Cryptology and redaction – a strange symbiosis

Dermot Turing
Kellogg College
60-62 Banbury Road
Oxford OX2 6PN UK
dermotturing@btinternet.com

Abstract

This paper explores the relationship between cryptology and redaction. Redaction can be a frustration to historical cryptology research. Examples of redactions of historical papers relevant to cryptology are presented. It is concluded that the practice of redaction is often ineffective and the policy rationale behind redactions difficult to understand.

1 Introduction

Cryptography is concealment: concealment of content of a communication, while the communication itself is overt. For historians of cryptology, the concealment can go further than the content of communications. The processes of cryptography and cryptanalysis may themselves be secret, requiring a further layer of obfuscation, created through security laws, non-disclosure contracts and censorship. When disclosures are allowed, they are frequently partial, with documentation released into the public domain only with redactions. This paper examines the interplay between redaction and cryptology.

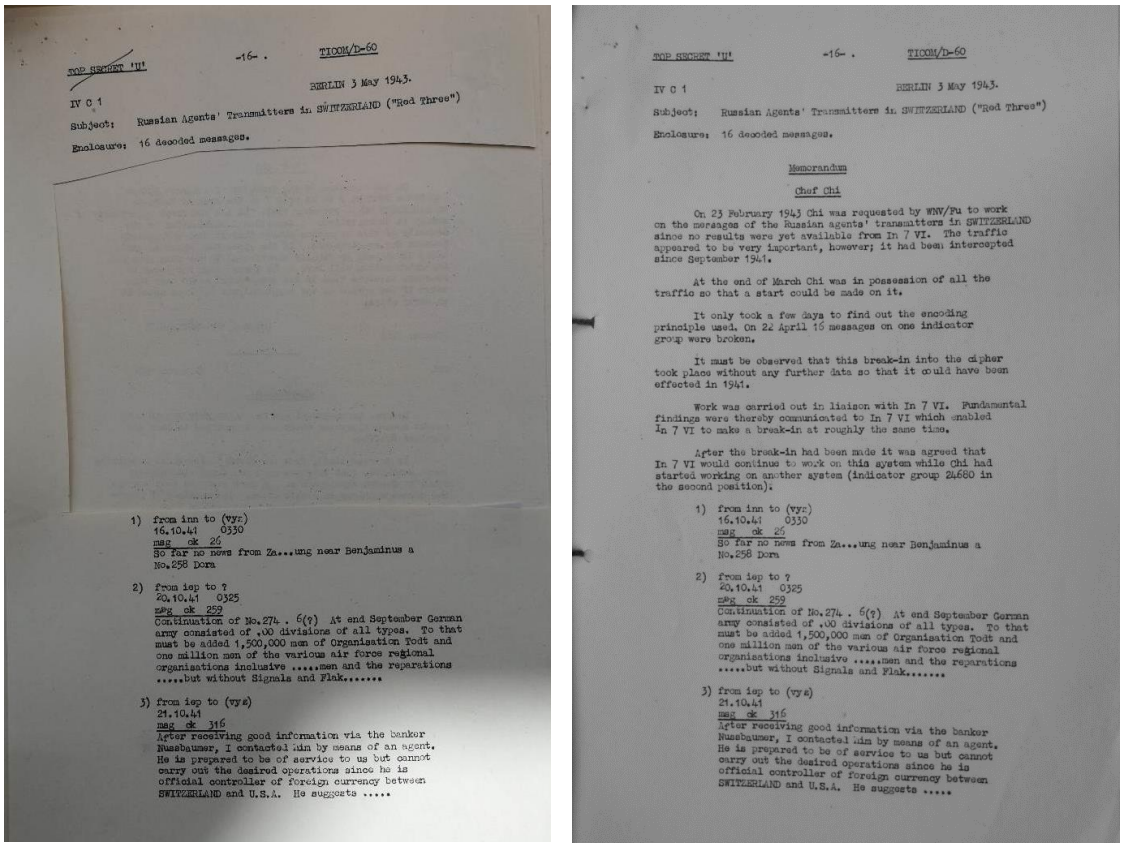
State-imposed secrecy concerning the cryptologist's art is probably as old as the art itself. For the last hundred years it has become increasingly difficult for state authorities to deny or obscure the existence of official cryptanalysis. Public demand can encourage disclosure of historical documents, but disclosure is rarely comprehensive. In different countries, there are different policy objectives and different standards. Some documents are withheld, others redacted. The UK's Public Records Act 1958 requires that public records be transferred to the National Archives within 20 years of their creation, unless they 'are required for administrative purposes or ought to be retained for any other special reason'.[1] 'Retained' is an expression broad enough to include redaction. In the United States, redaction may be justified under section 3605 of the National Security Agency Act of 1959 (50 USC 3605), which states: '… nothing in this chapter or any other law … shall be construed to require the disclosure of the organization or any function of the National Security Agency … or of the names, titles, salaries, or number of the persons employed by such agency.'

