Cryptology and statecraft in the Dutch Republic

de Leeuw, K.M.M.

Citation for published version (APA):
Introduction and summary

This dissertation consists of six articles that have been published elsewhere and a general overview that render an account of the history of cryptology in the Netherlands, mainly during the 18th century. The two main articles deal with the interception of mail and the breaking of codes and ciphers, respectively during the periods roughly coinciding with the War of the Spanish Succession (1707-1715) and the Seven Years' War (1751-1763). The main purpose of these articles is to identify the factors that explain the existence of a Black Chamber in the Dutch Republic, both from the perspective of international affairs and of the proliferation of the skills required to engage in such an enterprise. Secondly, two articles are included that were written with Hans van der Meer. These articles deal with the solution of two unidentified, enciphered messages that were found respectively in the archives of Grand Pensionary Laurens Pieter van de Spiegel and Stadholder William V and with their place in history. The fifth article deals with the use of ciphers by Princess Wilhelmina of Prussia during the exile of the House of Orange in the period of the Revolutionary and Napoleonic wars. This article focuses particularly on a very remarkable cipher used for the correspondence between the Stadholder and his wife in London and the members of their family in Germany, in particular the Hereditary Prince in Berlin. It tries to identify the man or woman who constructed this cipher and investigates the motives that account for its use. The sixth article, also written with Hans van der Meer, deals with another turning grille used by the Hereditary Prince in 1800 for his communication with Alexander van Spaen who acted as a liaison with the Batavian Government. It shows that the turning grille was still being used by a member of the House of Orange some 50 years after its introduction, albeit on special occasions only. In the preceding overview the context for these articles is presented. The main goal in the overview is to establish the connection, if any, between activities in the field of codebreaking and the construction of ciphers and codes. This overview, however, covers a much longer period than found in the articles. It gives an outline of the practices in the field of mail interception and code-breaking from the beginning of the Eighty-Years' War onwards; it accounts for the use of codes and ciphers by the States-General during the existence of the Dutch Republic and it ends with a survey of the factors that contributed to the closing of the Black Chamber during the Batavian period and of the consequences for the use of codes during the period thereafter. The overview also pays attention to the theories that have been forwarded by others about the history of cryptology in general and it investigates whether any of these theories are relevant for the situation in the Dutch Republic and if so, in what way. It should be noted, however, that the actual role of codebreakers in the construction of codes and ciphers is only part of the problem treated here. The overview also deals with the influence of contemporary, cryptological literature and with possible links between the development of cryptology and other fields of knowledge, such as linguistics, probability theory and mathematics proper. The conclusions yielded by this research should be differentiated according to period. During the period before 1650 various codebreakers can be proven active that all focused on intercepted, Spanish code-material, but there is no evidence that these codebreakers were also involved in the construction of codes and ciphers for use of the Dutch authorities themselves other than occasionally. To make things worse, it is not clear whether there has been a 'Dutch school' in cryptanalysis or not. It is not sure, for instance, whether
Constantijn Huygens the Elder who was active after the Twelve-Years’ Truce was trained by Jacques d’Aleaumé who was active as a codebreaker before the Truce, although there can be no doubt that Huygens was trained at an early stage in his career. The same question applies to D’Aleaumé who may have been trained by Marnix, but it cannot be ruled out that he received his training abroad and he may even have been self-taught. Additionally, the question remains whether or not there was any exchange of information between Marnix and the French mathematician Viète who was engaged in the breaking of intercepted Spanish code-letters too. This may seem likely, but any corroborating evidence is lacking, for the moment at least.

The period after 1650 is marked by a systematic effort in the use of secret writing, particularly so in the context of diplomacy. This was a result of the Peace of Westphalia and the establishment of permanent diplomacy between the Protestant and the Catholic powers. Surprisingly, the construction of these codes and ciphers was put into the hands of ordinary clerks at the Registry of the States General who had no experience as codebreakers whatsoever and who probably did not even know that there were any cryptanalysts around at all. This didn’t mean, however, that Dutch codes and ciphers lacked all quality during this period. This was mainly a result of the application of Athanasius Kircher’s ‘Arca Steganographica’ in combination with a codebook that consisted of 10,000 items or more; a codebook much larger than those customary elsewhere. This seems to indicate that whoever initially introduced this system (possibly the Greffier himself, possibly somebody else) was aware of the risks of interception of diplomatic despatches and of the possibilities of limiting the consequences through encryption. The only hazards of the system were that it remained unchanged for a hundred years or so and that it could also be used unintelligently, unlike other polyalphabetic devices such as the cipher-wheel or the Vigenère. It depended in large measure on those who happened to be in charge of the encryption of diplomatic mail at any particular moment whether this elaborate system was any better than a simple homophonic substitution cipher.

