(17

CONFIDENTIEL JUSQU'À LA RÉUNION DE LA COMMISSION D'ACCOMPAGNEMENT

COMITE PERMANENT DE CONTROLE DES SERVICES DE RENSEIGNEMENT ET DE SECURITE

Numéro de notice 2020.275

Les conséquences des réseaux de surveillance étrangers pour les services de renseignement belges : les affaires CRYPTO AG, RUBICON et MAXIMATOR

Rapport final – 13 octobre 2022

TABLE DES MATIÈRES

I. INTRODUCTION

I.1. ORIGINE ET PORTÉE DE L'ENQUÊTE DE CONTRÔLE

Au premier semestre 2020, des révélations ont été reprises dans la presse sur le programme d'espionnage dénommé RUBICON. Certains articles de presse faisaient état de la prise d'intérêts, au début des années 60, des services de renseignement américains CIA et NSA ainsi que du service de renseignement allemand *Bundesnachrichtendienst* (BND) dans la société CRYPTO AG. Par la suite, la *Central Intelligence Agency* (CIA) et le BND en deviendront même les propriétaires exclusifs.

La société CRYPTO AG fabriquait du matériel permettant de crypter des communications.

Fort de leur contrôle exclusif de ladite société, les services de renseignement américains CIA et *National Security Agency* (NSA) ainsi que le service de renseignement allemand BND ont pu, des décennies durant, prendre connaissance des messages envoyés par nombre pays ou institutions ayant acquis le matériel de codage CRYPTO AG, ce programme d'espionnage portant le nom RUBICON.

Dans le cadre de ce programme d'espionnage, il s'agissait non seulement d'espionner les communications émanant des puissances ennemies mais également celles échangées entre des pays amis voire alliés au sein de l'OTAN, notamment.

L'Affaire RUBICON se déroulera essentiellement dans le courant du 20ème siècle, et plus spécialement dans les années 70, 80 et 90, soit pendant une bonne partie de la Guerre froide.

La présente enquête de contrôle ne vise pas un examen exhaustif du scandale des écoutes CRYPTO AG / RUBICON mais il s'agit ici de vérifier si les services de renseignement belges, VSSE et SGRS, ont pris part à ce scandale ou s'ils ont été touchés par celui-ci.

Dans le contexte du scandale des écoutes, un autre volet fut mis à jour. Ainsi, un universitaire néerlandais et expert en sécurité informatique, le Professeur Bart Jacobs, a révélé l'existence, dans un article scientifique, de l'alliance secrète SIGINT entre plusieurs pays européens [1]. Cette structure de coopération fut reprise sous la dénomination MAXIMATOR. Quant à cette problématique spécifique, la présente enquête de contrôle s'est attachée à vérifier de quelle manière la Belgique avait été impliquée dans cette structure de coopération secrète.

I.2. DÉROULEMENT DE L'ENQUÊTE ET MÉTHODOLOGIE

La décision d'enquête de contrôle a été approuvée par le Comité permanent R le 30 septembre 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.

Entre le dernier trimestre 2020 et le premier trimestre 2022, la littérature scientifique et diverses autres sources ouvertes ont été consultées. En outre, différents devoirs d'enquête ont été effectués et un entretien a été organisé avec les responsables du musée de la cryptographie *('cryptomuseum')* à Eindhoven (Pays-Bas).

I.3. COMPÉTENCE DU COMITÉ PERMANENT R

L'article 33 de la loi du 18 juillet 1991 relative au contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (Loi Contrôle) stipule que le Comité permanent R enquête sur les activités et les méthodes des services de renseignement.

I.4. PAS D'ACCORD DU SPF AFFAIRES ÉTRANGÈRES

Le Comité permanent R n'a pas la possibilité, légalement, d'exercer un contrôle sur d'autres services que la VSSE et le SGRS (et sur l'OCAM, en collaboration avec le Comité permanent P).

Il ressort cependant de l'enquête effectuée que des appareillages CRYPTO AG auraient pu être utilisés par d'autres services ou instances belges, pour transmission de la correspondance diplomatique, par exemple.

Par lettre du 3 mars 2020, le ministre des Affaires étrangères d'alors a été informé par le Comité permanent R de la présente enquête de contrôle effectuée, et son accord a été demandé pour obtenir du SPF Affaires étrangères tous les renseignements utiles concernant le scandale des écoutes. La demande formulée est restée sans réponse. 4

I.5. ATTENTION PARLEMENTAIRE

Le Comité permanent R a pu vérifier que le scandale des écoutes a fait l'objet de quatre questions parlementaires en Belgique [2], ce dans le courant du mois de février 2020.

Il s'agissait plus précisément de :

- la question du Député Stefaan Van Hecke au ministre Philippe Goffin (Affaires étrangères et Défense) sur « Les mises sur écoutes par les États-Unis au moyen d'un appareil de Crypto AG » [3] ;
- la question du Député Chris Verduyckt au ministre Philippe Goffin (Affaires étrangères et Défense) sur « L'opération d'écoute Rubicon au moyen d'appareils de la société CRYPTO » [4] ;

---

2 À diverses questions parlementaires, posées au *minister van Binnenlandse Zaken en Koninkrijksrelaties*,la réponse apportée à la *Tweede Kamer* : « *In het openbaar worden geen uitspraken gedaan over het kennisniveau en de werkwijze van de inlichtingen- en veiligheidsdiensten* » pouvant se traduire par « On ne fait aucune déclaration en public sur le niveau de connaissances et les pratiques des services de renseignement et de sécurité (traduction libre), *Tweede Kamer der Staten generaal*, 2019 - 2020, Quest. n° 2640 du 14 avril 2020.

