Only Gentlemen Read Each Other's Mail: Over 50 Years of Sittler Codebooks in the Dutch Diplomatic Service

Jip Boer
iHub, Radboud university
Nijmegen - The Netherlands
jip.boer@ru.nl

Abstract

The Dutch diplomatic service's prolonged reliance on commercially available Sittler codebooks, despite repeated indications the books had been compromised, presents an interesting case study spanning the late nineteenth century to the early 1930s. With the use of the Sittler code as its focal point, this article explores how cryptographic practices were shaped as much by social norms, administrative capacities and financial constraints as by awareness of strategic security risks.

Drawing primarily on archival material from the Dutch Ministry of Foreign Affairs, it demonstrates that continued use of the Sittler code reflected neither ignorance nor technological backwardness. Instead, it exposes a class-based, "gentlemanly", conception of secrecy in which codes fulfilled a primary function of shielding information from subordinate staff and telegraph personnel, rather than from senior officials of foreign governments. Only under the external pressures of the First World War did concerns of foreign cryptanalytic threats lead to incremental security measures.

1 Introduction

As the famous quote by U.S. Secretary of State Henry Stimson goes, 'Gentlemen do not read each other's mail', this article will demonstrate, Dutch gentlemen of the diplomatic class thought very differently of the matter. From at least 1878 to 1931, and possibly beyond, the Dutch diplomatic service relied on various editions of the commercially available 'Sittler codebooks' for confidential communications. These French-language dictionary codebooks were authored by the water company director and later postal and telegraph director F.J. Sittler (dates unknown). Within Dutch diplomatic circles, the code was commonly known as the 'Sittler code' after its author, or simply, the 'French code'. As one might expect, over the roughly fifty years in which these codebooks were in use, the Dutch Department of Foreign Affairs in the Hague had repeatedly received warnings that its codes had been compromised.

The historical considerations and attitudes towards diplomatic communication security in neutral countries has been a little studied subject. The Netherlands is an interesting case because from a modern perspective it is difficult to understand why the Dutch diplomatic service continued to rely on compromised codebooks for such an extended period. This article examines that continued use, taking the Sittler code as a case study to explore historic attitudes toward communication security among Dutch diplomats and policymakers, as well as the considerations that ultimately led to the institutionalisation of cryptologic capabilities within the Dutch state apparatus. In this article, I will argue that the answer to the question is three-fold.

In true Dutch fashion, the first and most straightforward factor was financial in nature. Producing codebooks for the entire diplomatic service was a laborious task that required a certain expertise and thus was costly. By contrast, the commercially available Sittler codebooks were relatively inexpensive. Their use also reduced the length of messages and thus the cost to transmit them telegraphically.

The second factor was the existence of a somewhat nonchalant attitude towards secrecy within Dutch diplomatic circles, especially prior to the First World War. Diplomats during this period, mostly hailing from the nobility and gentry, generally displayed little concern about their communications being known to foreign government

officials. Possible explanations for this attitude range from the idea that the neutral Netherlands was not a significant European power and had few things to hide, to the existence of a class-based conception of secrecy that meant some Dutch diplomats were primarily concerned with shielding their communications from the prying eyes of "commoners" rather than the gentlemen in senior positions of foreign governments. Evidence of this "gentlemanly" attitude will be provided, in the form of historical correspondence.

The third factor was the gradual introduction of additional security measures on top of the Sittler code, mainly during and after the First World War. Increasing geopolitical pressure threatened Dutch neutrality and positive results of cryptanalytic efforts seemingly galvanized the Dutch Department of Foreign Affairs to introduce these additional measures. Techniques such as superencipherment would come to be applied on top of the Sittler codebooks, mitigating some of their weaknesses and reducing the perceived urgency of replacing them altogether.

1.1 Sources

This article is mainly based on the archives of the Cabinet of the Minister of Foreign Affairs of the Netherlands.[1] This Cabinet was responsible for dealing with all confidential matters until the start of the Second World War. This included correspondence with Dutch diplomatic envoys and matters related to Dutch ciphers used for this correspondence. The several archival entries concerning these matters will be central to this paper. The sources consist of a somewhat eclectic, largely chronologically ordered collection of codebooks, correspondence with envoys related to the use of codes, correspondence from sellers trying to advertise new cryptographic systems, and correspondence with other Ministries' Departments discussing the establishment of an interdepartmental cipher bureau. Correspondence by diplomats was typically addressed to the Minister of Foreign Affairs, but letters were delivered to and handled by the Cabinet. Furthermore, this paper uses the shortened versions "Cabinet of Foreign Affairs" or simply "Cabinet" interchangeably.

First an important note regarding Dutch cryptologic terminology at the time. In most of the correspondence the terms code and cipher are used interchangeably. Basically, any message that was communicated in numbers could be considered to be in 'cipher'. This also led to the codebooks (*codeboek*) being alternately referred to as cipher book (*cijferboek*) or even encipher book (*vercijferboek*) by some diplomats.

This article continues with a brief description of the codebooks in question. In the sections following thereafter, it presents a chronological overview of how these codebooks were used and how thinking on their use evolved. This overview includes an examination of several of the security incidents that took place as well as the developments towards institutional cryptology within the Dutch government.

