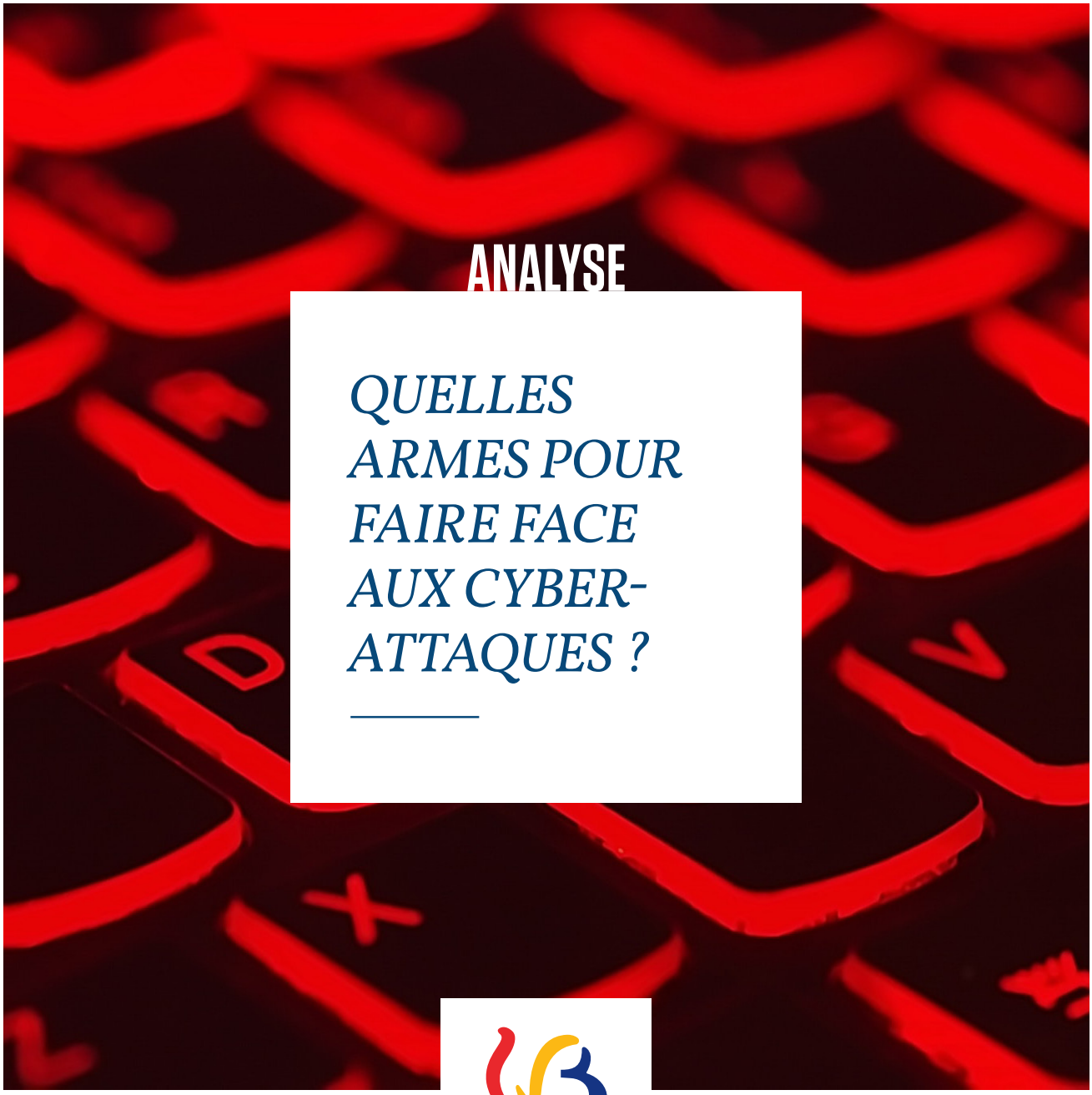
Centre Jean Gol



ANALYSE

QUELLES ARMES POUR FAIRE FACE AUX CYBER-ATTAQUES ?

FÉDÉRATION
WALLONIE-BRUXELLES

Une analyse réalisée par

FRÉDÉRIC FANUËL

Richard Miller, Administrateur délégué du CJG
Corentin de Salle, Directeur du CJG

