Das Chiffrierwesen des Ministeriums für Staatssicherheit der DDR

Bernd Lippmann

Forschungs- und Gedenkstätte Normannenstraße
Ruschestraße 103
10365 Berlin

0 Vorbemerkungen

In einem Rückblick auf die fünfziger Jahre vermerkt einer der bekanntesten Funktionäre des MfS, daß man ein sowjetisches Chiffriersystem verwendet habe, „…bis wir erfuhren, daß westliche Dienste es mittels EDV geknackt hatten und die Telegramme nicht nur dechiffrieren, sondern sogar noch Empfängern zuordnen konnten“.[1] Diese Aussage stammt aus einem der wenigen Dokumenten, die bisher zum Thema Chiffrierwesen des MfS veröffentlicht worden sind. Neben der Erwähnung des von ihr verwendeten Chiffrierverfahrens durch die Spionin Gabriele Gast finden sich in der Literatur ansonsten nur lapidare Hinweise darauf, daß es solche Einrichtungen in der DDR gab. Ein wenig erstaunlich scheint dies deswegen, weil inzwischen eine unübersehbare Menge von Veröffentlichungen über die DDR im allgemeinen und das MfS im besonderen erschienen ist. Viele Darstellungen darunter stammen von ehemaligen MfS-Leuten. Das Chiffrierthema findet sich darin kaum. Andererseits aber ist gerade die DDR in hohem Maße von Vorschriften zur Geheimhaltung der Kommunikation gekennzeichnet.

Das Chiffrierwesen der DDR war im Wesentlichen das Chiffrierwesen des MfS, also des Geheimdienstes. Einrichtungen des zivilen oder militärischen Chiffrierwesens in der DDR unterstanden der Anleitung und Kontrolle durch das MfS. Diese Einbettung in die Geheimdienststrukturen bezog sich sowohl auf die technischen Mittel als auch auf die Personen. Die Bezeichnung Zentrales Chiffrierorgan (ZCO) für die Abteilung XI des MfS diente der Verschleierung dieses Zusammenhanges.

Kurz nach der Gründung des Ministeriums für Staatssicherheit wurde mit Befehl des Ministers Zaisser vom 16.12.1950 die Abteilung XI, die Chiffrierabteilung, eingerichtet. Erster Leiter war der 1912 in Dresden geborene Erich Schürrmann. Ursprünglich gelernter Lackierer, nahm er 1948 an Lehrgängen teil, die ihn zum Kriminalpolizisten werden ließen. Sein politischer Hintergrund war die KPD, der er 1932 beitrat. Nachdem im Jahre 1953 im MfS militärische Dienstgrade eingeführt wurden, wurde ihm der Grad

[1] Markus Wolf, Spionagechef im geheimen Krieg. List Verlag 1997, S.274.

eines Obersten zuerkannt. Weitere leitende Mitarbeiter der ersten Stunde waren die Oberstleutnante Baruth und Lunau sowie die Majore Finsterbusch und Montag.[2] Letzter Leiter der Abteilung XI war Wolfgang Birke. Der 1931 in Pirna geborene Birke erlernte den Beruf eines Bäckers. Anfang der 50er Jahre trat er in die Reihen der Polizei ein. Dort wurde er Offizier für Nachrichtenverbindungen in der VP Berlin. 1956 wurde er ins MfS übernommen. An der MfS-eigenen Hochschule in Potsdam erwarb er den Titel des Diplom-Juristen. Leiter der Abteilung XI wurde er 1974. Sein letzter Dienstgrad war Generalmajor.

