A new perspective on Dutch WWI codebreaking with its international ramifications

Bart Jacobs
iHub, Radboud University
Nijmegen – The Netherlands
bart.jacobs@ru.nl

Florentijn van Kampen
iHub, Radboud University
Nijmegen – The Netherlands
florentijn.vankampen@ru.nl

Abstract

During the First World War, the Netherlands maintained a stance of carefully guarded neutrality. International telecommunications in the form of telephone and telegraph were closely monitored and censored by so-called censorbureaus. In 2019 new files were declassified and released to the Dutch National Archive about these censorship bureaus at Amsterdam and Rotterdam, covering 1914 to 1918. They provide detailed insight in the day-to-day business, the codebreaking efforts and specific cryptanalytic results.

The material provides a completely new perspective on the genesis of modern Dutch codebreaking. This article gives a first survey of the development of these interception bureaus. It analyses their pioneering codebreaking activities and presents historic material on German diplomatic ciphers. Also, it provides new insight into the mysterious sale in 1919 of German codebooks from the Netherlands to the United States, as reported earlier in the literature.

1 Introduction

More than a century later, the First World War (WWI), also known as the Great War or la Grande Guerre, continues to fascinate from a cryptological perspective. It marked the systematisation and institutionalisation of cryptological activities in the belligerent countries — necessitated by the wide-scale adoption of wireless communication. It also involved a unique cryptanalytical achievement — the uncovering of the Zimmermann telegram — with geopolitical effects: it brought the United States to the battlefields in Europe, changing the balance of power. The recent overview book (Smoot, 2023) on American cryptology during WWI demonstrates this continued interest.

This article fits in the same line, yet from a Dutch perspective. It is based on an old dossier[1] that was made public recently. In this paper we refer to it as the 'GSIV dossier', where GSIV is the fourth section of the General staff. The dossier has been released in 2019 by the Dutch General Intelligence and Security Service (AIVD), to the Dutch National Archive. It covers reports by heads of the two military censorship bureaus, stationed at the central telegraph offices in Amsterdam and Rotterdam. Their task was to monitor telegraph and telephone communications. It also contains detailed cryptanalytic reports on German and American codes. Little was known about such activities in the Netherlands during WWI because the Dutch intelligence organisations destroyed their own archives in May 1940, as Nazi-Germany invaded the Netherlands. This remarkable dossier, that apparently survived and showed up recently, sheds new light on Dutch cryptological activities from those early years. It has the workfloor perspective of the military censors, how they started themselves to try and decrypt coded diplomatic messages that went through their hands, and how succesful they were in doing so. They systematically broke German encrypted communication and they succeeded in breaking some British, French and American codes as well. Moreover, the dossier contains a few orginal coded German telegrams, including their decryption, see for example Figures 4 and 5 below.

This article consists of four parts: Section 2 starts with a general description of the activities at the censorship bureaus of Amsterdam and Rotterdam, as described in the GSIV dossier. Subsequently, Section 3 will go into more detail on the

[1] Available via the Dutch National Archive: nationaalarchief.nl/onderzoeken/archief/2.13.70, Generale Staf, §8.A.1, GS IV.

cryptanalytic efforts together with historic examples. The main focus will be on German diplomatic communication. Further details, in particular about cryptanalysis of British and American codes will appear in follow-up publications. Section 4 presents some of the more anecdotal material in the GSIV file to provide some *couleur locale* to the codebreaking efforts. At the end, Section 5 will present new clues in the case of the mysterious procurement of German codebooks by the Americans in 1919 as described in book 'the American Black Chamber' (Yardley, 1931) and in Mendelsohn's study on German Diplomatic Ciphers (Mendelsohn, 1937).

As a general reminder to the reader, during WWI the Netherlands remained neutral. The Dutch army had been mobilised, but stayed out of the conflict. Maintaining this neutrality was a challenge. The two opposing sides in the war were keenly watching the Netherlands and could interprete any action as choosing sides and as a *casus belli* (Abbenhuis, 2006; Tuyll van Serooskerken, 2001). At the same time, the neutral territory attracted many spies, from all sides (Klinkert, 2013). In this situation the Dutch government acted cautiously and needed what is now called 'situational awareness'. Being able to decrypt secret diplomatic communications was definitely helpful.

2 WWI censorship at Amsterdam and Rotterdam: general findings

This section gives an overview of the military censorship activities at the central telegraph offices at Amsterdam and Rotterdam, as described in the GSIV dossier. After a general introduction, some specific findings are high-lighted in separate subsections.

The fourth section, GSIV, of the General Staff (GS) of the Dutch military organisation had a broad task, notably censorship, but also prevention and combatting smuggling. Intelligence gathering was done by GSIII. Immediately after the war broke out, on July 28 in 1914, two censorship teams of military officers from GSIV were formed and dispatched to the central telegraph offices of Amsterdam and Rotterdam. The newly formed teams started working on August 1, in close coordination with the local staff — which was under orders to cooperate and keep it all secret. The offices at Amsterdam and Rotterdam functioned as national hubs, through which 'suspicious' telegrams were routed from local offices.

The recently released GSIV dossier contains detailed reports[2] of (successive) heads of these military censorship bureaus, covering especially the first two years of the war. These reports were written for the General Staff and look like personal retrospects of the bureau chiefs. They are full of personal observations and remarks, and describe in a rather informal and casual manner what worked well and also what went wrong. They are a pleasure to read. The rapporteurs were Captain P. Schaafsma (at Amsteram) and Captain P.J.A. van Mourik, Lt. Colonel A.W.A. Michielsen and Captain G.W. Nyweide (at Rotterdam). The reports from Rotterdam are the most extensive and informative, covering about two hundred pages; they form the main basis for what follows. Initially, both censorship bureaus consisted of two (military) persons, but they grew during the war to 10 or 11 persons. They worked closely together with several more telegraph staff members.