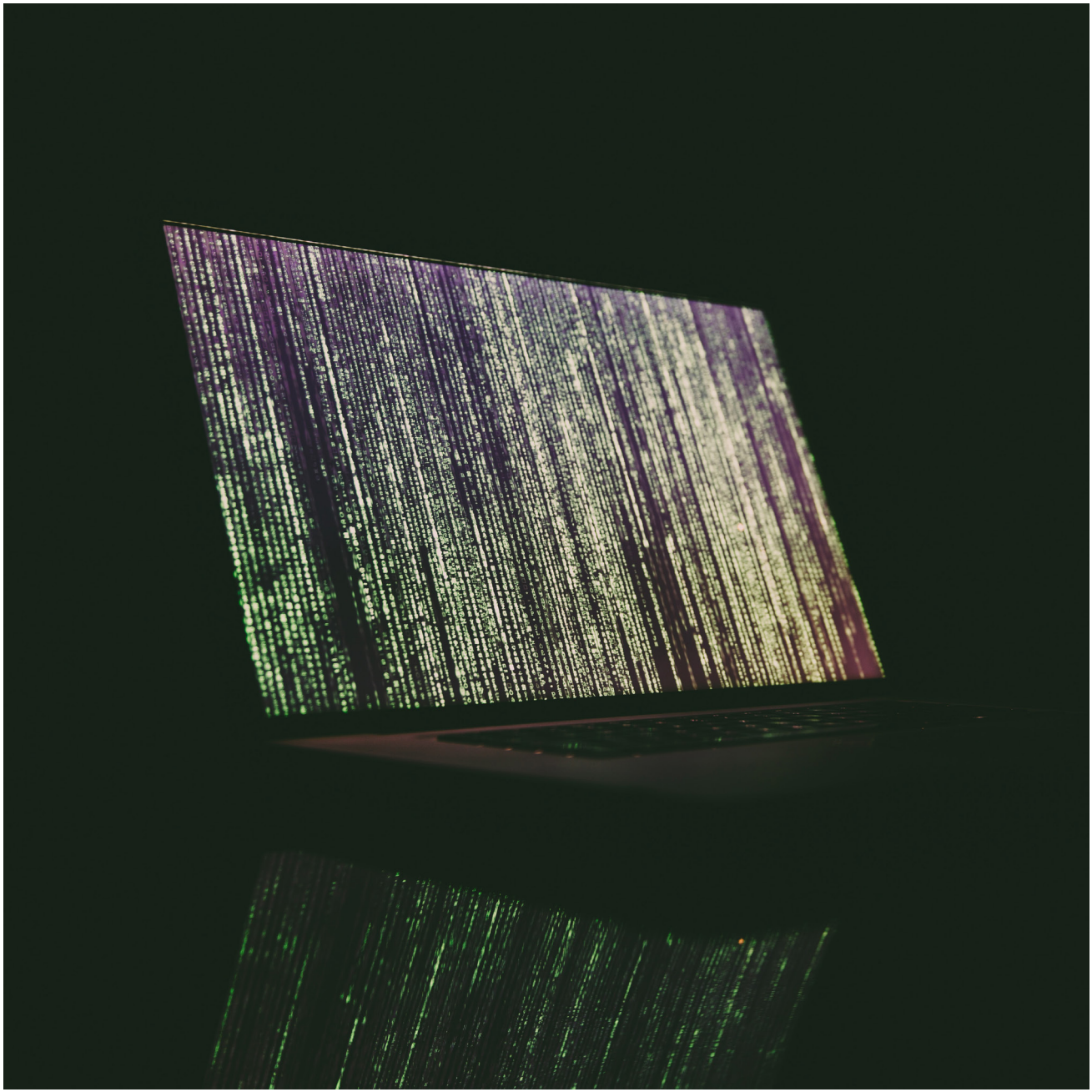
Novembre 2019

Avenue de la Toison d'Or 84-86
1060 Bruxelles
Tél. : 02.500.50.40
cjg@cjg.be

www.cjg.be

QUELLES ARMES POUR FAIRE FACE AUX CYBER-ATTAQUES ?

We don't wanna cry but some would like us to cry



INTRODUCTION

Le mot « cyber » est tiré du mot grec *Kubernêtikê* signifiant « gouvernail ». A l'origine le préfixe « cyber » n'existe pas ! Il provient du mot « cybernétique » qui lui, a une origine étymologique et signifie la science du gouvernement (du grec kubernêtiké, de kubernein, kubernaô : gouverner, diriger, se diriger ou encore kubernan : Le pilote du navire). La cybernétique est, quant à elle, l'étude des mécanismes d'information des systèmes complexes, explorés en vue d'être standardisés lors des conférences Macy et décrits (en 1947) par Norbert Wiener dans ce but.

La cybernétique fait ensuite l'objet dans les années 50 d'une « récupération » intellectuelle d'ordre technique et de développements nouveaux par des mathématiciens, des scientifiques et des informaticiens. En effet, cette notion est reprise pour étudier et expliquer les aspects relatifs à la communication, aux interactions et aux échanges d'informations dans au sein de systèmes, au sein de l'univers. On pourrait dire que la cybernétique est à l'origine de l'automatisation de l'information. Cependant, le terme cybernétique étant très large (il s'applique, par exemple aux termes suivants : cyberespace, cybersécurité, cyberdéfense, cyberattaque, cybercrime, cybercafé, cyberculture, cyberdémocratie, cybermarché, cyber-réputation, etc.) et visiblement compliqué, le terme « informatique » est apparu pour désigner une science et un thème plus spécifique qui à son tour évolue toujours plus rapidement que son ombre.

Aujourd'hui on emploie couramment, souvent à mauvais escient, les thermes « cybersécurité », « cybercriminalité », « cybercrime » pour désigner l'insécurité sur Internet causée par des actions malveillantes au détriment de personnes et/ou d'autres systèmes informatiques, néfastes au bon fonctionnement de la société économique et industrielle, à l'exercice de la justice et ne participant pas de l'exercice de la démocratie. Cependant, ces notions ne signifient pas la même chose.

En effet, tandis que la *cybersécurité* vise les mesures de politique de sécurité, par exemple d'un gouvernement ou d'une entreprise, en matière d'automatisation de l'information à développer et à mettre en œuvre par l'intermédiaire de mesures stratégiques et opérationnelles, la *cybercriminalité*, quant à elle, vise l'ensemble des actes répréhensibles et illégaux.

Cette différenciation est primordiale. Par cybersécurité, nous désignons *le cadre de référence* en termes de politique de sécurité à développer pour le monde « cyber » établie par des gouvernements, par des responsables « sécurité IT » d'entreprise, des écoles, des hôpitaux, etc. Par cybercriminalité, nous visons *les actes de délinquances* produit sur les réseaux d'informations et leurs infrastructures combattus par des policiers dans le cadre d'actions policières.

