(17

VERTROUWELIJK TOT DE VERGADERING VAN DE BEGELEIDINGSCOMMISSIE

VAST COMITÉ VAN TOEZICHT OP DE INLICHTINGEN EN VEILIGHEIDSDIENSTEN

Notitienummer 2020.275

De gevolgen van buitenlandse monitoringnetwerken voor de Belgische inlichtingendiensten: de zaak CRYPTO AG, RUBICON en MAXIMATOR

.

Eindverslag – 13 oktober 2022

INHOUDSTAFEL

I. INLEIDING

I.1. AANLEIDING VAN HET TOEZICHTONDERZOEK EN ONDERZOEKSCOPE

In de eerste helft van 2020 werden in de pers onthullingen gedaan over het zogenaamde RUBICON-spionageprogramma. Uit bepaalde persberichtgeving bleek dat bij het begin van de jaren '60 van de vorige eeuw de Amerikaanse inlichtingendiensten CIA en NSA en de Duitse inlichtingendienst *Bundesnachrichtendienst* (BND) belangen hadden genomen in de onderneming CRYPTO AG. Uiteindelijk werden de *Central Intelligence Agency* (CIA) en de BND zelf exclusieve eigenaar van dit bedrijf.

Het bedrijf CRYPTO AG vervaardigde apparatuur voor het tot stand brengen van gecrypteerde communicatie.

De Amerikaanse inlichtingendiensten CIA en NSA en de Duitse inlichtingendienst BND konden door hun zeggenschap binnen de betrokken firma gedurende tientallen jaren berichten meelezen, die verstuurd werden via deze CRYPTO-coderingsapparatuur door een groot aantal landen en instellingen die deze technologie hadden aangekocht. Dit spionageprogramma werd RUBICON genoemd.

In het kader van dit spionageprogramma werd niet alleen communicatie onderschept van vijandige mogendheden, maar ook van bevriende en zelfs geallieerde NAVO-landen.

De zaak RUBICON situeert zich in hoofdzaak in de jaren '70, '80 en begin van de jaren '90 van de 20e eeuw, met andere woorden gedurende een belangrijk deel van de Koude Oorlog.

Het huidig toezichtonderzoek heeft niet de intentie heeft om het afluisterschandaal AG CRYPTO/RUBICON in zijn totaliteit te behandelen. Het gaat enkel na of de Belgische inlichtingendiensten VSSE en ADIV, een aandeel hadden in het betreffende afluisterschandaal, of er door getroffen werden.

Lopende het onderzoek kwam een tweede luik aan het licht: in de context van het afluisterschandaal werd immers door de Nederlandse academicus en expert computerbeveiliging prof. Bart Jacobs in een wetenschappelijk artikel het bestaan onthuld van een geheime SIGINT-alliantie tussen een aantal Europese landen[1]. Dit samenwerkingsverband was gekend onder de naam MAXIMATOR. Huidig toezichtonderzoek gaat in het laatste deel na op welke wijze België betrokken was bij dit geheime samenwerkingsverband.

I.2. ONDERZOEKSVERLOOP EN METHODOLOGIE

De onderzoeksbeslissing die de basis vormde voor dit onderzoek werd door het Vast Comité I goedgekeurd op 30 september 2020.

---

1 "Maximator: European signals intelligence cooperation, from a Dutch perspective, *Intelligence and National Security*", Routledge, Volume 35, Number 5, August 2020, pp.659-668.

Tussen het laatste kwartaal van 2020 en het eerste kwartaal van 2022 werden wetenschappelijke literatuur en andere open bronnen geconsulteerd, en diverse onderzoeksdaden gesteld. Ook werd een onderhoud georganiseerd met de verantwoordelijken van het cryptomuseum in Eindhoven (Nederland).

I.3. BEVOEGDHEID VAN HET VAST COMITÉ I

Artikel 33 van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse stelt dat het Vast Comité I onderzoeken instelt naar de activiteiten en de werkwijze van de inlichtingendiensten.

I.4. GEEN TOESTEMMING VAN DE FOD BUITENLANDSE ZAKEN

Het Vast Comité I heeft wettelijk gezien niet de mogelijkheid om toezicht uit te oefenen op andere diensten dan de VSSE en ADIV (en op het OCAD, samen met het Vast Comité P).

Uit het toezichtonderzoek bleek dat AG CRYPTO-toestellen ook door andere Belgische diensten of instanties zou kunnen zijn gebruikt, zo bijvoorbeeld voor diplomatieke correspondentie.

Bij brief van 3 maart 2020 werd dan ook de toenmalige minister van Buitenlandse Zaken van het huidige toezichtonderzoek op de hoogte gebracht door het Vast Comité I en werd toestemming gevraagd om alle nuttige inlichtingen betreffende het afluisterschandaal te bekomen van de FOD Buitenlandse Zaken. Op deze vraag van kwam geen reactie.

I.5. PARLEMENTAIRE AANDACHT

Het Vast Comité I kon nagaan dat in België in de maand februari 2020 bij vier gelegenheden parlementaire vragen gesteld die betrekking hadden op het afluisterschandaal.[2] Het betrof meer in het bijzonder:

- de vraag vanwege volksvertegenwoordiger Stefaan Van Hecke aan minister Philippe Goffin (Buitenlandse Zaken en Defensie) over "De afluisterpraktijken van de VS d.m.v. apparatuur van CRYPTO AG; [3]
- de vraag vanwege volksvertegenwoordiger Chris Verduyckt aan minister Philippe Goffin (Buitenlandse Zaken en Defensie) over "De afluisteroperatie door middel van CRYPTO-apparaturen";[4]

---

2 Verschillende parlementaire vragen, gericht aan de Nederlandse minister van Binnenlandse Zaken en Koninkrijksrelaties werden als volgt beantwoord in de Nederlandse Tweede Kamer: "*In het openbaar worden geen uitspraken gedaan over het kennisniveau en de werkwijze van de inlichtingen- en veiligheidsdiensten.*", Tweede Kamer der Staten generaal, vergaderjaar 2019 – 2020, vraag 2640 van 14 april 2020.

3 55003359C van 19/02/2020.

4 55003428C van 19/02/2020.

