Teil 1:
Enigma oder die Automatisierung der Verschlüsselung

Das erste Kapitel ist den geschichtlichen Hintergründen und Fakten zur Chiffriermaschine Enigma gewidmet – sie werden gleichsam als Einführung ins Thema dargestellt; nach dem eben Gesagten ist dies allerdings nur mit einem hintersinnigen Lächeln möglich. Existieren denn diese Hintergründe und Fakten überhaupt unabhängig vom Mythos? – Oder ist es nicht vielmehr so, dass der vom Mythos geprägte Diskurs immer Neues hervorbringt?

Wie dem auch sei – ein Minimum an faktischen Informationen und Hintergründen ist notwendig. Dazu gehört etwa die Erklärung dessen, was diese Chiffriermaschine überhaupt war, wie sie funktionierte und wie ihr Geheimnis gelüftet werden konnte. Auch einige allgemeine Erörterungen zum Thema Kryptografie sind Teil dieser Einführung. Die umfangreiche Fakten- und Literaturlage soll knapp aber kritisch zusammengefasst werden. Als Exkurs ist der zweite Teil dieses Kapitels zu verstehen, in dem es um die Schweizer Enigma und ihre Nachfolgemaschine, die Nema, geht.

Forschungslage und Literatur

Zur Enigma-Geschichte existiert eine wachsende Menge von Literatur und medialen Zeugnissen, die auch Teil dieser Untersuchung – vor allem im dritten Kapitel – sind. Schon an dieser Stelle lassen sich eine Reihe von Feststellungen machen: Ein grosser Teil der Literatur gibt im Wesentlichen die Aussagen einiger weniger Werke angelsächsischer und vor allem britischer Provenienz wieder; wichtige Werke wurden zudem von Personen verfasst, die an der Enschlüsselungsoperation selber mitbeteiligt waren. Könnte es sein, dass es einen Zusammenhang zwischen dieser Tatsache und der wiederkehrenden, fast kultähnlichen Beschäftigung mit

diesem Thema gibt? – Wir behalten diese Frage im Auge und versuchen, im dritten Kapitel eine Antwort darauf zu finden.

Der Anfangspunkt der Beschäftigung mit der Enigma lässt sich klar benennen: Es ist nicht das Ende des Zweiten Weltkriegs, sondern das Ende der Informationsblockade zur Operation Ultra, wie das gesamte britische Entschlüsselungs-Unternehmen hiess. Das erste Buch zur Geschichte der Enigma, ›The Ultra Secret‹, erschien 1974 und stammte aus der Feder des britischen Offiziers Frederick W. Winterbotham, der an der Entschlüsselungsoperation selber beteiligt war.[1] Sowohl die USA als auch Grossbritannien hatten ihre Erfolge im Dekodieren deutscher Meldungen nach dem Krieg zur Geheimsache erklärt. US Präsident Truman entschied dies bereits am 28.August 1945, drei Wochen nach dem Abwurf der Atombombe über Hiroshima. Es gab dafür einen handfesten Grund: Die Maschinen verschwanden nicht nach dem Waffenstillstand, sondern blieben offenbar noch für Jahrzehnte in Gebrauch, vorab in den Commonwealth Staaten. Die letzte Enigma soll erst 1975 aus dem Verkehr gezogen worden sein.[2] David Kahn vermutet, dass diese Staaten sehr wohl wussten, dass Grossbritannien ihre Nachrichten entschlüsseln konnte. Das kümmerte sie wenig, denn ihre Sorge galt vor allem den Nachbarstaaten.[3]

Zu den am meisten zitierten Darstellungen gehört die mehrbändige Darstellung »British Intelligence in the Second World War«[4] von Francis H. Hinsley (1918-1998). Hinsley war wie Frederick W. Winterbotham selber an der Operation von Bletchley Park beteiligt.

Die erste mir bekannte umfassende technische Darstellung zum Thema Enigma ist »Machine Cryptography and Modern Cryptanalysis« von Cipher A. Devours und Louis Kruh von 1984. Das Buch gilt auch 20 Jahre nach seinem Erscheinen als Standardwerk und wird zu hohen Preisen antiquarisch gehandelt.[5] Ein weiterer Name, der in unserem Kontext oft auftaucht, ist Alan Stripp, der in seinem zusammen mit Harry Hinsley

1 Frederick W. Winterbotham: The Ultra Secret. New York 1974. Harper & Row. (Deutsch: Aktion Ultra. Frankfurt/Berlin 1976. Ullstein.)

2 Cipher A. Deavours; Louis Kruh: Machine Cryptography and Modern Cryptoanalysis. Norwood 1985. S. 40.

3 David Kahn: The Codebreakers. New York 1996. Scribner. (Erste Auflage 1967) S. 979.

4 F. H. Hinsley: British Intelligence in the Second World War. London 1979-1990. 5 Bände.

5 Devours/Kruh: Machine Cryptography. Wie oben.

publizierten Werk »Codebreakers: the Inside Story of Bletchley Park«[6] zahlreiche Zeugnisse von Zeitzeugen präsentiert.

Schliesslich muss hier auch Tony Sale, wiederum ein Brite, erwähnt werden: Der 1931 geborene Tony Sale gehört zu den Gründern des Bletchley Park Trust, jener Organisation, die sich mit der Erhaltung von Gebäuden und Einrichtungen von Bletchley Park beschäftigt. 1991 startete der Ingenieur mit der Rekonstruktion der Entschlüsselungsmaschine Colossus.[7] Waren die zur Entzifferung der Enigma gebauten »Bomben« rein elektromechanische Maschinen, so stellte Colossus die erste digitale, mit Röhrenelektronik bestückte Rechenmaschine dar. Sie wurde zur Entschlüsselung des verschlüsselten deutschen Funkfernschreiber-Verkehrs entwickelt. Tony Sale veröffentlicht seine Erkenntnisse vorzugsweise im Internet.[8]

Eine wichtige Rolle spielt das Buch des amerikanischen Journalisten und Pulitzer-Preisträgers David Kahn »The Codebreakers«,[9] das 1967 zum ersten Mal erschienen ist und 1996 in einer überarbeiten Ausgabe aufgelegt wurde. Kahns Werk ist die erste umfassende Darstellung zum Thema Kryptografie, allerdings fehlt in ihrer ersten Auflage von 1967 jeglicher Hinweis auf die Enigma. Sehr zum Verdruss des Autors übrigens, aber davon wird später noch ausführlicher die Rede sein. David Kahn ist auch Mitherausgeber der seit 1977 existierenden wissenschaftlichen Zeitschrift »Cryptologia«,[10] die sich unter anderem mit historischen Fragen der Kryptographie beschäftigt und zahlreiche Einzelstudien zum Thema Enigma publiziert hat.

Eine wichtige Figur im Kontext der Entschlüsselungsoperation war der Mathematiker Alan Matheson Turing; Andrew Hodges – ebenfalls Mathematiker – hat ihm 1984 eine Biographie[11] gewidmet. Sie gehört zu

---

6 Alan Stripp; Hinsley, Harry Francis: Codebreakers: The Inside Story of Bletchley Park. Oxford 1993. Oxford University Press.

7 Tony Sale: The Colossus Computer, 1943-1996 and How it Helped to Break the German Lorenz Cipher in WWII. Shropshire 1998. M&M Baldwin.

8 Internet-Seite von Tony Sale: www.codesandciphers.org.uk vom 16.2.2008

9 David Kahn: The Codebreakers. New York 1996. Scribner (Erste Auflage 1967).

10 Cryptologia. An International Journal Devoted to Cryptology. Philadelphia 1977ff. Taylor & Francis.

11 Andrew Hodges: Alan Turing the Enigma. London 1983. Burnett Books. Deutsch: Andrew Hodges: Enigma. Wien 1994. Springer. vgl. auch David Leavitt: The Man who knew too much: Alan Turing and the Invention of the Computer. London 2005. W. W. Norton & Company.

den am meisten zitierten Werken im Kontext der Enigma und wird heute als massgebliche Biografie des britischen Mathematikers angesehen.

Die umfassendste Darstellung zur Geschichte der Kryptografie stammt aus der Feder des deutschen Mathematikers Friedrich L. Bauer.[12] Die Geschichte der Enigma spielt in diesem Werk eine wichtige Rolle; Bauer hat den jeweils neuesten Forschungsstand bei den verschiedenen Überarbeitungen berücksichtigt. Sein Werk wird zusammen mit einer Darstellung zur wissenschaftlichen Aufarbeitung der Entschlüsselungsoperation im dritten Teil dieser Untersuchung eingehend vorgestellt.

Eine kurze Geschichte der Kryptografie

Zur Begriffserklärung: Zur Kryptografie[13] (griechisch: ›kryptos‹ verborgen und ›grafein‹ schreiben) im engeren Sinn gehören alle Methoden, die sich im weitesten Sinn als Geheimschriften bezeichnen lassen. Dazu zählen Texte, die im einfachsten Fall mit einer Alphabetverschiebung erzeugt oder im komplexesten mit asymmetrischen Schlüsseln und mit aufwendigen Computeroperationen berechnet wurden. Die Steganographie (griechisch: ›steganos‹ eng und ›grafein‹ schreiben) zielt auf das Verstecken eines Textes ab. Schon mit einfachen Geheimtinten wie Zwiebelsaft oder Milch lassen sich unsichtbare Texte erzeugen, die man später mit Wärme wieder sichtbar machen kann. Signale lassen sich technisch so verändern, dass sie sich nicht mehr vom Umgebungsrauschen unterscheiden lassen. Auch die Mikropunkt-Fotografie, die vor allem im Kalten Krieg beliebt war, gehört zu diesen Methoden. Die Beschreibung und Analyse von kryptografischen und steganografischen Methoden hat eine grosse thematische Nähe zur Entzifferung alter Schriften, wie etwa der mykenischen Linear B, der Hieroglyphen oder der bis heute nicht lesbaren Schrift der Etrusker[14].

Der Begriff der Kryptografie ist verhältnismässig jung – der lateinische Ausdruck Cryptologia und auch Cryptographia wurden 1641 erstmals vom englischen Bischof John Wilkons mit der Bedeutung Geheim-

12 Friedrich L. Bauer: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Berlin und Heidelberg 2000. Springer. Ders.: Decrypted Secrets. Methods and Maxims of Cryptology. Berlin und Heidelberg 2006. Springer.

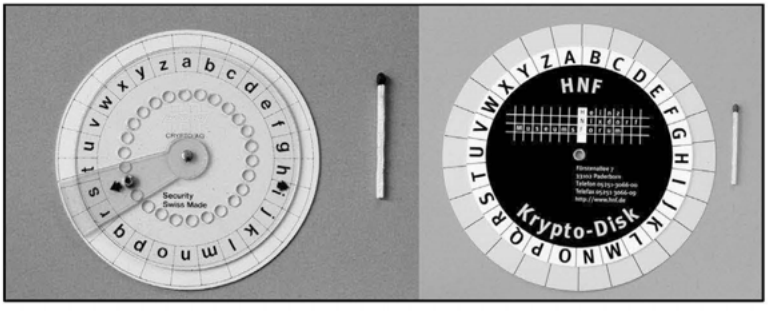
13 Ebenda.

14 Kahn: The Codebreakers: S. 895-937. Simon Singh: Geheime Botschaften. S.235-280.

sprache benutzt. Gebräuchlich sind heute sowohl die Begriffe Kryptologie als Oberbegriff sowie Kryptografie und Kryptoanalysis als Unterbegriffe, wobei die Unterscheidung in Ober- und Unterbegriffe meist nicht so streng gemacht wird.[15]

Eines der einfachsten kryptografischen Hilfsmittel ist die Chiffrierscheibe. Ihre Erfindung wird dem italienischen Architekten Leon Albert im 15. Jahrhundert zugeschrieben. Sie funktioniert denkbar einfach und besteht aus zwei Kreisen mit je einem Alphabet darauf. Den verschlüsselten Text erhält man, indem man die eine Scheibe gegen die andere verdreht und dann den resultierenden Buchstaben abliest. Solche Scheiben waren während Jahrhunderten im Gebrauch.

Abbildung 1



Zwei Chiffrierscheiben aus jüngerer Zeit: Die Scheibe links wurde von der Firma Crypto AG als Werbegeschenk benutzt. Die Scheibe rechts wird heute vom Heinz Nixdorf Museumsforum für museumspädagogische Zwecke eingesetzt. (Fotos D. Landwehr)

Die Chiffrierscheibe wurde noch in den Zeiten des amerikanischen Bürgerkrieges benutzt und ist gleichzeitig auch zum Sinnbild für Geheimschriften überhaupt geworden: Noch in den 70er Jahren setzte der Schweizer Chiffriergeräte-Hersteller Crypto AG Chiffrierscheiben als Kundengeschenke ein und kein museumspädagogischer Kurs zum Thema Geheimschriften kommt ohne diese Scheibe aus.

15 Friedrich L. Bauer: Entzifferte Geheimnisse. S. 9.

Funk und Radio als Beschleuniger

Das Bedürfnis nach der Chiffrierung akzentuierte sich dramatisch mit der Einführung des Mediums Funk für die Übermittlung von Botschaften. Kittler hat die übermittlungstechnische Rückkoppelung zwischen der (drahtlosen) Erteilung von Befehlen und der Rückmeldung als unerlässliches Element der modernen Kriegsführung bezeichnet[16]. Die drahtlose Übermittlung erhöhte die Geschwindigkeit und Effizienz der Nachrichtenübermittlung in einem nie da gewesenen Masse – brachte aber gleichzeitig ein neues Problem mit sich: Ein Funkspruch war immer gleichzeitig eine Botschaft an alle. Dieses Problem hatte bereits Guglielmo Marconi (1874-1937), den Erfinder der drahtlosen Nachrichtenübermittlung beschäftigt:

»Als mir vor 42 Jahren in Pontecchio die erste Radioübertragung gelang, sah ich schon die Möglichkeit voraus, elektrische Wellen über grosse Entfernungen zu senden, aber ich hegte dennoch keine Hoffnung, zur Erlangung jener grossen Genugtuung zu kommen, die mir heute wiederfährt. Denn damals wurde meiner Erfindung in der Tat ein grosser Defekt zugeschrieben: die mögliche Interzeption übermittelter Nachrichten. Dieser Defekt beschäftigte mich so sehr, dass meine hauptsächlichen Forschungen viele Jahre auf seine Behebung gerichtet waren. Und nichtsdestoweniger wurde genau dieser ›Defekt‹ nach etwa 30 Jahren ausgenutzt und ist zum Rundfunk geworden.«[17]

Der Physiker Guglielmo Marconi sah den Nutzen seiner Entdeckung vor allem in der Übertragung militärischer Nachrichten. Funk wurde erst später zum Rundfunk. Bezeichnenderweise war der erste deutsche Rundfunkdirektor jener Nachrichtenoffizier Hans Bredow, der sich Jahre zuvor im Ersten Weltkrieg den »Missbrauch von Heeresgerät« hatte zu Schulden lassen kommen![18]

Prinzipien der Kryptografie

Die Kryptografie war als Wissenschaft in den 30er Jahren in den Kinderschuhen und benutzte, wie der Mathematiker Andrew Hodges feststellte,

16 Friedrich Kittler: Grammophon – Film – Typewriter. Brinkmann und Bose. 1986. S. 363.

17 Ebenda.

18 Jochen Hörisch: Eine Geschichte der Medien von der Oblate bis zum Internet. Frankfurt am Main 2004. Suhrkamp. S. 331.

»wenig brauchbare Methoden«.[19] Fast alle beruhten auf den Prinzipien der Addition und der Substitution.

- **Addition**: Man addiert eine Zahl Schritte zum Buchstaben, der sich in einem als Kreis dargestellten Alphabet befindet.
- **Substitution**: Man ersetzt Buchstaben nach bestimmten Regeln (Algorithmen) durch andere.

Beide Methoden sind leicht zu durchschauen. Im Fall der Additionsmethode gibt es grundsätzlich nur 26 Lösungen, im Fall der Substitution kommt man mit einer Frequenzanalyse schnell zum Ziel. Jede Sprache hat ihre Eigengesetzlichkeit, dazu gehört zum Beispiel die Häufigkeitsverteilung von Vokalen und Konsonanten.[20]

Die einzig wirklich sichere Verschlüsselungsmethode des frühen 20. Jahrhunderts war der individuelle Einmal-Schlüssel, auch One-Time-Pad genannt, der von Gilbert Vernam (1890-1960) im Jahr 1918 erstmals beschrieben und bis in die neuere Zeit verwendet wurde. Die Methode ist denkbar einfach: Sie beruht auf einem fortlaufend und zufällig generierten Schlüssel, von dem genau zwei Kopien existieren und der nur für eine Meldung benutzt wird. Die Buchstabenfolge des Schlüssels muss streng zufällig sein und der Schlüssel muss genau so lang sein wie die Nachricht, die er codiert.[21] Die Methode des One-Time-Pads wurde vor allem in der Sowjetunion gerne verwendet.

Die Methode gilt heute noch als sicher, wenn sie sauber angewendet wird, und genau hier liegt die Crux: Zuerst muss eine riesige Menge von Schlüsseln mit wirklich zufälligen Zahlenfolgen hergestellt werden. Dann müssen diese Schlüssel sicher verteilt werden, in der Praxis ein oft unüberwindbares Hindernis. Und schliesslich ist auch die Produktion von einwandfreien Zufallszahlen alles andere als banal. Trotzdem verwendeten sowohl die Briten als auch die USA, die Sowjetunion und auch die Wehrmacht dieses System, allerdings nur in einem sehr reduzierten Um-

19 Andrew Hodges: Turing Enigma. S. 190.

20 Cryptool Programm: Die Deutsche Bank stellt ein Programm zur Verfügung, mit dem sich die verschiedenen kryptografischen Methoden von der einfachen Cäsar-Verschlüsselung bis zur modernen RSA Chiffrierung nachvollziehen lassen: www.cryptool.de vom 17.2.2008.

21 Friedrich L. Bauer: Entzifferte Geheimnisse. S.156-159. Bruce Schneier: Angewandte Kryptografie. Protokolle, Algorithmen und Sourcecode in C. München etc. 2006. Pearsons Studium. S. 17ff.

fang. In der ehemaligen Sowjetunion sollen solche Zahlentabellen gelegentlich sogar von Hand hergestellt worden sein.[22]

Der Informationstheoretiker Claude E. Shannon (1916-2001) hat im Rahmen seiner allgemeinen Informationstheorie bereits 1949[23] definiert, unter welchen Bedingungen eine Verschlüsselung als sicher gelten kann. Der nach ihm benannte Shannonsche Hauptsatz lautet – etwas kryptisch: »In einer klassischen Shannonschen Chiffrierung ziehen je zwei der drei Eigenschaften *ist perfekt, ist individuell, ist vom Vernamschen Typ,* die dritte nach sich.«[24]

Der Auftritt der Maschine

Die Idee der maschinellen Verschlüsselung von Texten war naheliegend, gerade auch da sich gegen Ende des 19. Jahrhunderts die Schreibmaschine als Bürogerät mit grossem Erfolg durchzusetzen begann.[25] Nach der Mechanisierung des Schreibens sollte auch die Verschlüsselung, zumal im militärischem Kontext, automatisiert werden.