Redaction is, evidently, integral to the process of declassification of historical records. Declassification has previously been covered extensively in the literature (summaries can be found in Bennett, 2002, and on the NSA's 'Declassification and Transparency Initiatives' webpage[2]). However, this paper is not about declassification per se: its aim is to consider redactions in the field of cryptology, and to highlight certain curious relations between the two subjects.

2 Redaction of Cryptological Papers

To understand the theory and practice of redaction as applied to cryptology, one may consider a few examples, chosen from among the many instances which researchers encounter. The first is a file seized at the end of World War 2 by the Allied TICOM squads sent to Germany to obtain materials and information relating to German cryptanalytic capabilities (Rezabek, 2016). This was numbered T-1650 by the TICOM registry and, many years later, returned to Germany as part of a collection now in the

[1] Section 3(4).
[2] https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/ (accessed 3 April 2024), which has links not only to declassified material but also to policy memoranda.



TOP SECRET 'U' -16- TICOM/D-60

IV C 1 BERLIN 3 May 1943.

Subject: Russian Agents' Transmitters in SWITZERLAND ("Red Three")

Enclosure: 16 decoded messages.

1) from inn to (vyz)
16.10.41 0330
msg ck 26
So far no news from Za...ung near Benjaminus a
No.258 Dora

2) from isp to ?
20.10.41 0325
msg ck 259
Continuation of No.274 . 6(?) At end September German army consisted of ,00 divisions of all types. To that must be added 1,500,000 men of Organisation Todt and one million men of the various air force regional organisations inclusive .....men and the reparations .....but without Signals and Flak.....

3) from isp to (vyz)
21.10.41
msg ck 316
After receiving good information via the banker Nussbaumer, I contacted him by means of an agent. He is prepared to be of service to us but cannot carry out the desired operations since he is official controller of foreign currency between SWITZERLAND and U.S.A. He suggests .....

TOP SECRET 'U' -16- TICOM/D-60

IV C 1 BERLIN 3 May 1943.

Subject: Russian Agents' Transmitters in SWITZERLAND ("Red Three")

Enclosure: 16 decoded messages.

Memorandum

Chef Chi

On 23 February 1943 Chi was requested by WNV/Fu to work on the messages of the Russian agents' transmitters in SWITZERLAND since no results were yet available from In 7 VI. The traffic appeared to be very important, however; it had been intercepted since September 1941.

At the end of March Chi was in possession of all the traffic so that a start could be made on it.

It only took a few days to find out the encoding principle used. On 22 April 16 messages on one indicator group were broken.

It must be observed that this break-in into the cipher took place without any further data so that it could have been effected in 1941.