- de vraag vanwege volksvertegenwoordiger Stefaan Van Hecke aan Koen Geens, vice-eerste minister en minister van Justitie en Regie der Gebouwen over "De afluisterpraktijken van de VS d.m.v. apparatuur van CRYPTO AG;[5]
- de vraag vanwege volksvertegenwoordigster Kattrin Jadin aan Koen Geens, vice-eerste minister en minister van Justitie en Regie der Gebouwen over "De spionagezaak";[6]

Afgaand op de antwoorden van de betrokken ministers kon alvast op dat ogenblik worden vastgesteld dat, wat betreft de VSSE, in de voorbije 10 jaar geen AG CRYPTO-materiaal werd gebruikt, maar dat voor de periode voordien nog één en ander zou worden nagetrokken. Er werd in de ministeriële antwoorden gewezen op de toenemende complexiteit van de betrokken technologieën, wat het moeilijk maakt om over te waken dat er geen *backdoors* werden geïnstalleerd in de betrokken apparatuur. Voor wat betreft Defensie en ADIV in het bijzonder bleek dat toestellen in de jaren '50 tot midden de jaren '60 zouden zijn gebruikt om operationele communicaties in het buitenland te verzekeren, maar dat naderhand Defensie en ADIV ni het bijzonder enkel encryptietoestellen aankocht die door de NAVO en de EU waren goedgekeurd.

I.6. POLITIEKE IMPLICATIE IN HET BUITENLAND

Op 12 mei 2021 werd in Zwitserland via een officieel communiqué het ontslag aangekondigd van Jean-Philippe Gaudin, de directeur van de *Service de renseignement de la Confédération* (SRC). Hoewel het communiqué stelt dat het aftreden van het hoofd van de Zwitserse dienst gebeurde *in onderling overleg*, werd dit ontslag in de pers, onder meer, gekoppeld aan het afluisterschandaal, nu het hoofd van de Zwitserse inlichtingendienst zou hebben nagelaten de politieke verantwoordelijken op de hoogte te brengen van het geheim akkoord tussen de Amerikaanse en Duitse inlichtingendiensten.[7]

In Denemarken werd in augustus 2020 Lars Findsen, het hoofd van de *Forvarets Efterretningstjeneste* (FE), de Deense buitenlandse militaire inlichtingendienst, een tijdlang geschorst en gearresteerd op verdenking van het lekken van staatsgeheimen. Ook dit incident wordt door bepaalde pers deels gelinkt aan het afluisterschandaal,[8] hoewel deze bewering volgens het Comité niet echt gegrond lijkt. Wel kadert deze schorsing in een brede discussie over de toelaatbaarheid van verregaande SIGINT-samenwerking tussen Denemarken en de US, en wijst de schorsing erop dat in de schaduw van het AG CRYPTO-schandaal, de verhouding tussen de inlichtingendiensten en de politieke Deense overheden een tijdlang zeer gespannen waren.

---

5 55003358C van 19/02/2020.

6 55003380C van 19/02/2020.

7 Le Départ du chef du renseignement suisse dû à des tensions avec Viola Ahmerd, RTS, 12 mei 2021.

8 Zie bijvoorbeeld: We know about the US-Danish spy collaboration, www.Intelnews.org/2021/06/01/01/01-3012, 1 juni 2021. Zie ook: www.ad.nl/binnenland/oud-mivder-maakte-onderdeel-uit-van-spionageschandaal, 30 januari 2022.

I.7. MOEILIJKHEDEN EN COMPLEXITEIT BIJ HUIDIG TOEZICHTONDERZOEK

Het toezichtonderzoek werd lopende de onderzoeksverrichtingen enigszins bemoeilijkt door het gegeven dat in de marge van de AG CRYPTO-affaire ook de compromittering van andere aan België geleverde toestellen opdoken. Het gaat in hoofdzaak, maar niet uitsluitend over de AROFLEX- en de BEROFLEX-toestellen die geproduceerd werden door de firma Philips. De problematiek inzake AROFLEX/BEROFLEX is complex en valt voor een groot deel buiten het toezichtonderzoek.[9] Het Vast Comité I besliste dus om in het kader van huidig onderzoek, dat al complex is, desbetreffende toestellen buiten beschouwing te laten.[10]

Verder bleek dat het afluisterschandaal maar een relatief beperkte persaandacht genoot, wat het onderzoek bijkomend bemoeilijkte.

Daarnaast waren bepaalde bronnen bijzonder schaars, wat zeker het geval was met info over het MAXIMATOR-netwerk (zie verder - DEEL III) waar vele persartikels en bronnen in werkelijkheid bijna exclusief gebaseerd zijn op één enkele wetenschappelijke bijdrage, namelijk die van de reeds vermelde Nederlandse professor Bart Jacobs in een Brits wetenschappelijk tijdschrift.[11]

Tot slot moet ook worden gewezen op het lange tijdsverloop tussen de feiten startend in de jaren '60 en het moment van het toezichtonderzoek. Boekhoudkundige documenten (zoals bv. bestelbonnen) van de aanschaf van de toestellen zijn nog nauwelijks aanwezig, en evenmin waren nog werkende communicatieapparatuur van die periode zelf bij de diensten aanwezig, wat verhinderde dat fysiek kon worden nagegaan welk operationeel specifiek toestel al dan niet zou zijn afgezwakt/gecompromitteerd.

9 De AROFLEX-versie zou zeer betrouwbaar zijn, terwijl de BEROFLEX- toestellen afgezwakte (en dus minder betrouwbare) versies van de AROFLEX waren.

10 In haar (geclassificeerd) antwoord aan het Vast Comité I maakt zowel de ADIV als de VSSE wel melding van beide toestellen.

11 Bart Jacobs, *'MAXIMATOR, European signals intelligence cooperation from a Duitch perspective, Intelligence and National Security*, volume 35, nummer 5, augustus 2020, 659-668, en ook consulteerbaar op *https://tandfonline.com.*

II. SITUERING VAN HET ONDERZOEK

II.1. VOORAFGAANDELIJK: HET BELANG VAN CRYPTOGRAFIE EN CRYPTOANALYSE

Cryptografie is activiteit die erin bestaat om een bericht door de verzender van dat bericht dermate te verhullen op basis van een code die alleen de ontvanger en de verzender van het bericht, zodanig dan enkel de ontvanger de inhoud kan zien.

