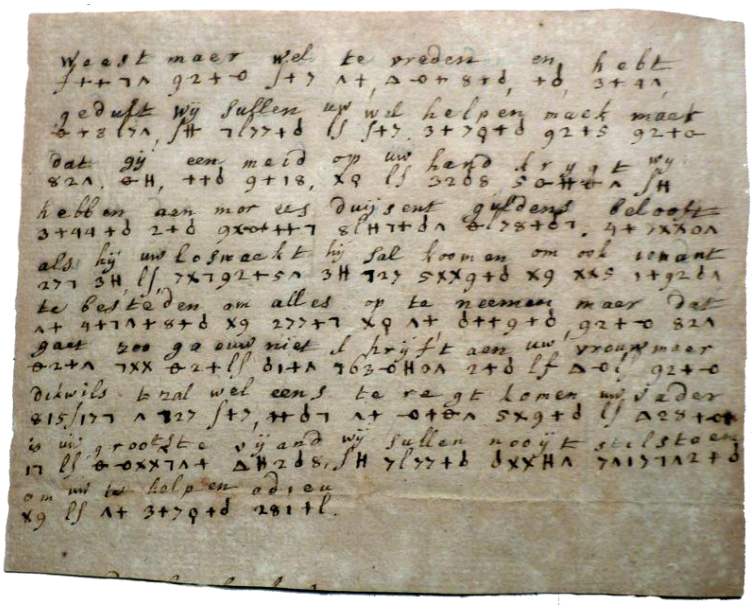
(ON)MISBAAR

HET ONDERSCHEPPEN EN ONTCIJFEREN VAN GEHEIME DIPLOMATIEKE CORRESPONDENTIE IN DE REPUBLIEK IN DE ACHTTIENDE EEUW.



21 januari 2011
Jan Willem Boer
post@janwillemboer.nl
studentnummer 9451781

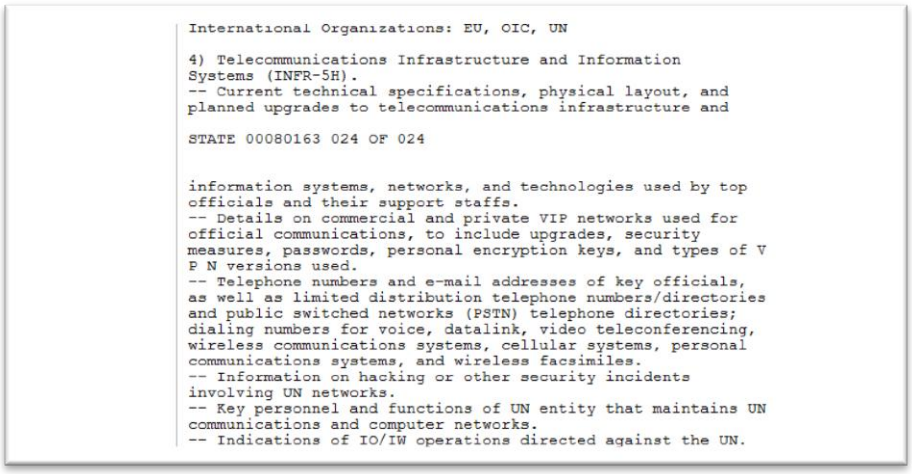
Scriptie voor de cursus Diplomatieke Praktijken (OS III)
Universiteit Utrecht, faculteit Geesteswetenschappen

INHOUD

Inleiding 2
1. Introductie in de cryptologie 5
1.1 Cryptografie 5
1.2 Cryptoanalyse 6
1.3 Historiografie van de cryptologie 8
2. Cryptologie tot en met de zeventiende eeuw 10
2.1 Europa 10
2.2 De Republiek 14
3. Institutionalisering: de achttiende eeuw 18
3.1 Europa 19
3.2 De Republiek 21
3.2.1 Onder Pierre Lyonet 22
3.2.2 Onder Samuel Egbert Croiset 27
Conclusie 30
Overzicht van geraadpleegde werken 33
Bronnen 33
Literatuurlijst 33
Anachronistische bijlage 34

INLEIDING

Eind 2010 deed de website WikiLeaks veel stof opwaaien door een begin te maken met het publiceren van 250.000 vertrouwelijke diplomatieke notities. In een van deze notities gaf de minister van buitenlandse zaken van de Verenigde Staten haar diplomaten instructie om van buitenlandse mogendheden de wachtwoorden, elektronische sleutels, gegevens over beveiligde communicatielijnen en dergelijke te achterhalen.[1]



International Organizations: EU, OIC, UN

4) Telecommunications Infrastructure and Information Systems (INFR-5H).
-- Current technical specifications, physical layout, and planned upgrades to telecommunications infrastructure and

STATE 00080163 024 OF 024

information systems, networks, and technologies used by top officials and their support staffs.
-- Details on commercial and private VIP networks used for official communications, to include upgrades, security measures, passwords, personal encryption keys, and types of V P N versions used.
-- Telephone numbers and e-mail addresses of key officials, as well as limited distribution telephone numbers/directories and public switched networks (PSTN) telephone directories; dialing numbers for voice, datalink, video teleconferencing, wireless communications systems, cellular systems, personal communications systems, and wireless facsimiles.
-- Information on hacking or other security incidents involving UN networks.
-- Key personnel and functions of UN entity that maintains UN communications and computer networks.
-- Indications of IO/IW operations directed against the UN.

Figuur 1 – de instructie om beveiligingsgegevens te achterhalen

De officiële internationale verontwaardiging die deze onthulling zou hebben kunnen oproepen, bleef uit. Een belangrijke reden hiervan zou kunnen zijn dat een dergelijke instructie de andere landen ook niet vreemd zal zijn geweest – nieuwsgierigheid naar de correspondentie van vreemde mogendheden is van alle landen, en van alle tijden. Juist om die reden is het beveiligen van gegevens tegen onbevoegde ogen ook van alle tijden, zij het met minder succes dan de beveiliging die in 2011 mogelijk is door geautomatiseerde encryptie.

In de vroegmoderne tijd, vanaf de vijftiende eeuw, werd Europa gekenmerkt door de transformatie van middeleeuwse feodaal georganiseerde vorstendommen naar moderne staten. Een onderdeel van deze transformatie was de opkomst van de diplomatie, die gepaard ging met kenmerken die nu als modern geclassificeerd kunnen worden, zoals de permanente vertegenwoordiging, het alleenrecht van een soeverein op het sturen van diplomaten en de toenemende communicatie tussen de diplomaat en het thuisland. Aan de hand van deze kenmerken is het mogelijk te meten hoe modern of traditioneel een bepaalde staat was. Het doel hiervan is niet om staten te kwalificeren, maar het biedt een handvat voor het onderzoek naar de toestand van de diplomatie in die staat.

[1] http://www.guardian.co.uk/world/us-embassy-cables-documents/219058, voorlaatste alinea.

Een van de kenmerken die samenging met de opkomst van moderne diplomatie, was het toenemen van communicatie tussen staten. Van diplomaten in den vreemde werd verwacht dat ze veel en vaak rapporteerden over de toestand aan het hof waar ze dienden. Het valt te begrijpen dat ook het gastland een levendige belangstelling voor deze correspondentie aan de dag legde, zodat er in toenemende mate mechanismen ontstonden om de deze te onderscheppen. Zo was het niet ongebruikelijk dat diplomatieke koeriers onderweg simpelweg beroofd werden van hun post. Er werden middelen aangewend om het transport te beveiligen, maar omdat dit moeilijk en duur was, werd er meer aandacht besteed aan het onleesbaar maken van de inhoud van de post. Als de correspondentie onderschept werd, dan konden de onbevoegde ogen de inhoud ervan niet begrijpen. Dit gebeurde door middel van geheimschriften, cryptografie.[2] Hand in hand met de opkomst van de cryptografie ontwikkelde zich de tegenhanger hiervan, de cryptoanalyse. De cijferschriften waren meestal met een combinatie van wiskundige en taalkundige analyse, stukjes bekende tekst, en wat geluk te ontcijferen zonder dat men hiervoor de sleutel had. Met het ingewikkelder worden van de geheimschriften werd de ontcijferkunst ook beter, en omdat het vaak dezelfde personen waren die geheimschriften maakten en kraakten, was dit een ontwikkeling die zichzelf in stand hield. Vanaf de zestiende eeuw waren er in de belangrijkere staten vaak fulltime cryptoanalisten in dienst van een minister van buitenlandse zaken.[3]

Omdat de toenemende communicatie tot gevolg had dat er meer gebruik werd gemaakt van cryptologie, kan de opkomst en professionalisering van deze beroepsgroep, die in verschillende staten plaatsvond, gezien worden als een onderdeel van de modernisering van de diplomatie in Europa.

Een van de staten die zich in de vroegmoderne tijd ontwikkelde was de Republiek der Zeven Verenigde Nederlanden, die zich vanaf de Vrede van Münster in 1648 mocht verheugen in de officiële erkenning door de omringende landen. Deze scriptie probeert een onderdeel van de modernisering van de diplomatie in de Republiek zichtbaar te maken, door te laten zien hoe de Republiek in de vroegmoderne tijd omging met briefgeheim en cryptologie. De vraag die deze scriptie probeert te beantwoorden luidt: hoe heeft de cryptologie zich in de vroegmoderne tijd in de Republiek ontwikkeld?

[2] M.S. Anderson, *The rise of modern diplomacy 1450-1919* (New York 2001) 22
[3] *ibidem* 44

Om de vraag goed te kunnen beantwoorden, moet de vraag opgesplitst worden in een aantal deelvragen waarmee de context geschetst kan worden en waarmee het onderwerp in detail benaderd kan worden.

- Wat houdt cryptologie in?
- Hoe ontwikkelde de cryptologie zich in Europa?
- In hoeverre was er in de Republiek sprake van professionalisering van een beroepsgroep rondom de cryptologie, zoals in andere Europese landen gebeurde?

Vanwege de beschikbaarheid van materiaal en bronnen besteedt deze scriptie voor de Nederlandse situatie extra aandacht aan de achttiende eeuw.

Voor de helderheid van het betoog is het nodig eerst een korte introductie te geven in de cryptologie en de geschiedenis ervan. De cryptologie heeft een eigen jargon waar de lezer die zich in het onderwerp verdiept, al snel mee geconfronteerd wordt. In het eerste hoofdstuk wordt een korte inleiding gegeven om het gebruikte jargon te introduceren en inzicht te geven in het werk van de cryptologen. In de hoofdtukken daarna wordt in twee delen een overzicht gegeven van de ontwikkeling van de cryptologie in Europa en wordt per periode de ontwikkeling in de Republiek hiermee vergeleken.

1. INTRODUCTIE IN DE CRYPTOLOGIE

Cryptologie wordt in de context van dit betoog gebruikt als verzamelnaam voor cryptografie en cryptoanalyse. Deze twee begrippen worden hieronder verder uitgewerkt. Hierbij dient te worden opgemerkt dat deze paragraaf uitgaat van de cryptologie zoals die in de vroegmoderne tijd gold. Door de opkomst van de computer in de twintigste eeuw heeft cryptologie vanaf de zeventiger jaren van die eeuw een totaal ander karakter gekregen.[4] Hierover in een bijlage meer.

1.1 CRYPTOGRAFIE

Cryptografie wordt toegepast om informatie veilig tussen twee partijen te kunnen uitwisselen zonder dat derden over de informatie kunnen beschikken. Cryptografie lost het probleem op dat ontstaat als het transportmedium waarover de communicatie loopt, onveilig is. Als derden de communicatie kunnen onderscheppen, zorgt cryptografie ervoor dat de informatie die ze in handen krijgen, onleesbaar is.