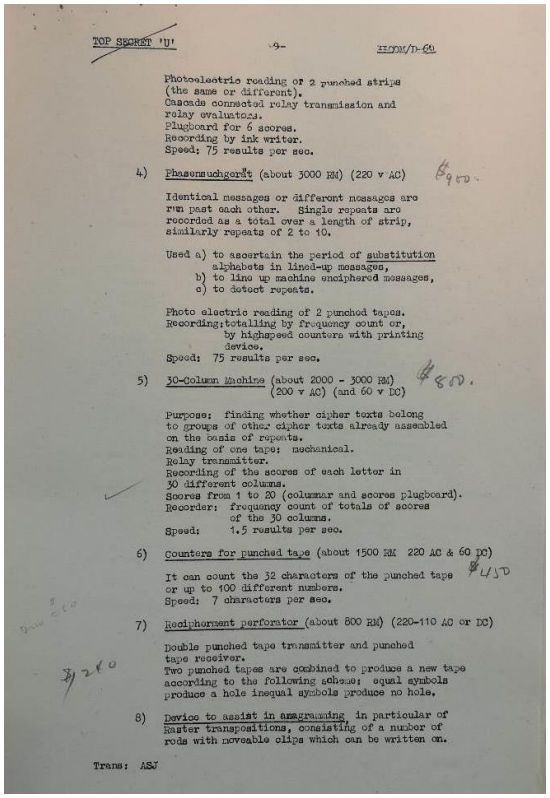
Work was carried out in liaison with In 7 VI. Fundamental findings were thereby communicated to In 7 VI which enabled In 7 VI to make a break-in at roughly the same time.

After the break-in had been made it was agreed that In 7 VI would continue to work on this system while Chi had started working on another system (indicator group 24680 in the second position).

1) from inn to (vyz)
16.10.41 0330
msg ck 26
So far no news from Za...ung near Benjaminus a
No.258 Dora

2) from isp to ?
20.10.41 0325
msg ck 259
Continuation of No.274 . 6(?) At end September German army consisted of ,00 divisions of all types. To that must be added 1,500,000 men of Organisation Todt and one million men of the various air force regional organisations inclusive .....men and the reparations .....but without Signals and Flak.....

3) from isp to (vyz)
21.10.41
msg ck 316
After receiving good information via the banker Nussbaumer, I contacted him by means of an agent. He is prepared to be of service to us but cannot carry out the desired operations since he is official controller of foreign currency between SWITZERLAND and U.S.A. He suggests .....



TOP SECRET 'U' -9- TICOM/D-60

Photoelectric reading of 2 punched strips (the same or different).
Cascade connected relay transmission and relay evaluators.
Plugboard for 6 scores.
Recording by ink writer.
Speed: 75 results per sec.

4) Phasenzuchgerät (about 3000 RM) (220 v AC)

Identical messages or different messages are run past each other. Single repeats are recorded as a total over a length of strip, similarly repeats of 2 to 10.

Used a) to ascertain the period of substitution alphabets in lined-up messages,
b) to line up machine enciphered messages,
c) to detect repeats.

Photo electric reading of 2 punched tapes.
Recording: totalling by frequency count or, by highspeed counters with printing device.
Speed: 75 results per sec.

5) 30-Column Machine (about 2000 - 3000 RM) (200 v AC) (and 60 v DC)

Purpose: finding whether cipher texts belong to groups of other cipher texts already assembled on the basis of repeats.
Reading of one tape: mechanical.
Relay transmitter.
Recording of the scores of each letter in 30 different columns.
Scores from 1 to 20 (columnar and scores plugboard).
Recorder: frequency count of totals of scores of the 30 columns.
Speed: 1.5 results per sec.

6) Counters for punched tape (about 1500 RM 220 AC & 60 DC)

It can count the 32 characters of the punched tape or up to 100 different numbers.
Speed: 7 characters per sec.

7) Reciphorment perforator (about 800 RM) (220-110 AC or DC)

Double punched tape transmitter and punched tape receiver.
Two punched tapes are combined to produce a new tape according to the following scheme: equal symbols produce a hole unequal symbols produce no hole.

8) Device to assist in anagramming in particular of Raster transpositions, consisting of a number of rods with moveable clips which can be written on.

Trans: ASJ

Exhibit 1. TICOM document D-60. Above left: page 16, redacted in the US copy. Above right: page 16 in the UK copy. Below: page 9, withheld from the UK copy. US declassification authority NW48901.