Cryptografie werd aanvankelijk voornamelijk toegepast in een context van oorlogsvoering, terwijl dit later werd uitgebreid naar een ruimer scala van gevoelige berichten (zoals bijvoorbeeld bij diplomatieke correspondentie).

Sinds cryptografie bestaat, is ook **cryptoanalyse** ontstaan. Het doel van cryptoanalyse bestaat er in om versleutelde berichten om te vormen tot verstaanbare berichten. Elk versleuteld bericht kan in beginsel worden ontcijferd. Cryptoanalyse vereist vanzelfsprekend meer tijd en inspanningen, die recht evenredig zijn met de complexiteit van de wijze waarop berichten werden gecrypteerd.

De mogelijkheden om berichten steeds complexer te crypteren en decrypteren kwamen de laatste decennia in een stroomversnelling door het mechanisch, maar vooral het elektronisch versleutelen van berichten.

II.2. RUBICON: EEN ZOVEELSTE AFLUISTERSCHANDAAL IN EEN LANGE REEKS VAN SCHANDALEN

Het besproken afluisterschandaal kan worden toegevoegd aan een indrukwekkende reeks van spionageschandalen die aan het licht kwamen in het begin van deze 21e eeuw. Het Vast Comité I, dat aan de meeste van deze schandalen een toezichtonderzoek wijdde, somt hier kort de belangrijkste op:

II.2.1. Het elektronisch afluisterpproject ECHELON[12] [13] [14]

ECHELON is het afluisterprogramma dat sedert de jaren '70 operationeel is en voor de zogenaamde 5 EYES alle satellietcommunicatie opvangt en filtert op basis van vooraf ingevoerde trefwoorden, targets, namen of telefoonnummers. Dit spionageprogramma kwam onder de aandacht nadat het Europese parlement een tijdelijke onderzoekscommissie had opgericht om onderzoek uit te voeren naar de omvang van interceptie-activiteiten.

---

12 Onderzoek over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, ECHELON genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België, Activiteitenverslag 1999, Vast Comité I, pp. 24 – 51.

13 Aanvullend verslag over de wijze waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een netwerk « ECHELON » genaamd, voor het onderscheppen van communicaties, Aanvullend activiteitenverslag 1999, Vast Comité I, pp. 27 – 60.

14 Syntheseverslag van het onderzoek over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, « ECHELON » genaamd, voor het onderscheppen van telecommunicatie in België, Activiteitenverslag 2000, Vast Comité I, pp. 27 – 60.

II.2.2. Het bespioneren van het Justus Lipsiusgebouw in Brussel 15

In 2003 werd door het veiligheidsbureau binnen de Europese Raad vastgesteld dat verscheidene delegaties van de lidstaten die hun kantoor hadden in het gebouw, waaronder die van Spanje, Duitsland, Frankrijk, Italië, het Verenigd Koninkrijk en Oostenrijk in het Justus-Lipsius-gebouw telefonisch werden afgeluisterd. De officiële vaststellingen gebeurde op 28 februari 2003, maar er waren eerder al geruchten in die zin. Het afluisteren zou zijn gebeurd tussen 1995 en 2003. De Veiligheid van de Staat verleende haar medewerking bij het onderzoek naar het incident. Na zeven jaar strafonderzoek werd het dossier door het Federaal Parket zonder gevolg geklasseerd. In 2008 volgde een tweede schandaal, dit op basis van door Edward Snowden vrijgegeven documenten, waaruit zou moeten blijken dat pogingen werden ondernomen om het Justus Lipsius-gebouw af te luisteren vanuit een voor de NSA gereserveerd NAVO-lokaal in Evere.

II.2.3. Het afluisteren van de firma SWIFT[16]

SWIFT is een bedrijf dat het internationaal betalingsverkeer van duizenden financiële instellingen uit 200 landen regelt. Het hoofdkwartier van het bedrijf bevindt zich in Terhulpen (Waals-Brabant) en zou het slachtoffer geworden zijn van een inbraak in haar computersystemen.

II.2.4. De hacking van het computernetwerk van Buitenlandse Zaken

In 2013 werd ADIV er door de CIA van op de hoogte gebracht dat Russische *hackers* via een Snake-virus erin geslaagd waren computers van Buitenlandse Zaken te kraken. Daarop probeerden de ADIV, de VSSE en de FCCU na te gaan welke documenten er werden onderschept. Ook dit dossier werd strafrechtelijk geseponeerd.

II.2.5. Het onthullen van het computerprogramma PRISM door de NSA-systeembeheerder Edward Snowden[17] [18]

PRISM is een spionageprogramma dat sedert 2007 gebruikt wordt door de NSA om inlichtingen te vergaren die verstuurd worden via grote Amerikaanse internetbedrijven. Het bestaan van dit programma werd onthuld op basis van een PowerPointpresentatie, dat door Edward Snowden naar de kranten The Guardian en The Washington Post werden gelekt. Het bestaan van PRISM werd langs Amerikaanse weg officieel bevestigd. Het programma is bedoeld om via directe toegang tot de servers van internetbedrijven (versleutelde of niet

---

15 Onderzoek naar de manier waarop de Belgische inlichtingendiensten (Veiligheid van de Staat en ADIV) hebben gehandeld in een zaak van telefoontaps in kantoren van delegaties van de Raad van de Europese Unie in Brussel, www.comiteri.be/index.php/nl/publicaties-mainmenu-9/onderzoeksverslagen-mainmenu-75.

16 De zaak Swift, Activiteitenverslag 2006, Vast Comité I, p. 42 – 51.

17 De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten, Activiteitenverslag 2014, Vast Comité I, p. 8-35.

18 De bescherming van het wetenschappelijk en economisch potentieel en de Snowden-onthullingen, Activiteitenverslag 2016, Vast Comité I, p. 52 – 56.

versleutelde) communicatie te onderscheppen, van zodra één van de deelnemers aan een communicatie zich buiten de Verenigde Staten bevindt. Het overgrote deel van de data (zowel geschreven communicatie als gesprekken en videobeelden) wordt gestockeerd in databanken, terwijl ook *live monitoring* mogelijk is.

II.2.6. Het BELGACOM/BICS-incident [19]

In september 2013 kwam na instabiliteit van haar netwerk aan het licht dat telecombedrijf BELGACOM (het huidige PROXIMUS) vermoedelijk sedert 2011 het voorwerp uitmaakte van een hacking.