D'un côté, *la sécurité informatique*. De l'autre, *les menaces* relatives à la cybersécurité.

La sécurité informatique désigne l'ensemble des techniques et des moyens organisationnels, juridiques et humains, mis en œuvre pour conserver ou rétablir, la disponibilité, la confidentialité et l'intégrité d'un système informatique. Les systèmes informatiques peuvent, en effet, faire l'objet de différents types de menaces, résultant d'un acte de malveillance ou de circonstances accidentelles. Les menaces, quand elles sont susceptibles de porter atteinte à l'intégrité, à la confidentialité ou à la disponibilité de l'information, peuvent être qualifiées de « hacking ». La criminalité informatique, ce sont les menaces appliquées à la sécurité informatique ; elle recouvre notamment les infractions informatiques, telles que le faux et la fraude informatiques, les infractions se rapportant au contenu et les infractions liées à la propriété intellectuelle[1]. Une autre question qui ne sera pas étudiée ici est de savoir si toutes les menaces cybers sont érigées en infraction.

1 Site web du SPF Economie

NAISSANCE ET ÉVOLUTION D'UN PHÉNOMÈNE

QUEL PHÉNOMÈNE ?

Les risques et les menaces liés à l'automatisation de l'information ne naissent que lorsqu'on en prend conscience et connaissance. Cette prise de conscience s'est constituée petit à petit. La notion de sécurité de la cybernétique et ensuite de l'informatique s'est développée au fur et à mesure de l'identification de risques et des menaces et de la prise de conscience de l'importance de ces risques et menaces dans la société du XX^{ème} siècle et du XXI^{ème} siècle.

Le passage dit de « l'an 2000 » a constitué un tournant dans la prise de conscience des risques et menaces pour les informaticiens, les développeurs et les analystes.

> *« La cybersécurité porte aussi bien sur la protection et l'attaque d'équipements informatiques (la guerre pour ou contre l'information), afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur la Toile (la guerre par l'information), avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique et autres campagnes de dénigrement. » (Nicolas Arpagian)* [2]

UN PHÉNOMÈNE EN AUGMENTATION ? CYBERATTACK : NO SCIENCE-FICTION, BUT REALITY IN BELGIUM[3]

Le SPF Economie précise[4]que la Federal Computer Crime Unit a estimé le préjudice financier causé par la criminalité informatique entre 1 à 3 milliards d'euros par an pour la Belgique. Les conséquences du phénomène sont énormes d'un point de vue économique.

Inovatech.be mentionne sur son site que *dans notre pays, le coût de la cybercriminalité était estimé à 3,5 milliards d'euros, soit plus de 1% du produit intérieur brut, au premier semestre 2014*[5]*. Durant cette période, l'équipe fédérale d'intervention d'urgence en sécurité informatique (CERT.be) a reçu plus de 751.000 notifications d'ordinateurs infectés en Belgique.* Le site web précise que le CERT.be *a également reçu, au cours du même semestre, en moyenne 614 avis d'incidents cybernétiques par mois, soit 80% de plus qu'en 2013.*

Fort heureusement, en 2015, le gouvernement fédéral a mis en place le Centre belge pour la Cybersécurité (le CCB) qui a repris la gestion du CERT.be. Ensemble, le CCB et le CERT.be ont pu, avec leurs partenaires, développer de multiples initiatives et actions concrètes et projets favorisant la prévention du phénomène par une approche adéquate[6][7].

---

2 N. Arpagian, ***La Cybersécurité****, Que-Sais-je, PUF, 16/5/2018*
3 https://intersentia.be/nl/cyberattack-noscience-fiction-but-reality-in-belgium
4 https://economie.fgov.be/fr/publications/barometre-de-la-societe-de
5 http://www.innovatech.be/la-cybersecurite-un-secteur-tendance-dans-lequel-investir/
6 https://www.safeonweb.be/fr/home
7 https://www.ccb.belgium.be/fr

Le CERT.be indique en 2016[8] que 30 incidents lui sont rapportés quotidiennement.

Sur son site web, EUROPOL rappelle que les cybercriminels se font aussi plus agressifs. Pour cette raison, EUROPOL a considéré la lutte contre la **cybercriminalité** comme une priorité pour sa politique 2018-2021. En effet, la cybercriminalité est un problème croissant dans les États membres de l'Union européenne. La cybercriminalité concerne le plus souvent des actes criminels nécessitant une haute technologie (« high tech crime »), c'est-à-dire mobilisant la technologie électronique et numérique de pointe pour attaquer les ordinateurs ou les réseaux informatiques au moyen notamment des malwares ou logiciels malveillants. Le malware (ou «maliciel») est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, botnet, infecteur de fichiers, ransomware, scareware ainsi que d'autres menaces. Le «spyware» désigne un programme installé sur un ordinateur à l'insu de son propriétaire pour surveiller leurs activités et transmettre les informations à un tiers. Rootkit, ver, etc. en sont les modes opératoires auxquels sont confrontés des milliers d'ordinateurs tous les jours. D'autres attaques cyber du type DDOS[9] (*Distributed Denial of Service attack*) ou en français « attaque par déni de service »[10] peuvent être réalisées avec des moyens techniques peu élaborés que tout un chacun peut commander pour moins de 50 € sur le darkweb[11]. Le site web « digitalattackmap.com » donne un aperçu « à la minute » des attaques DDOS dans le monde.

