11

Geheimschrijverij bij De Meijer

Een zijdelingse blik op de Nederlandse cryptografie

Bart Jacobs & Florentijn van Kampen

> 'Onze eigen installatie voor radio-telegrafie vangt tegenwoordig de draadlooze telegrammen op, die op bepaalde uren van de Duitsche duikboten worden verzonden, wij zullen nu wel spoedig de geheime code ontcijferen door de handigheid van den genialen Koot.'
>
> (De Meijer citeert Van Woelderen, 8 februari 1918, p. 52)

Dit citaat gaat over de situatie in 1918, het laatste jaar van de Eerste Wereldoorlog. Die oorlog werd pas in de laatste maanden van dat jaar beslist en is militair tot het einde toe spannend gebleven. Nederland was neutraal en is relatief ongeschonden door de oorlog heen gekomen. Het handhaven van die neutraliteit was een constante zorg van de regering,[1] omdat Nederland werd omringd door oorlogvoerende landen. Geen daarvan wilde dat Nederland een andere partij zou helpen. Ook waren er incidenten,[2] waarbij de soevereiniteit werd geschonden, zowel op het land als ter zee. Verschillende malen zijn Duitse of Engelse schepen in Nederlandse territoriale wateren beland, waarbij het niet direct duidelijk was of het ging om een navigatiefout, een noodsituatie of om militaire agressie. Onder dergelijke omstandigheden is het voor een neutraal land van belang de situatie goed in te kunnen schatten. Een gestrand schip of duikboot zal aan het thuisfront willen laten weten wat er aan de hand is. Toegang tot die communicatie was voor Nederland van strategisch belang, juist om de neutraliteit

te handhaven. Het berichtenverkeer was versleuteld, om te voorkomen dat de inhoud zomaar gelezen kon worden, en moest eerst worden ontcijferd.

'De handigheid van den genialen Koot'

Uit het citaat spreekt de verwachting dat 'wij' spoedig na het opzetten van ontvangstantennes aan de kust in staat zullen zijn de geheime, versleutelde radiografische communicatie van Duitse duikboten te 'ontcijferen'. Dat hadden we te danken aan 'den genialen Koot'. Bedoeld wordt Henri Koot, een Nederlandse officier die in 1883 geboren is op Bali, in de noordelijke kuststad Singaradja. Zijn moeder was van Chinese komaf en zijn vader was Nederlandse ambtenaar. Na zijn middelbare school werd Henri militair in het Koninklijk Nederlandsch-Indisch Leger (KNIL). In 1911 kwam hij naar Nederland voor zijn officiersopleiding aan de Koninklijke Militaire Academie (KMA) in Breda. Door het uitbreken van de Eerste Wereldoorlog in 1914 kon hij niet terug naar Indië. Dat zou grote invloed hebben.

Na zijn opleiding aan de KMA bleek dat Koot spitsvondig en vasthoudend was, en dat hij beschikte over een scherp gevoel voor taal. Waarschijnlijk om die reden werd hem gevraagd bij de net opgerichte afdeling IV van de Generale Staf (GS IV) te proberen om de geheimen uit versleutelde berichten van andere landen te achterhalen.[3] Dit was een gouden greep, want Koot bleek een natuurtalent te zijn in de cryptologie[4]. Hij maakte zich dit vakgebied zelf snel eigen en ontpopte zich tot Nederlands belangrijkste codekraker van de eerste helft van de twintigste eeuw. Een leerling van Koot, J.R. van der Schrieck, maakt hem van dichtbij mee en vertelde later: 'Generaal Koot had een fantastisch brein, dat zo snel en diep dacht dat weinig mensen hem konden volgen. Zijn lievelingsonderwerp en werk was cryptografie. Volgens mij was hij een van de meest vooraanstaande crypto-analisten ter wereld.'[5] Een Amerikaanse collega-cryptoloog omschreef hem volgens Van der

Schrieck in een fraaie oneliner: 'If you give Koot a telegram in a code unknown to him, he just sniffs it and tells you what's in it.'