Toen in 2012 de hulp werd ingeroepen van MICROSOFT, kon aanvankelijk de oorzaak niet worden opgespoord. Uit documenten van klokkenluider Edward Snowden bleek dat de hacking het werk was van de Britse inlichtingendienst, de *Government Communications Headquarters* (GCHQ), de Britse overheidsdienst verantwoordelijk voor inlichtingen van elektromagnetische oorsprong en voor de beveiliging van informaticasystemen, die daarbij nauw samenwerkte met de NSA.[20]

De hacking was niet zozeer op het telecombedrijf gericht maar wel op haar dochterbedrijf *Belgacom International Carrier Services* (BICS), dat datatransmissiediensten levert aan honderden internationale telecomoperatoren die op het bedrijf beroep doen om hun internationaal verkeer te regelen. Vermeldenswaard is dat BICS ook telecomleverancier is van de NAVO, de Europese Commissie, het Europees Parlement, SWIFT en de Belgische overheid.

II.2.7. De door Julian Assange georchestreerde WIKILEAKS-onthullingen

Programmeur, *hacker* en internetactivist Julian Assange richtte in 2006 WIKILEAKS op, met de bedoeling klokkenluiders een platform te geven om gevoelige informatie te laten lekken naar het grote publiek, door ze de garantie te bieden dat de identiteit van de klokkenluider niet traceerbaar zou zijn. Op het platform werden ophefmakende operaties en documenten gelekt[21]. Bepaalde documenten geven zeer openlijk (en zelfs vaak denigrerende) standpunten weer over sommige wereldleiders. In 2017 werden dan weer documenten gelekt die aangaven dat de CIA toegang heeft tot smartphones en computers.

Ondertussen werd oprichter Assange werd op 11 april 2019 ondertussen in Londen gearresteerd. Hij wordt op heden door de Verenigde Staten aangeklaagd voor inbreuken het tegen de US-spionagewetgeving.

---

19 De malware bij Belgacom, Activiteitenverslag 2013, Vast Comité I, p. 170 – 171.

20 De Standaard, 13 december 2014.

21 In 2010 werden duizenden documenten over de oorlog in Afghanistan en vervolgens over de oorlog in Irak via de website openbaar gemaakt. Ook werd de inhoud van 250.000 Amerikaanse diplomatieke telegrammen onthuld, die vanuit Washington naar diverse Amerikaanse ambassades waren gestuurd. Uit deze documenten bleek dat leden van Amerikaanse ambassades er vergaande spionageactiviteiten op nahielden. Bijzonder veel informatie werd zeer waarschijnlijk gelekt door Chelsey Manning.

II.2.8. PEGASUS

Lopende het huidig toezichtonderzoek kwam het afluisterschandaal PEGASUS aan het licht. PEGASUS is een spyware-product dat vooral op mobiele telefoons (maar ook op andere elektronische apparaten) kan worden geïnstalleerd. De ingevoerde spyware zorgt ervoor dat volledige controle wordt gekregen over het communicatieapparaat en laat zelfs toe de microfoon en de camera zonder medeweten van de gebruiker te activeren.

Dit nieuwe afluisterschandaal maakt het voorwerp uit van een afgescheiden toezichtonderzoek, dat eveneens door het Vast Comité I wordt gevoerd.[22]

II.3. HET ONTHULLEN VAN HET AFLUISTERSCHANDAAL RUBICON

In de loop van 2017 kreeg de Duitse journalist Peter F. Müller, medeauteur over een boek over de Duitse inlichtingendienst BND [23] een aantal opzienbarende rapporten aangeboden. Deze rapporten waren enerzijds afkomstig van de Amerikaanse inlichtingendienst CIA en anderzijds van de Duitse BND. Alles samen ging het over bijna 300 pagina's. Belangrijk is dat deze rapporten in werkelijkheid niet via dubieuze of illegale weg werden gelekt, wel integendeel. Duizenden pagina's waren integendeel na wettelijke declassificatieprocedures in de openbaarheid terechtgekomen. De reeds vermelde 300 pagina's maakten daarvan deel uit.

De journalist Müller ontdekte deze rapporten niet zelf. Een onbekende bron bezorgde de documenten aan de journalist. Geconfronteerd met een omvangrijk onderzoek legde Müller daarop deze rapporten voor aan collega-journalisten van de Duitse televisieomroep *Zweites Deutsches Fernsehen* (ZDF), de krant The Washington Post, de Zwitserse publieke omroep *Schweizer Radio und Fernsehen* (SRF), het cryptomuseum in Eindhoven en het Nederlandse onderzoekplatform ARGOS. Het gemeenschappelijke journalistieke onderzoek dat daarop volgde, gaf tussen februari en april 2020 aanleiding tot een aantal persartikels. Het eerste persartikel na het vrijgeven van de officiële rapporten werd op 11 februari 2020 gepubliceerd door The Washington Post en hernomen door SRF, en de ZDF.[24] De persaandacht was overigens slechts van korte duur. Algemeen kan zelfs gesteld worden dat de publieke opinie maar matig geïnteresseerd was in dit afluisterschandaal.

22 Vast Comité I, Toezichtonderzoek ter navolging van de bekendmaking van het gebruik van de software PEGASUS, (2021.286)

23 Peter F. Müller (soms ook geschreven als Mueller), "*Gegen Freund und Feind, die Geschichte des BND*", Reinbek, 2002, 719 p.

24 www.electrospaces.net/2020/05/maximator-and-other-european-sigint-alliance

II.4. DE ONTSTAANSGESCHIEDENIS VAN DE FIRMA CRYPTO AG[25]

De firma AB Cryptoteknik werd in 1920 door Arvid Gerharm Damm in Stockholm gesticht. Bij zijn overlijden, kort vóór de Tweede Wereldoorlog, kwam de firma in handen van Boris Hagelin. Boris Hagelin was een in het huidige Azerbeidzjan geboren ingenieur die de Zweedse nationaliteit had.

Tijdens een reis naar de Verenigde Staten in de jaren '30, op een moment dat hij al in Zwitserland verbleef, leerde Hagelin de Amerikaan William Friedman kennen die later het hoofd zou worden van de dienst cryptologie van de Amerikaanse spionagedienst NSA.