3 55003359C du 19/02/2020.

4 55003428C du 19/02/2020.

- la question du Député Stefaan Van Hecke à Koen Geens, Vice-Premier ministre et ministre de la Justice et de la Régie des Bâtiments sur « Les mises sur écoutes par les États-Unis au moyen d'un appareil de Crypto AG » [5] ;
- la question de la Députée Kattrin Jadin à Koen Geens, Vice-Premier ministre et ministre de la Justice et de la Régie des Bâtiments sur « L'affaire d'espionnage » [6].

À en juger par les réponses des ministres concernés, l'on pouvait établir qu'en ce qui concernait la VSSE, aucun matériel CRYPTO AG n'avait été utilisé ces dix dernières années. Pour la période antérieure à ces dix années cependant, il conviendrait d'approfondir la vérification. La complexité croissante des technologies en question était encore soulignée dans les réponses ministérielles, complexité qui compliquait la détection d'éventuelles portes dérobées (« *backdoors* ») dans l'appareillage concerné. En ce qui concerne la Défense et le SGRS en particulier, il apparaissait que lesdits appareillages avaient été utilisés dans les années 50 jusqu'au milieu des années 60, ce pour assurer les communications opérationnelles à l'étranger, mais que par la suite, la Défense et le SGRS en particulier achetèrent uniquement des appareillages de cryptage approuvés par l'OTAN et l'EU.

I.6. IMPLICATION POLITIQUE À L'ÉTRANGER

Le 12 mai 2021, en Suisse, la démission de Jean-Philippe Gaudin, le directeur du Service de renseignement de la Confédération (SRC) a été annoncée officiellement par communiqué. Si, selon ce communiqué, le départ du Chef du service de renseignement avait été convenu d'un *commun accord*, la presse a lié cette démission, entre autres, au scandale des écoutes. Il aurait, en effet, omis d'informer les responsables politiques de l'accord secret conclu entre les services de renseignement américains et allemand [7].

Au Danemark, en août 2020, Lars Findsen, le patron du *Forsvarets Efterretningstjeneste* (FE), le service de renseignement militaire, a été suspendu un moment et arrêté pour suspicion de fuites de secrets d'État. Cet incident a également été lié, par une certaine presse, au scandale des écoutes [8] bien que cette affirmation, selon le Comité permanent R, ne semble véritablement pas fondée. Cette suspension s'inscrivait néanmoins dans une discussion plus large sur l'admissibilité d'une coopération SIGINT poussée entre le Danemark et les États-Unis et, dans l'ombre du scandale des écoutes, cette suspension démontra les très fortes tensions qui émaillèrent pendant un certain temps les relations entre les services de renseignement et les autorités politiques danois.

---

5 55003358C du 19/02/2020.

6 55003380C du 19/02/2020.

7 *RTS*, 'Le départ du chef du renseignement suisse dû à des tensions avec Viola Ahmerd', 12 mai 2021.

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

I.7. DIFFICULTÉS ET COMPLEXITÉ DANS LA PRÉSENTE ENQUÊTE DE CONTRÔLE

Les devoirs d'enquête ont quelque peu compliqué l'enquête de contrôle par le fait qu'en marge de l'affaire CRYPTO AG, il apparaissait que d'autres dispositifs livrés à la Belgique avaient également été compromis. Il s'agissait essentiellement, mais pas exclusivement, des appareillages de chiffrement AROFLEX et BEROFLEX, produits par la firme Philips. La problématique relative à AROFLEX et BEROFLEX est complexe et sort, pour la plus grande partie, de l'enquête de contrôle [9]. Le Comité permanent R a donc décidé, dans le cadre de la présente enquête qui est déjà fort complexe, de ne pas tenir compte desdits appareillages [10].

Il apparaissait, en outre, que la presse n'avait accordé qu'une attention toute relative au scandale des écoutes, ce qui n'a pas facilité le travail d'enquête, non plus.

Par ailleurs encore, il convenait de souligner la particulière pauvreté de certaines sources, ce qui s'est notamment révélé dans le cadre des informations disponibles quant au réseau MAXIMATOR (voir partie III). Ainsi, de nombreux articles de presse et des sources diverses se basaient presqu'exclusivement sur une seule contribution scientifique, soit celle du Professeur néerlandais Bart Jacobs, déjà cité, parue dans une revue scientifique britannique [11].

Enfin, mentionnons le long laps de temps écoulé entre les faits ayant débuté dans les années 60 et le moment où l'enquête de contrôle a été effectuée. Il n'y avait plus que quelques pièces comptables, par exemple des bons de commande, encore disponibles et relatives à l'achat des appareillages de chiffrement, et plus aucuns dispositifs eux-mêmes datant de cette période en fonctionnement dans les services de renseignement, ce qui ne permit aucun contrôle physique opérationnel ayant pour objectif de déterminer si ceux-ci avaient été fragilisés ou compromis.

9 La version AROFLEX présentait un très haut niveau de fiabilité, tandis que les dispositifs BEROFLEX étaient des versions « édulcorées » et donc moins fiables.

10 Dans sa réponse (classifiée) au Comité permanent R, tant le SGRS que la VSSE ont mentionné les deux dispositifs de chiffrement.

11 Bart Jacobs, *'MAXIMATOR, European signals intelligence cooperation from a Duitch perspective, Intelligence and National Security*, volume 35, numéro 5, août 2020, pp. 659-668. Peut également être consulté sur le site Internet suivant : https://tandfonline.com.