Cryptologie is de wetenschap van het omzetten van boodschappen in geheimschrift (en terug). Deze berichten zijn dan 'gecodeerd'. Het vakgebied van de cryptologie kan verder onderverdeeld worden in het *maken* en het *breken* van codes, respectievelijk aangeduid met de termen cryptografie en cryptoanalyse. In de tijd van Koot was alle cryptologie handwerk: slim gepuzzel met pen en papier. Twee opgaven aan het eind van het hoofdstuk geven een indruk van dit werk. Moderne cryptosystemen maken gebruik van geavanceerde wiskunde en zijn zelfs met krachtige computers niet te breken.

Nederlandse ontsleutelingen

GS IV hield zich bezig met censuur, contra-inlichtingen en het tegengaan van smokkelhandel.[6] Kapitein der artillerie W.J.C. Schuurman gaf leiding aan de afdeling censuur, waar, naast het controleren van buitenlands telegram- en telegraafverkeer, ook de cryptoanalyse, het ontcijferen van codeberichten, plaatsvond.[7] Hij vroeg Koot deze laatste activiteit vorm te geven. Die verzamelde in korte tijd een groep enthousiastelingen om zich heen. Versleutelde telegrammen van ambassades en buitenlandse gezanten werden op postkantoren gekopieerd en doorgestuurd naar GS IV. Ook versleutelde radiografische berichten kwamen er terecht. Vaak lukte het Koot met zijn team om de inhoud te achterhalen. De Meijer beschrijft hoe Carel Albert van Woelderen, kapitein der artillerie en plaatsvervangend hoofd van de inlichtingendienst GS III tijdens de Eerste Wereldoorlog, iedere morgen eerst bij GS IV langsging om de laatste ontcijferde berichten en geheime telegrammen in te zien.[8] Later volgde hij H.A.C. Fabius op als diensthoofd.[9] Hij

hield van 19 juli 1916 tot 24 juli 1919 een handgeschreven dagboek bij. De Meijer besteedt er in zijn rapport een heel hoofdstuk aan en het is zijn voornaamste bron van informatie over Koot en over het breken van codes.

De eerste vermelding in het rapport van een succesvolle ontsleuteling is van augustus 1916, wanneer de code van de Duitse attaché M. Renner wordt gebroken.[10] Hierdoor las GS IV zijn geheime diplomatieke correspondentie, waardoor indirect ook waardevolle gegevens werden verkregen over Engelse troepenbewegingen. Tegen het einde van de oorlog werd ook de Engelse code gekraakt die GS IV in de onderschepte communicatie had aangetroffen. Volgens Van Woelderen leverde dat 'belangrijke gegevens' op, zonder hierover verdere details te verschaffen. Koot en zijn team braken nog twee andere Duitse codes. De Duitse duikbootcode valt[11] in 1918 en de 'Waco code' in 1919.[12] Door dit laatste kreeg Nederland zicht op het verloop van de vredesonderhandelingen in Versailles. De ontcijferde berichten verschaften Nederland een opmerkelijk inkijkje in de vredesvoorstellen: '[...] waaruit wij nauwkeurig de machinaties lezen van de Amerikanen, die de Duitschers aanzetten, om de vredesvoorstellen niet aan te nemen.'[13] Het belang van Koot is in 1919 zo groot geworden dat Van Woelderen waarschuwde: 'De positie van kapitein Koot moet dringend worden vastgesteld, anders dreigt het gevaar dat deze allereerste kracht in het ontcijferen van codes toch nog door vertrek naar Nederlands-Indië voor G.S. III verloren gaat.'[14]

Inderdaad, aan het einde van de Eerste Wereldoorlog leidde Koot een goed functionerende ontcijferdienst, ofwel, met een in die tijd gangbare en wat mysterieuze omschrijving, een geheime 'Zwarte Kamer'. Die had zijn waarde bewezen. Over de successen van GS IV is vooralsnog weinig meer bekend dan hierboven beschreven, omdat in mei 1940 de archieven van de geheime diensten GS III en GS IV grotendeels zijn vernietigd om te voorkomen dat ze in handen van de Duitse bezetter zouden vallen. Daardoor is ons beeld gefragmenteerd.

