Regierungsnachrichtenverbindungen - **ВЧ** - **WTsch** - **ACAN ...**

Im Russischen hat **ВЧ** verschiedene Bedeutungen; für die Klärung der Bedeutung von **WTsch** im Zusammenhang mit dem Nachrichtenwesen sind folgende interessant:

- **в**ысоко**ч**астотная связь Hochfrequenzverbindung, HF - Verbindung
- по **ВЧ** über WTsch Verbindung, in der Literatur übersetzt auch „über HF“
- **в**ысоко**ч**астотный Hochfrequenz also eine Alternative zur Niederfrequenz NF
- **в**ысокая **ч**астота **Trägerfrequenz-** Fernverbindungen aber auch:
  - **в**ысочайший allerhöchst
  - **в**ерный sicher , treu
  - **в**ерховный oberste ...

  aber auch:
  - **в**ысшего партийного и советского руководства СССР

Heute finden wir im russischen Sprachgebrauch für **ВЧ** den Begriff für eine Technologie zur Informationsübertragung auf Hochspannungsleitungen und –kabel.
Die eigentliche Bedeutung im Zusammenhang mit der Sicherung der Gesprächsinhalte von Telefonaten und dem Inhalt von, über technische Nachrichtenmittel übertragenen, schriftlichen Nachrichten vor Kompromittierung besteht aber darin, daß für diese Zwecke der **правительственная связь** und darin besonders der **правительственная засекреченная ВЧ- связь** benutzt wurden.
Das sind die Regierungsverbindungen und darin besonders die „geheimhaltenden“ Regierungsverbindungen.

Wie es dazu kam :

In der Sowjetunion bestanden bei der Entwicklung dieser Verbindungsarten folgende Probleme und Prinzipien.
Zunächst bestand zu Beginn der Entwicklung der Sowjetunion (damals RSFSR) nach der Großen sozialistischen Oktoberrevolution die Notwendigkeit**, überhaupt Nachrichten-verbindungen** und besonders effiziente **Fernverbindungen** zur Führung und Verwaltung, nicht zuletzt auch zur Verteidigung dieses Landes mit einer Ausdehnung über 8 Zeitzonen, aufzubauen, da die Entwicklung des Nachrichtenwesens außer in einigen westlichen Städten Russlands auf dem Niveau eines rückständigen Agrarstaates stehengeblieben war.

Dabei wurde von Anfang an von dem erfolgreichen Prinzip ausgegangen, daß die Sicherheit der Gesprächsinhalte und Telegramme so zu gewährleisten war, daß das Prinzip der Reduzierung der Kenntnisnahme der Nachrichten auf die minimal notwendige Personenzahl, in Abhängigkeit von den jeweiligen technischen und organisatorischen Möglichkeiten, ständig eingehalten wurde.

Mit dem Umzug der Regierung und des ZK der KP Russlands(B) in den Kreml wurde z. B. deshalb ein sicheres handvermitteltes ZB-Telefonnetz im Inneren des streng bewachten Kreml-Bereiches mit 100 Anschlüssen geschaffen, das 1922 durch eine 300-stellige ATS (automatische Vermittlung) ersetzt wurde. Dieses als „**Вертушка**“ bekannte geschlossene und gesicherte Telefonsystem der Partei- und Staatsführung war der Anfang für die weitere Entwicklung des Systems. Die Benutzer waren alles Funktionäre der höchsten Führungen „связи для абонентов **в**ысшей категории“.
(In **в**ысшей und in **В**ертушка kommt wieder an hervorragender Stelle das **В** vor**.)**
Nebenbei erwähnenswert ist, daß Дзержинский im Teilnehmerverzeichnis von 1922 die Apparatenummer **007** hatte.

Dieses Netz, welches ich vor 20 Jahren noch als ein klassisches GON bezeichnet hätte, hatte natürlich auch Ausgänge zu Fernverbindungen zu anderen Großstädten und Gebietsvermittlungen. Diese Verbindungen wurden zu dieser Zeit offen, d. h. ohne technische Geheimhaltungsmittel betrieben.

Verwirrspiel oder Absicht

Die international 1909 begonnene Schaffung der wissenschaftlich-technischen Voraussetzungen für TF-Telefonie auf Drahtverbindungen war die Voraussetzung für die 1923 in der Sowjetunion beginnende Schaffung von (**ВЧ) Trägerfrequenz-** Fernverbindungen. Denn wenn man **sicher sprechen** will, muß man zunächst erst einmal überhaupt **sprechen können.**

Im Mai 1921 wurde der kryptografische Dienst des Landes gegründet.
5 мая - День рождения криптографической службы.