Chiffriermaschinen haben eine doppelte Funktion: Sie vollziehen nicht nur die Chiffrierschritte, sie erzeugen auch ihre eigene Schlüsselzeichenfolge für die Auswahl dieser Chiffrierschritte. Solche Maschinen waren zunächst etwas wenig Spektakuläres: »Sie taten nichts, was nicht durch das Nachschlagen von Tabellen in Büchern hätte getan werden können, ermöglichten aber, dass die Arbeit schneller und genauer getan werden konnte.«[26]

Die Existenz solcher Maschinen war kein Geheimnis. Jeder wusste davon. Allerdings waren die Folgen alles andere als banal, wie schon ein zeitgenössisches, populärwissenschaftliches Werk folgert: »Was derzeitige kryptoanalytische Methoden anlangt, sind von einigen dieser Maschinen stammende Chiffriersysteme der praktischen Unlösbarkeit sehr nahe.«[27]

---

22 Vgl. Peter Gendolla und Thomas Kamphusmann: Die Künste des Zufalls. Frankfurt 1999. Suhrkamp. In unserem Kontext ist vor allem der erste Aufsatz interessant: Claus Grupen: Die Natur des Zufalls. S. 15-33.

23 Claude E. Shannon: Communication Theory of Secrecy Systems. Bell Systems Technical Journal 28 (1949) S. 656-715.

24 Bauer: Entzifferte Geheimnisse. S.470.

25 Kittler: Typewriter. S. 273.

26 Walter Rouse Balls: Mathematical Recreations. Zitiert nach Hodges: Turing: Enigma. S. 193.

27 Ebenda.

Enigma – die erste mechanische Chiffriermaschine?

In den 20er Jahren des 20. Jahrhunderts wurde eine Vielzahl von kryptografischen Erfindungen patentiert, wie Devours/Kruh in einer quantitativen Untersuchung der Patente zum Thema Kryptografie und Kryptografie-Maschinen nachgewiesen haben. Dieselbe Statistik verzeichnet einen erneuten Anstieg der Patente ab 1950 und eine noch steilere Zunahme nach 1970.[28]

Die Enigma war nicht die erste mechanische Chiffriermaschine, aber die erste, die kommerziell Erfolg hatte.[29] Zentrales Element der Enigma sind ihre Rotoren, und solche Rotoren oder Walzen standen im Mittelpunkt der Ideen dreier Erfinder, die unabhängig voneinander auf die Idee zur Konstruktion einer Chiffriermaschine gekommen waren.

- Alexander Koch liess das Prinzip der Rotor-Verschlüsselung am 7. Oktober 1919 in Holland patentieren – als ›Geheimschrijfmachine‹ unter Patent Nr. 10 700. Zu den Besonderheiten seiner Erfindung zählte die sogenannte Umkehrwalze. Er glaubte, dass seine Erfindung ein gewisses kommerzielles Potential hatte, und überschrieb die Patentrechte 1927 an Arthur Scherbius. Ein Jahr später verschied er.[30]
- In Schweden erhielt Arvid Damm 1919 ein ähnliches Patent und versuchte verschiedene Maschinen zu bauen, was ihm nur teilweise gelang (Patent Nr. 52 279). Aber: Der Schwede Boris Hagelin kannte Arvid Damm und entwickelte aus dessen Grundidee seine Chiffriermaschine C-36, die zuerst von den Franzosen gekauft wurde. 1940 erwarben auch die Amerikaner eine Lizenz und entwickelten daraus die M-209, gebaut von der Schreibmaschinen-Fabrik Smith & Corona. Boris Hagelin verliess nach dem Zweiten Weltkrieg Schweden und liess sich in der Schweiz nieder, wo er 1952 die heute noch aktive Crypto AG gründete.[31]

---

28 Cipher A. Deavours; Louis Kruh: Machine Cryptography and Modern Cryptoanalysis. Norwood 1985. S.1-2.

29 Ebenda S. 10.

30 David Kahn: The Codebreakers. S.420. Deavours/Kruh: Machine Cryptography. S. 3-10.

31 Zur Geschichte der Firma Crypto AG existiert nur sehr wenig Literatur. David Kahn gibt in seinem Standardwerk ›The Codebreakers‹ einen kurzen Abriss. Die Firma Crypto AG selber veröffentlichte im Jahr 1992 zum 100-jährigen Geburtstag des 1983 verstorbenen Firmengründers eine kurze Firmengeschichte, die allerdings bereits in den frühen 50er Jahren

- Der Amerikaner Edward Hebern entwickelte zwischen 1912 und 1920 verschiedene kryptografische Apparate, die er patentieren liess, und baute auch eine Fabrik für solche Geräte. Es gelang ihm Ende der 20er Jahre, einige seiner Maschinen an die Navy zu verkaufen. Nach einem kompletten Misserfolg mit einer neuen Maschine im Jahr 1934 hörte die Navy auf, mit ihm Geschäfte zu machen. Hebern klagte später, dass man ihm seine Ideen gestohlen habe. Er starb 1952 und erhielt posthum 30 000 USD für seine Ideen. David Kahn: »Hebern deserved better. His story, tragic, unjust, and pathetic, does his country no honour.«[32]

Bemerkenswert: Das verrückteste der geschilderten Konzepte erreichte das Patentamt nur gerade drei Tage nach dem klarsten: Arvid Damm reichte sein Patent in derselben Woche ein wie Koch, nämlich im Oktober 1919.[33]

1918 erwarb der Deutsche Arthur Scherbius ein erstes Patent. Zusammen mit Julius Ritter gründete er 1918 die Firma Scherbius und Ritter. 1925 begann die Serienfertigung der Enigma, die es in drei verschiedenen Ausführungen gab:[34]

- Modell A: So gross wie eine Registrierkasse.
- Modell B: Erstmals Koppelung mit einer normalen Schreibmaschine.
- Modell C: Portables Modell, das mit Lampen ausgestattet war.

Scherbius selber starb 1929 nach einem Unfall mit einer Pferdekutsche. 1934 wurden die Titel seines Betriebs an eine neue Firma übertragen: Heimsoeth und Rinke.

---

abbricht. Behandelt wird nur die Ära der mechanischen, nicht aber der elektro-mechanischen und elektronischen Chiffriergeräte. Die Crypto AG hat anfangs 90er Jahre von sich reden gemacht, als ihr Verkaufsingenieur Hans Bühler während sechs Monaten im Iran inhaftiert war. Die Firma Crypto AG wurde immer wieder beschuldigt, in ihre Software sogenannte Hintertüren für den US Geheimdienst einzubauen. Der Vorwurf taucht in zahlreichen im Internet kursierenden Verschwörungstheorien auf, konnte aber bisher nie bewiesen werden. Die Kontroverse wirkt bis auf den heutigen Tag nach. Vgl. dazu auch: Res Strehle: Verschlüsselt. Der Fall Hans Bühler. Zürich 1994. Werd Verlag.

32 Kahn: The Codebreakers. S. 420.

33 Ebenda.

34 Louis Kruh, Cipher Devours: The Commercial Enigma. Beginning of Machine Cryptography. In: Cryptologia. 26/1 (2002) S. 1-16.

Im militärischen Kontext relevant wurde einzig Modell C, als mobiles Gerät war es wesentlich kleiner als die beiden anderen, allerdings benötigte es eine Stromquelle in Form einer Batterie. Die anderen Varianten gerieten schnell in Vergessenheit. Von diesem mobilen Modell existieren verschiedene Varianten für Wehrmacht, Post, Eisenbahn und die Marine. Schliesslich wurde auch eine Version für kommerzielle Zwecke gebaut.[35]

Wieviele solcher Maschinen wurden überhaupt gebaut? Eine Frage, die nicht nur für Historiker, sondern auch für Sammler von Bedeutung ist. Schätzungen variieren zwischen 40 000 und 200 000 Geräten. Bauer geht von einer Zahl von 100 000 aus.[36]

Das Prinzip der Enigma war einfach und robust und diente deshalb auch für verschiedene Weiterentwicklungen in anderen Ländern als Vorbild: So geht die in England benutzte Typex Maschine auf die Enigma zurück, ebenso die amerikanische M-325, die allerdings unter Feldbedingungen nicht befriedigte, sowie eine japanische Maschine, die unter dem Namen ›Green‹ bekannt wurde.[37]

Fast ebenso erfolgreich, wie das Konzept der Enigma mit Rotoren und einem elektrischen Stromkreis war, zeigte sich die auf Arvid Damm zurückgehende Konstruktion einer rein mechanischen Chiffriermaschine, die Boris Hagelin übernahm und weiterentwickelte: Frankreich, Russland und Schweden bauten ihre Chiffriermaschinen nach diesem Prinzip.[38]

35 Hamer/Sullivan/Weierud unterscheiden im Einzelnen: Wehrmacht-Enigma benutzt von Land- und Luftstreitkräften; Marine-Enigma in zwei Varianten mit 3 respektive 4 Walzen; Abwehr-Enigma und schliesslich die kommerziell vertriebene Enigma D und K, die auch von der Eisenbahn und der Post benutzt wurde. Dieser Typ Maschine wurde auch an die Schweiz verkauft. David H. Hamer; Geoff Sullivan; Frode Weierud: Enigma Variations. An Extended Family of Machines. In: Cryptologia. 22/3 (1998) S. 211-223.
Heinz Ulbricht: Die Chiffriermaschine Enigma. Trügerische Sicherheit. Ein Beitrag zur Geschichte der Nachrichtendienste. Braunschweig 2004.

36 Friedrich L. Bauer: Enzifferte Geheimnisse. S.117.

37 Devours; Kruh: Machine Cryptography. S. 10.

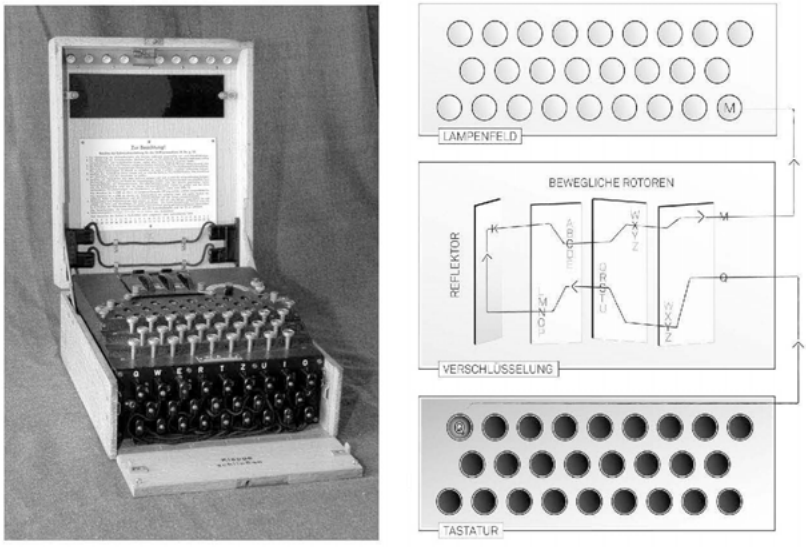
38 Ebenda S. 12.

Enigma: Eine Schreibmaschine für Geheimschriften

Die Enigma war nichts anderes als eine Schreibmaschine für Geheimschrift. Sie bestand aus drei Elementen: Der Tastatur für die Eingabe, eine im inneren der Maschine versteckte Verschlüsselungseinheit und einer Ausgabe-Einheit. Diese Ausgabe-Einheit bestand beim Kriegsmodell aus einem Lampenfeld und nicht etwa aus einem Drucker. Die Verschlüsselungseinheit im Innern der Maschine bestand aus Rotoren, die sich mit jedem Buchstaben einen Schritt weiter drehten. Wenn man zehn Mal denselben Buchstaben eingibt, erhält man also zehn Mal ein unterschiedliches Resultat. Allerdings mit einer bemerkenswerten Ausnahme: Egal wie oft derselbe Buchstabe hintereinander gedrückt wird – das verschlüsselte Resultat ist nie der Buchstabe selber. N wird niemals zu N. Diese bemerkenswerte Tatsache machten sich die Codebrecher zu Nutze. Umgekehrt liess ein Text, dessen Analyse das Fehlen eines einzigen Buchstabens zeigte, einen ganz einfachen Schluss zu: Der Operateur hatte wiederholt die Taste des gleichen Buchstabens gedrückt.

Schematisch lässt sich das so darstellen: Wenn auf dem Tastenfeld der Buchstabe K gedrückt wird, wandert ein elektrischer Strom in der Verschlüsselungseinheit durch die drei beweglichen Walzen. Dabei wird der Buchstabe durch die drei Rotoren dreimal vertauscht und kommt dann zur Umkehrwalze. Dort wird er gespiegelt und ein weiteres Mal vertauscht, bevor er dann ein zweites Mal durch die drei Rotoren geschickt wird und nochmals dreimal vertauscht wird. Das austretende Signal wird dann auf einem Lampenfeld als U abgebildet. Gleichzeitig wird bei jedem Tastendruck der Rotor um eine Position weiter bewegt. Nach 26 solchen Bewegungen wird der nächste Rotor eine Position nach vorn geschoben, ganz ähnlich wie bei einem analogen Kilometerzähler.

Abbildung 2



Chiffriermaschine Enigma und schematische Darstellung.
(Foto D.Landwehr; Schema I. Sterzinger)

Nur auf dem Foto und nicht im Schema abgebildet ist ein zusätzliches Steckerbrett, das eine erneute Vertauschung der Buchstaben ermöglichte. Diese Vertauschung war allerdings statisch – das heisst, sie wurde über eine gewisse Zeit beibehalten und war deshalb auch nicht so effektiv für die Verschlüsselung, wie man dies rein rechnerisch vermuten, respektive konstruieren könnte.

Die frühen Enigma besassen nur drei verstellbare und vertauschbare Walzen plus eine fix eingebaute Umkehrwalze. Später wurde die Anzahl der zur Verfügung stehenden Walzen auf 6, dann auf 8 erhöht – sie trugen römische Ziffern I, II III, IV, V, VI, VII und VIII. Die Marine Enigma, deren Code am schwierigsten zu knacken war, wurde 1942 mit einer zusätzlichen Walzenposition ausgerüstet, so dass dort schliesslich vier Walzen plus die Umkehrwalze im Einsatz waren. Die neue Walze wurde mit dem griechischen Buchstaben Beta bezeichnet und deshalb auch die Griechenwalze genannt.

Der erste Hersteller der Enigma rechnete aus, dass 1000 Operateure mehrere Millionen Jahre brauchen würden, um alle Möglichkeiten durchzuprobieren, was wiederum die deutschen Käufer im Glauben liess,

die Maschine sei sicher genug. Die Maschine war sehr sicher, wenn beim Übermittlungsprozess keine Fehler gemacht wurden.[39]

Vor einer Verschlüsselung musste der Operator sein Gerät folgendermassen vorbereiten – wir folgen der Darstellung von Rudolf Kippenhahn:[40]

- Er musste aus mehreren Walzen drei auswählen. Zu Beginn standen ihm dazu allerdings nur drei zur Verfügung, später waren es mehr.
- Er musste jede Walze in die vorgeschriebene Ringstellung bringen.
- Die Walzen waren in einer bestimmten Reihenfolge ins Gerät einzusetzen. Bei 3 Walzen gab es 6, bei 4 Walzen 24 Möglichkeiten.
- Danach mussten die 3 Walzen in eine Anfangsstellung gebracht werden.
- Diese Manipulation liess sich vornehmen, ohne die Maschine zu öffnen. Die Stellung der Rotoren war auch von aussen ablesbar.
- Schliesslich musste er die Steckerverbindungen schalten, respektive stöpseln.

Zur Verschlüsselung gab es einen Tagesschlüssel, der die Walzen mit berücksichtigte – das Verstellen der Walzen war eine relativ umständliche Operation – und einen Spruchschlüssel, der nur noch die Grundstellung der Walzen veränderte. Der Empfänger musste grundsätzlich dieselben Operationen vornehmen. Eine der wichtigsten Eigenschaften der Enigma bestand genau in der Tatsache, dass Verschlüsseln und Entschlüsseln zwei identische Prozesse waren, die natürlich auch mit der gleichen Maschine und denselben Einstellungen vorgenommen werden mussten.[41]

Die Entschlüsselung der Enigma

Ohne auf die mathematischen Permutationsmöglichkeiten näher einzugehen, lässt sich doch sagen: Bei aller Komplexität erzeugte diese Ver-

39 Die Autoren Deavours und Kruh kommen zum Schluss, dass die kryptografischen Maschinen der Achsenmächte genau so adäquat und sicher waren wie die Maschinen der Alliierten und schwer zu knacken. Beide basierten auch auf denselben Prinzipien. Die Alliierten waren aber strenger und konsequenter im Einhalten von Protokollen und Richtlinien. Devours/Kruh: Machine Cryptography S. 20.

40 Rudolf Kippenhahn: Verschlüsselte Botschaften. Geheimschrift, Enigma und Chipkarte. Hamburg 1997. Rowohlt. S. 213-214.

41 Ebenda.

schlüsselungsmaschine[42] vorhersagbare Resultate. Aber mit den damaligen Mitteln waren solche Botschaften nicht zu entziffern; erst der massive Einsatz von modernster Computertechnik vermag diese Technologie in die Knie zu zwingen.

Warum gelang die Entschlüsselung trotzdem? Zwei grundlegende Faktoren sind zu nennen: Systematische und wiederholt begangene Fehler auf der Seite Deutschlands und der Achsenmächte – und äusserste Entschlossenheit und eine Konzentration der verfügbaren Ressourcen auf der Seite der Alliierten, vor allem der Briten.

Die Entschlüsselung der Enigma gelang nicht nur aufgrund der Genialität und des Einfallsreichtums der Beteiligten, allen voran Alan Turing. Es brauchte mehr als das. Verrat und Spionage auf der Seite der Angreifer gehörten ebenso dazu wie Ignoranz auf der Seite der Angegriffenen. Es brauchte klug geplante und brachial durchgeführte Kapermanöver von Schiffen, aber schliesslich auch Maschinen, die stur Millionen von Möglichkeiten durchrechnen konnten.

In der Entschlüsselung lassen sich drei verschiedene Perioden unterscheiden:

- In den 30er Jahren bis zum Ausbruch des Krieges 1939 waren polnische Mathematiker in Warschau führend.
- 1939 bis 1943 operierten britische Spezialisten vom geheimen Standort Bletchley Park aus – zunächst allein.
- Ab 1943 wurden sie dabei von US Spezialisten unterstützt, die ihre Operationen in Washington D.C. durchführten.

Die polnischen Pioniere

Die Enigma wurde in Deutschland bereits ab 1926 eingesetzt. Funksprüche, die mit diesem Gerät verschlüsselt wurden, waren von diesem Zeit-

42 In der Kryptologie wird zwischen Entschlüsseln und Entziffern unterschieden: Für das Entschlüsseln muss ein Schlüssel vorliegen. Der Begriff des Entzifferns bezeichnet den Vorgang, den Klartext ohne Kenntnis der Regeln mittels Analyse zu ermitteln. In Bletchley Park wurde beides gemacht: Es wurden Texte entziffert und mit dem daraus gewonnenen Schlüssel zahlreiche weitere Texte entschlüsselt (Schriftliche Mitteilung von Oskar Stürzinger an den Autor vom 27.1.2007). In der vorliegenden Untersuchung werden die Begriffe aber, näher an der umgangssprachlichen Bedeutung, synonym verwendet.

punkt an auch für die Spezialisten nicht mehr lesbar. Als erstes gelang es den Polen, solche Nachrichten zu entschlüsseln.