Na het uitbreken van de Tweede Wereldoorlog emigreerde Boris Hagelin van Zweden naar de Verenigde Staten. Tijdens de oorlog leverde zijn bedrijf mechanische cryptomachines aan het Amerikaanse leger.

In 1951 werd hun samenwerking tussen Hagelin en Friedman pas heel concreet. Friedman werkte op dat ogenblik voor de *Armed Forces Security Agency* (AFSA) [26] en stelde Boris Hagelin voor om een monopolie te ontwikkelen op het vlak van de nieuwste, geavanceerde crypto-machines. De verkoop van deze machines moest dan, via een *gentlemen's agreement* afgesloten tussen beide protagonisten exclusief worden voorbehouden aan door de VS goedgekeurde landen.

Hagelin was het idee genegen, en na het sluiten van de deal met Friedman zou de Zweedse firma in 1952 definitief de verhuis maken naar Zwitserland in 1952, op een moment dat de cryptomachines verschillende wijzigingen ondergingen en een groot internationaal succes kenden.

Ondertussen bemoeiden zowel de CIA als de AFSA, de voorloper van de NSA zich met de activiteiten van de firma, die doen AG CRYPTO heette. De Verenigde Staten eisten het patent op de ontwikkelde machines en bedongen dat de *gentleman's agreement*, voordien afgesloten tussen Hagelin en Friedman een formele overeenkomst werd dat specificeerde welke landen de nieuwste encryptie-machines konden verwerven.

Halverwege de jaren '60 legde de CIA en de NSA de hand op de verdere technische ontwikkeling van de crypto-machines, die maakte dat van mechanische machines werd overgeschakeld naar elektronische crypto-machines. Op die manier werd twee jaar later, in 1967, inderdaad een elektronisch model op de markt gebracht waarvan het elektronisch circuit toen al volledig ontworpen was door de NSA. Vanaf dat ogenblik hing de verdere ontwikkeling van de encryptie-machines quasi volledig afhing van de NSA, wat een eerste stap was in het verlies van de onafhankelijkheid van de firma AG CRYPTO.

---

25 Dit overzicht steunt in grote mate op de bijdragen van (1) Melina J. Dobson, Operation RUBICON, Germany as an Intelligence Great Power, Intelligence and National Security, volume 35, nummer 5, augustus 2020, 608-622, van (2) Richard Aldrich, Peter Müller, David Ridd and Erich Schmidt-Eenboom, Operation Rubicon: sixty years of German-American success in Signals Intelligence, ibidem, p.603-607, van (3) Sarah Mainwaring, Operation Rubicon and the CIA's secret SIGINT empire, ibidem, 623-640 en van (4) Greg Miller, Washington Post, The Intelligence coup of the century, 11 februari 2020.

26 AFSA was de dienst die binnen de U.S. vanaf mei 1949 alle crypto-activiteiten centraliseerde. De dienst viel onder de *US Department of Defence* en werd in december 1951 omgevormd tot de NSA.

In 1969 stelde het hoofd van de dienst Duitse cryptodienst, William Goeing, aan Hagelin voor om de firma aan Duitsland te verkopen, en de Verenigde Staten partner te maken in de deal. De CIA-directeur Richard Helms keurde het voorstel goed, en bepaalde de verdere details van de overeenkomst, waarbij onder andere werd afgesproken dat er alleen een samenwerking kon zijn tussen de Verenigde Staten en Duitsland, terwijl hij eiste dat Frankrijk buiten de deal werd gehouden.

Op 4 juni 1970 voltrok zich de formele koop van de firma in München. De firma werd verkocht voor 25.000.000 Zwitserse frank aan de Duitse Treuhand Gesellschaft-Munich. Enkele dagen later, op 12 juni 1970, werd de concrete afspraak tussen de beide diensten geformaliseerd in een *memorandum of understanding* (MoU) tussen de CIA en de BND.

In de daaropvolgende decennia, volop in de Koude Oorlog, leverde de controle over de CRYPTO AG-machines de Duitse en Amerikaanse inlichtingendiensten een schat aan informatie op. Volgens sommige schattingen zou in de jaren '80 ongeveer 40% van alle onderschepte internationale communicatie afkomstig zijn van de AG CRYPTO-machines.

De firma AG CRYPTO was ondertussen reeds jaren een gerenommeerde Zwitsers bedrijf geworden, dat een quasi-monopolie had op het vlak van cryptologie in de hele wereld. De firma had klanten in meer dan 120 landen, niet alleen de landen zelf maar ook internationale organisaties. Zo leverde de firma toestellen onder meer aan België, Egypte, Irak, Iran, Saoedi-Arabië, Syrië, Jordanië, India, Indonesië, Maleisië, Zuid-Korea, Thailand, Italië, Ierland, Spanje en zelfs aan Vaticaanstad. Ook worden toestellen geleverd aan Japan, Vietnam, Portugal, Pakistan, Bangladesh, Myanmar (Birma), de Filippijnen en aan de militaire junta's in Zuid-Amerika.

In 1993 besliste Duitsland om uit het programma te stappen. Ze liet de firma AG CRYPTO volledig in handen van de CIA, die de daaropvolgende 25 jaar alleen eigenaar werd van de firma.

Het spionageprogramma RUBICON kwam nooit in de openbaarheid, maar uit de studie van de opgestelde rapporten blijkt dat tijdens de jaren die volgden op het opstarten van de operatie RUBICON meerdere landen kennis kregen, in meerdere of mindere mate, van zekere aspecten van het spionageprogramma, vooral dan in de jaren '80, wanneer de eerste vragen opdoeken naar de activiteiten van de firma AG CRYPTO.[27] In augustus 2020 wijdde het tijdschrift *Intelligence and National Security* een deel van één van zijn nummers aan de zaak RUBICON.[28] In vier artikels van academische deskundigen wordt ingegaan op de SIGINT-activiteiten van de Amerikaanse en Duitse inlichtingendiensten via de Zwitserse firma CRYPTO AG.

---

27 James Bamford, 1982, The Puzzle Palace, A Report on America's Most Secret Agency.

28 "Special Section: SIGINT in the Late Twentieth Century: Operation RUBICON", *Intelligence and National Security*, Routledge, Volume 35, Number 5, August 2020.