Anfangs war der Geheimdienst auf altes Militärmaterial angewiesen (z.B. T301). 1951 wurde das Chiffrierwesen in der KVP und im Außenministerium eingerichtet. 1954 wurde das Referat „Chiffriermittel" in der Abteilung XI des MfS begründet. Ein Jahr später stellte man eigene Chiffriermittel her. Während in den 60er Jahren noch Handverfahren und elektromechanische Verfahren verwendet wurden, begann etwa 1967 der Einsatz von EDV im Chiffrierdienst. Die ersten Chiffriergeräte auf der Basis der Mikroprozessoren-Technologie wurden Anfang der 80er Jahre entwickelt. Etwa zur selben Zeit wechselte man von der Fernschreibstrecke zur Funkstrecke. In den 60er Jahren ist eine Abkoppelung von der Sowjetunion zu verzeichnen. Die eigenständige Kompetenz innerhalb des MfS war inzwischen recht hoch. Dennoch hatte man innerhalb des MfS bis zuletzt eine gewisse Hochachtung gegenüber der technischen Leistungsfähigkeit sowjetischen Chiffriergerätes und gegenüber den Personen. Die Leistungsfähigkeit des DDR-Chiffrierwesens wird von westlichen Fachleuten als hoch eingeschätzt. Auf taktischer Ebene wurden wechselseitig die Verfahren geknackt, was für die High-Level-Verfahren allerdings nicht galt. Beide Seiten standen dort im wesentlichen vor unlösbaren Aufgaben.[3]

Neben dem Gründungsbefehl und der Richtlinie Chiffrierwesen von Otto Grotewohl von März 1951 ist die IM-Chiffrierordnung von Juli 1970 erwähnenswert. Der Nachrichten-Verkehr mit IM unterschied sich naturgemäß erheblich von der Kommunikation zwischen Dienststellen in der DDR untereinander. Zum Beispiel fanden neben dem teilmaschinellen Ziffernadditionsverfahren JUPITER (T-307/3) einfache (also manuelle) one-time-pad-Verfahren bis zum Ende der DDR Verwendung.[4]

1 Strukturen des Chiffrierwesens der DDR

Alle sicherheitsrelevanten Einrichtungen verfügten über die Möglichkeit der geschützten Kommunikation. Dies erklärt die vergleichsweise hohe Anzahl von Einrichtungen des Chiffrierwesens und auch die hohe Steigerungsrate. Gab es im Jahre 1975 noch 888 Objekte, so nahm die Anzahl bis zum Jahr 1989 auf 1675 zu. Analog dazu entwickelte

[2] Entwurf Referat GM Geisler 15.101981. BStU ZA AGM 2088, Bl. 356.
[3] Gespräch mit einem Mitarbeiter des BSI, Bonn 2001.
[4] Ein solches Verfahren ist bei richtiger Anwendung sicher und für den individuellen Gebrauch geeignet.

sich die Zahl der Mitarbeiter: von 3817 (1975) auf 10231 (1989).[5] Diese Mitarbeiter hießen GTCW (Geheimnisträger des Chiffrierwesens); sie wurden als Personen definiert, die innerhalb des Chiffrierwesens mit Geheimnissen, z.B. Geräte-Spezifika, zu tun hatten. Weiterhin wurde von „befugten Personen“ gesprochen. Diese wiederum erhielten neben Geheimnissen des Chiffrierwesen auch keine anderen Staatsgeheimnisse zur Kenntnis.[6]

Details des Chiffrierwesens wurden zu den Staatsgeheimnissen gezählt. Die allgemein verwendeten Geheimhaltungsstufen waren DS (Dienstsachen), VVS (Vertrauliche Verschlußsachen), GVS (Geheime Verschlußsachen) und als höchste Stufe GKdos (Geheime Kommandosachen).

Im Jahr 1989 hatten die NVA (Hauptnachrichtenzentrale= HptNZ, CO = Chiffrierorgan mit 550 Einheiten) und der Ministerrat (CBD=ChiffrierbetriebsdienstCOM= Chiffrierorgan des Ministerrates mit 376 Einheiten) die meisten Einrichtungen des Chiffrierwesens.[7] Durch das einschlägige MfS-Schriftgut zieht sich andererseits die Forderung, die Anzahl der Geheimnisträger, insbesondere des Chiffrierwesens, möglichst gering zu halten.

2 Strukturen des Chiffrierwesens im MfS

Die technischen Diensteinheiten gehörten zum Unterstellungsbereich von Generalleutnant Schwanitz, eines Stellvertreter von Minister Mielke.

Schwanitz, geb. 1930, war von 1951 an Angehöriger des MfS. Öffentlich bekannt wurde er, als er in das ZK der SED aufgenommen wurde. Schwanitz wurde im November 1989 Leiter des Amtes für Nationale Sicherheit, der kurzzeitigen MfS-Nachfolgeinstitution.