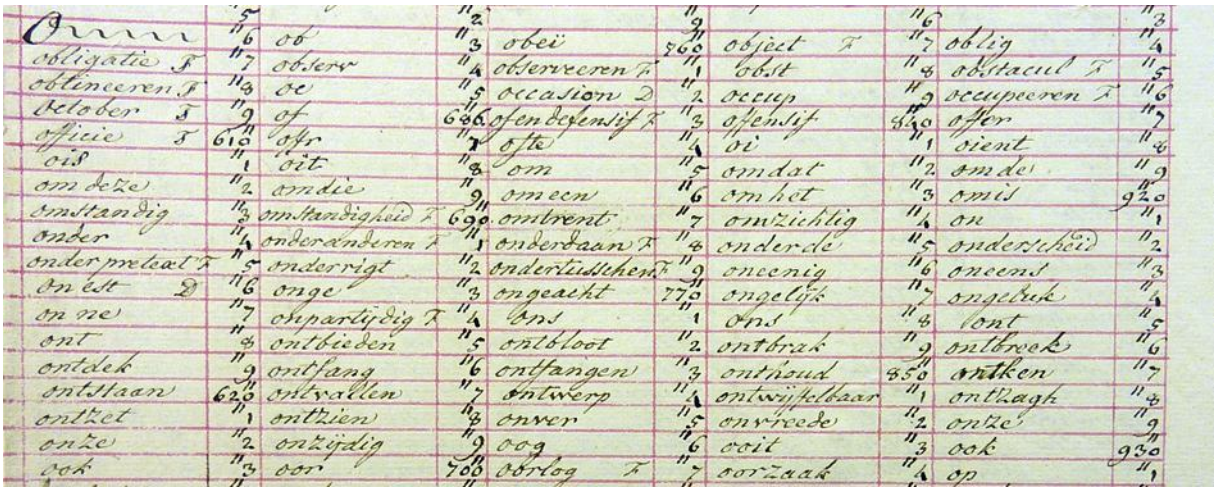
Cryptografie is het omzetten van teksten in geheimschrift of het terugvertalen van het geheimschrift naar de oorspronkelijke tekst. Het omzetten van de tekst heet het versleutelen of in cijfer zetten van de tekst, het terugvertalen het ontcijferen. Er zijn hoofdzakelijk twee manieren om een tekst te versleutelen. Ten eerste met behulp van een code en ten tweede middels een substitutiealfabet.

Een code is een lijst met namen en woorden waar codecijfers of codewoorden tegenover staan. Een tekst wordt gecodeerd door elk woord van de tekst in de codelijst op te zoeken en te vervangen door het corresponderende codewoord of codecijfer. Het ontcijferen van de tekst gebeurt door de lijst in de andere richting te gebruiken. Bij een code is het woord de atomaire eenheid waarmee wordt gewerkt.

Het versleutelen van een tekst met een substitutiealfabet houdt in dat de letters in de tekst de atomaire eenheid zijn waarmee de cryptograaf werkt. Een substitutiealfabet is een lijst met letters waar elke letter wordt vervangen door een andere letter. De eenvoudigste vorm hiervan is een monoalfabetisch substitutiealfabet, waarbij elke letter door één andere letter of teken wordt vervangen. Meer veiligheid bieden de polyalfabetische substitutievarianten. Hierbij wordt een bepaalde letter volgens een bepaald systeem door meerdere letters of tekens vervangen. Omdat de individuele letters de atomaire eenheid vormen, zijn substitutiegeheimschriften taal-agnostisch, en dus breder toepasbaar dan codelijsten.

[4] Vgl. S. Singh, *The code book. The secret history of codes and codebreaking* (Londen 2000) 243-316.

In de praktijk kunnen codering en substitutie door elkaar worden gebruikt. Een deel van de tekst wordt bijvoorbeeld gecodeerd en een ander deel gesubstitueerd. Een andere variant is dat de tekst eerst wordt gecodeerd en vervolgens extra beveiligd door de gecodeerde tekst te substitueren.



Figuur 2 - een nederlandse codelijst uit de achttiende eeuw

Om een geheimschrift te kunnen uitwisselen, maken de verzendende en ontvangende partij een afspraak over de gebruikte methode van codering of substitutie. Deze afspraak wordt de sleutel genoemd. Deze sleutel is altijd de achilleshiel van de cryptografie geweest. Voordat twee partijen veilig gegevens kunnen uitwisselen, zijn ze eerst genoodzaakt de sleutel uit te wisselen via een onveilig kanaal. De enige veilige oplossing is om de sleutel – vaak in de vorm van uitgebreide codeboeken – persoonlijk te overhandigen.

In de vroegmoderne tijd werd er over de theorie van de cryptologie veel gepubliceerd. De veiligere systemen waren meestal een complex stelsel van op substitutie gebaseerde algoritmen. In praktijk was dit voor de meeste diplomaten veel te ingewikkeld. Men gebruikte dan ook meestal alleen het systeem van de codelijsten of een simpele monoalfabetische substitutie.[5]

1.2 CRYPTOANALYSE

Als de ontvanger van een geheimschrift de sleutel daarvan in zijn bezit heeft, kan hij de boodschap op eenvoudige wijze ontcijferen. Soms gebeurt het echter dat er partijen zijn die wel het geheimschrift in handen hebben, maar niet de sleutel. Als deze partijen de oorspronkelijke tekst willen achterhalen, dan zullen ze van andere methoden gebruik moeten maken om de tekst leesbaar te maken. De wetenschap die zich hiermee bezig houdt, is de cryptoanalyse.

[5] David Kahn, *The codebreakers. The story of secret writing* (New York 1967) 150

Een cryptoanalist probeert vanuit een geheimschrift de oorspronkelijke tekst te reconstrueren zonder dat hij over de sleutel beschikt. Om dit te doen heeft hij verschillende methoden tot zijn beschikking.

Met statistische tekstanalyse kan hij in kaart brengen welke patronen de letters, lettercombinaties en woorden volgen. Als hij de taal van de oorspronkelijke tekst kent, is het mogelijk deze frequentietabellen te vergelijken met de frequentietabellen die gebruikelijk zijn bij die taal. Op die manier kan hij triviale delen van de tekst reconstrueren en de gevonden patronen extrapoleren naar de minder triviale gedeelten van de tekst. Verder kan de cryptoanalist naar herhalende patronen zoeken, die bepaalde veelvoorkomende fragmenten kunnen verraden.

Een bijzonder belangrijk instrument tot het ontcijferen van teksten zonder dat de cryptoanalist de sleutel daarvan heeft zijn de zogenaamde *cribs*, stukken tekst die zowel als de oorspronkelijke tekst als in versleutelde variant bekend zijn. Als bijvoorbeeld bekend is wie de verzendende en ontvangende partij zijn, is makkelijk te raden wat de beleefdheidsfrasen zijn waarmee een brief begint en afgesloten wordt. Opnieuw kan de cryptoanalist op die manier met triviale gedeelten de minder triviale gedeelten proberen te achterhalen.

Verder gebeurt het vaak dat complete teksten na enige tijd via andere kanalen verkregen kunnen worden. De noodzaak voor cryptoanalyse is dan natuurlijk weggenomen, maar de complete vertaling van een tekst kan zeer behulpzaam zijn bij het ontcijferen van een volgende tekst die volgens het zelfde systeem in geheimschrift is gesteld.

1.3 HISTORIOGRAFIE VAN DE CRYPTOLOGIE

Het belangrijkste werk over de geschiedenis van de cryptologie is het boek van David Kahn, *The Codebreakers*, voor het eerst gepubliceerd in 1967. Het is een boek dat veel invloed heeft gehad op de historiografie van de cryptologie. Het is bijzonder volledig, grondig en gedetailleerd, en daardoor het standaardwerk over de geschiedenis van de cryptologie. Omdat het een goed geschreven, soms zelfs spannend boek is, en de onderwerpen tot de verbeelding spreken, heeft het boek ook in de populaire beeldvorming over cryptologie in belangrijke mate bijgedragen.[6] Er moeten echter wel twee kanttekeningen bij dit boek geplaatst worden.

In de eerste plaats stelt Kahn dat de ontwikkeling van de cryptologie in de Middeleeuwen heeft stilgestaan en dat de antieke kennis van cryptologie verloren is gegaan en tijdens de Renaissance is herontdekt.[7] Maar blijkens de woordkeuze is Kahn van een school historici die van de Middeleeuwen spreekt als "The Dark Ages". Als een auteur op deze manier over de Middeleeuwen spreekt doet dit het vermoeden rijzen van een vooringenomen manier van geschiedschrijving. Het is dus belangrijk om dit in het achterhoofd te houden.

In de tweede plaats is het Kahn er zeker niet om te doen om zijn vaderland, de Verenigde Staten van Amerika, in een ongunstig daglicht te stellen. Dit is bijvoorbeeld af te leiden uit de eufemismen die hij debiteert over de ontwikkeling van de vroege Amerikaanse cryptologie. Uit zijn beschrijving is op te maken dat dit vooral het werk van amateurs was, die met eenvoudige, achterhaalde geheimschriften werkten. Kahn typeert de ontwikkeling echter als volgt: "[In America] cryptology reflected the free, individualistic nature of the people from which it sprang[8]". Het is niet bijzonder belangrijk voor het onderwerp van deze scriptie, maar toch het vermelden waard.

Uitgezonderd het noemen van Philips van Marnix van Sint Aldegonde gaat het boek van Kahn niet op de Nederlandse situatie in.

Na Kahn is er niet opnieuw een standaardwerk in die orde van grootte of met vergelijkbare invloed verschenen. Het onderwerp is wel aan een update toe, omdat de cryptologie vanaf het computertijdperk zo ingrijpend is veranderd. Als kandidaten hiervoor zouden de volgende twee boeken in aanmerking kunnen komen.

---

[6] Alle artikelen in Wikipedia die met dit onderwerp te maken hebben, en veel boeken over cryptologie verwijzen naar Kahn als hun eerste informatiebron.
[7] David Kahn, *The codebreakers,* 89
[8] *ibidem*, 174

In 2007 is er een handboek verschenen onder redactie van Karl de Leeuw en Jan Bergstra, getiteld *The history of information security*, dat zowel op de recente geschiedenis ingaat als op de geschiedenis van de vroegmoderne tijd. Voor het onderwerp van deze scriptie is het werk van De Leeuw zelf belangrijk. Hij heeft met gebruikmaking van primaire bronnen uitgebreid onderzoek gedaan naar de Nederlandse situatie. Hij concentreert zich vooral op de door de Republiek en haar machthebbers gebruikte geheimschriften, maar beschrijft ook de activiteiten van de verschillende cryptoanalisten die de Republiek heeft gekend.

Een werk dat ook het noemen waard is, is een populairwetenschappelijk werk van Simon Singh dat in 1999 verschenen is, *The Code Book*. "The evolution of Secrecy from Mary, queen of Scots to quantum cryptography" was de ondertitel bij eerste publicatie, maar later is die veranderd naar het wat populairdere "the secret history of codes and code-breaking". Voor een groot deel is ook in dit boek de lijn van Kahn te ontdekken, maar Singh gaat gedetailleerder dan Kahn op bepaalde punten in en probeert op die manier vooral een instructief boek te schrijven over zowel de geschiedenis als de praktijk van de cryptologie, en hij breidt het overzicht uit naar het computertijdperk. Een opmerkelijk onderdeel van zijn verhaal is een serie opgaven die hij in een bijlage heeft gepubliceerd. Hij loofde bij het uitkomen van het boek 10.000 Britse pond uit aan de eerste die de codes van alle opgaven zou kunnen kraken. Dit is ongeveer een jaar later gebeurd na een inspanning door duizenden mensen over de hele wereld.[9] Het belang van het boek om het onderwerp bekendheid te geven moet dus niet onderschat worden. Het boek van Singh geeft verder een goed inzicht in de manier waarop cryptoanalisten te werk gaan.