Gelukkig keerde Koot niet terug naar Indië. Hij bleef in Ne-

derland en droeg bij aan de institutionalisering van cryptologie, al verliep de ontwikkeling rommelig. Eerst werd GS IV gereduceerd tot een afdeling 'C' van GS III, aangeduid als GS IIIC.[15] Daarna verhuisde Koot van de Generale Staf naar het ministerie van Buitenlandse Zaken, waar hij de fraaie titel 'directeur van het cijfer' kreeg. Vanuit die functie leidde hij een nieuwe generatie van tientallen militaire cryptologen op via een cursus aan de Hogere Krijgsschool. Tijdens de financiële crisis van de jaren dertig werd het bureau van Koot bij Buitenlandse Zaken opgeheven. Het zwaartepunt van de Nederlandse cryptologie verschoof toen naar Nederlands-Indië. Daar werden codes van de Japanse diplomatieke dienst en de keizerlijke marine gebroken.[16] Tijdens de Tweede Wereldoorlog werd het grote belang van cryptologie voor de nationale veiligheid door de Nederlandse regering in Londen erkend. Zoals nu algemeen bekend is, behaalden de Engelsen en Amerikanen doorslaggevend militair voordeel uit het kunnen lezen van versleutelde Duitse en Japanse berichten. Destijds hielden zij deze cryptoanalytische successen strikt geheim. De Nederlandse regering kreeg enig zicht op deze resultaten via kolonel Jacobus Verkuyl, een leerling van Koot die tijdelijk in Washington bij Amerikaanse codekrakers gestationeerd was.[17]

Na de oorlog vond er een herschikking plaats van de Nederlandse cryptologische activiteiten. Op 1 oktober 1947 werd aan Koot eervol ontslag verleend en verliet hij de militaire dienst. De code-'makers' kwamen terecht bij het Code Coördinatie Bureau (CCB) en de 'brekers' werden in 1947 samengebracht in afdeling VI van de MARID. Tot 1950 was kolonel Verkuyl directeur van beide organisaties. De onderlinge verbondenheid van makers en brekers was daarmee in de jaren vlak na de Tweede Wereldoorlog groot. Met de herverkaveling kwamen de codeactiviteiten geheel los te staan van de in 1949 opgerichte BVD, waar De Meijer werkte. Dat is terug te zien in zijn rapport.

Internationale successen

Bij het grote publiek zijn vooral de cryptoanalytische successen uit de Tweede Wereldoorlog bekend, die uit de Eerste Wereldoorlog veel minder. In 1974 werd openbaar dat de Britten tijdens de Tweede Wereldoorlog het geheime Enigmaverkeer van de nazi's mee hadden kunnen lezen.[18] De Enigma was een apparaat dat met behulp van mechanische rotors berichten relatief snel en makkelijk kon coderen. Het breken van de code heeft naar verluidt de oorlog met een aantal jaren verkort en miljoenen levens gered. De Meijer schreef zijn rapport in het midden van de jaren zestig, maar ook toen was het belang van cryptografie in de Nederlandse militaire literatuur al uitgebreid aan de orde gekomen. In 1955 publiceerde majoor J.W. Henning twee artikelen in de *Militaire Spectator*, waarin hij op basis van historische gebeurtenissen het belang van militaire berichtenbeveiliging overtuigend aantoont.[19] Hij beschrijft hoe in de Eerste Wereldoorlog de Duitse troepen de Slag bij Tannenberg (augustus 1914) wonnen ondanks een Russische overmacht. Dit kwam, volgens hem, doordat de Russen door slechte voorbereiding hun militaire berichten onversleuteld, 'in klare taal', verzonden. Henning beschrijft ook al de beslissende rol van cryptoanalyse tijdens de Tweede Wereldoorlog in de strijd van de Amerikanen tegen de Japanse marine, onder leiding van admiraal Yamamoto. Na de aanval op Pearl Harbor, in december 1941, brachten de Amerikanen de Japanse vloot in juni 1942 grote verliezen toe in de Slag bij Midway, dankzij voorkennis uit ontsleutelde berichten. Henning schrijft: 'Om dezelfde reden als Yamamoto de slag van Midway verloren had, verloor hij ook zijn leven.' De Amerikanen waren op de hoogte van de vluchtdetails van zijn geplande bezoek in juni 1943 aan de Salomonseilanden. Het werd hem fataal. Henning concludeert:

> Sedert Wereldoorlog I is, mede als gevolg van de uitgebreide toepassing van de electrische en electronische verbindingsmiddelen, welke de interceptie door de vijand vergemakkelijken, en

de gemaakte vorderingen op het gebied van wetenschappelijke cryptoanalyse, de cryptografie zeer in belangrijkheid gestegen. Zonder cryptografie is een moderne beweeglijke oorlogvoering, die zich over grote gebieden tot werelddelen uitstrekt, ondenkbaar.

