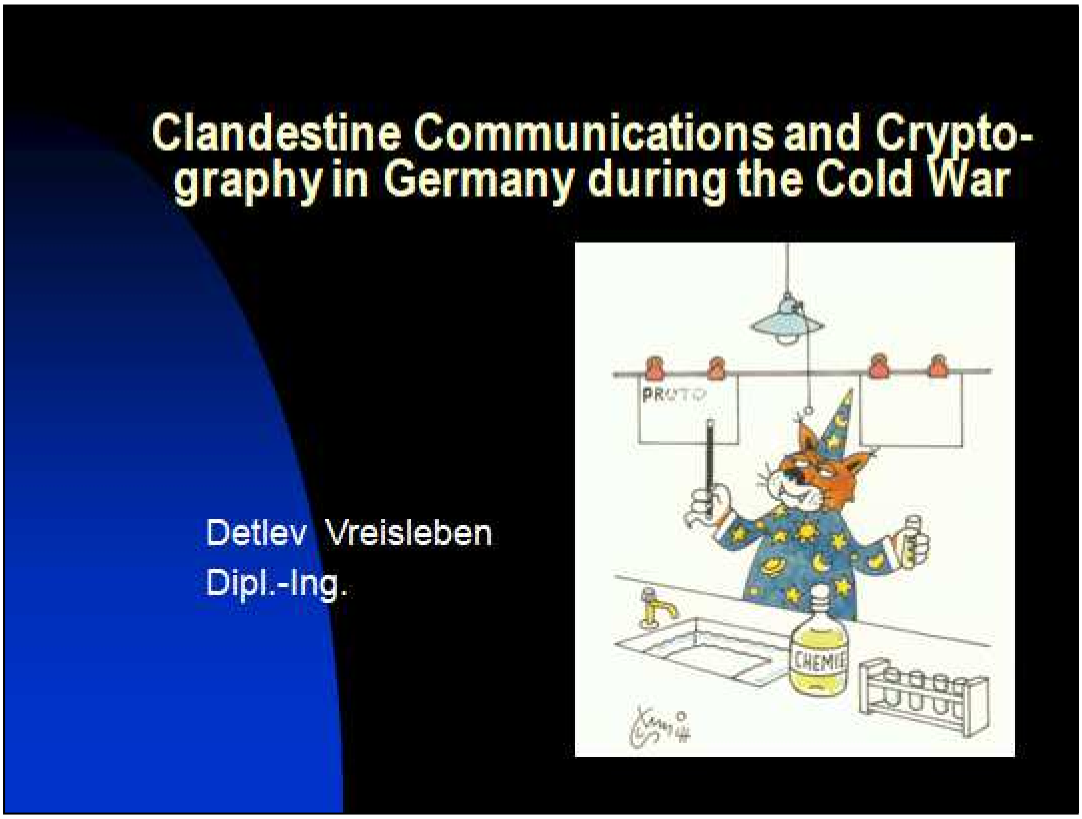


Good afternoon, ladies and gentlemen,

My name is Detlev Vreisleben and I would like to speak about clandestine communications and cryptography in Germany during the Cold War.

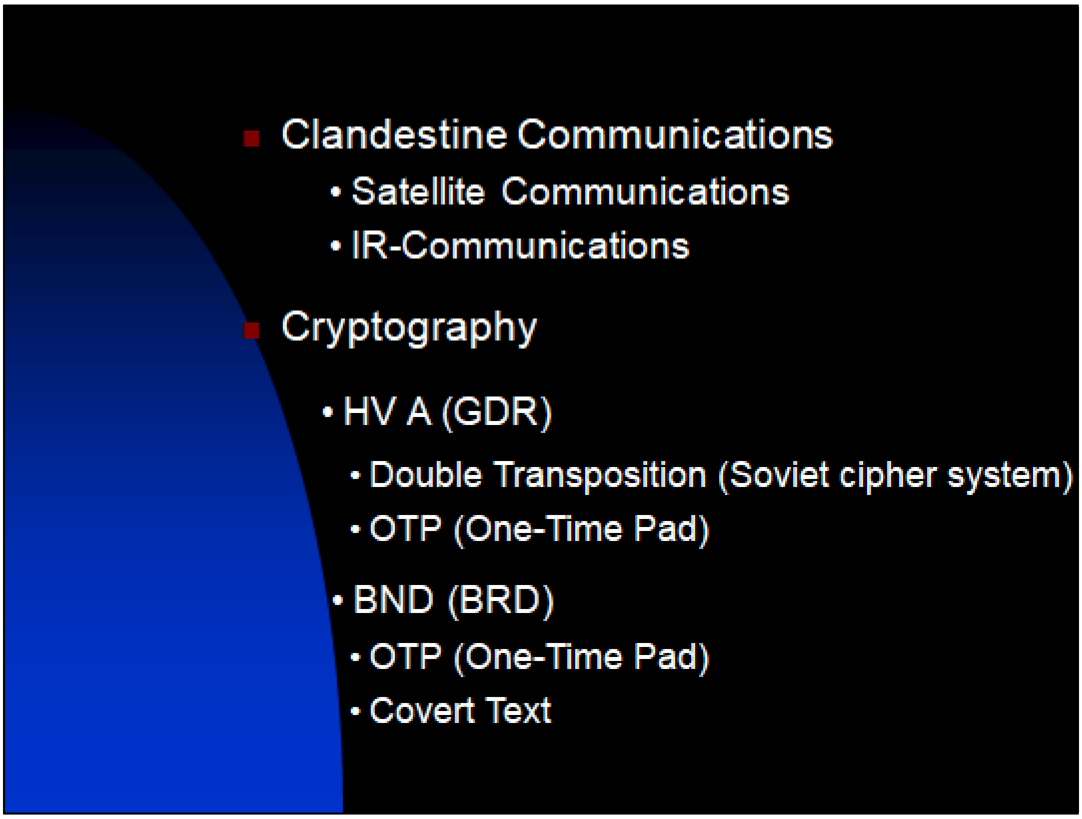
Here you see Markus Wolf the head of the HV A – the Foreign Intelligence Service of the GDR – portrayed as a lynx demonstrating the use of disappearing ink. This cartoon was drawn by GDR-Cartoonist Erich Schmitt for Markus Wolf‘s 60th birthday in 1983. In fables, the lynx is a crafty animal without the negative association of the wolf.

Negative: Like eating Little Red Ridinghood‘s grandmother.

I would like to show various possibilities of clandestine communications.

The electronic Dead Drop is also called SRAC (Short Range Agent Communications)

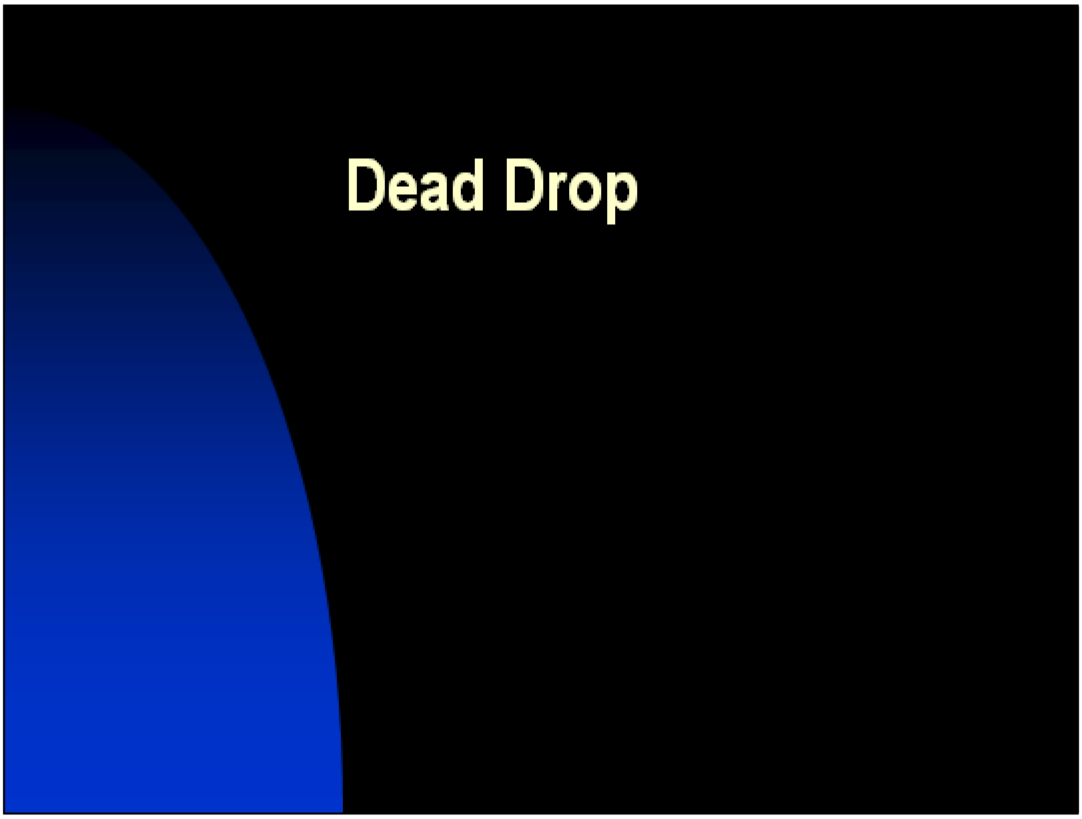
The mikrat is a larger negative than a microdot.



- Satellite
- Infrared

-And in the second part cryptography

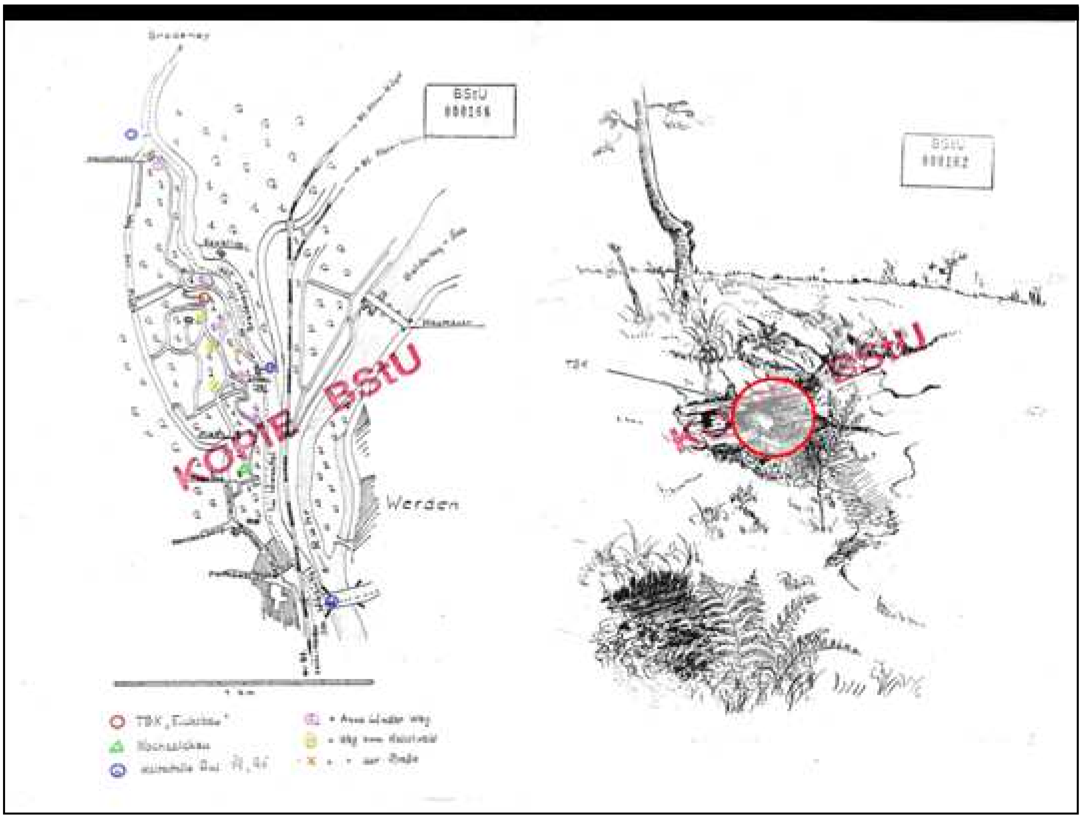
-Used bei HV A (Foreign Intelligence Service of the GDR)
-and BND (German Intelligence Agency)

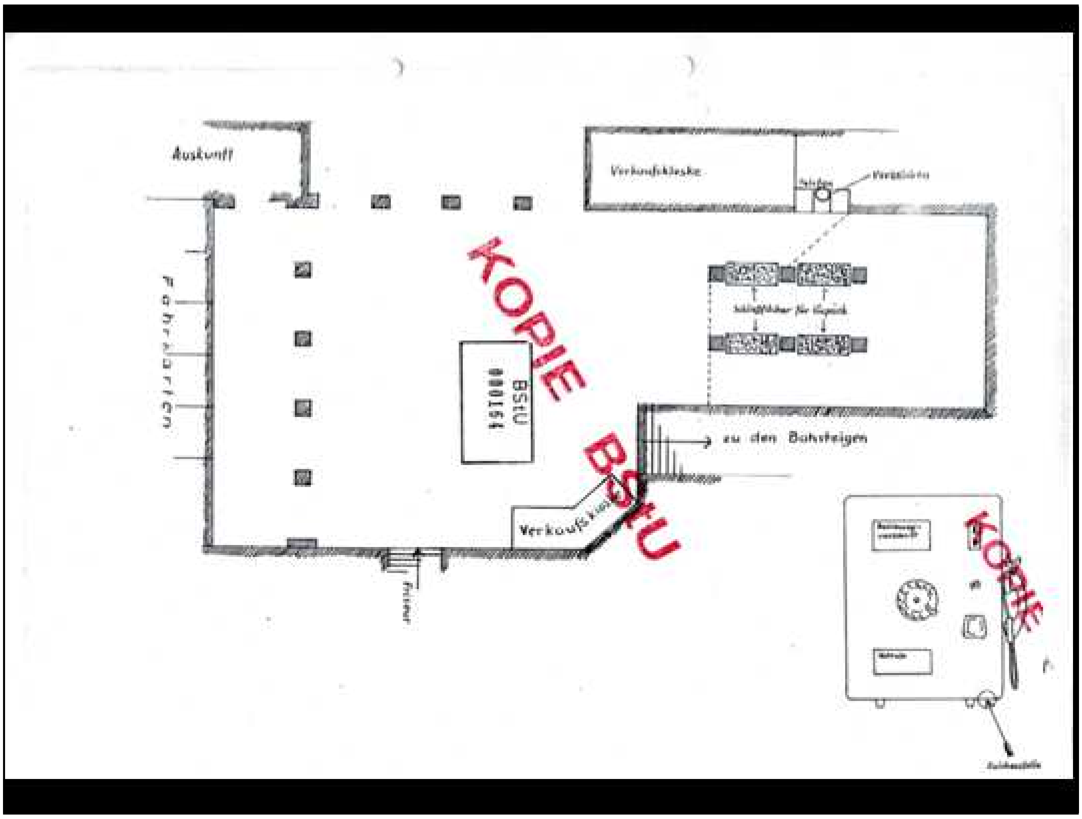


A dead drop is a prearranged location at which spies can leave information or from which they can collect instructions or material.

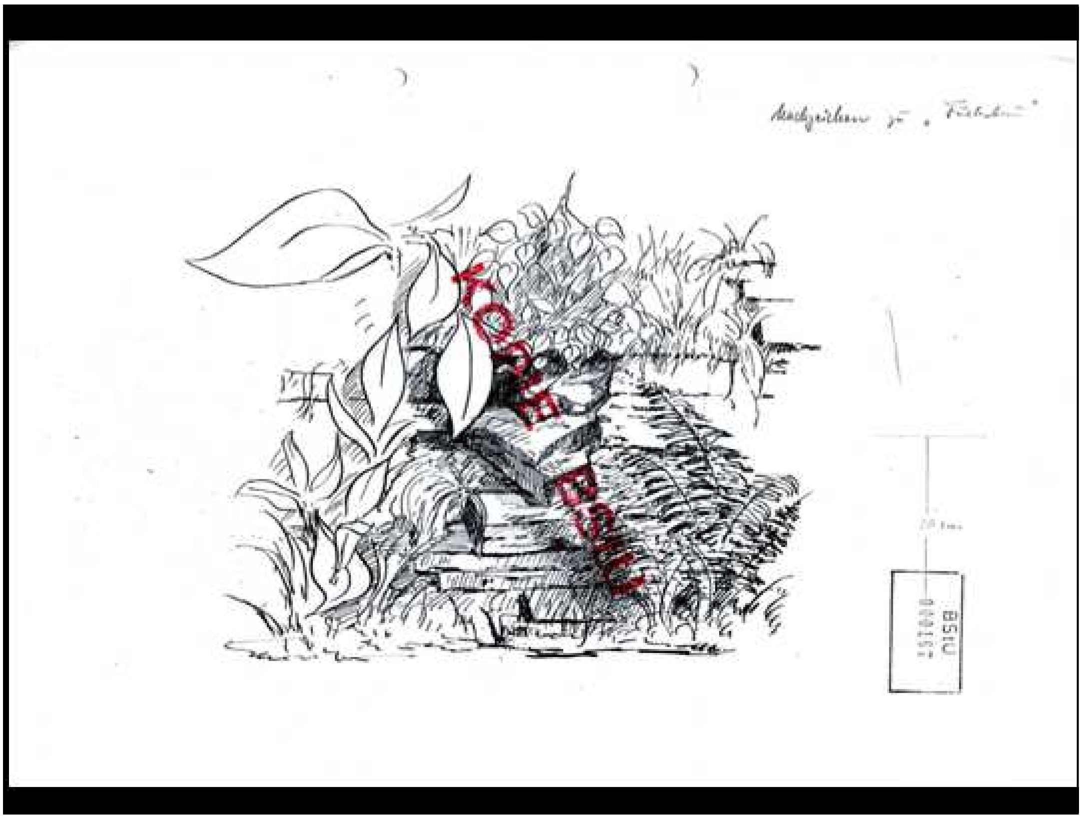
The picture shows a Russian container used for a dead drop. This one could be used for money, films and cipher pads.

A dead drop is used to avoid having personal contact which could lead to exposure.


BStU
Werden
KOPIE BStU
BStU
TBK
KOPIE BStU



There were additional signs when to go to the dead drop. You see here a telephone, and here at the bottom right, the telephone with a chalk mark.



And a sign when the dead drop had been emptied. An empty cigarette pack „Ernte 23“ was dropped down there.

These devices can store information sent by an agent as he passes by. Later, the information can be picked up by other agents with no physical contact to the device. The SRAC had a very limited range i.e. 100 m.

The MfS (Ministry for State Security of the GDR) began developing such devices in the 1980s.