[9] Singh geeft op zijn website een verslag, http://www.simonsingh.net/Cipher_Challenge.html. De winnende groep, een stel wetenschappers uit Zweden, heeft zijn bevindingen en de oplossingen uitgebreid gedocumenteerd op http://codebook.org/codebook_solution.html

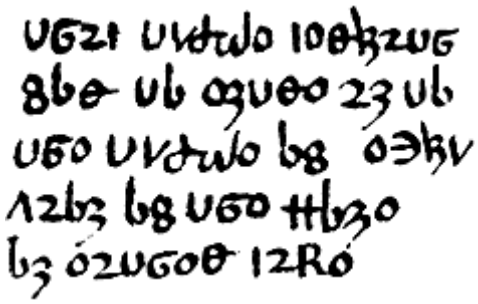
2. CRYPTOLOGIE TOT EN MET DE ZEVENTIENDE EEUW

2.1 EUROPA

De geschiedenis van de cryptologie is geen exclusief Europese aangelegenheid. In de Indische en Arabische geschiedenis is al vroeg ver-ontwikkelde cryptologische kennis aanwezig.[10] Deze paragraaf beperkt zich echter tot de geschiedenis van de cryptologie in Europa. Ruwweg ontwikkelde die zich zelfstandig zonder invloed van andere beschavingen.[11]

Bij het ontstaan van het schrift zal in het begin het kunnen lezen en schrijven zo zeldzaam zijn geweest, dat het überhaupt op schrift stellen van een tekst al geheimschrift genoeg was.[12] Maar naarmate de geletterdheid vorderde, werd de behoefte aan geheimhouding groter. In de oudheid ontwikkelden zich gaandeweg diverse soorten geheimtaal. De bekendste hiervan is het substitutiealfabet dat Caesar gebruikte om zijn boodschappen in te versleutelen. Dit geheimschrift, dat nog steeds het Caesarcijfer of de Caesarrotatie wordt genoemd, hield in dat elke letter van de tekst vervangen werd door een letter die een vastgesteld aantal letters verderop in het alfabet stond.

Volgens Kahn is er tijdens de middeleeuwen niet veel over cryptografie gepubliceerd en lijkt er weinig behoefte aan het gebruik er van te zijn geweest. Er zijn monniken geweest die teksten met een substitutiealfabet versleutelden. Het lijkt er op dat het gebruik van dit geheimschrift geen enkel doel diende dan persoonlijke interesse of vermaak.[13] Een bekend cryptogram uit die tijd is terug te vinden in een werk dat toegeschreven wordt aan Geoffrey Chaucer.



Figuur 3 - Een versleuteld stuk tekst, mogelijk van Chaucer[14]

[10] Kahn, *The codebreakers,* 95
[11] *Ibidem,*108
[12] *Ibidem*, 87
[13] *Ibidem*, 89
[14] *The equatorie of the planetis*. Het werk is toen het gevonden werd, toegeschreven aan Chaucer, maar tegenwoordig wordt dit betwijfeld. Vgl Jennifer Arch, A case against Chaucer's authorship of the equatorie of the planetis, *The Chaucer review volume 40*, 1 (2005) 59-79 en Kari Anne Rand Schmidt, *The authorship of the equatorie of the planetis* (Cambridge 1993).

Door het weinige gebruik van cryptografie en doordat de aard van dit gebruik vooral op persoonlijke interesse gebaseerd was, is er aan het kraken van codes via cryptoanalyse waarschijnlijk weinig behoefte geweest.

Een oorzaak voor de kleine rol van cryptografie in de Middeleeuwen is geweest dat cryptologie omgeven was door een waas van geheimzinnigheid.[15] Religieuze en magische groepen behoorden vaak tot de eersten die hun tradities op schrift stelden en later hun geheime rituelen in geheimschriften vastlegden. Verder maakten alchemisten en astrologen gebruik van tekens en symbolen om hun kennis mee te noteren. Hoewel dit laatste niet bedoeld was om de inhoud te verhullen, zal het op leken een geheimzinnige indruk hebben gemaakt. De occulte waas die deze wetenschappen omhulde, straalde op die manier als vanzelf af op de cryptografie.[16] In de huidige populaire literatuur wordt cryptologie nog steeds geassocieerd met religie en geheime occulte rituelen. Een recent voorbeeld hiervan is *The Da Vinci code* van Dan Brown.

Dat er weinig informatie over cryptologie in de Middeleeuwen beschikbaar is, kan ook komen door de beperkte aandacht die Kahn hieraan in zijn invloedrijke werk heeft gegeven. In andere werken wordt het onderwerp meestal compleet genegeerd. Het zou de moeite waard zijn om over cryptologie in de Middeleeuwen meer onderzoek te doen.

Aan het eind van de veertiende eeuw werd de basis gelegd voor wat eeuwen de standaard voor de cryptografie zou blijven. Lavinde, secretaris voor de anti-paus Clements VII, introduceerde in 1379 voor de correspondenten van de paus een geheimschrift dat een combinatie van een substitutiealfabet en een verzameling codes was, waarin vooral de namen waren gecodeerd. Deze lijsten werden nomenclaturen genoemd. Waar de nomenclatuur in het begin nog een kort lijstje met enkele namen was, werden de lijsten vanaf 1400 ingewikkelder en uitgebreider, waaruit blijkt dat de makers ervan op de hoogte moesten zijn geweest van pogingen tot cryptoanalyse.[17]

Gedurende de zestiende eeuw nam door de toename van de diplomatieke activiteit ook de behoefte aan communicatie en aan beveiliging van die communicatie toe.[18] Bij de meeste staten werd een trend zichtbaar dat de machthebbers structureel met één of meer cryptologen in verbinding stonden. De cryptoloog kreeg in het begin incidenteel een opdracht om een brief “te vertalen”, maar als de opdrachtgever ontdekte hoe waardevol deze bron voor hem was, nam het aantal opdrachten toe. Cryptologen in dienst van een staat probeerden niet alleen de correspondentie van andere staten te ontcijferen, maar zorgden er ook voor dat de codes die

[15] Anderson, *The rise of modern diplomacy*, 22
[16] Kahn, *The codebreakers,* 91-92
[17] *Ibidem*, 107
[18] Anderson*, The rise of modern diplomacy,* 21

door de eigen diplomaten werden gebruikt, aan de eisen des tijds voldeden. In de zestiende eeuw werd de toegankelijkheid van kennis over cryptologie beter, omdat er boeken en traktaten over het onderwerp verschenen.[19] Dat moet betekend hebben dat de cryptologie veranderde in een voortdurend achterhaalde wetenschap. Immers, het publiceren over de geheime methoden maakte deze direct kwetsbaar, omdat een groot deel van de geheimhouding juist in de geheimhouding van de methode lag. Gedurende de zestiende en zeventiende eeuw kwam de ontwikkeling van de cryptologie dan ook in een stroomversnelling waarbij de codes steeds ingewikkelder werden en het ontcijferen van correspondentie steeds vaker werd geprobeerd.

Aan het einde van de zestiende eeuw hadden de belangrijke staten in Europa vaste cryptologen in dienst, die de nomenclaturen van hun diplomaten verzorgden en daarnaast van onschatbare waarde bleken voor de informatievoorziening, doordat ze de geheime correspondentie van vriend en vijand konden ontcijferen. In Engeland maakte een cryptoanalist bijvoorbeeld mogelijk dat het Babington complot ontmaskerd kon worden. Mary Stuart, de belanghebbende in het complot, werd veroordeeld op basis van uitlatingen die zij in gecodeerde brieven had gedaan, die echter in handen waren gevallen van Walsingham, de rechterhand van Elisabeth I, tegen wie het complot was gericht. Mary werd veroordeeld en geëxecuteerd.[20]

François Viète, vooral bekend geworden om zijn wiskundige publicaties, timmerde in Frankrijk op het gebied van cryptoanalyse aan de weg. Ten tijde van de godsdienstoorlogen onder Hendrik III en Hendrik IV wist hij de Spaanse nomenclaturen te kraken, die voor een groot deel door Philips II zelf waren opgesteld. Die klaagde dan ook bij de paus dat de Fransen hiervoor zwarte magie moesten hebben gebruikt.[21]

Een andere cryptoanalist die Spaanse codes wist te ontcijferen, was Philips van Marnix van Sint Aldegonde, die van tijd tot tijd zijn diensten op dit gebied aan Willem van Oranje verleende. Een van de belangrijkste wapenfeiten hierbij is geweest dat het tweetal op deze manier de plannen van Don Juan kon verijdelen, die met Mary wilde trouwen en Elisabeth van de troon wilde stoten.[22] Niet iedereen gelooft in de kundigheid van de baron op dit gebied. Hij zou een Spaanse medewerker hebben omgekocht en de codeboeken van hem hebben gekregen. Om zijn bron te beschermen kon Marnix niet anders dan veinzen alsof hij zelf de

Figuur 4 - Philips van Marnix van Sint Aldegonde

[19] Kahn, *The codebreakers,* 110
[20] Singh, *The code book,* 32-44
[21] *Ibidem*, 28
[22] Kahn, *The codebreakers,* 120

brieven had ontcijferd.[23] Desondanks heeft hij ook Portugese brieven kunnen vertalen en brieven van verschillende personen, die vaak niet dezelfde nomenclaturen gebruikten.[24] Het een sluit het ander niet uit.

Scepsis over het nut van cryptografie en cryptoanalyse was er ook. François Callières, schrijver en diplomaat, was bijvoorbeeld van mening dat cryptoanalisten alleen succes konden hebben omdat de geheimschriften zwak waren, en de diplomaten knoeiers in het gebruik ervan. Hij heeft hierin gedeeltelijk gelijk. Er werd bezuinigd op het maken van nieuwe geheimschriften terwijl van de oude al bekend was dat ze gebroken waren. Voor het gemak werd door de beleidsmakers aangenomen dat het onmogelijk was hun codes te breken en dat er, voordat dat zou gebeuren, magie aan te pas zou moeten komen.[25] Een ander zwak punt waren diplomatieke berichten, in code verstuurd, waarvan de inhoud aan het gastland meegedeeld moest worden. Na ontcijfering van het ingekomen bericht stuurden de diplomaten het bericht vaak grotendeels ongewijzigd naar het hof, waarmee ze de cryptoanalisten onbedoeld van waardevolle *cribs* voorzagen.

Een bekende scepticus is Voltaire geweest, die botweg weigerde te geloven dat cryptoanalyse mogelijk was, en cryptologen gelijk stelde aan charlatans die het slecht geïnformeerde publiek een rad voor ogen draaiden.[26] Dichter bij huis, maar om een andere reden, was Johan de Witt niet van het nut van goede cryptografie overtuigd. Wat voor code men ook zou verzinnen, hij zou toch gekraakt worden.[27]

Verder moet opgemerkt worden dat de theorievorming over cryptografie ver vooruit liep op de praktijk. Er waren al in de zestiende eeuw systemen bedacht die een stuk veiliger waren dan de nomenclaturen (codelijsten), die echter tot in de negentiende eeuw in gebruik bleven. De oorzaak hiervan is waarschijnlijk het gemak geweest dat een codelijst van woorden met zich meebracht in vergelijking met het letter voor letter volgens een ingewikkeld algoritme moeten coderen van de boodschap.[28]

De periode tot en met het begin van de zeventiende eeuw zag dus de opkomst van de cryptologie in het maken en breken van geheimschriften, twee toepassingen die elkaar over en weer beïnvloedden. Het niet meedoen aan deze ontwikkeling betekende dus automatisch een achterstand. Aan de Republiek ging deze ontwikkeling echter grotendeels voorbij, zoals in de volgende paragraaf duidelijk zal worden.