De operatie die uiteindelijk bekend stond onder de codenaam RUBICON mag zonder meer een overweldigend succes worden genoemd. Gedurende decennia domineerde CRYPTO AG de wereldmarkt van encryptiemachines. Zij verkochten aan zo'n 120 landen en enkele internationale organisaties AG CRYPTO-toestellen, en lieten de kopers geloven dat het om bijzonder veilige toestellen ging. De toestellen werden dermate als betrouwbaar beschouwd, dat er niet de minste vragen werden gesteld omtrent hun betrouwbaarheid.[29]

II.5. EEN ZWITSERSE PARLEMENTAIRE ONDERZOEKSCOMMISSIE

De onthullingen over de banden tussen de Zwitserse firma CRYPTO AG en bepaalde buitenlandse inlichtingendiensten veroorzaakten opschudding in Zwitserland. De Zwitserse overheden gelastten een voormalig federaal rechter, Niklaus Oberholzer, met een onderzoek naar dit dossier.

In februari 2020 maakte de Délégation des Commissions de gestion des Chambres fédérales (DélCdG), de Parlementaire Commissie die verantwoordelijk is voor het toezicht op de inlichtingendiensten, bekend dat ook zij een onderzoek zou instellen naar eventuele banden die er zouden bestaan tussen de federale inlichtingendiensten en de buitenlandse inlichtingendiensten die bij deze zaak betrokken waren. Een ander aandachtspunt van het onderzoek zou zijn of en in hoeverre de Bondsraad op de hoogte was van de feiten betreffende CRYPTO AG. De DélCdG keurde eind 2020 haar inspectieverslag over de zaak CRYPTO AG goed, en maakte haar bevindingen bekend.[30]

Uit het onderzoeksrapport van de DélCdG blijkt dat de vroegere Services de Renseignement Stratégique (SRS), een voorloper van de huidige inlichtingendienst Service de Renseignement de la Confédération (SRC), vanaf de herfst 1993 wist dat buitenlandse inlichtingendiensten achter de firma CRYPTO AG schuilgingen, dat het bedrijf in handen was van buitenlandse inlichtingendiensten en dat het kwetsbare apparatuur exporteerde, waarvan de encryptie kon worden gedecodeerd met een minimum aan inspanning.

Hoewel het wettelijk kader binnen Zwitserland toestond dat Zwitserse en buitenlandse inlichtingendiensten gezamenlijk een in Zwitserland gevestigd bedrijf inschakelden om informatie in het buitenland in te winnen, betreurde de DélCdG het dat de Zwitserse politieke overheden pas eind 2019 op de hoogte werden gebracht. Bovendien werd vastgesteld dat de SRS toentertijd informatie had over CRYPTO AG en dat dit een goed bewaard geheim was binnen de leiding van deze dienst.

De DélCdG doet in haar onderzoeksrapport een aantal aanbevelingen. De belangrijkste aanbevelingen waren de volgende:

1. De Confederatie koopt geen encryptie-apparatuur van buitenlandse leveranciers. Zwitserse leveranciers moeten de Confederatie de verzekering geven dat zij de veiligheidsaspecten van de ontwikkeling en productie onder controle hebben.

---

29 Richard J. Aldrich, « Operation RUBICON: sixty years of German-American success in signals intelligence », *Intelligence and National Security*, Routledge, Volume 35, Number 5, August 2020.

30 www.parlament.ch/organe/delegations/delegations-des-commissions-de-gestion/affaire-crypto-ag

2. Het Federaal Departement van Defensie zorgt ervoor dat de strijdkrachten voldoende cryptologische deskundigheid behouden. Het zorgt er tevens voor dat de bevoegdheden op het vlak van cryptografie en cryptoanalyse optimaal worden benut.
3. Het Federaal Departement van Defensie zorgt ervoor dat de cryptoanalyse-mogelijkheden aan de bestaande voorschriften op het gebied van interceptie van communicatie blijven voldoen.

II.6. RUBICON EN DE BELGISCHE INLICHTINGENDIENSTEN

Het Vast Comité I bevroeg de beide Belgische inlichtingendiensten - de VSSE en de ADIV - over hun evaluatie is van mogelijke interne compromittering als gevolg van het dossier RUBICON.

II.6.1. Het standpunt van de VSSE.

Samenvatting van de geclassificeerde informatie
Enerzijds nam de VSSE enkel via de onthullingen in de pers kennis van de banden tussen het bedrijf CRYPTO AG met de Amerikaanse inlichtingendiensten CIA en NSA en de Duitse inlichtingendienst BND. Anderzijds kan niet uitgesloten worden dat bepaalde Belgische overheidsdiensten wel degelijk gebruik hebben gemaakt van AG CRYPTO-toestellen, maar ook van gelijkaardige toestellen. Bij het bevragen van haar partners heeft de VSSE nauwelijks bruikbare informatie bekomen.

II.6.2. Het standpunt van de ADIV.

Op het moment van de eerste melding van het RUBICON-schandaal in de pers, liet de ADIV op 12 februari 2020 via het persbureau Belga een communiqué publiceren waarin het volgende gesteld werd: "*De ADIV is op de hoogte van de RUBICON-affaire en onderzoekt de mogelijke omvang van de vermelde afluisterpraktijken.*" De ADIV bevestigde dit ook aan de krant De Tijd en stelde: *"De ADIV doet er alles aan om zich tegen hen (bedoeld wordt: afluisterpraktijken) te wapenen en maakt er vooral een erezaak van om het wettelijk kader op dit gebied te respecteren en anderzijds een morele code te hanteren ten opzichte van zijn partners/bondgenoten in een wereld waar, zonder naïef te zijn, vertrouwen vaak met voorzichtigheid gepaard gaat."*

Het Vast Comité I vroeg aan de ADIV verdere verduidelijking, vermits de woordkeuze van de persmededeling immers liet verstaan dat militaire inlichtingendienst al veel eerder op de hoogte was van de RUBICON-operatie. ADIV verklaarde achteraf dat het geenszins de bedoeling was te bevestigen dat ADIV vóór de persaandacht op de hoogte was van het bestaan van gecompromitteerde AG CRYPTO-apparatuur en van de heimelijke samenwerking tussen de Amerikaanse en Duitse inlichtingendiensten in deze kwestie.