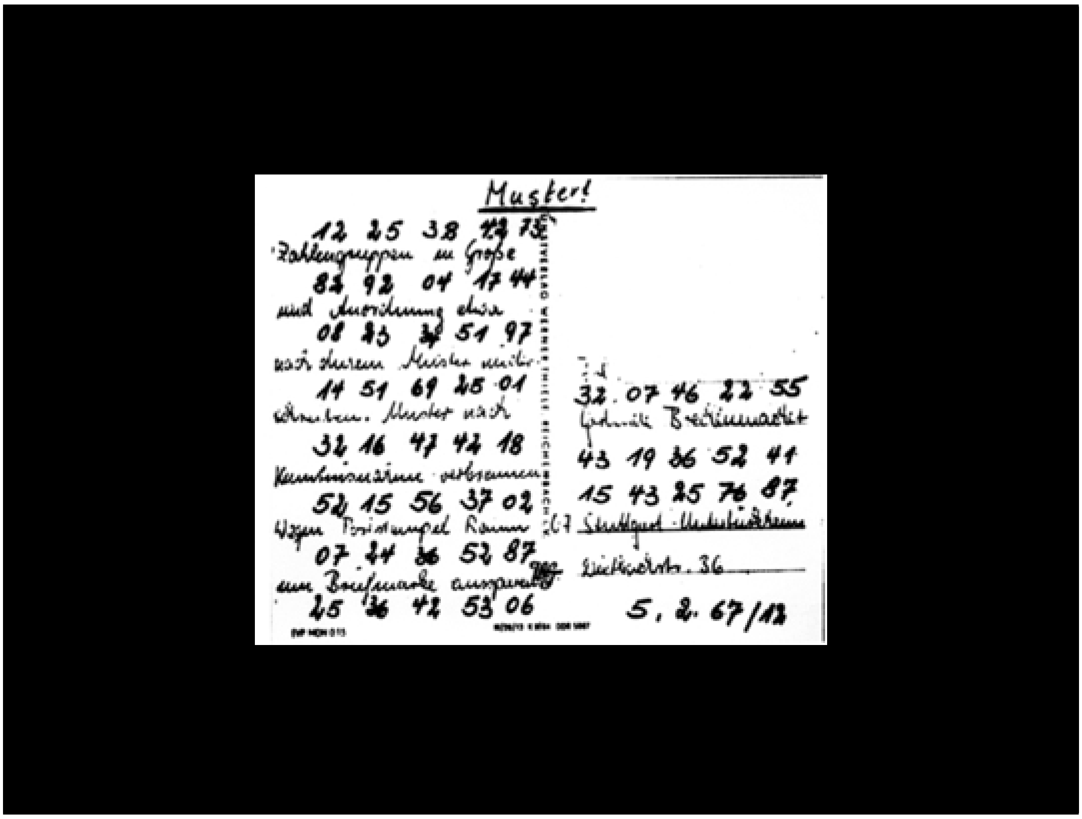
And here is a more recent example: In 2006 the FSB (Federal Security Service of the Russian Federation) uncovered 2 such British SRAC devices disguised as rocks in Moscow.


Stone Visitor
Каменный
гость
Russian TV documentary movie

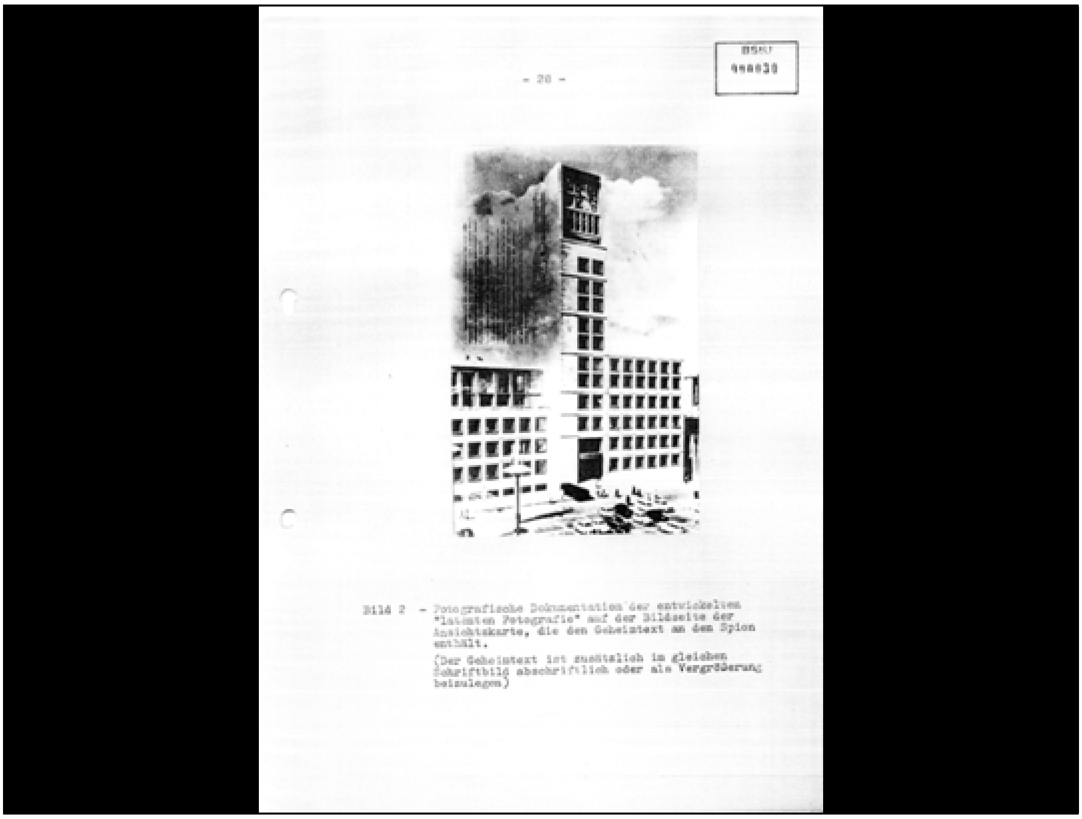
Secret Writing

Secret writing / invisible ink

Coded information
i.e. the picture of a postcard



Here is a sample postcard for an agent showing how to write with invisible ink between the lines of text.



BStU
000039

- 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)

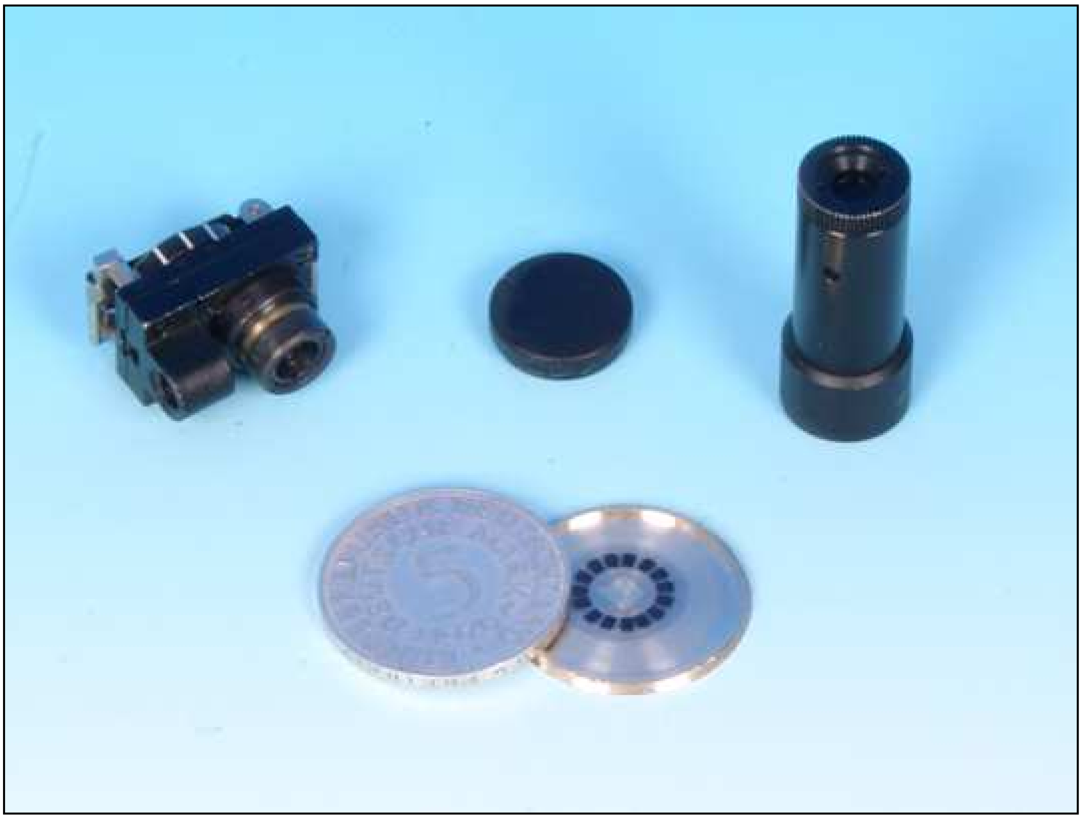
A postcard from headquarters to the agent with the text hidden in the picture on the postcard.

A welcoming message in plain text for a new agent!

Mikrat Communications

The mikrat process is a two-way process, instructions from the head office to the agent and copies of documents from the agent to the head office.

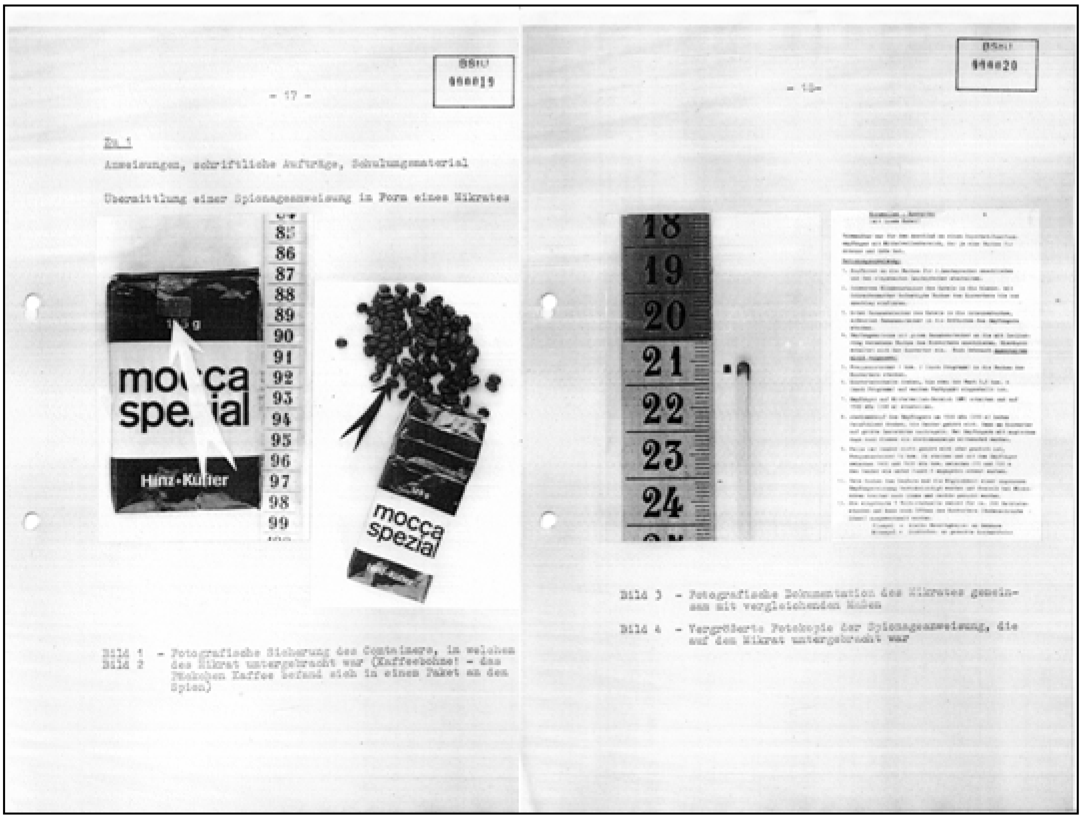
A mikrat is a film 1.4 by 2 mm larger than a microdot. Due to the small size they could be hidden under stamps, in letters, between the layers of a postcard or in packets.



A picture of an agents camera. In the forefront a film disc with 15 negatives. Each negative corresponds to a DIN A4 page. All hidden in a 5DM coin.

A mikrat reader for agents.

The negative is slipped into the slot on the left-hand side, and the agent can view the film by looking into the eye-piece on the right.


BStU
000019

- 17 -

Zu 1

Anweisungen, schriftliche Aufträge, Schulungsmaterial

Übermittlung einer Spionageanweisung in Form eines Mikrates

Bild 1 – Fotografische Sicherung des Containers, in welchem
Bild 2 des Mikrat untergebracht war (Kaffeebohne! – das Päckchen Kaffee befand sich in einem Paket an den Spion)

BStU
000020

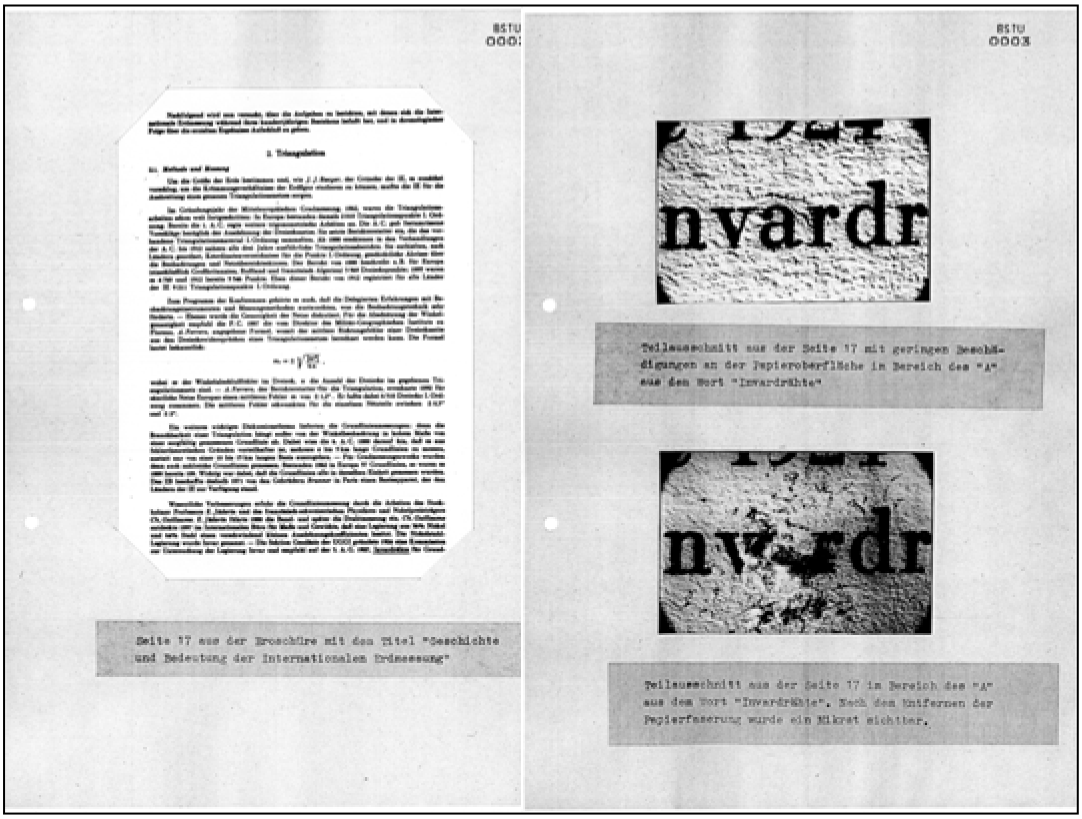
- 18 -

Bild 3 – Fotografische Dokumentation des Mikrates gemeinsam mit vergleichenden Maßen

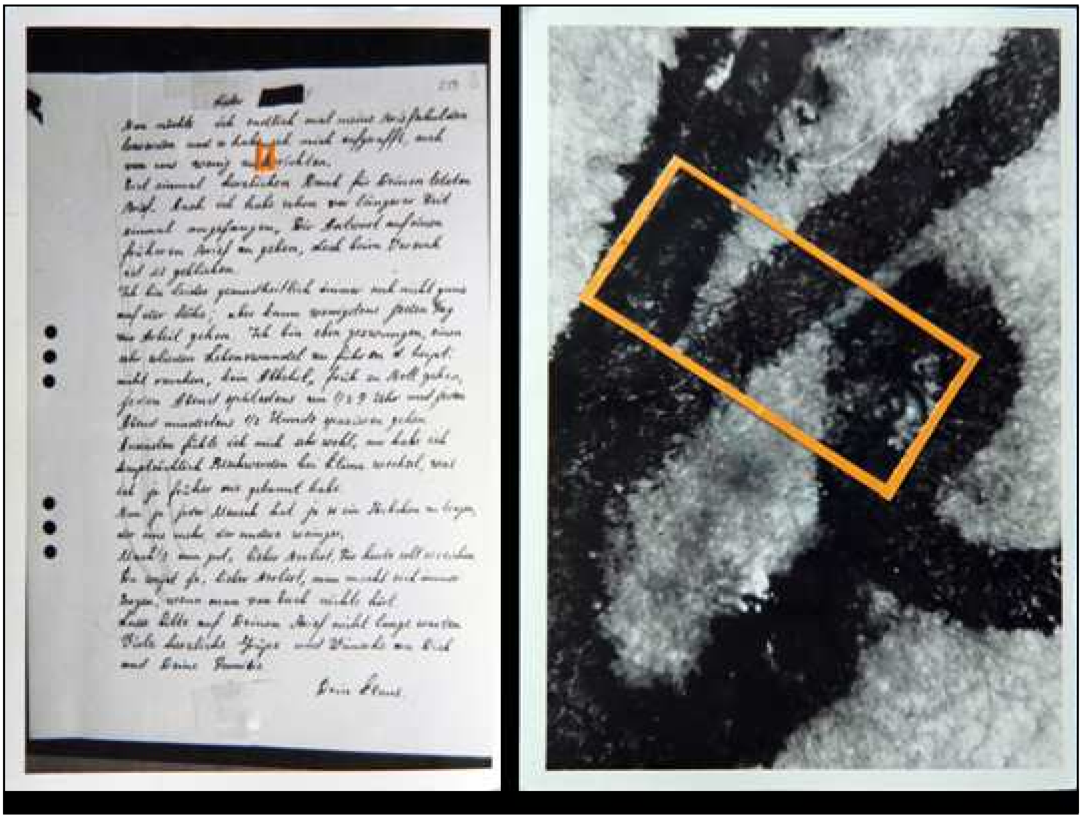
Bild 4 – Vergrößerte Fotokopie der Spionageanweisung, die auf dem Mikrat untergebracht war

Here you see a mikrat hidden in a coffee bean. It contained the instructions for the shortwave converter of the BND.

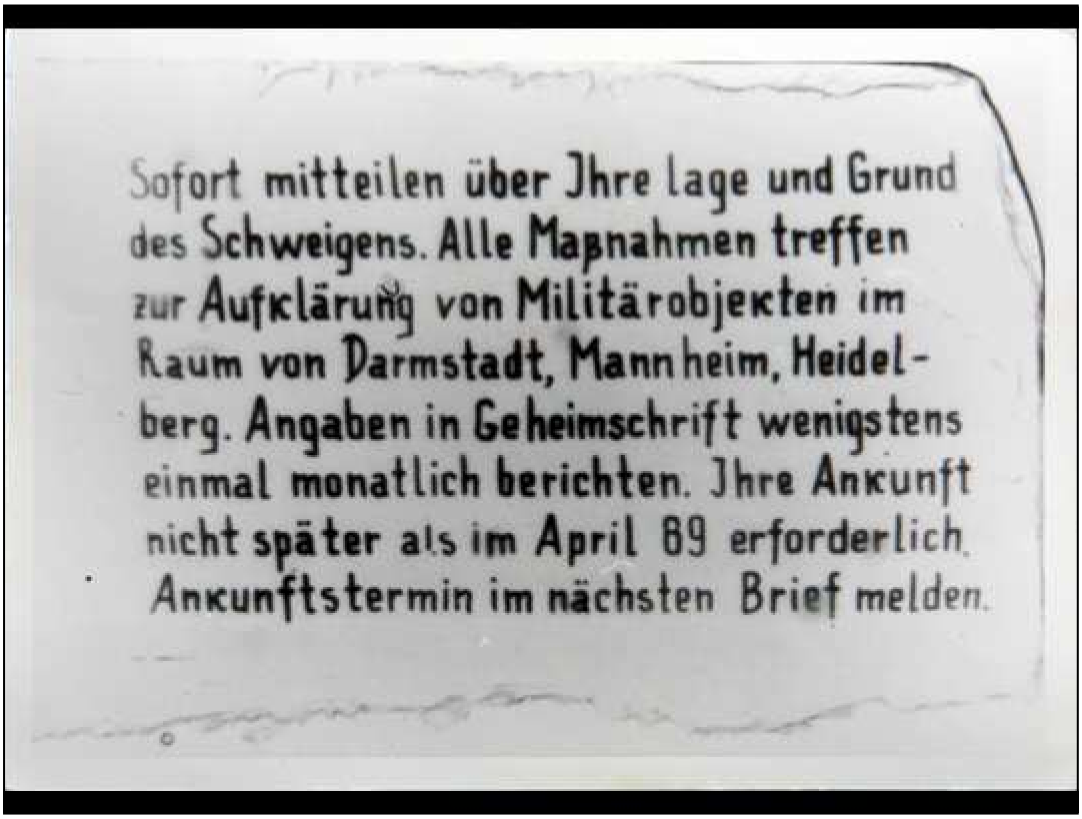
Somehow... The agent knows there is a mikrat in the package in the fourth item on the table of contents. And how did the Stasi find out? They observed that several packages with the same contents and the same packaging materials were being sent, so they had a clue.