---

[23] Karl de Leeuw, *Cryptology and statecraft in the Dutch Republic,* (Amsterdam 2000) 13
[24] Kahn, *The codebreakers,* 120
[25] *Ibidem,* 173-174
[26] Voltaire, *Dictionnaire Philosophique*, (Paris 1838) 798
[27] De Leeuw, *Cryptology and statecraft,* 16
[28] Kahn, *The codebreakers,* 150

2.2 DE REPUBLIEK

De geschiedenis van de cryptologie in de Republiek valt in drie delen uiteen. Ten eerste de periode van de Opstand, voor 1650, ten tweede de periode van 1650 tot 1750, waarin de Republiek een officieel erkende staat was, en tenslotte de periode van 1750 tot ongeveer 1810, de nadagen van de Republiek.[29]

In de periode voor 1650, de tijd van de Opstand, maakte de Republiek gebruik van eenvoudige geheimschriften. De communicatielijnen die in gebruik waren, waren kort, en veel diplomatieke betrekkingen waren er nog niet, dus de mogelijkheden van de Spanjaarden om de post te onderscheppen waren beperkt.[30] Wel werden er pogingen gedaan de Spaanse codes te kraken. Er is weinig over deze periode bekend, maar het is duidelijk dat er drie personen waren die zich met cryptoanalyse voor de Republiek hebben beziggehouden, te weten Philips van Marnix van Sint Aldegonde, hierboven al genoemd, Jacques Aleaume, een Franse wiskundige die door Viète was opgeleid[31] en die onder Oldenbarnevelt geheimschriften ontcijferde, en Constantijn Huygens, die vooral na het twaalfjarig bestand actief was.

Ook toen de eerste diplomaten naar het buitenland werden gezonden, werd er van buitengewoon makkelijk te kraken codes gebruik gemaakt. Het lijkt dus onwaarschijnlijk dat de vroege cryptoanalisten van de Republiek betrokken zijn geweest bij het samenstellen van de procedures voor de cryptografie.[32]

Een tekenend geval is terug te vinden in de besluiten van de Staten Generaal. In juli 1626 kwam de stalmeester van Frederik Hendrik bij de Staten Generaal met een zelfbedacht geheimschrift waarvan hij dacht dat het nuttig zou zijn deze ter beschikking van de Republiek te stellen. Het is een “uit verschillende tekens samengesteld geheimschrift dat correspondeert met het alfabet”. Dit houdt in dat het een substitutiealfabet was, een van de makkelijkst te kraken soorten geheimschrift. De Staten Generaal liet een onderzoek naar het geheimschrift doen door de leden Schagen en Nieupoort, respectievelijk schout van Alkmaar en burgemeester van Utrecht. Later die maand is het geheimschrift waarschijnlijk in gebruik genomen voor de correspondentie van François van Aarssen, Heer van Sommelsdijk, ambassadeur extraordinaris naar Frankrijk. De stalmeester, van wie weinig meer bekend is dan dat hij Du Champs heette, kreeg een gouden ketting ter waarde van 600 gulden.[33] Dat de “uitvinding” van zo’n verouderd en weinig

[29] De Leeuw, *Cryptology and statecraft, 1-2*
[30] *Ibidem,* 12
[31] P.C. Molhuysen en P.J. Blok (ed.), *Nieuw Nederlandsch biografisch woordenboek. Deel 2,* (Leiden 1912) 17-18
[32] De Leeuw, *Cryptology and statecraft,* 16
[33] Besluiten Staten Generaal 1626-1630, inghist.nl, afschriften van 1626: 18 juli, nr. 1, 21 juli, nr. 11, 27 juli, nr. 5 en 29 juli, nr. 10.

bescherming biedend geheimschrift als zo waardevol werd beloond is een haast onwaarschijnlijke gebeurtenis.

Resumerend was er in de periode rond 1600 in de Republiek dus weinig te merken van professionele cryptografie vanwege het ontbreken van de beïnvloeding door de cryptoanalisten zoals die in andere landen wel plaatsvond. De codes waren eenvoudig en het zal de meeste buitenlandse cryptoanalisten weinig hoofdbrekens hebben gekost om de Nederlandse codes te kraken. De afwezigheid van goede codes kan waarschijnlijk verklaard worden uit de speciale positie die de Republiek innam: het land was klein, zodat communicatielijnen kort waren, en de regering van het land was nog jong en had vanwege het ontbreken van internationale erkenning nog weinig diplomaten. Er was dus vooralsnog vanuit de overheidsinstellingen van de Republiek weinig behoefte aan gedegen cryptografie.

Op het gebied van de cryptoanalyse daarentegen maakte de Republiek in deze periode een ontwikkeling door die vergelijkbaar was met die in andere staten. Er waren cryptoanalisten verbonden aan de machthebbers, die in het begin op afroep beschikbaar waren, maar gaandeweg officiëlere status kregen. De eerder genoemde Jacques Aleaume werd door de Staten-Generaal in dienst genomen als "deciffreur" tegen een vergoeding van zeshonderd gulden, maar al een half jaar daarna werd zijn vergoeding, waarschijnlijk op zijn eigen verzoek, verhoogd naar duizend gulden, met de mededeling dat, als hij dat nog niet genoeg vond, "men op een kleyncke nyet en sal sien", zodat een paar dagen later zijn vergoeding naar twaalfhonderd gulden werd verhoogd.[34] Of zijn aanstelling daarna veel praktisch nut voor de Staten-Generaal opleverde valt te betwijfelen, want kort daarop verhuisde hij naar Parijs. Desondanks is het duidelijk dat de Republiek in deze periode enkele gerenommeerde personen employeerde voor het ontcijferen van de vijandelijke codes.

Na 1650

In de periode waarin de Republiek officieel erkend werd door de andere mogendheden, de periode na 1650, en er dus ook meer diplomatie werd bedreven, besteedden de Staten-Generaal meer aandacht aan het beveiligen van de correspondentie. Elke diplomaat kreeg standaard een codeboek mee dat hij geacht werd te gelegener tijd te gebruiken. Deze codeboeken maakten gebruik van een veilig systeem: het had enorme codelijsten en was volgens de regelen der kunst opgesteld. De veiligheid werd echter in gevaar gebracht doordat het systeem daarna honderd jaar ongewijzigd in gebruik is geweest.[35] Dit moet betekenen dat de Republiek zeker negentig jaar zonder goed geheimschrift heeft gecorrespondeerd – dat is dan nog een voorzichtige

[34] P.C. Molhuysen, *Nieuw Nederlandsch biografisch woordenboek. Deel 2,* 17-18
[35] De Leeuw, *Cryptology and statecraft*, 2

schatting als men bedenkt dat de meeste geheimschriften binnen een jaar gekraakt konden worden. Wie de lijsten heeft opgesteld is niet duidelijk, maar het moet iemand geweest zijn die met de stand van zaken van dit onderwerp op de hoogte was. Na het opstellen van de lijsten hield zijn bemoeienis ermee blijkbaar ook op.

Waar er in de periode voor 1650 al weinig kruisbestuiving tussen cryptoanalyse en cryptografie was, werd dat in deze periode nog minder waarschijnlijk. De cryptoanalisten die hun diensten aan de machthebbers van de Republiek verleenden, kwamen uit het buitenland.

Willem III maakte voor het ontcijferen van onderschepte correspondentie veel gebruik van de diensten van de Engelse cryptoanalist Wallis. Verder had hij vriendschappelijke betrekkingen met Celle (Hannover), wat een belangrijk knooppunt was van het diplomatieke briefverkeer van Frankrijk naar Noord-Europa. Daar werd alle post gekopieerd, ontcijferd, en in gevallen waar men dat nodig achtte, ter beschikking gesteld van Willem III. Omstreeks 1700 kwam er een kink in deze kabel. Door een conflict tussen twee Franse postmeesters ontstond er een nieuwe route voor het Franse diplomatieke verkeer, waardoor Celle zijn taak als doorvoerstation voor een groot deel verloor.[36] Omdat Brussel en Amsterdam deze taak overnamen, besloot raadpensionaris Heinsius tot het onderscheppen van de post in verschillende Amsterdamse postkantoren en legde hij contacten met het postkantoor in Brussel waarvan hij regelmatig kopieën kreeg doorgestuurd. De onderschepte brieven werden vervolgens ter ontcijfering aan Hannover aangeboden.[37]

Heinsius had een privé secretaris in dienst, Abel Tasien d'Alonne, volgens hardnekkige geruchten een onwettige zoon van stadhouder Willem II. Door de vondst van cryptoanalytische aantekeningen en het vergelijken van handschriften is gebleken dat hij cryptoanalytisch werk voor Heinsius verrichtte.[38] Dit is blijkbaar geheim gehouden. Een verklaring hiervoor zou kunnen zijn dat zijn werk geheim werd gehouden uit angst voor het uitlekken van de informatie, wat door de structuur van de Republiek zeker niet ondenkbaar was en wat ook irritatie bij Hannover had gegeven.[39] Vanaf de mislukte onderhandelingen in Geertruidenberg in 1710 bekoelde de relatie met Hannover definitief en werd er geen gebruik van elkaars diensten meer gemaakt.[40]

In de periode na 1650 lijkt het alsof de cryptologie in de Republiek in vergelijking met andere landen en in vergelijking met de periode daarvoor op een wat lager pitje kwam. Hoewel er een

[36] De Leeuw, *Cryptology and statecraft,* 59-60
[37] *Ibidem,* 65-66
[38] A.J. Veenendaal jr*, Inventaris van het archief van Anthonie Heinsius, raadpensionaris van Holland en West-Friesland, (1682) 1689-1720* (Den Haag 2001) 12
[39] De Leeuw, *Cryptology and statecraft,* 23 en 65
[40] *Ibidem,* 71

goed begin gemaakt werd met naar verhouding gedegen codelijsten, werd deze ontwikkeling niet doorgezet. De geheimschriften kregen dus niet de aandacht die ze vanwege de voortdurende ontwikkeling van de ontcijferkunst zouden hebben moeten krijgen. Waar er rond 1600 nog officiële cryptoanalisten in dienst waren, werd in de periode na 1650 de cryptoanalyse meestal uitbesteed aan andere landen, of onder Heinsius, in het geheim beoefend. Praktische overwegingen kunnen wellicht de oorzaak zijn geweest. De internationale connecties met Engeland en Hannover zorgden ervoor dat de Republiek makkelijk van de cryptoanalyse aldaar gebruik kon maken, zodat er geen reden was hiervoor zelf mensen en geld vrij te maken.

3. INSTITUTIONALISERING: DE ACHTTIENDE EEUW

Vanaf halverwege de zeventiende eeuw ontstonden in West-Europa de zogenaamde "zwarte kamers". Volgens een definitie die De Leeuw geeft, waren dit *entities, usually located in a seperate quarter of the General Post Office. Their main task was the opening, copying and, ultimately, decoding of letters of foreign diplomats. They consisted of a small team of clerks with superior language skills, professional forgers of seals and trained cryptanalysts, who, more often than not, transferred their arcane knowledge from one generation to the next.*[41] De term en deze definitie zijn niet voor elke situatie even verhelderend, omdat het beeld wordt opgeroepen van een geheimzinnige, slecht verlichte kamer in een postkantoor waar postzakken verspreid door de kamer staan en mannen met kaarsen, zegellak en codetabellen in de weer zijn om hun ingenieus maar bedenkelijk werk te verrichten.