2 The Sittler codebooks

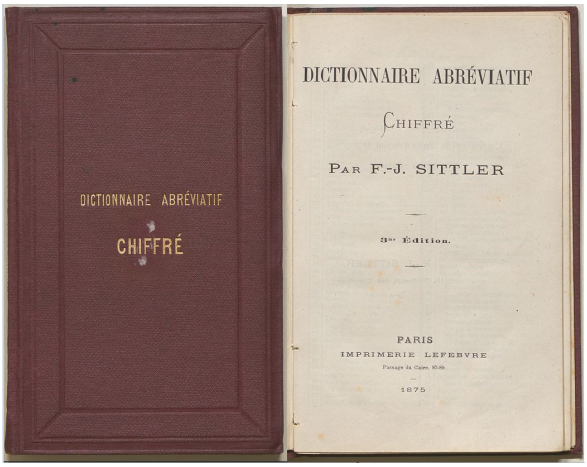

Figure 1: This 1875 third edition of the 'Sittler-booklet', used by the legation in London, is the earliest version present in the archive of the Cabinet of the Minister of Foreign Affairs; NL-HaNA-2.05.18, no. 149.

The Sittler codebooks, or *Dictionnaire Abrévatif Chiffré*, as seen in Figure 1 above, were commercially available hundred-page booklets. They were initially published by the Paris-based *Imprimerie Lefebvre* and later sold by the international book wholesalers Boyveau & Chevillet.[2] The earliest mention of a Sittler book being used for Dutch diplomatic communication can be

[1] Nationaal Archief, The Hague (NL-HaNA), Inventory of the Cabinet Archives of the Ministry of Foreign Affairs, 1871-1940, 2.05.18, nos. 149-153; Hereafter NL-HaNA-2.05.18.

[2] Abbreviated cipher dictionary; Lefebvre Printing Company. These and all following translations have been done by the author.

found in 1878.[3]

French words, or combinations of words, were encoded by taking the two assigned page numbers and following these with the two numbers assigned to each word on the page.[4] These four-digit numbers would then be written down in groups of five. Since most of the entries in the booklet exceeded four letters, encoding them in this way shortened messages, making them cheaper to send. Minor adjustments, such as changing rarely used words, to words not included in the book or changing page numbers, offered limited additional security.[5] This did have an adverse side effect, since the many different Dutch consulates and legations possessed codebooks with different paginations and thus could not communicate with one another. This resulted in larger consulates, like that of Constantinople for example, having to maintain a multitude of codebooks corresponding with those of smaller consulates in the region.

3 The long road to awareness

Before, during, and after the First World War, the Dutch Cabinet of Foreign Affairs received numerous indications, usually through correspondence with Dutch diplomats, that the codes used by the diplomatic service had been compromised or broken by foreign governments. The next two sections trace how the Cabinet and Department of Foreign Affairs, as well as the diplomats themselves, responded to these concerns, examining their views and considerations regarding communication security, the incidents that occurred, and the measures taken to secure communications further.

The period from the adoption of the Sittler codebooks up until the First World War passed without major developments in terms of improvements to procedure and security. Despite incidents regularly occurring, envoys made mistakes and at several points indications were received that foreign governments read Dutch communications. Nevertheless, improvements were sporadic and small-scale, some legations implemented security tricks like adding nulls, reversing the code when written down, using multiple sets of paginations or adding a certain number to specific groups of numbers based on a chosen lawbook or day of the year, but no major, universal, adaptations were made.[6]

3.1 Van Vredenburch's first memorandum

In 1908, the diplomat Jhr.[7] dr. C.G.W.F. van Vredenburch (1874-1927), sent a letter to the Cabinet stating that the Dutch use of the Sittler codebook was known to German, Austrian and possibly Russian officials, and that any "*bureau noir*" would make short work of them. In an appended memorandum, he proposed the implementation of additional superencipherment or self-produced codebooks for confidential telegrams unique to each legation. These propositions were promptly shot down by the Cabinet. An unknown official argued in their reply that no code was completely safe, and because the "key" (i.e. pagination), was not universal to all codebooks, only few had been compromised. The official goes on to conclude that creating distinct superencipherments or codebooks for each legation simply was too labour-intensive to be feasible.[8] This response illustrates that the Cabinet prioritised administrative convenience over absolute secrecy, accepting the risk of compromised communications as a normal part of diplomatic practice.

One reason for this lack of urgency possibly lay in a common sentiment regarding the purpose of encoding communications. As the following section will demonstrate, the perceived primary aim of using codes was not to prevent content from being known by foreign governments, but rather to shield information from subordinate officials and telegraph personnel, people who, because of their social background, were implicitly assumed to be less trustworthy and discreet.[9]

[3] NL-HaNA-2.05.18, no. 149, Cyfer voor het gezantschap te London, June 26, 1878.

[4] Meaning the 42nd word on page 55 would be encoded as 5542.

[5] Over the decades these paginations were divided in increasingly smaller segments, a codebook from 1879 was cut up in two even sections, pages 99-50 followed by pages 00-49, later codebooks, like the one used in 1921 by the Dutch legation in Warsaw, were divided up in many uneven sections, pages 36-44, 09-00, 87-99, 56-45, 10-21, 65-74, 22-35, 86-75 and 57-64.

[6] Correspondence concerning these mistakes and security tricks can be found in NL-HaNA-2.05.18, no. 149.