II. CONTEXTUALISATION DE L'ENQUÊTE

II.1. PRÉAMBULE : L'IMPORTANCE DE LA CRYPTOGRAPHIE ET DE LA CRYPTOANALYSE

La **cryptographie** est l'activité qui consiste, pour l'expéditeur d'un message, à le masquer sur base de codes connus par les seuls partenaires, de sorte que seul le destinataire du message puisse en appréhender le contenu.

Au départ, la cryptographie était surtout utilisée dans un contexte de guerre, mais elle a ensuite été étendue à un éventail plus large de messages sensibles, comme ceux de la correspondance diplomatique.

La **cryptoanalyse** est naturellement contemporaine de la cryptographie. Elle permet de transformer les messages cryptés en messages compréhensibles. Tout message crypté peut, en principe, être déchiffré. La cryptoanalyse requiert naturellement davantage de temps et d'efforts, moyens proportionnels à la complexité du mode de cryptage des messages envoyés.

Les possibilités de crypter / décrypter des messages de plus en plus complexes ont été véritablement facilitées et largement accélérées par le passage du cryptage / décryptage au mécanique, et ensuite encore à l'électronique.

II.2. RUBICON : LE ÉNIÈME SCANDALE D'ÉCOUTES

Le scandale des écoutes étudié dans le cadre de la présente enquête de contrôle peut être ajouté à une liste impressionnante de scandales de ce type ayant été révélés au début de ce 21ème siècle. Le Comité permanent R, qui a consacré par le passé une enquête de contrôle à la plupart de ces scandales, énumère ici les plus importants traités :

II.2.1. Le projet d'écoutes électroniques ECHELON [12] [13] [14]

ECHELON est le programme d'écoutes opérationnel depuis les années 70. Il capte et filtre pour les *FIVE EYES* toutes les communications satellitaires en fonction des mots-clés saisis au préalable, des *targets*, des noms et des numéros de téléphone. Ce programme d'espionnage a attiré l'attention après la création par le Parlement européen d'une commission d'enquête chargée d'examiner l'ampleur des activités d'interception.

---

12 COMITÉ PERMANENT R, *Rapport d'activités 1999*, Enquête sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système américain "Echelon" d'interception des communications téléphoniques et fax en Belgique, pp. 23-47.

13 COMITÉ PERMANENT R, *Rapport complémentaire d'activités 1999*, Rapport complémentaire sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau "Echelon" d'interception des communications, pp. 2-47.

14 COMITÉ PERMANENT R, *Rapport complémentaire d'activités 2000*, Rapport de synthèse de l'enquête sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un réseau "Echelon" d'interception des communications en Belgique, pp. 27-57.

II.2.2. L'espionnage du bâtiment Juste Lipse à Bruxelles [15]

En 2003, le bureau de la sécurité du Conseil européen a constaté que plusieurs délégations des États-membres dont le bâtiment Juste Lipse abritait les bureaux, et notamment celle d'Espagne, d'Allemagne, de France, d'Italie, du Royaume-Uni et d'Autriche, étaient mises sur écoute téléphonique. Les constatations officielles en furent faites le 28 février 2003 mais des rumeurs en ce sens avaient déjà circulés précédemment. Les écoutes auraient eu lieu entre 1995 et 2003. La Sûreté de l'État collabora à l'enquête sur l'incident. Après sept ans d'enquête pénale, le dossier fut classé sans suite par le Parquet fédéral. En 2008 encore, un autre scandale concernant le bâtiment Juste Lipse vit le jour sur la base de documents dévoilés par Edward Snowden faisant état de tentatives de mises sur écoute de ce bâtiment depuis un local de l'OTAN situé à Evere et réservé à la NSA.

II.2.3. La mise sur écoute de la société SWIFT [16]

SWIFT est une société qui règle les transactions financières internationales de milliers d'institutions financières de 200 pays. Le siège de la société se trouve à La Hulpe (Brabant wallon) et aurait été victime d'une intrusion dans ses systèmes informatiques.

II.2.4. Le piratage du réseau informatique des Affaires étrangères

En 2013, la CIA informa le SGRS que des *hackers* russes étaient parvenus à pirater des ordinateurs des Affaires étrangères en utilisant le virus Snake. Le SGRS, la VSSE et le FCCU tentèrent alors de déterminer quels documents avaient été interceptés. Ce dossier pénal fut également classé sans suite.

II.2.5. Les révélations du programme informatique PRISM par le gestionnaire de système de la NSA, Edward Snowden [17] [18]

PRISM est un programme d'espionnage utilisé depuis 2007 par la NSA et vise la collecte des renseignements envoyés via de grandes entreprises du net américaines. L'existence de ce programme a été dévoilée par le biais d'une présentation PowerPoint qu'Edward Snowden a fait fuiter vers les journaux *The Guardian* en *The Washington Post*. L'existence de PRISM a été confirmée officiellement par les États-Unis et vise à intercepter, via un accès direct aux serveurs des entreprises du net, des communications, cryptées ou non, dès qu'un des participants à une communication se situe aux États-Unis. La grande majorité des données,

---

15 Enquête sur la manière dont les services de renseignement belges (Sûreté de l'État et SGRS) sont intervenus à propos d'une affaire d'écoutes de bureaux de délégations du Conseil de l'Union européenne à Bruxelles, www.comiteri.be/index.php/fr/publications/rapports-denquetes-3.