Elemente des Chiffrierwesens fanden sich in allen Diensteinheiten. Hier sollen einige technische und andere Institutionen innerhalb des MfS erwähnt werden, die in engerem Zusammenhang mit dem Chiffrierwesen standen.

Die Abteilung Nachrichten mit dem Dienstsitz Normannenstraße/Gotlindestraße unterhielt mit der Abteilung N/2 einen Funk- und Chiffrierbetriebsdienst, die Abteilung N/15 war zuständig für die Sicherung des diplomatischen Funkdienstes.

In der ZAIG (Zentrale Auswertungs- und Informationsgruppe) mit dem Dienstsitz Normannenstraße war die AG 10 für Datensicherheit zuständig. Der ZAIG unterstellt war die Abt. XII, das Archiv des MfS. Auch am Dienstsitz Normannenstraße befand sich die ZAGG (Zentrale Arbeitsgruppe Geheimnisschutz) Im Referat 3 der Abteilung 3 der

[5] JHS-Diplomarbeit Rainer Löschinger (1.6.1989) VVS JHS 423/89,“Zur weiteren Qualifizierung der politisch-operativen Sicherung von Geheimnisträgern des Chiffrierwesens unter Berücksichtigung der Entwicklung im Chiffrierwesen bis zum Jahr 2000“, Bl. 32.
[6] vgl. JHS- Diplomarbeit Löschinger, Bl. 9.
[7] JHS- Diplomarbeit Löschinger, Bl. 12.

ZAGG wurde dort die Kontrolle des Geheimnisschutzes realisiert. In enger Beziehung zum Chiffrierwesen befand sich der OTS (Operativ-Technischer Sektor), der seinen Sitz in Hohenschönhausen hatte. Die Hauptabteilung III (Funkaufklärung) mit Dienstsitz in Köpenick, Biesenthal und Gosen, und in dieser Diensteinheit insbesondere die Abteiluggen T4 und T/N waren eng mit der Abteilung XI des MfS verbunden. In der Hauptverwaltung Aufklärung (HVA) waren insbesondere der Stab und die Abteilungen VIII (Operative Technik und Funk) und XX (EDV) mit dem Chiffrierwesen verbunden.

In der Hauptabteilung II (Spionageabwehr) war das Referat 3 der Abteilung II/16 für die Chiffriersicherheit zuständig. Chiffrierstellen existierten in der ZKG (Zentrale Koordinierungsgruppe) und in der HA I (Sicherung NVA und Grenztruppen). In den 15 Bezirksverwaltungen waren Chiffrierstellen innerhalb der Abteilung OT (Operative Technik) eingerichtet, in den Kreisdienststellen war ein Mitarbeiter für Chiffrierungsaufgaben zuständig.

2.1 Die Abteilung XI (ZCO= Zentrales Chiffrierorgan)

Die Arbeit der eigentlichen Abteilung Chiffrierwesen des MfS war durch folgende Aufgabendefinition gekennzeichnet (zitiert aus dem MfS-Schriftgut):

1. Festlegung einheitlicher Verfahrensweisen zur Gewährleistung der Sicherheit und Ordnung bei der Anwendung von Chiffrierverfahren in allen Organen und Einrichtungen der DDR,
2. Beratung zentraler staatlicher Organe bei der Organisation des Chiffrierwesens sowie die Anleitung und Unterstützung der Leiter der Chiffrierorgane bei der Einführung und Anwendung von Chiffrierverfahren sowie bei der Spezialausbildung der Nutzer,
3. Forschung und Entwicklung auf dem Gebiet der Kryptologie,
4. Beschaffung und Instandsetzung von Chiffriertechnik, Produktion von Schlüsselmitteln,
5. Analyse fremder Chiffrierverfahren, Unterstützung von Funkabwehr und Funkaufklärung,
6. Schutz vor kompromittierender Strahlung,
7. Gewährleistung des Auslandschiffrierdienstes.