Le rapport 2019 de la cybercriminalité d'Europol[12] donne un aperçu des menaces émergentes et développements clés : le « *cybercrime continue de mûrir et se montre de plus en plus audacieux, déplaçant son centre à des cibles plus grandes et plus rentables ainsi que de nouvelles technologies* ».

La multiplication des actions et des acteurs en cybersécurité dans différents domaine (acteurs de la sécurité, sociétés fournissant des services proposant des formations, des solutions du type CERT en cas d'infections et d'attaques, niveaux et nombre d'instances se préoccupant et prenant en charge la cybercriminalité et en corolaire « sa » cybersécurité tels que l'Union européenne, l'OTAN, et chaque Etat-membre de l'union) indique que le phénomène étudié est en plein essor. C'est une entreprise qui ne connait pas la crise.

Le phénomène est aujourd'hui devenu une source importante d'emploi dans le secteur de la cybersécurité, en pleine activité, en particulier et dans le secteur des technologies de l'information et de la communication (TIC) en général comme nous le confirme Clément Grégoire dans son article « La cybersécurité dans les entreprises : un marché en pleine croissance »[13]. Des entreprises spécialisées en la matière se développent et cherchent des talents de tout niveau en sécurité informatique. Certaines sociétés proposent même des plans de formation pour leur personnel. Ces dernières fournissent des services d'audit et de certification, d'analyse de risque, de consultance, de formation de talents, de *capacity building*, de résilience et de *response team*, la mise en place de *security policing* interne, le développement de logiciels et la protection des réseaux d'information et des ordinateurs.

---

8 https://www.vanbreda.be/en/news/cyber-incidents/?highlight=cyber
9 https://www.digitalattackmap.com/understanding-ddos/
10 https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service
11 https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
12 https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene
13 https://geolink-expansion.com/actualites/la-cybersecurite-un-marche-en-pleine-croissance/

La cybersécurité est devenue un véritable marché. Selon Gartner[14], le marché mondial de la cybersécurité a cru de 3.1 Mds € en 2004 à 67 Mds € en 2015 et devrait atteindre 152 Mds € en 2020. Le marché US représente à lui seul plus de 40 % du marché mondial, l'Europe environ 25 %, c'est-à-dire 17 Mds €, sans inclure la Russie[15]. Le marché est favorisé par l'activité de la **cybercriminalité** en plein essor, par la prise de conscience de la nécessité d'agir, de se prémunir et de réagir rapidement et de manière qualitative dans le cadre d'une société et d'une industrie toujours plus connectées et high tech.

PRISE EN CHARGE DU PHÉNOMÈNE ET DÉVELOPPEMENT D'UN CADRE JURIDIQUE POUR PRÉVENIR ET COMBATTRE LES MENACES CYBER

1. L'Union européenne met aujourd'hui la priorité sur la prévention de la cybercriminalité et sur la sécurisation des systèmes d'information notamment par le biais de la directive NIS[16] transposée depuis peu dans tous les Etats-Membres.

2. En Belgique, la directive a été transposée en loi depuis le 7 avril 2019. Cette loi prévoit : l'identification des services essentiels en Belgique ainsi que leurs opérateurs. Elle loi veille à ce que ces opérateurs prennent des mesures de sécurité suffisantes et signalent tout incident significatif comme une cyberattaque auprès des autorités nationales en charge de la cybersécurité.

3. En cybersécurité, la sécurité des données est bien sûr au centre des discussions. Le « RGPD », à savoir le règlement de protection des données générale, fait partie de l'arsenal juridique de la sécurité cyber. En effet, cette directive européenne donne un cadre de référence clair et sans détour en matière de protection des données personnelles. Cette directive impose des obligations en termes de confidentialité, d'intégrité et de disponibilité dans le chef de détenteurs de données qui impliquent des mesures de protection.

4. La sécurité des réseaux et systèmes d'information est un défi majeur pour les gouvernements, les entreprises et les citoyens. L'enjeu principal réside dans le niveau de confiance à maintenir coûte que coûte dans le cyber au même titre qu'il y a lieu de pouvoir maintenir la confiance des actionnaires d'une entreprise ou des adeptes de la bourse. Si la confiance s'effondre, c'est tout un monde qui s'écroule. La confiance est une combinaison de trois facteurs : l'efficacité et l'efficiente d'une part (l'aspect fonctionnel et opérationnel), l'authenticité et la disponibilité du système d'information cyber, d'autre part.

5. L'analyse de risques est une mesure qui est aujourd'hui très bien développée et maitrisée par les autorités, les organismes d'audit, de certification tant au niveau national qu'au niveau européen. Ces autorités et organismes tant privés que publics ont acquis, parfois en réseau, des connaissances et expertises colossales en la matière au profit de la sécurité globale (info risk management, monarc, EWS, etc.). En effet, les autorités nationales et européennes ont par exemple mis en œuvre des CERT (Computer emergency and response team) qui ont développé des compétences tant préventives que réactives. Souvent partagées, elles permettent de lutter efficacement contre le phénomène, réduire les risques et menaces et favoriser la cybersécurité.

---

14 Société de conseil et de recherche dans le domaine des techniques avancées.
15 https://misskonfidentielle.com/2019/01/26/fic-2019-les-chiffres-cles-de-la-cybersecurite/
16 DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.


fn
control
option
command
command
option

6. Les domaines cyber aujourd'hui principalement concernés par l'insécurité des réseaux et le risque d'attaques cyber sont : les télécoms de manière générale, les systèmes IT bancaires, les systèmes IT militaires, les systèmes IT aéronautiques et les systèmes d'information relatifs à des banques de données proprement dites.

