COMITE PERMANENT DE CONTROLE DES SERVICES DE RENSEIGNEMENT ET DE SECURITE

Notice n°2021.286

Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel PEGASUS

Rapport final – le 17 octobre 2022

TABLE DES MATIERES

I. INTRODUCTION

I.1. ORIGINE DE L'ENQUETE

Le 18 juillet 2021, dix-sept médias internationaux, dont *Le Soir* et *Knack* en Belgique, révélaient l'existence du logiciel PEGASUS, vendu par une société israélienne, NSO Group, à des gouvernements et à leurs services de renseignement et/ou de sécurité pour leur permettre d'administrer les smartphones de leurs 'cibles'. Selon les révélations, le logiciel PEGASUS permet de se rendre secrètement administrateur d'un smartphone et d'en puiser toutes les informations possibles, à savoir des notes vocales, des textes (messages et e-mails), des photos, mais également des données de géolocalisation, etc.

Le consortium de journalistes révélait avoir eu accès à plus de 50.000 numéros de téléphone qui auraient été pris pour cibles par des clients utilisateurs du logiciel PEGASUS. Parmi les personnes ciblées figureraient des personnes soupçonnées de crimes graves, mais aussi des chefs d'État, des responsables politiques, des diplomates, des avocats, des hommes et des femmes d'affaires, des militants des droits humains, des journalistes, des acteurs de la société civile, etc.[1]

Parmi les 50.000 numéros de téléphone figurent plusieurs numéros belges.[2] Par ailleurs, *Le Soir* faisait état du fait que selon trois sources, « *la Belgique figurerait parmi les clients de NSO* ». Ni la Sûreté de l'État (VSSE), ni le Service Général du Renseignement et de la Sécurité (SGRS), ni la Police fédérale n'ont souhaité réagir auprès des médias, évoquant une information « confidentielle ».[3]

Alors que dans le cadre de l'affaire Snowden[4], les révélations portaient sur l'existence d'un programme de surveillance de masse mis en place par les Américains et les Britanniques, l'affaire PEGASUS a mis en évidence la commercialisation par une société privée, à des États

---

1 *Le Monde*, 18 juillet 2021, ('Projet Pegasus : révélations sur un système mondial d'espionnage de téléphones') ; *Le Soir*, 18 juillet 2021, ('Projet Pegasus : un logiciel de cyberespionnage quasiment indétectable').

2 *Le Soir*, 18 juillet 2021, ('Projet Pegasus : un logiciel de cyberespionnage quasiment indétectable').

3 *Ibidem.*

4 Le Comité a effectué une enquête de contrôle à cet égard, à savoir l'affaire PRISM - Snowden en 2013 (*Rapport d'activités 2014*, 8 et s.). Dans le cadre de cette enquête, le Comité avait fait appel à une expertise externe. Mathias Vermeulen ('*Les révélations de Snowden, interception massive de données et espionnage politique. Étude des sources ouvertes*'). Professeur Annemie Schaus ('*Consultation sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique*'). Ajoutons que ce n'était pas la première fois que le Comité permanent R effectuait une enquête de contrôle sur l'interception de données. Le Comité a ainsi remis un rapport dans le dossier ECHELON (*Rapport d'activités 1999*, 23 et s.) et l'affaire SWIFT (*Rapport d'activités 2006, 39* et s.).

et à leurs services de sécurité, d'un logiciel permettant de s'introduire pernicieusement dans un smartphone.

Ces révélations posent une série de questions qui sont à l'origine de la présente enquête. Force est en effet de s'interroger sur l'utilisation (éventuelle) de ce (type de) logiciel par nos services de renseignement. Mais il y a lieu également de s'atteler à vérifier si nos services de renseignement sont en capacité de détecter l'usage de ce (type de) logiciel en Belgique et/ou sur des citoyens et des intérêts belges.

Ne sommes-nous pas confrontés à la situation où cette utilisation permettrait à des puissances étrangères de chercher notamment à réduire au silence des journalistes, à s'en prendre aux militants, à écraser leur opposition qui résiderait sur notre territoire, voire à mettre d'innombrables vies en péril comme le souligne Amnesty International ?[5] En tout état de cause, les révélations de l'affaire PEGASUS soulèvent la question de la protection de la vie privée des citoyens. Il s'agirait potentiellement d'une atteinte grave aux droits humains en violation de l'article 12 de la Déclaration des Droits de l'Homme.

I.2. FINALITES DE L'ENQUETE

L'article 33 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L. Contrôle) dispose que le Comité permanent R enquête sur les activités et les méthodes des services de renseignement. L'article 1er L. Contrôle précise que ce contrôle porte en particulier sur *« la protection des droits que la Constitution et la loi confèrent aux personnes, ainsi que sur la coordination et l'efficacité de l'Organe de coordination pour l'analyse de la menace »*.

Le Comité permanent R n'est pas compétent pour s'enquérir de l'utilisation d'un logiciel tel PEGASUS par d'autres services publics (police, douanes, etc.) ou par des personnes morales ou physiques, comme les détectives privés. Ainsi, l'enquête portera exclusivement sur les services de renseignement belges, à savoir la VSSE et le SGRS.

Si les révélations autour du logiciel PEGASUS soulèvent plusieurs questions, le Comité distingue deux volets dans la présente enquête. Il s'agit, d'abord, de vérifier si les services de renseignement belges utilisent le logiciel commercialisé par NSO Group (ou équivalent) dans le cadre de leurs missions, et si cette utilisation est conforme au cadre légal en vigueur. Ensuite, face à l'utilisation du logiciel PEGASUS par des services étrangers (services de renseignement et/ou de sécurité, entreprises privées, etc.) contre des personnes physiques

[5] Amnesty International, 18 juillet 2021 ('Espionnage téléphonique à grande échelle : le projet Pegasus').

et/ou morales belges, l'enquête vise à déterminer si les services de renseignement belges sont outillés pour identifier et gérer, voire contrer, cette menace.

I.3. DEROULEMENT DE L'ENQUETE ET METHODOLOGIE

Le 27 juillet 2021, le Comité permanent R a informé la présidente de la Chambre des représentants, ainsi que les ministres de la Justice et de la Défense, de l'ouverture de la présente enquête de contrôle.
Par la suite, la première étape a consisté à composer un dossier d'information, en s'appuyant sur des informations provenant de sources ouvertes.

Le 20 août 2021, le Comité a communiqué une première série de questions à la VSSE et au SGRS. Dans les mois qui ont suivi, des questions complémentaires ont été posées. Les services ont quant à eux transmis des notes et autres documents au Comité. Plusieurs rencontres ont par ailleurs été organisées avec des collaborateurs du SGRS.

Le Comité a reçu les dernières informations de la part des services le 29 août 2022.

II. L'EXISTENCE DU LOGICIEL PEGASUS RÉVÉLÉE PAR LA PRESSE

Fin juillet 2021, *Forbidden Stories*, un consortium de plus de 80 journalistes de dix-sept médias dans onze pays, a révélé l'utilisation – abusive voire illégale – du logiciel PEGASUS de la société israélienne NSO Group.[6] Ce logiciel – de type *Remote Infection Technologies*, c'est-à-dire pouvant être installé à distance sur un smartphone – permet d'avoir entièrement accès au contenu de l'appareil infecté (SMS, e-mails, activités sur Internet, micro, appareil photo, appels téléphoniques et contacts).[7]

La base de l'enquête des journalistes de *Forbidden Stories* est constituée d'une liste de 50.000 numéros de téléphone qui ont fuité vers le collectif et qui auraient été la cible d'une infection par PEGASUS. Après plusieurs mois d'enquête, les journalistes ont révélé comment, dans de nombreux pays, des responsables politiques, des centaines d'opposants, avocats et journalistes sont devenus la cible des gouvernements qui utilisent cette arme digitale.

