CAHIER DU CIRB 37

VERS UN PLAN RÉGIONAL DE **CYBERSÉCURITÉ**

Protéger et servir la population, les entreprises et les administrations dans leurs activités numériques

cirb.brussels
IT is for you

bps-bpv
.brussels
Bruxelles Prévention & Sécurité
Brussel Preventie & Veiligheid

TABLE DES MATIÈRES

LA RÉGION DE BRUXELLES-CAPITALE CONCENTRE DE NOMBREUSES INFRASTRUCTURES CRITIQUES D'INTÉRÊT POUR LES CYBERCRIMINELS.

PRÉAMBULE

Enfant, nous apprenons tous à regarder de chaque côté de la rue avant de la traverser. Nous intégrons en cela des concepts d'analyse du risque, appliquons des méthodes de prévention et, le cas échéant, apprenons de nos erreurs pour nous corriger. Pourquoi, dans la majorité des cas, sommes-nous incapables de procéder de manière identique lorsque nous empruntons les allées du cyberespace ?

L'actualité le rappelle sans cesse : des citoyen·ne·s aux entreprises en passant par les administrations, les attaques informatiques concernent et visent tout un chacun au quotidien. Les dégâts, s'ils ne se comptent pas nécessairement en vies humaines, peuvent en revanche se chiffrer en millions voire milliards d'euros. Cela sans parler de l'atteinte à l'image : malheur à qui faillit en la matière ! La cybersécurité constitue donc un enjeu de sécurité nationale, au même titre que la lutte contre le terrorisme.

Nos systèmes d'informations – aujourd'hui centraux dans notre fonctionnement, spécialement à l'ère de la smart city et de la mutualisation – sont-ils suffisamment préparés pour identifier ces menaces, les prévenir, les parer et, le cas échéant, s'en relever ?

Par sa population, par sa concentration d'entreprises ou de services publics touchant des millions de personnes dans des registres aussi variés que la finance, la mobilité, la santé et par la présence sur son territoire d'institutions internationales, la Région de Bruxelles-Capitale concentre de nombreuses infrastructures critiques d'intérêt pour les cybercriminels. À cet égard, il importe de pouvoir développer des réponses publiques pertinentes, adéquates et appropriées à la hauteur des enjeux et des compétences qui sont les nôtres.

Le présent Cahier répond à cette problématique essentielle. Il est le fruit d'un travail de réflexion commun du Centre d'Informatique pour la Région Bruxelloise (CIRB) et de Bruxelles Prévention & Sécurité (BPS), et s'inscrit dans le prolongement de nos collaborations déjà étendues. Nous y dressons l'état des lieux de la cybermenace, en proposant un cadre méthodologique pour y répondre.

Nous ne partons certes pas d'une feuille blanche. Tant le CIRB que BPS ont construit des bases solides en matière de cybersécurité. C'est le cas au niveau des infrastructures du CIRB (le Data Center Régional et le réseau IRISnet en premier lieu) et des services qu'il propose au niveau de la sécurité IT, de la mise en conformité avec le nouveau Règlement général sur la protection des données (mieux connu du public sous ses initiales anglaises GDPR) et d'outils de sécurité à la disposition de ses clients. BPS, quant à lui, a consacré à la cybersécurité une thématique de son Plan global de sécurité et de prévention validé le 2 février 2017 par le Gouvernement de la Région de Bruxelles-Capitale. Par ailleurs, des collaborations se mettent en place avec les acteurs du monde de la sécurité et de la formation notamment au sein de l'École régionale des métiers de la sécurité afin de développer une véritable filière dans le domaine de la cybersécurité au sein de la Région bruxelloise. Il importe donc de capitaliser ces acquis.

Pour cette raison, ce Cahier s'achève par une série de recommandations : celles-ci peuvent composer la trame dun plan régional de cybersécurité nécessaire pour asseoir le droit à la sécurité de tou·te·s les Bruxellois·e·s dans leur usage des services et des ressources numériques. Sa mise en application ne dépend pas seulement du CIRB et de BPS, mais doit impliquer toutes les parties prenantes à la sécurité au sein de notre Région.

Hervé Feuillien
Directeur général
CIRB

Robert Herzeele
Directeur général adjoint
CIRB

Jamil Araoud
Directeur général
BPS

INTRODUCTION

La Région de Bruxelles-Capitale voit dans la vague de la transformation digitale des opportunités pour les services publics leur permettant d'améliorer leur offre et de développer des capacités d'une smart city ou ville intelligente. Par ailleurs, un environnement numérique performant et sécurisé permet d'amplifier les capacités des entreprises privées les rendant plus compétitives par une offre de services et de produits adaptée à la demande d'un monde qui évolue en permanence. Les secteurs académiques et associatifs participent et bénéficient d'une numérisation sécurisée.

Le coût d'une transformation digitale et son risque sont des freins que rencontrent souvent ces acteurs. Un facteur qui fait croître ce prix de manière régulière est le risque de la cybersécurité et le coût lié à la mise en place de protections devenues essentielles.

L'augmentation des menaces et la multiplication de vulnérabilités causées par une complexité croissante, sont des challenges auxquels devront faire face tous les acteurs de cet univers économique devenu essentiel.

Le 20 novembre 2017, le Conseil des affaires générales de l'Union européenne a préconisé un renforcement de la cybersécurité européenne ainsi que de la cyber-résilience à l'échelle de l'Europe entière. Il nous semble important que la Région bruxelloise donne l'importance nécessaire à ce sujet et élabore un plan régional de cybersécurité.