DO WE WANT TO CRY ? WE DON'T WANNA CRY

En 2015 et 2016, « Anonymous » défraye la chronique. Justicier de nobles causes, c'est aussi une menace pour les gouvernements en ce compris le gouvernement belge.

Malgré des attaques cyber mondiales importantes ces dernières années, comme celles menées par les virus WannaCry, Petyia et NotPetyia, les Etats s'organisent et développent des capacités de résiliences. Les attaques et les virus portent des noms de la même manière que les météorologues donnent des prénoms aux ouragans et les classifient.

On se souvient du virus WannaCry de mai 2017 qui a touché le monde entier en bloquant et infectant des ordinateurs en y installant un logiciel de rançon (ransomware) malveillant (malware) profitant des failles de sécurité relatives au protocole SMB (Server Message Block) permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows. Le virus WannaCry a été utilisé lors d'une cyberattaque mondiale massive, touchant plus de 300 000 ordinateurs, dans plus de 150 pays. Cette cyberattaque est considérée comme le plus grand piratage à rançon de l'histoire d'Internet, l'office européen des polices Europol la qualifiant « d'un niveau sans précédent » et ajoutant « qu'il ne faut en aucun cas payer la rançon »[17].

Ces attaques ont également touché la Belgique mais dans des proportions minimes. En effet depuis l'installation du Centre Cybersécurité Belgique (CCB) en 2015 et l'augmentation de la capacité de cyberésilience du CERT.be et des spécialistes cyber du Service Général de Renseignement et de Sécurité (SGRS), bon nombre d'actions préventives ont été mises en place en Belgique en matière de lutte contre des ransomwares.

C'est à la lumière de ces expériences que les Etats doivent construire leurs plans de cybersécurité et développer les actions préventives, correctrices ou réparatrices nécessaires ; ce qu'ils font. Néanmoins, le risque zéro n'existe pas.

En 2018 et 2019, le gouvernement fédéral renforce la sécurité du système d'élections électronique pour les élections communales, régionales et fédérales et une campagne de sensibilisation de la population a été lancée par la Sûreté de l'Etat via une brochure : « Surfer en toute sécurité pendant la campagne électorale »[18]. Le Président du comité R, M. Lipszyc, lors d'une interview pour Sud Info en décembre 2018, publiée le 2/1/219, s'inquiète[19] :

« On verra si, en Belgique, nous avons les outils pour veiller à ce que les élections se déroulent parfaitement bien. En 2019, il faudra que les services de renseignement[20] appréhendent toute possibilité d'ingérence extérieure susceptible de modifier le résultat des élections. À cause des « fake news », il y a un risque de voir un État se fragiliser. Or, nos démocraties sont déjà assez fragilisées. C'est pour cette raison que nos deux services de renseignement et le comité R sont soucieux et conscients de cet enjeu ».

---

17 https://fr.wikipedia.org/wiki/WannaCry
18 https://www.vsse.be/fr/surfer-en-toute-securite-pendant-la-campagne-electorale
19 https://www.sudinfo.be/id93715/article/2019-01-02/des-elections-menacees-par-les-russes-en-mai-2019-verra-si-nous-avons-les-outils.
20 Rapport d'activité de la Sûreté de l'Etat 2017-2018 (p24) https://vsse.be/sites/default/files/1-ra-fr-2018.pdf

En effet, la voie royale pour s'ingérer dans un processus électoral démocratique est l'espace médiatique par le canal cyber. A un moment donné, dans le processus d'ingérence, l'action prend des formes de cybercriminalité au-delà de l'ingérence même. Les élections se sont déroulées sans problème.

« Le Point Tech et Net », un magazine web spécialisé en la matière, explique que « *l'Agence nationale de la sécurité des systèmes d'information (Anssi) trouve un motif de se réjouir des attaques informatiques qui se sont multipliées ces derniers mois: elles ont permis une prise de conscience des enjeux de la cybersécurité* » et cite Guillaume Poupard directeur général de l'Anssi «*Si l'on cherche un slogan, 2016, c'est l'année de la prise de conscience par l'ensemble de nos publics des questions de cybersécurité*».

Les agences nationales et les gouvernements des Etats développent leurs politiques de préventions et leurs capacités de résilience. Par exemple, le gouvernement fédéral a, avec ses partenaires, développé le Plan national pour des investissements stratégiques[21] dans lequel figure la lutte contre la cybersécurité. Le plan est aujourd'hui dans sa phase de mise en œuvre. Ce plan fixe la sécurité cyber comme deuxième priorité d'investissement après la thématique liée à la transition numérique :

« *Si nous voulons être un précurseur du numérique, nous avons besoin de la cybersécurité. Cela signifie une infrastructure sûre, des normes univoques et des réglementations claires. De cette façon, les entreprises, les citoyens et les autorités peuvent utiliser l'infrastructure numérique en toute sécurité. Cela alimente la confiance dans la technologie et protège notre pays contre les cyberattaques. Parmi les initiatives concrètes, citons la mise en place du portail ISAC permettant un partage rapide et efficace des connaissances. Notre volonté est aussi que les services de police, les services militaires et les services de sécurité soient mieux préparés aux incidents. Ils doivent être en mesure de réagir plus vite et plus efficacement en cas de cyberincidents. Nous devons en outre accorder une attention plus soutenue aux matières cyber dans l'enseignement secondaire tout comme il s'agit d'intensifier la recherche dans les matières cyber et la cybersécurité. Concernant le domaine de la cybersécurité, nous chiffrons les investissements à 15 milliards d'euros.* »

Le plan fixe 5 domaines de cybersécurité prioritaires :

- Infrastructure critique sécurisée,
- Protection de la population et des entreprises,
- Capacités et expertise adéquates en cybersécurité,
- Talent cyber,
- Recherche cyber.