2.1 Rules and regulations

The telegraph and telephone censorship operated under a special legal framework that was not available or announced to the public. This framework for the military was established by a secret Royal Decree (*Koninklijk Besluit*), dated July 31, 1914, which formulated a wide-ranging goal: to prevent any communication that forms a threat to national security. Telegrams could be withheld, changed, or partially deleted. Encrypted telegrams were not allowed: the contents should be formulated in an understandable language (in Dutch, or English, German, French) when submitted to a telegraph office. There was one diplomatic exception: consuls and chargé d'affaires of other countries were allowed to communicate in encrypted form. Such encrypted telegrams were copied, by the Dutch censors, for later analysis. Also, encrypted communication, in the form of cipher blocks, was red aloud by phone, for instance by the German consul stationed in Rotterdam, Martin Renner, talking to the German intelligence station (*Nachrichten Sammelstelle*) at Wesel (that covered the Netherlands). Such exchanges were also copied. Communications (via telegrams or phone) with relevance for national security were passed on to the General Staff in the Hague.

[2] Labeled with numbers 1937, 1938, 1939 within the 2.13.70 archive of footnote 1.

A part of the reports written by the censorship chiefs involved suggestions for improvement to the Royal Decree, based on experiences so far. In cases where the provisions of the Decree were unclear or incomplete, clarifying instructions were asked to the head of GSIV at the General Staff in The Hague, *e.g.* about whether or not to tap international phone calls only, or national calls as well (answer: yes). From today's perspective we notice that there is a legal framework in place, but no independent oversight. The surveillance was not universal but selective, driven by target information and by resource constraints. For instance, in mid 1916 the censorship bureau at Rotterdam had listed 55 individuals for phone taps, including the consuls of Germany, Britain, France and Belgium. Of course, in those days, phone calls were not so common, especially international calls. The report shows that the Rotterdam switch handled at the time almost 10.000 phone calls per day.

2.2 Origin of GSIV dossier

At the end of this general introduction we briefly discuss the surprising recent emergence of the WWI dossier on GSIV that forms the basis of this article. As mentioned, the Dutch intelligence dossiers were destroyed in May 1940, in order to prevent that they would fall in German hands. Why and how did this dossier on censorship and cryptanalysis by GSIV escape destruction? Frankly, we have no idea. What we can recover from the records in the Dutch National Archive is that after WWII the dossier existed, first at CCB (*Code Coördinatie Bureau*, 1944 – 1960) and at its successor NBV (*Nationaal Bureau Verbindingsbeveiliging*, 1960 – 2001); the latter organisation eventually merged into the AIVD, which transferred the dossier to the National Archive in 2019. This CCB and NBV had the role of national communication security organisations, see *e.g.* (Wiebes, 2001) for more information. As an aside, the CCB was first run by Colonel Jacobus Verkuijl, who worked on Japanese codes in the Dutch Indies in the 1930s and who was invited by the Americans to stay a year at Arlington Hall during WWII. There he worked (too) closely with J.S. Peterson, see (Wiebes, 2008), and learned that the Netherlands had to protect its communication better.

3 Cryptologic work in Amsterdam and Rotterdam

At the central telegraph offices in Amsterdam and Rotterdam, military censors were instructed to block all encrypted communication, with the exception of diplomatic ones. Copies of all ciphertexts had to be sent to the General Staff in The Hague. Soon, two months after the start of the censorship activities on August 1, 1914, the General Staff reported back that they should stop sending the ciphertexts because no-one was doing anything with them in The Hague. They were just piling up.

Interestingly, the military censors of GSIV at Amsterdam and Rotterdam then got interested and decided to give it a try themselves to break the encryptions. These officers were well-educated in general but not in cryptanalysis. Their reports clearly show an analytical mindset and are written in an almost academic style. The first reconstruction — of 2300 words, a substantial part — of a German code book (called 'code I' in the reports) happened in April 1915. What helped was that the code book was alphabetic in nature and that the Germans occasionally made mistakes in using it, and sometimes even duplicated messages (or phrases) in plaintext or in other codes. Also, the German consul in Rotterdam standardly reported about ships going in and out of the Rotterdam harbour. Thus, the contents of the encoded messages were often predictable[3].

The official top-down Dutch policy in 1914 was aimed at censorship (blocking 'dangerous' communication) not at uncovering secret, encrypted information. Once decryption succeeded, locally at Amsterdam and Rotterdam, and decrypted secret messages were sent to the General Staff, their value was recognised at the highest levels.

3.1 Cryptanalytic pioneering

The censorship officers at Amsterdam and Rotterdam were not prepared in any way for the cryptanalytical work that they chose to perform. They were autodidacts, who learned by doing, but also by studying. They did collect all the literature that they could find at the Department of War in The Hague. This included the following texts.

- A. Colon, *Étude sur la Cryptographie*, a Belgian text that appeared in *Revue de L'Armee*

[3] The censorship officers soon found out that the Germans used a mono-alphabetic substitution cipher for the names of ships, inside their code-book messages.

Belge and was apparently also known to the American WWI cryptographer Parker Hitt, see (Hatch, 2014).

- Eduard A. Fleissner von Wostzowitz, *Handbuch der Kryptographie*, Wien, 1881;[4]
- M. Muirhead, *Military Cryptography*, an article from 1912;[5]
- Rudolf Schmid Von Schwarzenhorn, *Universal geheimschrift*, and also *Neues Geheimschrift-verfahren*, two undated (and unfamiliar) manuscripts.

The Dutch censorship officers were cryptological autodidacts at a personal level. But one could say, the Netherlands, as a small neutral country without strategic partners, was also autodidactical as a nation. In contrast, Smoot (2023, p.2) writes:

> But the United States could not have developed its system so rapidly had it not been for the significant contribution of the United Kingdom (the Admirality's Room 40, the War Office's MI1(b), and the British Expeditionary Forces I(e) wireless and cryptologic staff), as well as France (the Deuxième Bureau's Bureau de Chiffre and subordinate army cryptologic units).

In Section 5 we shall see that the Netherlands also contributed to the cryptological position of the US.