Le Centre d'Informatique pour la Région Bruxelloise (CIRB), le partenaire informatique de confiance des institutions publiques régionales, locales et communautaires, se trouve à l'avant-plan pour aider sa région à planifier les risques de la cybersécurité et à s'en protéger. Il est, par nature, le partenaire privilégié pour conduire et coordonner les actions de conscientisation et de remédiation. Il est le fournisseur idéal pour offrir des services de base permettant d'offrir aux parties prenantes les fondations de base d'une protection responsable.

Par ailleurs, au travers de la mise en œuvre du Plan global de sécurité et de prévention (PGSP), notamment dans les thématiques « atteintes aux personnes », « radicalisme », « cybercriminalité » et « gestion de crise et résilience », Bruxelles Prévention & Sécurité (BPS) est aussi concerné par les actes de cybercriminalité et de la gestion des incidents graves dans l'univers du digital ayant des impacts réels conséquents.

La Région bruxelloise a joué depuis longtemps un rôle de leader dans l'automatisation et dans l'adoption des technologies nouvelles. Il est normal pour ses responsables de prendre la balle au bond et de proposer un plan régional de la cybersécurité qui est responsable, prévoyant et modulable. C'est en se basant sur des initiatives existantes au niveau régional, national et européen qu'elle identifie au mieux ses axes prioritaires selon les enjeux et les risques.

Ce plan décrit au mieux l'environnement existant, évalue les risques et les menaces et propose des actions prioritaires pour les différents acteurs principaux de la Région bruxelloise, notamment les services publics, les entreprises privées, le secteur académique et, surtout, le·la citoyen·ne. Les méthodes utilisées pour l'élaboration de ce plan se basent sur des cadres de référence reconnus et récents ainsi que sur des pratiques éprouvées.

Ce plan est ambitieux. Il exige de son public-cible une vigilance et une persévérance pour pouvoir profiter au mieux de la digitalisation et des bénéfices qu'elle apporte à la position concurrentielle des différents acteurs de notre région.

Professeur Georges Ataya
Directeur académique des formations en Sécurité de l'information et de la cybersécurité
de Solvay Brussels School of Economics and Management

© John Stapels

LA CYBERSÉCURITÉ CONSTITUE
UN ENJEU DE SÉCURITÉ NATIONALE,
AU MÊME TITRE QUE LA LUTTE
CONTRE LE TERRORISME.

1.

Les deux vagues mondiales de cyberattaques survenues à quelques semaines d'intervalle en 2017 (Wannacry et NotPetya), pour ne citer que ces deux exemples d'une année riche en actualité dans le domaine de la cyber(in)sécurité, ont éveillé l'attention non seulement sur ces avatars de la cybermenace mais aussi, voire surtout, sur la perméabilité des systèmes informatiques aux attaques.

1. DE LA CYBERCRIMINALITÉ AUX CYBERCONFLITS

La cybermenace n'épargne plus personne ni aucune organisation. Ses victimes ne sont en effet plus seulement ces utilisateurs isolés qui courent le risque d'une cyberattaque en raison des sites qu'ils fréquentent sur Internet, de leur naïveté (ouvrir une pièce jointe à un e-mail douteux) ou encore de la protection insuffisante de leur PC ou smartphone. Aujourd'hui, quelques heures suffisent pour rendre totalement inopérantes des entreprises de la taille d'une multinationale ou des administrations touchant des centaines de millions d'usagers. Quand ce n'est pas la stabilité même d'un État qui est visée.

Les fuites de données et les vulnérabilités informatiques subissent une inflation galopante. Dans son rapport dédié à l'année 2016, la division sécurité d'IBM estime à plus de 4 milliards le nombre de données compromises sur l'année, soit une progression de 566% par rapport à 2015[1]. Plus inquiétant : IBM souligne par ailleurs un glissement de la cybercriminalité organisée car, si les particuliers continuent d'être exposés, les utilisateurs professionnels ou « corporate accounts » constituent en effet la cible à atteindre désormais.

QUELQUES HEURES SUFFISENT POUR RENDRE TOTALEMENT INOPÉRANTES DES ADMINISTRATIONS TOUCHANT DES CENTAINES DE MILLIONS D'USAGERS

Ce glissement révèle le premier mobile généralement cité pour le cybercrime : l'argent. Attaquer le monde des entreprises et des institutions se révèle plus profitable en raison de leur meilleure solvabilité par rapport aux personnes physiques. Comme l'analyse le même rapport IBM : « *Les bandes organisées tendent à cibler le monde des entreprises parce qu'elles peuvent y voler des montants plus importants qu'auprès des personnes physiques. Dans l'arène de la cybercriminalité, les bandes sont par ailleurs le type d'acteurs qui disposent des ressources requises pour voler des sommes d'argent plus importantes.* »

L'enrichissement n'est cependant pas le seul dessein des attaques informatiques. Les enjeux de pouvoir entre États, sur les plans politique et militaire notamment, dominent également la scène. « *Les cyberattaques peuvent être plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars* » déclarait à ce propos le président de la Commission européenne Jean-Claude Juncker dans son discours sur l'état de l'Union en septembre 2017. De la cybercriminalité aux cyberconflits, la frontière est à cet égard parfois ténue. L'attaque de Wannacry a ainsi donné lieu à une accusation