The third period that can be discerned in our investigation reaches roughly from the reign of Stadholder William III until the War of the Spanish Succession and its aftermath. These years are marked by the re-emergence of the Dutch Black Chamber under the supervision of Abel Tassin d’Alonne, who acted also as private secretary to Princess Mary and, presumably, an illegitimate brother of the Stadholder. D’Alonne’s activities as a codebreaker probably started in 1684 with the decoding of an intercepted letter written by the French Ambassador in the Republic, D’Avaux, but the peak of his career came later, during the War of the Spanish Succession, when he, acting as private secretary of Grand Pensionary Heinsius, focused on French and Bavarian code-material that was intercepted in Brussels. In D’Alonne’s case too it is not known how or where he acquired his skills as a codebreaker. It is quite possible that he was educated by Huygens, but it isn’t totally out of the question that he was, in some way, trained by a codebreaker working in Brussels under supervision of the Spanish Governor, De Grana.

It should be noted, however, that D’Alonne’s activities didn’t result in an overall revision of the codes and ciphers that had been, by that time, in use by the States General already for fifty years. This was most likely to be an unintended consequence of the secrecy that surrounded D’Alonne’s work. Grand Pensionary Heinsius was keen to avoid any debate about the interception of mail in Brussels even within the circle of his close collaborators,
because this all happened without the consent of the British. Only those who really ‘needed to know’ were informed. This meant that even the Secret Committee of the States General or prominent Dutch politicians that represented the Dutch Government weren’t informed and one may even ask whether Greffier François Fagel was properly told; however unlikely it may at first seem that he wasn’t. In general, it can be said that the confederative structure of the Dutch state and a lack of ambition in the field of foreign affairs that marked the period after the War of the Spanish Succession, prevented the Black Chamber from becoming an institution. This was very different from countries like England or Austria that after the war had come to consider the interception of diplomatic despatches as an integral part of their foreign policy, even in peace-time.

This practice was to be introduced in the Dutch Republic also, but much later. This happened only from 1751 onwards, with the interception of the despatches of the envoys of Prussia, France, Saxony-Poland and Cologne. Initially, the breaking of codes that protected these letters happened in London, but later this task was taken over by the natural scientist Pierre Lyonet who was particularly famous as an engraver of insects. Probably to his own surprise and certainly to that of others, he proved to be able to teach himself the trade on the basis of the, often incomplete, solutions of letters that arrived back from London. This became of the utmost importance in 1755 when, as a result of the changing conditions in international relations, the Dutch state could no longer rely on the support of Great Britain, in this field as indeed in others. Much to the regret of the most prominent Dutch statesmen, the Dutch Republic had to embark on a course of neutrality. During the Seven Years’ War, this meant that it had no natural allies left and that the best it could do was to stay out of conflict, a position that did not fundamentally alter after the war. The changing political climate also resulted in the Black Chamber becoming permanent and Lyonet was allowed to take on his cousin S.E. Croiset as an assistant. This development also resulted in a thorough revision of the codes and ciphers of the States-General. Lyonet had been acting as a code-clerk from 1738 onwards. This meant that he had been engaged in the encoding and decoding of letters exchanged between the States General and Dutch diplomats abroad and in that capacity he had also been responsible for devising of codes and ciphers. As a result of his experience as a codebreaker he learned what the weak spots were in the system used by the Dutch themselves and from 1755 onwards he tried to improve it. Finally this resulted in the abolishment of Kircher’s Arca Steganographica and the introduction of a new codebook that contained roughly 4000 items. The code was fundamentally one-part in structure, but this was difficult to see because every page was divided into five columns and the codegroups would follow the columns whereas their meanings would follow the rows. Moreover, every double page contained a cipher of its own, that also yielded codegroups for frequently occurring, small letter combinations, such as particles and conjunctions. Also various measures were taken to make sure that the codebooks were changed regularly.