16 COMITÉ PERMANENT R, *Rapport d'activités 2006*, L'affaire SWIFT, pp. 39-48.

17 COMITÉ PERMANENT R, *Rapport d'activités 2014*, Les révélations d'Edward Snowden et la position d'information des services de renseignement belges, pp. 8-36.

18 COMITÉ PERMANENT R, *Rapport d'activités 2016*, La protection du potentiel économique et scientifique et les révélations d'Edward Snowden, pp. 52 -56.

soit les communications écrites, les discussions et les images vidéo sont stockées dans des banques de données tandis que le *live monitoring* reste également possible.

II.2.6. L'incident BELGACOM/BICS [19]

En septembre 2013, suite à une instabilité de son réseau, il apparut que l'entreprise de télécommunications BELGACOM, devenue PROXIMUS, était vraisemblablement victime de piratage depuis 2011.

Lorsqu'en 2012, une demande d'assistance fut faite auprès de MICROSOFT, la cause ne put être initialement déterminée. Il ressortit de documents du lanceur d'alerte Edward Snowden que le piratage avait été l'œuvre du *Government Communications Headquarters* (GCHQ), service britannique responsable du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information, qui collaborait étroitement avec la NSA [20].

Le piratage ne visait pas tant l'entreprise de télécommunications que sa filiale *Belgacom International Carrier Services* (BICS) qui fournissait déjà des services de transmission de données à des centaines d'opérateurs de télécommunications internationaux faisant appel à l'entreprise pour régler leur trafic international. Signalons encore que BICS est également le fournisseur de télécommunications de l'OTAN, de la Commission européenne, du Parlement européen, de SWIFT et des autorités belges.

II.2.7. Les révélations de WIKILEAKS orchestrées par Julian Assange

Le programmeur, *hacker* et activiste de l'Internet, Julian Assange, fonda WIKILEAKS en 2006 avec pour objectif d'offrir une plateforme à des lanceurs d'alerte, ce afin de faire fuiter des informations sensibles vers le grand public tout en garantissant l'intraçabilité de l'identité du lanceur d'alerte. Des opérations et documents controversés fuitèrent sur cette plateforme [21]. Dans certains documents figuraient des opinions très ouvertes, voire souvent dénigrantes, concernant certains dirigeants du monde. En 2017, il y eut même une fuite de documents indiquant que la CIA avait accès à des smartphones et des ordinateurs.

Le fondateur Assange a, entre-temps, été arrêté à Londres le 11 avril 2019 et les États-Unis réclament actuellement son extradition pour violation de la législation américaine en matière d'espionnage.

---

19 COMITÉ PERMANENT R, *Rapport d'activités 2013,* Le logiciel malveillant chez Belgacom, pp. 172-173.

20 *De Standaard*, 13 décembre 2014.

21 En 2010, des milliers de documents sur la guerre en Afghanistan et, par la suite, sur la guerre en Irak ont été publiés via le site web. En outre, le contenu de 250.000 télégrammes diplomatiques américains a été divulgué, télégrammes qui étaient envoyés depuis Washington vers diverses ambassades américaines. Il ressortait de ces documents que des membres des ambassades américaines s'adonnaient à des activités d'espionnage poussées. Chelsey Manning est très probablement à l'origine de la fuite d'un nombre particulièrement élevé d'informations.

II.2.8. PEGASUS

Le scandale des écoutes PEGASUS a été révélé alors que la présente enquête était déjà en cours. PEGASUS est un logiciel espion pouvant être installé essentiellement sur des téléphones mobiles mais également sur d'autres appareils électroniques. Une fois installé, le logiciel espion permet de prendre le contrôle de l'appareil de communication et même d'activer le microphone et la caméra à l'insu de l'utilisateur.

Ce nouveau scandale d'écoutes fait l'objet d'une enquête de contrôle distincte effectuée par le Comité permanent R [22].

II.3. LA RÉVÉLATION DU SCANDALE DES ÉCOUTES RUBICON

Courant 2017, le journaliste allemand Peter F. Müller, co-auteur d'un ouvrage sur le service de renseignement allemand BND [23] s'est vu remettre plusieurs rapports surprenants de quelque 300 pages provenant, d'une part, du service de renseignement américain CIA et, d'autre part, du BND allemand. En réalité, ces rapports n'ont pas « fuité » de manière douteuse ou illégale. Tout au contraire, des milliers de pages, dont les 300 pages déjà mentionnées, ont été rendues publiques après des procédures légales de déclassification.

Le journaliste Müller n'a pas découvert ces rapports par lui-même mais c'est une source inconnue qui les lui a fournis. Et confronté à une enquête exhaustive, celui-ci a soumis ces rapports à des collègues journalistes de la *Zweites Deutsches Fernsehen* (ZDF), chaîne de télévision allemande, au journal *The Washington Post*, à la *Schweizer Radio und Fernsehen* (SRF), chaîne de radio-télé diffusion publique suisse, au *cryptomuseum* à Eindhoven et à la plateforme de recherche néerlandaise ARGOS. L'enquête journalistique commune qui a suivi a donné lieu, entre février et avril 2020, à une série d'articles de presse dont celui du 11 février 2022 publié par *The Washington Post* et repris par la SRF et la ZDF [24]. L'attention médiatique n'a d'ailleurs été que de courte durée. De manière générale, l'opinion publique n'était que modérément intéressée par ce scandale des écoutes.

---

22 COMITÉ PERMANENT R, Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel PEGASUS (2021.286).

23 Peter F. Müller (également ortographié '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. APERCU HISTORIQUE DE LA SOCIÉTÉ CRYPTO AG [25]

La société AB Cryptoteknik fut fondée en 1920 par Arvid Gerharm Damm à Stockholm. A son décès, peu avant la Seconde Guerre mondiale, la société passa aux mains de Boris Hagelin, ingénieur, né dans l'actuel Azerbaïdjan et de nationalité suédoise.