Onderbelichte rol bij De Meijer

De Meijer werd midden jaren zestig gevraagd een interne geschiedenis te schrijven van de BVD. Hij werd gezien als de aangewezen kandidaat, juist omdat hij al zo lang in die wereld verkeerde. Volgens De Meijer werd met enige regelmaat een telefoon getapt, een microfoon geplaatst, een brief geopend of een informant uitgehoord, maar ontsleutelingen bij zijn veiligheidsdienst vermeldt hij niet. Het grote belang van verbindingsinlichtingen en van cryptoanalyse lijkt daarmee niet tot De Meijer te zijn doorgedrongen. Hij noemt weliswaar aan het begin van zijn rapport een aantal Nederlandse cryptoanalytische successen uit de Eerste Wereldoorlog, maar doet dat toch vooral indirect, door te citeren uit het dagboek van Van Woelderen. Hij laat het daarbij, zonder verdieping en zonder het grote strategische belang te benadrukken – iets wat Henning eerder al wel had gedaan. Het onderwerp keert niet terug in het rapport. Dat is enigszins begrijpelijk vanuit zijn achtergrond: in De Meijers dagelijkse praktijk waren inlichtingen afkomstig van personen, niet van signalen. Zijn specialisatie was HUMINT, niet SIGINT. In zijn rapport blijven de grote cryptoanalytische successen en het belang van berichtenbeveiliging daardoor onderbelicht.

Inmiddels zijn de Nederlandse codemakers en -brekers onderdeel geworden van de twee diensten, de AIVD en de MIVD. De codemakers van het CCB zijn uiteindelijk beland bij de AIVD, de codebrekers van de marine bij de MIVD. Beide diensten werken op dit vlak nauw samen. Het strategisch belang van cryptografie en digitale beveiliging voor de nationale veiligheid wordt nu breed erkend.

Naschrift

In de klas bij Koot

In 1930 volgde de marineofficier Johannes Nuboer[20] lessen cryptografie bij Henri Koot. Het onderricht was privé, want in dat jaar werd de cursus niet gegeven aan de Hogere Krijgsschool. Mogelijk als tegenprestatie heeft Nuboer de lessen van Koot uitgeschreven in een dictaat.[21] Het bevat een aantal oefeningen van Koot voor zijn leerlingen. Hieronder staan er twee, voor wie zelf een poging wil wagen en zich daarmee bij Koot in de klas kan wanen. De versleutelde teksten zijn in het Frans en in het Engels. De oplossingen staan op pagina 285 en 286.

1 Enkelvoudige vervanging

Gegeven: In een verondersteld oorlogsgeval Nederland-België vangt een tegen KNOCKE – HEYST – ZEEBRUGGE verkennend Nederlandsch eskader het volgende cryptogram op, vermoedelijk afkomstig van een in die kuststrook gelegen Belgisch waarnemingsstation.
Gevraagd: Ontsluiering v/h cryptogram.

ODVAK FHYVD AADDA CUVMO KRFYA
DFMIV NNAKU AMVPD FEPAE ACVNU
DLADA OBQAO KAMVD AOBQA OKAMN
KADNA MVHKA MADEA VEFUD EULAV
RAEYF IMAKR VNUFD LODAE KVDLA
BOCAA VYQFK UZFDD

2 Dubbele verplaatsing

Gegeven: Cryptogram. Het gaat om een onderliggend engelsch bericht.
Gevraagd: Ontsluiering v/h cryptogram. Dubbele verplaatsing, compleet figuur.

WVGAE EGENL TFTOH TEIEF RBTSE
INENG ONWRM GXIXN GOITN ROMRO
ESPAL HNEAC UDNNH DERME