En outre, le gouvernement fédéral développe chaque année une campagne médiatique pour promouvoir la cybersécurité à l'occasion du mois de la cybersécurité en octobre. Cette année, la campagne vise la lutte contre le phishing et s'intitule « Relax ! Réfléchissez à deux fois avant de cliquer sur un lien ». Le phishing est des modes opératoires des cybercriminels le plus répandu et le plus facile. Il s'agit d'une escroquerie commise en ligne au moyen de faux e-mails, sites web ou messages. Les cybercriminels tentent de duper leur victime en utilisant quelque chose digne de confiance ou en se faisant passer pour une personne digne de confiance. La Police fédérale et le Centre pour la Cybersécurité Belgique (CCB) travaillent en collaboration pour lutter contre ce mode opératoire. M. De Bruycker, directeur du CCB signale que, depuis le début du mois d'octobre et le lancement d'une campagne de sensibilisation à grande échelle, environ 5.000 courriels suspects ont été signalés quotidiennement au CCB, occasionnant la fermeture d'une centaine de sites web frauduleux par jour, soit trois fois plus qu'avant la campagne (une trentaine de sites fermés par jour).

---

21 https://www.premier.be/sites/default/files/articles/PNIS_Brochure_FR-WEB.pdf

En 2016, le gouvernement fédéral a validé un plan de gestion de crise cyber développé par le CCB, par le Centre de crise fédéral et leurs partenaires respectifs.

Les actions prises et le travail en matière de prévention ont permis à la Belgique d'améliorer sa position dans la liste des bons élèves en matière de cybersécurité.

En 2018, la Belgique occupe la 18ème place européenne et la 30ème place mondiale en termes de niveau de cybersécurité selon le « Global Cybersecurity Index » de 2018[22]. Dans une interview, le directeur du CCB[23] signale que « *la Belgique se débrouille plutôt bien face aux cybermenaces, qui touchent tant les citoyens que les entreprises et les administrations à l'ère du tout numérique. En l'espace d'un an et demi, notre pays est passé de la 11e à la 5ème place*[24] *dans le classement des pays européens les plus sûrs en termes de cybersécurité», à l'occasion de la Convention belge sur la cybersécurité, qui se tient à Malines* ».

Les approches des deux systèmes d'index sont différentes ; la première est davantage axée sur la bonne gouvernance et la deuxième est axée sur les incidents mêmes. Il y a lieu de comprendre que les actions préventives menées jusqu'ici sont positives et que le degré de conscientisation de la menace et du risque est élevé ; cependant, elles ne nous mettent pas à l'abri d'attaques cyber. En effet comme dans tout domaine, le risque zéro est un horizon vers lequel tendre mais qui ne peut être considéré comme un acquis permanent.

---

22 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
23 https://www.lalibre.be/economie/digital/cybersecurite-une-centaine-de-sites-web-frauduleux-par-jour-en-belgique-5da72f749978e218e341ea63
24 https://www.bitsight.com/sovereign-security-ratings

LA CYBERCRIMINALITÉ EN CHIFFRES EN BELGIQUE

La police fédérale mentionne l'évolution de faits enregistrés liés à la « *criminalité informatique*[25] » comme suit[26] :

FAITS LIÉS À LA CRIMINALITÉ INFORMATIQUE

2008	9.113
2009	11.673
2010	14.480
2011	15.772
2012	22.042
2013	18.057
2014	17.037
2015	18.074
2016	20.814
2017	21.419
2018	24.582

Soit une augmentation de 259% en 11 ans.

LA CYBERCRIMINALITÉ PAR SECTEUR

Secteur bancaire[27] : au deuxième trimestre 2019, 1.810 personnes ont été victimes de fraudes par phishing (hameçonnage). Cela représente une augmentation de 52% par rapport au premier trimestre, où 1.189 personnes avaient été victimes de ce type d'escroquerie. Cette augmentation est le résultat d'une nouvelle «vague» d'actes de phishing ou hameçonnage. Les 1.180 cas de fraude recensés au deuxième trimestre représentent un butin total de 1.919.540 euros. Cela signifie que les cybercriminels dérobent en moyenne 1.060 euros par victime. Cependant, ces moyennes couvrent une grande variété de cas individuels : alors que certains clients ont perdu 0,99 euro, il y a aussi des cas où le butin atteint plusieurs dizaines de milliers d'euros.

Secteur des entreprises en général : selon une étude de PwC, près des deux tiers (65%) des organisations belges ont été victimes de criminalité économique au cours des deux dernières années. La cybercriminalité reste le délit le plus répandu (53%) selon cette étude. Cette dernière précise que la cybercriminalité est le délit économique le plus courant en Belgique, 53% des personnes interrogées se déclarent en être victimes. Fait important à souligner : près des deux tiers (62%) des personnes interrogées en Belgique estiment que la cybercriminalité continuera d'être le délit économique le plus perturbateur au cours des 24 prochains mois, dépassant les autres types de criminalité.

25 Une des figures criminelles fixées par la Police fédérale pour leurs statistiques.
26 http://www.stat.policefederale.be/assets/pdf/crimestat/nationaal/rapport_2018_trim4_nat_belgique_fr.pdf
27 Article du 27 septembre 2019 sur febelfin.be

Les techniques les plus couramment utilisées par les cybercriminels sont le « hameçonnage » (66%), les logiciels malveillants (56%) et le scannage de réseau (16%).