Verantwortlich war dort Maximilian Ciezki. Er hatte eine kommerzielle Enigma, stand aber auch damit bald vor Rätseln, die er nicht mehr lösen konnte. Über den französischen Geheimdienst kamen die Polen an Dokumente des Beamten Hans Thilo Schmid, die weitere wichtige Hinweise lieferten. Ein entscheidender Durchbruch gelang den Polen, als man begann, Mathematiker für die Aufgabe des Entschlüsselns zu rekrutieren: Jerzy Rozycki, Henryk Zygalski und Marian Rejewski. Die Enigma, so dachte man, wäre schliesslich eine mechanische Verschlüsselungsmaschine und deshalb für einen naturwissenschaftlichen Geist eher zugänglich.[43] Unter den Neuen war Marian Rejewski. Er stützte sich in seiner Arbeit hauptsächlich auf die Beobachtung, dass die Wiederholung der Feind der Geheimhaltung ist. Die Deutschen wiederholten den Spruchschlüssel am Anfang, um Irrtümern zu begegnen. Die Polen arbeiteten zunächst mit einem von Hand erstellten Katalog, danach mit einem System von Blättern, den sogenannten Zygalski-Sheets und schliesslich mit einer Maschine, welche das Durchprobieren der Kombinationen übernahm und die von ihnen Bomba oder Bombe genannt wurde. Man dachte bei dieser Namensgebung offenbar weniger an eine Explosiv-Bombe als vielmehr an eine Eis-Bombe.[44] Dank ihren Erkenntnissen konnten die Polen jahrelang deutsche Nachrichten abhören – so auch als Göring 1934 Warschau besuchte.

43 Simon Singh: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München 1999. Hanser. S.186.

44 Eine ausführliche Beschreibung der Arbeit der polnischen Spezialisten findet sich bei David Kahn: The Codebreakers. S. 973 ff; bei Friedrich L. Bauer S. 411-22 und auch auf den Internet Seiten von Tony Sale: www.codesandciphers.org.uk/virtualbp/poles/poles.htm vom 16.2.2008. Ausserdem: W. Kocaczuk: Geheimoperation Wicher. Polnische Mathematiker knacken den deutschen Funkschlüssel Enigma. Bonn 1999. Bernard & Graefe Verlag.

Government Code and Cipher School und Bletchley Park

1938 kamen zu den drei bisherigen zwei neue, austauschbare Walzen: Das bedeutete, dass es nun für die Enigma fünf Walzen für drei Positionen gab. Dies führte zu sechzig möglichen Rotorlagen anstelle von bisher sechs.[45] Zwar wussten die Polen um Rejewski, was zu tun gewesen wäre – allein ihnen fehlten die Mittel, ihre Bomben hochzurüsten. Bei einer Konferenz in Warschau am 25. Juli 1939 präsentierten die drei polnischen Mathematiker die Resultate ihrer Bemühungen den staunenden Briten und Franzosen und schenkten ihren Gästen auch eine Replika der Enigma made in Poland.[46]

In England befasste sich eine spezielle Gruppe des Foreign Service mit der Entschlüsselung von chiffrierten Botschaften. Sie hatten ihre Adresse zuerst in Westminster (Adresse 56 Broadway Whitehall) und arbeiteten in einem als ›Room 40‹ bezeichneten Zimmer. Aus naheliegenden Gründen verlegten sie ihren Dienst nach Kriegsbeginn ausserhalb der Stadt. Die Wahl fiel dabei auf ein grosszügiges Landhaus genau zwischen Oxford und Cambridge, Bletchley Park genannt.

Die Bilder des im Tudor Stil gebauten Landhauses von Bletchley Park erscheinen heute fast als Ikone. Wer sich mit dem Thema befasst, stösst sofort auf das Bild dieses Hauses und wird es später mit der Entschlüsselung der Enigma in Verbindung bringen. Das Bild des Hauses trägt mit zur Vorstellung bei, dass die Entschlüsselungsoperation die Angelegenheit einer kleinen, überschaubaren Gruppe von Leuten gewesen war. Tatsächlich arbeiteten die ersten Mitarbeiter dieser Behörde in diesem Haus. Der Dienst wuchs aber bald an und am Ende des Krieges gingen täglich bis zu 10 000 Personen auf dem Gelände ein und aus. Die meisten lebten allerdings nicht hier, sondern in Unterkünften in der Nachbarschaft.

45 Friedrich L. Bauer: Entzifferte Geheimnisse. S. 417.

46 Ebenda S. 221.

Abbildung 3

Das Mansion von Bletchley Park präsentiert sich heute rein äusserlich noch genau so wie vor 60 Jahren. Die Anlage war allerdings sehr weitläufig und bestand zum grösseren Teil aus Baracken und einfachen Zweckbauten, von denen heute noch einige wenige zu sehen sind. (Fotos D. Landwehr)

Die neue Behörde gab sich den Namen ‹Government Code and Cipher School› – sie war alles andere als eine gewöhnliche Dienststelle und schon gar keine streng militärische Organisation – wie etwa Görings Luftfahrts-Forschungsamt – sondern »eine lose Sammlung von Gruppen, von der jede die Dinge improvisiert vorantrieb und sich aufs Beste bemühte, den relevanten militärischen Köpfen etwas Vernunft einzubleuen, bevor es zu spät war.«[47] Kaum ein Autor unterlässt es, auf die Heterogenität der hier beschäftigten Spezialisten hinzuweisen. Neben den Mathematikern und Linguisten gab es auch noch Porzellanspezialisten, einen Kurator vom Prager Museum, den britischen Schachmeister und zahlreiche Bridge Experten. Bei einem Besuch soll Churchill dem Chef des Secret Intelligence Service ins Ohr geflüstert haben: »Ich habe sie angewiesen, jeden Stein umzudrehen, aber dass sie mich so wörtlich nehmen, hätte ich nicht erwartet.«[48]

Bei allen skurrilen Details darf nicht übersehen werden: Bletchley Park war ein Ort der Arbeit und ein grosser Teil der Arbeit muss aus stumpfsinniger Routine bestanden haben, deren Sinn allerdings das Opfer der Langeweile mehr als rechtfertigte. Unter den Persönlichkeiten, die ihren Weg nach Bletchley Park gefunden hatten, waren mehrere namhafte Wissenschafter, allen voran der Mathematiker Alan Matheson Turing. Zusammen mit anderen vermittelte er der Entschlüsselungsarbeit entscheidende Ideen. Die überwiegende Mehrheit der hier Tätigen waren al-

47 Andrew Hodges: Turing. S. 236.

48 Simon Singh: Geheime Botschaften. S. 226.

lerdings nicht Männer, sondern Frauen und sie arbeiteten in untergeordneten, aber unerlässlichen Funktionen.

Die Operation von Bletchley Park – auch Ultra genannt – knüpfte an die Ergebnisse der polnischen Spezialisten an, ergänzte sie mit eigenen Beobachtungen. Man konstruierte schliesslich eine Maschine, die der polnischen Bombe nicht unähnlich war und im Grunde demselben Zweck diente: Dem mechanischen Durchprobieren von möglichen Kombinationen. Dies war nur möglich, wenn man bereits vor dieser Operation mindestens einen Teil des chiffrierten Textes entschlüsseln konnte. Dafür bedurfte es präziser Beobachtung, Imagination und Kenntnisse der deutschen Vorgehensweise. Wetterbeobachtungen oder ritualisierte Eröffnungsformeln boten willkommene Anhaltspunkte für solche Wörter, die ›Cribs‹ genannt wurden.

Die Arbeit der britischen Spezialisten führte in vielen Fällen zum Erfolg und wurde auch entsprechend gewürdigt. Trotzdem fehlte es an Mitteln, um schneller und effektiver arbeiten zu können. In dieser Situation gelangte eine Gruppe von Bletchley Park Mitarbeitern an den britischen Premierminister Winston Churchill persönlich. Man bat ihn – unter Umgehung des Dienstweges – um zusätzliche Mittel: »We find it hard to believe that it is really impossible to produce quickly the additional staff that we need, even if this means interfering with the normal machinery of allocation.«[49]

Die Antwort von Winston Churchill hat Geschichte gemacht. Sie bestand nur aus zwei Sätzen: »Action this day. Make sure they have all they want on extreme priority and report to me that this has been done.«[50]

49 Andrew Hodges: Turing. S. 220.

50 Ebenda S. 221.

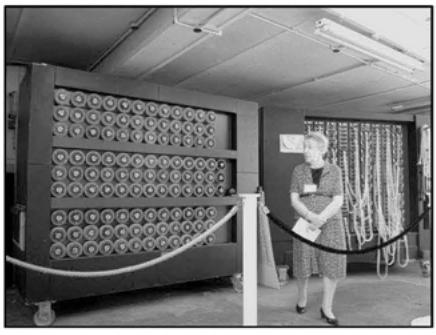


Abbildung 4

Die Replica einer Bombe aus Bletchley Park. Die Museumsführerin Jean Valentine im Vordergrund gehörte im Krieg zu den Operateurinnen dieses Gerätes. (Foto D. Landwehr)

Elektromechanische Hilfsmittel - die Bomben

Die Methoden der britischen und später amerikanischen Kryptoanalytiker zum Knacken des Enigma-Codes können hier nur sehr summarisch dargestellt werden, sie sind aber in der Literatur vielerorts ausführlich dokumentiert.[51]

Im Mittelpunkt standen Bemühungen möglichst viel Material zu erhalten, so dass damit die Anzahl der theoretisch möglichen Kombinationen reduziert wurde. Was übrig blieb, war von Hand immer noch nicht zu bewältigen – aber eigens konstruierte Maschinen halfen hier nach: Die sogenannten Bomben, die Alan Turing analog zu den Apparaten der polnischen Spezialisten entwickelte. Seine Bomben hatten eine ähnliche Funktion: Sie konnten Steckerverbindungen sowie die Walzenlage ermitteln. Sie taten dies allerdings nicht direkt, sondern arbeiteten nach dem Ausschlussverfahren. Jene Kombinationen, die übrig blieben, mussten von Hand getestet werden.

Das Gerät bestand aus einer Serie von Enigma-Replicas ohne Steckerbrett. Sie waren miteinander verbunden. Getestet wurden alle 17 576 möglichen Walzenpositionen. Die erste dieser Maschinen wurde 1940 eingesetzt. Im Frühjahr 1941 waren 8 Bomben in Betrieb, im August 1942 bereits 60 und am 30. März 1943 schliesslich deren 300.[52] Hergestellt wurden sie von der British Tabulating Machine Company in Letchworth. Nach dem Besuch von Alan Turing Ende 1942 begannen

51 So unter anderem bei Friedrich L. Bauer: Entzifferte Geheimnisse. S. 421-435; Andrew Hodges: Turing. S. 187-299. Auch bei Tony Sale: http://www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm vom 16.2.2008. Besonders ausführlich: Hugh Sebag-Montefiore: Enigma. The Battle for the Code. London 2000. Phoenix. S. 370-426.

52 Friedrich L. Bauer. Entzifferte Geheimnisse. S. 431.

auch die amerikanischen Verbündeten solche Maschinen zu nutzen und herzustellen. Trotz grossem Druck wurden von NCR die ersten dreizehn Geräte erst im Juli 1943 fertig gebaut. Ende 1943 waren 50 Bomben gebaut und weitere 30 in der Produktion. Ab Dezember 1943 dauerte die Entzifferung eines Enigma-Spruches noch rund 18 Stunden – ein halbes Jahr zuvor waren es noch 600 Stunden gewesen.

Die Rolle der Schiffsüberfälle

Die Entschlüsselung der Enigma war nicht nur die Leistung der klugen Köpfe von Bletchley Park. Ohne militärische Erfolge wäre es kaum möglich gewesen, die Maschine zu entschlüsseln. Entscheidend waren die Operationen im Atlantik und in der Nordsee. Dort gelangen den Briten spektakuläre Aktionen, im Lauf derer sie zu wichtigem Geheimdienstmaterial gelangten: Codeschlüssel, Rotoren und weitere Unterlagen. Der amerikanische Publizist David Kahn hat diese Kaperungen im Buch »Seizing the Enigma« ausführlich beschrieben.[53] Die wichtigsten Aktionen sind hier kurz zusammengefasst:

- Am 11. Februar 1940 begegnet das britische Minensuchboot HMS Gleaner dem deutschen U-Boot U-33. Das U-Boot wird zuerst mit Wasserbomben kampfunfähig gemacht und zum Auftauchen gezwungen. Der britischen Crew gelingt es, die Schiffbrüchigen aufzufischen. Bei der näheren Untersuchung der Geborgenen stellt sich heraus, dass einer der Crewmitglieder vergessen hatte, zwei Enigma-Rotoren wie befohlen ins Meer zu werfen. Es handelt sich um die bisher unbekannten Rotoren VI und VII. Rotor VIII wurde später bei einem ähnlichen Zwischenfall gefunden.[54]
- Am 26. April 1940 gelang es der Besatzung des britischen Zerstörers Arrow einen Leinensack mit wertvollem Enigma-Material zu bergen; der Sack wurde wahrscheinlich vom deutschen Fischerboot Polaris, das einen militärischen Auftrag hatte, über Bord geworfen.[55]
- 7. Mai 1941: Eine besondere Rolle für die deutsche Kriegsführung spielte die Wetterbeobachtung. Weil das Wetter immer vom Westen nach Osten kam, mussten weit im Meer draussen Schiffe stationiert werden, die das Wetter beobachteten und weitermeldeten. Das Ober-

53 David Kahn: Seizing the Enigma. The Race to Break the German U-Boat Codes. 1939-1943. London 1992. Souvenir Press.

54 Ebenda S. 100-111.

55 Ebenda S. 116-117.

kommando betrachtete solche Schiffe nicht als Kriegsschiffe und liess sie von einer zivilen Crew betreiben. Trotzdem waren sie mit Chiffriersystemen – dazu gehört auch ein Wetterkurzschlüssel – ausgerüstet. Diese Tatsache entdeckten die Codespezialisten von Bletchley Park bereits im Frühjahr 1941. Eine entsprechende Operation wurde vorbereitet und am 7. Mai 1941 gelang es, zwei Wetterschiffe aufzubringen. Sie hatten zwar die Enigma-Maschinen bereits über Bord geworfen, die Schlüssel jedoch konnten geborgen werden.[56]

- 9. Mai 1941: Eine wichtige Rolle spielt auch die Begegnung mit dem deutschen U-Boot U-110. Das Schiff wurde ebenfalls von einem britischen Zerstörer aufgebracht. Die britischen Matrosen konnten das leck geschossene U-Boot unter Lebensgefahr entern und wichtige Dokumente bergen. Die Geschichte lieferte den Rohstoff für den Hollywood Film U-571, in dem der Ruhm der heldenhaften Angreifer allerdings einem US Schiff zugeschrieben wird.[57]

Eher von anekdotischem Wert – gerade in unserem Kontext aber wertvoll – war der Plan für eine abenteuerliche See-Operation, die nie ausgeführt wurde. Die originelle Idee wurde vom Assistenten des Direktors des Marine-Nachrichtendienstes vorgebracht, einem »imaginative civilian«, wie David Kahn ihn nennt. Seine Operation ›Ruthless‹ sah vor, dass die Briten ein erbeutetes deutsches Flugzeug im Ärmelkanal in der Nähe eines deutschen U-Bootes würden notwassern lassen. Es würde Hilfesignale aussenden und sich von einem deutschen Schiff retten lassen. Die Fortsetzung liest sich wie ein Drehbuch: »Once aboard rescue boat, shoot German crew, dump overboard, bring rescue boat back to English port«. Die Idee erwies sich in der Folge als undurchführbar und wurde aufgegeben. Andere Ideen dieses phantasievollen Zivilisten wurden nach dem Krieg umgesetzt – und zwar in geeigneterer Form: Bei diesem phantasievollen Assistenten handelte es sich nämlich um Ian Fleming, den Erfinder der Roman- und Filmfigur James Bond.[58]

56 Ebenda S.127-136.

57 Ebenda S.170-182.

58 Ebenda S.127. Vgl. Simon Winder: The Man who Saved Britain. A Personal Journey into the Disturbing World of James Bond. London 2006. Picador.

Kryptografie wird zur mathematischen Wissenschaft

Das Knacken der Enigma hat neben der historisch-politischen auch eine kulturhistorische Bedeutung: Mit der Operation Ultra hatte sich nämlich die Mathematik endgültig als Königsdisziplin in der Kryptografie, respektive in der Kryptoanalyse etabliert. Das mag aus heutiger Sicht banal erscheinen. Die Kryptografie als Wissenschaft steckte noch am Ende des Ersten Weltkrieges in den Kinderschuhen. Zwar unterhielten die Grossmächte spezialisierte Chiffrier-Dienste. Aber ihre Methoden waren mit einfachen Mitteln zu durchbrechen. Kryptografie war keine etablierte Wissenschaft, die Kenntnisse darin waren bescheiden.

Die wenigen Spezialisten waren in der Regel Sprachwissenschafter oder Leute, die im weitesten Sinn mit Sprache zu tun hatten. Das darf nicht erstaunen – bei der Chiffrierung ging es ja um die Verschlüsselung von sprachlichen Mitteilungen. Das galt etwa für die Briten, die 1914 einen ersten kryptografischen Dienst gründeten, der in der Admiralität von London im Raum 40 untergebracht war. Dort arbeiteten in erster Linie Philologen unterschiedlichster Provenienz, Historiker und auch ein Archäologe[59]. Ähnlich in den USA: 1921 gründete dort Herbert Osborne Yardley (1889-1958) einen Dienst, der unter dem Namen ›Black Chamber‹ berühmt wurde.[60] William Friedman (1891-1961), der Pionier der amerikanischen Kryptografie, hatte seine erste Anstellung bei einem exzentrischen Textilhändler namens George Fabyan, der sich zum Vergnügen eine kryptologische Abteilung aufbaute mit dem Ziel zu beweisen, dass Bacon der Verfasser der Texte von Shakespeare war.[61]

Modernen Chiffrierverfahren ist nur mit Mathematik beizukommen. Die ersten, die dies erkannten, waren die Polen:

»Die Angriffspitze gegen die Enigma bildete ein neuer Typ von Kryptoanalytikern. Jahrhundertelang hatte man angenommen, die besten Kryptoanalytiker wären Sprachwissenschaftler, doch als die Enigma auf die Bühne kam, änderten die Polen ihre Rekrutierungsstrategie. Enigma war eine mechanische Verschlüsselung und im ›Biuro Szyfrow‹ (Chiffrierbüro DL) kam man zu dem Schluss, ein eher naturwissenschaftlicher Geist hätte vielleicht eine grössere Chance sie zu knacken. Das ›Biuro Szyfrow‹ organisierte einen Kryptografie-

59 David Kahn: The Codebreakers. S. 274.

60 Ebenda S.351.

61 Ebenda S.370.
Ausserdem: William F. Friedman und Elizabeth S. Friedman: The Shakespearean Ciphers Examined. Cambridge 1957. Cambridge University Press.

Lehrgang und lud dazu 20 Mathematiker ein, die man auf Stillschweigen einschwor.«[62]

Mathematik ergänzte und ersetzte nach und nach die Methoden der Sprachwissenschaft. Dieser Vorgang – die mathematische Umschreibung von Sprache – darf nicht unterschätzt werden. Sie stellt einen Baustein dar, der später auch zur Grundlage der digitalen Umsetzung von Sprache wurde. Und auch dieser Schritt wurde in Bletchley Park – allerdings in einem anderen Kontext – vollzogen: Die Colossus – gebaut mit 1500 Rundfunkröhren – ermöglichte die Entzifferung des Funkfernschreibers, den Nazi-Deutschland für die Verschlüsselung und Übertragung von Nachrichten auf oberster Ebene benutzte. Colossus war der erste digitale Röhrenrechner.[63]

Der Erfolg von Ultra

Operation Ultra war ohne Zweifel ein Erfolg für die Briten und die Alliierten. Bis Ende 1943 beherrschten die deutschen U-Boote mit ihrer von Admiral Dönitz erfundenen Taktik der Wolfsrudel-Attacke den Nordatlantik und versenkten alliierte Schiffe zu Dutzenden. Die Taktik der deutschen U-Boot Jäger war denkbar einfach und wirkungsvoll: Zunächst verteilten sich die U-Boote im Nordatlantik. Wurde ein alliierter Konvoi gesichtet, so wurden so viele U-Boote wie möglich zusammengezogen, um dann einen konzertierten Angriff zu führen. In einzelnen Fällen wurden so 50 und mehr U-Boote für einen Angriff versammelt.[64]

Es war vor allem ›Ultra‹ zu verdanken, dass die Schiff-Konvois, die Grossbritannien mit fast allen lebensnotwendigen Gütern versorgten, ab 1943 mit zunehmender Sicherheit passieren konnten.