[7] Jhr., short for Jonkheer, is the title carried by Dutch lower nobility.

[8] NL-HaNA-2.05.18, no. 150, Letter Jhr. van Vredenburch to the Minister of Foreign Affairs (MinFA), Lisbon, March 4, 1908; Response from Cabinet March 24, 1908; Dutch institutional cryptographic expertise to perform these tasks had not been present for a time, possibly since the early nineteenth-century. See de Leeuw, 2000.

[9] For a foundational work on class distinctions and resulting social practices and judgements see Bourdieu, 1984.

3.2 De Stuers' letters

A letter by the long-time Dutch resident minister in France, A.L.E. ridder[10] De Stuers (1841-1919), presents a clear and frank example of this attitude regarding the use of codes.[11] When the First World War was still in its infancy, in September of 1914, De Stuers wrote to the Cabinet of Foreign Affairs in response to a French ban on communications in cipher by envoys of neutral nations. In this letter, De Stuers reports that he had assured Pierre de Margerie (1861-1942), the political director of the French Ministry of Foreign Affairs, the following:

> The cipher had no state secrets to conceal, it was only used to assure messages of a certain delicate nature would not be disclosed to subordinate officials and to the public of the postal offices.

In isolation, this statement might be read as an insincere reassurance, offered by a diplomat seeking to placate French officials. In context, however, it reveals De Stuers' underlying view of the main purpose of using codes. As he indicates in the same letter that he was far less troubled by French government officials reading his correspondence.

De Stuers further explains that he had gotten de Margerie to agree to a concession whereby the latter would arrange for encoded Dutch dispatches to be sent to the French ambassador in the Hague, who would have them delivered to the Dutch Department of Foreign Affairs. But, to appease the supreme commander of the French armed forces, General Joffre, who apparently was not a fan of diplomats, de Margerie requested to be informed of the nature and subject of the dispatches.[12] De Stuers found himself agreeable to the request since:

> The officials of the *Kabinet noir* (sic) - that in regular times deciphered all ciphered telegrams – have gone to war. Since the contents of our telegrams were previously known in their entirety, it matters little whether I now disclose the subject matter discussed.

He goes on to somewhat ironically add the following remark:

> Incidentally, I intend to replace our cipherbook with a new one in any case.

This letter perfectly demonstrates the aloof attitude of De Stuers at the outset of the war. He writes nonchalantly about French officials reading Dutch correspondence almost as a commonly known fact that warranted little concern. This unconcerned attitude, echoing that same untroubled point of view in the Cabinet reply to Van Vredenburch six years earlier, seems to have been typical of the Dutch diplomatic service in the decades leading up to WWI.

3.3 Growing concerns

De Stuers' letter, along with other archival material, demonstrates that this nonchalance was not a result of naïveté regarding the existence and success of foreign black chambers, either before or after WWI. Foreign efforts to decipher Dutch communications are referenced in correspondence between high government officials as well as in letters by Dutch diplomats, often in relation to a mistake having been made or in relation to having received indications their communications had been compromised.[13]

As WWI progressed, Dutch neutrality continued to be threatened and diplomatic controversies occurred (Abbenhuis, 2006; van Tuyll van Serooskerken, 2001). These external developments heightened awareness of the risks associated with insecure diplomatic communications. At the same time, Dutch General Staff cryptanalysts started booking the first results in breaking German codes in April of 1915 (Jacobs and van Kampen, 2024). The intelligence derived from these efforts likely reached the Minister of Foreign Affairs

[10] *Ridder* (knight) is the lowest noble rank after Jonkheer.

[11] NL-HaNA-2.05.18, no. 151, Letter A.L.E. ridder De Stuers to MinFA, Bordeaux, September 21, 1914.

[12] De Stuers remarks in his letter that: '[General Joffre,] like so many that know little of diplomats, must think they are nothing but official spies in an embroidered uniform'.

[13] To list a number of examples: Rijks Geschiedkundige Publicatieën (RPG) 116, pages 390-391, 570; NL-HaNA-2.05.18, no. 152, Letter Minister of War to Ministers of the Navy, the Colonies and MinFA, February 19, 1919; Letters of diplomats: NL-HaNA-2.05.18, no. 150, Letter Jhr. van Vredenburch to MinFA, Lisbon, March 4, 1908; NL-HaNA-2.05.18, no. 151, Letters ridder van Rappard to MinFA, Washington February 28, 1916 and October 18, 1916; Letter D. baron van Asbeck to MinFA, Tokio, March 9, 1915; Letter Jhr. van Vredenburch to MinFA, Stockholm, March 27, 1919; Letter Jhr. Van Weede van Berencamp to MinFA, July 2, 1919; NL-HaNA-2.05.18, no. 152, Letter P.B. Hubrecht to MinFA, Washington D.C., September 14, 1921; Letters W.A.F. baron Gevers to MinFA, Berlin April 12, 1923 and June 9, 1926; Letter J.C. Pabst to MinFA, Tokio, June 14, 1923; Letter consul in Jeddah to MinFA, Jeddah, July 4, 1923.

and the chief official of his Cabinet shortly thereafter,[14] leading them to further realise the risks associated with the evident shortcomings of existing Dutch communication security.