1930 wurde die ersten mehrkanaligen **TF-Verbindungen** zwischen Charkow – Moskau und Leningrad - Moskau genutzt. Seit dieser Zeit existiert auch der Begriff „**Спецсвязь**“, für die Regierungsverbindungen. Das dazu benutzte TF-Gerät hieß CMT-34 .

„по **ВЧ“** (s.o.) sprachen im Zusammenhang mit der Führung und Organisation des Landes immer die Mächtigen mit den Provinzen, weil das Trägerfrequenznetz die Fernverbindungen ab 1934 beherrschte .
„по **ВЧ“** (s.o.) war auch ein besonderes Achtungsmerkmal. „по **ВЧ“** sprach auch Jemand, der über einen größeren Raum zu führen hatte, in der Hierarchie höher stand.
„по **ВЧ“** war auch ein Mystikum für Wichtigkeit und Geheimhaltung. Im Buch „August 44“ über eine erfolgreiche Smertsch-Operation spielt Bogomolow Ge-sprächsprotokolle und Telegramme ein, die deutlich mit „über HF“ gekennzeichnet sind. Daß das nur ein Mystikum war, davon zeugt z. B. die chiffrierte Anweisung über die Neuverteilung von Hundefutter in den Truppenteilen.

<u>засекречивающая аппаратура</u>

1935 kann als das Jahr der breiten **Einführung der ersten technischen Geheimhaltungsmittel** für Telefonate auf Endgerätebasis in der SU betrachtet werden. Es handelte sich um **einen Inverter mit der Bezeichnung ES**. 1938 wurden die Inverter ES-2 und die Geheimhaltungsapparatur für Funkverbindungen EIS-3 eingeführt. Die Sicherheit des so gesicherten Kanals war natürlich begrenzt, denn der inverter-gesicherte diplomatische Telefonverkehr der UdSSR z. B. zwischen Moskau und Paris wurde seit 1935 permanent durch einen der deutschen Dienste (Forschungsamt) mitgelesen und lag dann als textliche Kryptoanalyse nach einigen Tagen vor. Bei Invertierungen der von der Sowjetunion benutzten Art, war ein Online- mitlesen nicht möglich.

Seit dieser Zeit wuchs beständig der Teil der Regierungsverbindungen die nun verschlüsselt (invertiert) betrieben wurden. Damit konnte im Vorfeld des 2. Weltkrieges der Deckungsgrad kontinuierlich erhöht werden. Die ersten automatischen Zentralen mit 5 Teilnehmern, begannen im **<u>System der gedeckten Regierungstelefon-verbindungen</u>** zu arbeiten.

Auch die Anzahl der **SAS-Kanalchiffriergeräte für Telegrafie** mit garantierter Sicherheit (online), damals **C-308-M** (S 308 M), im Netz der Regierungsverbindungen stieg seit 1938 kontinuierlich.
So ist auch die Darstellung in einer Dissertation aus dem Jahre 1979 unrichtig, daß die Amerikaner die ersten waren, die 1943 automatische Online-Kodierungsgeräte verwendeten. Bis April 1941 wurden, bei gleichzeitiger Erhöhung der Anzahl der Drahtverbindungen um ca. 35%, schon ca. 50 % dieser Telefonverbindungen mit Spezialgeräten, besonders nach dem Inverterprinzip, abgedeckt.

Das war nicht zuletzt der Einführung des Gerätes **ПЖ-8** zu verdanken, die aus der ungedeckten TF-Verbindung mit CMT-34 eine leitungsverschlüsselte mehrkanalige gedeckte Übertragungsstrecke machte. Das war der Beginn der massenweisen Nutzung von Leitungsverschlüsselungen im Netz der Regierungsverbindungen der UdSSR. Zu diesem Zeitpunkt wurden auch, sicher in Voraussicht des bevorstehenden Krieges, die hohen Führungsstellen der Roten Armee in dieses Netz einbezogen.
1940 wurde zur Erhöhung der Kanalzahl das zwölfkanalige TF-System K-12 einge-führt.
Nachdem 1931 im sowjetischen Generalstab die sogenannte 8. Abteilung geschaffen wurde, war bereits im Jahr 1932 die Einführung der ersten von **Волосок** entwickelten sowjetischen Chiffriergerät ШМВ–1 (offline) zu verzeichnen. 1934 wurde bereits die nächste Maschine B-4, besser bekannt als M-100, in die Bewaffnung eingeführt. Im Jahr 1943 folgte die M-101 Изумруд (Smaragd).