Slechts in enkele gevallen, zoals in Wenen, ging het inderdaad om een complete, georganiseerde afdeling. Maar in de meeste gevallen was de praktijk anders geregeld. Het onderscheppen van de post werd vaak op meerdere postkantoren gedaan als er geen centraal postkantoor was. Soms werd dit door een omgekochte ambtenaar gedaan; in andere gevallen was het officieel geregeld. Dan was er een ruimte ingericht waar speciale ambtenaren onder geheimhouding doende waren de post te openen, te kopiëren en weer te sluiten. Omdat de meeste – maar niet alle – diplomatieke post in geheimschrift was gesteld, was het vaak nodig dat de brieven ontcijferd werden. De kopieën werden dan doorgestuurd naar een cryptoanalist, wat in de meeste gevallen steeds dezelfde persoon was, omdat er vaak maar één cryptoanalist aan het hof werkte. Vanwege de aard van het werk werden de kopieën vaak bij hem thuis bezorgd. Bij een bekende code betekende dit niet veel werk, maar het ontcijferen van een nieuwe code kon een cryptoanalist soms maanden of jaren kosten, en van de meeste cryptoanalisten is bekend dat ze weinig rust namen voordat de code gekraakt was.[42] Er stond dan ook vaak een vorstelijke vergoeding tegenover.[43]

De term "zwarte kamer" moet dus tegen deze achtergrond gezien worden, en een betere definitie zou als volgt kunnen luiden. Onder de term "zwarte kamer" wordt verstaan het geheel van activiteiten, geïnitieerd door een regering, met als doel het kennis kunnen nemen van de

[41] De Leeuw, *Cryptology and statecraft,* 76
[42] Kahn, *The codebreakers,* 168 en Nationaal Archief, Collectie 306 Familiearchieven Croiset en anderen, 1694-1964 (2.21.045) 16. De toen zeventigjarige Engelse wiskundige Wallis zegt bijvoorbeeld: "I have already employed about seven weeks on them, and have studied hard thereupon eight or ten hours in a day, or more than so very often, which, in a business of this nature is hard service for one of my years unless I would crack my brains at it". Het is ook een veelvuldig terugkerend thema in de brieven van de Nederlandse secretaris van de cijfers Croiset. Die meldt bijvoorbeeld dat hij "niet zelden geheele dagen tot in den nagt" bezig was met het kraken van een set nieuwe geheimschriften.
[43] Vgl. Kahn, *The codebreakers,* 157, 168 en 165, voor respectievelijk de Franse, Engelse en Oostenrijkse situaties.

inhoud van diplomatieke correspondentie van vreemde mogendheden, door het systematisch kopiëren en ontcijferen daarvan.

In het hieronder volgende overzicht en ook in het geval van de Republiek wordt duidelijk dat deze definitie beter aansluit op de praktijk dan een definitie die uitgaat van een fysieke afdeling.

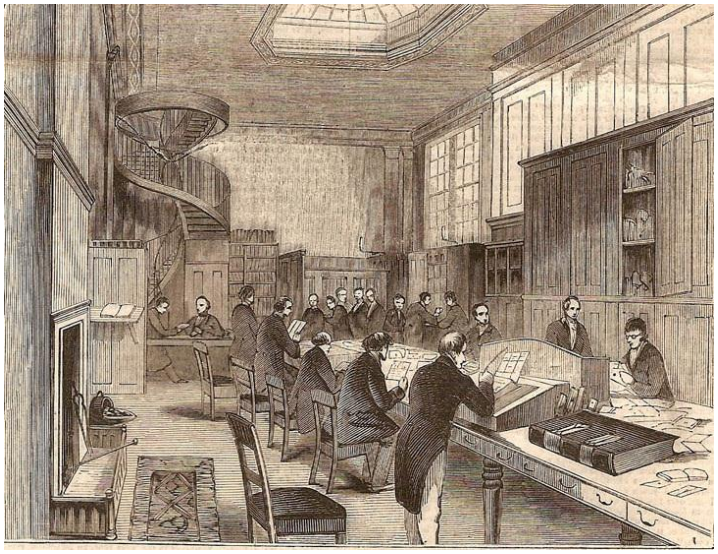
3.1 EUROPA

In Frankrijk werd het werk van het *cabinet noir* georganiseerd rondom Antoine Rossignol. Het nut van zijn talent werd door Hendrik II, prins van Condé, in 1628 ontdekt, toen hij de Hugenoten van Réalmont kon verslaan dankzij informatie die Rossignol uit een vercijferde brief wist te halen.[44] De rest van zijn leven is Rossignol aan het hof werkzaam geweest, eerst onder Richelieu en later onder Lodewijk XIV. De schat aan informatie die hij voor zijn opdrachtgevers wist te ontcijferen maakte hem een graag geziene figuur aan het hof en bracht hem macht en rijkdom.[45] Rossignol zorgde er tevens voor dat de codes van de Franse diplomaten beter tegen cryptoanalyse bestand werden. Samen met zijn zoon Bonaventure, die hij later als zijn leerling opleidde en die hem na zijn dood opvolgde, ontwierp hij het beroemde geheimschrift van Lodewijk XIV. Omdat de sleutel hiervan na de dood van Bonaventure verloren ging, is het geheimschrift twee eeuwen lang ongebroken gebleven, zodat de geheime correspondentie van Lodewijk XIV voor lange tijd niet voor historici leesbaar was. Pas rond 1900 is het geheimschrift door een medewerker van het Franse ministerie van buitenlandse zaken gekraakt.[46]

Engeland kende een vergelijkbare ontwikkeling. In 1643 kreeg de wiskundige John Wallis door toeval een gecodeerde brief in handen, die hij zonder al te veel moeite ontcijferde. Daarna kreeg hij van het Parliament meer opdrachten en werd hij voor elke gelukte opdracht rijkelijk beloond met titels, onroerend goed en functies.[47] Toen hij in 1703 stierf, werd zijn kleinzoon als vaste cryptoanalist aangesteld. Die maakte echter al vroeg een einde aan zijn glansrijke carrière doordat hij zichzelf in een koortsachtige toestand doodschoot. Hij werd in 1716 door Edward Willes opgevolgd, die met zijn zonen net als zijn voorgangers een loopbaan met veel geld en functies tegemoet ging.[48] In 1714 werd de keurvorst van Hannover als George I koning van Engeland. Hierdoor ontstond een samenwerking tussen de zwarte kamer van Hannover en de

[44] Kahn, *The codebreakers*, 157
[45] *Ibidem,* 161
[46] Singh, *The codebook,* 55-58
[47] Kahn, *The codebreakers,* 168
[48] *Ibidem,* 171

Engelse *Decyphering Branch.*[49] George I formaliseerde de werking van de Britse zwarte kamer en zorgde voor een systematische onderschepping en ontcijfering van brieven.[50]



Figuur 5 - Het Engelse Secret Office in het Post Office

In het *Post office* werd belangrijke binnenlandse en buitenlandse post gekopieerd. Om dit mogelijk te maken legde het Engelse parlement in de tweede helft van de zeventiende eeuw en begin zeventiende eeuw in een serie wetten vast dat overheidsbeambten middels een volmacht brieven mochten openen.[51] De onderschepte brieven die in cijfer waren gesteld, werden naar de *Decyphering Branch* gestuurd. Dit moet men niet als een formele organisatie zien. Cryptoanalisten werkten vaak vanuit hun eigen huis en kregen de brieven thuis om ze te vertalen.

De *Geheime Kabinets-Kanzlei* van Wenen was beroemd en berucht. In de achttiende eeuw was het een zeer efficiënt opererend apparaat. Alle post werd op systematische wijze opengemaakt en gekopieerd. De Oostenrijkers hadden valse zegels waarmee ze de correspondentie weer konden sluiten alsof er niets was gebeurd. Er waren verschillende cryptoanalisten in dienst. Ze kregen een goede opleiding in talen, cryptologie en cryptoanalyse. Ze hadden vaste werktijden, een vast salaris, en kregen veel waardering van hun opdrachtgevers.[52]

[49] Jeremy Black, Intelligence and the emergence of the information society in eighteenth-century Britain, in Karl de Leeuw en Jan Bergstra (ed.), *The history of information security. A comprehensive handbook,* (Amsterdam 2007) 371
[50] De Leeuw, *Cryptology and statecraft,* 53
[51] Kahn, *The codebreakers,* 172
[52] *Ibidem,* 165

3.2 DE REPUBLIEK

In de Republiek vond in deze periode een vergelijkbare ontwikkeling plaats. Rond 1750 kwam er een omslag in het gebruik van cryptografie en cryptoanalyse. In deze tijd nam ook in de Republiek het onderscheppen en ontcijferen van diplomatieke correspondentie vaste vormen aan. En in dezelfde tijd ontstond in de Republiek voor het eerst een beïnvloeding van cryptoanalyse op cryptografie.

Tussen 1747 en 1752 werd het postwezen gecentraliseerd, waardoor het aftappen van de post een stuk makkelijker werd.[53] De aanleiding om post te onderscheppen was dat de koning in Pruisen, Frederik II, een theoretische bedreiging voor de Republiek vormde vanwege claims op de titel van Stadhouder. De eerste pogingen om structureel brieven in handen te krijgen waren gericht op de correspondentie van Pruisische gezanten

Omdat de brieven in code gesteld waren, probeerde Hendrik Fagel, de griffier van de Staten-Generaal, in eerste instantie de codeboeken van de gezant te stelen. Toen dat mislukte doordat de potentiële dief niet door het keukenraampje van de gezant paste, omdat hij te dik was, schakelde Fagel de Engelse zwarte kamer in.[54] De Engelsen waren bereid mee te werken, omdat dit in hun plannen voor het Heilige Roomse Rijk paste, plannen waarvan Brandenburg een tegenstander was. Al snel werd het onderscheppingswerk door Raadpensionaris Steyn in Den Haag gereguleerd en waren er twee beambten in het betreffende postkantoor aangesteld die in het geheim de uitgaande post kopieerden.[55]

Vanaf 1751 veranderde de manier van werken. Vanaf die tijd mengde een ambtenaar in dienst van de griffier zich in het ontcijferen van de codeboeken. Deze ambtenaar, Lyonet, zou belangrijke invloed gaan uitoefenen op de manier waarop de geheimtalen van de Republiek werden gelezen en geschreven.

[53] De Leeuw, *Cryptology and statecraft,* 83
[54] *Ibidem,* 85
[55] W.J.M. Benschop, "Secrete regeeringszorg met medewerking van het Haagsche postkantoor (1752-1795)", *Bijdragen voor vaderlandsche geschiedenis en oudheidkunde deel 4* (1943) 240-241

3.2.1 ONDER PIERRE LYONET

Pierre Lyonet[56] (1706-1789), was in 1743 in dienst genomen door de griffier François Fagel als opvolger van de vertaler Saurin, die de besluiten van de Staten-Generaal in het Frans en Latijn vertaalde. Een paar maanden later werd Lyonet behalve vertaler patentmeester (een administratief medewerker voor de milities[57]) en codeklerk, een beambte die de brieven van en naar de eigen diplomaten in code zette of vertaalde. François Fagel had Lyonet ontmoet via de schilder Hendrik van Limborch[58], die een portret van Lyonet geschilderd had, zie Figuur 6.