A microdot hidden in a brochure. It is only .6 by .9 mm!



The HV A used that method still in 1989. The agent knew where the micrat was.


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

Here the enlarged Text of the microdot:

Communicate immediately your situation and the reason for the silence. Take all measures for reconnaissance of military objects in the area of Darmstadt, Mannheim, Heidelberg. Report details in invisible ink at least once a month. Your arrival is required not later than April 89. Report the arrival date in the next letter.

Telephone

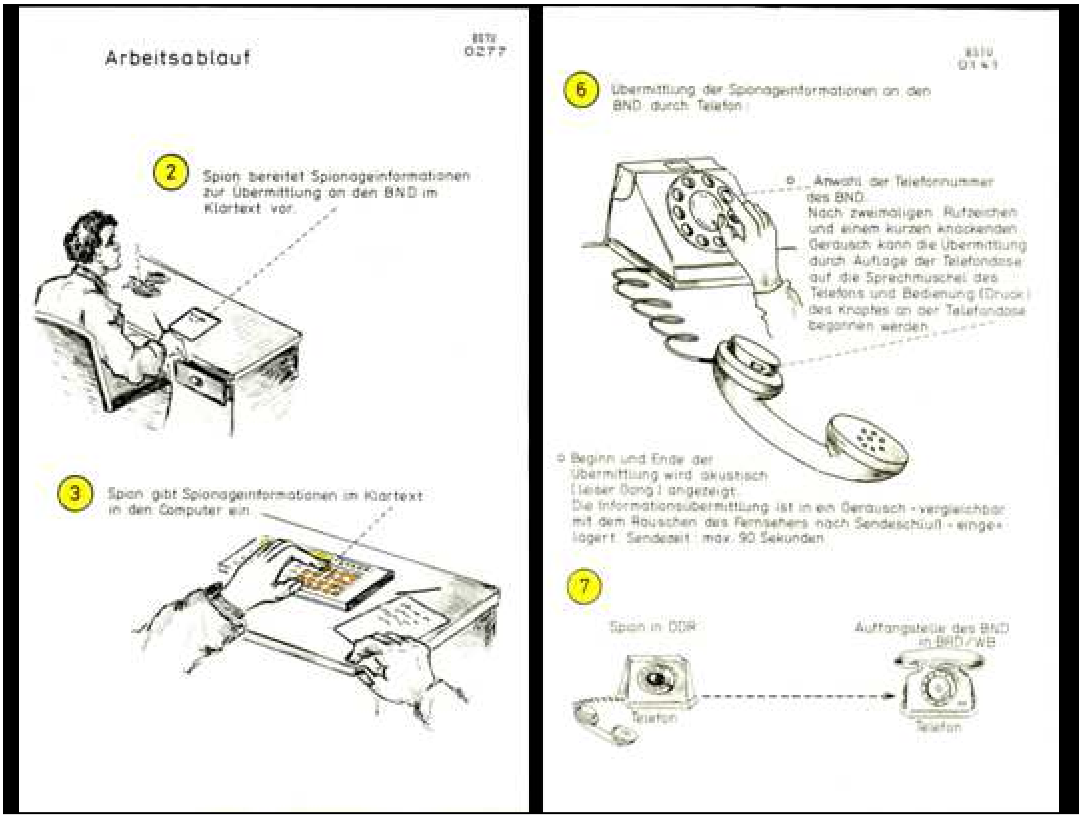
Transmission of a data stream by public telephone

The agent transmits encrypted messages stored in the calculator with an acoustic coupler via a public telephone

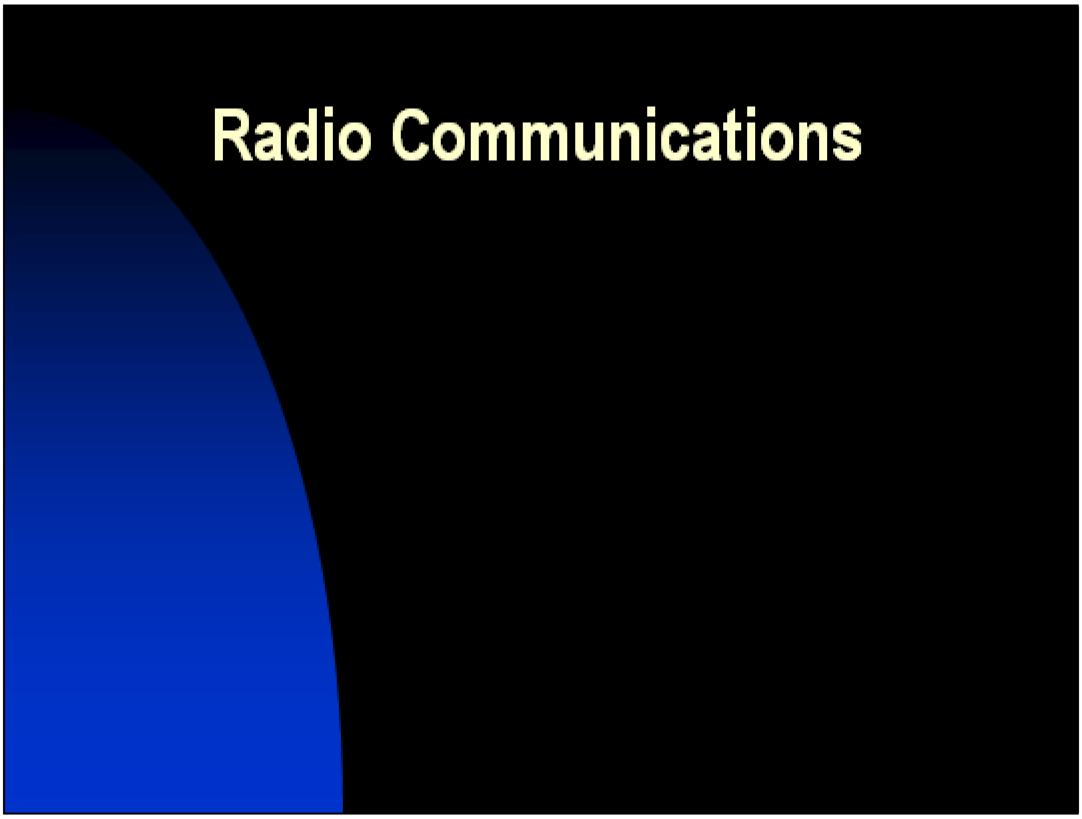
On the left agent's calculator

On the right a computer at the headquarters to receive and print the message

The famous NATO-spy Rainer Rupp used such a device camouflaged as a calculator in 1983 during the NATO manoeuvre Able Archer.



The BND used a similar procedure, here pictures of the HA II, counter-espionage. Unfortunately, there is no information as to whether the Sharp computer was used to encrypt.



There are two types of radio communications.

One way representing communications from headquarters to the agent and

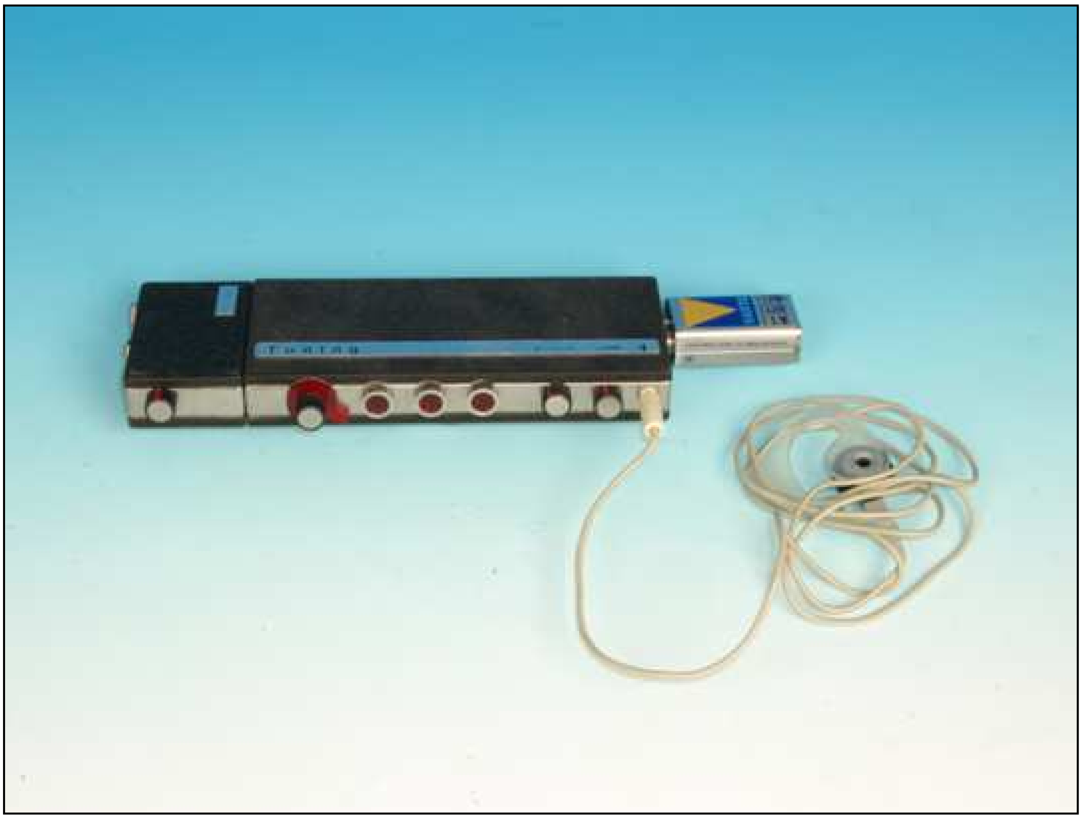
two ways where the agent can reply.

Radio communication was fairly common. Roughly 200 HV A agents received their instructions via radio, but in time of war only 15 would have been able to transmit messages.

This is a voice generator for encoded messages.

The face behind the voice.

Usually the agents used ordinary radios to receive their messages.
They switched them on at a pre-arranged time.



For special cases the MfS had special receivers

In the early years, the BND gave their agents in the GDR a converter to receive their transmission, as the GDR radios could not receive the BND frequencies.

Later, the BND agents were equipped with a FE-10 SW receiver.

The HV A transmitting site was in Zeesen near Berlin, the receiving site in Wernsdorf.

BND used three transmitting sites: Munich, Monschau and Frankfurt/Main (together with CIA)

Here is a view inside the Zeesen transmitting site. They used 1 to 20 kW transmitters.

The antenna farm in Zeesen

And this is how the Polish transmitting site near Warszaw looks today. There are about 15 antennas.

StreetView makes it easier to see the antennas, the 'BRAMA WJAZDOWA' sign (keep the entrance free) on the gate is pixelated!

On the left the HV A transmitter, on the right the BND transmitter. As you see they are almost identical.The East Germans probably copied the design.

BND agents used two way shortwave communication last time in 1974.

A BND container with SP 15 (FSS-7) and 20 crystals

The CIA used also the FSS-7 in the GDR. The agent JADUR had thrown his device into the EMSTER canal near Berlin

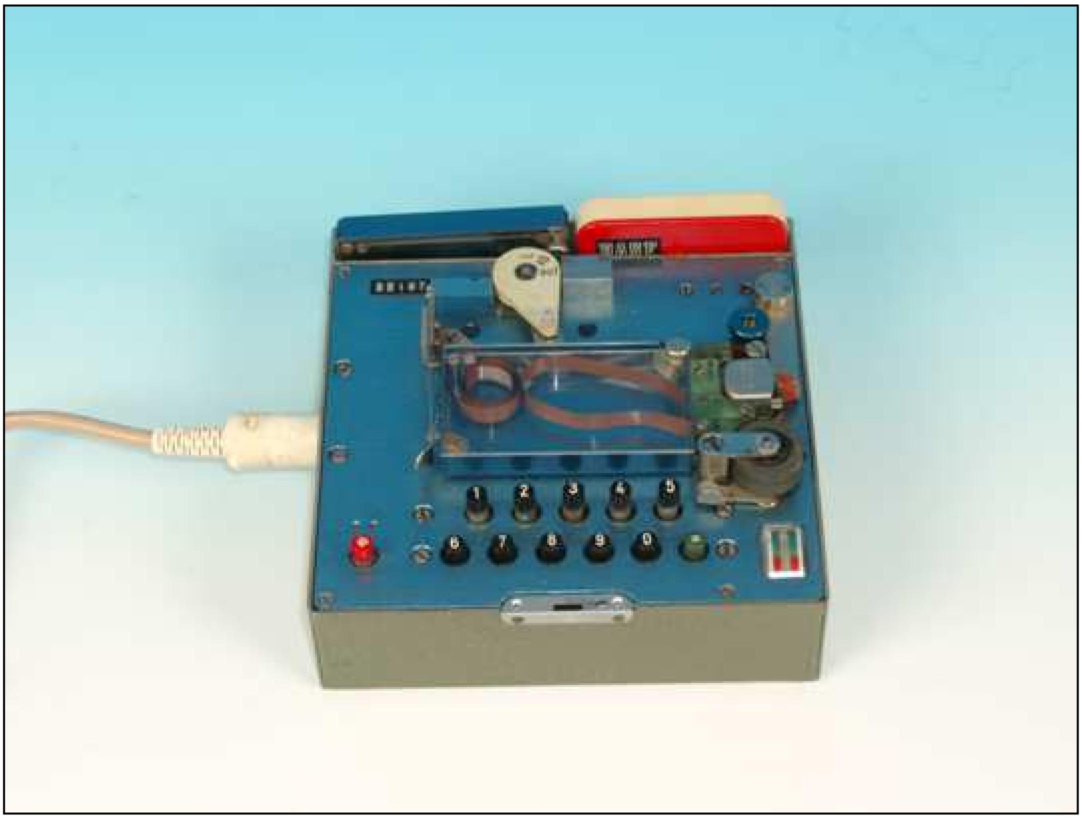
They used the KE 8 keyer adapted to the FSS-7

CIA gave JADUR 72 crystals!

At the end of the 1980s, the BND equipped its stay behind agents with a digital device FS 5000 (Harpoon) developed and manufactured by AEG Telefunken

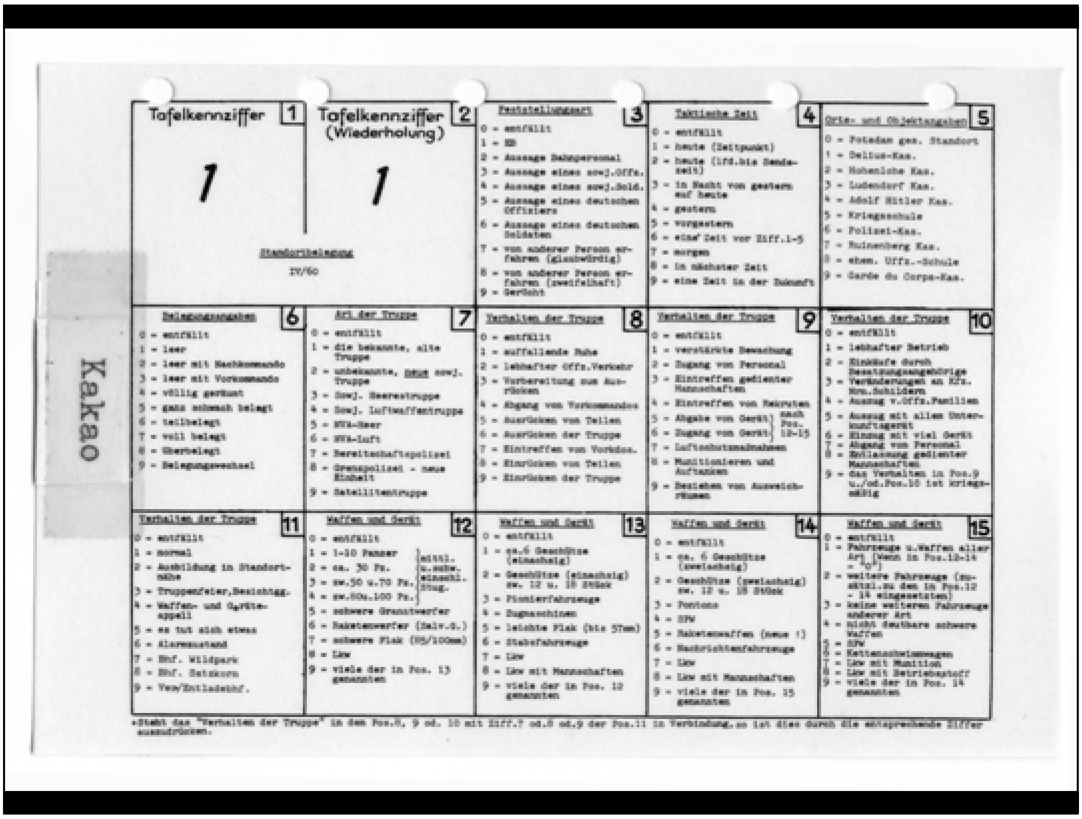
The 3WU was the first radio developed by the OG in 1947. It was built in the USA. The name means 3 watts universal device, because it should look like a multimeter.

The successor 12 WG (12 Watt device) was built by the OG, not by Wandel & Goltermann.



To reduce the risk to be detected while transmitting, the agent used a burst encoder to reduce the transmission time. Here is a device of the HV A that allowed sending encrypted messages.

This BND burst encoder allows the transmission of 25 characters. What can be forwarded thereby?



Tafelkennziffer 1

1

Tafelkennziffer (Wiederholung) 2

1

Standortbelegung

IV/60

Feststellungsart 3
0 = entfällt
1 = EB
2 = Aussage Bahnpersonal
3 = Aussage eines sowj.Offz.
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 = eine Zeit vor Ziff.1-5
7 = morgen
8 = in nächster Zeit
9 = eine Zeit in der Zukunft

Orts- und Objektangaben 5
0 = Potsdam ges. Standort
1 = Delius-Kas.
2 = Hohenlohe Kas.
3 = Ludendorf Kas.
4 = Adolf Hitler Kas.
5 = Kriegsschule
6 = Polizei-Kas.
7 = Ruinenberg Kas.
8 = ehem. Uffz.-Schule
9 = Garde du Corps-Kas.