3.2 Two teams of cryptologists

In the limited available sources, before the release of the GSIV dossier discussed here, one does find mention of Dutch cryptanalytical WWI successes, for instance, in (Klinkert, 2013) or in personal recollections, but without details. The achievements are always attributed to one single individual, namely to Henry Koot (1883 – 1959), an officer originally from the Royal Netherlands Indies Army. Koot is mentioned for instance in (Wiebes, 2008), as "considered to be one of the best Dutch cryptologists", and in (Kruh and Deavours, 2002). The *NSA Daily – History Today*, of August 24, 2011[6] writes about Koot :

> The Netherlands had its counterpart to Herbert Yardley … in Henri Koot, the "godfather" of Dutch military cryptology … one of the greats in cryptology, albeit little known outside of his homeland.

The censorship reports from Rotterdam and Amsterdam give a new, more nuanced picture. There were multiple people doing cryptanalysis, in a real team effort. They each had their own breakthroughs, with different codes. Successes are for example due to Rotterdam officers Bennewitz, Berenschot, Boomsma, Lettinga and Vis and to Amsterdam officer Van Tricht. It is interesting to note that also the acting station chiefs contribute to the succes as with Van Mourik and Nyweide. Koot was the most proficient in breaking codes, but definitely not the only one. Because of his skills, he was allowed to spend all his time on cryptanalysis and was freed from bureaucratic duties. Describing him as the sole Dutch WWI cryptologist is a misrepresentation.

3.3 Breaking German Diplomatic Codes

The GSIV dossier contains several sources with information about German diplomatic codes, their properties and the efforts of breaking them. First, there are the Rotterdam reports that describe successes but also *how* these were achieved, what mistakes were made and how information was gathered. In addition to the reports, there is also a separate file with descriptive and cryptanalytic articles about several German Diplomatic ciphers. These articles, or 'notes' as the Dutch called them, were used to summarise and archive the analysis of a certain code. These reports were exchanged between Amsterdam and Rotterdam to benefit from each others results and insights. Unfortunately, some of these notes are missing, for unclear reasons: there are some references in the Rotterdam reports to notes about German code systems with name, date and author that are not in the GSIV dossier.

The Rotterdam report describes in detail how the staff of the censorbureau had to bootstrap their codebreaking activities. Every aspect of the codebreaking metier had to be invented on the spot. When they broke[7] their first code in april 1915, it is simply referred to as 'code I'. After a while the Dutch codebreakers discovered more new codes with new systems and new variants, so they had to invent a scheme to order and catalogue the codes.

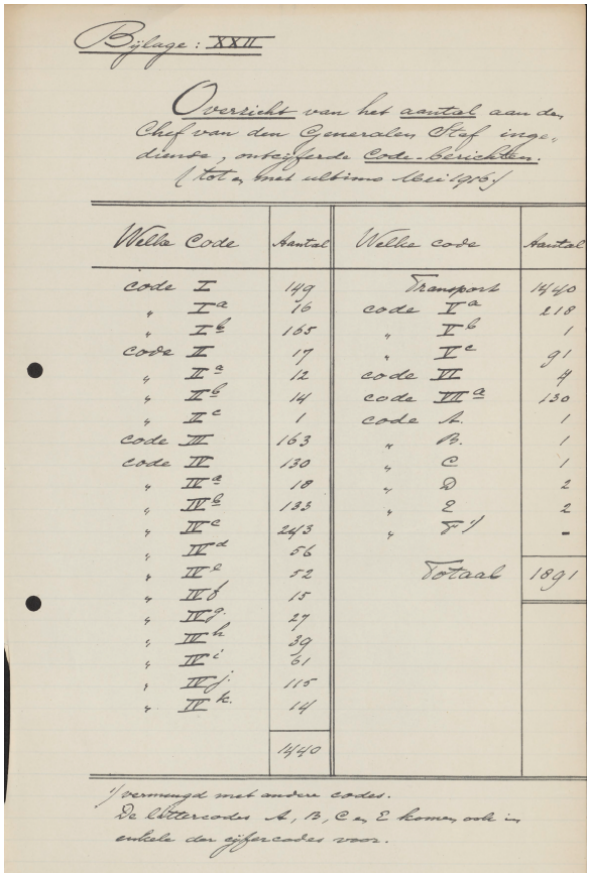
The Dutch codebreakers started to number different codes with a Roman number: code I, II, III, IV etc. After a while this system had te be

[4] See kryptografie.de/kryptografie/personen/eduard-fleissner.htm

[5] Republished as (Muirhead, 1912), see doi.org/10.1080/03071841209417859.

[6] Released in 2015, see pdf link

[7] The rapporteurs use a very peculiar but effective phrase for when a code is solved or broken; They would say that a code has "fallen"



Bijlage: XXII

Overzicht van het aantal aan de Chef van den Generalen Staf ingediende, ontcijferde Code-berichten. (tot en met ultimo Mei 1916)

Welke Code	Aantal	Welke code	Aantal
code I	149	Transport	1440
" I^a	76	code I^a	218
" I^b	165	" I^b	1
code II	17	" I^c	91
" II^a	12	code III	4
" II^b	14	code III^a	130
" II^c	1	code A.	1
code III	163	" B.	1
code IV	130	" C	1
" IV^a	18	" D	2
" IV^b	133	" E	2
" IV^c	243	" F	-
" IV^d	56		
" IV^e	52	Totaal	1891
" IV^f	15		
" IV^g	27		
" IV^h	39		
" IV^i	61		
" IV^j	115		
" IV^k	14		
	1440		

*) vermengd met andere codes.
De lettercodes A, B, C en E komen ook in enkele der cijfercodes voor.