---

6 Les articles de presse ont fait état de l'utilisation de PEGASUS par des services de renseignement et de sécurité pour espionner des journalistes, politiques, diplomates, activistes des droits humains dans de nombreux pays tels l'Arabie Saoudite, l'Azerbaïdjan, le Maroc, la Hongrie, le Mexique, l'Inde, la France, le Royaume-Uni, la Finlande, le Rwanda, le Togo, la Turquie, l'Espagne, les Émirats arabes unis, le Bahreïn, la Pologne, le Kazakhstan, le Salvador, la Thaïlande, l'Ouganda et Israël. Depuis la fin de l'été 2021, des incidents ont été relevés dans le monde entier. La Belgique n'a pas été épargnée.

7 https://www.amnesty.be/infos/actualites/pegasus.

II.1. DES CIBLES BELGES

Selon *Knack* et *Le Soir*, on retrouve, dans la liste des numéros de téléphone qui a fuité, une douzaine de numéros belges. Parmi ceux-ci, *Knack* a rapporté que les numéros de téléphone des hommes politiques belges Louis et Charles Michel figurent sur la liste.[8]

Le *Security Lab* d'Amnesty International et le *Citizen Lab* de l'Université de Toronto ont développé un programme baptisé *Mobile Verification Kit* permettant de retrouver des traces du logiciel grâce à des indicateurs de compromission (*Indicators of Compromise* (IoC)).[9] En juillet 2021, le programme a identifié des traces de PEGASUS dans le téléphone de Carine Kanimba, la fille de l'opposant rwandais Paul Rusesabagina.

En septembre 2021, a également été rapportée l'infiltration des smartphones du journaliste belge Peter Verlinden, spécialiste de l'Afrique centrale, et de son épouse, Marie Bamutese, politologue et écrivaine qui a notamment écrit sur le génocide rwandais. L'intéressé a fait savoir dans les médias que son smartphone et celui de son épouse avaient été analysés par le SGRS.[10]

Début novembre 2021, le smartphone de Maliha El Mahjoub, un activiste belge de 36 ans originaire du Sahara occidental qui travaille comme bénévole pour un collectif de défenseurs sahraoui des droits humains, a été analysé par le Security Lab d'Amnesty International. Selon ce laboratoire, des traces d'un logiciel malveillant (*malware*), associé à PEGASUS, ont été décelées. Le premier *malware* aurait été installé dans son GSM en janvier 2021, une période au cours de laquelle l'intéressé dit avoir été en contact avec l'ambassade américaine à Rabat. Des traces ont également été retrouvées dans son GSM en mars, avril, mai et juin 2021.[11]

II.2. LES REVELATIONS DU *NEW YORK TIMES*

Le 28 janvier 2022, le *New York Times* (NYT) a publié de nouvelles révélations sur l'utilisation du logiciel PEGASUS.[12] Dans cet article, le NYT révèle qu'en juin 2019, le service de sécurité américain *Federal Bureau of Investigation* (FBI) menait des tests avec le logiciel PEGASUS, en présence d'ingénieurs israéliens. À ce moment-là, il y avait déjà des indications selon lesquelles PEGASUS était utilisé au Mexique et en Arabie Saoudite pour espionner des journalistes et des activistes des droits humains.

Le NYT a également révélé comment, à la demande des autorités américaines, il a été demandé à NSO de programmer l'outil afin qu'il ne puisse pas être utilisé pour espionner les

---

8 K. CLERIX, *Knack*, 20 juillet 2021 ('Pegasus Project: Macron en Michel in het vizier van Marokko').

9 *Knack*, 27 juillet 2021 ('Dit is Carine, het eerste Belgische slachtoffer van Pegasus').

10 K. CLERIX, *Knack*, 17 septembre 2021, ('Pegasus-spyware: iPhone van journalist Peter Verlinden gehackt').

11 J. MATRICHE, Le Soir, 23 novembre 2021, ('Une nouvelle victime belge du logiciel espion Pegasus').

12 M. HILLGARTNER, *The New York Times Magazine*, 28 janvier 2022, ('The Battle for the World's most Powerful Cyberweapon').

numéros de GSM américains. Toutefois, à partir du moment où le FBI a manifesté son intérêt pour lui-même utiliser PEGASUS, un nouveau projet PHANTOM a été lancé. Ce programme aurait permis aux seuls services de sécurité américains d'utiliser PEGASUS sur des cibles américaines.

Finalement, il aurait été décidé à l'été 2021 de mettre un terme à la collaboration entre le FBI et NSO Group, à la suite des révélations dans la presse qui ont même eu pour conséquence de voir NSO Group repris comme entité dans une *blacklist* du Département du commerce des États-Unis (*infra*).

II.3. REACTIONS AUX REVELATIONS DANS LA PRESSE

Les révélations autour de l'utilisation/du détournement du logiciel PEGASUS aux quatre coins du monde ont suscité des réactions aussi bien dans le privé que dans le public et lancé un débat de société sur l'utilisation des technologies de surveillance électronique sur des entreprises privées, des mouvements citoyens ou des autorités politiques.

II.3.1. Au sein du secteur privé

II.3.1.1. Les contestations de NSO Group

Le 18 juillet 2021, le *Washington Post* a publié une lettre de la société NSO Group qui a commercialisé PEGASUS, en réaction aux premiers articles du consortium journalistique dans le cadre du projet PEGASUS.[13] NSO Group y contestait les allégations selon lesquelles la société aurait eu accès à des données des 'cibles' recueillies et traitées par ses clients, et affirmait ne pas exploiter elle-même les systèmes qu'elle vendait. La société niait également que les autorités israéliennes contrôlaient les systèmes utilisés par les clients de NSO Group.

En octobre 2021, NSO Group a par ailleurs adressé un courrier aux Nations Unies, dans lequel la société affirmait soutenir la création d'un cadre légal sous les auspices des Nations Unies pour prévenir les atteintes aux droits et libertés du secteur. NSO disait avoir lancé une enquête interne sur l'utilisation de son outil pour permettre aux gouvernements de lutter contre les réseaux criminels et les groupes terroristes. Le groupe affirmait suivre des règles strictes avant d'octroyer à ses clients le droit d'utiliser son logiciel et avoir également mis en place des procédures sévères en cas de mauvaise utilisation. Ces règles auraient déjà été appliquées pour écarter des clients potentiels de NSO Group. [14]

Le 3 novembre 2021, le Département du commerce des États-Unis a décidé de placer NSO Group sur une liste noire en raison *« du déploiement d'activités portant atteinte à la sécurité*

---

[13] *The Washington Post*, 18 juillet 2021, ('Response from NSO Group to the Pegasus Project').
[14] *Le Figaro*, 5 octobre 2021, ('Affaire Pegasus : NSO appelle à une régulation internationale').

nationale ou aux intérêts de la politique étrangères des États-Unis ».[15] Cela implique des restrictions en matière d'importation et de commerce et des contrôles sévères, susceptibles de compliquer les activités de NSO Group. Cette décision constitue également un message politique, susceptible de décourager les sociétés situées dans des pays alliés des États-Unis quant à la fourniture de biens et de services à NSO Group.

La société israélienne a dit toute sa consternation, assurant disposer d'« *une charte éthique rigoureuse, basée sur les valeurs américaines»*. Le 6 novembre 2021, le ministre israélien des Affaires étrangères, Yair Lapid, a tenu à rappeler que *« NSO est une entreprise privée, ce n'est pas un projet gouvernemental et donc, même si [elle] est désignée comme telle [par le Département du commerce des États-Unis], cela n'a rien à voir avec le gouvernement israélien »*.[16] Le ministère israélien de la Défense octroie cependant des licences d'exportation à NSO Group.[17]

II.3.1.2. Le secteur des télécommunications

Dans une interview du 24 juillet 2021 avec le journal britannique *The Guardian*, le CEO de WhatsApp déclarait que son entreprise avait, dès 2019, retrouvé des traces de pratiques d'espionnage illégales par le biais du logiciel espion de NSO Group.[18] Pas moins de 1.400 utilisateurs de l'application de messagerie instantanée WhatsApp auraient été victimes du logiciel espion, en ce compris des *« personnes occupant des postes de haute sécurité nationale »*.