Selon l'étude « The Impact of Cybercrime on Belgian Businesses" de 2017[28], un grand nombre d'entreprises sont victimes de la cybercriminalité ; au total, les deux tiers (66,5 %) des entreprises déclarent avoir été victimes, au cours des 12 derniers mois, d'au moins un des incidents des cinq types de cybercriminalité suivants : accès illégal aux systèmes IT (50 %); interférences entre les données et le système (46 %); cyber extorsion (24 %); fraude sur Internet (13 %) et espionnage d'entreprise (4 %). La majorité des entreprises qui ont déclaré avoir été victimes d'actes criminels ont indiqué avoir été attaquées plus d'une fois.

Secteur aéronautique : « The Brussels Times » a publié le 12 juin 2019[29] un article concernant la société « Asco, » un fabricant de pièces d'avion basé à Zaventem, qui confirme qu'il avait fermé ses opérations suite à une cyber-attaque sur les serveurs de la société. L'article précise que selon Data News, Asco a fermé sa base de Zaventem, ainsi que ses opérations dans d'autres pays, suite à une faille de sécurité. Environ 1 000 personnes ont été mise au chômage technique dans l'attente d'une reprise des activités de l'entreprise.

Secteur logistique et transport : le même « The Brussels Time » porte à la connaissance du public, le 28 juin 2017, que la cyber-attaque relative au ramsomware (logiciel de rançon) appelé « petya », qui visait initialement la Russie et l'Ukraine, s'étend également à d'autres régions du monde. La société danoise de transport et de logistique Maersk, qui opère notamment depuis le port de Zeebrugge, et la société biopharmaceutique MSD, active en Belgique, ont également été touchées. Les pirates exigeaient 300 dollars pour chaque ordinateur infecté. D'autres secteurs comme ceux de la santé ou de la mobilité par exemple font également l'objet de cybercriminalités.

Difficile de savoir si ces rançons sont acquittées par les entreprises victimes de ces chantages. Le principe de base est de ne pas payer. En effet, rien ne garantit que les fichiers volés ou cryptés par les cybercriminels seront retrouvés ou décryptés à la suite du paiement de la rançon. Par ailleurs, la rançon est à payer en bitcoins; encore faut-il donc disposer de ce type de monnaie. S'il s'avère après une analyse stratégique qu'il y a une raison impérieuse de retrouver les fichiers volés alors il peut être envisager de payer la rançon mais sans garantie aucune de retrouver les informations perdues. Cependant, il y a toujours lieu d'examiner préalablement la situation avec des experts cyber afin de vérifier s'il n'est pas possible de remettre la main sur les fichiers perdus/encryptés avant de prendre une décision. Quoiqu'il en soit, idéalement, il est préférable de ne pas en arriver à devoir se poser la question de payer ou de ne pas payer la rançon : la prévention est le maître mot en cybersécurité.

---

28 http://www.belspo.be/belspo/fedra/BR/BCC_ImpactCybercrimeBelgianBusinesses.pdf
29 https://www.brusselstimes.com/all-news/business/technology/58373/cyber-attack-causes-aircraft-parts-maker-to-close-indefinitely-asco/

PROPOSITIONS

La cybercriminalité est en augmentation : les modes opératoires évoluent, les techniques s'affinent et le nombre de victimes ainsi que les conséquences financières des attaques cybers augmentent. Parallèlement, nous vivons dans une société en pleine transition numérique, de plus en plus connectée et cybérisée, ce qui a pour conséquence que les opportunités d'attaques cybers se multiplient également. La cybersécurité est un challenge de tous les jours, un combat pour des moyens adéquats en qualité et en quantité. Les Etats ont largement pris conscience des menaces, dangers et risques, développent des politiques de prévention appropriées et augmentent leurs capacités de résilience.

Les Etats travaillent sur un mode collaboratif. L'Union européenne offre des structures et des coupoles de gestion adéquates ainsi que l'Agence de Communication de l'OTAN. Les pays s'exercent à la gestion de crise en matière cyber nationale et internationale. Certes, la dimension cyber est bien ancrée dans les réflexions politiques et gouvernementales. Cependant, il y a lieu de rester extrêmement prudent en matière d'analyse de risque et de se montrer très vigilant par rapport aux menaces. **Il importe de disposer des moyens budgétaires et de résilience les plus appropriés pour faire face à l'évolution de la cybercriminalité.**

Au niveau stratégique, par exemple, le Pacte national pour les investissements propose le développement d'écosystèmes stratégiques en Belgique dont celui du « *smart security* » en effet, comme le signale le Pacte d'Investissement Stratégique[30] :

« *La Belgique a de solides atouts pour développer un écosystème de smart security. La présence de grandes institutions européennes et de l'OTAN, ainsi que de centres de compétence de qualité en matière de cybersécurité, tels que la Cyber Security Coalition sont toutes à notre avantage. En outre, nous disposons d'acteurs solides sur le marché à croissance rapide de la cybersécurité. À ce jour, ce marché représente environ 350 millions d'euros en Belgique et croît chaque année d'environ 5% en moyenne, ce qui est supérieur à la croissance de l'économie dans son ensemble. Au cours des deux dernières années, ce marché a même connu une augmentation de 11 à 12%, laquelle est essentiellement due au développement de solutions de sécurité avancée, telles que la gestion des vulnérabilités et le suivi des incidents.* »

Les investissements dans ce secteur auront pour conséquence directe une amélioration de la cybersécurité nationale.