Figure 1: From appendix XXII of the Rotterdam report by van Mourik an overview, in Dutch, of decryptions until May 1916. In the left column, in Roman numerals, the codesystem and variant. In the right column the number of decryptions.

expanded because the Germans were constantly modifying their codes with new variations, modifications and additions. This was probably done in an attempt to increase security. So code I expanded to variant Ia and Ib and code II was refined to IIa and IIb and so on. The Rotterdam report states that during the first two years of the war in total 76 German codes, including variations, were broken. That is a non-trivial achievement. The Rotterdam office kept detailed statistics on the number of decrypted messages and the kind of code used. An example can be seen in Figure 1 where one finds in the last column the number of decrypted messages in a particular code sent to the head of the General staff from the start of the bureau until May 1916 — totalling 1891.

One of the code families was of special value. Van Mourik writes in his report: (translation by the authors): "Code III (...) is a very important (code) because it is the consular code, that means the code that is used to discuss the important political matters". Code III, and some of its successors, are the family of German diplomatic codes.

Below we present some distinctive properties to describe and catalogue German diplomatic codes and are also used internationally. This will make it easier to describe results and put things in a larger context. Every German (diplomatic) code has a certain designating number. This is a number that (almost) always appears at the beginning of the message and it ifunctions as an indicator which codebook or system is used. This is of course necessary for the recipient to be able to decode the message. So one might talk about the 2500 code or the 29000 code. These designating numbers will be used in the rest of this article.

German Diplomatic codes were based at the time on large codebooks. These books contain thousands of words, names and places with a corresponding number. The combination of this number, the page in the book and sometimes some other ingredients, would lead to a translation from a word to a number and vice versa. The Germans would make variations of a codebook by reordering the pages, renumbering the words or a modification in how to construct the final number. These encoding variations would get a new designating number so that the communicating parties would know exactly what to use. More about such variations can be found in (Lasry et al., 2020).

In the reports from Rotterdam, but also in international sources, these variants are ordered in some form of hierarchy. One code would be considered the main code and other codes are seen as descendants. Depending on the reconstructed codebooks available, it is not always certain which codebook should be considered the main one and which one a variation. It will depend on the kind of messages that are intercepted and which codebook is solved first. These different family trees of German diplomatic codes will turn out to be of value in the last section of this article. Figure 2 from (Mendelsohn, 1937) shows a graphic representation of such a hierarchy and also shows designated numbers of German diplomatic codes.

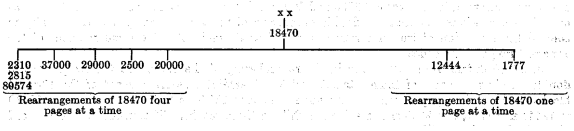


Figure 2: Cryptologic family tree of code 18470.

3.4 Examples of historic codebreaking

What makes the reports from Rotterdam so interesting is that they offer a peek at actual cryptanalysis during WWI, hidden in a back room at the Rotterdam Telegraph office between 1914 and 1918. Sometimes, results were achieved by statistics or logical reasoning. But often breakthroughs were made because of clever combination of operational possibilities.

Section 3 already mentioned code I. The break of code I started with a house search by the police in a case of suspected German espionage. During this search, the police found a note together with a letter to the German chief of naval Intelligence Prieger. The note is included in the report from Van Mourik and is reproduced in Figure 3.

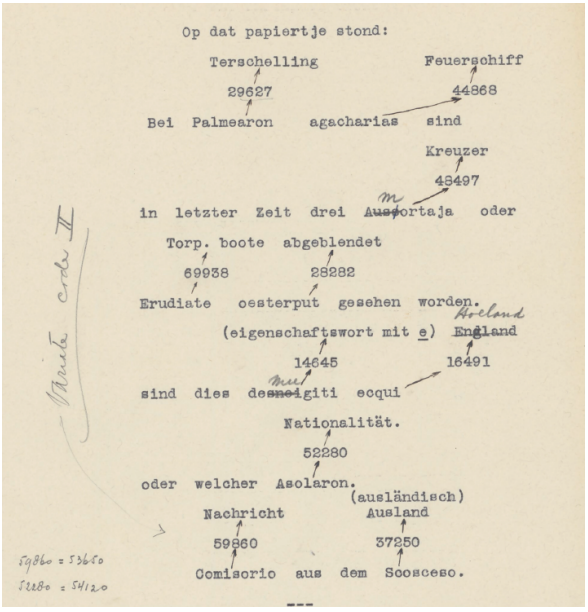


Figure 3: First clues to 'code I' in a note captured by the Dutch police from a suspected German spy.

These few codewords mark the start of the fall of code I. After a couple of days the Rotterdam bureau intercepts a phone call to the German intelligence station in Wesel, in which some words are replaced with code numbers. Van Mourik describes the process honestly: "We could still not draw any conclusions, since we had no idea how the German code was constructed". They keep combining intercepted phone calls with the word list reconstructed so far. At the same time they had to figure out how the code actually works (the fact that there is a code book, with page numbers and alphabetically ordered words). Van Mourik explains why he describes the breaking of this particular code in such great detail : "The discovery of code I is so important, because with that experience (...), we were able to find all the other codes".

The next example in Figure 4 shows an intercepted German coded telegram with added handwritten decryption. It starts with two numbers: 175 and 200. The handwritten notes above the numbers show that 175 is the number of the telegram and 200 is the *Erkennungszahl*, or designating number. As far as readable, it says:

> Dampfer aus England ist heute Vlissingen nicht parterop(?) ankommen. Feuer - schiff Nord - Hinder(?) doch nächtens nach Nord partirop(?) verlegen werden wegen substanti(?) Aus(?) English Meinen - feld bis 52 Grad Nord Breite und 2 Grad 22 Minuten Ost Länge. Genau Lage Feuer - schiff wird bei substantisch(?) Verlegen partizip bekannt. Gefahrlich is jetzt Fahrt zwischen 1 35(?) Ost und 3 18 Ost von 51 15 Nord bis 51 40 Nord Ferner zwichen 1 55 ost und 2 32 Ost von 51 40 Nord bis 52 Nord. Mueller.