Figuur 6 - Pierre Lyonet in 1742

Lyonet was een beroemd natuurkundige, bioloog, tekenaar en meester in de rechten. Hij ontwierp een eigen microscoop en bestudeerde hiermee voornamelijk insecten. Hij liet deze vervolgens gedetailleerd graveren door de bekende tekenaar Jan Wandelaar. Toen die na een paar tekeningen voor het vervolg op zich liet wachten, nam Lyonet een grafeerles en maakte sindsdien al zijn tekeningen zelf.[59]

Hij is vooral als natuurwetenschapper en verzamelaar beroemd geworden. Zijn verzameling van schelpen was volgens sommigen de beste van Europa.[60] Hij had contacten met internationale wetenschappers en was lid van verschillende buitenlandse wetenschapsverenigingen, zoals The Royal Society van Londen vanaf 1748, de Académie Royale uit Rouen vanaf 1757, de verenigingen van Halle en Berlijn vanaf 1760, en van de Russische wetenschapsvereniging.[61]

In 1744 werd François Fagel als griffier opgevolgd door zijn neef Hendrik Fagel. Tijdens diens ambtstermijn begon Lyonet in 1751 met het zelfstandig ontcijferen van de correspondentie van de Pruisische gezanten De Hellen en Michell, respectievelijk uitgezonden naar de Republiek en

---

[56] Er zijn verschillende schrijfwijzen in de omloop: Pierre/Pieter/Petrus Lyonet/Lijonet/Lyonnet/ Lijonnet/Lionet.
[57] Jan Wagenaar e.a., *Vaderlandsche historie, vervattende de geschiedenissen der Vereenigde Nederlanden Deel 15* (Amsterdam 1795) 302-303. De patenten waren orders of volmachten voor een militie die uitsluitend door de Staten konden afgegeven worden. Zonder zo'n patent mocht een militie niet een stad binnentrekken of verlaten. De bedoeling hiervan was dat de Stadhouder op die manier de soevereiniteit van de Staten niet kon schenden.
[58] W.H. van Seters, *Pierre Lyonet, 1706-1789. Sa vie, ses collections de coquillages et de tableaux, ses recherches entomologiques* (Den Haag 1962) 17
[59] Alexander Chalmers e.a., *The general biographical dictionary, volume 21* (London 1815) 15.
[60] A.J. van der AA, *Biographisch woordenboek der Nederlanden, deel 11* (Haarlem 1865) 822-823
[61] Diploma's en lidmaatschapsbewijzen Pierre Lyonet, Archief Museum Boerhaave, 162x.

Londen. Hoe dit precies tot stand is gekomen, is lastig te bepalen. Volgens een beschrijving die de neef en opvolger van Lyonet, Samuel Egbert Croiset, hier later van gaf[62], was dit voornamelijk op eigen initiatief van Lyonet. Deze had gehoord van de Engelse cryptoanalist Wallis, die zijn land grote diensten bewees en dienovereenkomstig beloond was. Hierdoor was hij geïnspireerd geraakt om zich zelf ook aan de ontcijferkunst te wagen. Hij was van mening dat hij zoiets ook zou kunnen en stelde aan Fagel en de Raadpensionaris Steyn voor om de brieven van de Franse en Pruissische gezanten te onderscheppen. Deze vonden het echter een hachelijke onderneming. Na lang aandringen kreeg hij hiervoor echter van Steyn toch toestemming en hielp hij een tijd lang in het postkantoor van Den Haag mee met het openmaken en kopiëren van de post. De aldus verkregen brieven onderwierp hij aan zijn cryptoanalytisch onderzoek. Het is onbekend hoe Lyonet aan de kennis kwam waarmee hij dit werk kon doen. Maar na anderhalf jaar tien uur per dag aan de zaak gewerkt te hebben wist hij in 1753 de Pruissische codes tenslotte te kraken.

Volgens De Leeuw moet het een fabel zijn dat Lyonet op eigen houtje het initiatief nam en zijn superieuren daarna pas het nut van zijn werk gingen inzien. Hij beschouwt dit als “too ridiculous to be true[63]”. Dit is een moeilijk te bewijzen of weerleggen stelling, omdat er geen argumentatie en geen alternatieve uitleg bij verstrekt worden.

Lyonet wilde voor zijn werk graag beloond worden. Maar tot zijn teleurstelling kreeg hij nul op het rekest. Hij stelde aan Steyn en Fagel voor dat hij voortaan de titel “Secretaris der Secrete Correspondentie” zou krijgen, maar die aarzelden lange tijd en Fagel liet hem uiteindelijk weten dat hij niet snapte waarom Lyonet überhaupt zelf het initiatief had genomen voor het ontcijferen van de Pruissische correspondentie, “niemand heeft je erom gevraagd”. Lyonet merkte vervolgens op dat een titel altijd nog goedkoper was dan een bisdom en duizend pond sterling per jaar, hiermee verwijzend naar de beloningen die zijn Britse collega had gekregen voor vergelijkbaar werk. Fagel ried hem vervolgens aan niet te hoog van de toren te blazen, en dat hij liever wat geld moest vragen. Dit gesprek tekent de gebrouilleerde verhouding die tussen Fagel en Lyonet bestond, en die nooit hartelijk zou worden. Zelfs na het overlijden van beide heren sprak Willem V nog van “de discontentie die zo lange jaaren tusschen dien Heer [Fagel] en wijlen den Heer Lijonet gesubsisteerd had[64]”.

Uiteindelijk kreeg Lyonet van Steyn een jaarlijkse toelage van zeshonderd gulden, maar een groot deel daarvan besteedde aan een secretaris, de reeds geïntroduceerde neef Samuel Egbert Croiset. Die nam hij op eigen kosten in dienst voor het voorbereiden van zijn werkzaamheden.

---

[62] S.E. Croiset, “Recit-abregé de ce qui s’est passé depuis l’an 1751 entre quelques uns des principaux membres de la Republique, et Mr Lyonet, par raport a l’affaire des Chiffres”, Archief Museum Boerhaave, 162r

[63] De Leeuw, *Cryptology and statecraft*, 102, vgl. voetnoot 46.

[64] Aantekeningen S.E. Croiset, Nationaal Archief, Familiearchieven Croiset, nr 17

De Leeuw zet hierbij een kanttekening.[65] Na het overlijden van Lyonet schreef Croiset een sollicitatiebrief naar de functie van Secretaris der Cijfers. Daarin meldde hij zelf dat hij vanaf april 1752 "door hare Kon. Hoogh. […] en den Heere Steijn, Raadpens. van Holl. en WF. tot desselfs adsistentie was toegevoegd[66]". Dit klopt volgens De Leeuw niet met het verhaal dat Lyonet hem een tijd lang zelf heeft betaald. Maar de context van de brief moet niet uit het oog verloren worden. Normaal gesproken zou Croiset als vanzelf als opvolger van Lyonet in de functie benoemd zijn, maar in dit geval speelden scherpe politieke tegenstellingen een rol. Croiset solliciteerde in de brief naar een functie waarbij zijn politiek voorkeur zeker geen pre was. Het zou voor hem weinig voordeel opgeleverd hebben om oude koeien uit de sloot te halen. Mogelijk is de brief een versimpeling van de werkelijkheid geweest ten gunste van zijn werkgevers, om ze niet onnodig voor het hoofd te stoten.

Uit de financiële administratie van Steyn blijkt in deze zaak het volgende. In september 1753 werd Lyonet zeshonderd gulden per jaar toegekend "voor sijn adjunct", die in maart van datzelfde jaar was beëdigd: een jaar nadat hij volgens zijn brief in dienst van Lyonet kwam.[67] Dat zou dus inderdaad betekenen dat Lyonet hem een jaar uit eigen zak zou hebben betaald. Helemaal zeker kunnen we hiervan niet zijn. Het kan ook zijn dat het jaartal 1752 uit de brief van Croiset een vergissing is geweest. Het zou immers wat vreemd zijn, dat Lyonet al een jaar een secretaris in dienst had, zonder dat deze een eed van geheimhouding had afgelegd. Verder komt het jaartal nergens in het CV van Croiset terug. In een overzicht dat Croiset eind 1813 van zijn functies en aanstellingen maakte, noemt hij 1753 als datum dat hij als assistent werd aangesteld.[68]

Croiset heeft verhaal van de gebeurtenissen van 1751 twee keer op schrift gesteld. In de tweede versie van het verhaal vertelt Croiset dat Lyonet na zijn eigengereide actie tevens te verstaan werd gegeven dat hij voor het ontcijferen van de correspondentie niet nodig was, omdat ze deze klusjes in Engeland konden laten opknappen.[69] Als wraak weigerde Lyonet daarna een paar keer de brieven voor zijn superieuren te ontcijferen toen het hem werd gevraagd. Maar na enkele maanden liet hij zijn weerstand toch varen "ten behoeve van zijn vaderland". Wat volgde, bleef een getouwtrek om geld en een titel, waarbij Lyonet gaandeweg wat toezeggingen kreeg, voornamelijk toezeggingen van een bedrag per gebroken geheimschrift. Maar de felbegeerde titels van Secretaris der Secrete Correspondentie, Secretaris der Cijfers van de Staten-Generaal,

[65] De Leeuw, *Cryptology and statecraft*, 102, vgl. voetnoot 47.
[66] Aantekeningen Croiset, Archief Museum Boerhaave, 162r.
[67] Benschop, "Secrete regeeringszorg", *Bijdragen voor vaderlandsche geschiedenis* (1943) 245.
[68] CV van S.E. Croiset, Nationaal Archief, Familiearchieven Croiset, nr 24.
[69] Croiset laat in zijn verslag namen weg omwille van de geheimhouding. Hij heeft het hier over het land "A……", wat wel "Angleterre" zal betekenen.

of, zoals hij aan de Gouvernante voorstelde, Secretaris van Buitenlandse Zaken, bleven buiten bereik.

Volgens Croiset was de reden hiervan vooral van persoonlijke aard. Fagel wilde niet dat Lyonet de titel kreeg die hij begeerde, omdat hij bang was dat Lyonet daarmee boven Fagel kwam te staan en dat buitenlandse diplomaten op basis van die titel eerder naar Lyonet zouden gaan dan naar Fagel. Lyonet zorgde er daarnaast totaal onverwacht voor dat de Republiek minder van Engeland afhankelijk werd, terwijl Fagel juiste erg op Engeland was georiënteerd. Het wantrouwen werd nog eens bevestigd door het feit dat Lyonet een gevierd lid van de internationale gemeenschap was. Hij was een graag geziene gast bij de ambassadeurs in Den Haag en Fagel dacht dat het maar al te makkelijk zou zijn dat hij daar zijn mond voorbij zou praten.[70]

Behalve de door Croiset genoemde redenen speelde mogelijk ook mee dat Lyonet en in zijn voetspoor ook Croiset niet bepaald als Oranjegezind bekend stonden. Bewijzen hiervan zijn inderdaad terug te vinden. In 1784 schreef Lyonet een anonieme brief aan de Stadhouder: hij vreesde dat er een poging gedaan zou worden om Willem V als soeverein vorst aan te stellen en dat op die manier de Staten aan de kant gezet zouden worden. Lyonet wees Willem V er in de brief op dat de Staten wettig soeverein “altoos zijn en blijven” en dat ze in die hoedanigheid de macht hadden om de bevoegdheden van de Stadhouder in te perken of hem die bevoegdheden zelfs helemaal af te nemen en aan een ander te doen toekomen. Hij riep de Prins op om zijn “idées van Despoticq te worden” af te leggen en zodoende verder onheil te voorkomen.[71]

Een ander voorval toont aan dat ook Croiset aan de kant van de patriotten stond. Toen de Fransen plotseling een veel moeilijker geheimschrift in gebruik namen, beschuldigde de secretaris van de Staten van Holland, A.J. Roijer, de “verdoemde canailles van patriotten” van het lekken van de informatie naar de Fransen. Croiset trok zich dat persoonlijk aan en antwoordde hierop heftig: “neen, die hebben dat niet gedaan, maar ’t zijn die verdoemde canailles van Prinsgezinden die het gedaan hebben!” Waarna Croiset zich uitputte in het oplepelen van beschuldigingen aan het adres van diverse prinsgezinden die bij het werk betrokken waren, zoals de familie Tinne.[72]

Behalve de persoonlijke motieven van Fagel en de tegenstelling staatsgezinden versus orangisten, heeft ook de geheime aard van het werk een officiële titel en evenredige beloning waarschijnlijk in de weg gestaan.[73] Een titel zoals die van Secretaris der Cijfers van de Staten-

[70] De Leeuw, *Cryptology and statecraft,* 89
[71] Kopie van een brief aan Willem V, 10 mei 1784, Archief Museum Boerhaave, 162u
[72] Verslag van S.E. Croiset van een gesprek op 12 november 1788, Archief Museum Boerhaave, 162r
[73] De Leeuw, *Cryptology and statecraft,* 89

Generaal, zou via een officiële benoeming in de Staten-Generaal tot stand moeten komen, waardoor het werk van Lyonet, dat met geheimhouding zeer gebaat was, openlijk besproken zou moeten worden in een orgaan dat niet bepaald om zijn geheimhouding bekend stond.