Beiderseits des Atlantic

Interessanterweise, das sei hier eingefügt, kam es auf amerikanischer Seite am Ende der 30-er Jahre zu einer ähnlichen Entwicklung eines Regierungsnetzes, dort wurde es aber **ACAN** (Army Command and Administrative Network) genannt. Aus dem angegebenen Namen ergibt sich auch die Nutzung.
Mit dem **WTsch**–Netz der sowjetischen Regierungsverbindungen, das durch die войск правительственной связи (Truppen der Sicherstellung der Regierungsnachrichtenverbindungen) sichergestellt wurde und dem **ACAN**, das durch die Truppen des Army Communikation Service des amerikanischen Signal Corps sicher-gestellt wurde, ist eine zeitlich parallele Entwicklung von geografisch wohlgetrennt und geheimgehaltenen Nachrichtennetzen erkennbar.

Auch einige der gegenwärtigen, den historischen Tatsachen nicht entsprechenden, Darstellungen im ZH mit diesem Thema, sind sicherlich dem Bedürfnis nach **„Geheimhaltung der Geheimhaltung“** der ehemaligen Alliierten und später erbitterten Gegner im kalten Krieg, geschuldet.
Ob der auf **diesem Gebiet** zu verzeichnende **immerwährende Krieg** während der Zeit des sogenannten “kalten Krieges“ nun angesichts von bis zum Jahr 1996 zu beklagenden **152 Todesopfern** auf Seiten der **NSA** immer noch als kalt zu bezeichnen ist, sei dahingestellt.

Die oben bezeichnete **„Geheimhaltung der Geheimhaltung“** geht zumindest soweit, daß solche **besonderen Vorgänge** des 2. Weltkrieges wie „Ultra“, „Sigsaly oder X“, „Kotelnikows Arbeiten im Institut 56“ und Shannons „Analogue of the Vernam System“ , Turings „Treatis of

the ENIGMA“ oder das Hauptwerk Friedmans zwischen 30 und 50 Jahre lang strengstens geheimgehalten wurden. Einige von den ROHRBACH-Dokumenten sind noch heute als Geheim eingestuft. Die russische Seite erklärte unlängst durch den ehem. KGB General Prof. KONDRASCHOW, „daß es eben in Russland auch viele kluge Leute gäbe, nur habe er leider ihre Namen alle vergessen....“

Kotelnikow

Владимир Александрович **Котельников** arbeitete 1940 am MEI, (Shannon wohl am MIT) dem Moskauer energetischen Institut, nachdem er bereits 1933 in seiner Arbeit „О пропускной способности эфира и проволоки в электросвязи — Всесоюзный энергетический комитет//Материалы к I Всесоюзному съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности“ (**Über die Bandbreite des Äthers**....) das grundlegende Theorem der Nachrichtentechnik, Signalverarbeitung und Informationstheorie, das der Abtastung, heute das WKS-Theorem und damit „die **Informationstheorie“** veröffentlichte. Seit den 50er Jahren ist seine Urheberschaft unumstritten.

Beauftragt mit der Schaffung von Sprachchiffriergeräten hat er den Artikel Homer Dudleys über Vokoder ausgewertet. Auch Potter; Ralph K. (Madison, NJ) bezog sich in seiner Patentschrift zu sicherer Telefonie der Art wie SIGSALY, Nr. 3,967,067 vom 24.9.1941, auf Dudley, der dazu ein Patent angemeldet hatte.

Die Reihe der Parallentwicklung von Sprach-Geheimhaltungsapparaturen in UdSSR und USA wird ergänzt durch die gleichen Probleme bei der erzielten Sprachqualität. Kotelnikow berichtet über die „zittrige Stimme“ am Ausgang des chiffrierten Kanals. Johnson, als Präsident der USA, lehnte die Benutzung seines Sprachchiffriergerätes strikt ab, weil am Ausgang des Gerätes eine „Donald Duck“ ähnliche Stimme zu hören war.
Auch der Ausgangspunkt der Entwicklung der amerikanischen und sowjetischen Sprachchiffriergeräte geht auf die gleiche Quelle, Dudleys Schrift s.o. im Bell Lab internen Mitteilungsblatt von 1939 über Vocoder, zurück.
Parallelenwicklungen gab es also genug. Auch folgende Parallelität ist interessant, daß die Amerikaner im transatlantischen Funkverkehr mit Churchill, gedeckt durch das Gerät Bell A 3 (den Vorgänger von „Sigsaly“), genauso wie die Russen auf ihrer, mit dem ES gedeckten, diplomatischen Drahtverbindung Moskau - Paris von einem deutschen Dienst belauscht