1 Étude sur un échantillon de plus de 8.000 clients IBM répartis dans 100 pays. Source : IBM X-Force Threat Intelligence Index, en ligne (consulté le 22/12/2017). Disponible sur https://www.ibm.com/security/data-breach/threat-intelligence-index.html.

musclée à peine voilée de Microsoft à l'égard de la National security agency (NSA) des États-Unis. Wannacry utilisait en effet un outil de piratage informatique exploitant une faille de sécurité de systèmes d'exploitation comme Windows 7 ou Windows XP. Cet outil, une véritable cyberarme en fait, avait été initialement développé par la NSA dans le plus grand secret, même de Microsoft, avant d'être dérobé à l'agence américaine de renseignement. Son détournement à l'origine de Wannacry a par conséquent poussé le directeur des affaires juridiques de Microsoft à écrire dans un communiqué officiel : « *Cette attaque démontre une nouvelle fois pourquoi le stockage des données vulnérables par les pouvoirs publics est un tel problème. C'est un schéma émergent en 2017. [...] Et cette attaque récente constitue un lien totalement non intentionnel et déconcertant entre les deux formes les plus sérieuses de cybermenaces dans le monde d'aujourd'hui – action de l'État-nation et action de la criminalité organisée* [2]. »

Non seulement les États utilisent les mêmes outils que les cybercriminels et les cyberterroristes pour s'en défendre mais, parfois, viennent à se confondre avec ceux-ci. Le cyberespace est devenu le nouveau théâtre d'opérations des services de renseignement. Le pouvoir de déstabilisation de cyberattaques menées par des États est réel. Les dernières campagnes électorales présidentielles aux États-Unis et en France en attestent. Dans les deux cas, la fuite de données informatiques sensibles, attribuée à une puissance étrangère, a mis en péril la campagne de candidats à ces élections, la défaite d'Hillary Clinton y trouvant sa source pour nombre d'analystes. Le pouvoir de manipulation des opinions publiques via les réseaux sociaux constitue ainsi l'un des risques globaux identifiés par le Forum économique mondial sur base du constat que 63% des utilisateurs de ces réseaux s'informent par leur intermédiaire.

2. LES RÉSEAUX ONT GLOBALISÉ LES RISQUES

Le concept même de cyberattaque suppose de pouvoir pénétrer un ordinateur voire un système informatique entier. Les portes d'entrées peuvent prendre la forme d'un support physique. L'histoire retient ainsi que l'un des premiers virus parmi les plus redoutables, Brain, se cachait dans des disquettes. C'est cependant le développement de l'informatique en réseau qui a réellement démultiplié les possibilités de transmission des attaques. Dès 1972, un chercheur trouva le moyen d'infecter des machines connectées au réseau de l'armée américaine ARPANET, l'ancêtre d'Internet. Avec l'essor du réseau des réseaux, la cybermenace est elle-même montée en flèche : le nombre de malwares a été multiplié d'un millier environ vers 1990 à plus de 200 millions en 2010. Dans le même temps, les premières attaques visant les terminaux mobiles se sont déroulées dans les années 2000.

Comme l'analyse le Forum économique mondial (FEM), notre dépendance croissante à Internet et aux technologies de l'information et de la communication (TIC) est devenue l'une des principales sources de risques globaux, dont ceux liés à la cybercriminalité. Dans les conclusions de l'édition 2017 de son rapport The Global Risks Report, le FEM écrit : « *Une plus grande interdépendance entre les différents réseaux d'infrastructure augmente la portée des échecs systémiques – qu'ils résultent de cyberattaques, d'erreurs logicielles, de catastrophes naturelles ou d'autres causes – pour dévaler en cascade dans les réseaux et affecter la société de manières inattendues.* »

2 SMITH, Brad. The need for urgent collective action to keep people safe online : Lessons from last week's cyberattack. Microsoft On the Issues, Microsoft, en ligne (consulté le 22/12/2017). Disponible sur https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack.

À chaque attaque se pose cette double question : qui sera la victime suivante et quelle sera l'envergure de l'attaque dont elle sera la cible ? Une étude conjointe des bureaux de consultance KPMG et de recrutement Harvey Nash [3] ne laisse planer aucune ambiguïté quant à l'ampleur de la vulnérabilité des systèmes informatiques. Selon cette étude réalisée auprès de 4.000 directeur·rice·s et responsables des systèmes d'information (DSI) dans 86 pays :

- un tiers des DSI a été confronté à une faille de sécurité informatique au cours des deux dernières années et un·e sur deux dans les grandes entreprises ;
- un cinquième seulement des DSI (21%) affirme que son organisation aurait la capacité de faire face à une cyberattaque ;
- près d'un·e DSI sur deux (47%) cite les attaques venues de l'intérieur parmi ses principales préoccupations.

Le volet belge de l'étude KPMG/Harvey Nash fait entrevoir une situation encore plus préoccupante dans notre pays : « *Plus de 42% des entreprises en Belgique ont subi des cyberattaques majeures au cours des 2 dernières années. Par ailleurs, par rapport à la moyenne générale, les entreprises belges déclarent se sentir à la fois moins confiantes et insuffisamment préparées à faire face aux attaques actuelles et futures.* [4] »

L'acuité de la menace est pareillement mise en lumière par l'agence de l'Union européenne chargée de la sécurité des réseaux et de l'information, l'European Network and Information Security Agency (ENISA [5]). Dans l'édition 2017 de son recensement annuel des 15 principales formes de cybermenaces, l'agence n'en mentionne qu'une seule en déclin, tandis que onze sont classées en progression, ce qui représente une aggravation par rapport à 2016 où neuf menaces seulement étaient répertoriées en progression.