Belegungsangaben 6
0 = entfällt
1 = leer
2 = leer mit Nachkommando
3 = leer mit Vorkommando
4 = völlig geräumt
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 = Beziehen von Ausweichräumen

Verhalten der Truppe 10
0 = entfällt
1 = lebhafter Betrieb
2 = Einkäufe durch Besatzungsangehörige
3 = Veränderungen an Kfz. Nrn.Schildern
4 = Auszug v.Offz.Familien
5 = Auszug mit allem Unterkunftsgerät
6 = Eingang 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,Besichtgg.
4 = Waffen- und Gerätеappell
5 = es tut sich etwas
6 = Alarmzustand
7 = Bhf. Wildpark
8 = Bhf. Satzkorn
9 = Ver/Entladebhf.

Waffen und Gerät 12
0 = entfällt
1 = 1-10 Panzer
2 = ca. 30 Pz.
3 = zw.50 u.70 Pz.
4 = zw.80u.100 Pz.
mittl. u.schw. einschl. Sturmg.
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 (einachsig)
2 = Geschütze (einachsig) zw. 12 u. 18 Stück
3 = Pionierfahrzeuge
4 = Zugmaschinen
5 = leichte Flak (bis 57mm)
6 = Stabsfahrzeuge
7 = Lkw
8 = Lkw mit Mannschaften
9 = viele der in Pos. 12 genannten

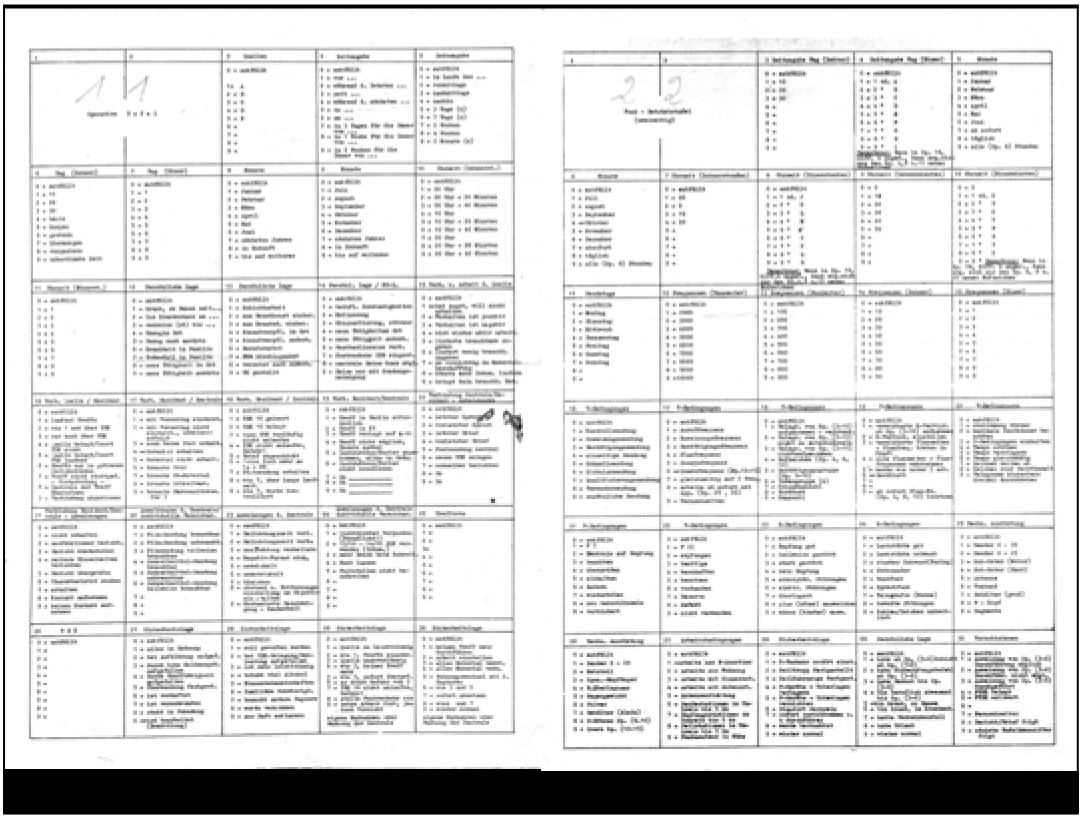
Waffen und Gerät 14
0 = entfällt
1 = ca. 6 Geschütze (zweiachsig)
2 = Geschütze (zweiachsig) zw. 12 u. 18 Stück
3 = Pontons
4 = SPW
5 = Raketenwaffen (neue !)
6 = Nachrichtenfahrzeuge
7 = Lkw
8 = Lkw mit Mannschaften
9 = viele der in Pos. 15 genannten

Waffen und Gerät 15
0 = entfällt
1 = Fahrzeuge u.Waffen aller Art (wenn in Pos.12-14 = "0")
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.

A complete review of the situation, there were several such panels to the needs of the agent adapted.

In 1960 the BND asked for information about the “Adolf-Hitler-Kaserne”



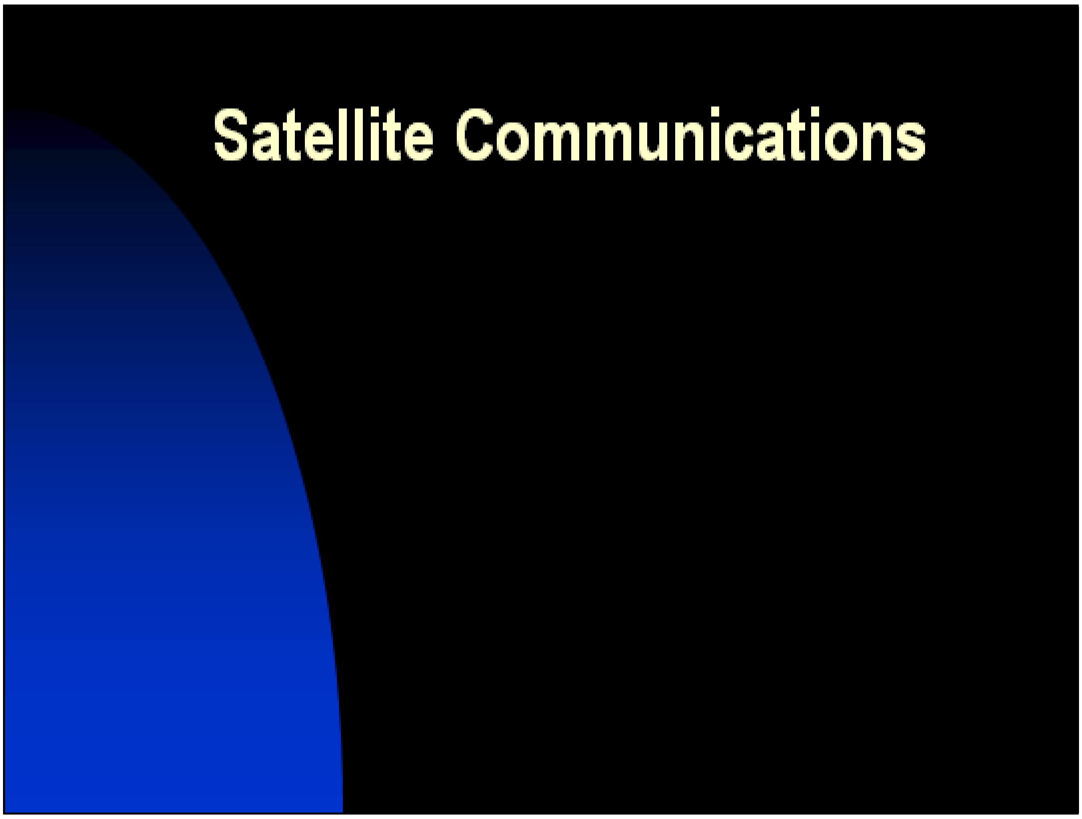
These are the rare panels for a resident

The East Germans were very inventive: Here is an Antenna made out of two umbrellas.

There was a VHF communication system 'Horizont', which was limited to about 100…150 km from the GDR border. Here you can see the successor system that didn't come into use. On the left is one of the „first laptops" for input to the transmitter, in the middle the transmitter, on the right the receiver.

Around 17 East German agents had been given the previous model – but none have ever been found.

One of the receiving antennas was on the Brocken – a high mountain near the border to West Germany.



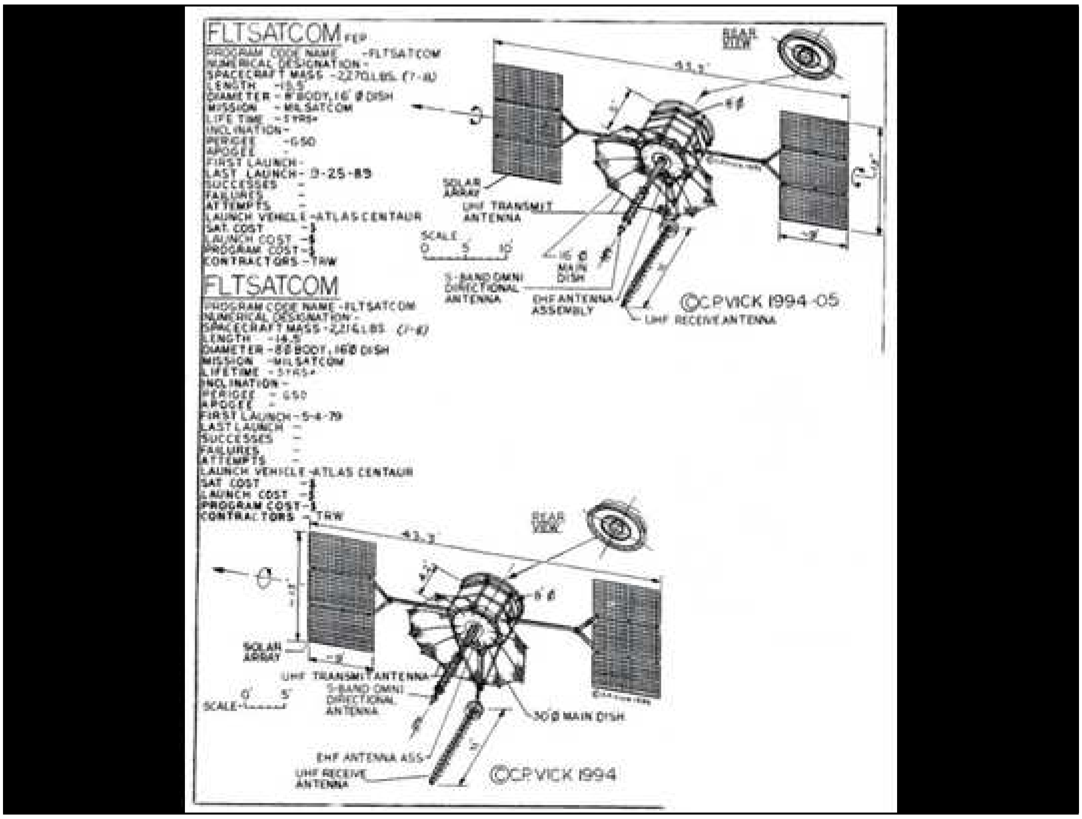
Satellite Communications began in the 1980s.

The KGB seized this American satellite transceiver in 1983 in Moscow from a diplomat. Today satellite communications have almost replaced shortwave communications.

(A KGB photo: The image shows the RT-804 transceiver unit, the CK-42 coder, the BS-804=A battery

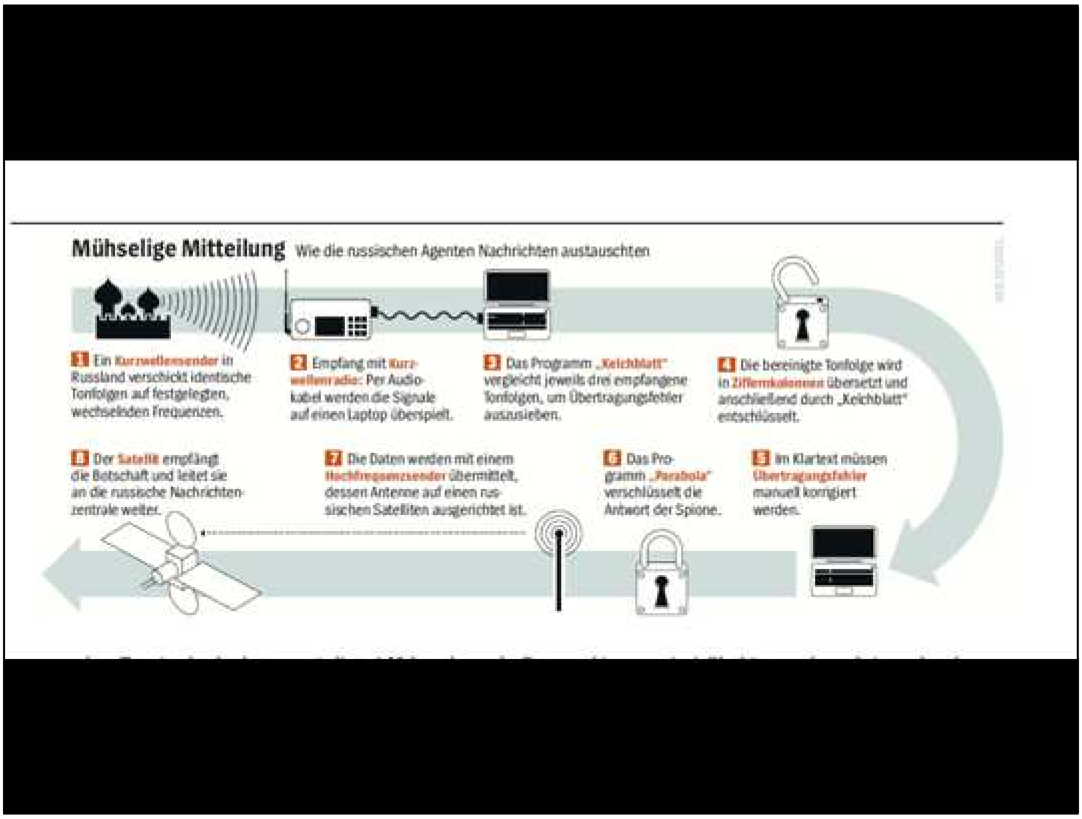
pack and power supply with the CPK-804=A remote control). The station operated on 311 MHz, the detection project had the code name “Pyramid”.

The photo comes from BStU MfS HA II Nr. 44310



The American Fleet Sat Com satellites were used to transmit the information sent by buried American probes. The British used S-band probes, which have probably remained undetected, but French and Russians also used probes.

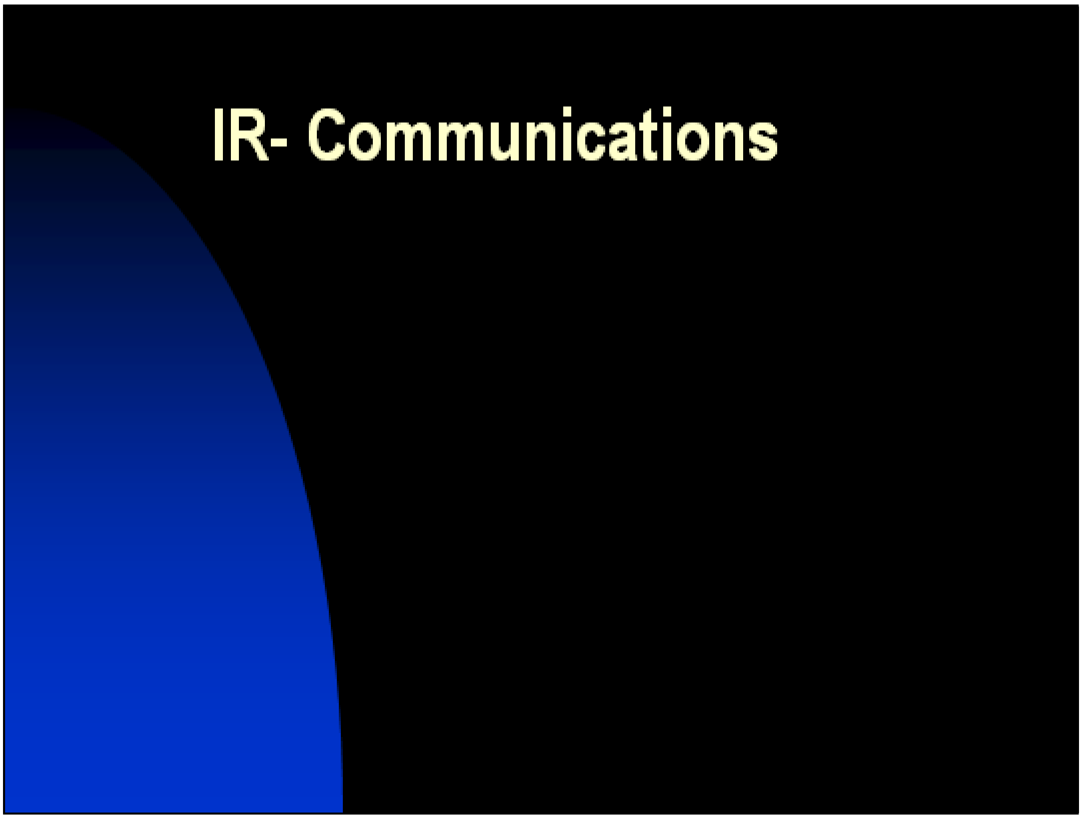
The HV A wanted to operate agent communication via these satellites, the OTS modified the horizon transmitters for this.



The SVR (Russian Foreign Intelligence Service) still uses Short Wave transmissions, but nowadays, instead of voice transmissions, only tonal signals are sent.

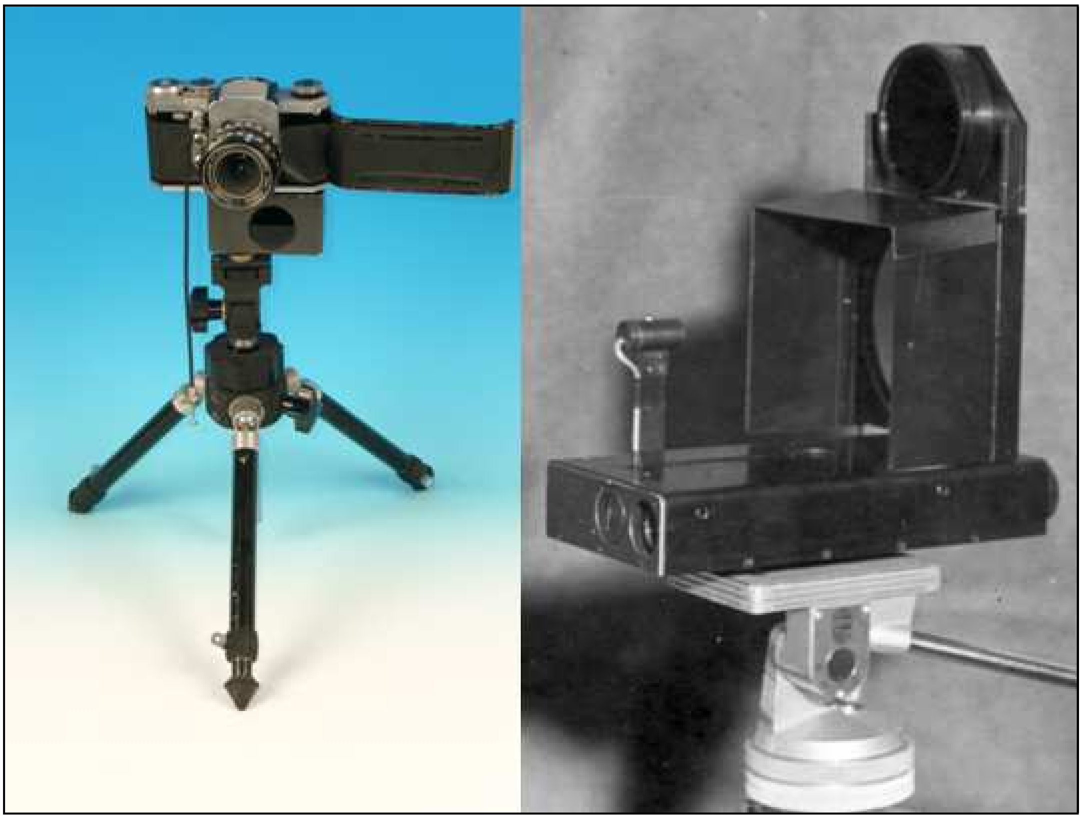
In October 2011 a married couple by the name of “Anschlag” was arrested. They were SVR spies getting their orders via tone transmissions on Short Wave and replying with a satellite transmitter hidden in a laptop case. By the way, the name “Anschlag” means “Attack” or “Strike” in German…!