Samenvatting van de geclassificeerde informatie
De mogelijke compromittering bij ADIV door een AG CRYPTO-toestel wordt, op basis van uitgevoerd archiefonderzoek, als uiterst miniem beschouwd. Wel kon in een geïsoleerd geval gewezen worden op het gebruik, binnen Defensie, van een toestel, en dit vóór de jaren '70.

II.7. DE EVALUATIE DOOR HET VAST COMITÉ I OP BASIS VAN DE VERSTREKTE ANTWOORDEN

Afgaand op de door de VSSE en de ADIV medegedeelde geclassificeerde informatie aan het Vast Comité I kan de mogelijke compromittering van de apparatuur gebruikt door de VSSE en de ADIV gekwalificeerd als *miniem*, terwijl de schade voor Defensie als *uiterst miniem* gekwalificeerd wordt.

Evenwel is het maken van een sluitende risicoanalyse door het Vast Comité I en door de inlichtingendiensten op heden allesbehalve eenvoudig. Er is vooreerst ondertussen een ruime tijdsverloop tussen het afluisterschandaal RUBICON en het toezichtonderzoek. Anderzijds vereist het onderzoek om uit te maken of een encryptie-toestel verzwakt is, een fysiek en operationeel onderzoek van elk verdacht toestel, wat op heden niet meer mogelijk is, gelet op het feit dat de toestellen AG CRYPTO niet meer beschikbaar zijn voor het uitvoeren van het vermeld onderzoek.

II.8. ACTUELE RELEVANTIE

Samenvatting van de geclassificeerde informatie

Uit het toezichtonderzoek blijkt dat voor de VSSE dat het inlichtingenschandaal aantoont dat bij het gebruik van buitenlandse cryptografie-apparatuur de nodige voorzichtigheid is geboden, terwijl de ADIV erop wijst dat er belangrijke lessen moeten worden getrokken uit het afluisterschandaal. De ADIV geeft mee dat de dienst in de betrokken materie overigens al geruime tijd zeer verregaande stappen heeft ondernomen.

III. MAXIMATOR

III.1. De onthullingen van Prof. Bart Jacobs over het SIGINT-netwerk MAXIMATOR

De afluisteraffaire RUBICON is op zich al een opzienbarende zaak. Deze afluisteraffaire bracht aan het licht dat Duitse en Amerikaanse inlichtingendiensten eigenaar werden van een Zwitserse encryptie-onderneming, die verzwakte cryptografische toestellen leverde. Op die manier verkocht CRYPTO AG gedurende tientallen jaren encryptie-toestellen aan andere landen of verscheidene internationale instellingen, waarbij ze de kopers in de overtuiging lieten dat het om zeer betrouwbare toestellen ging. Deze werkwijze liet Amerikaanse en Duitse autoriteiten toe om vervolgens alle door de kopers uitgewisselde gecrypteerde communicatie te kunnen decoderen.

Volgend op de onthullingen over CRYPTO AG, verscheen op 7 april 2020 een wetenschappelijke bijdrage hieromtrent van de hand van de Nederlandse professor Bart Jacob.[31] Jacobs publiceerde zijn bijdrage in het Britse wetenschappelijke tijdschrift *Intelligence and National Security*, met als titel: *'MAXIMATOR, European signals intelligence cooperation, from a Dutch perspective'*.[32]

Volgens Jacobs werd in 1976 heimelijk een Europese SIGINT-samenwerking opgericht. Oorspronkelijk gebeurde dit in 1976 met drie deelnemers: Denemarken, Zweden en Duitsland. Nederland vervoegde de alliantie in 1978, terwijl Frankrijk toetrad in 1985.[33] Volgens professor Jean-Jacques Quisquater nam overigens Frankrijk vanaf 2006 de *lead* en werden de vergaderingen vaak voorgezeten door de technische directie van de DGSE.[34] Dit "Noord-West-Europese" samenwerkingsverband, kreeg de naam MAXIMATOR[35] en was deels een antwoord op de FIVE EYES.[36]

Jacobs wijst erop - en dit is belangrijk - dat het MAXIMATOR-netwerk sterk leunde op de door de Duitse partner geleverde informatie die afkomstig was van het "kraken" van "AG CRYPTO"-communicatie. Jacobs laat uitschijnen dat de diensten die deelnemen aan het programma niet enkel Duitse onderschepte informatie kreeg, maar ook de middelen kreeg om de berichten zelf de ontcijferen.

---

31 Prof. Dr. Bart Jacobs doceert sedert 2003 computerbeveiliging aan de universiteit van Nijmegen en schreef al tientallen wetenschappelijke bijdragen over de materie. Hij is ook lid van expert board van de Nederlandse Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten (CTIVD, Nederland).

32 Gepubliceerd in het Britse wetenschappelijke tijdschrift *Intelligence and National Security*, volume 35, nummer 5, augustus 2020, pp. 659-668, en ook consulteerbaar op *https://tandfonline.com*

33 www.electrospaces.net/2020/05/maximator-and-other-european-sigint-alliance

34 Jean-Jacques Quisquater, Cruel paradoxe de la cryptographie belge, 20 mei 2020, www.regional-it.be/detached/cruel-paradoxe-de- la-cryptographie-belge

35 www.electrospaces.net/2020/05/maximator-and-other-european-sigint-alliance

36 FIVE EYES is een SIGINT-samenwerkingsverband door diensten van Australië, Canada, het Verenigd Koninkrijk, Nieuw-Zeeland en de Verenigde Staten.

Niettegenstaande het bijzonder geheime karakter van het programma kwamen een aantal andere Europese landen op de hoogte van het bestaan van het netwerk. Deze namen het initiatief om te verzoeken deel uit te maken van het MAXIMATOR-netwerk. De meesten werden geweigerd, vaak op basis van het feit dat ze geen voldoende cryptoanalyse-ervaring of expertise beschikken.

Belangrijke vaststelling is dat België werd uitgesloten van het MAXIMATOR-netwerk.