L'ENISA commente à ce propos que « *la complexité des attaques et la sophistication des actes de malveillance dans le cyberespace continuent d'augmenter* ». L'agence européenne retire de ses observations de la cybermenace en 2017 les six faits marquants suivants :

- Les agents de menace en tous genres ont progressé dans l'offuscation, c'est-à-dire la capacité à effacer ses traces.
- Les infrastructures malveillantes continuent à évoluer vers des fonctions configurables à objectifs multiples, parmi lesquelles l'anonymisation, le cryptage et l'évasion (qui contourne la détection d'intrusion).
- La monétisation du cybercrime devient la principale motivation des agents de menace, en particulier des cybercriminels. Ils tirent avantage de l'anonymat offert par les cybermonnaies.
- Les acteurs sponsorisés par l'État comptent parmi les agents malveillants les plus omniprésents dans le cyberespace. Ils sont une des priorités dans ce qui préoccupe les défenseurs du monde des affaires et des pouvoirs publics.
- La cyberguerre fait une entrée dynamique dans le cyberespace, engendrant des préoccupations accrues pour les opérateurs d'infrastructures, surtout dans les domaines qui souffrent de certaines sortes de cybercrises.

3 KPMG. À l'ère des cybermenaces, les DSI relèvent les défis de la sécurité et de l'innovation digitale. Communiqué de presse. Communiqués de presse, KPMG, 28 juin 2017, en ligne (consulté le 22/12/2017). Disponible sur https://home.kpmg.com/fr/fr/home/media/press-releases/2017/06/cio-survey-cybermenaces-dsi-defis-innovation-digitale.html

4 KPMG Belgium. Harvey Nash/KPMG International CIO Survey 2017. Press releases, KPMG Belgium, 18 août 2017, en ligne (consulté le 22/12/2017). Disponible sur https://home.kpmg.com/be/en/home/media/press-releases/2017/08/harvey-nash-kpmg-international-cio-survey-2017.html.

5 À propos du rôle et de l'action de l'ENISA, lire en page 32 la section 3.2. « Les acteurs clés de la cybersécurité ».

• Le savoir-faire et les capacités demeurent le souci principal des organisations. L'offre de programmes de formation et de cursus adaptés à la situation est quasi inexistante.

LES 15 PRINCIPALES CYBERMENACES RECENSÉES EN 2017*

Rang	Menace**	Tendance d'évolution de la menace	Évolution classement 2016 - 2017***
1	Malware	→	=
2	Attaques provenant du Web	↑	=
3	Attaques visant des applications Web	↑	=
4	Phishing	↑	+2
5	Spam	↑	+2
6	Attaques par déni de service	↑	-2
7	Rançongiciel	↑	+1
8	Botnets	↑	-3
9	Menace interne (malveillante ou accidentelle)	→	=
10	Dommage/vol/perte physique	→	=
11	Violation de données	↑	+1
12	Vol d'identité	↑	+1
13	Fuite d'informations/de données	↑	+1
14	Kit exploitant une faille de sécurité	↓	-3
15	Cyberespionnage	↑	=

*Source : ENISA, Threat Landscape 2017 report : cyber-threats becoming top priority, janvier 2018 [6].
**Pour une définition des menaces, lire ci-après le tableau «Les outils et stratégies des cybercriminels» en pages 16 et 17.
***Nombre de places gagnées ou perdues dans le classement d'une année à l'autre.

3. LES SERVICES DE PREMIÈRE NÉCESSITÉ COMME CIBLES

« *Je ne serais pas étonné qu'avant 5 ans, il y ait des tentatives d'utiliser Internet pour commettre des attentats. C'est-à-dire entrer dans le Scada (NDLR : Supervisory Control and Data Acquisition), le centre de gestion d'une centrale nucléaire, d'un barrage, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer* », analysait Gilles de Kerchove, le coordinateur de l'Union européenne pour la lutte contre le terrorisme, au lendemain des attentats du 22 mars 2016 [7].

Les services publics et, notamment, **les fournisseurs d'utilités** ne sont évidemment pas épargnés. Les exemples ne manquent pas à ce niveau. Le plus célèbre d'entre eux concerne l'Ukraine où, à la fin décembre 2016, quelque 700.000 foyers furent privés d'électricité suite au premier cas communément admis de cybersabotage réussi du réseau électrique d'un pays tout entier [8]. Quelques mois plus tard, en juin 2017, l'Ukraine paya à nouveau un lourd tribut cette fois à l'attaque NotPetya. Ce fut notamment au tour du réseau de métro de Kiev ou de la centrale nucléaire de Tchernobyl d'être mis à l'arrêt.