À la suite de ces constatations, WhatsApp a intenté une action en justice contre NSO Group en octobre 2019, accusant la société privée d'être à l'origine *« d'une série de cyberattaques extrêmement raffinées et incontestablement abusives en violation de la loi américaine »*.[19]

Le 23 novembre 2021, Apple annonçait dans un communiqué de presse qu'elle intentait à son tour une action en justice contre NSO Group *« pour les tenir responsables de la surveillance et*

---

[15] Federal Register, 24 juin 2021, ('Addition of certain entities to the Entity list'). U.S. Department of Commerce, 3 novembre 2021, (Press release: 'Commerce adds NSO Group and other foreign companies to entity list for malicious cyber activities').

[16] *Reuters*, 6 novembre 2021, ('Israeli foreign minister distances government from blacklisted NSO Group').

[17] Les conditions d'exportation des biens à double usage, c'est-à-dire des technologies qui peuvent également être utilisées à des fins militaires, sont ancrées dans l'Arrangement de Wassenaar (*on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*) de 1996. Quarante-deux pays y ont adhéré, parmi lesquels la Belgique et les États-Unis. En revanche, Israël n'y a pas adhéré, mais a déclaré publiquement adhérer au principe de la politique d'exportation de l'arrangement. (https://mfa.gov.il/MFA/PressRoom/2019/Pages/Israeli-statement-at-the-conclusion-of-the-Wassenaar-arrangement-Outreach-Delegation-visit-20-November-2019.aspx).

[18] S. KIRCHGAESSNER, *The Guardian*, 24 juillet 2021, ('Officials who are US allies among targets of NSO malware, says WhatsApp chief').

[19] N. HOPKINS, S. KIRCHEGAESSNER, *The Guardian*, 29 octobre 2019, ('WhatsApp sues Israeli firm accusing it of hacking activists phones').

de l'investigation ciblées d'utilisateurs d'Apple ». Apple annonçait dans le même temps qu'elle offrirait 10 millions USD *« pour soutenir les enquêteurs et les partisans de la lutte contre la cybersurveillance »*.[20] Dans son communiqué, Apple mentionnait *« les parties financées par une autorité étatique, comme NSO Group »,* établissant ainsi un lien direct entre NSO Group et les autorités israéliennes.

II.3.2. Au sein du secteur public

Les premières révélations autour de l'utilisation du logiciel PEGASUS ont également encouragé les acteurs publics à réagir, notamment les ministres et services publics compétents. Des enquêtes judiciaires et/ou parlementaires ont également été ouvertes dans différents pays.[21] Plusieurs institutions intergouvernementales se sont par ailleurs saisies de cette affaire.

II.3.2.1. Les réactions du gouvernement fédéral belge

Les ministres de la Justice et de la Défense sont intervenus plusieurs fois sur l'affaire PEGASUS dans les premiers mois qui ont suivi les révélations dans la presse. Les questions parlementaires auxquelles ils visaient à répondre portaient notamment sur la question de savoir si les services de renseignement belges utilisaient ce logiciel, mais aussi si ceux-ci étaient en mesure de confirmer que des téléphones portables de Belges avaient été infectés à la demande de services étrangers.

- Quant à l'utilisation de l'outil par les services de renseignement belges :

En Commission de la Justice du 22 septembre 2021, le ministre de la Justice confirmait que les services de renseignement et de sécurité belges utilisaient eux aussi une technologie similaire dans le cadre de leurs missions, sans en préciser le nom, et ce pour des motifs opérationnels : *« Nos services de police et de renseignement utilisent dans le cadre des enquêtes pénales et des méthodes particulières de renseignement diverses solutions commerciales afin de leur permettre de répondre aux réquisitions des autorités compétentes et de prendre connaissance des informations privées. Toutefois, afin de garantir l'efficacité et la pérennité de ces capacités utilisées dans le cadre de la prise de connaissance légale des communications privées, aucun détail […] sur les outils et les méthodes utilisées ne peut être communiqué publiquement. […] In het algemeen kan ik u echter verzekeren dat in ons land dergelijke intrusieve en privacygevoelige onderzoeksmethodes alleen worden ingezet binnen het strikt wettelijk kader*

---

[20] *Apple*, 23 novembre 2021, ('Apple sues NSO Group to curb the abuse of state-sponsored spyware').

[21] En France, en Belgique, en Bulgarie et en Hongrie notamment, les autorités judiciaires se sont saisies de l'affaire. En Pologne, une commission spéciale de surveillance a été mise en place au Sénat afin d'analyser l'affaire et formuler des propositions pour réformer les activités des services de renseignement. Pour plus d'informations à ce sujet, voir European Parliament, 'Europe's Pegasus Gate – Countering spyware abuse, July 2022, pp. 28-33.

van de Bijzondere Opsporingsmethoden (BOM) voor de gerechtelijke diensten en de Bijzondere Inlichtingenmethoden (BIM) voor de inlichtingendiensten. […]." [22]

Et d'ajouter que les services de renseignement et de sécurité belges avaient fréquenté des salons commerciaux où NSO Group était représenté : *« Onze diensten hebben contact gehad met heel wat aanbieders van producten in het raam van de zoektocht naar nieuwe technieken en technologieën om zo goed mogelijk aan onze wettelijke opdrachten te kunnen voldoen. Bedrijven als NSO frequenteren dezelfde gespecialiseerde beurzen voor inlichtingen- en veiligheidsdiensten waar ook de Veiligheid van de Staat en de politie aanwezig zijn* ».[23]

Le ministre précisait encore que l'utilisation de ce type d'outils était nécessaire pour permettre aux services de renseignement et de sécurité en Belgique de remplir leurs missions : « *In een wereld waarin technologie en digitale communicatie steeds complexer en meer alomtegenwoordig worden, is het niet onlogisch dat inlichtingen- en veiligheidsdiensten op zoek gaan naar middelen om waardevolle informatie in te winnen. Waar grotere mogendheden de middelen hebben om eigen capaciteit te ontwikkelen op dit vlak, verkiezen andere ervoor om deze aan te kopen bij private bedrijven. Indien nodig worden dit soort tools ook ad hoc ontwikkeld in het kader van een bepaald dossier. Gezien de complexiteit om dit soort software te detecteren en het grote belang dat deze diensten hechten aan de afscherming van hun operationele middelen, is het niet mogelijk om hier een overzicht van op te maken omwille van de veiligheid van de staat* ».[24]

- Quant à l'utilisation du logiciel par des puissances étrangères contre des personnes de nationalité belge :

Le ministre de la Justice a qualifié cette pratique, si elle était confirmée, d'inacceptable : « *Dat deze middelen door buitenlandse mogendheden ook worden ingezet tegen politici, journalisten en activisten, is dan ook niet onwaarschijnlijk. De detectie ervan is bijzonder complex op technisch vlak. Dat neemt niet weg dat de inzet van zulke software door vreemde mogendheden tegen Belgische personen onaanvaardbaar is. Het is voor mij eens te meer een illustratie van het belang om zwaar te investeren in een versterking van onze inlichtingendiensten, los van het strafrechtelijk aspect […]* ».[25]

En octobre 2021, la ministre de la Défense indiquait pour sa part que « *le SGRS n'est actuellement pas en possession de la liste dite des 50.000 victimes évoquées par Amnesty ni de la liste partielle des éventuelles victimes belges. Un certain nombre de téléphones*

---

[22] Commission de la Justice du 22 septembre 2021, *Doc. Parl.,* CRIV 55 COM 577.