Source: Der Spiegel



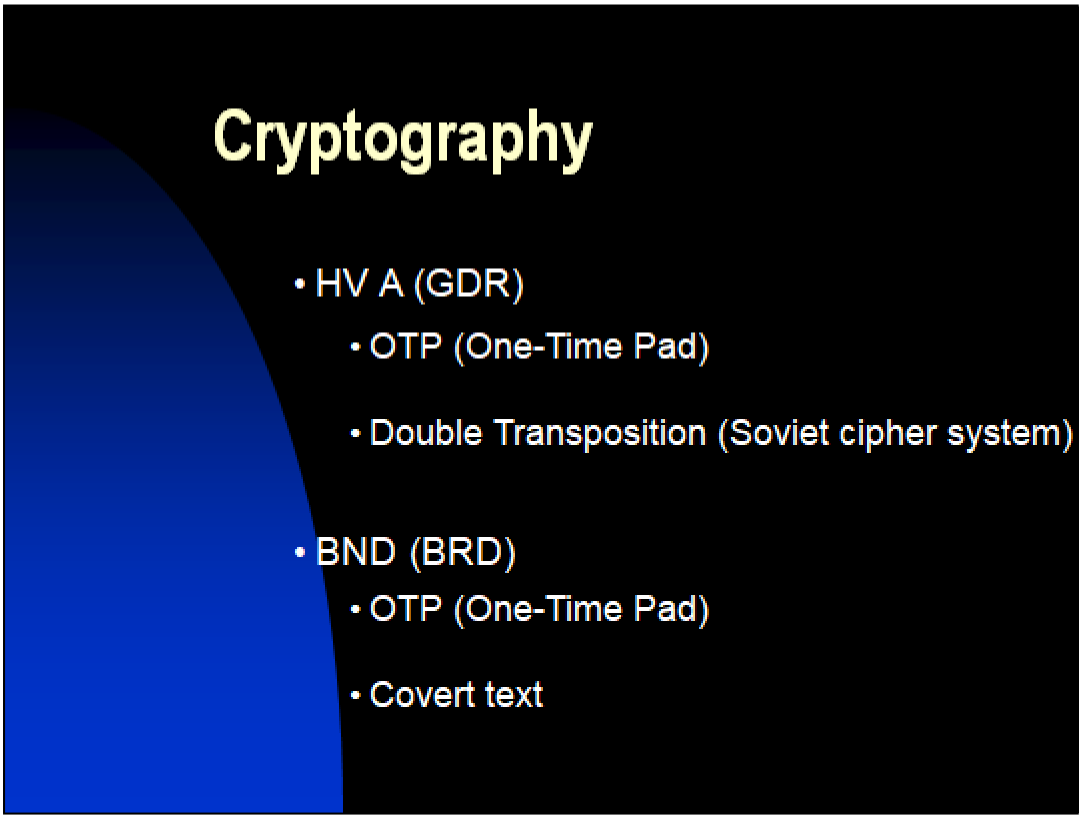
IR-Communications are a relatively secure type of communication. IR is light in a spectrum below visible light.

This is an American IR communication device (Communication Set XE-2) uncovered in 1959 in the possession of the US agent Gisela Gebhardt in East Berlin.

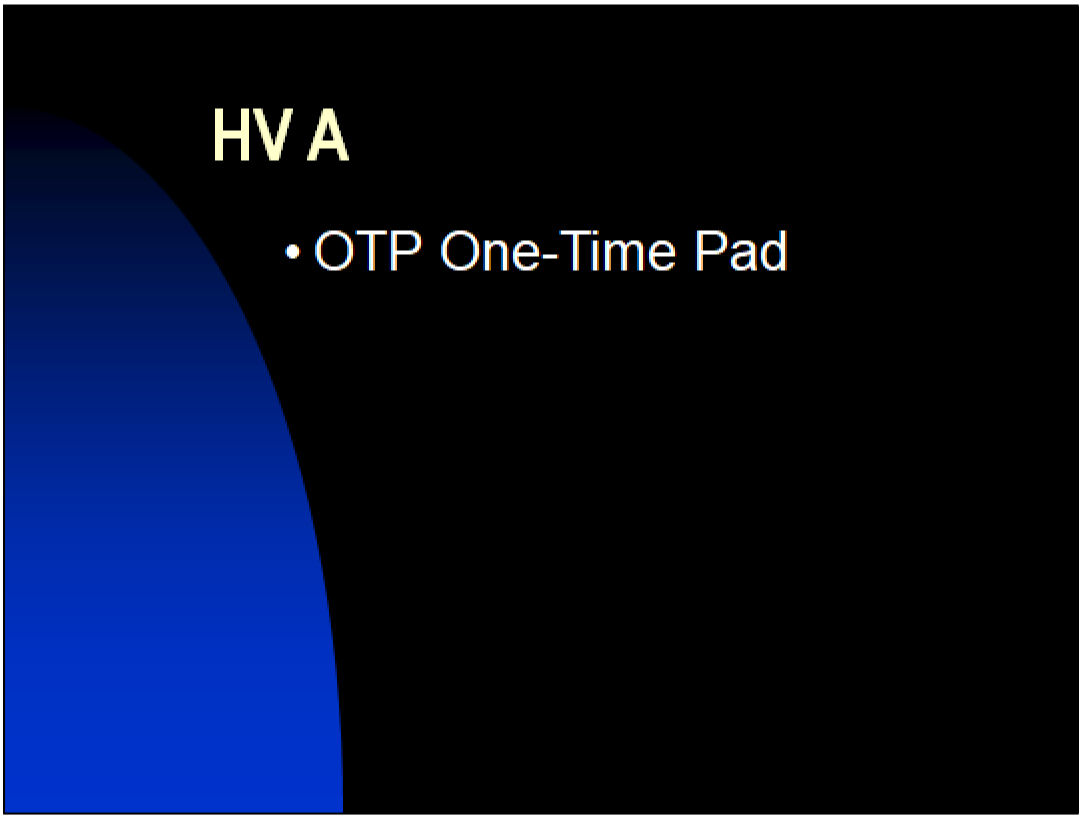


Based on this discovery the MfS began developing their own devices. The first MfS device was uncovered in 1963 in West-Berlin. The IR-transmitter is under the camera, the receiver is in the camera. The remote station was a Dahme, a replica of the American device

This is an overwiew of various IR devices of the MfS

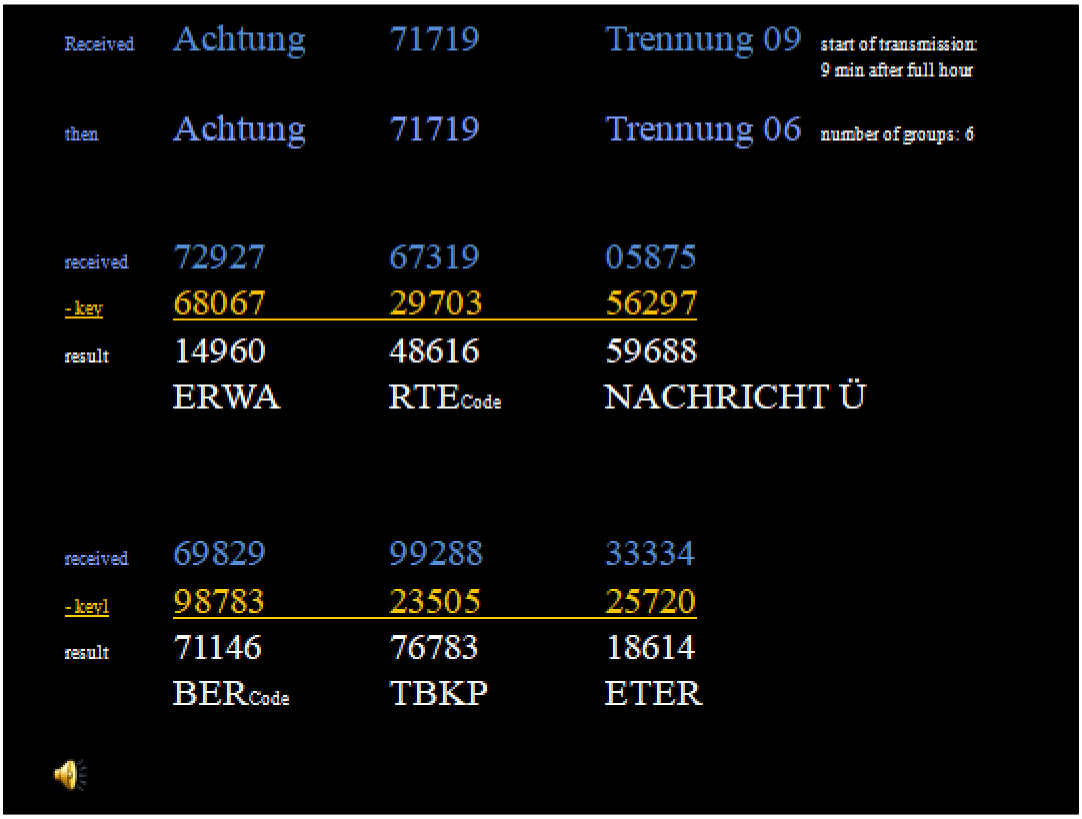


And now the second part of the presentation: Cryptography



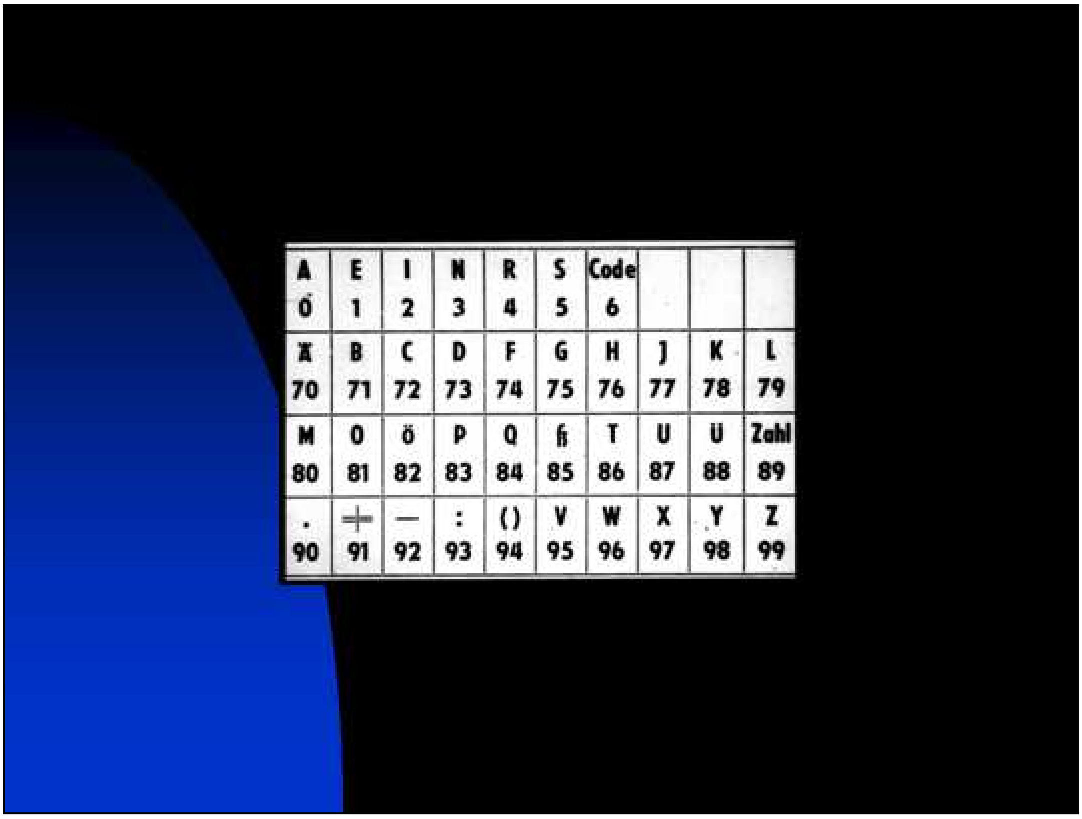
The HV A Hauptverwaltung Aufklärung was the Foreign Espionage Service of the GDR (East Germany) and used the OTP which I will now explain.

OTP is a safe encryption method if properly used, OTP (One Time Pad) means only once!



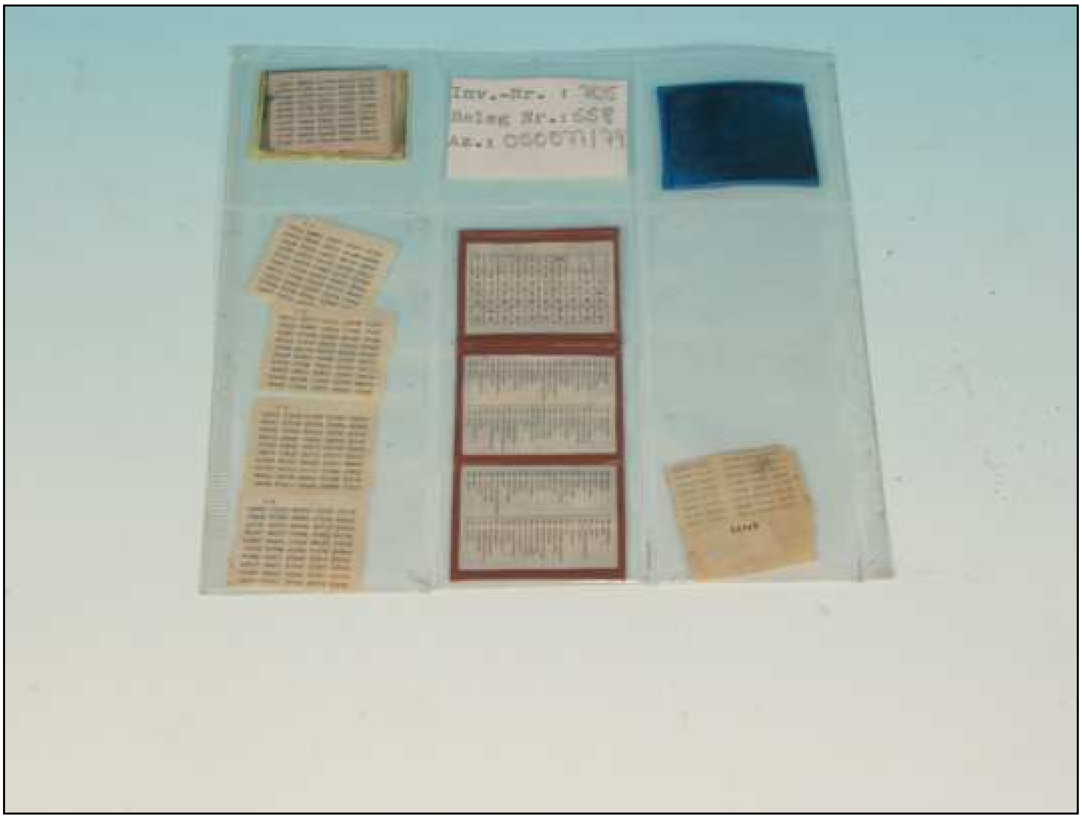
Blue is the message the agents receives, he substracts the yellow key from the OTP. The result is shown in white.

TBK (Toter Briefkasten) is a Dead Drop



A	E	I	N	R	S	Code			
0	1	2	3	4	5	6			
Ä	B	C	D	F	G	H	J	K	L
70	71	72	73	74	75	76	77	78	79
M	O	ö	P	Q	ß	T	U	Ü	Zahl
80	81	82	83	84	85	86	87	88	89
.	+	—	:	()	V	W	X	Y	Z
90	91	92	93	94	95	96	97	98	99

With this key he converted the numbers to letters.

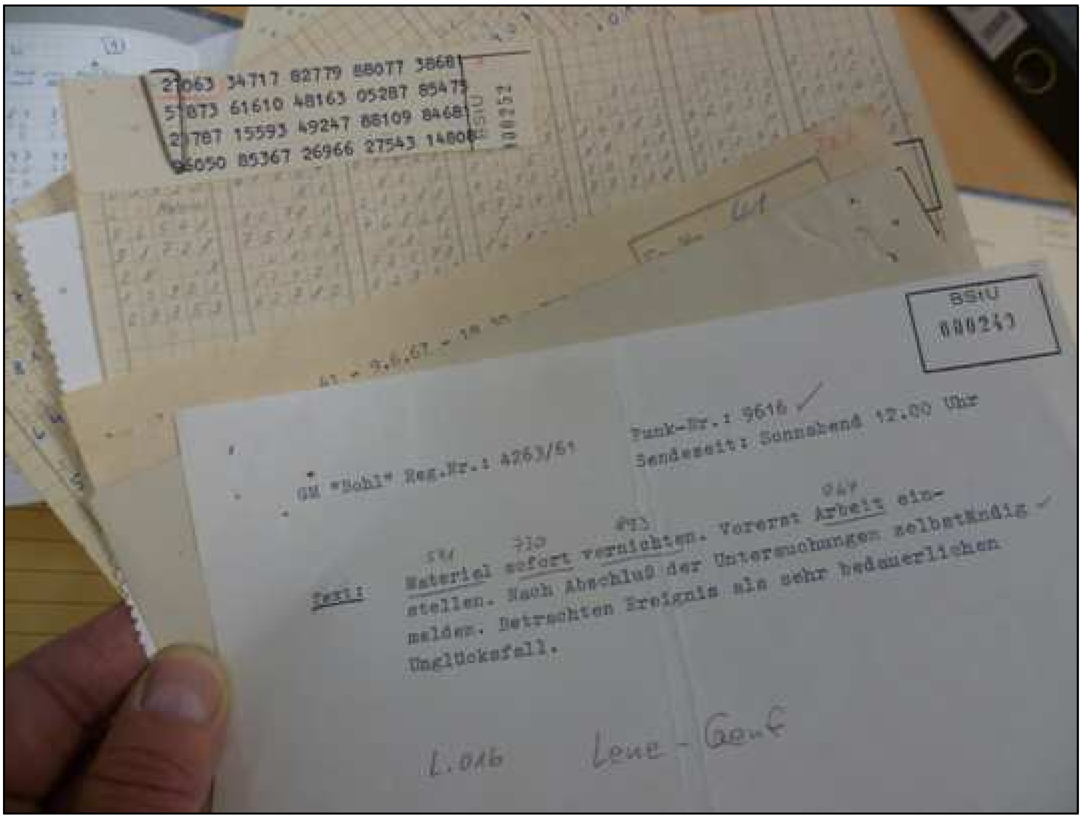


Here you see the actual documents that the East German agent had.

On the left the decryption OTPs, on the right the encryption OTPs, in the middle the key and the code book for 100 code words

The headquarters had similar documents as the agent. A sealed OTP for each individual agent.

It contains a copy of the agents OTP.