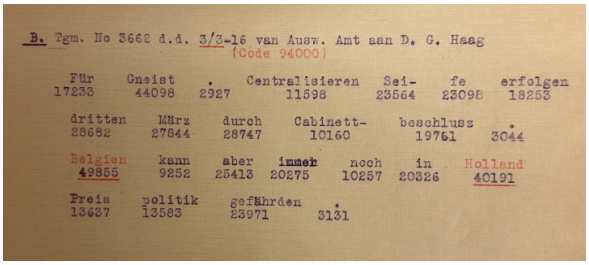


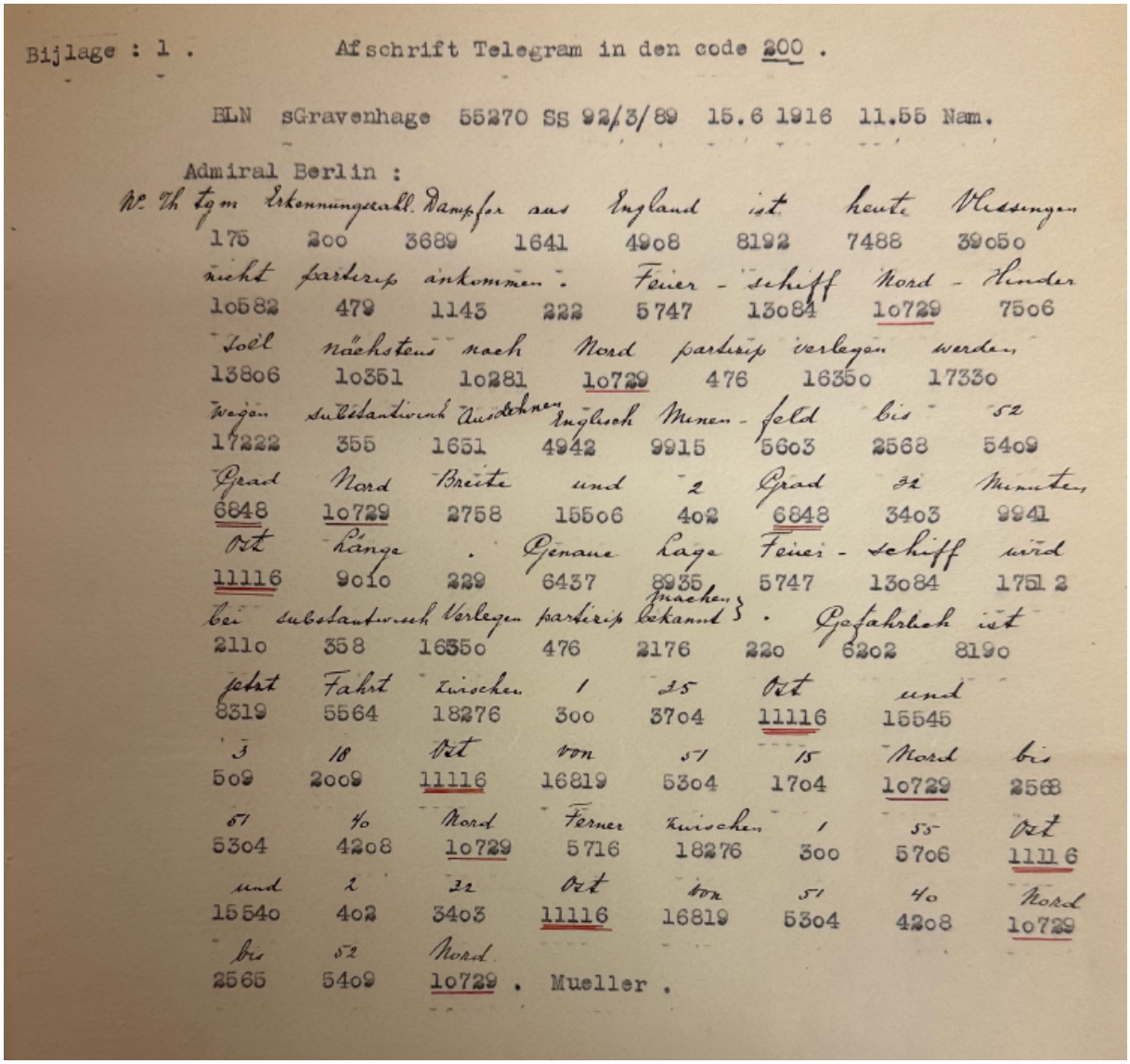
Figure 5: Decryption of a German telegram in code 94000 dated March 3rd 1916

Figure 5 shows another original German telegram, in code 94000. This code was used between the *Deutsche Gesandtschaft* in The Hague and *Auswärtig Amt Berlin* about matters of import and export. The censors in Rotterdam therefore called it the 'trade code'. As in this telegram, the designating number is sometimes omitted when both communicating parties considered it to be obvious in which code they were communicating. The message is as follows.

> Für Gneist. Centralisieren Sei- fe erfolgen dritte März durch Cabinett- beschlusz. Belgien kann aber immer noch in Holland Preis politik gefährden.

4 Anecdotal observations

As previously mentioned, the telegraph station staff, under the instruction of the censors, monitored selected phone calls. Summaries of the calls



Bijlage : 1 . Afschrift Telegram in den code 200 .

BLN sGravenhage 55270 SS 92/3/89 15.6 1916 11.55 Nam.

Admiral Berlin :

W. Th tgm Erkennungsmarkl. Dampfer aus England ist heute Vlissingen
175 200 3689 1641 4908 8192 7488 39050
nicht fahrplanmäßig ankommen. Feuer-schiff Nord-Hinder
10582 479 1145 223 5747 13084 10729 7506
soll nächstens nach Nord fahrplanmäßig verlegen werden,
13806 10351 10281 10729 476 16350 17330
wegen substantiellen Ausdehnen englischen Minen-feld bis 52
17222 355 1651 4942 9915 5603 2568 5409
Grad Nord Breite und 2 Grad 32 Minuten,
6848 10729 2758 15506 402 6848 3403 9941
Ost Länge . Genaue Lage Feuer-schiff wird
11116 9010 229 6437 8935 5747 13084 17512
bei substantiellen Verlegen fahrplanmäßig bekannt machen .
2110 358 16350 476 2176 220 6202 8190
Gefährlich ist
jetzt Fahrt zwischen 1 35 Ost und
8319 5564 18276 300 3704 11116 15545
3 18 Ost von 57 15 Nord bis
509 2009 11116 16819 5304 1704 10729 2568
57 40 Nord Ferner zwischen 1 55 Ost
5304 4208 10729 5716 18276 300 5706 11116
und 2 32 Ost von 57 40 Nord
15540 402 3403 11116 16819 5304 4208 10729
bis 52 Nord
2565 5409 10729 . Mueller .