6 Le rapport complet (en anglais) peut être téléchargé depuis la page www.enisa.europa.eu/news/enisa-news/enisa-report-the-2017-cyber-threat-landscape.
7 de KERCHOVE, Gilles. Attentats : «D'ici 5 ans, ils pourraient prendre le contrôle d'une centrale nucléaire». La Libre Belgique, IPM, 26/03/2016, en ligne (consulté le 22/12/2017). Disponible sur http://www.lalibre.be/actu/belgique/attentats-d-ici-5-ans-ils-pourraient-prendre-le-controle-d-une-centrale-nucleaire-56f58f4d35708ea2d3e8e878.
8 COLLINS, Katie. Ukraine blackout is a cyberattack milestone. CNET – Security, CNET, CBS Interactive, 05/01/2016, en ligne (consulté le 22/12/2017). Disponible sur https://www.cnet.com/news/cyberattack-causes-widespread-power-blackout-in-ukraine/.

Le **secteur de la santé et les hôpitaux** en particulier constituent également une cible des cyberattaques. La diffusion de Wannacry en mai 2017 a par exemple largement déstabilisé les services du National Health Service (NHS - Service national de santé) britannique. Aux États-Unis, en février 2016, l'attaque subie par le Hollywood Presbyterian Medical Center de Los Angeles a mis en lumière la vulnérabilité globale du secteur. L'hôpital en question s'est trouvé bloqué pendant une dizaine de jours. Non moins de 900 dossiers de patients ont été perdus et, au final, une rançon de quelque 15.000 dollars a été versée pour remettre le système informatique de l'hôpital en fonction. Ce cas n'est pas isolé : les médias américains ont rapporté à l'époque que quatre autres hôpitaux avaient déjà été victimes de telles attaques. Selon l'éditeur de solutions de sécurité informatique Symantec, les données médicales représentent un trésor de premier choix pour les pirates informatiques. « *Les dossiers médicaux contiennent la plupart des données qui intéressent les cyberpirates, et sont une cible idéale pour les voleurs d'informations* », analyse Symantec [9]. Ce risque est d'autant plus avéré que le secteur hospitalier se distingue par la forte dispersion de ses sites, beaucoup de faible taille, le manque de culture de leur personnel en matière de cybersécurité, le faible niveau d'investissement en sécurité informatique ainsi que la forte progression d'équipements connectés, dont le manque de protection constitue une nouvelle porte d'entrée pour les cybercriminels.

L'explosion du marché de ces objets connectés (ou Internet of things), en nombre comme en variété, suscite l'inquiétude croissante des milieux spécialisés en sécurité informatique. Or, leur mise en réseau les expose à la cybermenace de même que les terminaux traditionnels (PC, smartphone) auxquels ils peuvent être connectés. Cette fragilité est d'autant plus avérée que, souvent, ces objets connectés ne bénéficient pas d'un niveau de protection à la hauteur des attaques dont ils peuvent être les vecteurs. Les équipements médicaux cités plus haut ne sont ainsi pas les seuls concernés. Le thermostat d'ambiance commandé à distance, ce gadget poussé par la vague de la domotique, expose le smartphone de son propriétaire à une intrusion malveillante. Même les équipements de sécurité ne sont pas sans faille : en mai 2017, un fournisseur de matériel informatique s'est vu assigné en justice par la Federal Trade Commission (FTC) pour ne pas avoir sécurisé ses caméras de surveillance connectées via Internet. Après les voitures connectées, les véhicules autonomes qui dépassent peu à peu le stade du prototype, représentent déjà la prochaine cible annoncée des cyberattaques. Les déficiences des objets connectés en termes de sécurité interpellent également les gestionnaires de la smart city où se généralisent les capteurs communicants connectés à des réseaux soutenant les services essentiels à la communauté comme les utilités (énergie, eau...), le trafic, la sécurité...

LES DÉFICIENCES DES OBJETS CONNECTÉS EN TERMES DE SÉCURITÉ INTERPELLENT ÉGALEMENT LES GESTIONNAIRES DE LA SMART CITY

9 Symantec. Cybersecurity in Healthcare : Why It's Not Enough, Why It Can't Wait. (Infographie). Symantec - Healthcare Symantec, Symantec, en ligne (consulté le 22/12/2017). Disponible sur https://www.symantec.com/content/dam/symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf.

LES OUTILS ET STRATÉGIES DES CYBERCRIMINELS

Advanced persistent threat (APT)	Backdoor (Porte dérobée)	Botnet
Attaque cumulant diverses techniques (phishing, malware, exploit kit...) s'étendant sur une période prolongée, avec un objectif de compromission ciblée (une donnée, un processus en particulier)	Fonction d'accès à un logiciel, inconnue de son utilisateur, soit dans un but légitime (par exemple mise à jour à distance prévue par le concepteur du logiciel), soit malveillant (pour prendre le contrôle des données du logiciel voire plus largement de la machine ou de son réseau)	Réseau de machines asservies, aussi dites « zombies », par un élément de code permettant d'en prendre le contrôle à distance pour des attaques de type DDoS, à l'insu de leur utilisateur
Déni de service	**Déni de service distribué DDoS**	**Exploit kit**
Saturation d'un réseau ou d'un service par l'envoi massif de requêtes aboutissant à empêcher ou limiter fortement sa capacité à fournir le service attendu	Attaque faisant intervenir un grand nombre de machines (souvent constituées en botnet) comme vecteurs des requêtes massives	Ensemble de données ou de codes exécutables programmés pour exploiter les failles de sécurité des logiciels et du système d'exploitation d'une machine en vue de la contaminer, d'en extraire les données...
Ransomware (rançongiciel)	**Rootkit**	**Spam**
Logiciel malveillant reçu par e-mail ou via Internet provoquant le blocage d'un ordinateur ou d'un réseau par chiffrement de ses fichiers, voire l'ordinateur entier, et exigeant une rançon en vue d'obtenir une clé de déchiffrement	Ensemble d'outillages informatiques permettant de prendre furtivement le contrôle d'une machine à son niveau le plus profond (root = administrateur) offrant les privilèges les plus élevés sur la machine	Bien connu pour polluer les messageries électroniques de messages non désirés, le spam constitue plus spécifiquement le support d'infection de systèmes informatiques à l'aide de pièces jointes malveillantes. En décembre 2016, selon IBM, près de 50% des spams contenaient des malwares sous forme de pièce jointe, dont 85% de rançongiciels [10]
Wiper (Effaceur)	**Zero day (Vulnérablité jour 0)**	
Logiciel malveillant effaçant les données d'un ordinateur, sans possibilité de les récupérer	Faille d'un logiciel inconnue de son éditeur offrant par conséquent à son découvreur malveillant un avantage de poids en raison de l'inexistence de parade à cette faille	

