GEHEIME BERICHTEN EN AGENTEN

Luitenant-kolonel b.d. G.J. Huijsman, met dank aan de heer Paul Reuvers

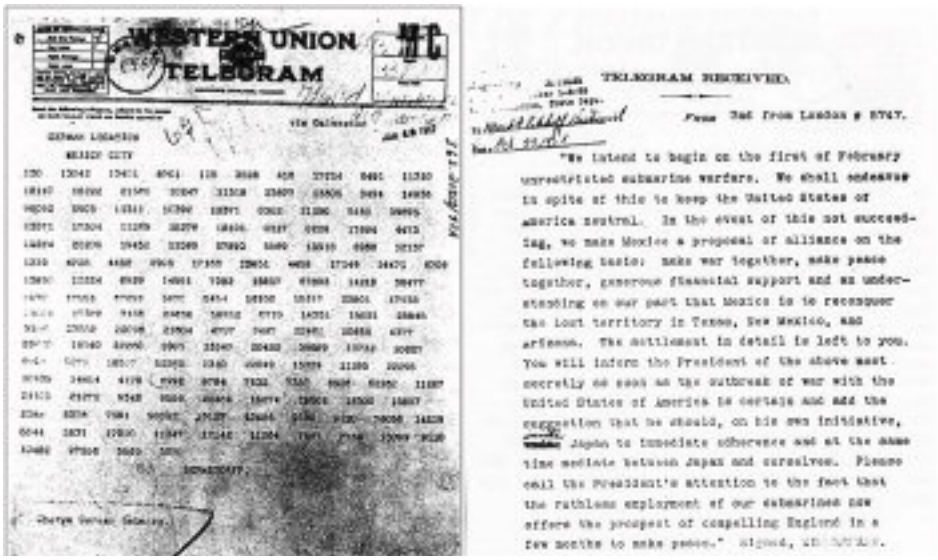
Lkol Vbdd b.d. Gerrit Jan Huijsman heeft een groot deel van zijn dienstijd besteed aan de planning van verbindings- en EOV-systemen. Na zijn KMA-tijd (promotie 59) was hij instructeur bij de School Reserve Officieren Verbindingsdienst (SROV) en daarna paraat bij 108 Verbindingsbataljon. Al gauw kwam hij bij het bureau Plannen van de Inspectie Verbindingsdienst en Afdeling TE van de Generale Staf, waar hij werkte aan de indeling van nieuwe radioapparatuur en waar de eerste stappen werden gezet op weg naar ZODIAC. Later volgde een plaatsing bij de Defensiestaf waar hij veel internationale contacten op EOV-gebied onderhield. Daarna was hij onder meer projectofficier EOV bij de afdeling Plannen van de Landmachtstaf.

Dit artikel geeft een kort historisch overzicht van het belang van de veilige overdracht van geheime informatie tussen overheidsinstanties, geheime agenten en hun opdrachtgevers en, in het bijzonder, eenheden van de Koninklijke Landmacht gedurende de Koude Oorlog. Ook wordt kort stilgestaan bij de destijds uiterst geheime operatie Gladio. De huidige stand van zaken valt buiten de scope van dit artikel.

HET BELANG

In januari 1917 speelde de Britse geheime dienst de klare tekst van een telegram van de Duitse minister van Buitenlandse Zaken aan de Duitse ambassadeur in Mexico in handen van het Amerikaanse ministerie van Buitenlandse Zaken. De inhoud van dit telegram (zie afbeelding 1) werd gepubliceerd in vele Amerikaanse kranten en veroorzaakte een storm van verontwaardiging.