Vanaf 1755 had de Republiek geen keus meer dan Lyonet en Croiset in te schakelen voor het ontcijferwerk. De verhouding met Engeland was bekoeld, zodat de Republiek geen werk meer naar de Engelse zwarte kamer kon uitbesteden. Lyonet wist het moment volledig te benutten, want hij weigerde de Pruissische en Franse codes te kraken, met als reden dat hij voor zoiets geen tijd had omdat hij bezig was met het schrijven van een boek over slakken.[74] De Gouvernante, prinses Anna, trad als financier op en wist zodoende de impasse te doorbreken. Ze zorgde er voor dat Lyonet duizend gulden per jaar kreeg in afwachting van een officiële beloning door de Staten-Generaal, waardoor hij weer aan het werk ging. De officiële beloning van de Staten-Generaal is er echter nooit gekomen. En ook een titel bleef uit. Er kwam wel een compromis tot stand. Lyonet mocht vanaf 1762 met goedkeuring van Fagel en Steyn de titel "Secretaris der Cijfers van Hunne Hoog Mogenden" voeren, maar deze titel werd hem nooit officieel door de Staten-Generaal verleend.[75]

Gedurende de jaren daarna kwam het "werk der cijffers" in rustiger vaarwater. Van die tijd zijn veel ontcijferde brieven in de archieven terug te vinden, en weinig van het getouwtrek van de jaren '50. Tijdens deze jaren hielden Lyonet en Croiset zich ook bezig met het samenstellen van de codeboeken voor de diplomaten van de Republiek in den vreemde. Deze codes waren een enorme verbetering ten opzichte van de codes die gebruikt werden voordat Lyonet zijn werk als cryptoanalist begon.[76]

In de periode van Lyonet maakte de Republiek dus een ontwikkeling door zoals die ook in andere staten plaatsvond. De geheimschriften kwamen op een hoger plan, en de cryptoanalyse nam structurele vormen aan. Het gedoe over de status hiervan leek vanaf de zestiger jaren afgelopen te zijn, maar onder de oppervlakte bleven de spanningen bestaan, zoals uit het vervolg zou blijken.

[74] De Leeuw, *Cryptology and statecraft,* 94
[75] A. Ising, "Een dialoog in 1756", *De Nederlandsche Spectator, no 24* (1860) 187
[76] De Leeuw, *Cryptology and statecraft,* 28

3.2.2 ONDER SAMUEL EGBERT CROISET

Figuur 7 - Samuel Egbert Croiset (1734-1816)

Na de dood van Lyonet op 10 januari 1787 begon de strijd om titel, geld en erkenning opnieuw. Croiset stuurde een brief waarin hij verzocht om de opvolger van Lyonet te worden. Hij werd inderdaad officieel door een besluit van de Staten-Generaal tot opvolger benoemd, maar dat was slechts in een van de drie functies die Lyonet had bekleed, en tot zijn verbijstering kreeg hij de titel die Lyonet in 1743 had gekregen, "klerk der cijfers".[77] Een vaste aanstelling als secretaris der cijfers met bijbehorend traktement zat er dus niet in. Het cryptoanalytische werk, dat tijdens het leven van Lyonet structurele vormen had aangenomen, werd plotseling weer teruggezet tot een werk dat op afroep en ad-hoc basis werd gedaan. Croiset komt hierdoor tot de bittere constatering dat hij "dus bijkans den ouden knegt zou blijven, 't geen mij niet zeer bevallen zoude[78]". Croiset moest het doen met een bedrag per ontcijferde code. Omdat de codes steeds moeilijker werden, kostte het hem evenredig meer moeite om de codes te ontcijferen, en soms lukte het hem helemaal niet. In het eerste geval daalde zijn uurloon en in het tweede geval kreeg hij voor zijn moeitevol werk helemaal niets.[79]

Ondanks de beperkte beloning die er tegenover stond, was zijn werk toch van grote waarde voor de Republiek. Dat is althans iets wat Croiset uit het gedrag van zijn opdrachtgevers kon opmaken. Tijdens hij ontcijferen van nieuwe geheimschriften werd hem herhaaldelijk gevraagd of het werk al gereed was en van bevriende staatslieden kreeg hij te horen hoeveel belang de Raadpensionaris en griffier in zijn werk stelden.[80]

Croiset vroeg regelmatig om een vaste beloning voor zijn werkzaamheden. Hij kreeg wel mondelinge toezeggingen, maar die werden niet ingelost. Croiset herinnerde Van der Spiegel, de raadpensionaris van Holland, herhaaldelijk aan een beloofde verhoging van zijn traktement. En de prins beloofde hem dat Croiset met terugwerkende kracht vanaf de dood van Lyonet een jaargeld van vijfhonderd gulden zou ontvangen. Nadat Croiset de datum van het overlijden van

[77] Resolutie Staten-Generaal 12 januari 1789, Archief Museum Boerhaave, 162d
[78] Dagboek van Croiset, Archief Museum Boerhaave, 162r.
[79] Brief aan Van der Spiegel, Nationaal Archief, Familiearchieven Croiset, nr. 16
[80] Dagboek van Croiset, Archief Museum Boerhaave, 162r.

Lyonet had doorgegeven, vergat de prins zijn belofte echter. Er zijn geen bewijzen dat Croiset dit geld ooit gekregen heeft.[81]

Raadpensionaris Van der Spiegel probeerde Croiset vanaf 1790 op weinig subtiele wijze buiten spel te zetten. Hij gaf bijvoorbeeld aan dat hij het nut van het ontcijferen niet inzag, en liet doorschemeren dat hij met het onderscheppen van de post niet gelukkig was en dat werk maar helemaal wilde stoppen. Ook vond hij dat Lyonet en Croiset weliswaar goed werk gedaan hadden, maar je dat niet moest overdrijven, en dat zijn secretaris, Matthijs Tinne, dit werk misschien ook wel zou kunnen doen.[82] Dit is een wonderlijke constatering voor iemand die heel goed wist wat het werk met geheimschriften inhield: Van der Spiegel was zelf een liefhebber van het onderwerp en had eerder veel interesse in het werk van Croiset getoond.[83] Bovendien hield Van der Spiegel zijn secretaris Tinne zoveel mogelijk buiten zaken van enig belang, omdat diens aanstelling politiek gezien een vergissing was geweest en de raadpensionaris hem geen geheimen toe durfde te vertrouwen.[84] Dat hij hem zou kunnen inzetten voor het ontcijferen van geheime correspondentie lijkt dan ook een loos dreigement. In 1791 deed Van der Spiegel zelfs pogingen om Croiset in het onderscheppen van brieven te passeren. Croiset betrapte Tinne tijdens het kopiëren van een Russische brief, die de raadpensionaris in Engeland wilde laten ontcijferen. De reden van dit optreden was dat Van der Spiegel Croiset vanwege zijn politieke voorkeur wantrouwde en de geheime correspondentie niet meer via diens tussenkomst wilde laten lopen. Hij ontwierp zelfs eigenhandig een geheimschrift voor de bondgenoten van de stadhouder, de Engelse en Berlijnse gezant, zodat het niet “door zeekere handen” zou passeren.[85]

Na de Bataafse Revolutie kwam aan deze botsende belangen een einde. Het werk van de cryptoanalisten werd door het nieuwe regime op waarde geschat en dit keer waren er geen politieke redenen om de cryptoanalisten buiten spel te zetten. Het Bataafse regime stelde Croiset vrijwel onmiddellijk aan als *secretaris der cijfers van de staat*. Deze keer gebeurde dat officieel, via een besluit van de Nationale Vergadering. Gezien zijn hoge leeftijd kreeg Croiset een adjunct secretaris, Lodewijk van Toulon. Hij kreeg voor zijn werk een vast traktement van drieduizend gulden per jaar, Van Toulon kreeg een salaris van duizend gulden per jaar. Daarnaast kreeg Croiset per gekraakt cijferschrift een bonus van tweehonderd gulden.[86]

Hierna brak opnieuw een periode van relatieve kalmte aan voor de cryptoanalisten. De emotioneel geladen aantekeningen die Croiset over de bewogen perioden maakte, ontbreken

[81] Diverse brieven en verslagen van gesprekken, Nationaal Archief, Familiearchieven Croiset, nr. 16-18
[82] Dagboek van Croiset, aantekening 11 september 1790, Archief Museum Boerhaave, 162r.
[83] De Leeuw, *Cryptology and statecraft,* 32
[84] W.J.M. Benschop, “Secrete regeeringszorg”, *Bijdragen voor vaderlandsche geschiedenis* (1943) 252-3. Er waren twee Tinnes werkzaam als secretaris onder Van der Spiegel, in 1790 was dat Matthijs Tinne.
[85] De Leeuw, *Cryptology and statecraft,* 141
[86] Besluit Nationale Vergadering 25 maart 1796, Nationaal Archief, Familiearchieven Croiset, nr 20

rond de eeuwwisseling. Rond 1810 werd het ministerie van buitenlandse zaken gereorganiseerd en werd de functie van Croiset opgeheven, waarna hij met pensioen ging. Na de restauratie en de instelling van Willem I als soeverein vorst werd hem vanaf 1814 een pensioen van tweeduizend gulden toegekend.[87]

Onder Lyonet was in de Republiek de ontwikkeling van de cryptologie in een stroomversnelling gekomen, maar latent waren er voortdurend andere krachten aanwezig, die om persoonlijke en politieke motieven het werk niet stimuleerden of zelfs tegenwerkten. Deze krachten verdwenen met de Bataafse Revolutie, maar na een paar jaar werd de cryptoanalyse in Den Haag om bestuurlijke redenen opgeheven. Met de pensionering van Croiset kwam er een na bijna zestig jaar een einde aan de cryptoanalyse in de Republiek.

[87] CV S.E. Croiset, Nationaal Archief, familiearchieven Croiset, nr 24

CONCLUSIE

De cryptologie maakte in de Republiek in verschillende opzichten een vergelijkbare ontwikkeling door als in andere landen, maar het recente ontstaan van het eigen bestuur, de afwijkende staatsinrichting en de politieke tegenstellingen in de Republiek maakten deze ontwikkeling tot een bijzonder geval.