Hier zeigt sich ein weiterer Aspekt der informationstheoretisch interessant ist: Ultra lief Gefahr, Opfer seines eigenen Erfolges zu werden, und musste mit aufwendigen Massnahmen geschützt werden. Informationstheoretisch interessant ist auch die an sich banale Beobachtung, dass es nicht reicht, die gegnerischen Funksprüche zu entziffern, sie müssen auch noch verstanden werden.

---

62 Simon Singh: Geheime Botschaften. S. 186.

63 Tony Sale hat einen Nachbau der Maschine in Bletchley Park eingerichtet: www.codesandciphers.org.uk/lorenz/rebuild.htm vom 16.2.2008. Jack Copeland: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford 2006. Oxford University Press.

64 Eine detaillierte Liste mit der Aufzählung aller derartigen Überfälle findet sich hier: http://uboat.net/ops/convoys/battles.htm vom 16.2.2008.

»Auf einer Maschine basierend und durch eine Maschine entschlüsselt, wurden die chiffrierten Enigma-Meldungen mechanisch direkt in normale Sprache verwandelt, so dass sie ein Endprodukt von füllhornartigem Überfluss erbrachten, sobald einmal die tägliche Einstellung gelöst war.«[65]

Die Aktensysteme von Bletchley Park mussten das Deutsche Kommandosystem widerspiegeln, um dem Chiffrierverkehr als Ganzem eine Bedeutung zu geben. Es wird geschätzt, dass 15 bis maximal 29 Prozent des deutschen Fernmeldeverkehrs über die Enigma abgewickelt wurde. Weitere 40 Prozent wurden schätzungsweise vom Siemens Geheimschreiber kodiert und ebenfalls in Bletchley Park mit einer Maschine namens Colossus entziffert.[66] Richtig zusammengesetzt liessen die abgefangenen Botschaften eine Rekonstruktion des gesamten feindlichen Nachrichtensystems zu.

Von Admiral Dönitz wird berichtet, dass er ein konstantes Misstrauen gegenüber der Sicherheit der Enigma gehabt hat. Trotzdem konnte oder wollte man sich nicht vorstellen, dass die Enigma nicht sicher war, dass ihr Code gebrochen werden konnte: »They failed to imagine that scores of speedy, brute force codebraking machines might be used: their own few cryptoanalytic mechanisms were much more primitive.«[67]

Über die Frage, was insgesamt der Wert von Operation Ultra war, wird immer wieder spekuliert. Die Historiker sind sich im allgemeinen darüber einig, dass diese Operation den Verlauf des Krieges erheblich beeinflusst und verkürzt hat. Wäre es den Deutschen gelungen, bis 1945 weiter zu kämpfen, so hätte die erste Atombombe möglicherweise nicht Hiroshima, sondern Berlin getroffen.[68]

Die Operation Ultra rettete Menschenleben – eine Feststellung, die verschiedene Autoren immer wieder machen, so auch David Kahn. Die pathetische Färbung wird uns im dritten Kapitel noch ausführlicher beschäftigen.

»One day during the war, a can of spam appeared on the table of Leonard Forster, a translator in Hut 4. ›Look‹, said his wife ›here's this new thing that's come from America.‹ When he saw the can Forster felt a great swelling of pride. For he had had a hand in getting that food to Britain. Ultra had helped bring food to his table and to millions of others in Britain. It was one of the

65 Friedrich Kittler: Die künstliche Intelligenz des Weltkriegs: Alan Turing. In: Ders./Georg Christoph Tholen (Hg.): Arsenale der Seele. Literatur- und Medienanalyse seit 1870. München 1989. Fink. S. 197

66 Ebenda.

67 David Kahn: Seizing the Enigma. S. 279.

68 Ebenda S. 278.

great intellectual achievements of the century, no less remarkable because it was achieved against a secret produced by men rather than one of nature. The unraveling of the Enigma was the equivalent of those endeavors that are awarded Nobel prizes. And, like those, it benefited humankind by bringing peace closer, Ultra shortened the time that fathers were separated from their children, husbands, from wives. And it spared an untold number of people: men in cargo ships and their escorts, men at the fighting fronts, men and children under the bombs in the cities of the home fronts. That was Ultra's greatest gift: it saved lives. Not only British and American lives, but German lives as well. That is the debt the world owes the Bletchley codebreakers that is the crowning human value of their triumphs.«[69]

Kein Geheimnis: Die Schweizer Enigma

Stützte sich der erste Teil dieses Kapitels primär auf gedrucktes und publiziertes Material, so verhält es sich im zweiten Teil nun anders: Über die Geschichte der Schweizer Enigma und ihres ›Nachfolgemodell‹ ist nur sehr wenig publiziert worden. Die Untersuchung stützt sich deshalb stärker auf Interviews und Archivmaterialien.

Bei meiner Suche haben mich verschiedene Personen freundlich unterstützt. Dazu gehören unter anderem der ehemalige Schweizer Nachrichtendienstmann Rudolf J. Ritter,[70] der Elektroingenieur Frode Weierud[71] oder der damalige Leiter der Kryptografie-Dienste der Schweizer Armee, Peter Nyffeler.[72] Paul Glur in Bern war der letzte zum Zeitpunkt der Recherchen noch lebende Zeitzeuge aus dem inneren Kreis der Schweizer Kryptologen des Zweiten Weltkrieges, der für diese Arbeit befragt werden konnte.[73]

---

69 Ebenda S. 282.

70 Rudolf J. Ritter: Das Fernmeldematerial der Schweizerischen Armee seit 1875. 10. Folge: Codes und Chiffrierverfahren. Bern 2002. Publikationen des Generalstabs. Untergruppe Führungsunterstützung.

71 Vgl. dazu die Publikationen von Frode Weierud in der Bibliografie. Sowie: http://frode.home.cern.ch/frode/ vom 16.2.2008.

72 Peter Nyffeler war bis zum Jahre 2003 Leiter des Kryptografiedienstes der Schweizer Armee, genauer im Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). Er hat den Autor verschiedene Male zu Gesprächen empfangen und auch Geräte für Demonstrations- und Dokumentationszwecke ausgeliehen!

73 Das Gespräch mit Paul Glur (1917-2007) fand am 1.Oktober 2001 in Bern statt. Der liebenswürdige Berner Mathematiker verstarb am 2. Dezember 2007, kurz vor der Drucklegung dieser Arbeit.

Zu den wenigen gedruckten Arbeiten zum Thema gehört mein eigener Artikel, der im November 2001 in der Neuen Zürcher Zeitung erschienen ist.[74] Ein erster Aufsatz zu diesem Thema war im selben Jahr, am 5. Januar 2001, in der Westschweizer Tageszeitung Liberté zu lesen.[75] Die technischen Aspekte der Schweizer Enigma sowie ihres Nachfolgemodells sind zuvor im bereits erwähnten Aufsatz von Frode Weierud beschrieben worden.[76] Schliesslich hat Rudolf J. Ritter in seiner militärgeschichtlichen Publikation erhellende Hintergründe zur Schweizer Enigma publiziert. Nützlich erwiesen sich auch Informationen und Archivalien, die Walter Schmid zur Nema zusammengetragen hat.[77]

Stunde Null

Unsere Rückschau auf die Geschichte der Schweizer Enigma beginnt in der jüngsten Vergangenheit, in den 90er Jahren: Der 4. Mai 1994 war die Stunde Null der Schweizer Enigma. An diesem regnerischen und grauen Frühlingstag wurde das letzte Kapitel dieser Maschine im Dienst der Schweizer Armee geschrieben und ein neues eröffnet – das zweite Leben der Maschine würde sich aber nicht mehr in der Armee, sondern in den Händen von Sammlern und in den Räumen von Museen abspielen.

Die Reisenden, die an jenem Frühlingstag nach Meiringen ins Berner Oberland kamen, wurden angelockt durch eine trockene dienstliche Mitteilung, die drei Wochen zuvor vom Schweizer Verteidigungsministerium veröffentlicht worden war. Der Inhalt war nur Fachleuten verständlich und deutete auf nichts Aufregendes hin. Unter der Überschrift »Liquidations-Shop für Uem Material« konnte man lesen:

»Bis heute wurde das zu liquidierende Material je nach Anfall zu einem grossangelegten Verkauf in einem Zeughaus geführt. Zur Zeit steht aber nicht genü-

74 Dominik Landwehr: Das Rätsel der Neuen Maschine. Neue Zürcher Zeitung Nr. 279 vom 30.11 2001. S. 81-82.

75 Christian Campiche: Comment la Suisse a bradé des Enigma. Le plus célèbre codeur secret du monde a fait rêver le monde entier, sauf Berne. Liberté vom 5.1.2001. S.10.

76 David H. Hamer; Geoff Sullivan; Frode Weierud: Enigma Variations. An Extended Family of Machines. In: Cryptologia. 22/3. 1998. S. 211-229. Geoff Sullivan; Frode Weierud: The Swiss NEMA Cipher Machine. In: Cryptologia. 23/4.1999. S. 310-328.

77 Walter Schmid: Die Chiffriermaschine Nema. Hombrechtikon 2005. Typoskript.

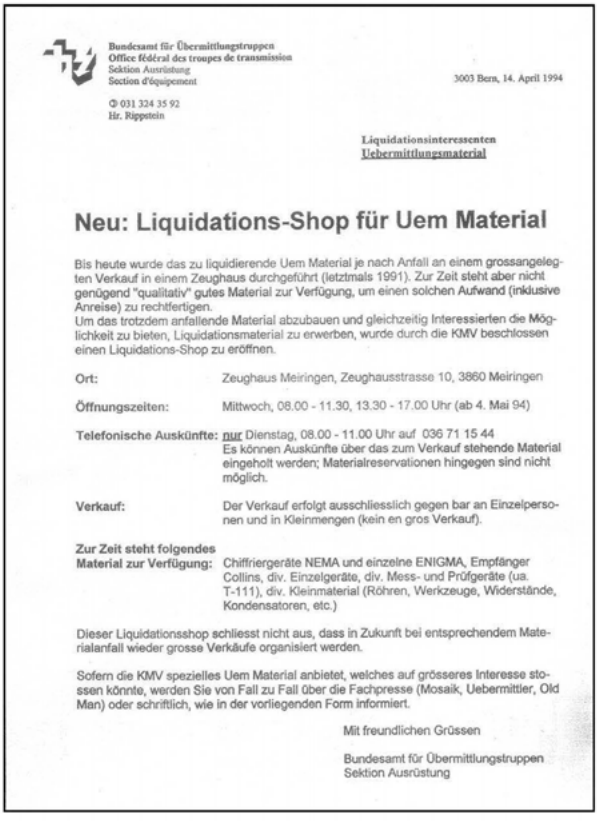
gend ›qualitativ‹ gutes Material zur Verfügung, um einen solchen Aufwand zu rechtfertigen. Um das trotzdem anfallende Material abzubauen und gleichzeitig Interessierten die Möglichkeit zu bieten, Liquidationsmaterial zu erwerben, wurde durch die Kriegsmaterialverwaltung beschlossen, einen Liquidationsshop zu eröffnen«.[78]

Die Überraschung kam erst am Ende des Schreibens. Kommentarlos wurde hier mitgeteilt, dass an diesem Mittwoch einzelne Enigma Chiffriergeräte verkauft würden sowie eine Maschine, die im Schreiben »Nema« genannt wurde. Hätte das Schreiben eine weitere Verbreitung gefunden, so wären wohl nicht nur Gäste aus der Schweiz und Deutschland, sondern auch aus den USA angereist. »Eine absolut unglaubliche Aktion«, nennt etwa Frode Weierud diesen Verkauf, nirgends auf der Welt hatte es etwas Derartiges zuvor gegeben. Wer davon wusste, hatte die grosse Chance, für den geringen Preis von 150 Franken[79] eine Enigma Chiffriermaschine zu erwerben und mit einem Stück Geschichte heimzukehren, für das Sammler Tausende von Franken zu zahlen bereit waren. Weil pro Person nur eine Maschine abgegeben wurde, reisten Sammler aus Deutschland mit Freunden an.

78 Vgl. dazu das weiter unten reproduzierte Dokument »Liquidationsshop«.

79 Ein Besucher dieses Liquidationsshops berichtet, die Maschinen seien zunächst zum Preis von 400 Franken abgegeben worden. Der Preis sei später möglicherweise gesenkt worden. In den Verkauf gelangten maximal 25 Maschinen. Diese Zahl hat Rudolf J. Ritter rekonstruiert. Siehe auch oben.

Abbildung 5



Bundesamt für Übermittlungstruppen
Office fédéral des troupes de transmission
Sektion Ausrüstung
Section d'équipement

3003 Bern, 14. April 1994

✆ 031 324 35 92
Hr. Rippstein

Liquidationsinteressenten
Uebermittlungsmaterial

Neu: Liquidations-Shop für Uem Material

Bis heute wurde das zu liquidierende Uem Material je nach Anfall an einem grossangelegten Verkauf in einem Zeughaus durchgeführt (letztmals 1991). Zur Zeit steht aber nicht genügend "qualitativ" gutes Material zur Verfügung, um einen solchen Aufwand (inklusive Anreise) zu rechtfertigen.
Um das trotzdem anfallende Material abzubauen und gleichzeitig Interessierten die Möglichkeit zu bieten, Liquidationsmaterial zu erwerben, wurde durch die KMV beschlossen einen Liquidations-Shop zu eröffnen.

Ort: Zeughaus Meiringen, Zeughausstrasse 10, 3860 Meiringen

Öffnungszeiten: Mittwoch, 08.00 - 11.30, 13.30 - 17.00 Uhr (ab 4. Mai 94)

Telefonische Auskünfte: nur Dienstag, 08.00 - 11.00 Uhr auf 036 71 15 44
Es können Auskünfte über das zum Verkauf stehende Material eingeholt werden; Materialreservationen hingegen sind nicht möglich.

Verkauf: Der Verkauf erfolgt ausschliesslich gegen bar an Einzelpersonen und in Kleinmengen (kein en gros Verkauf).

Zur Zeit steht folgendes Material zur Verfügung: Chiffriergeräte NEMA und einzelne ENIGMA, Empfänger Collins, div. Einzelgeräte, div. Mess- und Prüfgeräte (ua. T-111), div. Kleinmaterial (Röhren, Werkzeuge, Widerstände, Kondensatoren, etc.)

Dieser Liquidationsshop schliesst nicht aus, dass in Zukunft bei entsprechendem Materialanfall wieder grosse Verkäufe organisiert werden.

Sofern die KMV spezielles Uem Material anbietet, welches auf grösseres Interesse stossen könnte, werden Sie von Fall zu Fall über die Fachpresse (Mosaik, Uebermittler, Old Man) oder schriftlich, wie in der vorliegenden Form informiert.

Mit freundlichen Grüssen

Bundesamt für Übermittlungstruppen
Sektion Ausrüstung

Mitteilung aus dem Bundesamt für Übermittlungstruppen vom 14. April 1994. (Archiv des Autors)

Dass die Schweiz zur Zeit des Zweiten Weltkriegs mit der Chiffriermaschine Enigma arbeitete, war kein Geheimnis. Rudolf J. Ritter, unser erster Gewährsmann, beschreibt im Gespräch, wie er bereits in den 50er Jahren als Truppenkommandant mit diesem Gerät in Berührung gekommen war: »Die Enigma gehörte zum Chiffriermaterial, das man jeweils für Übungen separat in Bern bestellen musste«.[80] Besonderes Interesse brachte er dem Gerät aber nicht entgegen: »Das Telekryptogerät der Firma Gretener, das eine Verschlüsselung in Realzeit ermöglichte, war weit

80 Rudolf J. Ritter im Gespräch mit dem Autor am 22. Oktober 2001 in Grub im Kanton Appenzell.

moderner und hat mich darum viel mehr fasziniert«.[81] Trotzdem: Mit dem Wissen, das er sich zum Thema Schweizer Enigma angeeignet hatte, entstand später eine wichtige Publikation zum Thema.[82] Seinen Angaben zufolge spielte die Enigma bei der Schweizer Nachrichtenübermittlung eine wichtige Rolle: »Die ersten Maschinen kamen 1938 als Beigabe mit 14 schweren Funkstationen, welche die Schweiz 1937 in Deutschland bestellt hatte«.[83] Ein Test zeigte, dass diese Maschinen in Sachen Sicherheit nicht zu übertreffen waren. Sofort wurde eine weitere Tranche von 60 Maschinen und nur wenig später eine weitere von 180 bestellt. Im Juli 1942 waren 265 Enigma K Maschinen vorhanden. Die Kriegsmaterialverwaltung modifizierte die Geräte und änderte unter anderem die Verdrahtung der Walzen sowie den Fortschaltmechanismus.[84]

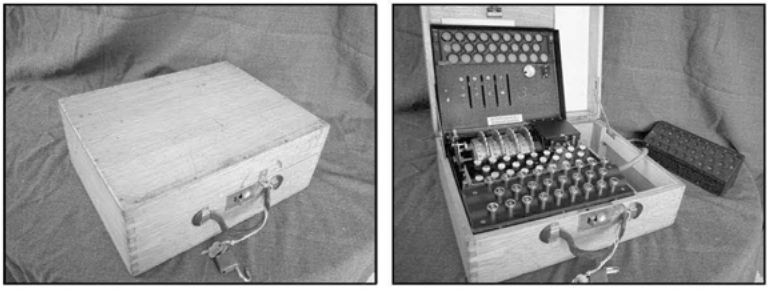
81 Ebenda.

82 Rudolf J. Ritter: Das Fernmeldematerial der Schweizerischen Armee seit 1875. Wie oben.

83 Die Maschinen wurden mit einer Beschreibung geliefert. Dort findet sich auch der Hinweis auf den Lieferant, die Chiffriermaschinen-Gesellschaft Heimsoeth & Rinke. Der Name der früheren Firma Chiffriermaschinen AG ist überstempelt.