[23] *Ibidem.*

[24] *Ibidem.*

[25] *Ibidem.*

appartenant à ces cibles potentielles ont bien été examinés. Les services de renseignement belges approfondissent ce dossier, mais il est trop tôt pour communiquer des conclusions. »[26]

Au cours de la même période, le ministre de la Justice répondait que « *la Sûreté de l'Etat n'a pas encore enregistré de constats propres de l'utilisation de logiciels-espions à l'encontre de politiciens, journalistes ou activistes belges* ».[27]

- Quant aux liens entre NSO Group et les autorités israéliennes :

Un lien direct entre les deux est établi par la ministre de la Défense, qui déclarait en octobre 2021 à cet égard : « *il est de notoriété publique que le groupe NSO est sous la supervision directe et la réglementation du ministère israélien de la Défense, qui doit approuver toutes les ventes de ce logiciel Pegasus au préalable* ».[28]

II.3.2.2. L'Union européenne

II.3.2.2.1. La Commission européenne

Dès juillet 2021, l'utilisation présumée du logiciel PEGASUS à l'encontre de journalistes, d'hommes politiques ou d'activistes politiques a été publiquement condamnée par la présidente de la Commission européenne, Ursula Von der Leyen.[29]

En avril 2022, la Commission européenne a indiqué cependant qu'elle n'enquêterait pas sur les États membres ayant utilisé PEGASUS pour espionner des hommes politiques, des journalistes ou d'autres individus étant donné que « *it is really something for the national authorities and that the EU commission cannot deal with national security issues: people should seek justice at national courts' level* ».[30]

II.3.2.2.2. Le Parlement européen

Lors de sa séance du 10 mars 2022[31], le Parlement européen n'a pas adopté la même vision et a décidé de la constitution d'une commission chargée d'enquêter sur l'utilisation de

---

[26] Question de E. VAN HOOF au ministre de la Défense sur 'Le logiciel espion Pegasus' (Q.R., Chambre, 2020-2021, 6 octobre 2021, Q. n°326).

[27] Question de E. VAN HOOF au ministre de la Justice sur 'Le logiciel espion Pegasus' (Q.R., Chambre, 2020-2021, 25 août 2021, Q. n°135).

[28] Question de E. VAN HOOF au ministre de la Défense sur 'Le logiciel espion Pegasus' (Q.R., Chambre, 2020-2021, 6 octobre 2021, Q. n°326).

[29] *DW*, 19 juillet 2021, ('Pegasus spying reports 'completely unacceptable' says EU's von der Leyen').

[30] European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs, In-depth analysis 'Pegasus and surveillance spyware', 6 mai 2022, p.15.

[31] Pour un aperçu de l'ensemble des débats menés au sein du Parlement européen à cet égard, voir European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs, In-depth analysis 'Pegasus and surveillance spyware', 6 mai 2022, pp.15-16.

PEGASUS et de logiciels espions de surveillance équivalents au sein de l'Union européenne (DECISION (UE) 2022/480).[32] Les travaux de la Commission ont démarré en avril 2022 et les résultats sont attendus en avril 2023.

À la demande de cette Commission, une analyse approfondie (*In-Depth Analysis*) a été réalisée par le département des droits des citoyens et affaires constitutionnelles du Parlement européen sur l'utilisation du logiciel PEGASUS au sein de l'Union européenne.[33]

II.3.2.2.3. Le European Data Protection Supervisor

Le 15 février 2022, le Contrôleur européen de la protection des données (*European Data Protection Supervisor* (EDPS)), a publié un rapport sur l'utilisation des technologies de surveillance, plus précisément PEGASUS, au sein de l'Union européenne.[34]

Dans ce rapport, l'EDPS estime très peu probable qu'un logiciel malveillant tel que PEGASUS, qui fournit *de facto* un accès illimité à des données à caractère personnel (dont des données sensibles), pourrait satisfaire aux exigences de proportionnalité existantes.

L'EDPS écrit par ailleurs que *« PEGASUS constitue un changement de paradigme en ce qui concerne l'accès à une communication privée et un appareil privé, qui peut porter atteinte à l'essence de nos droits fondamentaux, c'est-à-dire le droit à la vie privée. (…) L'EDPS estime dès lors qu'une interdiction de développement de spywares dotés des possibilités de PEGASUS dans l'UE serait l'option la plus efficace pour assurer la protection de nos libertés et droits fondamentaux ».*

Néanmoins, dans l'hypothèse où ce type d'outils serait utilisé à l'avenir dans des situations exceptionnelles (telles que celle de prévenir une menace très sérieuse et imminente), l'EDPS dresse, en conclusion de son rapport une liste de huit étapes et mesures – qu'elle présente comme étant non exhaustives – visant à garantir un usage conforme à la loi de ce type d'outils. Parmi les mesures avancées, figure au premier rang celle de « ***Strengthening of democratic oversight over surveillance measures****: EU Members States should ensure effective oversight over the use of such surveillance measures. The role of data protection authorities, judicial control (ex ante and ex post), and democratic forms of scrutiny are absolutely necessary. Any form of evaluations and monitoring must be meaningful and effective. While there is no 'one-size-fits-all' solution, there is a need for a broad spectrum of actions in a modern checks and balances system. […]* ».[35]

---

[32] Parlement européen, 2019-2024, P9TA(2022)0071 https://www.europarl.europa/doceo/document/TA-9-2022-071_Fr.pdf .

[33] European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs, In-depth analysis 'Pegasus and surveillance spyware', 6 mai 2022.

[34] *"Preliminary Remarks on Modern Spyware"*, European Data Protection Supervisor, 15 February 2022, 11 p.

[35] *Ibidem*, pp. 9-10.

II.3.2.3. Les Nations Unies

En août 2021, plusieurs Rapporteurs spéciaux des Nations Unies aux droits de l'homme ont appelé la communauté internationale à imposer un moratoire mondial sur la vente et le transfert des technologies de surveillance jusqu'à la mise en place d'une réglementation robuste garantissant une utilisation conforme aux standards internationaux en matière de droits humains.[36]

Déjà en 2019, le Rapporteur spécial des Nations Unies sur les droits humains (*Special Rapporteur on Human Rights*) avait initié une enquête sur l'utilisation de technologies de surveillance électronique et sur l'impact de celles-ci sur les droits de l'homme. [37] Le rapport d'enquête révélait que des traces de PEGASUS avaient été décelées dès 2015 dans les smartphones de personnes, actives dans la lutte contre la corruption et le trafic de drogue au Mexique. Il était également établi qu'entre 2015 et la publication du rapport, des indices d'utilisation de PEGASUS avaient été trouvés dans quarante-cinq pays.

II.3.3. Le secteur associatif

De nombreuses organisations non gouvernementales[38] ont également réagi aux révélations parues dans la presse en dénonçant les menaces pour les droits de l'homme que ce type d'outils représente, et les abus constatés sur les journalistes et activistes notamment. Elles insistent sur l'urgence pour les États de légiférer afin de faire cesser ces menaces et abus.

III. LE FONCTIONNEMENT DU LOGICIEL PEGASUS : UNE ANALYSE TECHNIQUE SUCCINCTE

L'objectif de cette section est d'offrir au lecteur un aperçu succinct du fonctionnement du logiciel PEGASUS. Pour ce faire, on s'intéressera, dans un premier temps, aux méthodes utilisées pour infecter les téléphones ciblés, et ensuite, à l'impact d'une infection sur les téléphones contaminés. L'infrastructure sur laquelle le logiciel prend appui pour se déployer sera ensuite présentée, avant de se pencher sur les méthodes développées pour parvenir à détecter la présence du logiciel sur un smartphone infecté. Enfin, la question de l'existence d'éventuelles méthodes pour se prémunir d'une infection sera abordée.

---

[36] European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs, In-depth analysis 'Pegasus and surveillance spyware', 6 mai 2022, p.18.

[37] "*Surveillance and human rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression"*, UN General Assembly, 28 May 2019, p. 21 https://undocs.org/A/HRC/41/35.

[38] Telles que Amnesty International, Human Right Watch ou encore International Press Institute.

III.1. LES METHODES D'INFECTION

Le logiciel PEGASUS a été conçu pour s'introduire à distance dans un smartphone.

Il existe plusieurs méthodes pour infecter un smartphone via le logiciel PEGASUS :

- Infection physique : dès lors qu'on a un accès physique au téléphone.
- Infection par phishing : via un e-mail ou un sms avec un lien frauduleux sur lequel la cible clique.
- Infection '*zero-click*' : l'infection se produit via le réseau GSM (3G, 4G, Stingray ou IMSI catcher), un réseau wifi ou encore une autre technique sans fil (mais toujours à proximité de l'utilisateur).