De Verenigde Staten waren al geruime tijd aan het bakkeleien met Mexico, waar gewapende bendes de belangen van de Amerikanen schaadden. Ook waren de verhoudingen met Japan gespannen, onder meer vanwege de Japanse pogingen om in Californië een vlootbasis te krijgen. De Duitse keizer Wilhelm wilde dit ongenoegen uitbuiten en liet zijn minister van Buitenlandse Zaken Zimmerman een telegram sturen aan zijn ambassadeur in Mexico. Keizer Wilhelm hoopte de Verenigde Staten, met een dreiging vanuit Mexico en Japan, te bewegen neutraal te blijven en niet in oorlog te komen met Duitsland. Het initiatief werkte averechts en was er mede de oorzaak van dat de Verenigde Staten in de Eerste Wereldoorlog betrokken werden, met fatale gevolgen voor Duitsland. Hoe is dit zo gekomen? Barbara Tuchman beschrijft het verhaal gedetailleerd in haar boek *The Zimmermann Telegram*. Het begon eigenlijk toen het Verenigd Koninkrijk als eerste offensieve daad, nadat het met Duitsland in oorlog geraakte, de trans-Atlantische kabels doorsneed die Duitsland met het Amerikaanse continent verbonden. Duitsland was hierdoor voor diplomatiek verkeer aangewezen op radioverbindingen, die uiteraard eenvoudig konden worden onderschept. De krachtige langegolf machinezender die vanuit Nauen, in de buurt van Berlijn, gebruikt werd, was overal op de wereld te ontvangen (zie afbeelding 2).



Afbeelding 1 Het Zimmermann-telegram in code en gedecodeerd (foto Paul Reuvers)

Afbeelding 2 Het Langegolfradiostation in Nauen bij Berlijn, dat model heeft gestaan voor het Nederlandse Langegolfstation bij Kootwijk (foto Paul Reuvers)

De grote aantallen gecodeerde telegrammen, waarvan men wist dat ze vaak dezelfde inhoud hadden, althans delen ervan, maakten het mogelijk dat Britse cryptologen geleidelijk aan over de gebruikte code konden beschikken. Daarbij kwam nog dat in Brussel een Engelse geheim agent werkzaam was die gedeelten van de diplomatieke codeboeken kon overschrijven en doorspelen naar Londen. Het decoderen van het in cijfergroepen opgestelde bericht was snel gedaan. Het werd nu zaak om het op het juiste moment door te spelen aan de Amerikanen die, president Wilson voorop, er eigenlijk niets voor voelden in de Europese oorlog betrokken te worden.
Duitsland liet in het gewraakte telegram blijken Mexico en Japan in de oorlog te willen betrekken en hun grote delen van de Verenigde Staten aan te bieden als Duitsland de oorlog zou winnen. En daarvan was het dat moment overtuigd. De onbeperkte duikbootoorlog die ook in het telegram werd aangekondigd zou Engeland snel op de knieën brengen. Hoewel aanvankelijk de authenticiteit van het bericht werd betwijfeld, gaf de Duitse minister volmondig toe dat hij het had verzonden. Er moesten wel nog enkele trucjes gevonden worden om te verdoezelen hoe men het gecodeerde bericht had ontcijferd. Deze gebeurtenis onderstreept het belang van de veilige overdracht van geheime informatie. In de loop van de moderne geschiedenis zullen meer voorbeelden volgen.

ONTWIKKELINGEN

Het is dan ook begrijpelijk dat regeringen en vooral militaire organisaties geworsteld

hebben met het veilig verzenden van geheime informatie. Vaak werd daarbij in eerste instantie gezocht naar een veilige transporteur, zoals een betrouwbare ordonnans of koerier. Ook postduiven werden gebruikt omdat de kans om een duif tijdens de missie te onderscheppen niet groot kon zijn. De betrouwbare ordonnans bleek echter niet altijd zo betrouwbaar en kon worden gepakt en worden gedwongen de informatie in klare taal af te staan. Al eeuwen geleden zocht men naar manieren om de inhoud van boodschappen te versluieren. De Romeinen veranderden bijvoorbeeld alle letters met een andere letter uit het alfabet volgens een afgesproken patroon en met behulp van een verschuifregel. Dit wordt een substitutiemethode genoemd omdat de letters zelf worden veranderd, maar de volgorde niet. Dan is er nog de permutatiemethode waarbij ook de volgorde van de letters wordt veranderd. In de loop van de twintigste eeuw dienden zich technische oplossingen aan, maar het was nog oppassen geblazen, zoals het Duitse Enigma-debâcle illustreerde. Daarover later meer.