84 Rudolf J. Ritter hat die genauen Beschaffungsdaten anhand der Originalakten rekonstruiert. Er schreibt in einer früheren, nicht publizierten Version seines Aufsatzes: «Die Kriegstechnische Abteilung des Eidgenössischen Militärdepartements beschaffte im Einzelnen: Im März 1938 14 Stück bei C. Lorenz AG Berlin mit 14 schweren 1,5 kW-Sendern, geliefert 1.7.38. Im Februar 1939 65 Stück bei der Chiffriermaschinen-Gesellschaft Heimsoeth & Rinke Berlin, geliefert 1.7.39. Im Januar und Juli 196 Stück bei derselben Gesellschaft, zögerlich geliefert 5.5.40-10.7.42.«

Abbildung 6



Eine Schweizer Enigma-Chiffriermaschine samt Koffer in geschlossenem (links) und geöffnetem Zustand (rechts). Gut zu erkennen ist rechts das zusätzliche Lampenfeld, das die Bedienung durch eine zweite Person vereinfachen sollte. (Fotos D. Landwehr)

Chiffriermaschinen sind heikle Geräte. Grosse Staaten stellen solche Maschinen lieber selber her, als sie bei Dritten einzukaufen. Kleine Staaten haben selten die Ressourcen, das zu tun, und sind darum auf Drittanbieter angewiesen. Trotzdem ist es erstaunlich, dass die Schweiz damals ein derart heikles Gerät ausgerechnet in einem Land beschaffte, von dem in jenen Jahren auch für die Schweiz eine erhebliche Gefahr ausging. Rudolf J. Ritter sieht zwei Gründe, die damals für dieses Gerät sprachen: »Erstens war man von der hohen Sicherheit überzeugt, zudem boten die eigenen Modifikationen einen zusätzlichen Schutz.«

Der Zeitzeuge Paul Glur erinnert sich an die Beschaffung dieser Enigma-Maschinen:

»1939 war man in der Schweiz in Sachen Kryptografie wenig informiert. Nach dem Ersten Weltkrieg liess man dieses Gebiet einschlafen – erst 1938 fand man, man müsse sich wieder um dieses Thema kümmern. Praktisch kannten sich hier nur die Funker etwas aus. Die Funker arbeiteten damals ziemlich primitiv mit Buchstabentabellen. Damals realisierte man, dass es diese Enigma-Maschine gab, und schaffte ein paar davon zu Versuchszwecken an. Der Funkfourier der damaligen Telegrafenkompanie Hadwiger erhielt den Auftrag, diese Sache etwas genauer anzuschauen. Als der Krieg 1939 los ging, musste Hadwiger übernehmen – da brauchte es noch einen Offizier und das war dann der Kollege von Hadwiger, Prof. Alder, Ordinarius für Versicherungsmathematik. So hat das alles angefangen. Es gab einen Bundesratsbeschluss, dass dieses Büro nun Leute suchen konnte, die sich mit Kryptografie befassen würden. Hier stiess Prof. Linder und einige weitere Personen aus dem Kollegenkreis von Hadwiger zu dieser Gruppe. Ich selber war damals Student von Prof. Hadwiger.

Wir waren damals nur gerade zehn Studenten am Berner Kolleg für Mathematik und Versicherungsmathematik. Ich hatte 1937 die Rekrutenschule gemacht, 1938 die Unteroffiziersschule und absolvierte 1939 den ersten Wiederholungskurs bei diesem neuen Büro. Wir hatten eine Sonderstellung und waren sogenannte Intellektuelle. Das bescherte mir dann ziemlich viele Diensttage – ich habe über 1000 Diensttage gemacht.«[85]

Man war offenbar in Eile mit Bestellen von Chiffriermaschinen. Eine grosse Auswahl gab es nicht, aber es gab durchaus Alternativen. Dazu zählten die Maschinen des Schweden Boris Hagelin, der sich ja nach dem Krieg in der Schweiz niederliess und die Firma Crypto AG in Zug gründete.

Abbildung 7

Oskar Stürzinger – der erste Angestellte von Boris Hagelin, Gründer der Firma Crypto AG in Zug. Die Bilder entstanden anlässlich einer Präsentation der Handchiffriermaschine CD 57 aus dem Jahre 1957, an deren Entwicklung Oskar Stürzinger mitbeteiligt war. (Fotos D. Landwehr)

Sein erster Schweizer Angestellter war Oskar Stürzinger. Er kannte die Schwächen der Geräte von Boris Hagelin, auch wenn er mit dieser Beschaffung nichts zu tun hatte und als junger Ingenieur erst Mitte der 50er Jahre in Kontakt mit dem Thema Kryptografie kam.

»Die Schweizer Armee hatte keine Berufssoldaten. Man befand die Hagelin Maschine als nicht miliztauglich. Bei der Enigma waren alle Teile gleich. Man konnte das Schlüsselwort aus fünf Worten zusammensetzen. Bei der Hagelin Maschine hatte jeder Rotor eine andere Teilung – gemäss den Primzahlen. Das

85 Zu den von ihm genannten Namen: Hugo Hadwiger (1908-1981) war 1937-1977 Professor für Mathematik an der Universität Bern; Heinrich Weber (1907-1997) war Ingenieur und 1948-1973 als Professor für Mathematik an der ETH Zürich; Arthur Linder (1904-1993) Professor für mathematische Statistik, Arthur Alder, Prof. für Versicherungsmathematik (Quellen: ETH Zürich sowie Historisches Lexikon der Schweiz).

wollte man dem Milizsoldaten nicht zumuten, dass er also eine Maschine hatte, die bei gewissen Rädern kein Z und kein Y hatte. Die Italiener benutzten die Chiffriermaschinen von Hagelin und auch die Franzosen. Die Maschinen waren sicher, ausser in Stresssituationen. Da war der Mensch diesem System nicht gewachsen und hat Fehler gemacht. Diese Fragen waren bei der Auswahl für die Schweizer Armee sehr wichtig. Man darf nicht vergessen, dass ein Milizoffizier anders reagiert als ein Berufsoffizier. Diese Entscheidung war wohl richtig. Man hätte allerdings das mit etwas Ausbildung beheben können.«[86]

Sehr genau an die Beschaffung erinnert sich hingegen Paul Glur, der zum fraglichen Zeitpunkt Student war.

»Wir kriegten immer Material zum Entschlüsseln geliefert, aber wir konnten nichts damit anfangen. So beschäftigten wir uns zuerst mit den eigenen Verfahren. Uns war klar, hier muss etwas geschehen. So stiess man ziemlich schnell auf die Enigma – man bestellte nach, und die Deutschen konnten sofort liefern. Wir schauten sie an und sagten: Gut, aber wir müssen sie sofort umlöten. Im Zeughaus Bern gabs eine Funkerwerkstatt und dort begann man mit dem Umlöten.«[87]

Technisch funktionierten die Maschinen genau gleich wie die Modelle, die Deutschland verwendete. Nur fehlte ihnen das sogenannte Steckerbrett, das die Komplexität der Verschlüsselung erhöhte. Und anders als in Deutschland blieb es während des ganzen Krieges bei den drei Rotoren.

Die Modifikationen, die durch die Kriegsmaterialverwaltung angebracht wurden, waren teils kosmetischer, teils kryptografischer Natur. Die meisten Maschinen erhielten ein zweites Lampenfeld. Dadurch wurde die Bedienung durch zwei Personen erleichtert. Das zweite Lampenfeld bedingte aber die Vergrösserung des hölzernen Schutzkastens. Zur Schonung der Batterie wurde ein Transformator hinzugefügt, der bis zu vier Maschinen gleichzeitig speisen konnte. Bei den Maschinen des Heeres wurde der Fortschaltmechanismus so geändert, dass bei jedem Schritt anstelle der rechten die mittlere Walze mitgenommen wurde. Diese nahm ihrerseits nach einem vollen Umlauf die linke Walze mit und diese nach einem vollen Umlauf die Umkehrwalze. Für die Maschinen existierten zwei Sätze mit Walzen: Ein Übungssatz und ein Satz für den Kriegsfall. Die Maschinen, die anfangs 90er Jahre in den Verkauf gelangten, waren alle mit den Übungssätzen ausgerüstet. Die Kriegsrotoren wurden ver-

86 Oskar Stürzinger im Gespräch mit dem Autor am 20. Februar 2003 in Zürich.

87 Paul Glur wie oben.

nichtet, nachdem zuvor deren Verdrahtung protokolliert worden war. Dies wiederum ist bemerkenswert: Die im Krieg in der Schweiz verwendeten Schlüssel sind demnach immer noch geheim!

Nachdem bereits während des Krieges Zweifel an der Sicherheit der Maschine aufgekommen waren – und mit dem Nachfolgemodell Nema auch für Abhilfe gesorgt war, wurden die Enigma-Maschinen zu Übungszwecken weiter benutzt und ab 1958 in der Kriegsreserve gelagert.[88] Nur die Flieger- und Fliegerabwehrtruppen verwendeten die Maschinen bis 1989 in einem Notfunknetz weiter.

Beim Heer trennte man sich schon Mitte der 70er Jahre von 102 Maschinen. Sie wurden zerlegt und vernichtet. Bei der Luftwaffe geschah dasselbe nur mit der Hälfte der 163 Maschinen. 1990 waren noch 94 Enigma K Maschinen vorhanden. Der grösste Teil davon wurde an interessierte Kreise innerhalb der Schweizer Bundesverwaltung abgegeben. Zurück blieben 25 Maschinen. Rudolf J. Ritter nimmt an, dass diese ab dem 4. Mai 1994 in Meiringen zum Verkauf kamen – möglicherweise aber nicht alle auf einen Schlag.[89] Es muss davon ausgegangen werden, dass die meisten der Maschinen, die nicht vernichtet wurden, erhalten sind und sich in den Händen von Sammlern, von Bundesstellen und von Museen befinden.

Deklassifiziert wurde das Enigma-Verfahren allerdings erst 1992 – und im Mai 1994 kamen die Maschinen unter den Hammer und begannen ihr zweites Leben.

Die Neue Maschine: Nema

Auf die letzte Serie ihrer Bestellungen – es handelte sich um 180 Enigmas – musste die Schweizer Armee nicht weniger als zwei Jahre warten. Das war entschieden zuviel – man musste sich nach einem neuen Lieferanten umsehen. Nach all den Jahren im Umgang mit der Enigma-Chiffriermaschine hatte man in der Kryptografie einige Fortschritte gemacht und auch die Schwachstellen der Enigma erkannt und deshalb beschlossen, eine eigene Maschine zu bauen.

88 Rudolf J. Ritter: Das Fernmeldematerial der Schweizerischen Armee seit 1875. S. 35.

89 Schriftliche Mitteilung von Rudolf J. Ritter an den Verfasser vom 20. August 2001.

Mitte 1943 wurde der Konstruktionsauftrag an die Firma Zellweger in Uster[90] erteilt. Zellweger hatte 1936 eine eigene Abteilung für Hochfrequenz-Technik eröffnet – die Firma produzierte das erste in der Schweiz entwickelte Funkgerät. Die Entwicklung der neuen Chiffriermaschine darf auch aus heutiger Perspektive als rasch bezeichnet werden: Nach der Konstruktion von zwei Protoypen 1943 und deren erfolgreicher Erprobung im Herbst 1944 wurde eine mechanisch nochmals verbesserte Version im Frühjahr 1945 als truppentauglich erklärt. In einem einzigen Los wurden gleich anschliessend 640 Maschinen gebaut, sie erhielten die Typenbezeichnung Nema Modell 45: »Die Maschinen wurden im Frühjahr 1947 ausgeliefert und bildeten während zwei Jahrzehnten das Rückgrat der offline Chiffrierung des Eidgenössischen Politischen Departementes und des Heeres«.[91] Offline will heissen, dass die Funksprüche in die Maschine getippt und dort, genau wie bei der Enigma, zunächst wieder abgelesen und erneut aufgeschrieben werden mussten, bevor sie per Funk oder Kurier übermittelt wurden.

Abbildung 8

Die Chiffriermaschine Nema. Auf dem Bild rechts ist die vergrösserte Anzahl der Rotoren gut zu erkennen. Die Nema erhielt 9 Rotoren plus eine Umkehrwalze – die Schweizer Enigma hatte nur 3 Walzen plus eine Umkehrwalze. (Fotos D. Landwehr)

Diese Nema war nichts anderes als eine Weiterentwicklung der Enigma: Sie verfügte über mehr Walzen als ihr Vorbild, zudem war der Walzenvortrieb unregelmässiger und damit schwerer zu rekonstruieren. Sie hatte neun auswechselbare Walzen plus eine Umkehrwalze. Eine direkte Aus-

90 Zellweger AG Uster: 1880 gegründet und bis gegen Ende des 20. Jahrhunderts einer der grossen Namen im Schweizer Apparatebau und Fernmeldegeschäft.

91 Ritter. Das Fernmeldematerial der Schweizerischen Armee seit 1875. S. 38.

wirkung davon war, dass es erheblich mehr Druck brauchte, die Chiffriermaschine zu bedienen. Wohl deshalb erhielt sie auch den Namen Fingerbrecher. Wie in späteren Jahren so oft, wurde in der Schweiz nichts Neues erfunden, sondern etwas Bestehendes optimiert:

»Verglichen mit der 20 Jahre zuvor entworfenen Enigma war die Nema – als Werk eines im feinmechanischen Apparatebau hoch angesehenen Unternehmens – konstruktiv eleganter, präziser und sorgfältiger ausgeführt; insbesondere war der Kontaktapparat der Walzen – im Gegensatz zur Enigma – robust ausgeführt und praktisch störungsfrei.«[92]

Verantwortlich für das Pflichtenheft der neuen Chiffriermaschine zeichneten drei Personen: Hugo Hadwiger, damals Professor für Mathematik an der Universität Bern, der Ingenieur und nachmalige ETH-Professor Heinrich Weber und Paul Glur, Student von Professor Hadwiger.[93] Paul Glur ist der einzige dieser drei, der vom Autor 2001 noch befragt werden konnte. Wir besuchten den damals 84-Jährigen in seinem Haus im Berner Schosshaldequartier. Der etwas rundliche Mann mit den lebhaften kleinen Augen freute sich und erzählte bereitwillig aus früheren Tagen: »Als 1939 der Krieg ausbrach war die Schweiz in Sachen Kryptografie nicht sehr weit – man hatte dieses Gebiet nach dem Ersten Weltkrieg einschlafen lassen«. Die Enigma löste für die Schweiz dieses Problem fürs Erste: »Es gab nichts Anderes oder man wusste nicht davon«. Erstaunlich ist, was Paul Glur über das Umfeld erzählt. Demnach hatten codierte Nachrichten schon damals einen grossen Reiz – auch für ein weiteres Publikum: »Wir kriegten immer wieder verschlüsselte Meldungen von Leuten. ›Könnt ihr etwas damit anfangen‹, fragte man uns. Wir konnten und haben praktisch alle Meldungen, die so hereinkamen, geknackt.« Paul Glur sieht hier eine Parallele zu den Hackern von heute, die das Aufspüren von Sicherheitslücken auch fast als Sport betreiben.[94]

Das Nema-Verfahren wurde ähnlich wie das Enigma-Verfahren 1992 deklassifiziert, die ausrangierten Nema Maschinen gelangten gleichzeitig wie die Enigmas in den Verkauf.[95] Die Nema wurde bei der Armee be-

92 Ebenda S. 40.

93 Walter Schmid weist darauf hin, dass die drei ohne einen offziellen Entwicklungsauftrag arbeiteten. Nach dem Krieg beanspruchten sie vom Bund eine Entschädigung für ihre Erfindung. Nach einem längeren Hin- und Her wurde ihnen am 3. Oktober 1948 die Summe von 6000 Franken zugesprochen. Walter Schmid: Die Chiffriermaschine Nema. S. 73.

94 Paul Glur im Gespräch mit dem Autor am 1.Oktober 2001 in Bern.

95 Rudolf J. Ritter: Das Fernmeldematerial der Schweizerischen Armee seit 1875. S. 40.

reits um 1960 durch den sogenannten Krypto-Fernschreiber ersetzt, zu umständlich war ihre Bedienung, zu langsam die Übermittlung und zu fehleranfällig das ganze Prozedere. »Selbst kleinste Fehler führten dazu, dass sich die beiden Stationen nicht mehr verstehen konnten«.[96] Zudem liess sich die Maschine nicht in ein EDV-System einbinden.

Geheim - aber nur für die Schweiz!

Natürlich ist heute auch das Chiffrierverfahren der damals moderneren Nema-Chiffriermaschine obsolet und mit Computern zu knacken. Ob ihr Code auch in der Zeit ihrer aktiven Verwendung, also zwischen 1947 bis in die 80er Jahre entschlüsselt wurde, ist nicht bekannt.[97]

Anders bei der Schweizer Enigma: Ihr Code wurde während des Zweiten Weltkrieges von den Polen, den Engländern und Amerikanern und natürlich auch von den Deutschen entschlüsselt.

Dass die Enigma Schwachstellen hatte, war auch den Schweizer Kryptologen bekannt. Zu den ersten Massnahmen zählte deshalb die Neuverdrahtung der Rotoren. Diese Massnahme wurde jedoch nicht bei allen Truppengattungen mit derselben Konsequenz durchgeführt: Schon 1941 erfuhren die Behörden auf ungewöhnlichem Weg von einer Schwachstelle bei den Flieger- und Flabtruppen wie ein Dokument aus dem Armeestab zeigt:

Abbildung 8a

Verwendung der Chiffrier-
maschine "Enigma".

Durch die Abteilung für Nachrichten- & Sicherheitsdiens konnte festgestellt werden, dass im Ausland das schweizerische Chiffriersystem angeboten worden ist. Dabei wurde Bezug genommen auf 2 Chiffretg., die nach Ermittlung des Chiffrebureaus der Armee nur von den Fl.-& Flabtrp. stammen konnten. Bei der Abklärung des Sachverhaltes wurde festgestellt, dass die gegenwärtige Handhabung der Schlüssel der Chiffriermaschine durch die Fl.-& Flabtrp., bei einem relativ geringen Chiffrierverkehr per Funk (20-30 Tg.), die Geheimhaltung der Meldungen nicht mehr gewährleistet.

Auszug aus einer Aktennotiz vom 3. Mai 1941 des Generalstabschef der Schweizer Armee: Der Befehl stützt sich auf eine nachrichtendienstliche Quelle, die sich in den Archiven nicht rekonstruieren lässt. Quelle: Schweizer Bundesarchiv Bern. Bestände E27/19007.

96 Walter Schmid: Die Chiffriermaschine Nema. S. 57.

97 Ebenda S.56.

Der Leiter der polnischen Kryptoanalytiker-Gruppe, Marian Rejewski berichtet in seinen Erinnerungen davon, wie Schweizer Enigma-Nachrichten von seinem Team, das damals im Rahmen der Operation Cadix in Südfrankreich stationiert war, gelesen wurden; allerdings wurde das Knacken des Schweizer Codes als eher marginale Tatsache empfunden, das Hauptaugenmerk galt den deutschen Maschinen. Belegt sind Lauschangriffe zwischen Dezember 1940 bis März 1941. Die Resultate gingen sofort zum britischen Nachrichtendienst, dem die polnischen Abhörer damals zudienten. Gelesen wurde offenbar nicht nur der militärische, sondern auch der diplomatische Verkehr.[98]

Die Informationen der polnischen Abhörer wurden in England ohne Zweifel verarbeitet – denkbar wäre allerdings auch, dass der Schweizer Funkverkehr direkt in England abgehört wurde. Ein britisches Geheimdokument »Swiss Random Letter Traffic«[99], das in den National Archives der USA zu finden ist, beschreibt die Schweizer Codierung minutiös. Der Begriff »Random Letter Traffic« steht wahrscheinlich für die Tatsache, dass der Verkehr unregelmässig war und den Briten deshalb zufällig erschien:

»The Swiss random letter traffic is encyphered on a commercial-type Enigma machine with specially wired wheels, the turnover mechanism being on the tyre. The first four letters of the message are the indicator which is repeated as the last four letters of the message. The actual text begins with the fifth letter of the message.«[100]

Und weiter folgt dann die Bestätigung für die erfolgreiche Durchdringung des Codes. Zur Erinnerung: Der Begriff ›crib‹ – auch ›mot probable‹ genannt – steht für ein bereits bekanntes oder erratenes Wort im Chiffrat:

»The Swiss have no spare wheels for the machine which thus has only six possible wheel-orders. As the machine was broken on a crib we have arrived at three wheels which we call Blue, Red and Green.«[101]

98 Ausführlicher Bericht über die Abhöraktion: W. Kozaczuk. Geheimoperation Wicher. Polnische Mathematiker knacken den deutschen Funkschlüssel. Bonn 1989. Karl Müller Verlag. S. 330-333.