Over deze uitsluiting van Belgische inlichtingendiensten aan dit MAXIMATOR-netwerk schrijft Jacobs [vrije vertaling]: *"Bepaalde landen werden met opzet uitgesloten (van het netwerk) omdat zij binnen de MAXIMATOR-alliantie werden beschouwd als zijnde landen met een gebrek aan relevante (Signal/crypto) ervaring en/of expertise. (...) België is de opvallende uitzondering in Noordwest-Europa; het werd niet uitgenodigd om lid te worden van MAXIMATOR door haar gebrek aan SIGINT- (en COMSEC-) capaciteiten."* [37]

De auteur verduidelijkt vervolgens in een voetnoot [vrije vertaling]: *"Als gevolg hiervan werd België niet beschermd door de activiteiten van MAXIMATOR-leden en kocht het (minder beveiligde) CRYPTO AG-apparatuur, wat ook blijkt uit de gelekte BND- en CIA-documenten. Op die manier werd haar communicatie die verliep over AG CRYPTO-toestellen afgeluisterd door zowel het FIVE EYES-verband als door het MAXIMATOR-samenwerkingsverband."* [38]

Deze uitspraak is volgens het Vast Comité I zeer ontnuchterend voor België.[39]

Volgens de beweringen van Jacobs zou (1) België in het verleden niet alleen moedwillig uit een belangrijk Europees inlichtingensamenwerkingsverband zijn gehouden, maar (2) zou het minder beveiligde cryptografietoestellen hebben gebruikt en (3) zou ons land zelfs door de westerse SIGINT-samenwerkingsbanden waartoe het niet mocht toetreden, zijn afgeluisterd.

III.2. MAXIMATOR en de Belgische inlichtingendiensten.

Het Vast Comité I legde heel specifiek de vraag voor aan beide diensten of zij op de hoogte waren van het MAXIMATOR-netwerk vóór het artikel van prof. Bart Jacobs.

Volgens de antwoorden van de VSSE en de ADIV aan het Vast Comité I zouden beide diensten niet op de hoogte zijn geweest van de alliantie MAXIMATOR-alliantie. De diensten stellen inderdaad zeer uitdrukkelijk dat ze pas van de alliantie op de hoogte werden gebracht naar aanleiding van verschijnen van het artikel van prof. Bart Jacobs.

---

37 "Certain countries were deliberately not allowed to join because within the Maximator alliance they were considered as lacking relevant (Signal/crypto) expertise and/or experience (...). Belgium is a notable exception in north-western Europe; it had not been invited to join Maximator because of its lack of SIGINT (and COMSEC) capabilities."

38 "As a result, Belgium was not 'protected' by the Maximator members and bought (weakened) CRYPTO AG equipment, as also reported in the leaked BND and CIA documents, so that its (CRYPTO AG based) communication was readable by both western five-member SIGINT alliances (Five-eyes and Maximator)".

39 Prof. Quisquater spreekt zelfs van 'pathetisch'. Zie : J.-J. Quisquater, Cruel paradoxe de la cryptographie belge, 20 mei 2020, www.regional-it.be/detached/cruel-paradoxe-de-la-cryptographie-belge

Naderhand werden de diensten door het Vast Comité I geconfronteerd met een bewering in een Nederlands persartikel in *The Post Online*, dat eigenlijk handelt over de wijze waarop de Nederlandse minister van Binnenlandse Zaken bepaalde parlementaire vragen over MAXIMATOR beantwoordde.[40] Het artikel beweerde dat België tot het netwerk wou toetreden, maar dat België werd afgewezen, omdat "de geheime dienst" van België te zwak zou zijn. Beide diensten bleven in hun antwoord zeer categoriek en stelden absoluut geen kennis te hebben gehad van het MAXIMATOR-netwerk vóór de onthullingen van 7 april 2020. De VSSE wijst er overigens op dat deze bewering afwijkt van de bewering van prof. Bart Jacobs, dat de bewering door geen enkel ander medium werd hernomen, terwijl de dienst er anderzijds ook op wijst dat *The Post Online* als een weinig betrouwbare publicatie werd omschreven.

[40] Anke Bijleveld schoffeert de Tweede Kamer, minister zwijgt over het geheime spionagegenootschap 'MAXIMATOR', The Post Online, 8 mei 2020.

IV. CONCLUSIES

1. De informatie verschenen naar aanleiding van het afluisterschandaal bracht aan het licht dat de Zwitserse firma CRYPTO AG gedurende decennia encryptietoestellen op de markt had gebracht, waarvan de gecrypteerde berichten - anders dan de landen en internationale diensten die deze toestellen hadden aangekocht dachten - gemakkelijk konden worden ontcijferd. De firma AG CRYPTO werkte daarbij lange tijd, heimelijk en op zeer intensieve wijze samen met Duitse en Amerikaanse inlichtingendiensten.

2. Het decennialang geheimhouden van het ontcijferen via AG CRYPTO-apparatuur van gecrypteerde berichten door de Verenigde Staten en Duitsland is opzienbarend.

3. Desondanks raakten bepaalde landen toch van de afluisteroperaties op de hoogte en werden er sommigen later zelfs in betrokken.

4. De Belgische inlichtingendiensten stellen dat zij, tot het verschijnen van de betrokken persartikelen, nooit op de hoogte waren van de AG CRYPTO-zaak.

5. De Belgische inlichtingendiensten werden opzettelijk buiten het geheime SIGINT-netwerk MAXIMATOR gehouden.

6. De kans is groot dat België zelf het voorwerp heeft uitgemaakt van interceptie-activiteiten van haar gecrypteerde berichten door het SIGINT-netwerk MAXIMATOR.

V. AANBEVELINGEN

Hoewel de onderzochte kwestie zeer oud is formuleert het Vast Comité I niettemin drie algemene aanbevelingen:

1. De Belgische inlichtingendiensten (alsook alle Belgische autoriteiten) dienen te allen tijde bewust te zijn van het risico dat op elk moment de verstuurde of ontvangen gecrypteerde berichten steeds het voorwerp kunnen uitmaken van ontcijferactiviteiten via bijzonder snel ontwikkelende technologie.

2. De inlichtingendiensten moeten bijzondere aandacht blijven schenken aan de buitenlandse technologische ontwikkeling op het vlak van encryptie.

3. De encryptiedeskundigen binnen elke Belgische inlichtingendienst dienen na te gaan op welke wijze encryptietechnologie zoveel mogelijk door betrouwbare nationale instanties moet worden ontwikkeld.