Figure 4: Decryption in handwriting of a German telegram in code 200 dated June 15th 1916.

were recorded[8]. At the time, the telephone system worked via switchboards with cables. Connections were added so that the sensitive calls could be copied to an additional 'tap' phone in an adjacent room. The report dryly remarks that the censors soon found out that it was wise to remove the microphone from this second tap phone.

The censorship itself was meant to be secret and the military censorship officers worked in plain clothes, but pretty soon almost everyone in the telegraph offices of Amsterdam and Rotterdam knew about them. Also outside, many journalists and diplomats were soon aware of the censorship.

During the war there were few limitations for the Dutch press. Occasionally, telegrams from journalists working at the border were redacted by the censors, in order not to leak military details. Foreign journalists were monitored systematically, also because several spies worked under journalistic cover, see also (Klinkert, 2013).

Encrypted messages were also passed on in phone conversations, in which the wordcodes, like 90987, were red aloud, in sequence. This could easily go wrong. The intended German receiver could ask for a repetition when a sequence of numbers was unclear, but the Dutch copiers could not, to their frustration. Copy mistakes were a constant concern: such coded telephone calls could easily last an hour.

[8]These summaries are not included in the GSIV dossier. In general, the dossier mostly describes procedures together with a few highlights and personal reflections.

The Dutch noticed that the German military attaché Renner was very careful and, for instance, never by accident mentioned the cleartext instead of the ciphertext. They assumed that Renner had been trained in these matters. In contrast, the German consuls in Rotterdam, first Gneist and then Bosenick, made more mistakes — to the advantage of the censors. Moreover, they were contemptuous when they erred and would say things like: "never mind, those Dutch don't understand such matters anyway".

The reports about the censorship activities describe several times how enthousiastic the (self-taught) censors were about their cryptanalytical activities. For instance, van Mourik write (translated by the authors):

> ... working on these codes is extraordinarily captivating and interesting. Hours and hours in succession — usually during our spare time — have we dedicated our efforts to this; nothing was more satisfying, so we found, than having fully decrypted a message. It is noteworthy that we sometimes spent hours thinking about one word, and days about one short message.

Van Mourik thinks ahead about how to train codebreakers in the future. He proposes that the elite school for senior rank officers (*Hogere Krijgsschool*) should develop a course on cryptology. He vividly describes in his report the discussions he had with Koot about this (translation by the authors):

> At the Military Academy, mr Koot and myself learned a thing or two about cryptography, but we did not realise, that this was such an extensive and interesting study. We both have expressed multiple times, that it would be very worthwhile, if cryptography would be part of the standard curriculum of the Military Academy, for example in the first couple of years at least one hour every week. What beautiful puzzles would we provide the students of this course; Mr Koot often salivated at this idea.

Indeed, after WWI Koot teaches at the military school and educates a whole new generation of dozens of Dutch military cryptologists, including Verkuijl (Wiebes, 2001). Van Mourik shows himself to be quite the visionary when he thinks about how to institutionalise the cryptologic activities in Netherlands. Van Mourik writes (translation by the authors):

> The undersigned has - for a long time - considered the question of whether it is not desirable - we need not doubt its feasibility - to establish a 'decryption bureau' in our country during peacetime. (...) Especially for times of tension, this measure seems to me very desirable. Knowing what is going on in Europe during such times is - needless to say - extremely important. To only take this measure when there is some tension on the political horizon does not seem wise to me. At that time, the individuals who would then be charged with this task could not fully immerse themselves in it; they must solve the various codes and collect the necessary data during peacetime, so as to be able to use them at the right time.

Many countries, including the Netherlands, would forget this lesson between the two world wars. In the economic crisis of the 1930's, many government cipherbureaus were closed.

4.1 Ships, spies and smugglers

The Rotterdam report of van Mourik also elaborates on the contents of the German messages that were decrypted, especially from the military attaché Renner. They cover many newspaper articles, both from Dutch and international media, and also much shipping information especially about the Rotterdam harbour and about its continued trade with the UK. Also, many smuggle activities showed up, and were shared by the censors with Dutch authorities. There are also several spy stories, partly overlapping with (Klinkert, 2013). The latter source was written before the release of the GSIV dossier at hand, giving opportunities for further study.

5 Selling German codebooks to the USA

During WWI the United States were also breaking German codes (Smoot, 2023). Herbert Yardley founded MI8 as a so called *Black Chamber* to focus the US cryptanalytic efforts (Yardley, 1931). Charles J. Mendelsohn reveals in his report 'Studies in German Diplomatic Codes Employed During the World War' (Mendelsohn, 1937) an intriguing story about German codebooks stemming from the Netherlands. He describes that in April 1919, in the Netherlands, American officials had been offered German Codes books for sale. At Christmas 1919 the material was sent from the Netherlands to Washington for inspection and analysis to see if it was worth buying.

Mendelsohn describes the person selling these codes as "The Dutchman" He also describes the uncertainty surrounding the identity or nationality of this person. On the one hand there is (Yardley, 1931) stating that the codes were offered to the Americans in The Hague, that is the Netherlands,

but by a German spy. Mendelsohn, on the other hand, makes a case for the fact that the Dutchman was, in fact, actually truly a Dutch person. Both scenarios have their merits and drawbacks and at the end Mendelsohn is reluctant to draw a final conclusion.