Many of the letters cited above include explicit questions about whether existing procedures should be revised or whether better alternatives to the Sittler codebooks were available.[15] Importantly, such concerns persisted even after additional measures were introduced, indicating a sustained shift in attitude toward communication security.

3.4 First additional measure

As far as we can surmise from the archive of the Cabinet of Foreign Affairs, in July 1915, the first additional encryption method was introduced to improve the security of diplomatic communications, initially called '*cijferstammen*' (cipherstems).[16] Because the Cabinet archive mainly contains correspondence about the cipherstems and their deliveries, it is difficult to reconstruct this first measure and its use fully, but we do know several things. The means to use this new method were mainly provided to the more important legations, usually those in capitals of warring powers. With the adoption of the cipherstems, a distinction started to be made between regular messages that required encryption with just the Sittler booklet, and "secret" messages that required an additional layer of encryption through superencipherment.

To provide this extra layer, the cipherstems were introduced. The single surviving example of a sheet with such cipherstems is shown in Figure 2. The sheet shows the same sequence of 34 numbers written by hand three times. The sequences are spaced out evenly over the page and a grid has been drawn in pencil in which the numbers appear. According to separately found instructions,

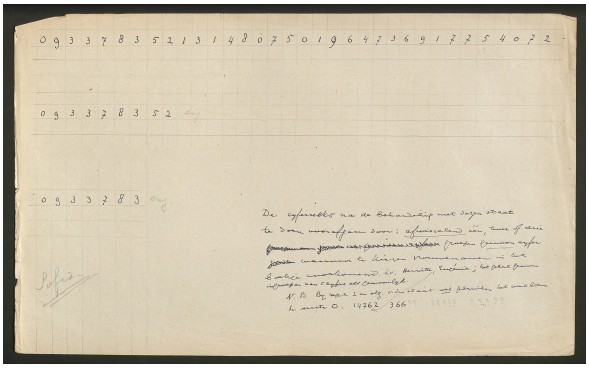

Figure 2: The only surviving example of the cipherstems (date unknown), used between 1915 and 1919. The text says: 'The series of numbers after treatment with these stems should be preceded by: alternately one, two or three groups of the regular cipher for which female names appearing in the booklet should be chosen.' In the bottom left corner, the name of the Bulgarian capital, Sofia, is pencilled in; NL-HaNA-2.05.18, no. 151.

this sequence of 34 numbers would be added in its entirety to a similarly long sequence of numbers that resulted from a regular encoding using the Sittler booklet.

The cipherstems were distributed in batches designated A, B, or C. These batches contained between fifteen and thirty-five sheets each. Unfortunately, no documentation within the Cabinet archive details the differences between the three designations. Correspondence does show a progression in their adoption, some legations first received undesignated cipherstems in 1915 (retroactively designated A). In the following years, the legations received batches of cipherstems marked B or C, always accompanied by an instruction to destroy the previously used stems. It is unclear how often a single stem was used. A 1919 letter by a diplomat suggests adopting a different sheet of cipherstems for each day of the month would further improve security, indicating each sheet differed from the others, and that they were used more frequently than once a month.[17]

As correspondence between the Cabinet and diplomats shows, the idea of using codes because of possible indiscretions by subordinate staff or telegraph personnel persisted later into the war and after it, but with one important difference. Now a clear distinction was being made between

[14] Intelligence officers made frequent visits to the chief official of the Cabinet during the war, dr. W.I. Doude van Troostwijk (1868-1957); See NL-HaNA-2.04.53.21, no. 17, Diary van Woelderen.

[15] See note 10; One such procedure was the requirement for consuls to send cleartext versions of their telegrams to the accounting department (staffed with unknown civil servants) in Netherlands through regular mail services every quarter, to account for telegraph costs made. A consul noted that these letters would be subject to censorship, giving host countries access to cleartext versions of coded communications.

[16] In the following years they would come to be alternately referred to as *cijferstaten* (cipher tables), the same name a later system would also carry. For clarity I will refer to this system only as the cipherstems and to the later system only as the *cijferstaten*.

[17] NL-HaNA-2.05.18, no. 151, Appendix letter Van Vredenburch to MinFA, March 27, 1919.

the use of the *geheimcijfer* (secret cipher) and the *gewoon cijfer* (regular cipher), the latter being employed 'exclusively to avoid possible indiscretions by telegraph personnel', and the former being employed only 'for telegrams of which the confidentiality is truly of importance'.[18] Interestingly, in contrast to other nations (Ferris, 2020; Larsen, 2017; Lasry, 2018), the Dutch diplomatic service seems to have continued using the same codebook for communications that required different levels of secrecy until 1931.[19]

3.5 Continued advocacy

The adoption of additional security measures did not stop the questioning of the use of the Sittler booklets. In 1919, the same Van Vredenburch who had criticised the use of the Sittler booklets before, wrote another memorandum to the Cabinet and the new Minister of Foreign Affairs in the Netherlands. Because Van Vredenburch had since studied contemporary cryptologic literature, he was now able to level much more substantive criticism at current Dutch practices, specifically the use of the Sittler booklets. His memorandum details the shortcomings of the Dutch encryption methods, some of the incidents that further compromised security, common cryptologic principles, the methods and techniques used by cryptanalysts, and suggestions on improvements in security. Van Vredenburch refers to the 'cipher of Sittler' as a 'one-part cipher of the simplest sort'. He goes on to sum up the reasons why 'Sittler's booklet is especially compromised':