Parmi ces trois méthodes, la plus redoutable est l'infection '*zero-click*' car elle ne requiert aucune « action » de la part de la personne ciblée. Pour la mettre en œuvre, des vulnérabilités dites '*zero-day*', c'est-à-dire inconnues par les fabricants de téléphones, sont utilisées. Il s'agit donc d'une faille critique contre laquelle il n'existe aucune protection. Les éditeurs de logiciels sont constamment à la recherche de bugs et de failles de sécurité afin de pouvoir les corriger. En parallèle, d'autres acteurs (sociétés privées telles que NSO Group, des hackers, voire des acteurs étatiques) cherchent eux aussi à détecter ces failles, non pas pour les corriger mais pour les exploiter.

NSO Group dispose (à l'instar de ses concurrents) d'une équipe de recherche étoffée dont le seul objectif est de déceler et d'exploiter de telles vulnérabilités car leur 'durée de vie' est très souvent limitée.[39] Il est, par exemple, tout à fait possible qu'une société décèle une vulnérabilité *'zero-day'* sur un iPhone et l'exploite, mais qu'Apple découvre cette vulnérabilité deux mois plus tard et effectue une mise à jour, la rendant inopérante. Il s'agit donc d'un jeu permanent du chat et de la souris.

C'est l'une des raisons pour laquelle un logiciel tel que PEGASUS nécessite des mises à jour régulières.

III.2. L'IMPACT POUR LE SMARTPHONE INFECTE

Dès qu'un smartphone est infecté, toutes les informations qu'il contient deviennent en théorie disponibles : photos, sms, messages cryptés désormais lisibles, position GPS, aperçu des sites web visités, accès caméras, etc.

En théorie car, dans la pratique, aucune infection n'est complète : cela dépend en grande partie du modèle du téléphone, de la version du système d'exploitation, du type de puce, etc.

---

[39] De la même façon, les géants de l'informatique (tels que Google, Apple, Microsoft, Facebook, par exemple) proposent en permanence des campagnes '*bug bounty*', pour être informés des vulnérabilités critiques qui leur étaient jusqu'alors inconnues. Il faut cependant savoir que ce type de vulnérabilités, surtout si elle est bien documentée, peut être vendu sur le darknet pour des montants supérieurs.

Ceci explique pourquoi certains smartphones peuvent être facilement piratés, tandis que d'autres demanderont plus d'efforts (par ex. pas de *'zero-click'*, mais une infection physique ou par phishing), ou ne seront pas piratables.

Une fois que l'infection initiale a eu lieu, le logiciel PEGASUS va corrompre des processus essentiels du téléphone en les remplaçant par des versions fournissant les mêmes services mais augmentées de capacités de *spyware*. Le logiciel va également mettre en place des techniques permettant de se dissimuler, et donc de rester invisible pour les anti-virus ou des méthodes d'analyse et de contrôle d'intégrité du téléphone.

Dans les limites des capacités d'infection liées au modèle de smartphone, le service utilisant PEGASUS pourra non seulement voir le contenu du téléphone, y compris les messageries cryptées, mais également activer des fonctionnalités, exfiltrer ou altérer des données.

Ces données peuvent être envoyées de différentes manières à partir du téléphone piraté (par ex. 4G, 3G, etc.), mais une préférence est toujours donnée au wifi si celui est activé, ceci afin que l'utilisateur ne remarque pas que son téléphone commence à fonctionner au ralenti. L'envoi des données du téléphone infecté se fait via des communications cryptées dans le but d'empêcher de remonter vers la source à l'origine de l'infection.

III.3. LES ASPECTS D'INFRASTRUCTURE

Si une partie de l'infrastructure de PEGASUS doit être installée chez le client (par ex. via les serveurs), le logiciel espion nécessite, en outre, une infrastructure de transit partagée qui peut être utilisée par tous les clients de NSO Group.

Concernant les pages web consultées sur l'appareil infecté, une tendance a été observée : la redirection du trafic vers des relais proxy à quatre niveaux DNS (*domain name service*, traduisant une URL en une adresse IP). Par exemple :

- La victime lance son navigateur pour aller sur Facebook ;

- PEGASUS intercepte la demande et la redirige sans que l'utilisateur ne puisse s'en apercevoir vers Fakbouk5.pegas1.pegas2.com ;

- La demande est ensuite redirigée à plusieurs reprises pour finalement arriver sur le site officiel de Facebook, où les informations sont récupérées puis transmises en repassant par cette chaîne de redirection, tout en fournissant une copie au client qui utilise PEGASUS ;

- pour finalement être redirigées de manière transparente vers le navigateur de la victime.

Le client peut soit installer lui-même cette infrastructure, soit utiliser l'infrastructure partagée mise à disposition par NSO Group. Cette dernière est composée de plusieurs centaines de serveurs (*'Pegasus Anonymizing Transmission Network'*). Grâce à ce mécanisme de redirection multiple, il est impossible pour la victime – même après avoir analysé son trafic réseaux en

utilisant des équipement externes (par ex. Wireshark, tcpdump, etc.) – de deviner l'origine de l'attaque, voire même de détecter l'interception.

III.4. LES METHODES DE DETECTION

Détecter si un smartphone a été infecté par un logiciel malveillant de type PEGASUS est particulièrement difficile, étant donné que celui-ci met directement en place des procédures afin de se rendre indétectable pour les anti-virus et de s'intégrer profondément dans le téléphone.

Il peut cependant y avoir des indices d'une éventuelle infection. Dans certains cas, seules de solides compétences techniques permettent de la découvrir, dans d'autres cas, cela relève davantage du ressenti de l'utilisateur du smartphone. Quelques exemples :

- Récupérer son smartphone après l'avoir laissé dans un casier et remarquer que le niveau de charge de la batterie a augmenté ou, au contraire, a fortement diminué (infection via câble USB) ;
- Avoir reçu un sms ou un e-mail contenant un lien sur lequel on a cliqué alors qu'on ne s'attendait pas à recevoir ce message ;
- Voir la connectivité du smartphone changer sans effectuer la moindre action (par ex. le wifi s'active seul, ou la 4G) ;
- Remarquer une grande vitesse de transmission de données alors que le téléphone est peu utilisé (NB : via les paramètres du smartphone, il est possible de voir à tout moment, dans la barre d'état, la vitesse de *transfert data* qui est utilisée);
- Confier son smartphone à un expert afin de le connecter à un PC en mode 'debug', permettant ainsi à celui-ci de comparer les '*hashes*' ('*hash*' = signature numérique unique) des fichiers et processus à ceux d'origine du vendeur, pour autant que les fichiers d'origine du vendeur soient disponibles ;
- N'activer que le wifi et le connecter à une borne d'analyse captant tous les paquets réseaux, ceci afin de déterminer si le trafic est normal : pas de flux de données cryptées inconnu, etc.[40]

III.5. LES METHODES DE PREVENTION

Comme mentionné précédemment, il n'existe pas de méthode de prévention en tant que telle pour éviter une infection de type *'zero-click'*. Tout dépend en réalité de l'existence de bugs et

[40] Ces deux dernières techniques sont assez poussées et requièrent la mise à disposition du smartphone pendant au moins 24 heures.

de vulnérabilités *'zero-day'* liés à l'appareil cible et qui seraient connus par l'équipe de développement du logiciel malveillant et intégrés à celui-ci.

Les efforts des développeurs de *malwares* se concentrent quasi exclusivement l'exploitation des modèles de smartphones les plus vendus ou sur les systèmes d'exploitation les plus répandus (par ex. iOS 13/14/..., Android 9/10/11, etc.). Cela s'explique par le retour sur investissement attendu.

On peut dès lors en conclure qu'il est plus difficile (mais pas impossible) de s'attaquer à des smartphones peu répandus sur le marché, comme ceux tournant sous Linux (par ex. PinePhone, Librem, Fairphone, etc.).[41] L'avantage ici réside dans le fait que le système d'exploitation du smartphone est *'open source'*, et donc qu'il peut être aisément audité par un technicien qui peut avoir accès au code source.

À ceux-ci s'ajoutent des téléphones qui ont été développés autour des enjeux de sécurité, vérifiant par exemple l'intégrité de celui-ci à chaque redémarrage (par ex. les smartphones de la firme israélienne SirinLabs coûtant 1.000 et 16.000 euros). Outre leur prix, reste encore ici la question de la confiance accordée à la firme privée assemblant ce type de téléphone.