Political Archive in Berlin.[3] TICOM translated the file's contents into English and circulated the translation as document D-60 among the American and British signals intelligence services. Copies of D-60 are available at the US National Archives Records Administration and the UK National Archives.[4] In the British copy, pages 8 and 9 have been excised completely, retained under the Public Records Act. These pages are, however, open to view in the American copy, but page 16 is heavily cut from the American version notwithstanding that the page is completely open to view in the British copy (see Exhibit 1). The differences are, perhaps, surprising, given the oft-celebrated cooperation between the US and UK signals intelligence services (Smith, 2022).

Such inconsistencies allow us to consider the content of the excised passages. The pages cut from the British copy of D-60 in 2004 concern eight types of machinery invented by German

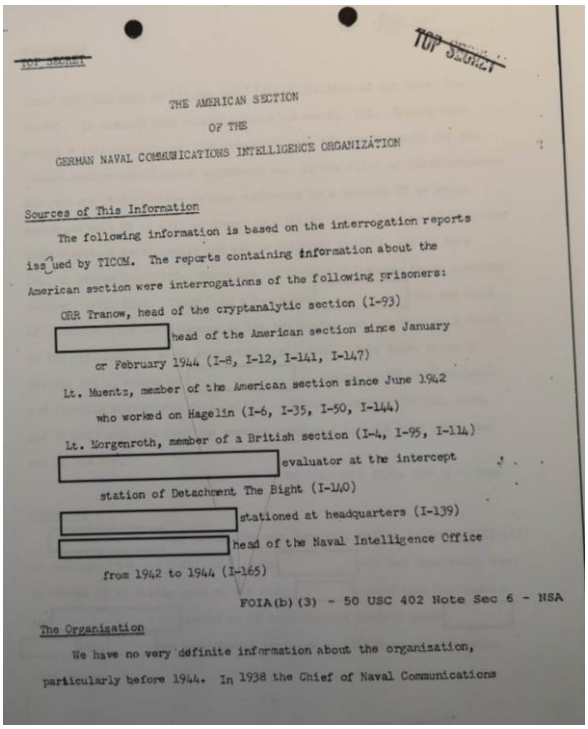
[3] Auswärtiges Amt, Berlin, Collection S8.

[4] NARA RG 457 Entry P4 Box 8; UK HW 40/174.

codebreakers to simplify attacks on superenciphered codes. Little technical detail is included in these pages. The heavily cut page 16 of D-60, cut out when the document was declassified in 2009, concerned the breaking of messages of a group of agents in Switzerland feeding intelligence on Germany to the Soviet Union (but not the decoded messages themselves). Why these subjects appeared to be sensitive to the different authorities, well after the discontinuance of code systems vulnerable to the machine methods outlined in D-60 and public knowledge of the German success against the agents' messages (Flicke, 1957) is hard to comprehend.

The next example relates to lesser redactions, where only individual words or phrases are covered up. One comes from another TICOM-related paper where people's names have been concealed (see Exhibit 2). Keeping people's names confidential might indicate a good rationale for redaction. But enough information remains to allow the researcher to fill in the blank spaces: the source documents (I-8, I-12, etc) are cited in the document, and these are publicly available, enabling the missing names to be reconstructed (here Schulze, Biege, Holtermann, and von Baumbach). It is unclear why these individuals' names were to be obscured, when that of Wilhelm Tranow, the German Navy's premier cryptanalyst who personally broke many Allied naval codes in World War 2 to devastating effect, was not. Perhaps the answer is that Tranow's achievements had been in the public domain for over thirty years by 2011 when this document was declassified (Kahn, 1978).

Similar examples can be found in the papers of the celebrated American cryptologist, William F. Friedman, which were declassified by the NSA in November 2014 and are available to view on its website in redacted form. Here, uniform length of each letter or number in the redacted telexed original facilitates a letter-count as a clue to the missing element. The potential solution can be checked by referring to other declassified documents, which freely give the names of the relevant personnel. Furthermore, so far from concealing information, the redaction has actually supplemented it. The redaction note references 50 USC 3605, implying that the persons whose names were concealed were linked to the NSA (see Exhibit 3).