> 1°. The booklet is commercially available, 2°. It has been in use for years, 3°. It has been in possession of representatives of foreign powers (among others in Tangiers, Caracas or Teheran), 4°. Honorary consular staff, non-Dutch persons, have been in possession of the books (among others in Bucharest, Belgrade, Lisbon, Kristiania etc.), 5°. Because almost none of the legations possesses a safe and the booklet is usually kept in a possibly unlocked drawer, 6°. Because the legations simply rip up draft papers and throw these in the refuse and do not burn them.[20]

As proof of the insecurity of the ciphers, Van Vredenburch follows with an anecdote of when he was the Dutch envoy to Vienna in 1906. There, he received a Sittler-encrypted telegram from the Netherlands containing a message for the Foreign Minister of Austria-Hungary. Before Van Vredenburch could relay this message, he had the displeasure of finding it had been decrypted and published in that day's evening edition of the *Neue Freie Presse*, a Viennese newspaper. He surmises that the Austro-Hungarian '*Chifferbureau*' had been able to promptly decrypt the message and had leaked it to the paper.[21] One could speculate that this earlier episode drove Van Vredenburch to share his earlier criticism and to educate himself on contemporary cryptology.

In the letter accompanying the memorandum, Van Vredenburch seems to plead for the establishment of more permanent cryptologic expertise, and urges the Cabinet to circulate his letter to the departments of War and the Colonies. He stressed that this had become more urgent than ever before, as Dutch communications not only had to be protected from foreign agents, but also against the agents of the '*Bolscheviki*, who are certainly no less to be feared'.[22] This concern leads to Van Vredenburch's closing remarks, in which he points to developments taking place in Sweden:

> As Sweden had unpleasant experiences with its unreliable cipher during the World War, the Commission responsible for reorganising this Department proposed that a separate office, headed by an official with the rank of chief archivist and assisted by a few clerks, should henceforth be responsible for ciphering and deciphering.[23]

In the surrounding context of his description of the development, Van Vredenburch seems to recommend a similar institutional arrangement for

[18] NL-HaNA-2.05.18, no. 151, Letter Cabinet to W.J. Oudendijk, Dutch envoy in Petrograd, May 16, 1918.

[19] After 1919, this was also true for the German diplomatic service, their codebook had the main purpose of shortening messages, in contrast to Dutch use, German communications were always superenciphered in different ways depending on their level of confidentiality (van der Meulen, 1998).

[20] NL-HaNA-2.05.18, no. 151, Appendix letter Van Vredenburch to MinFA, March 27, 1919.

[21] Ibidem.

[22] This letter was written just five months after a failed socialist revolution in the Netherlands, for additional information, see Linmans, 2024.

[23] NL-HaNA-2.05.18, no. 151, Letter Van Vredenburch to MinFA, March 27, 1919.

the Dutch Department of Foreign Affairs. Later that same year, a Dutch interdepartmental cipher bureau was indeed established, formally under the auspices of the Department of Foreign Affairs. Whether Van Vredenburch's letter played a decisive role in the bureau's establishment is unknown, but the letter demonstrates that members of the diplomatic service were actively advocating for improved communication security and the abandonment of the Sittler code.

4 The *Cijferbureau*

Following these developments with Dutch diplomatic codes as well as Dutch cryptanalytic successes during the First World War (Jacobs and van Kampen, 2024), a Dutch interdepartmental cryptologic agency practicing both cryptography and cryptanalysis was established in late 1919, becoming official in 1920 (de Leeuw, 2015).[24] This was a relatively unique arrangement for that time (Gentry, 2019). The '*Cijferbureau*' as it came to be called, was headed by H. Koot (1883-1959), a former officer that had shown a great level of proficiency in both cryptography and cryptanalysis during the First World War (Jacobs and van Kampen, 2024).[25] According to the personal journal of a high-ranking Dutch intelligence officer, the recently appointed Minister of Foreign Affairs, Jhr. H.A. van Karnebeek (1874-1942), had been the main proponent of the establishment of the *Cijferbureau*.[26] This marked a shift in thinking within the highest levels of the Dutch government regarding the necessity of establishing a more permanent cryptologic expertise.

4.1 Ramping up security

Shortly after the establishment of the *Cijferbureau*, the use of the Sittler booklets was updated to provide additional security. The earliest mention of this update can be found in September of 1920.[27] From now on, many of the booklets would have two different sets of paginations, meaning each page had two different page numbers. One was written in blue pencil, which was known as the regular cipher or blue pagination, and worked similarly as before.[28] The other pagination was written in black pencil, known as the secret cipher or black pagination. It was unique to each booklet and thus could mainly be used to communicate with the Cabinet, or with delegations to international conferences if identical codebooks were provided. In addition to this different pagination, the secret cipher would also be superenciphered using '*cijferstaten*'.[29] Like the cipherstems, this method for superenciphering seems to have initially only been made available to the larger and more important consulates, as well as attendees of international diplomatic conferences.