Diese Aufgaben schlugen sich in der Binnenstruktur der Abt. XI nieder. Die Abteilung befand sich anfangs in der Zentrale in der Normannenstraße und in Johannisthal, ab 1972 im (neuen) Dienstobjekt Hoppegarten (Kreis Strausberg). Zur Abt. XI gehörten zuletzt insgesamt 513 hauptberufliche Mitarbeiter. Für die Hauptaufgaben des Chiffrierdienstes waren 297 Mitarbeiter vorgesehen, 100 für den Auslandschiffrierdienst und 50 Mitarbeiter für sicherstellende Aufgaben. 170 Mitarbeiter hatten den Status des Offiziers im Besonderen Einsatz (OibE). Von der Abt. XI wurden 62 Inoffizielle Mitarbeiter (IM) geführt.

Die folgende (unvollständige) Übersicht zeigt grob die Struktur der Chiffrierabteilung:

Abt. XI/1
Forschung und Entwicklung von Chiffriertechnik
Leiter: OSL BÜTTNER (geb. 1944, Diplomingenieur für Elektrotechnik)

Abt. XI/3
EDV und Rechenzentrum
Leiter: OSL BREHM (geb. 1948, Diplommathematiker)

Abt. XI/5
Chiffriermittelproduktion
Leiter: OSL ZSCHALER (geb. 1936, Diplom-Ökonom)

Abt. XI/6
Dekryptierung
Leiter: OSL MICHLER (geb. 1937, Diplommathematiker)

Abt. XI/9
Auslandschiffrierdienst
Leiter: Hptm. KLUG (geb.1937, JHS-Jurist)

Abt. XI/10
Kryptologie
Leiter: OSL Dr. KREY (geb. 1938, Diplommathematiker)

Das Personal der Abteilung XI war gekennzeichnet durch einen relativ hohen Anteil von Mitarbeitern, die eine akademische Ausbildung durchlaufen hatten. Darunter waren relativ viele Mathematiker, etwa vergleichbar den Abteilungen XIII (EDV) und HVA/XX (EDV in der HVA). Dennoch scheint die Anzahl der Mathematiker aus der Sicht der Leitung der Abt. XI immer noch zu gering gewesen zu sein. Offensichtlich konnten Arbeiten der Entwicklung und der Überprüfung von Verfahren nicht immer unabhängig von verschiedenen Personen wahrgenommen werden.[8]

Die Mitarbeiter des MfS-Chiffrierdienstes unterlagen im Vergleich zu anderen Abteilungen auch einer besonders starken Forderung nach Konspiration. In einer typischen Verpflichtungserklärung kommt dies zum Ausdruck. Hierin hieß es:

„Ich verpflichte mich….

(1) über die Zugehörigkeit zum Chiffrierdienst gegenüber allen Personen einschließlich Familienangehörigen strengstes Stillschweigen zu wahren und ihnen keinerlei Informationen über Fragen des Chiffrierwesens zu geben…

[8] Um dazu einen groben Überblick zu erhalten, wurden 116 Kaderkarteikarten der Mitarbeiter der Abt. XI im MfS ausgewertet Dabei ergab sich: Mitarbeiter mit Abitur: 22 %, Diplom: 12 %.

(2) keinerlei direkte oder indirekte Verbindung mit Personen in oder aus Westberlin, Westdeutschland oder anderen kapitalistischen Ländern aufzunehmen oder zu unterhalten…
(3) auf meine Familienangehörigen…., daß sie keine solchen Verbindungen aufnehmen oder unterhalten…".

2.2 Die Verfahren und Geräte

Die Anzahl der Bezeichnungen für Verfahren und Geräte, die im Chiffrierwesen des MfS verwendet wurden, ist groß. Gelegentlich wurden Bezeichnungen für Geräte und Verfahren synonym verwendet, zum Beispiel das Gerät T-307 und das Verfahren Dudek.

Im Folgenden werden ausgewählte Verfahren/ Geräte benannt und durch Angabe einiger Kenndaten vorgestellt.