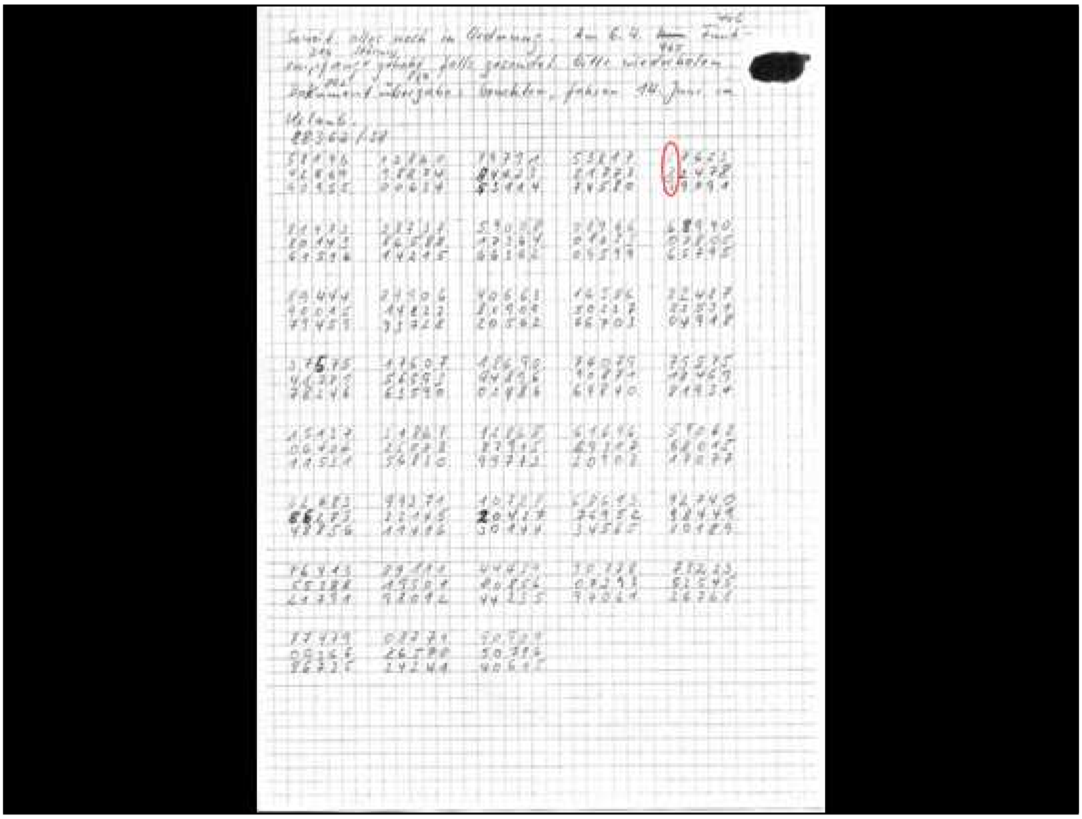


In the 1960 the messages were manually encoded in the HQ.

The agent behind the code name „Bohl“ is Karl-Heinz Kurras, the West Berlin policeman who shot the student Benno Ohnesorg in 1967. Only in 2009 was it discovered that he was a Stasi agent. The message shown here says that he is to destroy all material in his possession, discontinue work, report back after the end of the police investigation – and claim that the incident was just an unfortunate accident.

Strangely, the Stasi did not destroy the message or the OTP. Were they laying a false track?

Later the encryption was done electronically. The picture shows a T-307/3 device.



This page shows how an agent encrypted his message:

On the top the text,

And then step by step the encryption.

There is an intentional mistake in the 5th column. This a pre-arranged signal the agent is not exposed. If there is no mistake, this means that he has been discovered.

Double Transposition

(Soviet cipher system)

- Name: GRANIT E 160
- Description in http://scz.bplaced.net/index.html
- Was used by the HV A until 1958
- Was cracked by the West German „Verfassungsschutz“
- Led to exposure of Guillaume, a top agent and personal advisor of Chancellor Brandt

Double Transposition was a Soviet cipher system, used by the HV A until 1958. It was cracked by the West German

Verfassungsschutz = Office for the Protection of the Constitution and led to the exposure of Guillaume, a top agent and personal advisor of Chancellor 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	.	,

This system is based on a keyword which determines which number represents which letter. This is used for the initial conversion of text to numbers (substitution table)

Zs means numbers following

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

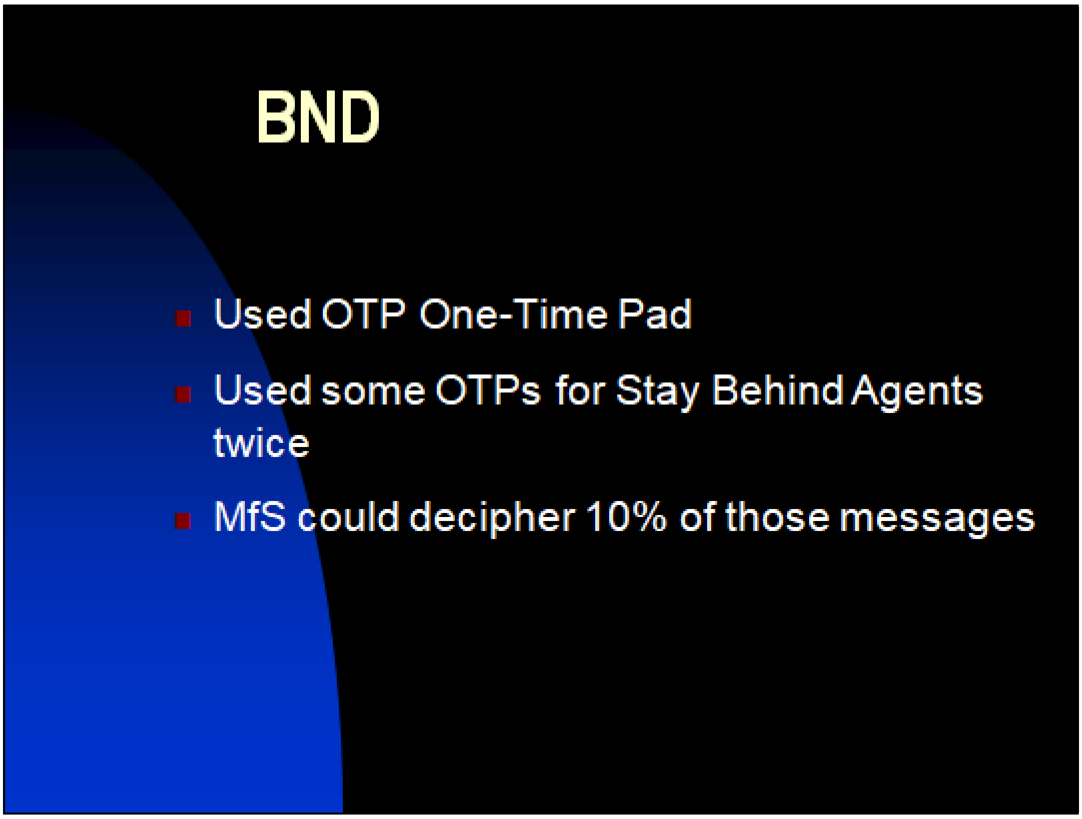
Text
WIR MELDEN UNS NACH FUENFUNDZWANZIGJAEHRIGEM EINSATZ ZURUECK ABCDEF
Ciphertext
DEEUNMIWLRFUCNEASNHNANZIZDUFWNIGHMEEJGRAZZ ARUSIETNCDAFEKEUBC

Example for a transposition with letters: We report back after 25 years in operation...

This example uses letters instead of numbers, and is only scrambled once.

The text is written below the key phrase. Then the key phrase with the columns is sorted in alphabetic order.

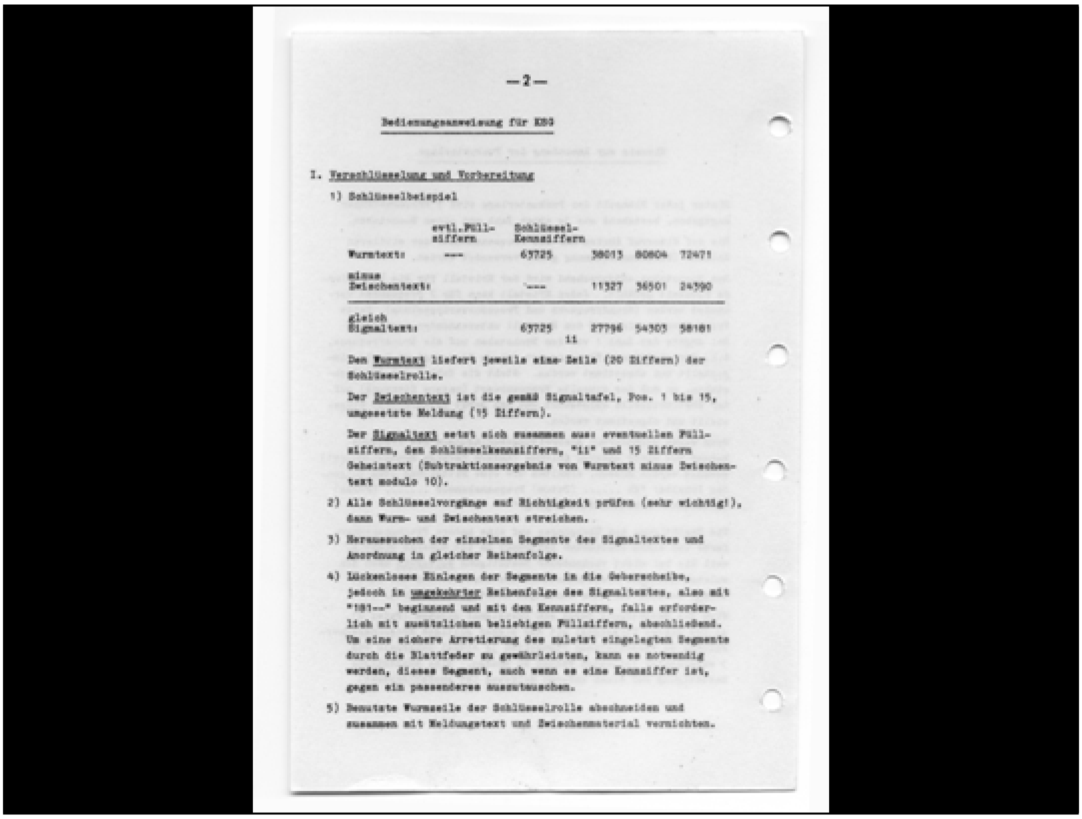
Guillaume received a note by radio transmission for his birthday and the birth of his son. The West German “Verfassungsschutz” intercepted the message and only years later was able to decipher it.



The BND (West German Foreign Intelligence Service) also used OTP.

	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	.	,

This is the BND key to convert numbers to letters (substitution table).



—2—

Bedienungsanweisung für KBG

I. Verschlüsselung und Vorbereitung

1) Schlüsselbeispiel

	evtl. Füllziffern	Schlüssel-Kennziffern			
Wurmtext:	---	63725	38013	80804	72471
minus Zwischentext:		---	11327	36501	24390
gleich Signaltext:		63725	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.

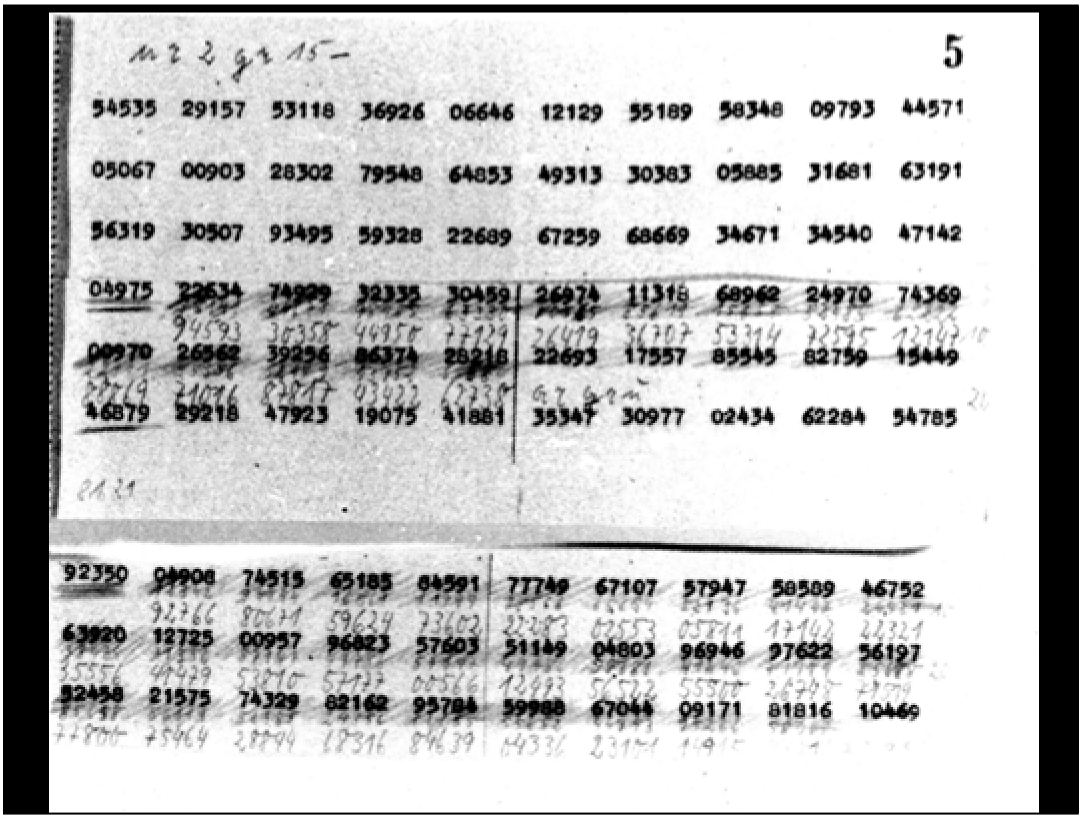
3) Heraussuchen der einzelnen Segmente des Signaltextes und Anordnung in gleicher Reihenfolge.

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.

This BND instruction shows how to use the OTP. The agent subtracted the numbers from OTP.

There is a slight difference between the East and West German use: In East Germany they added and subtracted the numbers on the OTP; in West Germany they subtracted twice from the OTP.



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
52458	21575	74329	82162	95784	59988	67044	09171	81816	10469

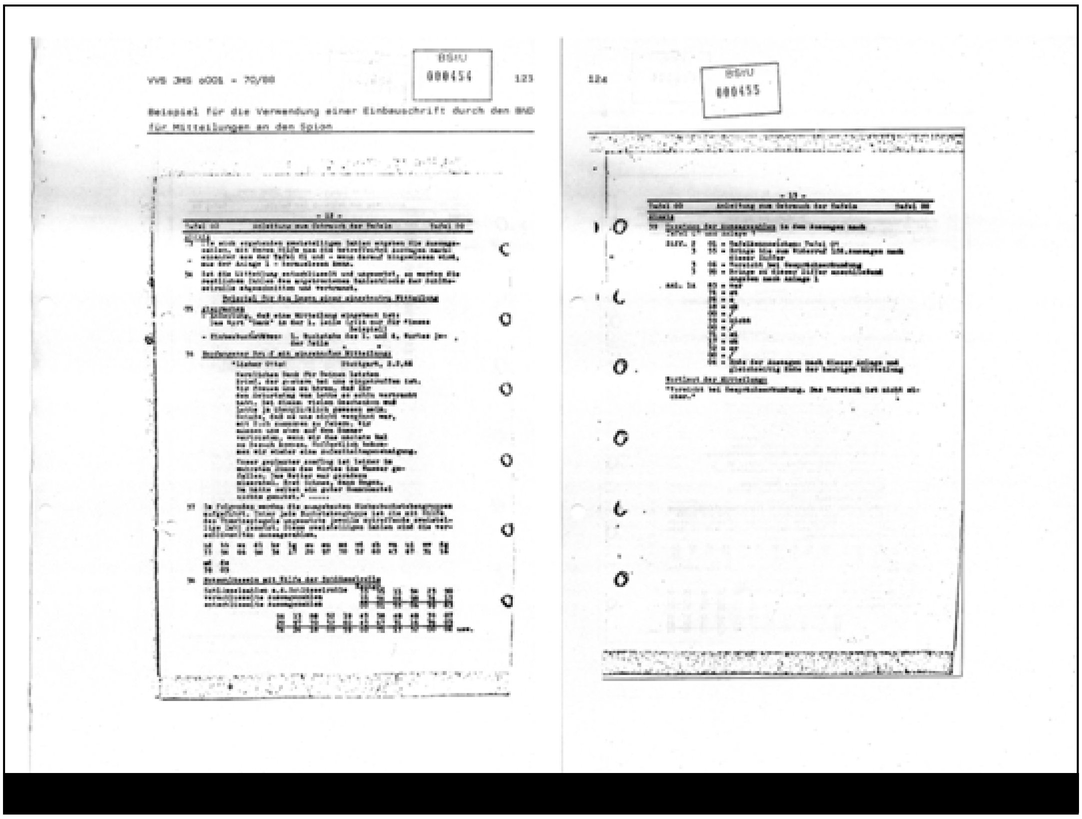
Here the agent decrypted two radio messages. The first is: Next on the January 30th at 10:15 pm. Greetings

Second saying: ZELOT wishes you all a happy 1956. Next on January 8th at 3:00 pm. Greetings

Covert Text

Used by BND in the 1960s

In German: „Einbauschrift“



VVS JHS o001 - 70/88

BStU 000454

123

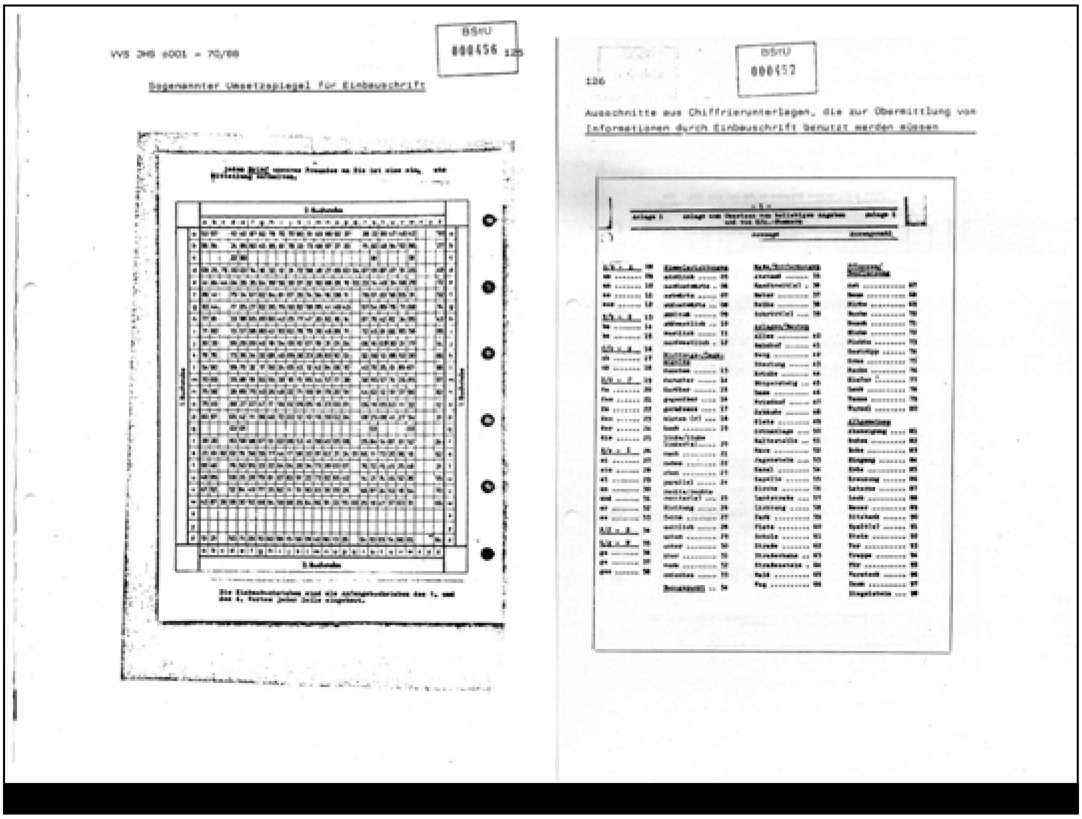
Beispiel für die Verwendung einer Einbauschrift durch den BND für Mitteilungen an den Spion

124

BStU 000455

„Covert Text“ is a previously relatively unknown method for encrypted communications. In a text the first letter of the first and fourth word of each line is converted into a two-digit number by the recipient with the help of a key table. These numbers were subtracted from the key numbers on the OTP.