4.2 The *cijferstaten*

The *cijferstaten* were a similar, albeit updated and more sophisticated version of the cipherstems. They comprised two to four file folders with six couplets of rows cut out of the front page each. In between these cut-away-rows were a series of "randomised" typed numbers. Differing from the earlier system, all rows contained a differing chain of numbers, see Figure 3. They were to be used as follows: a sender would place an empty page inside the folder, in the cut-out row above the numbers, users were instructed to fill in the ciphers (single file) following an encoding with the black pagination of their Sittler booklet. Then, each number of the resulting code would be added to the corresponding number from the chain of randomised numbers below. The resulting sum would be written down in the cut-out row below the numbers. The numbers were added modulo 10, so, 5+9 would become 4. This new system was both easier to apply (by only adding single digit numbers together), and provided better security than the previous system because it was much less repetitive.

Perceptive readers might have observed that this method, if used correctly, could function as a one-time pad (OTP). This was, however, not how the system was used. Recipients of the *cijferstaten* periodically (with unknown frequency), or after a request, received two or four file folders with a total of 12 or 24 numbered lines of 32 randomized numbers.[30] Because the Sittler code ascribed

[24] The several army branches and Ministry of the Colonies had come to similar conclusions about the need to improve communications security by 1920.

[25] Rijks Geschiedkundige Publicatieën (RPG) Grote Serie 116, pages 391, 570.

[26] NL-HaNA-2.04.53.21, no. 17, Diary van Woelderen, Entry March 3, 1919.

[27] NL-HaNA-2.05.18, no. 152, Letter Cabinet to Jhr. Mr. dr. R. de Marees van Swinderen, envoy in London, September 2, 1920.

[28] Note that this pagination would be similar for some books, but was not universal

[29] Cipher tables; On occasion they were also referred to as '*optelstaten*' or addition tables

[30] The number of folders received varied, it is unclear why,

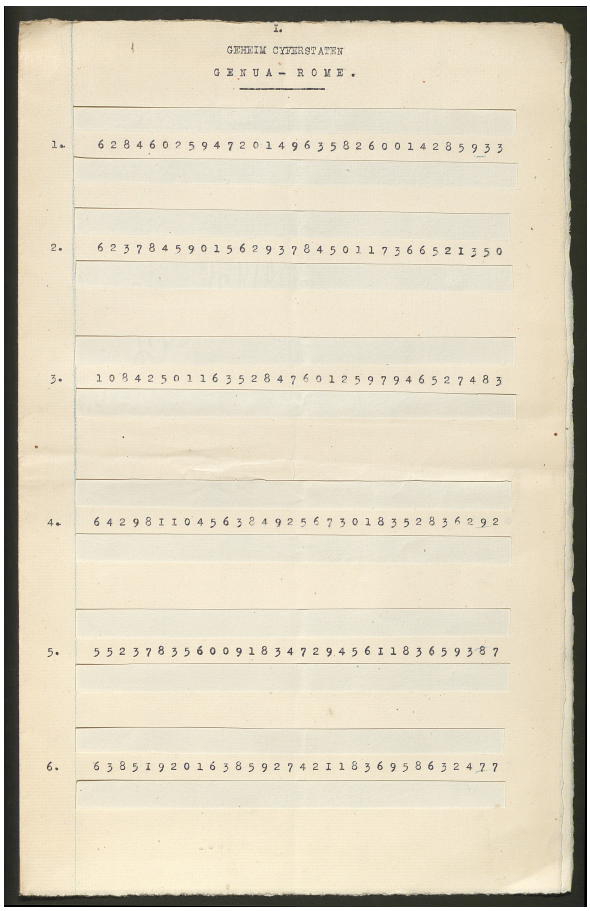

Figure 3: These *cijferstaten* were designed to superencipher communications between Dutch diplomats in Rome and attendees of the Genoa Economic and Financial Conference of 1922; NL-HaNA-2.05.18, no. 152.

four numbers to every word, this meant that without repetition, the *cijferstaten* could only superencipher a maximum of 96 or 192 words. So instead, its users were instructed to start the superenciphering with one of the 12 or 24 lines corresponding to the serial number of the telegram they were enciphering. If a serial number exceeded the total amount of lines, the starting line would be calculated modulo 12 or 24 depending on the number of folders. Meaning, if the telegram had the serial number of 55 and was superenciphered using two folders, the starting line for superenciphering would be the seventh (4x12+7=55). When a message exceeded 96 or 192 words, the numbered rows were to be reused in the same order. Correspondence between Dutch diplomats and the Cabinet suggests there possibly was a limited amount of allowed re-uses, or a limited timeframe in which they were to be used, but this amount is never specified in the letters nor in the available instruction materials.

but it is likely that consulates that corresponded more, received more folders. When Queen Wilhelmina travelled abroad, she received just a single folder with six lines to communicate in secret.