10 IBM X-Force Threat Intelligence Index. Déjà cité.

	Cheval de Troie	**Darknet**
	Technique consistant à installer sur un ordinateur un logiciel non sollicité, le plus souvent à caractère malveillant, à partir d'un logiciel téléchargé (le cheval proprement dit) par l'utilisateur	Ce réseau, souvent décrit comme la face cachée de l'Internet, repose sur un anonymat organisé tant des sites qu'il contient, que de ses utilisateurs. Si cette confidentialité offre un refuge à des personnes ou organisations en dissidence, elle est aussi exploitée pour diffuser de manière illégale des services ou produits, dont des ressources logicielles, matérielles ou humaines pour mener des cyberattaques.
	Malware (Logiciel malveillant)	**Phishing (Hameçonnage)**
	Terme générique regroupant des logiciels frauduleux ouvrant l'accès d'une machine à l'insu de son utilisateur : logiciels espions, virus, chevaux de Troie, vers informatiques, rootkits, rançongiciels, détourneur de navigateur...	Envoi à un grand nombre de destinataires d'un message générique usurpant l'identité d'un expéditeur de confiance (banque, fournisseur, administration...) afin de soutirer aux victimes des renseignements personnels (login et mot de passe, code bancaire...)
	Spear phishing	**Water holing (attaque de point d'eau)**
	Variante de l'hameçonnage consistant à l'envoi à un nombre limité d'utilisateurs (souvent un seul) d'un message fortement personnalisé grâce à des techniques d'ingénierie sociale (collecte d'un maximum d'informations sur la cible via des sources comme des registres publics ou des réseaux sociaux)	Ce type d'attaque fait référence au prédateur qui préfère attendre sa victime à un endroit (le point d'eau) ou moment précis, plutôt que de l'attaquer directement. Face à un système fortement protégé, le hacker pratiquant le water holing profitera d'une brèche liée aux habitudes de sa victime pour s'introduire dans son système. Début 2017, plusieurs banques de Pologne ont ainsi été infectées en raison de leurs visites récurrentes sur le site de l'autorité nationale de supervision des marchés

2.

LE CADRE DU PLAN RÉGIONAL DE CYBERSÉCURITÉ

Notre projet de plan de cybersécurité pour la Région de Bruxelles-Capitale s'appuie sur des bases solides. Ces fondations sont le résultat d'un benchmarking des approches déjà à l'œuvre dans d'autres pays et appliquent les méthodologies éprouvées en cette matière.

1. BENCHMARKING DES APPROCHES PUBLIQUES EN MATIÈRE DE CYBERSÉCURITÉ

Un tour d'horizon des approches publiques en matière de cybersécurité constitue une étape nécessaire afin d'identifier des objectifs et méthodes qui pourraient utilement inspirer la stratégie à mettre en place en Région de Bruxelles-Capitale.

Le présent benchmarking étudie à ce niveau les stratégies appliquées par les pays limitrophes de la Belgique ainsi que par des entités fédérées, une dimension essentielle s'agissant de définir une stratégie régionale.

1.1. Étendue du benchmark

Au niveau des États

Tous les États de l'Union européenne ont défini une stratégie de cybersécurité et mis en place des organes et méthodes en vue de la concrétiser. Certains pays, cependant, se distinguent par la maturité de leur approche, leurs plans ayant déjà connu diverses évolutions. C'est le cas en particulier de deux pays limitrophes de la Belgique : les Pays-Bas et le Luxembourg. Notre benchmark s'est également intéressé au cas de l'Estonie, pays visé notamment en 2007 déjà par une cyberattaque généralisée [1] et hôte du Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE) [2].

Au niveau d'entités fédérées

Les stratégies de cybersécurité sont rares à l'échelon d'entités fédérées voisines de la Belgique. En Allemagne, les deux Länder limitrophes de notre pays, la Rhénanie-Palatinat et la Rhénanie-Westphalie, ne disposent par exemple pas encore de leur propre stratégie en la matière. Les Régions françaises, quant à elles, ne possèdent ni les compétences, ni les capacités pour mettre en place une telle stratégie.

Il faut donc pousser plus loin la recherche pour analyser un cas de stratégie à l'échelon fédéré. En l'occurrence, l'exemple vient ici du Québec. La province canadienne dispose d'une stratégie de sécurité de l'information avec un objectif cybersécurité qui a été également analysé.