ONE TIME PAD (OTP)

Een methode die waarschijnlijk nog in gebruik is en als uitermate veilig kan worden aangemerkt, is die waarbij letters uit klare tekst door cijfers worden vervangen, waarna de cijfers met behulp van een sleutel, die na gebruik direct vernietigd moet worden en alleen bij beide partijen bekend is, een rekenkundige bewerking ondergaan. De gebruiker en zijn chef beschikken over een boekje met losse blaadjes, een soort blocnote, met de sleutel. Dit is de zogenaamde *One Time Pad* (OTP) methode. Het spreekt vanzelf dat deze manier van coderen , hoewel zeer veilig, tijdrovend is, terwijl de distributie zeer omslachtig is.

GEDICHTENCODE

De geheime agenten die vanuit Engeland naar het vaste land van Europa werden gezonden, maakten aanvankelijk gebruik van een 'gedichtencode' (*poem code*). Ze moesten de tekst van een gedicht onthouden, bijvoorbeeld *"Toen onze mop een mopje was…"*, en de letters daaruit gebruiken om de te verzenden tekst te vercijferen en de te ontvangen informatie te ontcijferen. Het mag duidelijk zijn dat deze methode in de praktijk niet veilig bleek te zijn. Bij gevangenneming konden de agenten door foltering worden gedwongen het gedicht prijs te geven waarna alle informatie kon worden achterhaald. Een OTP-systeem met de code gedrukt op zijde bleek uiteindelijk effectiever. Het zijden doekje kon op het lichaam worden verborgen en in noodgevallen snel worden verbrand.

TACTISCHE CODES

Voor tactisch operationeel gebruik werden al heel lang tactische codes gebruikt, die relatief eenvoudig te ontcijferen waren en die daardoor een beperkte tijd bruikbaar waren. Een voorbeeld is de Slidex (zie afbeelding 3) die in de Tweede Wereldoorlog door het Britse en Canadese leger werd gebruikt en na de oorlog ook nog wel bij de Koninklijke Landmacht, gelijktijdig met een eenvoudige manier om berichten te waarmerken.

Afbeelding 3 De Slidex verschafte een kortstondige beveiliging (foto Paul Reuvers)

GLADIO

Het is niet algemeen bekend dat na de oorlog in ons land potentiële geheime agenten werden getraind in het gebruik van radioapparatuur met bijbehorende vercijferapparatuur. Het betreft operatie Gladio. Wikipedia vermeldt daarover:
'Operatie Gladio is een in 1952 gestart geheim 'stay behind' netwerk in Italië, gesponsord door de CIA en de NAVO, om de communistische invloed zowel in Italië als in andere landen te neutraliseren.'
De eerste voorbereidingen werden al in 1947 getroffen. Hoewel de term Gladio alleen slaat op het Italiaanse deel, worden ook de soortgelijke netwerken die in andere landen bestonden veelal met die naam aangeduid. Uit recent onderzoek is bekend geworden dat soortgelijke netwerken in geheel West-Europa actief en aan elkaar gelinkt zijn geweest. In ieder geval was Gladio actief in België, Denemarken, Duitsland, Frankrijk, Griekenland, Luxemburg, Nederland en ook in Zwitserland. De oorsprong van deze organisaties lag in de Tweede Wereldoorlog. Tot ongeveer het midden van de jaren tachtig werd het met Operatiën en Inlichtingen (O&I) aangeduid. Oorspronkelijk was het netwerk alleen bedoeld voor het noodzakelijke berichtenverkeer met de regering in ballingschap, maar geleidelijk werd het ook een gevechtsorganisatie. De radioapparatuur die bestond uit kleine zendontvangers werd in Nederland onder meer door de firma Philips vervaardigd. In het museum Verbindingsdienst zijn er enkele voorbeelden van te zien (zie afbeelding 4).