4.3 Further incidents

The added security measures did not, however, prevent further incidents from occurring, especially not ones caused by human error. The earliest incident after the adoption of the *cijferstaten* known to us happened just a year later in September 1921. Following this incident, the temporary Dutch envoy to Washington, P.B. Hubrecht (dates unknown), wrote an apologetic, non-official, private letter to a relation within the Department of Foreign Affairs. In this letter, he describes an episode where, what he calls 'an unfortunate concurrence of events', led to a miscommunication between himself and a staff member. This miscommunication resulted in the same message being transmitted twice, once in the secret cipher, and once in cleartext.[31] He goes on to inquire whether it might be a good idea to replace the five rows of the *cijferstaten* that were used to superencipher the message, which got an affirmative reply from the Cabinet of Foreign Affairs.[32]

Although the proper adoption of the *cijferstaten* reduced the number of reports by diplomats that their communications were being read by foreign governments, they were not invulnerable. This became apparent during Dutch German trade negotiations taking place in 1926. Following these negotiations, W.A.F. baron Gevers (1856-1927), who had been critical of the continued use of the Sittler booklets before,[33] wrote that he had ample grounds to believe that the secret cipher was known to the German government. He reported receiving very clear indications that at least one ciphered telegram was known in its entirety to the German government. According to Gevers, this had negatively affected the outcome of agreements regarding seaport exemption rates.[34] This episode illustrated the very direct consequences of inse-

[31] This was not an uncommon occurrence, this type of mistake was and would continue to be the most prevalent type of human error.

[32] NL-HaNA-2.05.18, no. 152 Letter P.B. Hubrecht, Washington D.C., September 14, 1921; Ibidem, Reply by Cabinet.

[33] Baron Gevers had even proposed alternative cipher systems twice before.

[34] NL-HaNA-2.05.18, no. 152, Letter W.A.F. baron Gevers to the MinFA, Berlin, June 9, 1926.

cure communications. Other than scribbled notes asking and confirming that the telegram Gevers mentioned was indeed sent in secret cipher, the response to Gevers' remarks from the Cabinet is sadly lost to us.

4.4 More partial solutions

At some point in the early 1920s, an additional, possibly universal code was adopted for consular communications.[35] The so-called 'Bibabo-code' or 'bigramcode'. Sadly, correspondence regarding the specifics of the Bibabo-code is scarce. From circumstantial mentions, it seems to have been a cipher system designed to reduce telegraph costs and allow for communications between all consulates. The Bibabo-code made use of a Sittler book without adjusted pagination to encode messages. It is likely the resulting numbers would then be transformed into letter bigrams, which could form fictive words. Interestingly, with the adoption of the Bibabo-code, the use of the regular cipher was not abolished, meaning there were now three different levels of communications making use of the same codebooks, with each individual diplomat being entrusted to weigh the costs and benefits of using a particular system.[36]

4.5 Cipher machines?

In 1923 and 1924, the Department of Foreign Affairs was approached by the director of the Amsterdam-based trading company Koopman & Co., who acted as an agent for '*Hamelin*'(sic) from the Stockholm-based A.B. Cryptograph.[37] In February 1924 Koopman proposed a meeting to be set up between Hagelin and Koot for them to discuss a cryptographic machine. Koot accepted the meeting and later that same week, it took place.[38] It is difficult to ascertain what the results of the meeting were, but we have no evidence of cipher machines being used by the Dutch diplomatic service until the Second World War. We do know however, that other parts of the Dutch government did adopt cipher machines. Karl de Leeuw has described how in 1915 the Dutch Navy adopted a cipher machine on an experimental basis for the duration of the First World War (de Leeuw, 2003). The earliest known purchase of commercial cipher machines was done by the Department of the Colonies. By the beginning of 1926, an order had been placed for an unknown number of machines produced by A.B. Cryptograph, called the 'electric cipher machine "DAMM"' by Dutch officials. This description likely refers to the two-rotor machine B13, developed by the Swedish inventor A.G. Damm (1869-1928). Even with the adoption of cipher machines by the Ministry of the Colonies in 1926, a priority of safeguarding information from subordinates was still present. In an official document to the desk of the Minister of the Colonies, Koot states:

> In my opinion, in addition to cipher machines, however excellent they may be from a cryptographic point of view, there will always continue to be a need for separate secret codes, not only for the highest government bodies, but also for the secret radio operations between the Netherlands and the Dutch East Indies.[39]

His point being that even though cipher machines might provide better security, for communications of the highest levels, it was preferable to make use of a different, easier to use, cryptographic system (a system that he himself would provide). Such a system would not require the intercession of a specialized cipher machine operator, who was presumably regarded as less discreet. Here Koot makes the (likely correct) assumption, that the gentlemen in the highest government circles could not be trusted to operate a cipher machine by themselves, requiring a more manageable system, even if that meant it was less secure.

5 The Dutch code

Starting in 1931, after over fifty years of continuous use, the Sittler booklets finally started to be phased out within the Dutch diplomatic service. The *Cijferbureau* had developed new Dutch-language codebooks. Unfortunately, none of these books have been found in this archive or other publicly available archives, and very little circumstantial information regarding their nature remains. The new books were also used to send communications in both a regular cipher and a

[35] The first mentions can be found from January 1925, but it had been established earlier; NL-HaNA-2.05.18, no. 152.

[36] Ibidem

[37] Ibidem, Letter Koopman February 4, 1924; A misspelling of Hagelin; For more information on Koopman & Co see `https://www.cryptomuseum.com/manuf/koopman/`

[38] Letter Cabinet to Koopman & Co, February 5, 1924.

[39] NL-HaNA-2.13.70, no. 1812.

secret cipher with *cijferstaten* for superencipherment. The books were issued together with a secret-cipher-condenser manual, which described how to transcribe messages into pronounceable ten-letter words, making them cheaper to send.[40] Basically, the way codebooks were used changed very little, but the books themselves were replaced. This did not yet mean the definitive end of the Sittler books however, as recipients of the new Dutch codebooks were instructed to keep their Sittler books, in case any messages necessitated the use of French.