1.2. Les axes fondamentaux d'une stratégie de cybersécurité

La comparaison des stratégies de ces différentes sources montre trois objectifs communs :

- assurer une protection adéquate des administrations publiques et des infrastructures critiques contre les cybermenaces ;
- accroitre la confiance des citoyen·ne·s dans le cyberespace en luttant contre la cybercriminalité ;

1 Le cas de l'Estonie en 2007 est souvent décrit comme le premier exemple dans l'histoire d'Internet d'une attaque orchestrée par un État contre les réseaux d'un autre pays.
2 Pour plus d'informations sur le Centre d'excellence de cyberdéfense coopérative de l'OTAN, consulter le site https://ccdcoe.org/.

- développer une compétence propre en cybersécurité.

Les stratégies recensées par notre benchmark reposent par ailleurs sur trois approches comparables d'un pays à l'autre :

- l'approfondissement de l'expertise et des connaissances des administrations, des entreprises et des citoyen·ne·s en matière de cybersécurité ;
- le développement de la coopération et la coordination internationale (et inter-régionale) ;
- la centralisation des actions et de la veille en matière de cybersécurité.

De plus, les mesures concrètes pour mettre en place la cybersécurité dans les différents cas analysés partagent un même cadre méthodologique : le Cybersecurity Framework (CSF) formulé par le National Institute of Standards and Technology (NIST – USA) en vue d'assurer la protection des infrastructures critiques d'un pays (lire ci-après en pages 27 et 41).

2. LA CYBERSÉCURITÉ : QUELLE DÉFINITION ?

Contre quoi s'agit-il de s'organiser, avec quels objectifs et moyens, lorsqu'il est question de cybersécurité ? De multiples acteurs actifs dans le domaine livrent chacun leur définition de cette notion. Notre vision de la cybersécurité pour la Région de Bruxelles-Capitale s'inspire de ces sources.

2.1. Au niveau international

En 2010, déjà, l'**Union internationale des télécommunication (UIT)** a adopté la définition suivante de la cybersécurité : « *L'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants : disponibilité, intégrité (qui peut englober l'authenticité et la non-répudiation), confidentialité* [3]. »

L'**Union européenne**, pour sa part, a livré une définition dans sa Stratégie de cybersécurité[4], présentée en février 2013 et actualisée en septembre 2017. Pour l'Union européenne, « *la cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues* ». La Stratégie vise à ce titre à mettre en œuvre « *les mesures de sauvegarde et les actions auxquelles il est possible de recourir pour protéger le cyberespace, dans les domaines civil et militaire, des*

3 Union internationale des télécommunications. Les décisions phares de Guadalajara : cybersécurité. Compte-rendu en ligne de la Conférence de plénipotentiaires de l'UIT 2010 à Guadalajara, Nouvelles de l'UIT, UIT, novembre 2010, en ligne (consulté le 16/02/2018). Disponible sur http://www.itu.int/net/itunews/issues/2010/09/20-fr.aspx.

4 Commission européenne, Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité. Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé. 7/2/2013, Bruxelles, en ligne (consulté le 16/02/2018). Disponible sur http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_fr.pdf.

menaces associées à ses réseaux interdépendants et à son infrastructure informatique ou susceptibles de leur porter atteinte ». De plus, la Commission européenne rappelle que les enjeux de cybersécurité se placent également sur le terrain des droits fondamentaux des citoyen·ne·s européen·ne·s en affirmant que « la cybersécurité est essentielle pour protéger la vie privée et les données à caractère personnel des individus conformément aux articles 7 et 8 de la Charte des droits fondamentaux de l'UE » [5].

À l'occasion du 70e anniversaire de l'**Organisation internationale de normalisation (ISO)**, célébré en février 2017, son président en exercice a placé la cybersécurité parmi les défis d'envergure mondiale à relever à l'avenir, au même niveau que le changement climatique ou la rareté de l'eau [6]. En l'occurrence, l'ISO englobe la cybersécurité dans la famille de normes ISO 2700x décrite comme la boîte à outils de normes sur la sécurité devant mettre les organismes à l'abri des cyberattaques.

Parmi ces outils, on peut notamment pointer :

- la norme ISO/CEI 27001:2013 concerne la mise en œuvre de Systèmes de management de sécurité de l'information (SMSI) et, selon le professeur Edward Humphreys, coordinateur des normes ISO 2700x, « *apporte un cadre de gestion pour l'évaluation et le traitement des risques, cyberorientés ou non, qui peuvent porter préjudice aux entreprises et aux gouvernements, voire endommager la trame de l'infrastructure nationale d'un pays* » [7] ;
- la norme ISO/CEI 27032:2012 (en cours de révision) offre, quant à elle, des lignes directrices pour la cybersécurité, c'est-à-dire la protection du cyberespace qu'elle définit comme « *un environnement complexe, fondé sur les interconnexions entre personnes, logiciels et services, et rendu possible par la diffusion mondiale de dispositifs et de réseaux de technologies de l'information et de la communication (TIC)* ». En vue de se prémunir contre des attaques telles que notamment les manipulations relevant de l'ingénierie sociale, le piratage, les logiciels malveillants, elle se repose sur la trilogie détecter, maîtriser, affronter.