AGAT
Maschinelles Chiffrierverfahren garantierter Sicherheit, seit 1968 genutzt

ARGON
Chiffrierverfahren garantierter Sicherheit
Einsatz mit Gerät T-310/50

DUDEK
Chiffrierverfahren garantierter Sicherheit
Seit 1980

ELBRUS
Fernschreib-Chiffriergerät mit zeitlich begrenzter Sicherheit
Seit 1978

FIALKA
Elektromechanisches Chiffrierverfahren (Gerät), sowjetisches Gegenstück zu westlichen Rotormaschinen, seit 1968 genutzt, wohl vornehmlich bei der NVA

GO
Neuartiges Chiffrierverfahren (Gerät T-316), Zeitschlüssel mit einer Gültigkeitsdauer von 7 Tagen

INTERIEUR
Kanal-(Bündel-)Verschlüsselungsgerät garantierter Sicherheit (T-230)
Einsatz nach 1984

PUMA
Datenchiffrierverfahren, rechnerabhängig, ab 1975

SAMBO
Neues Verfahren (mit T-314), war vorgesehen für 1990/91

WECHA
Mobiles Kanalverschlüsselungsgerät für Fernschreiber (ab 1970)

WUMA
Älteres Chiffrierverfahren
Andere Geräte/ Verfahren waren etwa: ADRIA, AMETHYST, ARGON, BOA, DELTA, CM-2, DATSCHIK, JACHTA, JEL, JUPITER, KAIMAN, KOBRA, KRAKE, KUNAL, LAMBDA-1, LIANA, M-105, MAJA, MAMBA, MIRA, OPERATION, POLLUX, SAGA, SELEN, SIRENA, WOLNA.

2.3 Die T-310/50

Exemplarisch wird mit T-310/50 ein Gerät/ Verfahren vorgestellt, das in großer Stückzahl hergestellt und eingesetzt wurde. Es handelt sich um ein elektronisches Kanalchiffriergerät mit internem Schlüssel zur Chiffrierung von Fernschreib-Informationen. Das Gerät wurde 1983 eingeführt und in Serienproduktion gebracht. Es zeichnet sich durch garantierte kryptologische Sicherheit aus, woraus die Verwendbarkeit bis GVS (Geheime Verschlußsache = zweithöchste Geheimkategorie) folgte. Das Gerät sollte bis etwa 2005 verwendet werden. Es wurde in großer Stückzahl (rund 4000) produziert. Im Herbst 1989 waren etwa 3700 Geräte im Einsatz

Ein T-310/50-Spruch bestand aus einem offenen Teil (37 FS-Zeichen) und dem chiffrierten Teil. Der Zeitschlüssel basierte auf Zufallszahlenfolgen.

2.4 Gegenüberstellung ENIGMA und T-310/50

Die Schlüsselhierarchie der T-310/50 (elektronisch) ist (nach R. Staritz) derjenigen der ENIGMA-Rotormaschine (elektromechanisch) aus dem 2. Weltkrieg ähnlich. Der Hauptschlüssel (Langzeitschlüssel) ist bei der ENIGMA ein Schlüssel durch innere Walzenverdrahtung, der T-310/50 eine Platine (Wechsel durch Hardware-Austausch). Der Startschlüssel der ENIGMA sind die Reihenfolge der Walzen und die Ringstellung, bei der T-310/50 dagegen der Tagesschlüssel (mit Zeitcodeschlüssel gelochte Lochkarte). Der Tagesschlüssel der ENIGMA ist die Startstellung der Walzen, bei der T-310/50 wird der Spruchschlüssel durch einen Zufallsgenerator gebildet.[9]

2.5 Verbleib der Technik nach Zusammenbruch des SED-Staates

Es fällt auf, daß in Ausstellungen geheimdienstlicher Technik keine Chiffriergeräte des MfS zu finden sind. Sowohl in den Ausstellungen der Behörde der Bundesbeauftragten

[9] Staritz, Rudolf: HNF- Recherchesammlung: Krypto. Bamberg Berlin Paderborn 2004.

(„Gauck-Behörde“) als auch in der Ausstellung der Forschungs- und Gedenkstätte Normannenstraße (Mielke-Museum), fehlen solche Exponate.

Die Geräte aus sowjetischem Bestand wurden zu 100 % an die Sowjetunion übergeben, die DDR-Geräte wurden durch westliche Behörden sichergestellt. Vermutlich sind die als sehr modern geltenden Geräte weiterhin verwendet worden.