wurden; die sowjetischen vom Forschungsamt, die Amerikaner von der „Forschungsstelle„ der Reichspost „Forschungsanstalt“.
Andere Geräte der garantierten Sicherheit wie „Sobol“, die aber für die Deckung der Drahtverbindungen nutzbar waren hießen Newa und „Sowa“.
Die Draht-Telefonverbindungen des Oberkommandierenden zu den Frontbefehlshabern bestanden ab ca. 1941 aus den Geräten Newa, deren Netz durch ein KW- Sprechfunknetz, gesichert mit „Sobol“, überlagert war. Newa wurde nach Ausstattung der Streitkräfte auch im diplomatischen Dienst eingesetzt und löste die bisherigen Inverter ab.
Ab 1943 wurde eine ständige KW- Verbindung zwischen dem Hauptquartier und dem Stab der kaukasischen Front in Тбилиси, unter Nutzung von „Sobol“ als Ersatz für die von der Wehrmacht zerstörten Drahtverbindung, betrieben .
Nach Kotelnikows Sprachchiffriergerät zur Nutzung in der taktischen Ebene durch Vokoder und zeitlich wiederkehrendem Schlüssel der Zeit- und Frequenztransposition (begrenzte Sicherheit), wurde also mit Beginn der Kampfhandlungen des 2. Weltkrieges mit Hitlerdeutschland, die Aufgabe der Entwicklung eines Gerätes gestellt, welches den höchsten Sicherheitsanforderungen der Partei- und Militärführung entsprach. 1942 wurde von Kotelnikows Kollektiv das Gerät «Соболь-II» vorgestellt, das „garantierte Sicherheit“ verkörperte und zu dieser Zeit nichts Vergleichbares auf der Welt zu finden war. Damit ermöglichte das Gerät die Ausnutzung der hohen Mobilität und Geschwindigkeit von Funkverbindungen mit höchsten Ansprüchen der Sicherheit. Funksprechverkehr auch auf der Ebene der Kommandierenden der Fronten, denen bisher die Benutzung von Funk streng verboten war, war jetzt möglich. Eine wesentliche Arbeitserleichterung.

Damit enden die Aufzeichnungen von abgehörten Gesprächen sowjetischer Diplomaten in den Archiven des Forschungsamtes und des Auswärtigen Amtes.
Diese Sprachchiffrierer der garantierten Sicherheit wurden nach Kriegsende zu einer ganzen Klasse von Geräten der besonderen Verwendung entwickelt, die bis in die 70er Jahre benutzt wurden.
Eine weitere Parallelität: Im amerikanischen (SIGSALY) als auch im sowjetischen System SOBOL wurde durch eine Kompression/Abtastung im Vokoder eine Impulsfolge bereitgestellt, die das Sprachfrequenzspektrum charakterisierte. Dabei hat der sowjetische Konstrukteur das Kotelnikowsche Abtasttheorem (UdSSR, 1933) und der amerikanische Konstrukteur das Shannonsche Abtasttheorem (Bell 1948) benutzt. Das folgende Vernam-System war gleich, obwohl die Amerikaner Schallplatten als Schlüsseldatenträger und die Sowjets einen anderen Datenträger nutzten. Aber in beiden Systemen herrschte das OTP Prinzip.

Der Vollständigkeit halber sei erwähnt, daß auf sowjetischer Seite die Kryptierung nach den erfolgreichen Prinzipien der zufällig gesteuerten Zeit- und Frequenztranspositionen erfolgte, auf amerikanischer Seite durch eine logische Operation zwischen den Zeichen der codierten Sprache und einem zufälligen Zeichen von einer Schallplatte.

Auch der „Führerbefehl“ von 1943:
„ ... wer in der Lage ist, einen russischen Chiffreur oder russische Chiffriertechnik aufzubringen, erhält das Eiserne Kreuz, wird in die Heimat versetzt, nach Berlin und wird nach dem Krieg auf der Krim angesiedelt.“ änderte nichts daran, daß sich kein sowjetischer Chiffreur/Betriebsmechaniker je gefangen nehmen ließ.
Im internen Gespräch soll Hitler hypothetisch Kotelnikows unentschlüsselbares System „SOBOL“ gegen eine kriegsstarke allgemeine Armee eingetauscht haben.