Dans les années 30, lors d'un voyage aux États-Unis, Hagelin, installé alors en Suisse, fit la connaissance de l'Américain William Friedman qui deviendra, ultérieurement, le chef du service d'espionnage américain NSA.

Au tout début de la Seconde Guerre mondiale, Hagelin émigra aux États-Unis et durant la guerre, sa société fournit des machines de cryptographie mécaniques à l'armée américaine.

C'est en 1951 que la collaboration entre Hagelin et Friedman se concrétisa réellement. Friedman travaillait, à cette époque, pour la *Armed Forces Security Agency* (AFSA) [26] et il proposa à Hagelin de développer des machines cryptographiques les plus en pointe et de s'en assurer le monopole, la vente de ces machines devant être réservée exclusivement, par *gentleman's agreement* pris entre les deux protagonistes, aux pays approuvés par les États-Unis.

Hagelin s'inscrivit dans cette optique et après avoir conclu l'accord mentionné avec Friedman, la société déménagea définitivement en Suisse en 1952, année au cours de laquelle les machines de cryptographie évoluèrent sous de nombreuses variantes ayant le plus grand succès international.

Entretemps, tant la CIA que l'AFSA, agence précédant la NSA, se mêlèrent des activités de la société, devenue CRYPTO AG. Ainsi, les États-Unis exigèrent notamment les brevets sur toutes les machines inventées et forcèrent le *gentleman's agreement*, conclu précédemment entre Hagelin et Friedman, à devenir un accord formel qui stipulait quels pays étaient autorisés à acquérir les nouvelles machines de cryptage.

Au milieu des années 60, la CIA et la NSA reprirent la main sur le développement technique des machines de cryptographie, celles-ci passant de la technologie mécanique à la technologie électronique. C'est ainsi que deux années plus tard, dès 1967 donc, un modèle électronique dont la NSA avait entièrement conçu le circuit électronique fut mis sur le marché. Dès ce moment, le développement des machines de cryptage dépendra entièrement de la NSA, premier pas vers la perte d'indépendance de la société CRYPTO AG.

---

25 Cet aperçu se fonde en grande partie sur les contributions de (1) Melina J. Dobson, Operation RUBICON, Germany as an Intelligence Great Power, Intelligence and National Security, volume 35, numéro 5, août 2020, pp. 608-622, de (2) Richard Aldrich, Peter Müller, David Ridd and Erich Schmidt-Eenboom, Operation Rubicon : sixty years of German-American success in Signals Intelligence, ibidem, pp.603-607 de (3) Sarah Mainwaring, Operation Rubicon and the CIA's secret SIGINT empire, ibidem, pp. 623-640 et de (4) Greg Miller, Washington Post, The Intelligence coup of the century, 11 février 2020.

26 L'AFSA était le service qui, depuis mai 1949, centralisait toutes les activités de cryptographie aux États-Unis. Le service relèvait du *US Department of Defence* et devenait, en décembre 1951, la NSA.

En 1969, le chef du service de cryptographie allemand, William Goeing, proposa à Hagelin de vendre sa société à l'Allemagne en partenariat avec les États-Unis. Le directeur de la CIA Richard Helms approuva la proposition et finalisa les détails de l'accord stipulant l'unique collaboration entre les États-Unis et l'Allemagne et exigeant que la France en soit tenue strictement écartée.

Le 4 juin 1970, l'acquisition officielle de la société CRYPTO AG fut actée et passa, pour un montant de 25.000.000 francs suisses, à la Treuhand Gesellschaft-Munich. Quelques jours plus tard, le 12 juin 1970, l'accord concret conclu entre les deux services de renseignement américain et allemand, le *memorandum of understanding* (MoU), fut signé par la CIA et le BND.

Dans les décennies qui suivirent, en pleine Guerre froide donc, les machines de cryptage CRYPTO AG fournirent une mine d'informations aux services de renseignement américains et allemand. Selon certaines estimations, dans les années 80, environ 40 % de l'ensemble des communications provenaient des machines CRYPTO AG.

Entretemps, et depuis de nombreuses années, la société CRYPTO AG était devenue une société renommée détenant un quasi-monopole en matière de cryptologie aux quatre coins du monde. La société comptait ainsi des clients dans plus de 120 pays du monde, des états bien sûr mais également des organisations internationales. Ainsi, la société vendit des appareillages de cryptographie notamment à la Belgique, à l'Egypte, à l'Irak, à l'Iran, à l'Arabie Saoudite, à la Syrie, à la Jordanie, à l'Inde, à l'Indonésie, à la Malaisie, à la Corée du Sud, à la Thaïlande, à l'Italie, à l'Irlande, à l'Espagne et même à la Cité du Vatican ou encore au Japon, au Viêtnam, au Portugal, au Pakistan, au Bangladesh, au Myanmar (Birmanie) ainsi qu'aux Philippines et aux juntes militaires d'Amérique du Sud.

En 1993, l'Allemagne décida de se retirer du programme et laissa la société CRYPTO AG aux mains de la CIA qui fut, au cours des 25 années suivantes, seule propriétaire de la société.