99 Das Papier trägt den Namen »Swiss Random Letter Traffic«. Es findet sich in den Akten des US-Nationalarchivs. NSA Historical Collection, RG 457.

100 Ebenda.

101 Ebenda.

Der nun folgende Abschnitt gibt einen wunderbaren Einblick in die aufreibende Arbeit des Entzifferns; als sogenannter »crib« diente der Name KAMM, so hiess offenbar ein Mitglied der Schweizer Botschaft in London, nur war sein Name mit nur vier Buchstaben etwas kurz um eine wirkungsvolle Hilfe beim Entschlüsseln abzugeben. Der Text entbehrt nicht einer gewissen Komik und ist deshalb im vollen Umfang wieder gegeben.

»Keys are broken chiefly by the process of guessing beginnings. The majority of messages from Berne used to begin VON HANDEL, VON SURCOMMERCE or VON TRANSPORT with similar, though less definite, beginnings for messages addressed to Berne. Recently however these openings have fallen out of use, the department concerned is now denoted by a code-word attached to the signature: the words mostly used are MERKUR, SATURN and WEGA which correspond respectively to the openings quoted. (However what little Washington traffic we have suggests that messages from Washington may be being addressed inside and out.) The decay of these openings has recently considerably increased the difficulties of the London traffic, our most profitable cribs now being VOTREX, DEKAMM, FURKAMM, FUER KAMM and POURKAMM. IHRX would be as useful as VOTRE but is naturally harder to break with. KAMM is the head of the Swiss War Food Office in London: The shortness of his name is a source of great grief to us, but you should be better served by a gentleman named WANGER who appears to organise transport business.«[102]

102 Ebenda.

Abbildung 9

MOST SECH

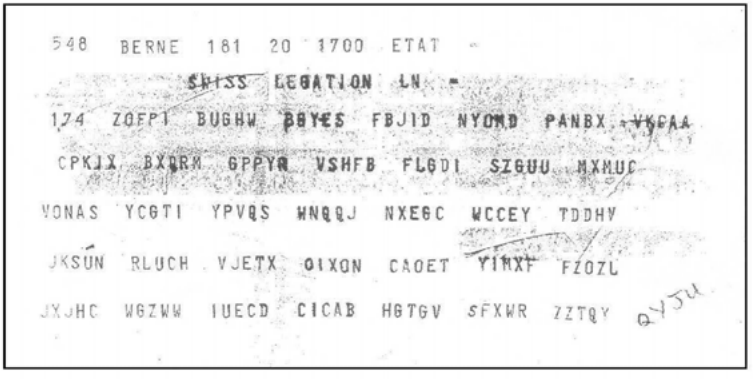
SWISS RANDOM LETTER TRAFFIC.

The Swiss Random letter traffic is encyphered on a commercial-type Enigma machine with specially wired wheels the turnover mechanism being on the tyre. The first four letters of the message are the indicator which is repeated as the last four letters of the message. The actual text begins with the fifth letter of the message. (There is also some Politique Interets traffic in which instead of repeating the indicator at the end of the message the letters as of the last group is repeated. This traffic is extremely rare between London and Berne and no serious attempt has been made to break any between Berne and Washington). The messages are in French or German with no punctuation except an occasional STOP. Numbers are always sandwiched between an X and a Y, the figures 1234567890 being denoted respectively by QWERTZUIOP: thus XQOREY will denote 1943.

Reproduktion aus dem britischen Abhörpapier »Swiss Random Letter Traffic« (Quelle: National Archives, Washington D.C.)

In den National Archives von Washington D.C. finden sich einige Botschaften samt ihrer Entschlüsselungen. Sie betreffen alle Massnahmen in Bezug auf die Rationierung von Lebensmitteln.

Abbildung 10



548 BERNE 181 20 1700 ETAT

SWISS LEGATION LN

174 ZOFPI BUGHW BBYES FBJID NYOMD PANBX VKCAA

CPKJX BXQRM GPPYR VSHFB FLGDI SZGUU MXMUC

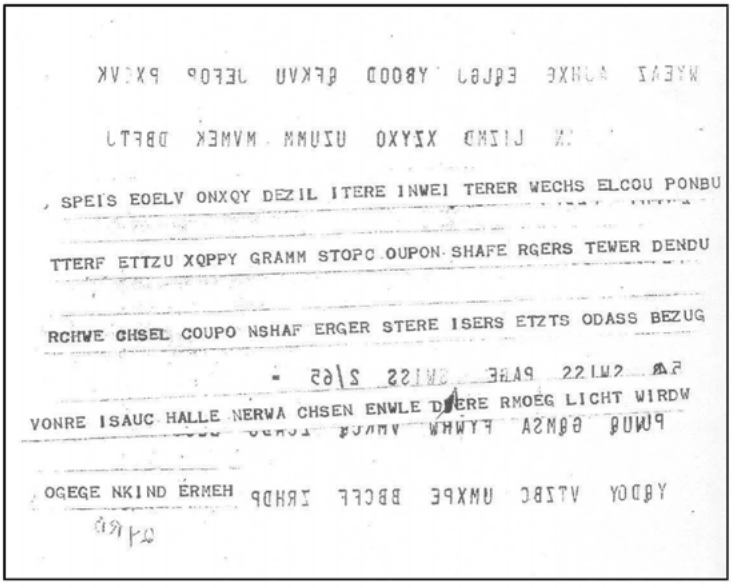
VONAS YCGTI YPVQS WNQQJ NXEGC WCCEY TDDHV

JKSUN RLUCH VJETX OIXON CAOET YIMXF FZOZL

JXJHC WGZWW IUECD CICAB HGTGV SFXWR ZZTQY

Reproduktion einer mit der Schweizer Enigma verschlüsselten Nachricht. (Quelle: National Archives, Washington D.C.)

Abbildung 11



Eine weitere Nachricht mit ihrer Entschlüsselung, deren Sinn allerdings auch im Klartext nicht ohne zusätzliches Wissen erschlossen werden kann. (Quelle: National Archives, Washington D.C.)

Der Text lautet folgendermassen:

»SPEIS EOELV ONXQY DEZIL ITERE INWEI TERER WECHS ELCOU PONBUTTERF ETTZU XQPPY GRAMM STOPC OUPON SHAFE RGERS TEWER DENDU RCHWE CHSEL COUPO NSHAF ERGER STERE ISERZ ETZTS ODASS BEZUG VONRE ISAUC HALLE NERWA CHSEN ENWLE DERE RMOEG LICHT WIRDW OGEGE NKIND ERMEH

SPEISEOEL VON XQX DEZILITER EIN WEITERER WECHSEL COUPON BUTTER FETT ZU XQPPY GRAMM STOP COUPONS HAFER GERSTE WERDEN DURCH WECHSEL COUPONS HAFER GERSTE REIS ERSETZT SO DASS BEZUG VON REIS AUCH ALLEN ERWACHSENEN WIEDER ERMOEGLICHT WIRD WOGEGEN KINDER MEH«

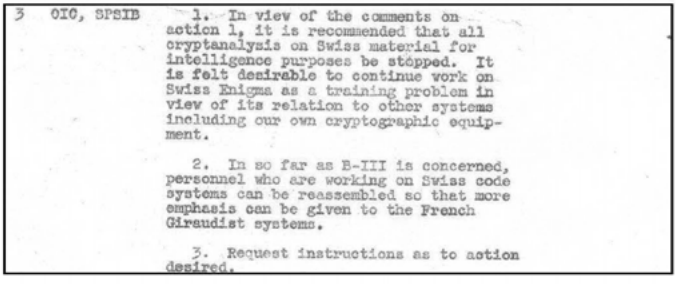
Es liegt auf der Hand, dass Grossbritannien die Erkenntnisse in Bezug auf den Schweizer Funkverkehr mit den US Dienststellen teilte. Diese Zusammenarbeit wurde im Lauf des Krieges und vor allem nach dem Besuch von Alan Turing in den USA Ende 1942 intensiviert. Dass die

Schweizer Maschine in einem US Dokument 1943 auftaucht, ist wohl so zu erklären: Das von einem Major Frank B. Rowlett gezeichnete Dokument vom 4. August 1943 zeigt die geringe Bedeutung, die man der Aufklärung des Schweizer Funkverkehrs zumass.

»In view of the comments on section 1, it is recommended that all cryptanalysis on Swiss material for intelligence purposes be stopped. It is felt desirable to continue work on Swiss Enigma as training problem in view of its relation to other systems including our own cryptographic equipment.«[103]

Immerhin wird aus einem späteren Dokument ersichtlich, dass es im US Nachrichtendienst so etwas wie eine Schweizer Sektion gegeben haben muss, die mindestens den existierenden Funkverkehr mitlas und protokollierte. Im gleichen Dokument wird eine Aufklärungsquote von 90 Prozent genannt, was bedeutet, dass bis auf einen kleinen Rest fast alles gelesen werden konnte.

Abbildung 12



3 OIC, SPSIB

1. In view of the comments on action 1, it is recommended that all cryptanalysis on Swiss material for intelligence purposes be stopped. It is felt desirable to continue work on Swiss Enigma as a training problem in view of its relation to other systems including our own cryptographic equipment.

2. In so far as B-III is concerned, personnel who are working on Swiss code systems can be reassembled so that more emphasis can be given to the French Giraudist systems.

3. Request instructions as to action desired.

Die US-Codebrecher hatten offenbar nur ein begrenztes Interesse am abgehörten Schweizer Funkverkehr. (Quelle: National Archives, Washington D.C.)[104]

103 National Archives USA: NSA Historical Collection, RG 457. Das Dokument stammt aus einer Sammlung von Beständen aus Akten der National Security Agency NSA, die Mitte der 90er Jahre deklassifiziert und den National Archives übergeben wurden. Sie sind auch für interessierte Besucher vor Ort leicht zugänglich. Die Bestände sind seit 2006 auch im Internet beschrieben: www.archives.gov/research/holocaust/finding-aid/civilian/rg-457.html vom 16.2.2008.

104 Ebenda.

Der militärische Nutzen, der den Alliierten durch die Entzifferung des Schweizer Enigma-Verkehrs erwuchs, war offensichtlich gering, zumindest während des Krieges. In mindestens einem Fall konnte jedoch eine der beiden Mächte, nämlich die USA, nach dem Krieg einen Vorteil aus dieser Tätigkeit ziehen. Im April 1946 befand sich eine Delegation der Schweiz in Washington um über eine Abfindungszahlung zu verhandeln. Die Schweiz hatte während des Krieges als Drehscheibe für das Nazi-Raubgold gedient, und die Alliierten verlangten nach dem Krieg eine Abfindung von Seiten der Schweiz.[105] Die Verhandlungen fanden fern von der Schweiz in Washington statt, die Verhandlungsschritte wurden per Funk in die Schweiz gemeldet. Da die USA den mit der Schweizer Enigma verschlüsselten Funkverkehr mühelos mitlesen konnten, kannten sie das Schweizer Verhandlungsangebot und wussten, dass die Schweiz maximal zu einer Zahlung von 250 Millionen Franken bereit war. Die US Forderung nach einer Zahlung von 560 Millionen Franken konnte somit gut abgesichert vorgetragen werden.[106]

Dass schliesslich auch Nazi-Deutschland den Schweizer Funkverkehr mitlesen konnte, darf nicht überraschen. Erklärungsbedürftig wäre allenfalls die Tatsache, weshalb man dies in der Schweiz ignorierte. Interessant ist aber der Weg, wie diese Tatsache bekannt wurde – und einmal mehr gewissermassen eine Geschichte für sich.

Nach dem Ende des Krieges meldete sich beim Kryptografiedienst der Schweizer Armee auf dem schriftlichen Weg ein Deutscher namens Bruno Kröger. Er gab an, im Krieg bei jener Behörde gearbeitet zu haben, die mit dem Mitlesen des verschlüsselten Schweizer Funkverkehrs

105 Eine ausführliche Darstellung bei: Philipp Sarasin; Regina Wecker: Raubgbold, Réduit, Flüchtlinge. Zur Geschichte der Schweiz im Zweiten Weltkrieg. Zürich 1998. Chronos. Ausserdem: Unabhängige Expertenkommission Schweiz Zweiter Weltkrieg: Die Schweiz, der Nationalsozialismus und der Zweite Weltkrieg. Schlussbericht. Zürich 2002. Pendo. Auch: www.uek.ch/de/ vom 16.2.2008.

106 Thomas Maissen: Schatten des Zweiten Weltkrieges / Wer verriet den Amerikanern die Zahl von 250 Millionen Franken? Abhöraktionen und Intrigen an der Washingtoner Konferenz von 1946. Neue Zürcher Zeitung vom 1. April 1998. S. 17.
Maissen gibt als Quelle Dokumente aus dem Schweizer Bundesarchiv E6100 (A) 25/2326 sowie aus den National Archives der USA RG 457 (Records of the National Security Agency; Central Security Service): Intercepts concerning Allied-Swiss negotiations on the Disposition of German Assets and Looted Gold 1945-1946.

betraut war. In zwei umfangreichen Dokumenten[107] bewies er den Schweizern seine Kenntnisse und beschrieb die benutzte Methode ausführlich. Bemerkenswert dabei ist, dass er zur Auflösung des Schweizer Enigma-Codes ein sogenanntes ›Papiermodell‹ benutzte, das ohne jede mechanische Unterstützung auskommt. Allerdings ist der dazu erforderliche Zeitaufwand nicht unbeträchtlich: Der Autor rechnet vor, dass es für die Ermittlung der Walzenverdrahtung der ersten Walze fünf bis sechs Arbeitskräfte während einer bis sechs Wochen braucht.[108]

Warum tat Bruno Kröger diesen Schritt? – Über die Motive kann heute nur spekuliert werden. Möglicherweise war er tatsächlich ganz einfach auf der Suche nach Arbeit und erhoffte sich Anstellung in Bern. Sicher ein ungewöhnlicher Schritt, was ihm sehr wohl bewusst war. Seine Argumentation ist mehr als interessant:

»Sollte ein von mir empfohlenes Geheimschriftverfahren sich trotz Beachtung der Anwendungsvorschriften als von unberufener Seite entzifferbar erweisen, so bin ich bereit, mir einen solchen Irrtum als ›bewussten Verrat‹ auslegen zu lassen. Obwohl ich mir über die Tragweite einer solchen Verpflichtung klar bin, kann ich diese übernehmen, da ich über genügend Erfahrung verfüge, die Sicherheit von Geheimschriften genau zu beurteilen und nur solche als absolut sicher zu bezeichnen, bei denen die Unmöglichkeit der Entzifferung von unberufener Seite nachweisbar feststeht.« [109]

107 Bruno Kröger: Bericht über allgemeine Erfahrungen bei der Entzifferung von Geheimschriften im Hinblick auf die Sicherheitsanforderungen, die an Geheimschriftverfahren gestellt werden müssen. Kaufbeuren 1948. Typoskript. Nicht veröffentlicht.
Bruno Kröger: Analyse der Chiffriermaschine ENIGMA Type K. Kaufbeuren 1948. Typoskript. Nicht veröffentlicht.

108 Bruno Kröger: Analyse S. 15.

109 Bruno Kröger: Bericht S. 10.

Abbildung 13

Sollte ein von mir empfohlenes Geheimschriftverfahren sich trotz Beachtung der Anwendungsvorschriften im Gegensatz zu meiner Beurteilung als von unberufener Seite entzifferbar erweisen, so bin ich bereit, mir einen solchen Irrtum als "bewussten Verrat" auslegen zu lassen. Obwohl ich mir über die Tragweite einer solchen Verpflichtung klar bin, kann ich diese übernehmen, da ich über genügend Erfahrung verfüge, die Sicherheit von Geheimschriften genau zu beurteilen und nur solche als absolut sicher zu bezeichnen, bei denen die Unmöglichkeit der Entzifferung von unberufener Seite nachweisbar feststeht.

Ausschnitt aus dem umfangreichen Schreiben von Bruno Kröger.[110]

Das Dokument ist ausserordentlich ausführlich und beginnt bei den Anfängen der Kryptographie. Ein Hinweis, dass der Autor viel Zeit für das Verfassen des Dokuments aufgewendet hat. Es beinhaltet jedoch eine interessante Analyse des Standes der Kryptografie zur Zeit des Zweiten Weltkrieges. Die Folgerungen sind auch aus heutiger Sicht weitgehend zutreffend, gerade auch was die Einschätzung der Bestrebungen der verschiedenen Länder angeht: »Aus einem allgemeinen Überblick ergibt sich, dass vom Sicherheitsstandpunkt aus Sowjetrussland an erster Stelle steht. Es werden fast nur Handverfahren benutzt, die höchsten Sicherheitsgrad besitzen.«[111] Kröger weist auch darauf hin, dass die Kontrolle über die benutzten Verfahren in diesem Land äusserst stark sein muss.

Was die Schweizer Enigma-Maschine angeht, so weist Kröger auf die Schwächen hin: »Vom Sicherheitsstandpunkt aus muss für jedes Verfahren gefordert werden, dass es für den Unberufenen selbst dann unlös-

110 Ebenda S. 11.

111 Ebenda.

bar bleibt, wenn das Verfahren als solches bekannt ist, wenn also im vorliegenden Fall die Maschine und die Walzenschaltung als bekannt vorausgesetzt werden. Einer solchen Sicherheitsanforderung entspricht die Enigma-Chiffriermaschine Type K keineswegs, da schon ein einziges vermutetes Textwort die Lösung des Spruchs ergibt.«[112] Und weiter: »Das an und für sich gute Prinzip der Walzenverschlüsselung würde nur bei einer völligen Neukonstruktion der Maschine Ergebnisse zeitigen können, die den Sicherheitsaspekten genügen«.[113]

Die Geschichte dieses Dokuments erscheint mysteriös: Das Schweizer Papier ist nicht im Bundesarchiv zu finden, sondern wird in der Fachabteilung für Kryptographie aufbewahrt. Es wurde mir allerdings ohne Zögern ausgehändigt, nachdem ich den zuständigen Leiter darauf angesprochen hatte. Er gab mir auch zu verstehen, dass das Dokument selber keine schützenswerten Inhalte mehr aufweise. Offenbar existiert aber ein Begleitbrief, der mir nicht gezeigt wude. Dort müssen Adresse und Absender genannt sein und dieser Begleitbrief scheint geheim zu sein. Gut möglich, dass der Brief über eine weitere Institution, die auch heute noch geschützt werden muss, in die Schweiz kam.

Zu Fragen Anlass gibt auch der Ort, an dem das Dokument verfasst wurde: Kaufbeuren (Bayern). Im dortigen Stadtarchiv weiss man nichts von einem Einwohner mit Namen Bruno Kröger. Hingegen weist man mich darauf hin, dass die US Armee den nahe gelegenen Fliegerhorst benutzte. Es handelt sich mit grosser Wahrscheinlichkeit um dieselben Gebäude, die dem Reichsluft-Forschungsamt, wo auch Bruno Kröger arbeitete, nach seiner Dislokation aus Berlin ab 1943 diente.[114] Denkbar wäre auch, dass Bruno Kröger das Papier als Kriegsgefangener der Alliierten geschrieben hat und dass das Dokument auf diplomatischem Weg in die Schweiz gelangte, deshalb vielleicht auch das Bedürfnis nach Geheimhaltung.

Was hat die Schweiz mit dem Angebot Krögers gemacht? – Nichts. Man war nicht an diesen Informationen interessiert: »Unsere Fachstellen fanden, der Bittsteller beschreibe keine Erkenntnisse oder Methoden, die hier nicht schon bekannt waren. Die Sache verlief deshalb im Sande«, erklärte unser Gewährsmann Rudolf J. Ritter 2001.[115]

---

112 Ebenda S.16.

113 Ebenda.

114 David Irving: Das Reich hört mit. Der geheimste Nachrichtendienst des Dritten Reiches. Kiel 1989. Arndt Verlag. S.121.