IV. PEGASUS ET LES SERVICES DE RENSEIGNEMENT BELGES

Afin de couvrir les deux volets dans la présente enquête, cinq questions seront discutées dans cette section. Il s'agira, dans un premier temps, de vérifier si le cadre légal en Belgique permet aux services de renseignement d'utiliser un logiciel de type PEGASUS (IV.1). Ensuite sera discuté de l'usage effectif ou non du logiciel PEGASUS (ou apparenté) par les services de renseignement belges (IV.2). La question de savoir si les services de renseignement belges sont compétents pour détecter l'utilisation par des puissances étrangères de ce type de logiciel contre des belges ainsi que la question de savoir s'ils en ont les capacités seront abordées dans un troisième temps (IV.3). Il sera ensuite question de la capacité de la VSSE et du SGRS à suivre les évolutions relatives à cette technologie (IV.4). Et, enfin, la position d'information de la VSSE et du SGRS relative aux cibles belges potentielles sera discutée (IV.5).

IV.1 LE CADRE LEGAL EN BELGIQUE PERMET-IL AUX SERVICES DE RENSEIGNEMENT BELGES D'UTILISER UN LOGICIEL DE TYPE PEGASUS ?

Le législateur belge a érigé en principe général l'interdiction des écoutes, des prises de connaissance et des enregistrements des communications et des communications électroniques privées pendant leur transmission et à l'aide d'un appareil quelconque. Ces

[41] Leur prix est légèrement supérieur aux smartphones classiques et les fonctionnalités sont limitées : seuls des logiciels libres sont accessibles, sans accès à Play Store/App Store, etc.

interdictions, qui concernent des atteintes graves à la vie privée, sont érigées en infractions sanctionnées par des peines correctionnelles d'amende et d'emprisonnement en vertu des articles 259*bis* et 314*bis* du Code pénal.

Toutefois, le législateur belge a été amené à encadrer le recours à titre exceptionnel à une atteinte à la protection des communications électroniques privées face à certaines menaces. Le législateur a en effet cherché à concilier des intérêts *a priori* contraires, soit, d'une part, le respect de la vie privée des personnes et, d'autre part, la nécessité d'une protection plus efficace de la société contre des menaces telles que le terrorisme ou encore la criminalité grave et organisée.

En effet, il s'imposait au regard des articles 12 et 22 de la Constitution ainsi que de l'article 8 de la Convention européenne des droits de l'homme, de déterminer de manière claire et précise les pouvoirs qui pouvaient être mis en œuvre par les services de renseignement lorsqu'ils s'immiscent dans l'exercice des droits et libertés individuels.

L'objectif recherché était de permettre, sans certaines conditions et dans le cadre d'un strict contrôle juridictionnel, d'intercepter, de prendre connaissance, d'explorer et d'enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou d'étendre la recherche dans un système informatique ou une partie de celui-ci.

Ces règles se retrouvaient « en miroir » dans le cadre judiciaire comme dans le cadre administratif. Dans le premier cas, ces règles seront régies par le Code d'instruction criminelle ; dans le second, c'est la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) qui a été adaptée en ce sens.

La L.R&S envisage ainsi l'ensemble des méthodes qui peuvent être mises en œuvre par les services de renseignement, moyennant, pour les méthodes les plus intrusives, un contrôle juridictionnel *a priori* et *a posteriori*. Toute technique particulière qui ne serait pas expressément autorisée par la loi serait, par voie de conséquence, interdite. En effet, l'article 18/3 L.R&S prévoit un double contrôle dans la mise en œuvre de ces méthodes de recueil de données (MRD) au niveau de la légalité, de la subsidiarité et de la proportionnalité : un contrôle *a priori* par la Commission administrative BIM et un contrôle *a posteriori* par le Comité permanent R. En outre, tout citoyen peut introduire une plainte auprès du Comité permanent R s'il estime avoir fait l'objet d'une MRD de manière illégale.

Plus précisément, l'article 18/16 de ladite loi autorise l'intrusion dans un système informatique et la collecte de données. Les interceptions, prises de connaissance et enregistrement des communications sont, quant à elles, encadrées par l'article 18/17 L.R&S. Il s'agit de méthodes dites « exceptionnelles » dont la mise en œuvre nécessite

impérativement une décision motivée du dirigeant de service concerné et ce, sous peine de nullité.[42]

Il nous faut relever que si la législation sur les services de renseignement encadre le principe de telles méthodes intrusives, elle ne traite nullement des 'techniques' de mise en œuvre. Ces questions dites techniques – entre autres, avec quels matériels et logiciels les méthodes sont mises en œuvre - sont laissées à l'appréciation des services, tenant compte des évolutions permanentes et exponentielles des technologies.

De ce qui précède, il y a lieu de conclure que le cadre légal actuel autorise les services de renseignement belges à faire usage de ce type de logiciel dans le cadre de la mise en œuvre de MRD moyennant le strict respect des principes de légalité, proportionnalité et subsidiarité. Un contrôle juridictionnel strict est exercé afin que l'utilisation de chaque MRD réponde aux exigences de légalité, de proportionnalité et de subsidiarité.

Par ailleurs, dans l'état actuel du droit, rien n'empêcherait le SGRS d'utiliser un logiciel de type PEGASUS dans le cadre de l'exercice de ses compétences prévues à l'article 44 L.R&S. Cet article prévoit la possibilité pour le SGRS de capter des communications émises ou reçues à l'étranger, de les intercepter, les écouter et les enregistrer. Un contrôle est également exercé sur le recours à ce type de procédés mais il diffère du contrôle pour les MRD. En effet, ici seul le Comité permanent R intervient et exerce un contrôle préalable, un contrôle concomitant et un contrôle *a posteriori* conformément à l'article 44/3 L.R&S.

Le Comité souhaite néanmoins attirer l'attention sur le fait qu'à l'heure actuelle, le contrôle juridictionnel exercé ne porte pas sur les aspects techniques de mise en œuvre des méthodes de recueil de données (notamment la question de savoir si un logiciel de type PEGASUS est utilisé pour mettre en œuvre la MRD autorisée) ou de l'article 44 L.R&S. Le Comité ne dispose, à l'heure actuelle, ni des ressources humaines suffisantes ni des compétences techniques requises pour exercer un tel contrôle. Ce manque de moyens peut avoir une influence sur l'appréciation du caractère subsidiaire et proportionnel de la MRD ou procédé visé à l'article 44 L.R&S.

IV.2. LES SERVICES DE RENSEIGNEMENT BELGES UTILISENT-ILS LA *REMOTE INFECTION TECHNOLOGY* DANS LE CADRE DE LEURS MISSIONS LEGALES ?

L'article 18/16 de la L.R&S prévoit que les services de renseignement peuvent accéder à un système informatique à l'aide ou non de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités. Il s'agit d'une méthode exceptionnelle dont le contrôle renforcé de légalité, de subsidiarité et de proportionnalité de l'usage est imposé par la Loi.

[42] Article 18/10 § 2 L.R&S.

IV.2.1. La VSSE

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

IV.2.2. Le SGRS

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Quant à la nécessité pour les services de renseignement belges de disposer de ce type d'outils, le Comité permanent R est d'avis qu'il est important que ces services puissent recourir, dans le strict respect du cadre légal, à ce type de technologie (autrement dit, en disposer) afin d'accomplir leurs missions. Le renforcement des capacités des services doit être en conséquence.

Face à l'évolution rapide et complexe des menaces dans un environnement digital lui-même en expansion, l'utilisation des technologies digitales les plus à la pointe apparaît essentielle pour assurer le meilleur niveau d'efficacité des missions des services de renseignement et de sécurité belges. En effet, sans nier toute l'importance que conservent des méthodes et techniques plus classiques de renseignement comme la collecte et l'analyse d'origine humaine ou « HUMINT » (*Human Intelligence*), il est incontestable que le recours à des outils technologiques de renseignement et de sécurité comme les *Remote Infection Technologies* est de nature à renforcer significativement la position d'information des services. En outre, force est de constater que la baisse de l'effectivité des mesures d'interception plus classiques des communications est démontrée par la complexification de la collecte et du traitement des informations. Cette situation contrarie de plus en plus, voire empêche, le cycle de renseignement et ses objectifs d'anticiper les risques de sécurité et de permettre un conseil adéquat aux autorités sur la manière de traiter les menaces, voire de les entraver directement.