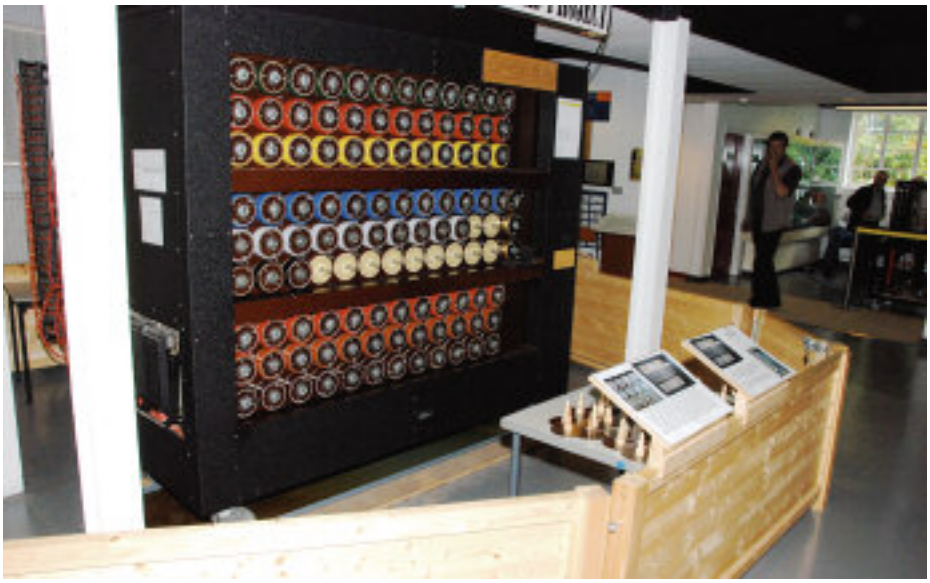
SCHIJVEN-METHODE

Aan het eind van de 19e eeuw werd een tabellen- of schijvenmethode bedacht. Hierbij werd al spoedig gebruikgemaakt van een speciale codeer- en decodeermachine. De letters van het alfabet werden, door elkaar gegooid, op de rand van een ronde schijf gezet. Daarna werden nog enige van zulke schijven gemaakt, waarop het alfabet steeds op een andere manier was verhaspeld (zie afbeelding 5).

Afbeelding 5 De schijvenmethode werd in verschillende vercijferapparaten toegepast, waaronder Enigma (foto Paul Reuvers)

Afbeelding 4 Communicatiemiddelen ten behoeve van de geheime operaties van O&I (foto Paul Reuvers)

Zo ontstonden verschillende schijven met elk een andere tabel.
De Enigma is waarschijnlijk de bekendste cryptomachine die dit principe toepaste. De Duitse Wehrmacht was ervan overtuigd dat er een niet te breken codering mee verricht kon worden, terwijl in werkelijkheid de Engelse inlichtingendienst met hulp van de Polen en dankzij procedurefouten van de Duitsers gauw in staat was de code te breken (zie afbeelding 6).



Afbeelding 6 Een replica van de zogenaamde Bombes waarmee men in Bletchley Park de Enigmacode kon breken (foto Paul Reuvers)

Het was vooral Churchill die het belang van geheimhouding van deze ontcijfering beklemtoonde. Men zegt dat hij zijn kennis over het door de Duitsers voorgenomen bombardement van Coventry geheim hield, terwijl hij daarvan door middel van Enigmaberichten op de hoogte was. Er werd zeer veel moeite gedaan om de Engelse kennis van Enigma geheim te houden. Slechts een handvol militaire commandanten maakten gebruik van deze ultra geheime inlichtingen. Zij mochten de informatie slechts sporadisch gebruiken en uitsluitend na een zorgvuldige afweging van de voordelen en de risico's. Deze methode van versluiering van geheime informatie, die wordt aangeduid als *off line* becijfering, is bijzonder tijdrovend en daardoor niet erg praktisch.