115 Schriftliche Mitteilung an den Verfasser von Rudolf J. Ritter vom 21. Oktober 2001.

Zwischenbericht Teil 1

Nach der Darstellung der wichtigsten Fakten drängt sich nun die Frage auf: Welche Schlüsse lassen sich daraus für unsere Untersuchung ziehen?

1. Riesige Operation mit konzentrierten Ressourcen: Das Brechen des deutschen Codes durch die Alliierten war eine riesige, gut durchdachte und zudem koordinierte Operation. Der Premierminister Churchill erkannte die strategische Wichtigkeit und stellte die entsprechenden Ressourcen zur Verfügung. In dieser Operation spielten zwar einzelne Individuen – unter ihnen Alan Turing – Schlüsselrollen. Die Resultate konnten aber nur durch die Konzentration der Ressourcen erreicht werden. Hier zählte nicht nur der Geist – auch wenn das einzelne Akteure heute so darstellen – sondern im richtigen Moment auch der kluge Einsatz von militärischer Gewalt, wie etwa die Bedeutung der Schiffsüberfälle zeigt.

2. Die Lösung des Enigma-Rätsels war eine britische Leistung: Die zweite Bemerkung liefert bereits Anhaltspunkte zur diskurskritischen Beurteilung: Die überwiegende Mehrzahl der relevanten historischen Untersuchungen stammt aus der Feder von britischen Autoren. Direkt oder indirekt wird immer wieder auf die grosse intellektuelle Leistung hingewiesen – und damit auch eine intellektuelle Überlegenheit über den einstigen Feind postuliert. Und weil gerade dieser Aspekt des britischen Sieges bis Mitte der 70er Jahre nicht gefeiert werden durfte, muss er am Ende des 20.Jahrhunderts und auch darüber hinaus so stark betont werden.

3. Der Enigma-Stoff ist eine gute Geschichte mit farbigen Personen: Die Geschichte der Enigma und ihrer Entschlüsselung liefert alle Ingredienzien für eine gute Geschichte: es gibt zwei Widersacher – Nazi-Deutschland und Grossbritannien – es gibt Geheimnisse und Leute, die diese Geheimnisse knacken wollen, und es gibt offenbar einen unerschöpflichen Fundus von Details, die diesem Bild immer wieder neue Aspekte hinzufügen. Ganz wichtig: Die Enigma-Geschichte lässt sich personalisieren – und gleich noch durch eine Person, die ausserordentlich facettenreich ist, den Mathematiker Alan Matheson Turing, der nebenbei auch gleich noch zum Miterfinder des Computers avanciert. Dass Turing homosexuell war macht die Geschichte noch ein Stück interessanter. Nicht alle, die sich an diesem Stoff versucht haben, konnten das verarbeiten, wie wir im drittten Teil noch sehen werden.

Seitenblick auf den Mythos

Was bringt nun diese umfangreiche Einführung in Bezug auf das Verständnis der Enigma-Geschichte als Mythos? – Alle drei genannten Aspekte scheinen den mythischen Charakter der Geschichte zu bestärken. Ganz vereinfacht gesprochen könnte man diese noch einmal so zusammenfassen: Lange Zeit verborgen gelangen die Heldentaten der britischen Codebreaker endlich ans Licht. Sie fügen der Tatsache des militärischen Sieges eine wichtige, vielleicht entscheidende Komponente hinzu: Jene der geistigen Überlegenheit. Und sie machen damit den Sieg noch grösser, runder, perfekter. In dieser Verknappung kommen die mythologischen Elemente noch stärker zum Vorschein: Zu nennen ist die lange Latenzzeit – die Tatsache, dass diese Geschichte so lange unbekannt, verborgen war. Und zweitens die Stilisierung der Entschlüsselung als kollektive, heroische Tat. Ganz entscheidend: Die Schlüsselpersonen in diesem Drama waren keine ›gewöhnlichen Soldaten‹, sondern eigenwillige Intellektuelle vom Schlag eines Alan Turing.

Diese Geschichte lässt sich auf unterschiedliche Arten erzählen, doch es bleibt letztlich immer dieselbe Geschichte. Damit ist die Bühne bereit, die in den nächsten beiden Kapiteln bespielt wird. Wir werden dort einmal die Akteure und das andere Mal ihre Zeugnisse untersuchen.

Der Krieg und die Geburt des Computers

Die Enigma und die Geräte, die zu ihrer Dekodierung ersonnen wurden, gehören ins Umfeld der Computergeschichte. Stimmt aber Friedrich Kittlers These, dass der Zweite Weltkrieg die Geburt des Computers »aus dem Geist Turings und seiner nie gebauten Prinzipienschaltung« hervorbrachte?[116]

Die Enigma und ihre Entzifferung liegen nicht auf der Hauptachse der Computer-Entwicklung, wie dies Pierre Lévy dargestellt hat. Er zeigt, wie die Entwicklungen des deutschen Computerpioniers Konrad Zuses vom Krieg unterbrochen wurden: das Heereswaffenamt weigerte sich nämlich, sein Vorhaben zu finanzieren.

Etwas komplexer lagen die Dinge in Grossbritannien: Die Geheimhaltung hinderte die Industrie daran, die Geräte von Bletchley Park weiter zu entwickeln. Nach dem Krieg wurden praktisch alle Unterlagen und auch die berühmten Entzifferungsmaschinen Bombe und Colossus zer-

116 Friedrich Kittler: Grammophon, Film, Typewriter. Berlin 1986. Fink. S. 363.

stört.[117] Die Akteure dieser Innovationen arbeiteten allerdings weiter und für sie waren ihre Arbeiten von Bletchley Park – auch wenn sie zerstört wurden – wichtig. Die im Krieg gewonnenen Erkenntnisse halfen ihnen mit, die Entwicklung des Computers voranzutreiben. Dies gilt sowohl für Alan Turing, der sich nach dem Krieg mit der Entwicklung des Computers beschäftigte, als auch für die Erfinder von Colossus, Max Newman und Tommy Flowers.[118]

Die Technologie-Entwicklung verlief nach dem Krieg auf zwei parallelen Schienen: Einer öffentlichen und einer geheimen. Eine kleine Geschichte mag die Absurdität dieser Situation verdeutlichen. Aufgrund dieser rigiden Geheimhaltung wurde die sogenannte Public Key Kryptografie – Grundlage der modernen, asymmetrischen Chiffrierung – zweimal erfunden: Einmal Mitte der 70er Jahre von den US Mathematikern Whitfield Diffie und Martin Hellmann und dem Trio Ronald Rivest, Adi Shamir, Leonard Adleman. Ende der 60er Jahre hatten allerdings die britischen Kryptografie-Spezialisten James Ellis, Clifford Cocks und Malcolm Wiliamson dieselbe Erfindung gemacht, nur durfte sie nicht publiziert werden.[119]

Wie steht es also um Kittlers These, dass nämlich der Krieg am Anfang der Entstehungsgeschichte des Computers stand? Nun, so wie es aussieht, liegt er damit richtig, wenn das auch nicht immer und in allen Teilen klar war.

Die Enigma und der Computer als universales Medium

Welche Rolle haben die Enigma und ihre Entschlüsselung für die Computergeschichte gespielt – und noch spezieller, für die Geschichte des Computers als universalem Medium? Vor dem Versuch einer Antwort bedarf die Frage selber einiger Erklärungen und Präzisierungen. Was ist mit Computergeschichte gemeint und was mit Computer als universersalem Medium?

---

117 Pierre Lévy: Die Erfindung des Computers. In: Michel Serres: Elemente einer Geschichte der Wissenschaften. Frankfurt am Main 1994. Suhrkamp. S.907.

118 Jack Copeland: Colossus and the Rise of the Modern Computer. In: Ders.:Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford 2006. Oxford University Press. S. 101-115.

119 Simon Singh: Geheime Botschaften. München 2000. Hanser. S. 347.

Nur allzu oft wird die Computergeschichte als linearer, zielgerichteter und damit geradezu teleologischer Vorgang dargestellt. Das mag mit einer gewissen Bequemlichkeit zu tun haben, Dinge ex post zu erklären und zielgerichtete Prozesse zu vermuten wo in Wirklichkeit eher Chaos und Kontingenz regierten. Kaum einer hat das treffender beschrieben als der französische Historiker und Philosoph Pierre Lévy:

»Die Geschichte der Informatik lässt sich (wie vielleicht jede andere Geschichte auch) als unbestimmte Verteilung schöpferischer Momente und Orte betrachten, als eine Art löchriges, zerrissenes, unregelmässiges Meta-Netz, in dem jeder Knoten, das heisst jeder Akteur, die Topologie seines eigenen Netzes, seinen eigenen Zielen entsprechend bestimmt und alles, was von den benachbarten Knoten zu ihm gelangt, nach seiner Weise deutet. Jeder lebendige Knoten dieses Geflechts reinterpretiert die Vergangenheit, die ihm von den anderen überliefert wird, als müsste sie geradewegs auf die eigenen Entscheidungen zu laufen, und entwirft eine Zukunft, in der sich seine Optionen geradlinig fortsetzen. Doch diese Zukunft liegt, ebenso wie das Bild der Vergangenheit, wieder in der Hand der nachfolgenden Knoten, und so ad inifnitum. Nach dieser Sicht der Dinge sind die Begriffe des Vorläufers oder Begründers – versteht man sie im strengen Sinne – wenig angemessen. [...] Technische Erfindungen erweisen sich als chaotisches Gewimmel von Basteleien, Neuverwendungen, prekären Verfestigungen, operativen Anordnungen.«[120]

Georg Christoph Tholen hat für diese Ausgangslage den Begriff der »dissipativen Ursprünge und Dispositive« benutzt.[121] Der Begriff der Dissipation stammt aus der Thermodynamik und meint eine Struktur, die nur durch Aufnahme von Energie erhalten bleibt. Gemeint ist damit, dass in der Geschichte des Computers immer wieder höchst heterogene Momente und Faktoren gewirkt haben oder eben wie Lévy es oben ausdrückt eine »unbestimmte Verteilung schöpferischer Momente und Orte«.[122]

Zum Begriff des Computers als Medium: Zwar ist der Computer auch heute eine Realisation der Vision von Leibniz und dient der »Befreiung von der ermüdenden Last eintöniger, geistiger Tätigkeit«.[123] Als

120 Pierre Lévy: Die Erfindung des Computers. In: Michel Serres: Elemente einer Geschichte der Wissenschaften. S. 943.

121 So im nicht veröffentlichten Gutachten zur vorliegenden Disseration. Basel Juni 2007.

122 Pierre Lévy: Die Erfindung des Computers. S. 943.

123 Friedrich L. Bauer: Kurze Geschichte der Informatik. München 2007. Fink. S. 2.

»Leitmedium der Gegenwart«[124] ist er aber mehr als nur der brave Rechenknecht und damit nicht mehr nur Gegenstand der Informatik – eleganter Englisch Computer Science – sondern zahlreicher anderer Disziplinen, darunter wie im vorliegenden Fall auch der Medienwissenschaft.

Dass der Computer als universelles Medium dient, mag heute unmittelbar einleuchten – dafür sprechen allein schon die unzähligen und sich ständig vermehrenden Computermedien – und wir ahnen in unserem Alltag gerade noch, dass hinter der rasant steigenden Verfügbarkeit von medialen vermittelten Informationen letztlich die Digitalisierung steckt, die Tatsache nämlich, dass die Information, egal ob in Musik oder Film, Foto oder Text, Zeitung oder Buch, letztlich auf die binären Elementarteile Null und Eins rückführbar sind.

Wissenschaftsgeschichtlich und -theoretisch steht dahinter aber ein epochaler Umbruch: Das universelle Medium Computer ist nicht Ergebnis einer stetig kumulativen Entwicklung in der Rechnertechnik, sondern folgt einem Paradigmenwechsel, der sich am Ende des Zweiten Weltkrieges im Umfeld neuester Waffentechnik ereignete.[125] Der Computer zeigt sich dabei als symbolverarbeitende Maschine, die er eigentlich auch in der Vision von Alan Turing immer schon war. Daraus ergibt sich eine »epistemische Nachbarschaft zwischen der Welt der Maschinen und der Welt des Symbolischen«[126] und »ein geistes- und naturwissenschaftliches Begriffsfeld der Information und Übertragung, welches nichtrückführbar auf das der Materie oder Energie ist und den kategorialen Rahmen auch des soziologischen und anthropologischen Wissens verschiebt.«[127]

Diese Feststellungen haben weitreichende Folgen:

»1. Mit dem Prinzip der strikten Sequentialität wurde dank der von John von Neumann architektural vorgegebenen, entscheidungssicheren Funktionslogik des Computers das bis heute gültige Verfahren, in Zahlen transformierte Daten und Befehle zu speichern, einschliesslich derjenigen Befehle, die diese Opera-

124 Norbert Bolz: Computer als Medium. Einleitung. In: Norbert Bolz; Friedrich A. Kittler; Christoph Tholen (Hg.): Computer als Medium. München 1994. Fink. S. 9.

125 Wolfgang Hagen: Die verlorene Schrift. Skizzen zu einer Theorie der Computer. In: Friedrich A. Kittler; Georg Christoph Tholen (Hg.): Arsenale der Seele. Literatur und Medienanalyse seit 1870. München 1989. Fink. S. 212.

126 Friedrich A. Kittler: Die Welt des Symbolischen – eine Welt der Maschine. In: Ders.: Draculas Vermächtnis. Technische Schriften. Leipzig 1993. Reclam. S. 58.

127 Georg Christoph Tholen: Die Zäsur der Medien. Kulturphilosophische Konturen. Frankfurt 2002. Suhrkamp. S. 186.

tionen wiederum steuern, technischer Standard und dadurch auch die universelle Eigenschaft des digitalen Mediums, material wie medial unspezfische Zustände von berechenbaren Zeichenprozessen zu simulieren. [...]

2. Die Auflösung des referentiellen Bezugs auf vorgegebene Zweckbestimmungen durch die universelle symbolische Maschine verkreuzt sich mit dem, was die moderne Sprachwissenschaft mit der Überwindung der vorher als natürlich oder referentiell gedachten Eigenschaft der Zeichen denkbar wurde: Arbitrarität, Differentialität und Substituierbarkeit der verweisenden Zeichen.«[128]

Was ist damit gemeint? – Daten und Zahlen werden digital gespeichert und transformiert. Dabei wird nicht zwischen Befehlen und Arbeitsdaten unterschieden. Dieses neue digitale Medium ist in der Lage, beliebige andere Zeichenprozesse und damit jedes andere Medium zu simulieren. In dieser maschinellen Verarbeitung löst sich der referentielle Bezug der verarbeitenden Zeichen vollends auf.

Die linear-diskrete Folge der Buchstabenschrift, so Hagen, ist im Computer sistiert und aufgehoben. Der universelle Rechner, der Buchstaben wie jedes andere alphanumerische Zeichen behandelt, kennt keine Schrift: Er simuliert sie nur umso besser.[129]

Wo genau die dissipativen Ursprünge des Computers liegen kann hier nicht im Einzelnen aufgezeigt werden. Sie sind aber, wie Wolfgang Hagen klarmacht, in einem grösseren Umfeld zu suchen, als vielleicht gemeinhin angenommen wird, wie auch das folgende Beispiel zeigt: Sie (die Computer DL) exekutieren ein »steuerlogisches Wissen, das eine eher profane und abseitige Nebenlinie der klassischen Steuertechnik bis zur Unkenntlichkeit radikalisierte: Nämlich die der Walzen und Räder der automatischen Glockenspiele im 14. Jahrhundert – die ersten extern gesteuerten Maschinenwerke, die das Abendland kennt. Freilich: das durch Walzen und Stifte, Kerben und Federn in die Musik- und Figurenmaschinen der Höfe und Kirchen eingefügte Wissen wurde als solches nicht erkannt: Es war schlicht Musik und Klang...«[130]

Zurück zur Enigma-Geschichte. Einen nicht unwesentlichen Anteil an ihrer Entschlüsselung hatte der britische Mathematiker Alan M. Turing, wie Andrew Hodges in seiner Turing-Biografie und dort namentlich im Kapitel »Relais-Rennen«[131] gezeigt hat. Turing hatte bereits 1934 in

128 Ebenda.

129 Wolfgang Hagen. Die verlorene Schrift. S. 227.

130 Ebenda. S. 212.

131 Andrew Hodges: Alan Turing. Enigma. Wien, New York 1994. Springer. S. 187-280.

seinem bahnbrechenden Aufsatz »On Computable Numbers«[132] eine universelle Maschine beschrieben, die in der Lage war, jede berechenbare mathematische Aufgabe zu lösen. Die Betonung liegt auf der Eigenschaft ›berechenbar‹, es ging nur um Aufgaben, für die es prinzipiell eine Lösung gab, und das ist in der Mathematik bei weitem nicht immer der Fall. Die in seinem Aufsatz beschriebene Einrichtung war zwar noch keine Blaupause für eine Maschine. Der moderne, programmierbare Automat ist, wie Wolfgang Coy schreibt, zuerst auf dem Papier entstanden, ohne dass seine Umsetzbarkeit ersichtlich wurde. Die Turing-Maschine ist ein formallogisches Modell der berechenbaren Funktionen, Urbild des programmierbaren Automaten – und in logischer Hinsicht schon sein Abschluss.[133] Die Maschine von Alan Turing war in einem gewissen Sinn eine wenn auch sehr abstrakt und modellhaft gedachte Schreibmaschine. Tatsächlich hatte Alan Turing schon als Kind davon geträumt, Schreibmaschinen zu erfinden,[134] und diese Faszination scheint ihm auch im Erwachsenenalter geblieben zu sein. Für seinen epochalen Aufsatz erinnerte er sich offenbar wieder daran:

»Statt die vorgeschriebene Handschrift seiner Public School zu lernen, reduzierte er (Turing) Schreibmaschinen auf ihr nacktes Prinzip: erstens das Speichern oder Schreiben, zweitens das Rücken oder Übertragen, drittens das (zuvor Sekretärinnen reservierte) Ablesen oder Berechnen von diskreten Daten, also Blockbuchstaben und Zahlen.«[135]

Tatsächlich ist die Schreibmaschine, wie wir seit Kittler wissen, ein Meilenstein in der Technisierung von Information und damit alles andere als ein harmloses Gerät.[136]

Die Enigma trat bekanntlich nur kurze Zeit nach der Veröffentlichung dieses Aufsatzes im Jahr 1937 ins Leben von Alan Turing: Alan Turing diente während des Krieges in Bletchley Park und hat entschei-

132 Vollständig: »On Computable Numbers, with an Application to the Entscheidungsproblem«. Deutsch: Über berechenbare Zahlen mit einer Anwendung auf das Entscheidungsproblem. In: Turing, Alan M.: Intelligence Service. Hg. von Bernhard Dotzler und Friedrich Kittler. Berlin 1987. Brinkmann und Bose. S. 17-60.

133 Wolfgang Coy: Aus der Vorgeschichte des Mediums Computer. In: Norbert Bolz; Friedrich A.Kittler; Christoph Tholen (Hg.): Computer als Medium. München 1994. Fink. S. 23.

134 Andrew Hodges S. 114.

135 Friedrich Kittler: Grammophon, Film, Typewriter. Berlin 1986. Brinkmann und Bose. S. 364

136 Ebenda S. 4.

dende Beiträge zur Entschlüsselung der komplizierten deutschen Maschine geleistet.