Le Comité permanent R insiste toutefois sur le fait que ces technologies devraient idéalement être développées en Belgique. À défaut, les technologies utilisées devraient être celles développées par des partenaires étrangers stratégiques avec lesquels un accord de sécurité a

été signé et être acquises après une analyse de risques, formalisée, approfondie et standardisée.

Par ailleurs, le Comité estime que le contrôle qui devra être exercé en cas d'usage de ce type de logiciel devra être 'plus approfondi' en raison de la gravité de l'intrusion dans la vie privée.

IV.3. L'UTILISATION DE PEGASUS (OU DE LOGICIELS SIMILAIRES) PAR DES SERVICES ETRANGERS : LA VSSE ET LE SGRS SONT-ILS COMPETENTS ?

Le point IV.1. a permis de constater que le cadre légal belge protège les citoyens d'un usage abusif d'un logiciel de type PEGASUS par les services de renseignement belges.

Bien entendu, d'autres acteurs (personnes, sociétés, États tiers amis ou non, organisations criminelles, etc.) sont à même de développer, de se procurer et d'utiliser sur le territoire belge des techniques matérielles et logicielles pour procéder à des écoutes ou des intrusions dans des systèmes informatiques. Ces actes sont punissables en vertu de l'article 314*bis* du Code pénal belge.

Mais encore faut-il réussir à détecter l'usage de ce type de procédés. Les révélations médiatiques ont montré qu'il existe un risque de menace pour les droits et la vie privée du citoyen belge par un éventuel espionnage par des services de renseignement *étrangers* via des technologies de type PEGASUS. Il s'agit dès lors d'évaluer la capacité de la VSSE et du SGRS à détecter et à gérer ce type de menace.

En vertu des articles 7 et 8 L.R&S, la VSSE a en effet pour mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité pouvant menacer la sûreté intérieure et extérieure de l'État ainsi que le potentiel scientifique ou économique de la Belgique, dont l'espionnage.

En outre, l'article 7, 3°/1 donne à la VSSE pour mission spécifique de *« rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge ».* L'article 11 § 1er, 5° prévoit la même mission pour le SGRS.

Le SGRS est quant à lui chargé *« de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer : (…) e) la sécurité des ressortissants belges à l'étranger »* (article 11 § 1er, 1°).

Afin de pouvoir évaluer la menace précise émanant de l'utilisation de certains moyens technologiques par des services de renseignement étrangers pour la Belgique et ses citoyens, il importe dès lors que les services belges suivent autant que possible l'évolution de ce genre de technologies et leur utilisation par ces services étrangers.

Nos services de renseignement en sont conscients. Ainsi, la VSSE écrit dans l'analyse contextuelle de son 'Plan stratégique 2021-2024' que « *(l)es évolutions technologiques se succéderont à un rythme de plus en plus rapide dans les années à venir et auront une influence sur les menaces. Notre service est censé identifier et aider à développer la résilience contre eux. L'utilisation croissante du cryptage avancé (portable) et l'introduction de la 5G nous présenteront de nouveaux défis. Nous devrons filtrer les informations pertinentes à partir de grandes quantités de données. Il ne faudra pas rater le train pour pouvoir détecter et neutraliser les risques que forment nos cibles. Cependant, l'anticipation des nouveaux développements technologiques nécessite des investissements importants. La recherche de synergies avec d'autres services de sécurité est nécessaire pour partager les connaissances et les coûts ».*[43]

Comme indiqué dans le passage ci-dessus, il est surtout question ici de moyens. Il s'agit souvent de technologies avant-gardistes/de pointe, dans lesquelles certains États et des sociétés privées sont actifs et qui peuvent investir des sommes considérables dans la conception d'instruments et de produits.

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

En 2013[44], le Comité permanent R a déjà effectué une enquête sur l'attention que les services de renseignement belges portaient (ou non) sur les menaces que pouvaient représenter pour le potentiel scientifique et économique de la Belgique des programmes de surveillance électroniques sur les systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou services de renseignement étrangers. Cette enquête avait donné lieu à plusieurs recommandations.

Une de ces recommandations s'énonçait comme suit : « *Le Comité permanent R estime que les deux services de renseignement doivent s'intéresser aux risques inhérents aux nouvelles possibilités offertes par la technologie en matière de captation massive de données et d'espionnage économique et politique, et ce même si ces risques émanent de « pays amis ». À cet égard, il conviendrait de procéder à des analyses de risques prenant également en considération la présence d'institutions internationales sur le territoire belge*.
La VSSE et le SGRS doivent prêter attention à ces phénomènes afin de se forger une bonne position d'information. Cela leur permettrait de connaître les possibilités et les méthodes de

---

43 *'Plan stratégique 2021-2024'*, Sûreté de l'État, 2021, p.7.
44 COMITÉ PERMANENT R, *Rapport d'activités 2014.*

travail d'autres services, non seulement pour pouvoir informer, le cas échéant, les autorités ou prendre des contre-mesures, mais aussi pour évaluer leurs propres techniques de recueil.
La VSSE doit évidemment s'intéresser à la captation massive de données, puisque ce phénomène constitue une réelle menace pour au moins deux intérêts qu'elle est légalement tenue de protéger, à savoir les droits et libertés fondamentaux et la souveraineté de l'État. Elle peut, par exemple, retrouver de nombreuses informations dans les sources ouvertes ou en demander au service de renseignement militaire. À la lumière de ces éléments, elle peut déjà se faire une idée globale du phénomène et des risques y afférents, et en faire écho dans une analyse de phénomène[45], envoyée à intervalles réguliers aux autorités concernées. Les citoyens et les entreprises devraient eux aussi être davantage sensibilisés à la problématique. ».

En 2020[46], le Parlement a chargé le Comité permanent R d'actualiser cette enquête datant de 2013. Dans le cadre de cette d'enquête d'actualisation, le Comité permanent R a demandé, entre autres, aux deux services de renseignement dans quelle mesure la recommandation reprise ci-dessus avait été mise en œuvre.

Cette partie fait l'objet d'une classification de degré « CONFIDENTIEL » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

IV.4. SUIVI DES EVOLUTIONS EN MATIERE DE *REMOTE INFECTION TECHNOLOGY* PAR LES SERVICES DE RENSEIGNEMENT BELGES

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

---

[45] Le Comité permanent R a déjà mis l'accent sur les atouts de ce que la VSSE appelle une « analyse du phénomène » : *« L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une « évaluation du risque » à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique »*, comme l'explique la VSSE dans sa première analyse de phénomène. De telles analyses se prêtent particulièrement bien à la problématique de l'interception de données, notamment parce qu'elles sont destinées à être largement diffusées.

[46] COMITÉ PERMANENT R, *« Suivi de l'enquête de contrôle « PRISM » et les implications pour les services de renseignements belges des réseaux de surveillance étrangers »*.

IV.4.1. La VSSE

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Dans le passé, la VSSE s'était déjà efforcée de sensibiliser les mandataires politiques, les autorités et le secteur privé sur les risques que représente l'espionnage technologique, entre autres la technologie *remote infection*, en donnant notamment des briefings de conscientisation. Le service a également déjà publié une série de brochures autour de cette problématique, telles que *« Surfer en toute sécurité pendant la campagne électorale », « L'espionnage : êtes-vous concerné ? »* (2019), et *"Travel security"* (2019).[47]

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

IV.4.2. Le SGRS

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

IV.5. ENQUETE DES SERVICES DE RENSEIGNEMENT BELGES SUR D'EVENTUELLES CIBLES BELGES DE L'UTILISATION DE PEGASUS (PAR DES SERVICES DE RENSEIGNEMENT ETRANGERS).

IV.5.1. La VSSE

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

[47] https ://vsse.be/fr/publications.

IV.5.2. Le SGRS

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

En termes de contre-mesures, le SGRS a procédé à la sensibilisation du personnel de la Défense sur l'importance de conserver une « cyberhygiène ».