Le programme d'espionnage RUBICON ne fut jamais rendu public mais de l'étude de rapports établis, il appert que, dans les années qui ont suivi le lancement de l'opération RUBICON, nombre pays avaient connaissance, dans une plus ou moins grande mesure, de certains aspects dudit programme d'espionnage, ce notamment depuis les années 80, époque des premiers questionnements sur les activités de la société CRYPTO AG [27]. En août 2020 encore, la revue *Intelligence and National Security* consacra une partie d'un de ses numéros à l'affaire RUBICON [28]. Quatre articles d'experts universitaires y traitaient des activités SIGINT des services de renseignement américains et allemand via la société 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.

L'opération, connue sous la dénomination RUBICON, peut tout simplement être considérée comme un succès phénoménal. Pendant des décennies, CRYPTO AG domina le marché des machines de cryptage. La société vendit des appareils de cryptage à quelque 120 pays du monde et organisations internationales et fit croire aux acheteurs que les appareillages étaient particulièrement sûrs, sans que les acquéreurs ne se posent jamais la moindre question quant à sa fiabilité [29].

II.5 UNE COMMISSION D'ENQUÊTE PARLEMENTAIRE SUISSE

Les révélations sur les liens entre la société CRYPTO AG et certains services de renseignement étrangers provoqua une vive émotion en Suisse. Les autorités helvétiques chargèrent un ancien juge fédéral pour enquêter sur ce dossier.

En février 2020, la Délégation des Commissions de gestion des Chambres fédérales (DélCdG), Commission parlementaire responsable du contrôle des services de renseignement, fit savoir qu'elle ouvrait, elle aussi, une enquête sur les liens éventuels entre les services de renseignement fédéraux et les services de renseignement étrangers impliqués dans ce dossier. Un autre point d'attention de l'enquête étant de déterminer si et dans quelle mesure le Conseil fédéral avait eu connaissance des faits relatifs à CRYPTO AG. La DélCdG approuva son rapport d'inspection CRYPTO AG et publia ses conclusions [30] en toute fin 2020.

Il ressort du rapport d'enquête de la DélCdG que le Service de Renseignement Stratégique (SRS), prédécesseur de l'actuel Service de Renseignement de la Confédération (SRC), savait depuis l'automne 1993 que des services de renseignement étrangers se cachaient derrière la société CRYPTO AG, que celle-ci était « entre les mains » de services de renseignement étrangers et qu'elle exportait des appareillages sensibles dont le cryptage pouvait être déchiffré avec un minimum d'effort.

Si le cadre légal, en Suisse, permettait aux services de renseignement suisse et étrangers de de faire appel conjointement à une société établie en Suisse pour collecter des informations à l'étranger, la DélCdG déplorait que les autorités politiques suisses n'en aient été informées qu'en toute fin 2019 seulement, constatant en outre que le SRS, à l'époque, avait accès à des informations sur CRYPTO AG et que celles-ci étaient un secret bien gardé au sein de la direction de ce service.

La DélCdG formula plusieurs recommandations dans son rapport d'enquête. Les recommandations les plus importantes étaient les suivantes :

1. La Confédération ne pouvait acheter d'appareillages de cryptage auprès de fournisseurs étrangers, les fournisseurs suisses devant garantir à la Confédération qu'ils avaient le contrôle des aspects liés à la sécurité du développement et de la production de ces dispositifs ;

---

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. Le Département fédéral de la Défense devait veiller à ce que l'armée conserve suffisamment de compétences spécialisées en matière de cryptologie. Il devait faire en sorte que les compétences en matière de cryptographie et de cryptoanalyse puissent être exploitées de manière optimale ;
3. Le Département fédéral de la Défense devait veiller à ce que les capacités de cryptoanalyse puissent rester adaptées aux besoins dans le domaine de l'interception des communications.

II.6. RUBICON ET LES SERVICES DE RENSEIGNEMENT BELGES

Le Comité permanent R a interrogé les deux services de renseignement belges, la VSSE et le SGRS, quant à leur évaluation d'une éventuelle compromission interne suite au dossier RUBICON révélé.

II.6.1. La position de la VSSE

Résumé des informations classifiées
D'une part, ce n'est que par les révélations dans la presse que la VSSE a été informée des liens entre la société CRYPTO AG et les services de renseignement américains CIA et NSA ainsi que le service de renseignement allemand BND. D'autre part, il ne peut être exclu que certains services publics belges aient fait usage de dispositifs CRYPTO AG ou de dispositifs similaires. La VSSE a interrogé ses partenaires mais n'a obtenu que très peu d'informations exploitables.

II.6.2. La position du SGRS

Dès le moment où le scandale des écoutes RUBICON fut mentionné dans la presse, le SGRS fit publier, le 12 février 2020, via Belga, un communiqué dans lequel il déclarait : « *De ADIV is op de hoogte van de RUBICON-affaire en onderzoekt de mogelijke omvang van de vermelde afluisterpraktijken* » [31]. Le SGRS le confirma également au journal De Tijd [32], affirmant que : « *De ADIV doet er alles aan om zich tegen hen (bedoeld wordt : afluisterpraktijken) te wapenen en maakt 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* » [33].

Le Comité permanent R demanda des précisions au SGRS, les mots choisis dans le communiqué de presse laissant supposer que le service de renseignement militaire était au courant depuis bien longtemps de l'opération RUBICON révélée. Aux dires ultérieurs du SGRS, l'intention du service n'était nullement d'affirmer qu'il était au courant de l'existence d'une

---

31 Le SGRS est au courant de l'affaire RUBICON et examine actuellement l'ampleur potentielle des mises sur écoute dont il est question (traduction libre).