Die Enigma nur als Verschlüsselungsmaschine zu bezeichnen, wäre kurzsichtig. Sie muss vielmehr in einem Kommunikations- und Medienverbund gesehen werden, deren letztes Ziel nicht die Verschlüsselung, sondern die Steuerung von taktischen Operationen war. Besonders eindrücklich und wirksam war diese Steuerung im Fall der Koordination der U-Boot Flotte von Admiral Dönitz. Ohne Übertragung von verschlüsselten Funksprüchen wäre die tödliche Koordination der U-Boote in der Wolfsrudel-Taktik nicht möglich gewesen. Und hier zeigt sich denn auch die Nähe zum Medium Radio, das ja, wie wir wissen, ein unerwünschtes Nebenprodukt einer Kriegserfindung war:

»Sechs Jahre lang, seit den ersten Frontmusiksendungen des Schützengrabenkrieges, hatte der deutsche Generalsstab die Möglichkeit eines Unterhaltungsrundfunkes bekämpft. Denn Marconis Erfindung erfüllte zwar den Zweck, das Risiko angezapfter Telegraphenkabel zu vermeiden, geriet aber selber in den Verdacht, das Risiko bis zur weltweiten Abhörbarkeit zu steigern. Worauf der Erfinder konterte, Admirale und Generale könnten sich immer noch durch Übermittlung chiffrierter Nachrichten schützen.«[137]

Was nun die Enigma und ihre Entschlüsselung so entscheidend im Kontext des Computers als Medium machte, war die Tatsache, dass beide Prozesse, Verschlüsselung und Entschlüsselung im Grunde sprachliche Prozesse waren, die mit maschinellen und im Grund mathematischen Methoden betrieben wurden. Damit war eine Maschine auf das Feld der Schrift und damit auch der Sprache vorgerückt – und damit war ein entscheidender Schritt in Richtung universalem Medium getan, auch wenn die Bearbeitung weit von dem weg war, was in Sachen Sprache und Schrift heute möglich ist.

Die Schrift ist, so Wolfgang Coy, Urbild der ›künstlichen‹ Medien, von der Bilder und Konsonantenschrift über den wesentlichen Einschnitt der Lautschrift mit Vokalen bis zur Produktion des Textes. Text im heutigen Sinn – mit Struktur und Absätzen – entstand erst im 12. Jahrhundert. Darauf gründete der Buchdruck. Der nächste Schritt war der elektrische Funke. Elektrische Signale und elektrisches Licht bestimmen die Medien nach der Erfindung des Buchdrucks. Kalkulations- und Textverarbeitungsprogramme waren entscheidende Anwendungen, die dem Sie-

137 Friedrich Kittler und Bernhard Dotzler in: Alan Turing. Intelligence Service. Berlin 1987. Brinkmann und Bose. S. 216.

geszug des Computers den Weg ebneten und den Computer aus der Bastlerszene herausrissen. [138]

Die Schrift und damit Sprache wurden in der Enigma manipuliert.

»Anstelle der eindeutigen Zuordnung von Tastenbedienung und Outprint, über die nur Tippfehler hinwegtrösten, bescherte die Enigma alle Freuden einer diskreten, nämlich kombinatorischen Mathematik. Die 26 Buchstaben des Alphabets liefen über Elektroleitungen in ein Verteilernetz aus drei (später vier oder fünf) Walzen, das immer wieder andere Schreibmöglichkeiten durchschaltete. Bei jedem Anschlag rückten die Walzen (wie Sekunden-, Minuten- und Stundenanzeiger) um eine Sechsundzwanzigsteldrehung vor, um erst nach 267 oder 8 Milliarden Textbuchstaben zur Ausgangsstellung zurückzukehren. Ergebnis möglicher Interzeption war also reiner Buchstabensalat, den nur eine antisymmetrisch betriebene Enigma auf Radio-Empfängerseite wieder decodieren konnte.«[139]

Und die Maschine zum Verschlüsseln hat auch eine Maschine zum Entschlüsseln auf den Plan gerufen. Denn was eine Maschine verschlüsselt muss eine Maschine auch wieder entschlüsseln können: »Als Pseudo-Zufalls-Generator produzierte die Geheimschreibmaschine Unsinn nur relativ auf Systeme, deren Periode die seine unterschritt. Turings Göttin aber fand im Buchstabensalat Regularitäten.«[140]

Alan Turing nannte sie, in Anlehnung an eine ähnliche von den Polen bereits eingesetzte Maschine, Bombe oder Bomba. Sie trat in Funktion, nachdem die Entschlüsselungs-Spezialisten für einen bestimmten Funkspruch einen so genannten Crib, ein wahrscheinliches Wort identifiziert hatten. Dieser musste mit allen möglichen Stellungen geprüft werden. Die Anzahl der Stellungen war aber sehr hoch. Turing schlug vor, drei Maschinen zu verbinden. Mit einer genialen Anordnung von Rückkoppelungsschleifen gelang es ihm, die Anzahl der zu prüfenden Möglichkeiten drastisch zu verringern. Cribs, Schleifen und elektrisch gekoppelte Maschinen erbrachten zusammen eine erstaunliche kryptoanalytische Leistung. [141]

Kombinatorik, nicht Arithmetik war das Kerngeschäft der Bomba. Anders als andere frühe Rechner waren ihr Output nicht berechenbare

138 Wolfgang Coy S. 29.

139 Friedrich Kittler: Die künstliche Intelligenz des Weltkriegs: Alan Turing. In: Kittler, Friedrich A.; Tholen, Georg Christoph (Hg.): Arsenale der Seele. Literatur und Medienanalyse seit 1870. München 1989. Fink. S. 194.

140 Friedrich Kittler: Grammophon, Film, Typewriter. S. 369

141 Im Einzelnen beschrieben bei Andrew Hodges. Turing. S. 203.

Tabellen wie sie etwa für die Artillerie als ›Firing Tables‹ in grosser Zahl und hoher Qualität verlangt wurden; der ENIAC Rechner beispielsweise wurde für solche ballistischen Echtzeitberechnungen entwickelt. Die kombinatorischen Operationen der Enigma-Entschlüsselungs-Maschinen erinnern vielmehr an eine andere frühe Maschinengeneration, deren Ziel ebenfalls nicht die Arithmetik war: Die Rede ist von den Maschinen, die Herman Hollerith (1860-1929) entwickelte und in der amerikanischen Volkszählung von 1890 zum ersten Mal einsetzte. Sie benutzten die bereits 1725 erfundene Lochkarte und dienten einzig und allein dem maschinellen Sortieren von Daten.[142]

Am selben Ort, an dem die Enigma entschlüsselt wurde, wurde eine weitere Maschine entwickelt, die in der verzweigten Geschichte des Computers wichtig geworden ist: Die Colossus. Sie diente der Entschlüsselung einer Maschine, die völlig anders funktionierte als die Enigma: Die Rede ist von der Lorenz Schlüsselzusatzmaschine SZ42, die mit einem Fernschreiber verbunden wurde und dessen digitale Signale verschlüsselte. Aufgrund eines katastrophalen Fehlers auf deutscher Seite – ein Operator hatte eine Meldung zweimal in identischer Chiffrierung übertragen – konnte in Bletchley Park die innere Struktur der unbekannten Verschlüsselungsmaschine rekonstruiert werden. Die Ermittlung der Anfangsstellung erforderte aber Tage mühsamer Arbeit. Abhilfe könnte nur eine Maschine schaffen, die diese mühsame Arbeit übernahm. Das war die Idee des Mathematiker Max Newman (1897-1984) – auch er ein Angehöriger der Bletchley Park Truppe. Konkret ging es um das Durchprobieren von zwei langen Zahlenkolonnen, die auf zwei parallel laufenden Fernschreiberstreifen aufgezeichnet waren. Auf dem einen Streifen befand sich der verschlüsselte Text, auf dem zweiten der rekonstruierte Code, gewonnen aus der Analyse der Maschine. So konnte der fragliche Text mit jeder möglichen Anfangsposition des Codes ausprobiert werden. Ein Algorithmus ermittelte die Relation von zwei Zeichen der beiden Streifen und gab bei besonders günstigen Kombinationen eine Botschaft aus. Damit mussten die Code-Brecher mit dem ›Tunny‹ genannten Nachbau der Verschlüsselungsmaschine, nur noch ganz wenige Möglichkeiten durchprobieren. Erste Versuche mit Fernschreiber-Streifen scheiterten, erst die Idee, für die Ermittlung der Wahrscheinlichkeiten Röhrenschaltungen zu verwenden, brachte den Durchbruch. Colossus war ein Meilenstein in der Computer-Entwicklung, auch wenn seine Existenz ähnlich wie die Enigma-Entschlüsselung, bis 1974 geheim

142 Wolfgang Hagen: Die verlorene Schrift. S. 215.

gehalten wurde und bis dahin der amerikanische ENIAC als erster, digitaler Rechner galt.[143]

Ein weiterer Meilenstein in der Entwicklung des Computers als Medium vollzog sich jenseits des Atlantiks, und zwar im ebenfalls geheimen Los Alamos Projekt, der Entwicklung der ersten Atom- und Wasserstoffbombe. Die mathematische Berechnung von Wasserstoffbomben war eine Aufgabe, welche Physiker und Mathematiker an ihre äussersten Grenzen brachte. Ein maschineller Rechner sollte dabei helfen – er erhielt den Namen EDVAC. In diesem Kontext formulierte der leitende Mathematiker von Los Alamos, John von Neumann, das Konzept, das später zur Blaupause und Modell aller weiteren Computer wurde. Die entscheidenden Ideen in seinem bahnbrechenden Aufsatz stammen indes, wie wir heute wissen, nicht von ihm selber, sondern von seinen Kollegen John Mauchly (1907-1980) und J. Presper Eckley (1919-1995). Man geht heute davon aus, dass John von Neumann auch die Arbeiten von Alan Turing kannte, namentlich seinen Aufsatz »On Computable Numbers«, der ja schon 1937 publiziert worden war, schliesslich waren sich die beiden ja während des Aufenthalts von Turing in Princeton in den Jahren 1937/38 begegnet.[144]

Zwischen der Entschlüsselungs-Operation von Bletchley Park und der Entwicklung der Atombombe gibt es einige weitere, bemerkenswerte Parallelen: Beide Male handelte es sich um wissenschaftliche Unternehmungen in riesigem, um nicht zu sagen, industriellen Ausmass. Beide

143 Jack Copeland: Colossus and the Rise of the Modern Computer. In: Ders.: Colossus. The Secrets of Bletchley Park's Codebreaking Computers. Oxford 2006. Oxford University Press. S. 101-115.
Dominik Landwehr: 10 000 Menschen und 1500 Elektronenröhren knackten die Nazi-Codes. In: Neue Zürcher Zeitung vom 2.3.2007. S. 63. Langversion unter: www.peshawar.ch/tech/docus/colossus.pdf vom 16.2.2008.

144 Andres Hodges: Turing S. 169.
Der Atomphysiker Stanley Frankel, der in Los Alamos Seite an Seite mit John von Neumann arbeitete, äusserte sich diesbezüglich offensichtlich sehr klar: »I know that in or about 1943 or 44 von Neumann was well aware of the fundamental importance of Turing's paper of 1936 ›On Computable Numbers‹ [...] Von Neumann introduced me to that paper and at his urging I studied it with care. Many people have acclaimed von Neumann as the ›father of the computer‹ (in a modern sense of the term) but I am sure that he would never have made that mistake himself. He might well be called the midwife, perhaps, but he firmly emphasized to me, and to others I am sure, that the fundamental conception is owing to Turing [...] « Zitiert nach Jack Copeland: Colossus. S. 114.

Unternehmungen – Los Alamos und Bletchley Park – waren von Regierungen ausgelöst und überwacht. Beides waren Geheimunternehmungen bei denen auch die Beteiligten möglichst wenig wissen sollten[145] und beide Unternehmungen sind mit der Geschichte des Computers verbunden. Der Leiter der Los Alamos Operation, Vannevar Bush schliesslich machte nach dem Krieg nicht nur durch seine Erinnerungen an das Manhattan-Projekt von sich reden sondern auch durch eine zunächst harmlos anmutende Ideenskizze, die er 1945 unter dem Titel »As We May Think« veröffentlichte. Er entwarf darin eine Art von multimedialem Schreibtisch, dem er den Namen ›Memex‹ für ›Memory Extender gab‹. In seinem Aufsatz nahm der amerikanische Ingenieur die mediale Entwicklung des Computers voraus.[146]

John von Neumann formulierte in seinem Aufsatz »First Draft of a Report on the EDVAC«zwei entscheidende Prinzipien: Erstens die absolute Sequentialität aller Prozesse im Computer. Was auch immer im Innern der Maschine passiert, es hatte in streng geregelter Abfolge zu passieren. Das zweite ebenso entscheidende Prinzip war die Forderung, dass auch Daten und Programme gleich zu behandeln sind und beide am gleichen Ort zu speichern seien. Erst dadurch konnten laufende Prozesse das Programm verändern.[147] Nun waren die Grundlagen da:

---

145 Im Fall von Los Alamos war dies aber nur schwer durchzusetzen. Robert Jungk berichtet in seinem Buch »Heller als tausend Sonnen« über die Schwierigkeiten, die so genannte ›compartmentalization‹ aufrecht zu erhalten: Sie verärgerte die beteiligten Wissenschafter, die sie mit aller Kraft zu umgehen suchten. Im Fall des Rechenzentrums von Los Alamos musste diese Politik offenbar sogar aufgegeben werden, weil die beteiligten Wissenschafter, ohne das Ziel ihrer Aufgaben zu kennen, kaum für die schwierigen mathematischen Aufgaben zu motivieren waren. Robert Jungk: Heller als tausend Sonnen. Das Schicksal der Atomforscher. München 1990. Heyne. S.138-146.

146 Vannevar Bush: As We May Think. In: The Atlantic Monthly. 176 (1) (1945) S.101-108. www.theatlantic.com/doc/194507/bush vom 16.2.2008 Auch in:Noa Wardrip-Fruin und Nick Montfort: The New Media Reader. Cambridge (MA), London, 2003 MIT Press. S. 35-48.

147 John von Neumann: First Draft of a Report on the EDVAC. In: Brian Randell: The Origins of Digital Computers. Selected Papers. Third Edition. Berlin, Heidelberg, New York 1982. Springer. S. 383-392.
»Selten ist ein handschriftlicher Konzept-Entwurf, unvollendet, fehlerhaft abgeschrieben und schlecht hektografiert, so berühmt und einflussreich geworden wie dieser. Denn von Neumanns ›First draft of a Report on the EDVAC‹ ist nichts anderes als der Architekturgrundriss aller unserer heutigen Computer und damit auch die Inauguration aller Maschinen-

»1945 waren die Prinzipien der Neumannschen Logik je für sich nicht neu, wohl aber in der paradigmatisch radikalen Kombination. Jetzt erst konnte die Maschine, durch Befehle gesteuert, dem Speicher Zahlen (oder Befehle) entnehmen, sie (wie Zahlen) verarbeiten und in gleiche oder andere Speicherzellen an den Speicher zurückgeben, d.h. sie kann den Inhalt des Speichers verändern, insbesonders auch die im Speicher gespeicherten Befehle, einschliesslich der Befehle, die ihren Operationslauf steuern. Den Inversionen und Rekursionen von Befehlen und Befehlsfolgen, die 1945 noch niemand hinreichend formulieren konnte, werden von nun an keine Grenzen gesetzt sein.«[148]

Tatsächlich spielte der Krieg eine entscheidende Rolle für die Entwicklung des Computers, wie wir ihn heute kennen. Beim genaueren Hinsehen überrascht die Tatsache, wie gut sich die einzelnen Exponenten kannten und wie sich deren Wege auch gelegentlich kreuzten: So lehrte John von Neumann in den 30er Jahren in Princeton in engster Nachbarschaft zu Alan Turing.[149]

Ein weiterer Name muss in diesem Kontext genannt werden: Norbert Wiener (1891-1964): Er versuchte im Zweiten Weltkrieg einen Rechner zu entwickeln, der die Position eines Flugzeugs im Voraus berechnen konnte, den so genannten Anti-Aircraft-Predictor.[150] Dem Versuch war

---

sprachen, die uns seither umgeben. So verständlich, dass jeder Verweis auf einen real existierenden ENIAC fehlt, so klar muß der Historiker festhalten: Es gibt buchstäblich kein Detail in dieser von Neumannschen Architektur, das nicht im ENIAC-Team, insbesondere also von Mauchly und Eckert, entwickelt worden wäre. Das hat nach dem Krieg zu bitterstem Blut und in der Folge auch zu einem Patent-Prozess geführt, der bis in die Mitte der siebziger Jahre andauerte.« In: Wolfgang Hagen: Das ›Los Alamos Problem‹. Zur Entstehung des Computers aus der Kalkulation der Bombe. Ursprüngliche Langfassung des Katalogtextes zu »7 Hügel. Wissen«. Berlin 2000. Publiziert unter: www.whagen.de vom 16.2.2008.

148 John von Neumann zitiert nach Wolfgang Hagen: Die verlorene Schrift. S. 219.

149 Ebenda S. 214 sowie Andrew Hodges: Turing. S. 112.

150 Norbert Wiener schrieb dazu: »Der entscheidende Faktor für diesen neuen Schritt war der Krieg.[…] Bei Kriegsbeginn richteten das deutsche Luftwaffenpotential und die defensive Lage Englands die Aufmerksamkeit vieler Wissenschaftler auf die Entwicklung der Flugabwehrartillerie. Schon vor dem Krieg war es klar geworden, dass die Geschwindigkeit des Flugzeugs alle klassischen Methoden der Feuerleitung überwunden hatte und dass es nötig war, alle notwendigen Rechnungen in die Regelungsapparatur selbst einzubauen. Diese waren sehr schwierig geartet

kein Erfolg beschieden, aber die Arbeiten Wieners führten zur einer ganz bestimmten Sichtweise von zunächst kriegsrelevanten Operationen, die später verallgemeinert wurden: der Kybernetik. Sie gründet auf der Idee, Flugzeug und Beobachter zusammen als System zu betrachten. Wiener führte den Begriff der Rückkoppelung in die Informationstheorie ein.[151]

Die Enigma und ihre Entschlüsselung nehmen einen genauen Platz in der Wissenschaftsgeschichte und in der Geschichte des Computers als Medium ein: Hier wurden keine Daten sortiert und keine Geschütztabellen berechnet, hier wurde mit den Mitteln der Kombinatorik in Schrift geronnene Sprache rekonstruiert. Hier wurden, wenn auch nur in ihren ersten Ansätzen, Sprache ›gerechnet‹; dass spätere Computer perfekte Medienmaschinen sein würden, die mit Schrift und Sprache, Bild und Ton ebenso souverän umgehen würde wie mit Zahlen, konnte damals noch niemand ahnen.

durch die Tatsache, dass nicht zu vergleichen mit allen vorher betrachteten Zielen – ein Flugzeug eine Geschwindigkeit hat, die ein sehr ansehnlicher Bruchteil der Geschwindigkeit des Geschosses ist, das zum Beschuss verwendet wird. Demgemäss ist es außerordentlich wichtig, das Geschoss nicht auf das Ziel abzuschießen, sondern so, dass Geschoß und Ziel im Raum zu einem späteren Zeitpunkt zusammentreffen. Wir mussten deshalb eine Methode finden, die zukünftige Position des Flugzeugs vorherzusagen.« Zitiert nach Friedrich Kittler: Grammophon. Film. Typewriter. S.374.

151 Peter Galison: Die Ontologie des Feindes. Norbert Wiener und die Vision der Kybernetik. In: Michael Hagner (Hg.): Ansicht der Wissenschaftsgeschichte. S. 430-487. Frankfurt 2001. Fischer.