Pour limiter la cybercriminalité ou son impact, le Pacte national préconise également d' « *investir dans la sécurisation de nos infrastructures (critiques) et dans les cybercompétences de nos services de sécurité.*

30 Pacte national pour les investissements stratégiques, p32.

Trois investissements sont essentiels pour la sécurisation de nos infrastructures :

1. *Investir dans une infrastructure réseau sécurisée pour tous. Cela nécessite des normes Internet plus sûres (sécurité DNS, routage sécurisé, cryptage, etc.). Ces normes permettent d'échanger des données en toute sécurité (safe datatransport layer). L'échange de données en ligne est intégralement sécurisé, ce qui limite le risque d'attaques d'un des maillons faibles de la chaîne.*

2. Élaboration d'un banc d'essai (*testbed) pour infrastructures. Un banc d'essai est une plateforme qui permet de tester une nouvelle infrastructure avant qu'elle ne soit utilisée plus largement. Il s'agit d'un environnement fiable, contrôlé et sûr. Cela permet à des acteurs majeurs de tester de nouvelles fonctionnalités sans risquer d'impacter la société. Cette technique permet également de tester les réponses en cas de panne et les réparations.*

3. *Mise en place d'un portail en ISAC[31] belge pour l'échange rapide et efficace de connaissances en matière de cybersécurité. »*

De cette manière, l'économie belge sera mieux protégée des potentielles attaques cyber.

Au niveau conceptuel et méthodologique, la lutte contre la cybercriminalité, la recherche en la matière et le développement d'expertise peuvent certainement être favorisés par la mise en place de partenariats de trois secteurs : privé, public et académique. En la matière, la « cyber security coalition » belge fait office de figure de proue[32]. En effet, depuis 2015, cette coalition réunit le savoir-faire du secteur public, des entreprises ayant une expertise en matière de cybersécurité ainsi que le monde académique pour partager et renforcer leur connaissance. Leur « *mission est de renforcer la résilience de la cybersécurité en Belgique en construisant un écosystème de cybersécurité solide au niveau national. Nous le faisons en réunissant les compétences et l'expertise du monde académique, du secteur privé et des pouvoirs publics sur une plate-forme de confiance visant à favoriser l'échange d'informations et à mettre en œuvre des actions conjointes* ». La « cyber security coalition » se concentre sur quatre domaines stratégiques : le partage d'expérience, la collaboration opérationnelle, les recommandations politiques, le renforcement de la sensibilisation. Une telle collaboration ne peut être qu'encouragée.

Au niveau opérationnel, la meilleure attitude stratégique consiste à développer des accords de collaboration opératives entre CERT de différents pays et à augmenter qualitativement la capacité de résilience des Etats.

Grâce à ces accords de collaboration, on pourrait procéder à de fructueux échanges d'informations à propos des menaces cyber, de l'évolution du modus operandi des cybercriminels, des attaques cyber passées, des secteurs économiques impactés et des risques de contamination nationale et internationale. De telles collaborations permettraient une gestion préventive de crise cyber.

Pour augmenter les capacités de résilience, il faut disposer des dernières techniques et technologies pour contrer les attaques et s'en prémunir. Comment ? En faisant collaborer des analystes et experts en suffisance de différents services tant publics que privés. La qualité des experts et leur degré et niveau de collaboration est tout aussi importante que leur quantité.

---

31 « Information Sharing and Analysis Centers »
32 https://www.cybersecuritycoalition.be/fr/

Au niveau plus pratique, il faut, chacun, améliorer notre sécurité cyber au quotidien tant chez soi que sur notre lieu de travail. En effet, notre comportement en tant qu'utilisateur doit se transformer en des attitudes plus conscientes des risques cyber. C'est la dimension préventive active. La vigilance de tous est nécessaire pour améliorer la sécurité cyber globale par des actions individuelles de vigilance quant à des tentatives de phishing ou de vol de données. Et cela, entre autres, par le biais de contrôles réguliers de fonctionnement de son antivirus, la réalisation régulière de scan antivirus et de sauvegardes de fichiers, la détection de comportement non habituels de son ordinateur ou de systèmes d'information, l'attitude prudente à avoir lorsque l'on souhaite télécharger une pièce jointe ou surfer sur un site non sécurisé, ... Le développement de comportements appropriés des utilisateurs est essentiel pour garantir et augmenter la cybersécurité. Les actions citées ci-dessus permettent à tout un chacun d'éviter que son ordinateur fasse subitement partie d'un réseau d'ordinateurs infectés (botnet)[33] par un malware (logiciel malveillant), pour être contrôlés à distance par des cybercriminels. Une fois infecté, un tel ordinateur peut servir à envoyer des virus à d'autres ordinateurs ou à réaliser des attaques DDoS[34] à l'insu de son propriétaire et sans leur accord. Les meilleures actions favorisant la prudence IT sont à retrouver sur le site *safeonweb.be*. A l'ère des menaces numériques, la vigilance n'est plus seulement un devoir. C'est une nécessité.

33 Wiki : un botnet (de l'anglais, contraction de « robot » et « réseau ») est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.
34 Distributed Denial of Service attack

Centre Jean Gol

Avenue de la Toison d'Or 84-86
1060 Bruxelles

02.500.50.40
info@cjg.be

www.cjg.be

FÉDÉRATION
WALLONIE-BRUXELLES

Mise en page : Maurane Ballez

Editeur responsable : Richard Miller, Avenue de la Toison d'Or 84-86, 1060 Bruxelles