Der wohl letzte Befehl des Chefs des Hauptstabes der NVA, Generalleutnant Gräz, gerichtet an den Leiter der Hauptnachrichtenzentrale, wurde Ende August 1990, also kurz vor dem Beitritt der DDR zur Bundesrepublik Deutschland, gegeben.[10] Die Überschrift hieß: „Übergabe von SAS-und Chiffriergeräten sowjetischer Produktion“.[11]

2.6 MfS-interne Literatur

Einige ausgewählte Grundsatzdokumente des MfS zum Chiffrierwesen sollen erwähnt werden:

22.5.1954
SfS GVS 115/54, Berlin
Arbeit der Abteilung XI

27.10.1959
VVS 837/59, Berlin
Errichtung von Funkstellen

2.7.1968
Hauptverwaltung B
Anweisung über die Einsatzvorbereitung der elektronischen Datenverarbeitung im Bereich der Hauptverwaltung B

15.11.1968
VVS 791/68, Berlin, Befehl 35/68
Befehl zur politisch-operativen und wissenschaftlich-technischen Auswertungs- und Informationstätigkeit für die Linie XI

13.6.1969
GVS 267/69, Berlin
Dienstvorschrift 2/69 über die Regelung des Chiffrierwesens im Ministerium für Staatssicherheit (Chiffrierordnung)

1.7.1970
GVS 226/70 Berlin
Ordnung für den Chiffrierverkehr mit IM (IM-Chiffrierordnung)

[10] Staritz, HNF, S. 6.
[11] SAS= Spezialnuie Apparaturui Swjasi= Spezialnachrichtengerät (russ.).

1.9.1982
VVS 62/82 Berlin
Befehl 18/82
Inhalt: ELOKA

1.7.1985
GVS 46/85 Berlin
1. Durchführungsbestimmung zur Dienstanweisung 3/84
Organisation und Sicherstellung des chiffrierten Nachrichtenverkehrs des MfS

Fachschul-Abschlußarbeiten, Diplomarbeiten und Dissertationen von Mitarbeitern des Chiffrierwesens an der Juristischen Hochschule Potsdam, der Hochschule des MfS

2.7 Die Akten, Möglichkeiten der Forschung

Von den Akten der Abt. XI, die von der Behörde der BStU („Gauck-Behörde“) verwaltet werden, sind zur Zeit etwa 47 lfm erschlossen. Dies entspricht einem Anteil von etwa 22 % des vorhandenen Materials.[12] Soweit bekannt, gibt es bisher nur zwei Forschungsprojekte, die sich direkt oder indirekt auf das Chiffrierwesen des MfS beziehen.

2.8 Aufgaben der Forschung

Hier sollen aus der Sicht der Forschungs- und Gedenkstätte Normannenstraße Aufgaben der weiteren Forschung genannt werden:

- Welche Aufgaben hatten die OibE der Abteilung XI konkret?
- In welchen Einsatzrichtungen führte die Abt. XI ihre Inoffiziellen Mitarbeiter?
- War die Abteilung XI an der Unterdrückung der Bevölkerung direkt beteiligt?
- Inwieweit wurde in der Abt. XI theoretische mathematische Forschung zur Kryptologie geleistet? In welchem Maße fand die internationale universitäre kryptologische Diskussion in dieser Forschung ihren Niederschlag?
- Inwieweit wurden Analysen zur historisch gewordenen Kryptologie erstellt?
- In welchem Maße arbeiteten zivile Mathematiker außerhalb des MfS dem ZCO fachwissenschaftlich zu?
- Wo wurden die Experten des Chiffrierwesens fachlich ausgebildet?
- Welche Rolle spielte die Ideologie bei der Motivation der Mitarbeiter der Abt. XI?
- Welche Erfolge wurden bei der Aufklärung westlicher Chiffrierverfahren und Einrichtungen erreicht? Welchen Stellenwert hat dabei der Fall Kuron?
- Welche Analysen wurden durch die Abt. XI im Hinblick auf verschlüsselte Botschaften in Haftanstalten und im Ost-West-Briefverkehr vorgenommen?

[12] Stand der Erschließung in der Berliner Zentralstelle 31.8.2004.