This seems to corroborate of course Kahn’s statement that the development of cryptology during the early modern period was induced primarily by the Black Chambers, but this doesn’t mean that he was also right in assuming that the proliferation of cryptological literature was relatively unimportant. The application of Kircher’s ‘Arca Steganographica’ for so many years in Dutch cryptography points, by itself, in a very different direction. The application of some remarkable, very sophisticated ciphers by some members of the House of Orange, long before these ciphers were described in books, seems to indicate that the
practices in this field were ahead of the literature on this subject and that this literature has
to be considered as a reflection of existing developments rather than the other way round. In
that sense it seems untenable to say that the devices described in cryptological literature had
no practical value at all. It seems appropriate, however, to assume that these sophisticated
ciphers were carefully studied particularly in those circles that were aware of the existence
of the Black Chambers and of what they were capable of.
This research has yielded nothing that could be interpreted as an affirmation of Straesser’s
statement that there should have been a link between the development of cryptography and any
efforts to construct artificial languages, because in the Dutch Republic no such efforts were
made. This doesn’t mean, however, that no links can be established with other fields of
knowledge at all. In a general way, it can be said that the rise of cryptography in the Dutch
Republic profited from a pragmatic and empiricist mental attitude that dominated such
diverse fields as linguistics and medicine too. With the exception of a small paragraph in a
book by Willem Jacob ‘s Gravesande, a definite link with probability theory could not be
established, however. If ‘s Gravesande introduced any new statistical methods at all in the
field of codebreaking, he didn’t put them on paper or communicate them to others.
Therefore one can safely assume that they were of no consequence for Dutch cryptography.
In order to prevent any misunderstandings some remarks must finally be made about the
way this dissertation developed. Initially there was no intention whatsoever to write a
general work of any kind about this subject and there could not possibly have been, because
it was unknown whether there were any sources available at all. Therefore the research
project started simply as a general survey to identify possible sources in Dutch archives.
This survey showed a positive result. There were documents to be found related in one way
or another to the use of cryptography and they mainly originated the 18th century. The main
problem was, however, to connect these documents to people and circumstances.
Subsequently a few case studies were put together about enciphered messages that seemed
interesting in order to get at least some idea. This resulted in the articles published in
*Cryptologia* and *De Achttiende Eeuw*. Subsequently the focus shifted to the role of the
Black Chamber. This resulted in the articles published in *The Historical Journal* and
*Diplomacy & Statecraft*. The research for the latter yielded new insights about the role of
Pierre Lyonet that were out of line with what had been stated previously in my article
about Princess Wilhelmina (pp. 101-102). The points that I am referring to is that Lyonet
did not get the idea to intercept Prussian and French diplomatic mail by himself, that he did
not organise this alone, and that he developed the skill to break codes not totally out of the
blue, as he all claimed in his diary. In this respect the article about Princess Wilhelmina
should be compared carefully with what is to be found in the article about Lyonet’s Black
Chamber. Secondly, it should be noted that there is a slight change of perspective between
the article about the Black Chamber during the War of the Spanish Succession and the
overview that was written later. In the article published in *The Historical Journal*, I put
much emphasis on the importance of Stadholder- King William III for the use of mail
interception and codebreaking as instruments in the struggle against Louis XIV. I still
believe that that is fundamentally true, but at the time I did not know that, in a way, Prince
William III used what was already there, because the Dutch had already been breaking
Spanish codes for over a hundred years. This only occurred to me when I did some
additional research for the overview. This brings me to a third point. The statements about
the sixteenth and seventeenth centuries to be found in the overview are
soley based on *printed* sources. Additional research in, for instance, the part of the Huygens correspondence that was not printed and that seems to be considerable, or the archives of Athanasius Kircher that used to be, until recently, under lock and key in a Vatican repository, may yield new insights still. I do not wish to leave the impression that the research about this period has been exhaustive. It has been more so for the 18th century proper, but one still has to bear in mind how scattered and fragmentary the material was that I had to work on. It may still be possible that something new will come up about people or systems we know nothing about as yet.

Finally, some errors that should be corrected. In the article about the War of the Spanish Succession (p. 138, footnote 18) a letter is quoted written by William III to Heinsius as CCLXXIX, 7 Feb. 1694 Kensington. This should be: CCCXXIII, 5/15 March 1695, Kensington. Secondly, D’Alonne’s second name is wrongly spelled as ‘Tassin’, whereas it should have been ‘Tassin’. As this name hardly ever occurs in contemporary documents related to him, this error of transcription escaped my attention until Dr. Veenendaal made me aware of it. Thirdly, on p. 152 of the same article I state that the exchange of intercepted letters between Hanover and The Hague was interrupted by Heinsius, because the Hanoverians found out too much about contacts between the Dutch and the Bavarians. I now think that it is more likely that this exchange was interrupted by the Hanoverians themselves, because they discovered that the information they made available for the Dutch had also reached the English. What is written in the article should be compared to what is written in the overview on page 38 (footnote xcvi). Fourthly, in the article about Princess Wilhelmina (p. 104) it is stated that Lyonet and Croiset introduced a two-part code with a substraction table for the Stadholder. I now believe, however, that this code may have been made by the same person who made the small bookcipher for Prince Frederick that was used as an example for the Hampton Court cipher, introduced by the Princess herself (quoted on p. 120, see also footnote 50 and 51 of the article about the bookcipher of Hampton Court). Fifthly, in the article about the homophonic substitution cipher by L.P. van de Spiegel, the Dutch title ‘Raadpensionaris’ is rendered in English as ‘Great Pensionary’ whereas in other articles the translation ‘Grand Pensionary’ is preferred which was more currently used at the time.