Cette partie fait l'objet d'une classification de degré « CONFIDENTIEL » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

IV.5.3. Constats

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteur des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

La mission légale de la Sûreté de l'État définie par l'article 7 L.R&S est (…) « *de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État* (…). La loi précise encore dans son article 8 ce qu'il faut entendre par « *activité qui menace ou pourrait menacer* », soit « *toute activité, individuelle ou collective, déployée, à l'intérieur du pays ou à partir de l'étranger* (…).

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Le Comité permanent R constate que lors de l'identification d'éventuelles cibles belges de services étrangers en lien avec l'utilisation de PEGASUS, le SGRS s'est uniquement concentré sur l'éventuelle implication des services de renseignement rwandais, et la VSSE sur les services de renseignement rwandais et marocains.

Des informations peuvent également être retrouvées dans les sources ouvertes selon lesquelles un lien a également été établi entre les services de renseignement saoudiens et émiratis et l'utilisation de PEGASUS ainsi que l'espionnage d'activistes des droits humains et

de journalistes occidentaux (notamment américains et britanniques). Mais il est vrai que jusqu'à présent, aucun nom de cible belge n'a été cité à cet égard.

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

V. CONCLUSIONS ET RECOMMANDATIONS

À la clôture de cette enquête, les conclusions et recommandations suivantes sont formulées :

V.1. CONCLUSIONS

I. Quant à l'utilisation du logiciel PEGASUS ou d'un logiciel similaire

En ce qui concerne l'utilisation de ce logiciel en Belgique, il existe une interdiction assortie d'une sanction pénale.

Sur le plan légal et réglementaire, les services de renseignement, comme les services de police, peuvent utiliser des outils similaires à PEGASUS moyennant le respect de strictes conditions, et dont l'usage doit être contrôlé de bout en bout.

Pour les services de renseignement, cela ne peut se faire que dans le cadre d'une MRD, qui requiert une décision formalisée du dirigeant du service concerné, un avis conforme de la Commission BIM et un contrôle *a posteriori* par le Comité permanent R. Ce contrôle est un contrôle juridictionnel dans le cadre duquel le respect des principes de légalité, subsidiarité et de proportionnalité sont/doivent pouvoir être vérifiés, à tout moment.

Pour le SGRS, le cadre légal permet en sus d'en faire usage dans le cadre des compétences décrites à l'article 44 L.R&S. Le contrôle exercé diffère de celui pour les MRD puisque seul le Comité intervient et exerce un contrôle préalable, concomitant et *a posteriori*.

Les compétences de contrôle susmentionnés du Comité sont renforcées par une compétence générale en tant qu'Autorité de protection de données octroyée au Comité permanent R par la L. Contrôle et la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Le Comité a examiné la question de savoir si les services de renseignement ont utilisé/utilisent PEGASUS ou des outils similaires. Afin d'assurer tant les missions des services que celle du Comité permanent R, la nécessité effective de classification des réponses a fait l'objet d'une concertation.

À l'issue de son enquête le Comité permanent R peut communiquer qu'il estime que les services de renseignement devraient être dotés de la capacité d'acquérir et d'utiliser la technologie la plus avancée.

En ce qui concerne l'acquisition de technologie la plus avancée, le Comité plaide en faveur de l'élaboration d'une stratégie nationale qui permette le développement de ce type de produits en Belgique. Avec comme objectif que les différents partenaires du monde de la sécurité et

de la Défense belge, seul ou ensemble, détiennent une indépendance technologique sur la matière.

Dans la perspective de l'acquisition de ce type de produits, les services doivent procéder à une analyse de risques préalable, particulièrement rigoureuse.
Dans cette hypothèse, le Comité permanent R encourage les services de renseignement (VSSE/SGRS) à uniformiser et standardiser cette analyse de risques en tenant très étroitement compte du contrôle du Gouvernement fédéral relatif à la légalité, la régularité, la faisabilité budgétaire et l'opportunité des dépenses publiques sous l'angle de l'efficacité, de l'efficience et de l'économie.

Cette stratégie devra se réaliser en tenant compte des développements européens, notamment ceux consécutifs aux conclusions du Contrôleur européen de la protection des données sur la nécessité d'interdire l'utilisation de ce type d'outils, ou à tout le moins de renforcer le contrôle des méthodes de surveillance les concernant.

II. Quant à la détection de l'utilisation de ce type de logiciels par des services étrangers

Cette mission incombe à la VSSE et au SGRS conformément au cadre légal.

Cette partie fait l'objet d'une classification de degré « SECRET » par l'autorité d'origine auteure des pièces étant donné qu'une utilisation inappropriée des éléments qu'elle contient est susceptible de porter gravement atteinte à un des intérêts visés par l'article 3 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Le Comité permanent R a constaté que les services de renseignement ont pris certaines initiatives, tant sur le volet détection que sur le volet prévention, pour limiter les infections des téléphones.

Le Comité invite les services à suivre étroitement cette problématique.

III. Quant à l'attention qui doit être portée par la VSSE et le SGRS aux nouvelles possibilités technologiques

Le Comité permanent R estime que les deux services de renseignement et de sécurité doivent être plus attentifs aux menaces que les nouvelles possibilités technologiques peuvent représenter en termes de captation de données et d'espionnage économique et politique, même si ces risques émanent de pays avec lesquels ils entretiennent des relations

stratégiques. À cet égard, des analyses de risques devraient être effectuées régulièrement en portant une attention renforcée aux impacts de la présence de nombreuses institutions internationales sur le territoire belge.

IV. Synergies entre la VSSE et le SGRS

Dans un souci de plus grande coordination et d'efficacité, (cf. article 1er 2° L.R&S), les deux services de renseignement et de sécurité belges devraient mutualiser leurs capacités techniques/technologiques.

Comme cela existe pour la police intégrée avec le 'National Technical and Tactical Support Unit', le Comité permanent R est d'avis que ces capacités devraient être intégrées dans un seul service, idéalement désigné par le Roi, définissant des obligations de moyens claires en termes d'objectifs tant en ce qui concerne le respect de la loi que la qualité du service.

V.2. RECOMMANDATIONS

I. Taskforce et Plan national de Sécurité Digitale

Afin d'améliorer sa position d'information à l'égard des menaces digitales, et donc la prévention et la réaction face à ces menaces, le Comité permanent R invite le gouvernement à créer, dans les six mois, une Taskforce nationale intégrale et intégrée sur le modèle d'autres taskforces déjà créées pour des situations de crise. Il s'agira donc d'un organe stratégique et politique spécifique qui élaborera des recommandations afin de prévenir et lutter efficacement contre les menaces digitales. Cette Taskforce sera également chargée d'établir un Plan National de Sécurité Digitale sur le modèle des autres plans nationaux développés en matière de sécurité.

II. Analyse de risques

Le Comité recommande aux deux services de renseignement de procéder régulièrement à des analyses de risques en portant une attention particulière aux risques supplémentaires liés à la présence d'institutions internationales sur le territoire belge. Une première analyse de risques devra être finalisée pour la première fois pour le 30 juin 2023 au plus tard.

III. Synergies entre la VSSE et le SGRS

Le Comité permanent R invite les ministres de la Justice et de la Défense à investir dans le développement, en propre, des outils permettant de remplir ces missions au mieux. Le Comité recommande qu'en cas de recours à des partenaires, un contrôle renforcé de légalité et de subsidiarité soit organisé.

Outre les contrôles *a priori* et *a posteriori* légalement prévus, le Comité permanent R invite les autorités à intégrer au sein des deux services, dans un délai de six mois, un système de contrôle de gestion des technologies utilisées afin de permettre d'optimaliser les réactions à incidents comme l'affaire PEGASUS, mais également un contrôle permanent du rapport entre les moyens engagés et les résultats en termes d'efficacité, d'efficience et d'économie.

IV. Adapter la capacité de contrôle du Comité permanent R

Le Comité permanent R recommande de voir ses capacités être adaptées au renforcement des capacités en personnel des services de renseignement et lui permettre ainsi de répondre à l'ensemble de ses missions légales, ce qui n'est plus le cas aujourd'hui.