The key table and the meaning of the results we‘ll see on the next slide.



On the left the keytable, on the right the meaning of the numbers.

A simplified example (without the use of an OTP) we‘ll see on the following slide.

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.

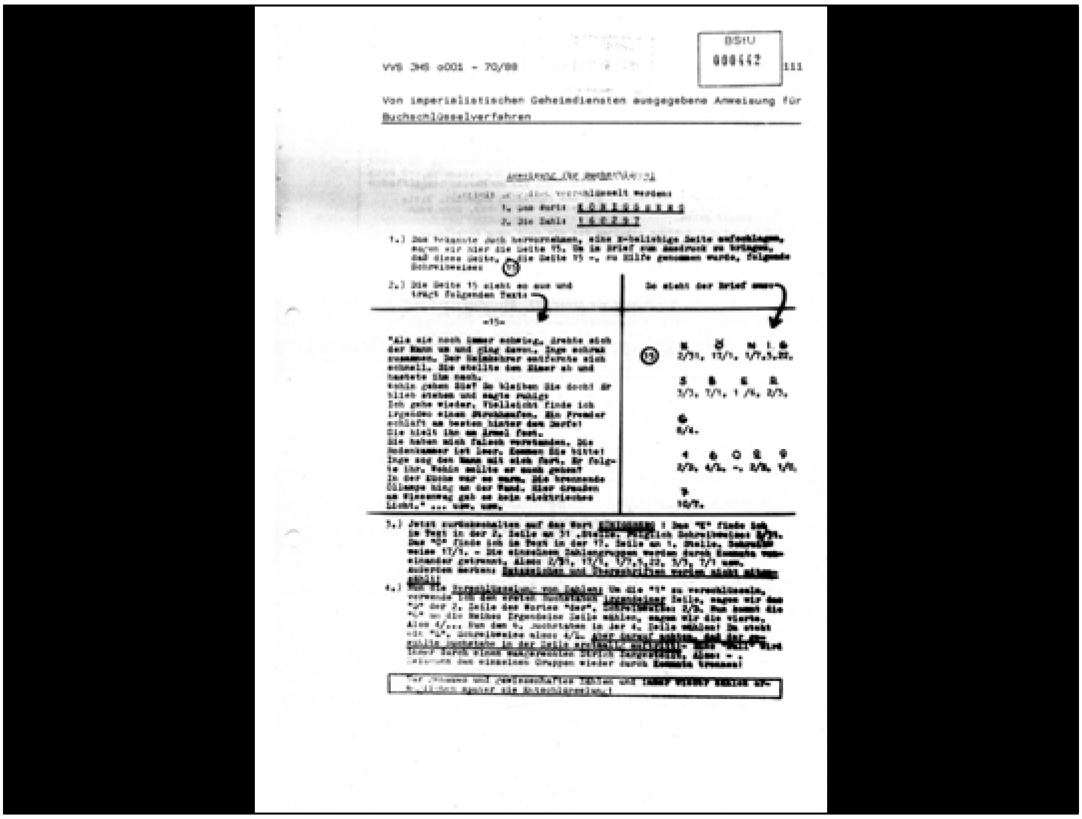
ls = 76 = Hecke (hedge)
fw = 31 = über (over)
fs = 57 = Landstraße (country road)
lf = 32 = vorn (ahead)
st = 73 = Fichte (...)
mt = 57 = ...
fh = 84 ...
sa = ...

An example I created using the obituary for Leonard Nimoy, who played Dr. Spock, without the use of an OTP.

Book key

Probably used by BND in the 1960s

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



VVS JHS o001 - 70/88

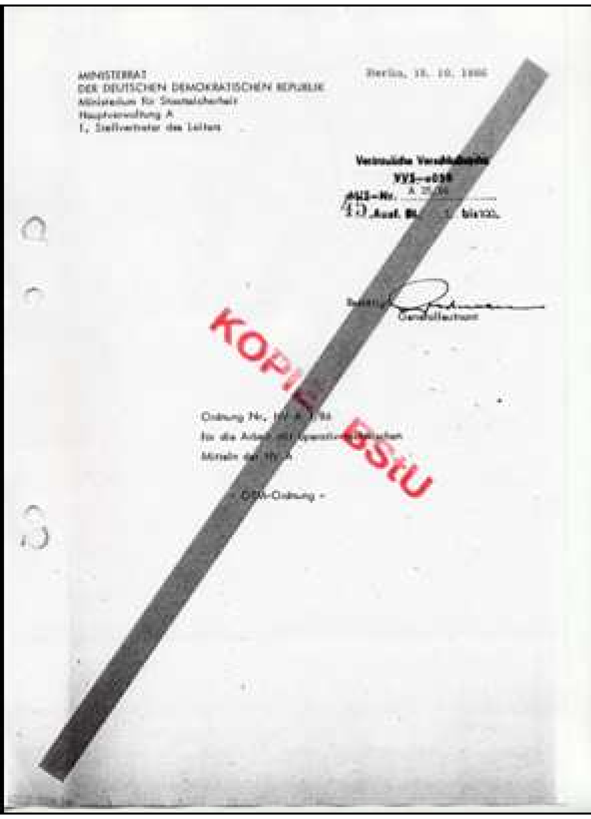
BStU 000442

111

Von imperialistischen Geheimdiensten ausgegebene Anweisung für Buchschlüsselverfahren

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

I end my presentation with another picture of clandestine communications. The lynx is transmitting a message to the headquarters that he is looking for a new agent.



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

Berlin, 18. 10. 1986

Vertrauliche Verschlußsache
VVS-o038
MfS-Nr. A 25/86
45 **. Ausf. Bl.** 1 **bis** 100.

Bestätigt:
Generalleutnant

Ordnung Nr. HV A 1/86
für die Arbeit mit operativ-technischen
Mitteln der HV A

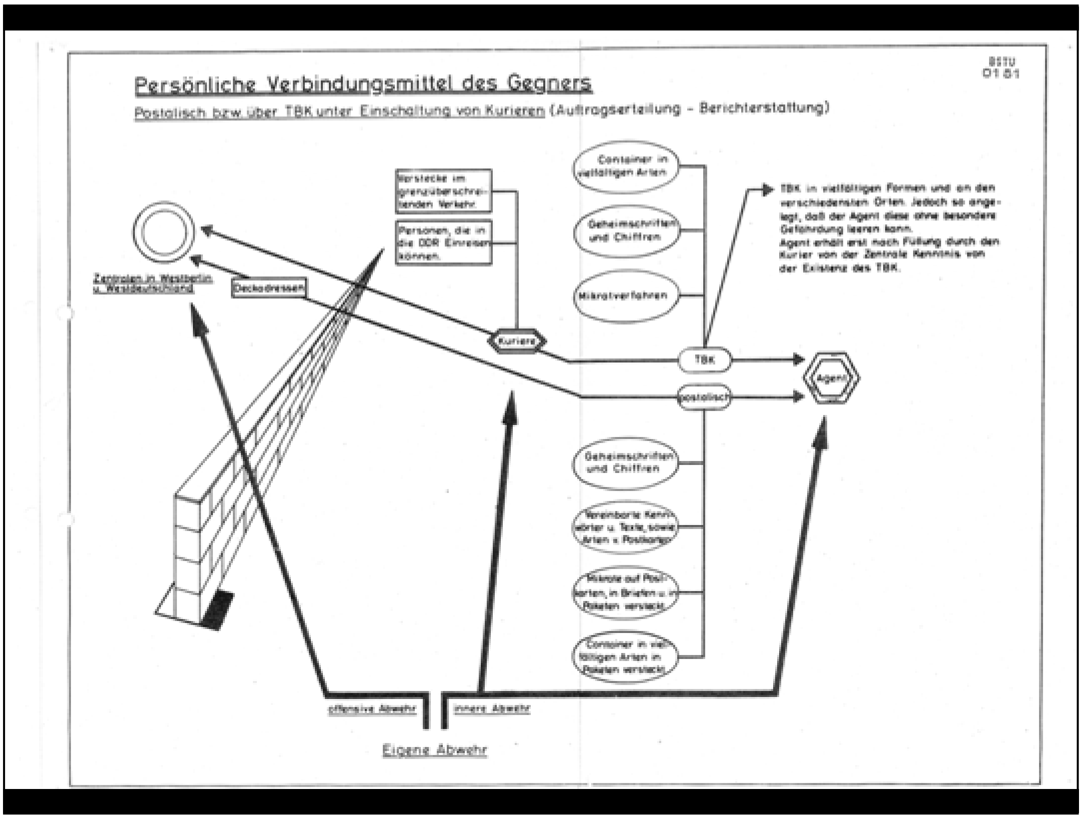
- OTM-Ordnung -

Tabelle 6/6: Verbindungsmittel (schließt Mehrfachnennungen ein)

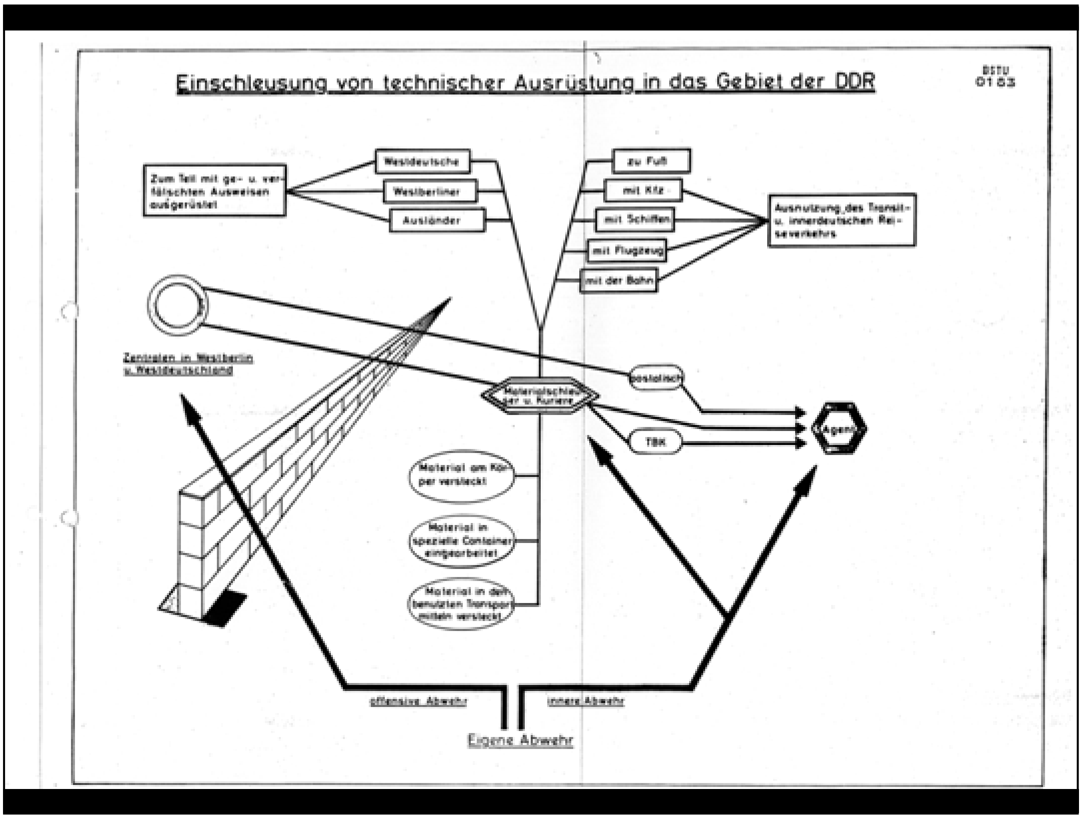
Verbindungsmittel	Anzahl
Deckadresse in der DDR	984
Instrukteurverbindung	786
Einseitiger KW-Funk	221
Chiffre	189
Geheimschreibmittel	148
Code	74
Persönliche Kurierverbindung	59
UKW-Signalsystem »Panorama«	43
Toter Briefkasten im Zug	42
Mikratfotografie	41
Toter Briefkasten	26
Verbindungsmittel »HD«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

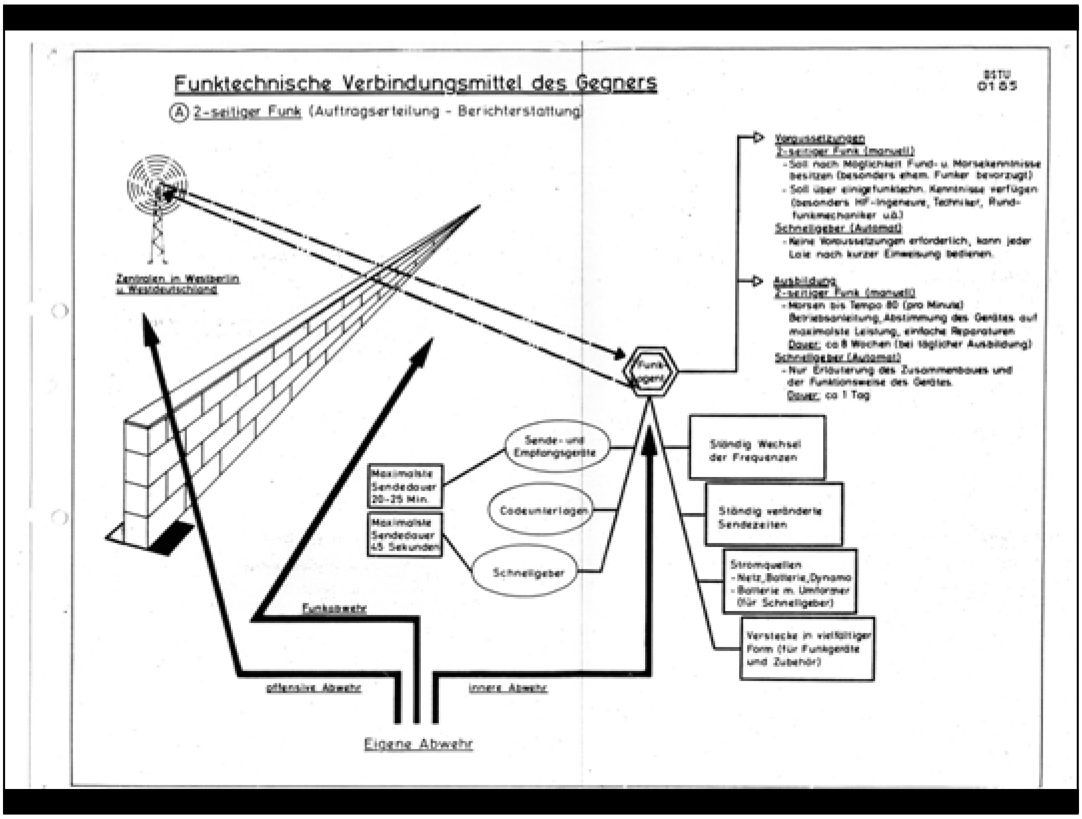
Communication system	Quantity
Cover address in the GDR	984
Instructor contact	786
One Way Shortwave Link	221
Chiffre	189
Secret Writing	148
Code	74
Personal Courier Contact	59
VHF-Signalling System »Panorama«	43
Dead Drop in Trains	42
Mikratphotography	41
Dead Drop	26
Telephone System »HD«	21
VHF-System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

(multiple mentions possible)

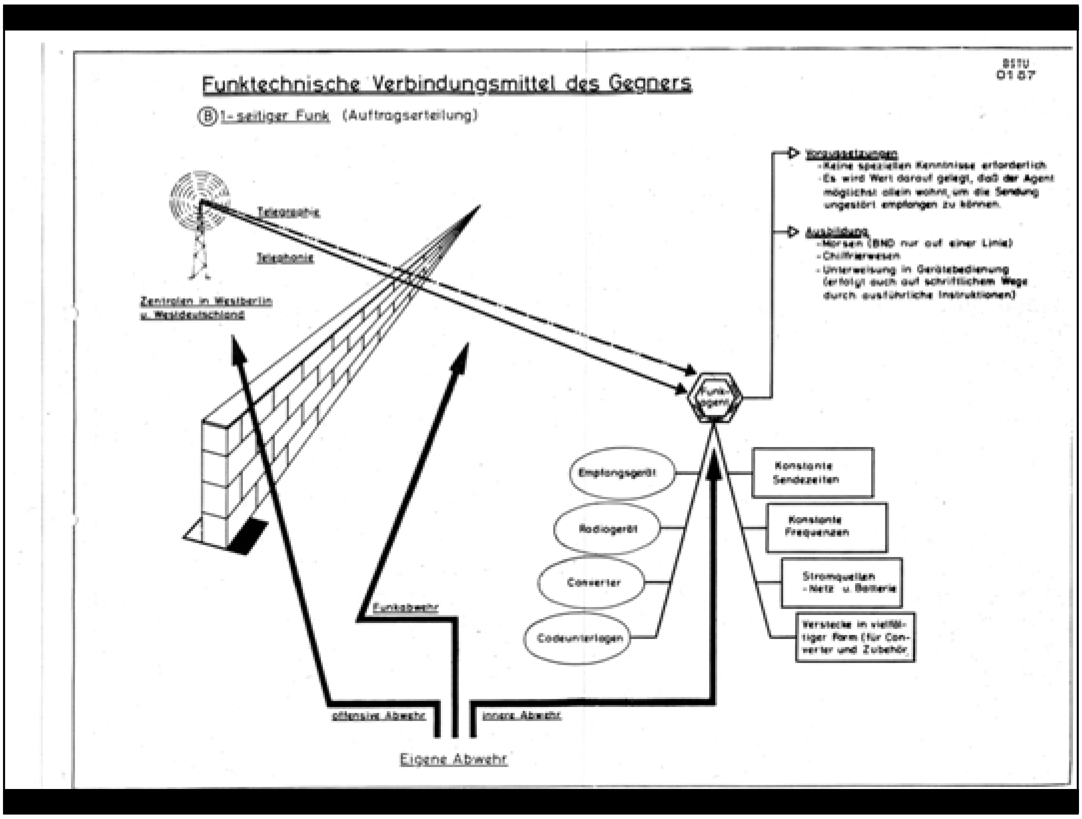


BSTU
01 81
Persönliche Verbindungsmittel des Gegners
Postalisch bzw. über TBK unter Einschaltung von Kurieren (Auftragserteilung - Berichterstattung)
Zentralen in Westberlin u. Westdeutschland
Deckadressen
Verstecke im grenzüberschreitenden Verkehr.
Personen, die in die DDR Einreisen können.
Kuriere
Container in vielfältigen Arten
Geheimschriften und Chiffren
Mikratverfahren
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.
TBK
postalisch
Agent
Geheimschriften und Chiffren
Vereinbarte Kennwörter u. Texte, sowie Arten v. Postkarten
Mikrate auf Postkarten, in Briefen u. in Paketen versteckt
Container in vielfältigen Arten in Paketen versteckt
offensive Abwehr
innere Abwehr
Eigene Abwehr