32 L. Bové, *De Tijd*, "België onderzoekt jarenlange spionage door CI", 12 février 2020.

33 Le SGRS met tout en œuvre pour s'en protéger (sont visées ici les mises sur écoute) et, surtout, met un point d'honneur à respecter le cadre légal en la matière d'une part et, d'autre part, à appliquer un code moral à l'égard de ses partenaires / alliés, dans un monde où, sans être naïf, la confiance va souvent de pair avec la prudence dans le cadre de l'utilisation de matériel de cryptographie (traduction libre).

quelconque compromission d'appareillages CRYPTO AG et de la secrète collaboration entre les services de renseignement américains et allemand en la matière.

Résumé des informations classifiées
Sur base d'une recherche effectuée dans les archives, l'éventuelle compromission par un dispositif CRYPTO AG au sein du service est considérée comme extrêmement minime. Des éléments indiquent toutefois l'utilisation, dans un cas isolé et avant les années 70, d'un tel dispositif au sein de la Défense.

II.7. L'ÉVALUATION DU COMITÉ PERMANENT R SUR LA BASE DES RÉPONSES FOURNIES

Sur base des informations classifiées fournies tant par la VSSE que par le SGRS au Comité permanent R, la compromission des dispositifs utilisés par les services est qualifiée de « minime », tout comme les dommages pour le Département de la Défense qualifiés d'« extrêmement minimes ».

Cependant, effectuer une analyse de risques probante fut tout sauf simple pour le Comité permanent R et les services de renseignement. En effet, d'une part, le laps de temps entre le scandale des écoutes RUBICON et le moment où l'enquête a été réalisée fut extrêmement long. D'autre part, l'enquête permettant de déterminer l'éventuelle fragilisation d'un dispositif de chiffrement requerrait une enquête physique et opérationnelle de chaque dispositif suspect, ce qui n'était plus possible, les appareillages CRYPTO AG n'étant plus disponibles pour réaliser une telle analyse.

II.8. PERTINENCE ACTUELLE

Résumé des informations classifiées

Il ressort de l'enquête de contrôle que, pour la VSSE, le scandale des écoutes démontre la nécessaire prudence à avoir lors de l'utilisation d'appareillages étrangers de cryptographie. Le SGRS souligne, lui, qu'il y a des leçons importantes à tirer de ce scandale et que le service a entrepris, depuis un certain temps déjà, des démarches extrêmement poussées en la matière.

III. MAXIMATOR

III.1. Les révélations du Professeur Bart Jacobs sur le réseau SIGINT MAXIMATOR

Le scandale des écoutes RUBICON est déjà en soi une affaire surprenante. Cette affaire d'écoutes a révélé que des services de renseignement américains et allemand étaient propriétaires d'une société suisse de cryptage fournissant des appareillages de cryptographie pouvant être compromis. En effet, cette société, CRYPTO AG, a vendu à d'autres pays ou organisations internationales diverses, pendant des dizaines d'années, des dispositifs de chiffrement, convainquant les acquéreurs de la très grande fiabilité de ceux-ci. Ce procédé, mis en œuvre, a ensuite permis aux autorités américaines et allemandes de pouvoir décoder toutes les communications cryptées, émises ou reçues, par les acheteurs.

Suite aux révélations sur CRYPTO AG, une contribution scientifique du Professeur Bart Jacobs est parue le 7 avril 2020 [34]. Jacobs publia sa contribution dans la revue scientifique britannique *Intelligence and National Security*, sous le titre : « *MAXIMATOR, European signals intelligence cooperation, from a Dutch perspective* » [35].

Selon Jacobs, une collaboration SIGINT, au niveau européen, fut instaurée secrètement en 1976. Au départ, seuls trois pays étaient concernés, soit le Danemark, la Suède et l'Allemagne. Les Pays-Bas rejoignirent l'alliance en 1978, la France l'intégrant en 1985 [36]. Selon le Professeur Jean-Jacques Quisquater, la France en prit d'ailleurs le *lead* dès 2006 et les réunions en étaient le plus souvent présidées par la direction technique de la DGSE [37]. Cette structure de coopération « d'Europe du nord-ouest », prendra par la suite la dénomination MAXIMATOR [38] et cette structure était, en partie, une réponse aux *FIVE EYES* [39].

Jacobs soulignait encore, et ceci est important, que le réseau MAXIMATOR s'appuyait considérablement sur les informations fournies par le partenaire allemand, informations émanant du « craquage » de communications « CRYPTO AG ». Jacobs laissait encore entendre que les services participant au programme recevaient non seulement des informations interceptées et décodées par les Allemands mais également les moyens de les déchiffrer eux-mêmes.

---

34 Le Prof. Dr. Bart Jacobs enseigne depuis 2003 la sécurité informatique à l'université de Nijmegen et est déjà l'auteur de dizaines de contributions scientifiques en la matière. Il est également membre du conseil d'experts de la *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* (CTIVD, Pays-Bas).

35 Publié dans la revue scientifique britannique *Intelligence and National Security*, volume 35, numéro 5, août 2020, pp. 659-668. Peut également être consulté sur le site Internet suivant : *https://tandfonline.com*

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

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

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

39 FIVE EYES est une structure de coopération SIGINT regroupant des services d'Australie, du Canada, du Royaume-Uni, de Nouvelle-Zélande et des États-Unis.

Nonobstant le caractère particulièrement secret du programme MAXIMATOR, plusieurs autres pays européens apprirent de l'existence de cette structure de coopération. Ceux-ci prirent alors l'initiative de demander à intégrer ledit réseau essuyant, pour la plupart, un refus, souvent pris en raison d'un manque d'expérience ou d'expertise en matière de cryptoanalyse.