TOP SECRET

THE AMERICAN SECTION
OF THE
GERMAN NAVAL COMMUNICATIONS INTELLIGENCE ORGANIZATION

Sources of This Information

The following information is based on the interrogation reports issued by TICOM. The reports containing information about the American section were interrogations of the following prisoners:

ORR Tranow, head of the cryptanalytic section (I-93)

[redacted] head of the American section since January or February 1944 (I-8, I-12, I-141, I-147)

Lt. Muentz, member of the American section since June 1942 who worked on Hagelin (I-6, I-35, I-50, I-144)

Lt. Morgenroth, member of a British section (I-4, I-95, I-114)

[redacted] evaluator at the intercept station of Detachment The Bight (I-140)

[redacted] stationed at headquarters (I-139)

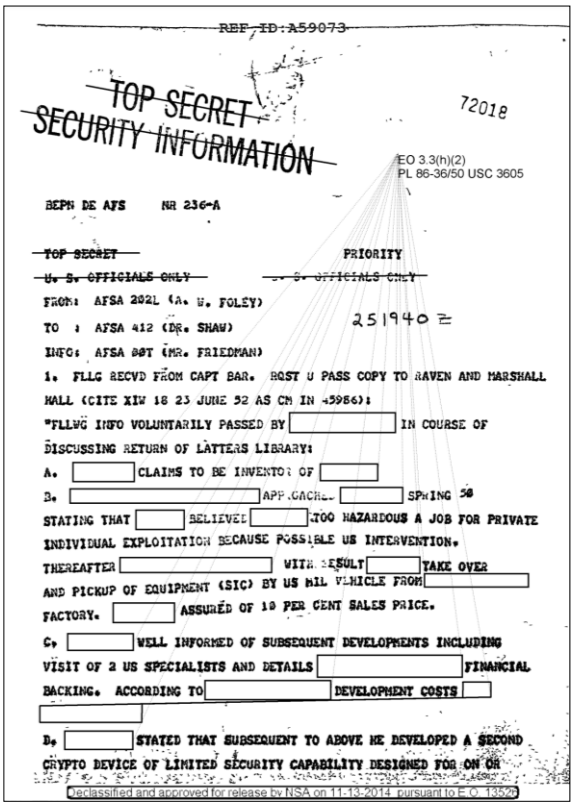
[redacted] head of the Naval Intelligence Office from 1942 to 1944 (I-165)

FOIA(b)(3) - 50 USC 402 Note Sec 6 - NSA

The Organization

We have no very definite information about the organization, particularly before 1944. In 1938 the Chief of Naval Communications

Exhibit 2. Page from NARA RG 38 Entry A1-1030 Box 74 Folder 3640/10. US declassification authority 003003.



REF ID:A59073

~~TOP SECRET~~
~~SECURITY INFORMATION~~

72018

EO 3.3(h)(2)
PL 86-36/50 USC 3605

BEPN DE AFS NR 236-A

~~TOP SECRET~~ PRIORITY
~~U. S. OFFICIALS ONLY~~ ~~U. S. OFFICIALS ONLY~~

FROM: AFSA 282L (A. W. FOLEY)
TO : AFSA 412 (DR. SHAW) 251940Z
INFO: AFSA 88T (MR. FRIEDMAN)

1. FLLG RECVD FROM CAPT BAR. RQST U PASS COPY TO RAVEN AND MARSHALL HALL (CITE XIW 18 23 JUNE 52 AS CM IN 45986):

"FLLWG INFO VOLUNTARILY PASSED BY [redacted] IN COURSE OF DISCUSSING RETURN OF LATTERS LIBRARY:

A. [redacted] CLAIMS TO BE INVENTOR OF [redacted]

B. [redacted] APP CACHE [redacted] SPRING 50 STATING THAT [redacted] BELIEVED [redacted] TOO HAZARDOUS A JOB FOR PRIVATE INDIVIDUAL EXPLOITATION BECAUSE POSSIBLE US INTERVENTION. THEREAFTER [redacted] WITH RESULT [redacted] TAKE OVER AND PICKUP OF EQUIPMENT (SIC) BY US MIL VEHICLE FROM [redacted] FACTORY. [redacted] ASSURED OF 10 PER CENT SALES PRICE.