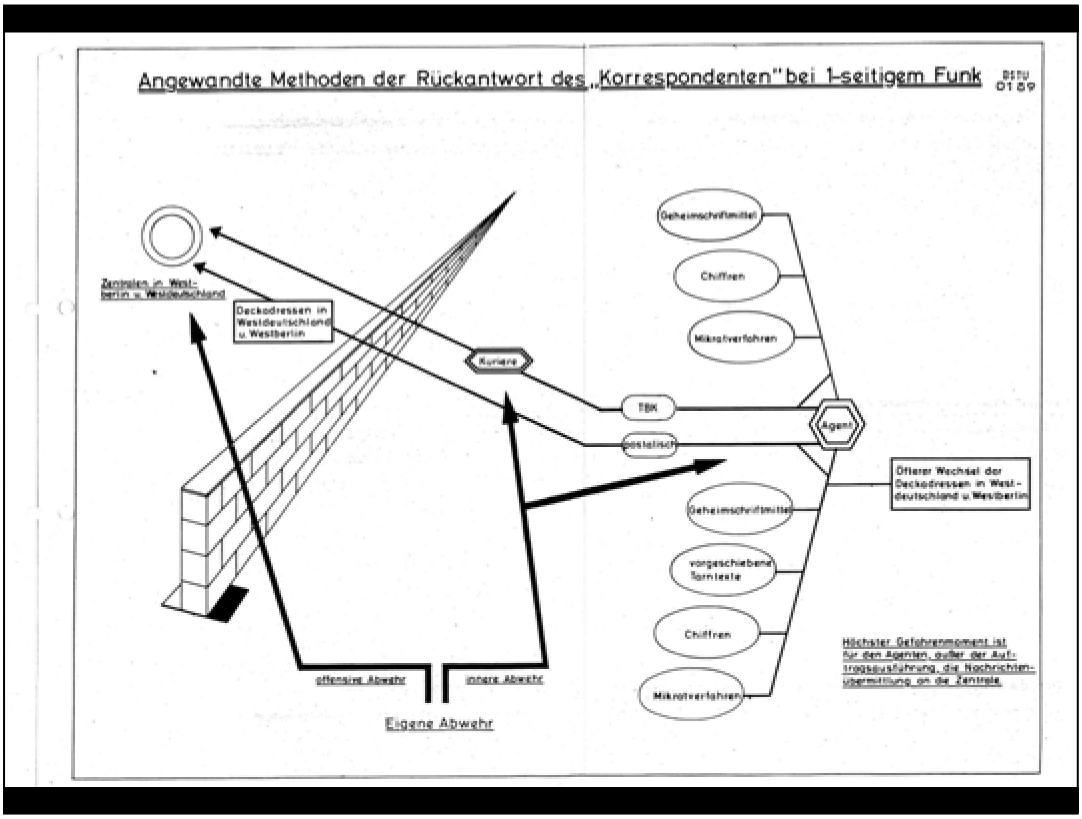

Einschleusung von technischer Ausrüstung in das Gebiet der DDR
BSTU
0183
Zum Teil mit ge- u. verfälschten Ausweisen ausgerüstet
Westdeutsche
Westberliner
Ausländer
zu Fuß
mit Kfz
mit Schiffen
mit Flugzeug
mit der Bahn
Ausnutzung des Transit- u. innerdeutschen Reiseverkehrs
Zentralen in Westberlin u. 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
(A) 2-seitiger Funk (Auftragserteilung - Berichterstattung)
BSTU
0185
Zentralen in Westberlin
u. Westdeutschland
Funk-
agent
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 veränderte 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
0187
Funktechnische Verbindungsmittel des Gegners
(B) 1-seitiger Funk (Auftragserteilung)
Telegraphie
Telephonie
Zentralen in Westberlin u. Westdeutschland
Vorraussetzungen
- Keine speziellen Kenntnisse erforderlich
- Es wird Wert darauf gelegt, daß der Agent möglichst allein wohnt, um die Sendung ungestört empfangen zu können.
Ausbildung
- Morsen (BND nur auf einer Linie)
- Chiffrierwesen
- Unterweisung in Gerätebedienung (erfolgt auch auf schriftlichem Wege durch ausführliche Instruktionen)
Funkagent
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
0189
Zentralen in West-
berlin u. Westdeutschland
Deckadressen in
Westdeutschland
u. Westberlin
Kuriere
TBK
postalisch
Agent
Geheimschriftmittel
Chiffren
Mikratverfahren
Öfterer Wechsel der
Deckadressen in West-
deutschland u. Westberlin
Geheimschriftmittel
vorgeschiebene
Tarntexte
Chiffren
Mikratverfahren
Höchster Gefahrenmoment ist
für den Agenten, außer der Auf-
tragsausführung, die Nachrichten-
übermittlung an die Zentrale.
offensive Abwehr
innere Abwehr
Eigene Abwehr

This is a very old shortwave transmitter with burst encoder using a punched tape

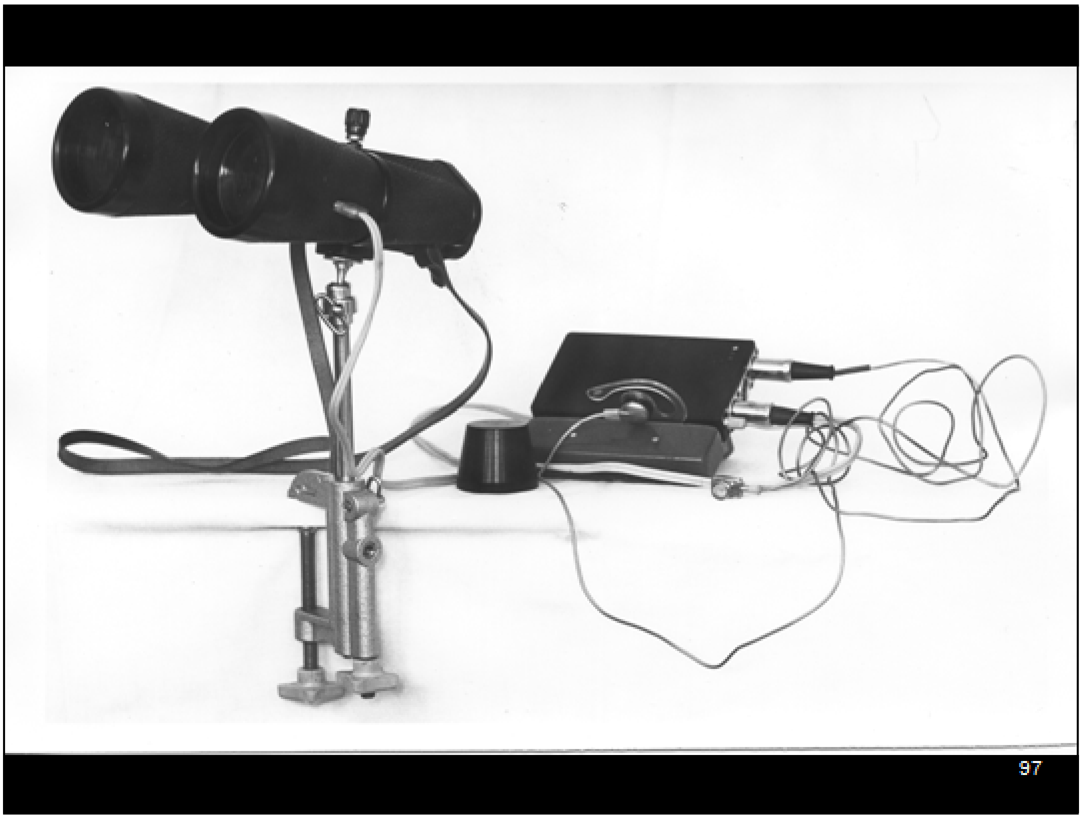
A next generation transmitter for HV A agents. On the left a burst encoder to pack the data and shorten the transmission. In the middle the transmitter, on the right the power supply.

HV A agent‘s transmitter WSA 1
Long Range Transmitter 1

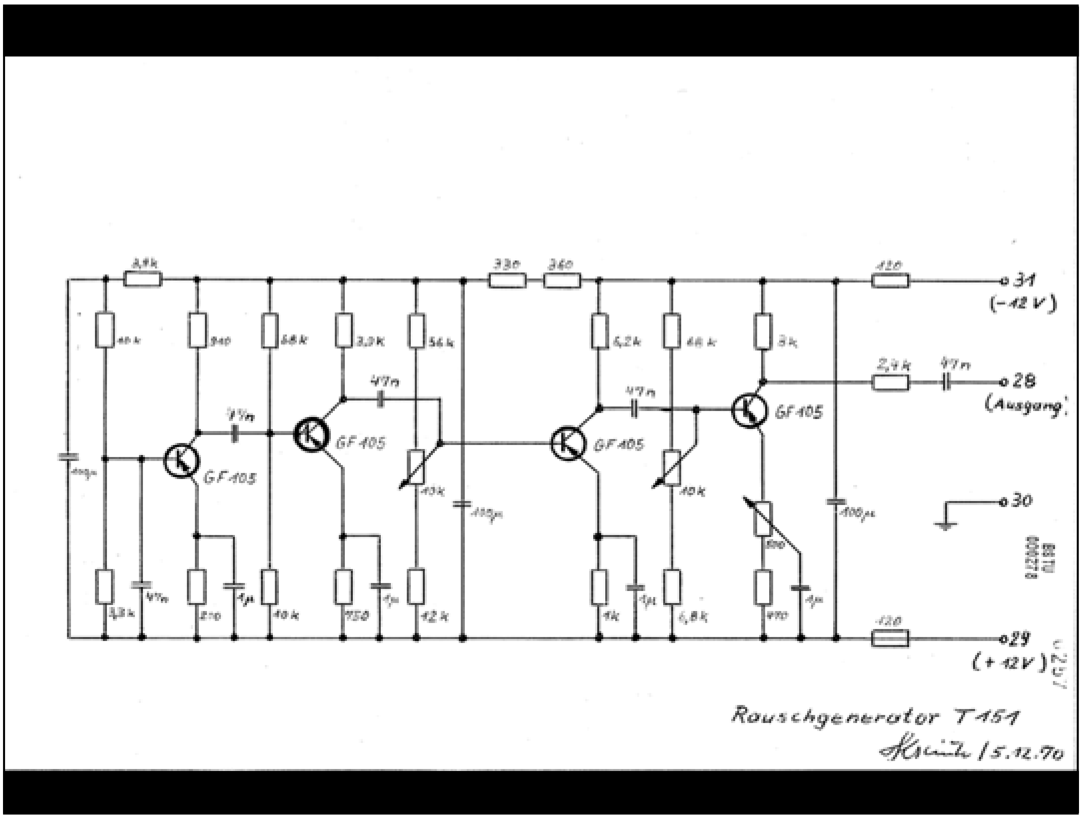
The last generation of HV A agent‘s transmitter WSA 6. It was never used.

The most recent generation of HV A transmitter. It uses a standard pocket calculator for input.

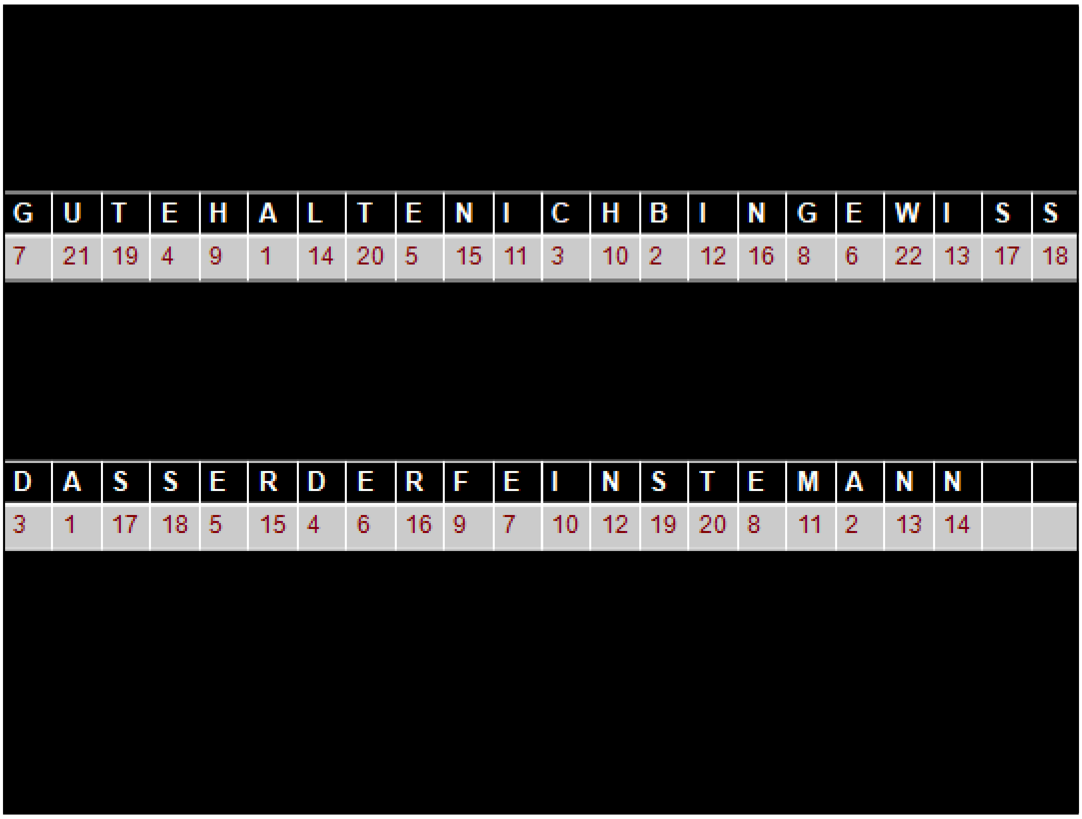
WSA 6 modular version, WSA Weitverkehrssendeanlage = Long Range Transmitter



An IR communication device embedded in binoculars. This was exposed by an MfS defector and never became operational.



This diagram shows the circuit of a random-number generator.
The generator was used OTPs.
Five generators were used to produce punched tapes.



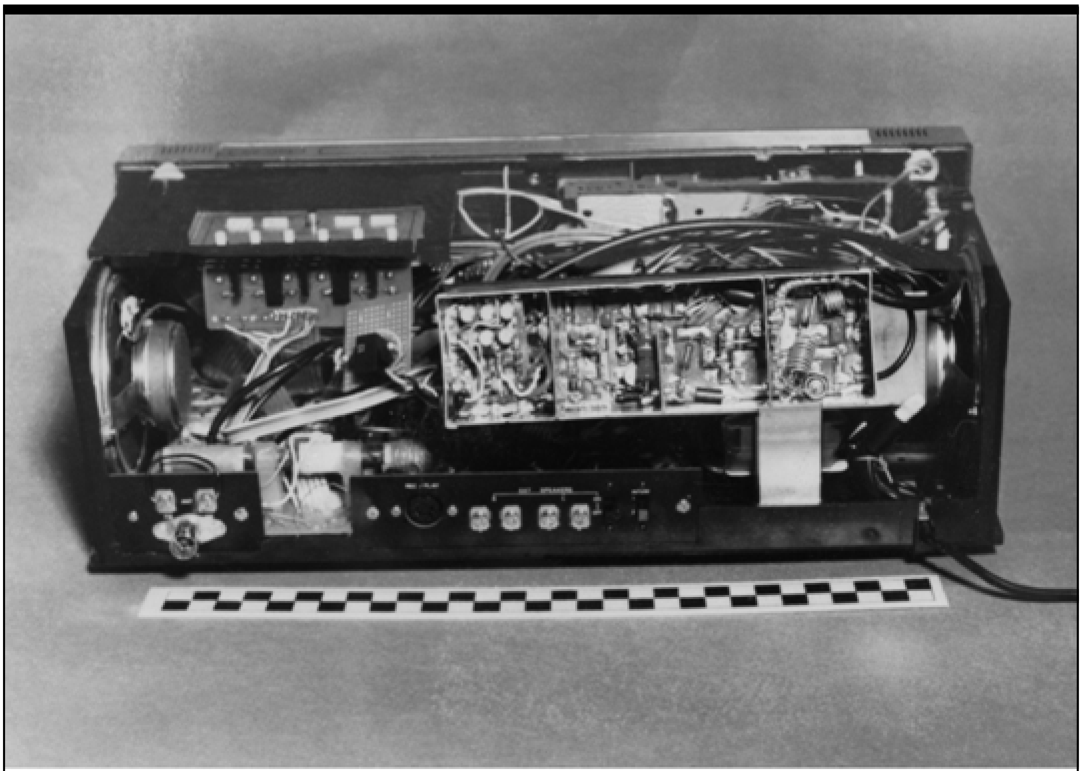
G	U	T	E	H	A	L	T	E	N	I	C	H	B	I	N	G	E	W	I	S	S
7	21	19	4	9	1	14	20	5	15	11	3	10	2	12	16	8	6	22	13	17	18

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		

Then two key phrases are used to scramble the numbers.

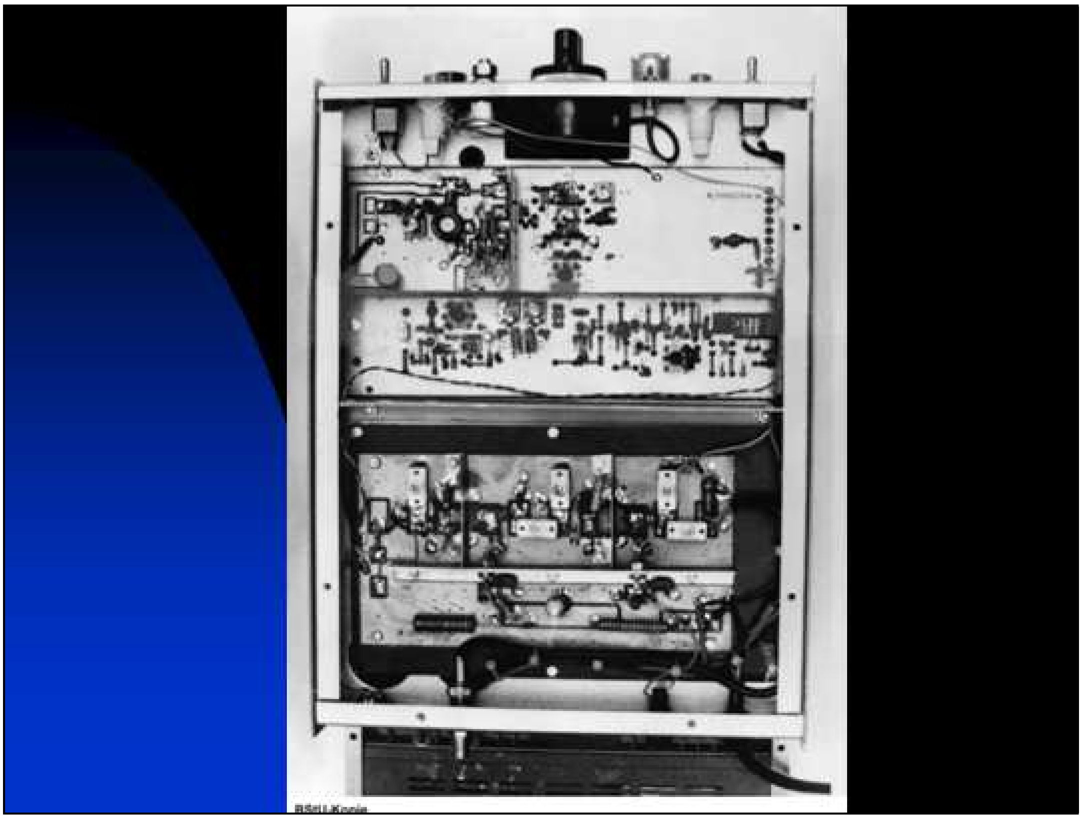
MfS found these devices with Western agents. There is no more information. Probably VHF-Transmitter


1
2



BStU-Kopie

This device has been found in Poland.



A sample of modern communication