Afbeelding 7 De TSEC-KL7 (Adonis) was lange tijd bij de Koninklijke Landmacht in gebruik (foto Paul Reuvers, met dank aan Museum Verbindingsdienst)

Ook de Koninklijke Landmacht gebruikte off line vercijfersystemen met schijven, zoals de TSEC-KL7 en de Hagelin codeermachine (zie afbeelding 7).

De TSEC-KL7, ook wel aangeduid als Adonis, produceerde na invoering van de cryptosleutel een cryptotekst in de vorm van een papierstrook waarop in groepen van vijf de cryptotekst werd afgedrukt. De verzending geschiedde doorgaans met een radiozender met morsetelegrafie. De auteur herinnert zich nog goed de geheimzinnige sfeer die om deze apparaten hing. Bij oefeningen waren vercijferaars achter een scherm bezig met hun arbeidsintensieve bezigheden. Het was vaak ondankbaar werk dat vanwege het tijdrovende karakter ervan steeds minder werd toegepast. Vooral toen on line vercijfermethoden hun intrede deden.

VERNAM CIPHER

De invoering van telexverbindingen in de jaren zestig van de vorige eeuw maakte het mogelijk de inhoud van berichten met eenmalige te gebruiken cryptoband te vercijferen. Dit systeem was omstreeks 1917 uitgevonden door Gilbert Vernam in de Verenigde Staten die werkzaam was bij AT&T Bell Labs. Het ging in feite om een OTP-systeem en het was uitermate veilig, mits aan enkele strikte voorwaarden werd voldaan. De eerste on line vercijferapparaten bij de Koninklijke Landmacht waren van Nederlandse origine. Het begon met een Ecolex-familie bestaande uit Ecolex 1, 2, 4 en 10 (zie afbeelding 8).

Afbeelding 8 De Ecolex 2, de voorloper van een hele familie online-vercijfer apparatuur geproduceerd door de Nederlandse firma USFA (foto Jan Lispet)

Aanvankelijk waren er ernstige problemen; de cryptoband moest in de pas blijven met de klaretaal-band, anders ontstond er wartaal. Elke stoorpuls op de verbinding veroorzaakte dit euvel. De Ecolex 2 werd opgevolgd door de Ecolex 4 (zie afbeelding 9), waarbij de cryptoband ook bij verstoringen in de verbinding gesynchroniseerd bleef doorlopen.

Een ander probleem kwam nu aan het licht. De cryptobanden moesten uiteraard zeer zorgvuldig worden gedistribueerd om te waarborgen dat uitsluitend de beide gebruikers van de beveiligde verbinding er over beschikten. De vernietiging van gebruikte cryptoband was wel geregeld, want de Ecolex 4 sneed de band na gebruik automatisch in onbruikbare stukken. Veel oldtimers bij de Verbindingsdienst herinneren zich de nukken van deze machine. De ponsbandlezer in de vorm van een soort gootje moest nauwkeurig worden afgeregeld met behulp van een piepkleine schroevendraaier, dit was een lastig karwei waar de dienstplichtig telexist nogal moeite mee had, vooral onder stress- situaties als er in een *Tape Relay* Centrum, waar er een stuk of twaalf in een nauwe ruimte naast elkaar stonden opgesteld ineens een groot aanbod van telexberichten optrad. De correcte distributie van de zogenaamde cryptobanden was altijd een grote zorg. Zonder de juiste cryptoband geen verbinding.
Een uitkomst bleek de invoering van de Tarolex die de cryptobanden overbodig maakte; (zie afbeelding 10) het werd een kwestie van een instelling van duimwielen aan beide zijden van de verbinding. De invoering van linkvercijfering bij het project Zodiac werd tenslotte voor telexverbindingen de ultieme oplossing; het berichtenverkeer kon in een latere fase van Zodiac zelfs geheel bij de gebruiker zelf neergelegd.