Il est important de constater que la Belgique fut exclue du réseau MAXIMATOR et quant à cette exclusion, Jacobs écrivait que « Certains pays ont été délibérément exclus (du réseau) parce qu'ils étaient considérés au sein de l'alliance MAXIMATOR comme des pays manquant d'une expérience et / ou d'une expertise (Signal / crypto) pertinente. (...) La Belgique est l'exception notable en Europe du Nord-Ouest ; elle n'a pas été invitée à devenir membre de MAXIMATOR par manque de capacités SIGINT (et COMSEC) » [40] (traduction libre).

L'auteur précisait encore, en une note de bas de page, que « Par conséquent, la Belgique n'était pas protégée par les activités des membres de MAXIMATOR et a fait l'acquisition du dispositif le moins sécurisé de CRYPTO AG, ce qui ressort également des documents du BND et de la CIA qui ont fuité. Ses communications qui transitaient par les dispositifs AG CRYPTO ont ainsi été écoutées tant par les FIVE EYES que par la structure de coopération MAXIMATOR » [41] (traduction libre).

Le Comité permanent R juge cette communication très préoccupante pour la Belgique [42].

Ainsi, selon les affirmations de Jacobs, la Belgique (1) aurait non seulement été tenue délibérément à l'écart d'une importante structure de coopération en matière de renseignement, mais aussi (2) aurait utilisé les dispositifs de cryptographie les moins sécurisés et (3) aurait même été mise sur écoute par les structures de coopération occidentales SIGINT auxquelles elle n'avait pas pu adhérer.

III.2. MAXIMATOR et les services de renseignement belges.

Le Comité permanent R a posé la question très spécifique aux deux services : connaissiez-vous l'existence du réseau MAXIMATOR avant la parution de l'article du Professeur Bart Jacobs ?

Selon les réponses apportées tant par la VSSE que par le SGRS au Comité permanent R, les deux services n'auraient pas été au courant de l'existence de l'alliance MAXIMATOR. Les services ont déclaré, en effet, très explicitement qu'ils n'avaient été informés de l'alliance qu'à la suite de la publication de l'article du Professeur Bart Jacobs.

---

40 *"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".*

41 *"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)".*

42 Le Professeur Quisquater va jusqu'à la qualifier de '*pathétique*'. Voir : J.-J. QUISQUATER, Cruel paradoxe de la cryptographie belge, 20 mai 2020, www.regional-it.be/detached/cruel-paradoxe-de-la-cryptographie-belge

Le Comité permanent R a ensuite confronté les services quant à l'affirmation figurant dans un article de presse néerlandais paru dans *The Post Online* traitant, en réalité, de la manière dont le ministre de l'Intérieur néerlandais avait répondu à certaines questions parlementaires concernant MAXIMATOR [43] et, selon lequel, la Belgique voulait rejoindre l'alliance mais que la trop grande faiblesse de « *son service de renseignement* » avait été avancée comme argument pour se voir refuser toute adhésion. Dans leur réponse, les deux services sont restés catégoriques affirmant n'avoir eu aucunement connaissance du réseau MAXIMATOR avant les révélations du 7 avril 2020, la VSSE indiquant d'ailleurs que cette affirmation n'était pas exactement en phase avec celle du Professeur Bart Jacobs et que cette information n'avait été reprise par aucuns autres média, pointant encore que *The Post Online* était généralement décrit comme une publication peu fiable.

[43] *The Post Online*, Anke Bijleveld schoffeert de Tweede Kamer, minister zwijgt over het geheime spionagegenootschap MAXIMATOR, 8 mai 2020.

IV. CONCLUSIONS

1. Les informations publiées suite au scandale des écoutes ont révélé que la société suisse CRYPTO AG avait mis sur le marché, des décennies durant, des dispositifs de chiffrement, permettant de déchiffrer également aisément les messages cryptés, contrairement à ce qu'en pensaient les pays et autres organisations internationales diverses en ayant fait l'acquisition. La société CRYPTO AG travaillait depuis longtemps, en secret et de manière très intensive, avec des services de renseignement américains et allemand.

2. Le secret entourant, pendant des décennies, tant le chiffrage que le déchiffrage par les États-Unis et l'Allemagne de messages cryptés par les appareillages de CRYPTO AG reste remarquable.

3. Certains pays ont néanmoins pris conscience des opérations d'écoutes et, par la suite, certains d'entre eux y ont même été impliqués.

4. Les services de renseignement belges affirment n'avoir jamais eu connaissance de l'Affaire CRYPTO AG, ce jusqu'à la parution d'articles de presse y relatifs.

5. Les services de renseignement belges ont été délibérément tenus à l'écart du réseau secret SIGINT MAXIMATOR.

6. La Belgique a fort probablement fait l'objet d'activités d'interception de ses messages cryptés par le réseau SIGINT MAXIMATOR.

V. RECOMMANDATIONS

Bien que la problématique étudiée soit très ancienne, le Comité permanent R formule néanmoins trois recommandations à caractère général :

1. Les services de renseignement (ainsi que toutes les autorités) belges doivent être conscients des risques qu'à tout moment les messages cryptés, tant envoyés que reçus, peuvent faire l'objet d'activités de décryptage selon l'évolution des technologies.

2. Les services de renseignement belges doivent garder une attention toute particulière aux développements technologiques étrangers en matière de cryptage.

3. Les experts en cryptologie des services de renseignement belges doivent vérifier dans quelle mesure une technologie cryptographique nationale ne doit pas être développée.