Die Entwicklung von Regierungsnachrichtenverbindungen ist also kein spezielles sowjetisches Projekt gewesen, sondern auch in den USA festzustellen gewesen.

Auch der Umstand, daß ein Geheimdienst die Führung und Sicherung eines solchen Komplexes übernommen hat, ist international: Signal Intelligence Service, NKWD/ KGB, SSSI/ FSO, NSA, BND ZfCh / BSI, MfS, GCHQ/CESG.

Alle Mächtigen waren sich über die besonderen strategischen Werte (Vorteile) der Kryptografie und Kryptoanalyse im Klaren (s.o. Hitler) .
Churchill: „Es war „Ultra“ zu verdanken, daß wir den Krieg gewonnen haben.“ Zu dieser Meinung passt die These von **Quellenschutz kontra Bombardierung der Stadt Coventry**.

In allen Fällen entsteht die Sicherheit der Verbindungen nach vorheriger umfänglicher Forschung und größeren Investitionen.

In allen Fällen ist zu diesem Thema noch nach bis zu 6 Jahrzehnten strengste Geheimhaltung (s.o.) festzustellen. Gewisse Dokumente aus Bletchley Park werden erst 2015, also 70 Jahre nach Kriegsende deklassifiziert.

Je höher die Hierarchieebene der Kommunikationspartner um so sicherer das Verfahren. (Rote Linie Moskau Washington – OTP, System Sigsaly – OTP ...)

Aber die Hauptsache:

In beiden Vorgängen wurde der, ich nenne es mal „**kryptologische Dreisatz**“, der besonders anschaulich bei Bauer dargestellt wurde, zugrunde gelegt, der in anderer Form in Shannons Grundsätzen seiner **Communication Theory of Secrecy Systems** von 1949 zu lesen ist. Dieser Dreisatz besagt, daß bei der Sicherheitsstufe „secrecy – garantierte Sicherheit“ es nur 2 wichtige Dinge zur Realisierung gibt:

1. Ein Chiffriersystem, und das kann jeder wissen, welches vom Typ **Vernam** ist.
2. Ein Schlüssel, der einem **echten physikalischen Zufallsprozeß** entspringt und zu dem entsprechend des **Prinzips der Schlüsselherrschaft** nur Berechtigte Zugang und Änderungsberechtigung haben (und zwar unmittelbar).

Damit aber reduziert sich das einzige Risiko/Unsicherheit des Systems auf den Schlüssel und den Umgang mit ihm.

Andere Systeme, die nicht Shannos Grundsätzen folgen, sind dann nur von „begrenzter Sicherheit“. Das heißt, die Sicherheit dieser Systeme wird von der Zeit repräsentiert, die der Unberechtigte benötigt, durch mathematische Methoden zum Klartext vorzudringen.
Bei den sowjetischen Regierungsverbindungen, besonders zur Führung der Truppen, wurde dazu zusätzlich das Prinzip der Direktverbindung (Ende zu Ende Verbindung) konsequent eingehalten.
Abschließend sei erwähnt, daß es heiße und kalte Kriege waren und sind, die die Entwicklung auf diesem, zugegebenermaßen schwer verständlichen Gebiet einer besonderen Kommunikationsform vorangebracht haben. Und dabei sei nicht nur der Krieg zwischen Staaten gemeint.

Entwicklung auf diesem Gebiet (der begrenzten Sicherheit) heißt es heute

1. Verzigfachung des Schlüsselraumes

Am Beispiel ELBRUS/JACHTA T-217/219 zum R-168NA(5)E
von: **$1{,}6*10^{3}$** zu: **10^{38}**

2. Miniaturisierung und daraus natürlich erhebliche Gewichtsreduktion

Am Beispiel ELBRUS/JACHTA T-217/219 zum R-168NA(5)E
von: 60x50x40 **cm** zu: ca. 50x100x20 **mm**

3. Sicherheitserhöhung durch interne Zusatzhardware

Am Beispiel R-168NA(5)E: Sicherste Schlüsseleinstellung und automatische Schlüsselvernichtung bei möglicher Kompromittierung.

So ist dann auch zu vermuten, daß auf dem Gebiet der garantierten Sicherheit für die höchsten Hierarchieebenen eine ähnliche Entwicklung vor sich geht.