The GSIV dossier about the Dutch code breaking efforts in Rotterdam and Amsterdam contains evidence, described below, that the material offered to the Americans actually came from GSIV. The evidence makes it plausible that the Dutchman from Mendelsohn's report was someone from or with access to our group of pioneering codebreakers at the telegraph offices.

5.1 The mysterious Dutchman

The first part of the puzzle is Mendelsohn's description of the Dutchman's material:

> This material contains (...) a skeleton of code known as 2500, with tables for changing this code into four encipherments called by the "Dutchman" (...) 37000, 29000, 20000 and 18400. The last turned out to be identical with 18470, although in the messages received by MI8 that designating number was never employed.

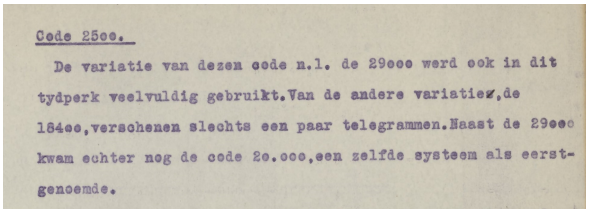
The list of codes is of course a clue, but more specifically the fact that one of the codes is referred to by the Dutchman with the designating number 18400. Apparently, MI8 never used that number, but used 18470 instead. This will be an important clue.

Mendelsohn writes in his report how the Dutchman thinks these codes relate to each other (which code is a variant of which code):

> Probably code 2500 is the original code book. From this code are derivated (sic!) the codes 18400, 29000, 37000 and 20000.

The Americans have a different codetree, see Figure 2, with 18470 as the main code with 2500, 29000, 37000 and 20000, and others, as variants. Now it is time to compare this with the material from Rotterdam to see how the three Rotterdam reports describe the various codes.

The reports from the Rotterdam bureau set out in quite some detail which codes are found, how they are broken, what name the bureau assigned to them and how the codes relate to each other.


Code 25oo.

De variatie van dezen code n.l. de 29ooo werd ook in dit tydperk veelvuldig gebruikt.Van de andere variatiew,de 184oo,verschenen slechts een paar telegrammen.Naast de 29ooo kwam echter nog de code 2o.ooo,een zelfde systeem als eerstgenoemde.

Figure 6: Section about code 2500 in the Rotterdam report by Nyweide. Translation: "Code 2500: The variation of this code, namely the 29000, was also frequently used in this time period. From the other variation, the 18400, only a few telegrams appeared. In addition to the 29000, however, there was also the code 20,000, a similar system to the aforementioned."

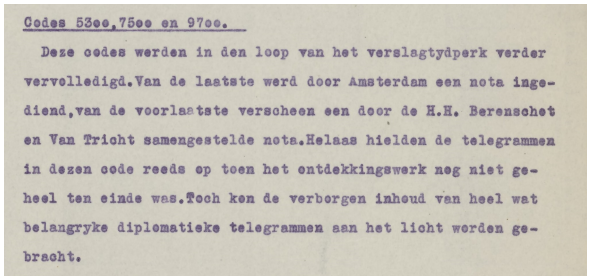
The third report from Rotterdam by Nyweide contains a separate section on code 2500. This section is shown in Figure 6. Here we clearly see that the group in Rotterdam consideres code 2500 to be the main code and the others (20000, 29000 and 18400) variants of that main code. We can also clearly see that they use the 18400 designator for what in the US and UK codebreaking literature mostly is referred to as the 18470 code.

These two elements, the code-tree with 2500 at the top and the designating number 18400 in stead of 18470, are a unique fingerprint for the Rotterdam and Amsterdam codebreakers. This makes it extremely likely that the mysterious Dutchman that Mendelsohn describes is, in fact, someone from or in the vicinity of our Dutch censor codebreakers.

5.2 How good were the Dutch Codebreakers?

As a final thought experiment, we try to position the Dutch codebreakers at an international stage. The most well known counterparts are Yardley's group MI8 in the United States, Room 40 in the United Kingdom, and the Deuxième Bureau in France. In no way do we present this as a systematic comparison of these different codebreaking group. But if we lift out one section from the last report from the Rotterdam bureau in the GSIV file, we obtain an interesting international perspective.

Nyweides report from Rotterdam mentions codes 5300, 7500 and 9300 quite casually. This short paragraph can be seen in Figure 7 .



Codes 53oo,75oo en 97oo.

Deze codes werden in den loop van het verslagtydperk verder vervolledigd.Van de laatste werd door Amsterdam een nota ingediend,van de voorlaatste verscheen een door de H.H. Berenschot en Van Tricht samengestelde nota.Helaas hielden de telegrammen in dezen code reeds op toen het ontdekkingswerk nog niet geheel ten einde was.Toch ken de verborgen inhoud van heel wat belangryke diplomatieke telegrammen aan het licht worden gebracht.

Figure 7: Description in Dutch from Nyweides report from Rotterdam about the cryptanalytic succes on German diplomatic codes 5300, 7500 and 9700. Translation: "These codes were further completed over the course of the reporting period. For the last one, a note was submitted by Amsterdam, and for the penultimate one, a note compiled by H.H. Berenschot and Van Tricht appeared. Unfortunately, the telegrams in this code already ceased when the discovery work was not yet completely finished. Nevertheless, the hidden content of quite a few important diplomatic telegrams could be brought to light."

One of the codes that immediately draws attention is 7500. It is remarkable to see that the Dutch were able to read it. This was the code that was used to encrypt the original Zimmerman telegram (Mendelsohn, 1938). Room 40 in the UK apparently was able to read this code and considered this to be a major achievement (Friedman and Mendelsohn, 1938). We dare to claim that, had the famous Zimmerman telegram been transmitted through telegraph offices in the Netherlands, the Dutch codebreakers would have decrypted it.