MODERNE SYSTEMEN

Moderne systemen berusten geheel op digitale technieken waarbij vercijfering van de informatie relatief eenvoudig is. Al gauw werd een vercijferingsmethode ontwikkeld die algemeen wordt toegepast bij het ver-

Afbeelding 9 De Ecolex 4, USFA produceerde er in 1959-1963 750 voor de Koninklijke Landmacht (foto Paul Reuvers)

zenden van e-mails en teksten via internet. Dit systeem, *Pretty Good Privacy* (PGP), is voor overheden niet veilig genoeg, maar het biedt particulieren een redelijk goede bescherming.

TENSLOTTE

Door de eeuwen heen heeft men geworsteld met het geheimhouden van informatie die niet voor anderen bestemd was. Aanvankelijk was de meest betrouwbare wijze het toevertrouwen van dergelijke informatie aan koeriers. Later werden er eenvoudige codes bedacht, die voor een korte periode wel veiligheid boden. Op diplomatiek niveau werden al gauw codeboeken toegepast waarin voor elk tekstbegrip een cijfer was opgenomen. De distributie van dit soort codemateriaal was echter een bijzonder moeilijke zaak. Altijd moest er rekening mee worden gehouden dat het codemateriaal in verkeerde handen zou kunnen vallen. Een goede oplossing, mits goed toegepast, bleek de *One Time Pad* methode te zijn; deze was echter arbeidsintensief en dus traag.

Er zijn voorbeelden waarbij het ontcijferen van geheime codeberichten grote invloed heeft gehad op de loop van de geschiedenis. Het Zimmermann-telegram is er een goed voorbeeld van. Van recentere tijd is het decoderen van Enigma-berichten door de geallieerden, zonder dat de Duitsers daar tot het einde van de oorlog weet van hadden. Door zorgvuldig van deze informatie gebruik te maken konden de geallieerden de U-boot-tactiek van de Duitsers volgen en dat inzicht in hun voordeel gebruiken. Ook op andere strijdtonelen, zoals in Noord-Afrika en direct na de landing in Normandië, verschafte informatie uit Enigma-berichten vaak positionele voordelen. Het is des te merkwaardiger dat het Duitse Ardennen-offensief een grote verrassing was.

Winterbotham in zijn boek *Project Ultra*, heeft hiervoor geen verklaring. Gebruikten de Duitsers uitsluitend landlijnen? Hadden ze een vermoeden? Ook in andere literatuur waarin het Duitse gezichtspunt tijdens dit offensief wordt beschreven, wordt daarvan met geen woord gerept.

Afbeelding 10 De Tarolex maakte de cryptoband overbodig. In 1966-1967 werden 150 Ecolex 4 hiervoor omgebouwd (foto Paul Reuvers)

LITERATUUR

- *The Codebreakers*, David Kahn
- *The Zimmermann Telegramm*, Barbera Tuchman
- *The Ultra Secret, Project Ultra*, F.W. Winterbotham
- *Between Silk and Cyanide, a codemaker's war*, Leo Marks
- *Seizing the Enigma, The race to break the German U-boat codes*, David Kahn
- *Hitlers Ardennes Offensive, The German view of the battle of the Bulge*. Edited by Danny S. Parker

BRONNEN

- Museum Jan Corver http://www.jancorver.org/
- Museum Verbindingsdienst http://www.museumverbindingsdienst.nl/
- Crypto Museum http://www.cryptomuseum.com/