Tot de zeventiende eeuw was de cryptoanalyse in de Republiek in de meeste opzichten vergelijkbaar met die in andere landen. De cryptografie daarentegen liep achter, maar de behoefte aan een goede cryptografie was door de geringe hoeveelheid diplomatieke correspondentie van en naar de Republiek minder dan in andere landen. In de zeventiende eeuw begon ook de cryptoanalyse achter te raken op die van andere landen, omdat er voor een groot deel van buitenlandse cryptoanalisten gebruik werd gemaakt.

Een ander verschil met de omringende landen was dat de cryptoanalyse in de Republiek – met uitzondering van Aleaume – vaak een privé aangelegenheid was van de verschillende griffiers, raadpensionarissen en prinsen van Oranje, vanwege de moeilijkheid van geheimhouding bij een officiële aanstelling. Dit stond dus institutionalisering en professionalisering in de weg. Er vond geen overdracht naar een opvolger plaats en er was geen uitwisseling tussen cryptoanalist en cryptograaf. De opstellers van de codelijsten waren zich niet bewust van de mogelijkheden voor cryptoanalyse en hadden dus ook niet de gelegenheid de codelijsten beter te beschermen tegen de mogelijkheden van analyse.

Een ander punt was dat de uitgaven die voor zoiets gedaan moesten worden, eerst door de Staten goedgekeurd moesten worden. Omdat mensen met de gaven om codes te breken zeldzaam waren, waren ze ook vrij duur. Men was eenvoudigweg niet bereid veel geld uit te geven aan zo'n zaak[88], waarvan het nut voor de beslissers nooit was bewezen, of in ieder geval verborgen werd gehouden.

Vanaf de achttiende eeuw vond in veel landen institutionalisering van de cryptologie plaats, aangeduid als de periode van de "zwarte kamers". Het is duidelijk dat er volgens de definitie op pagina 18 gedurende bepaalde perioden ook in de Republiek sprake was van een zwarte kamer. Een belangrijk onderdeel uit de definitie is het woord "systematisch". In de Republiek was vanaf de tweede helft van de achttiende eeuw zeker sprake van het structureel onderscheppen en ontcijferen van de diplomatieke post.

[88] G. de Bruin, *Geheimhouding en verraad. De geheimhouding van staatszaken ten tijde van de Republiek (1600-1750)* (Den Haag, 1991) 325-326

Gedurende die periode werd steeds meer diplomatieke post systematisch op het postkantoor in Den Haag opengemaakt en gekopieerd. Pierre Lyonet nam de rol van cryptoanalist op zich en wist met succes de meeste codes van andere mogendheden te kraken. Daarnaast was hij de klerk der cijfers, degene die de codes voor diplomaten van de Republiek in den vreemde samenstelde. Door de combinatie van deze werkzaamheden nam het niveau van de codes van de Republiek in die periode enorm toe. Zijn positie als cryptoanalist werd in 1762 min of meer officieel gemaakt met de titel "Secretaris der Cijfers van Hunne Hoog Mogenden". Van harte ging dit niet, want na zijn overlijden verviel deze titel onmiddellijk. Tijdens zijn werk leidde hij achterneef Samuël Egbert Croiset op, die hem na zijn dood in 1789 opvolgde. In de Bataafse Republiek bleef Croiset kort in functie en ook hij zorgde voor een opvolger, zijn neef L. van Toulon. De functie werd echter in 1810 opgeheven bij koninklijk besluit om het "werk der cijfers" op een andere manier te regelen.

In deze periode vond dus institutionalisering van het werk der cijfers plaats, in de zin dat de cryptoanalisten min of meer officiële status kregen, dat ze min of meer structureel beloond werden, dat het onderscheppen van de post gereguleerd was, en dat er op structurele wijze kennis werd genomen van buitenlandse diplomatieke post. Verder is duidelijk dat er sprake was van professionalisering. De cryptoanalisten zorgden voor een opvolger en trainden deze ook.[89] Daarnaast was er een wederzijdse beïnvloeding van cryptografie en cryptoanalyse, waardoor de kwaliteit van het werk toenam.

Toch zijn er diverse kanttekeningen te plaatsen. De institutionalisering vond erg schoorvoetend plaats. De reeds gemelde bezwaren golden hier nog steeds: het punt van geheimhouding en het probleem dat niemand voor de kosten wilde opdraaien. Uit het voorgaande is duidelijk geworden dat het bij zowel Lyonet als Croiset zeker niet vanzelfsprekend was dat hun inspanningen gewaardeerd werden met een aanstelling of vast salaris. De beloning voor het werk bleef op *ad hoc* basis: elke gekraakte code leverde een bedrag op, maar een periodiek traktement zat er niet in, ondanks eindeloos aandringen van zowel Lyonet als Croiset. In praktijk kwam er wel een jaarlijks vast bedrag tot stand, maar dit kwam vooral door tegemoetkomingen van de Oranjes. Ook met de aanstelling ging het erg stroef. Uiteindelijk bleef het bij het oogluikend toestaan van het gebruik van een bepaalde titel. Pas in de Bataafse Republiek kregen de cryptoanalisten officieel een titel en salaris.

Er lijkt in eerste instantie helemaal geen sprake geweest te zijn van het doelbewust aansturen op de instelling van een "zwarte kamer" of het realiseren van het ontcijferen van de geheime

[89] Trainingsmateriaal van Lyonet, Archief Museum Boerhaave, 162s. Lyonet had in zijn papieren een brief van Philips II aan de hertog van Alva in drievoud: een gecodeerde variant, een variant met de gewone tekst, en een hybride versie.

correspondentie in de Republiek zelf. Het werk van Lyonet werd zelfs afkeurend begroet. Later, nadat Fagel schoorvoetend het nut van het werk van Lyonet in begon te zien, en toen hij door de omstandigheden gedwongen werd, werd er van het werk van de cryptoanalyse meer gebruik gemaakt.

Van de professionalisering moet dus gezegd worden dat dit vooral de verdienste lijkt van de personen die zich met het werk bezig hielden. Het aannemen van een assistent was waarschijnlijk op eigen initiatief van Lyonet, en het verbeteren van de eigen diplomatieke geheimschriften was – volgens eigen zeggen – ook vooral toe te schrijven aan Lyonet en Croiset. Ook hier geldt dat er pas in de Bataafse tijd beleid van werd gemaakt dat er een officiële opvolger werd benoemd.

In vergelijking met landen zoals Frankrijk, Engeland en Oostenrijk is de opkomst van de zwarte kamer in de Republiek dus een knarsende aangelegenheid geweest. Behalve de reeds genoemde bezwaren die veroorzaakt werden door de staatsinrichting van de Republiek, is uit het voorgaande duidelijk geworden dat deze moeizame gang van zaken voor een groot deel veroorzaakt werd door de persoonlijke en politieke wrijving tussen de verschillende hoofdpersonen. Fagel had persoonlijke motieven om Lyonet geen titel te gunnen. En een bijzonder belangrijke rol werd gespeeld door de tegenstelling tussen orangisten en staatsgezinden.

Vanaf de ontdekking van de mogelijkheden van de cryptoanalyse was het ontcijferen van de buitenlandse geheime correspondentie voor de griffier en raadpensionaris een belangrijke en onmisbare bron van informatie geworden. Het misbaar door persoonlijke en politieke tegenstellingen was er echter de oorzaak van dat de Republiek hier niet optimaal van kon profiteren. Aan beide kanten heeft men zich niet over de verschillen heen kunnen zetten zodat de zwart kamer nooit geolied heeft kunnen functioneren. Zoals Croiset het verwoordde: “De dienaar is zijnen loon waardig. Deze geeft voedsel aan ijver en geestvermogen, die bij mangel van denzelve verdoofd en uitgebluscht worden.”

OVERZICHT VAN GERAADPLEEGDE WERKEN

BRONNEN

Archief Museum Boerhaave, Leiden
Documenten m.b.t. Pieter Lyonet: correspondentie, familie, werk, nalatenschap
Inv. nr. 162, aantekeningen S.E. Croiset

inghist.nl
Resolutiën Staten-Generaal 1626-1630
Afschriften van 1626: 18 juli, nr. 1, 21 juli, nr. 11, 27 juli, nr. 5 en 29 juli, nr. 10.

Nationaal Archief , Den Haag
Collectie 306 Familiearchieven Croiset en anderen, 1694-1964 (2.21.045)
Inv. nr. 15 t/m 25, aantekeningen en brieven S.E. Croiset.

Collectie Fagel, 1513-192 (1.10.29)
Inv. nr. 598, informatie over klerken ter griffie
Inv. nr. 1210 t/m 1258, codelijsten voor diplomaten

LITERATUURLIJST

Anderson, M.S., *The rise of modern diplomacy 1450-1919* (New York 2001)

Benschop, W.J.M., "Secrete regeeringszorg met medewerking van het Haagsche postkantoor (1752-1795)", *Bijdragen voor vaderlandsche geschiedenis en oudheidkunde deel 4* (1943)

Bruin, G. de, *Geheimhouding en verraad. De geheimhouding van staatszaken ten tijde van de Republiek (1600-1750)* (Den Haag, 1991)

Ising, A., "Een dialoog in 1756", *De Nederlandsche Spectator, no 24* (1860) 187

Kahn, David, *The codebreakers. The story of secret writing* (New York 1967)

Leeuw, Karl de, en Jan Bergstra (ed.), *The history of information security. A comprehensive handbook,* (Amsterdam 2007)

Leeuw, Karl de, *Cryptology and statecraft in the Dutch Republic,* (Amsterdam 2000)

Seters, W.H. van, *Pierre Lyonet, 1706-1789. Sa vie, ses collections de coquillages et de tableaux, ses recherches entomologiques* (Den Haag 1962)

Singh, Simon, *The code book. The secret history of codes and codebreaking* (Londen 2000)

ANACHRONISTISCHE BIJLAGE

Als klein onderdeel van het onderzoek voor deze scriptie heb ik gekeken naar de huidige stand van zaken in de cryptologie.

Met de opkomst van de computer zijn geheimschriften praktisch gezien onkraakbaar geworden. Een andere ontwikkeling die mogelijk is gemaakt door de opkomst van geautomatiseerde geheimschriften, is dat het zogenaamde *key distribution problem* is opgelost. Het uitwisselen van de sleutel van een geheimschrift is tot die tijd de achilleshiel van de cryptografie geweest. Dit probleem is in 1976 door de wiskundige Hellman en cryptoloog Diffie opgelost en door een groep wiskundigen in 1977 uitgewerkt in het RSA algoritme. Dit algoritme is op dit moment de standaard voor het veilig elektronisch uitwisselen van gegevens op het internet.

Hoewel het nu dus voor bijna iedereen mogelijk is geworden om zijn correspondentie zodanig te versleutelen, dat er redelijkerwijs decennia voor nodig zouden moeten zijn om deze beveiliging te kraken, is het in praktijk echter juist vele malen makkelijker geworden om correspondentie te onderscheppen en te lezen, omdat bijna iedereen van het uiterst onveilige communicatiemedium email gebruik maakt.

Daarom hierbij de introductie van een in het kader van deze scriptie ontwikkeld programma, PiC, Paranoia in Communication. De mogelijkheden van beveiliging die op dit moment mogelijk zijn, worden in dit programma toegankelijk gemaakt voor gebruik in conventionele email.

Details over dit programma zijn te vinden op http://bit.ly/pic2011.