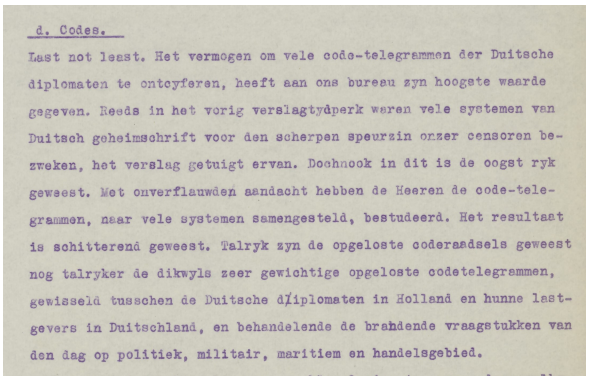
Mendelsohn remembers the Dutchman and what he had to tell about the other two codes: 9700 and 5300. MI8 also succesfully broke these codes, but considered them to be quite complex. Mendelsohn can almost not believe that the Dutch cryptologists would have been capable of breaking such complicated codes:

> In his description of codes 9700 and 5300, not belonging to the 18470 family of which he likewise furnished partial copies, the "Dutchman" has indicated certain additives, some of them running to many figures, which were used with these codes. To work out these long additives from the fractions of the codes at his disposal would have been a very rare cryptographic achievement.

For a group of self-taught enthusiasts, working in an improvised cipherbureau setup in a spare room at the local telegraph office in Amsterdam or Rotterdam, without any international collaboration, this is quite an achievement indeed.

6 Conclusions

A recently declassified GSIV dossier from the Dutch National Archives offers a novel perspective on the origins of twentieth century Dutch codebreaking, in particular during World War I. It reveals that codebreaking started as a bottom-up effort, initiated by two teams of intelligent, enthusiastic, and self-taught censor officers. This effort included the well-known cryptographer Henri Koot, but had many more contributors. The dossier demonstrates that the (isolated) cryptoanalytic achievements of the Dutch reached levels that are comparable to those of the British, French and Americans. In fact, the dossier also shows that German codebooks bought by the Americans in 1919 must have come from these Dutch teams.



d. Codes.

Last not least. Het vermogen om vele code-telegrammen der Duitsche diplomaten te ontcyferen, heeft aan ons bureau zyn hoogste waarde gegeven. Reeds in het vorig verslagtydperk waren vele systemen van Duitsch geheimschrift voor den scherpen speurzin onzer censoren bezweken, het verslag getuigt ervan. Dochnook in dit is de oogst ryk geweest. Met onverflauwden aandacht hebben de Heeren de code-telegrammen, naar vele systemen samengesteld, bestudeerd. Het resultaat is schitterend geweest. Talryk zyn de opgeloste coderaadsels geweest nog talryker de dikwyls zeer gewichtige opgeloste codetelegrammen, gewisseld tusschen de Duitsche diplomaten in Holland en hunne lastgevers in Duitschland, en behandelende de brandende vraagstukken van den dag op politiek, militair, maritiem en handelsgebied.

Figure 8: Michielsen reflects on the code breaking in Rotterdam.

6.1 "The result has been brilliant"

We end with one more (translated) quote illustrating the professional enthousiasm and pride of the Dutch codebreakers, see Figure 8.

> Last (but) not least. The ability to decipher numerous coded telegrams of German diplomats has given our office its highest value. Already in the previous reporting period, many systems of German secret writing had succumbed to the keen investigative sense of our censors, as the report testifies. But even in this period, the harvest has been ripe. With unwavering attention, the gentlemen have studied the coded telegrams, composed according to many systems. The result has been brilliant. Numerous have been the solved code puzzles, even more numerous the often very significant solved coded telegrams, exchanged between the German diplomats in Holland and their principals in Germany, addressing the burning issues of the day in political, military, maritime, and trade areas.

Acknowledgements

We thank the reviewers for their feedback, especially one of them who provided additional material which demonstrated that Code I in Subsection 3.3 is a variant of Code II and that Code II is actually the German naval code (the so called *Verkehrsbuch*). These connections will be further explored in future work.

References

Maartje Abbenhuis. 2006. *The Art of Staying Neutral. The Netherlands in the First World War, 1914–1918*. Amsterdam Univ. Press.

William F. Friedman and Charles J. Mendelsohn. 1938. *The Zimmerman Telegram of January 16, 1917 and its Cryptographic Background*. United States Government Printing Office.

David Hatch. 2014. The dawn of American communications intelligence: The Spanish-American war and after. *Cryptologic Quarterly*, 2024(1):17–29.

Wim Klinkert. 2013. A spy's paradise? German espionage in the Netherlands, 1914–1918. *Journ. Intelligence History*, 12(1):21–35.

Louis Kruh and Cipher Deavours. 2002. The commercial Enigma: Beginnings of machine cryptography. *Cryptologia*, 26(1):1–16.

George Lasry, Ingo Niebel, and Torbjörn Andersson. 2020. Deciphering German diplomatic and naval attaché messages from 1900-1915. *Cryptologia*, 45:1–43.

Charles J. Mendelsohn. 1937. *Studies in German Diplomatic Codes Employed During the World War*. United States Government Printing Office.

Charles J. Mendelsohn. 1938. *An Encipherment of the German Diplomatic Code 7500*. United States Government Printing Office.

Murray Muirhead. 1912. Military cryptography: A study of transposition cipher systems and substitution frequency tables. *Journ. of the Royal United Services Institution*, 56(418):1665–1678.

Betsy R. Smoot. 2023. *From the Ground Up: American Cryptology during World War I*. Series II, World War I, Volume 2. National Security Agency, Center for Cryptologic History.

Hans van Tuyll van Serooskerken. 2001. *The Netherlands and World War I. Espionage, Diplomacy and Survival*. History of Warfare, Volume 7. Brill Publishers, Leiden.

Cees Wiebes. 2001. Dutch sigint during the Cold War, 1945–94. *Intelligence and National Security*, 16(1):243–284.

Cees Wiebes. 2008. Operation 'Piet': The Joseph Sidney Petersen Jr. spy case, a Dutch 'mole' inside the National Security Agency. *Intelligence and National Security*, 23(4):488–535.

Herbert O. Yardley. 1931. *The American Black Chamber*. The Bobbs-Merrill Company.