6 Conclusions

The continuous use of the Sittler codebooks by the Dutch diplomatic service was not the result of simple ignorance or technological backwardness, but rather a collection of practical, cultural and institutional considerations that shaped policy for over fifty years. The continued use of the Sittler booklets, despite the recurring reports by diplomats that secret communications were compromised, can partially be explained through a practical lens, their low cost and the convenience of commercial availability, practical applicability by cryptographic novices, and reduced telegraph expenses. This shows that secure diplomatic communications were not seen as strictly essential for safeguarding national interests.

Equally significant was the prevailing diplomatic and class culture in which secrecy was understood as much in social as in strategic terms. Before WWI, the use of codes and ciphers primarily had the function of shielding sensitive communications from telegraph clerks and subordinate staff, not from foreign governments, whose senior officials would have likely been regarded as social peers. This attitude can help explain the tolerance for insecure communications and slow cryptographic reforms. Only under the geopolitical pressures of the First World War, when Dutch neutrality was increasingly threatened, the stakes of careful diplomacy rose, and the benefit from cryptanalysis of German codes became clear, did this perspective begin to adapt. The gradual implementation of additional security measures during and after WWI, like the different levels of secrecy, the different cipher tables and the establishment of the *Cijferbureau*, illustrates a more incremental approach to security improvements, rather than decisive breaks in practices.

This article has tried to show how cryptographic practices were shaped as much by social norms, notions of trust, administrative pragmatism and financial constraints as by awareness of strategic security risks. Practical, social and cultural considerations were continually balanced with more abstract concerns of secrecy and communication security in a changing diplomatic and geopolitical context. This case has shown it is valuable to study cryptology not merely as a technical domain, but also as a praxis of secrecy. In other words, by viewing cryptology as a way to 'do' secrecy, we find that how, when, why and where it is applied, is shaped by a myriad of factors. In turn, this can help us better understand shifting conceptions of state secrecy and the role of communications in international relations historically.

[40] This manual, as well as correspondence concerning the new codebooks can be found in: NL-HaNA-2.05.18, no. 153; The condenser is specifically described as being different from the Bibabo-code, because the condenser did not solely consist of bigrams.

Acknowledgements

The author would like to thank Bart Jacobs, Rowin Jansen and Florentijn van Kampen for their valuable feedback.

References

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

Pierre Bourdieu. 1984. *Distinction, A Social Critique of the Judgement of Taste*. Routledge & Kegan Paul, London.

Karl de Leeuw. 2000. *Cryptology and statecraft in the Dutch Republic*. Universiteit van Amsterdam, Amsterdam.

Karl de Leeuw. 2003. The Dutch Invention of the Rotor Machine, 1915-1923. *Cryptologia*, 27(1):73–94.

Karl de Leeuw. 2015. The Institution of Modern Cryptology in the Netherlands and in the Netherlands East Indies, 1914–1935. *Intelligence and National Security*, 30(1):26–46.

John Ferris. 2020. *Behind the Enigma, the Authorised History of the GCHQ, Britain's Secret Cyber-Intelligence Organisation*. Bloomsbury Publishing, London.

John A. Gentry. 2019. Selective SIGINT: Collecting Communications Intelligence While Protecting One's Own. *International Journal of Intelligence and Counterintelligence*, 32(4):647–676.

Bart Jacobs and Florentijn van Kampen. 2024. A new perspective on Dutch WWI codebreaking with its international ramifications. In *Proceedings of the 7th International Conference on Historical Cryptology, HistoCrypt 2024*, pages 135–145. Linköping University Electronic Press.

Daniel Larsen. 2017. British codebreaking and American diplomatic telegrams, 1914–1915. *Intelligence and National Security*, 32(2):256–263.

George Lasry. 2018. Deciphering German Diplomatic and Naval Attaché Messages from 1914-1915. In *Proceedings of the 1st International Conference on Historical Cryptology, HistoCrypt 2018*, pages 55–64. Linköping University Electronic Press.

Wouter Linmans. 2024. *Revolutiekoorts: Onrust en oproer in November 1918*. Athenaeum, Amsterdam.

C. Smit. 1964. *Bescheiden Betreffende de Buitenlandse Politiek van Nederland, 1848-1919, derde periode 1899-1919, Vijfde deel, 1917-1919, Eerste stuk*. Number 116 in Rijks Geschiedkundige Publicatieën, Grote Serie. Martinus Nijhoff, The Hague.

Michael van der Meulen. 1998. The Road to German Diplomatic Ciphers - 1919 to 1945. *Cryptologia*, 22(2):141–166.

Hubert P. van Tuyll van Serooskerken. 2001. *The Netherlands and World War I, Espionage, Diplomacy and Survival*. Brill Publishers, Leiden.

Carel Albert van Woelderen. 1919. *Dagboek van Van Woelderen, een medewerker van GSIII, met toegang, kopieën, 1916-1919*. Number 17 in NL-HaNA, 2.04.53.21 Inventaris van de collectie De Meijer: Binnenlandse Veiligheidsdienst (BVD). 1916-1940.