C. [redacted] WELL INFORMED OF SUBSEQUENT DEVELOPMENTS INCLUDING VISIT OF 2 US SPECIALISTS AND DETAILS [redacted] FINANCIAL BACKING. ACCORDING TO [redacted] DEVELOPMENT COSTS [redacted]

D. [redacted] STATED THAT SUBSEQUENT TO ABOVE HE DEVELOPED A SECOND CRYPTO DEVICE OF LIMITED SECURITY CAPABILITY DESIGNED FOR ON OR

Declassified and approved for release by NSA on 11-13-2014 pursuant to E.O. 13526

Exhibit 3. NSA Friedman collection, Folder 395, doc A59073. Papers enabling reconstruction are in NARA RG 457 Entry P4 Box 20 ("Professor Vierling's library"), previously declassified in March 2012. Note the redaction authority cited top right (50 USC 3605).

3 Discussion and Conclusions

What can we learn from these rather unsatisfactory redactions? First, it seems that redaction is a weak way to protect secrets. Redaction techniques are, in general, susceptible to textual analysis or even to simple copy-paste removal of superimposed blanking (Bland et al., 2023; Ingram, 2019). Redactions applied to historical cryptological papers are vulnerable to techniques which would be recognised by codebreakers of the period from which they originate: contextual analysis allowing linguistic interpolation; parallel availability of the same text in a different communication; word length analysis; and fingerprinting. The fact that these documents are likely to be of interest to students of cryptanalysis – the very techniques which the authorities wish to obscure – adds a spice of irony to the redaction exercise.

One may then ask why the redactions were made in the first place. In a democracy, there is a tug-of-war between the security imperative of protecting the state and the expectation of openness and accountability of state agencies. One category of legitimate non-disclosure arises from the need to protect vulnerable persons from reprisals or breach of privacy, a particular concern where the individuals concerned are or were agency members. Another is where the papers reveal a cryptanalytical technique, or a pathway towards a technique, which could expose current national secrets.

But other, more dubious rationales may be at play: protection of official or national reputation, predilection for secrecy ('if in doubt, leave it out'), the power of mystique, and so forth. It is odd that many mid-twentieth century papers on codebreaking remain classified: surely security-related reasons for concealment have now lapsed. It is, unfortunately for historians, possible that they may remain under wraps indefinitely, since political priorities and budgets do not lend themselves readily to reviews of previous classification decisions.

Acknowledgments

The author would like to thank the anonymous reviewers for helpful feedback. Thanks are also due to the staff of NARA for friendly advice during the conduct of research, and to the President of Kellogg College for a Visiting Fellowship.

References

Gill Bennett. 2002. Declassification and Release Policies of the UK's Intelligence Agencies. *Intelligence and National Security*, 17(1): 21-32.

Maxwell Bland, Anushya Iver and Kirill Levchenko. 2023. Story Beyond the Eye: Glyph Positions Break PDF Text Redaction. *Proceedings on Privacy Enhancing Technologies*, 2023(3): 43-61.

Wilhelm Flicke. 1957. *Agenten Funken nach Moskau*. Verlag Welsermühl, Wels, Austria.

Mathew Ingram. 2019. Thank you to everyone who can't redact documents properly. *Columbia Journalism Review*, 10 January 2019.

David Kahn. 1978. *Hitler's Spies*. Macmillan, New York, USA.

Randy Rezabek. 2016. *TICOM: the Hunt for Hitler's Codebreakers.* Rochester, NY, USA.

Michael Smith. 2022. *The Real Special Relationship*. Simon & Schuster, London, UK. p 401.