2.2. Au niveau de différents pays

Le **grand-duché de Luxembourg** – étudié dans le benchmarking introductif de ce chapitre – a publié en 2015 la seconde version de sa Stratégie nationale en matière de cybersécurité[8], trois ans à peine après la première mouture de celle-ci. Les autorités grand-ducales utilisent de multiples canaux de communication pour informer et mobiliser les publics-cibles que sont les entreprises et les citoyen·ne·s notamment. Dans sa version révisée en 2015 de Stratégie de cybersécurité, le Luxembourg s'est aligné sur la définition de l'UIT.

5 Commission européenne, Direction générale des réseaux de communication, du contenu et des technologies. Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité). Cybersecurity Package, site internet de la Commission européenne, en ligne (consulté le 16/02/2018). Disponible sur https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en.

6 Organisation internationale de normalisation. L'ISO fête ses 70 ans ! Communiqué de presse. Archives, Actualités, site Internet de l'ISO, en ligne (consulté le 16/02/2018). Disponible sur https://www.iso.org/fr/news/2017/02/Ref2163.html.

7 HUMPHREYS, Edward. La nouvelle cyberguerre. Archives, Actualités, site Internet de l'ISO, octobre 2013, en ligne (consulté le 16/02/2018). Disponible sur https://www.iso.org/fr/news/2013/10/Ref1785.html.

8 Gouvernement du grand-duché de Luxembourg, Ministère d'État Haut-Commissariat à la Protection nationale. Stratégie nationale en matière de cybersécurité II. Cybersécurité et sécurité de l'information, site Internet du Gouvernement du grand-duché de Luxembourg, en ligne (consulté le 16/02/2018). Disponible sur https://cybersecurite.public.lu/fr/securite-information/strategie-nationale.html.

Aux **États-Unis**, la définition officielle de la cybersécurité [9] rejoint partiellement celle adoptée par l'UIT et est en usage parmi toutes les agences fédérales : « *La prévention des dégâts, la protection et la restauration des ordinateurs, systèmes de communication électronique, services de communication électronique, communications filaires et communications électroniques, en ce compris les informations qu'ils contiennent, pour garantir leur disponibilité, leur intégrité, leur authentification, leur confidentialité et leur non-répudiation.* »

Les **Pays-Bas**, par l'intermédiaire du Nationaal Cyber Security Centrum (NCSC), dépendant du ministère néerlandais de la Sécurité et de la Justice, en donnent la définition suivante [10] : « *La cybersécurité tend à prévenir les dégâts consécutifs à des perturbations, pannes ou erreurs d'utilisation des TIC et, le cas échéant, à réparer les dégâts. Les dégâts aux TIC se présentent sous la forme d'une atteinte à la fiabilité des TIC, une limitation de la disponibilité et une violation de la confidentialité et/ou de l'intégrité des informations stockées dans les TIC.* »

En **France**, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au secrétaire général de la défense et de la sécurité nationale qui assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale, définit la cybersécurité comme « *l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* [11] ».

L'**Estonie** envisage sa cybersécurité comme les moyens à déployer pour anticiper les menaces potentielles et y répondre de manière appropriée, de manière à protéger le pays et ses citoyen·ne·s dans le cyberespace. Placée sous l'autorité du ministère des Affaires économiques et des Communications, la stratégie de cybersécurité estonienne s'articule selon trois axes : la défense des infrastructures critiques et des services vitaux, la lutte contre la cybercriminalité et la défense nationale.

3. LES ACTEURS ET POLITIQUES DE CYBERSÉCURITÉ EN PLACE

Comme le souligne l'ENISA : « *Vu que les menaces ne s'arrêtent pas aux frontières, il est essentiel de se concentrer sur une coopération internationale forte. La coopération au niveau paneuropéen est nécessaire pour se préparer efficacement aux cyberattaques, mais aussi pour les contrer. Les stratégies globales de cybersécurité nationale sont un premier pas dans cette direction.* [12] »

La Région ne peut donc agir seule. Le plan régional de cybersécurité doit s'intégrer dans les approches et les modèles définis aux autres niveaux que sont l'État fédéral et l'Union européenne, ainsi qu'en concertation avec les autres entités fédérées de notre pays.

9 United States of America, National Security Agency. Glossary. Committee on National Security Systems (CNSS), NSA, N° 4009, Avril 2015. Disponible sur le blog cryptosmith.com (consulté le 16/02/2018) : https://cryptosmith.com/glossary/.
10 Nederlandse rijksoverheid, Ministerie van Justitie en Veiligheid, Nationaal Coördinator Terrorismebestrijding en Veiligheid. Nationale Cybersecurity Strategie 2 - Van bewust naar bekwaam. Nationale Cybersecurity Strategie, site Internet du Ministerie van Justitie en Veiligheid, en ligne (consulté le 16/02/2018). Disponible sur https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie.
11 République française, Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information. Glossaire. Glossaire, site Internet de l'ANSSI, en ligne (consulté le 16/02/2018). Disponible sur https://www.ssi.gouv.fr/entreprise/glossaire/c/.
12 FALESSI, Nicole, GAVRILA, Razvan, KLEJNSTRUP, Ritter, MOULINOS, Konstantinos. National Cyber Security Strategies - Practical Guide on Development and Execution. Agence européenne chargée de la sécurité des réseaux et de l'information, Union européenne, 19 décember 2012, en ligne, (consulté le 16/02/2018). Disponible sur https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

3.1. La cybersécurité à l'échelle européenne

La cybersécurité fait partie intégrante des initiatives menées par l'Union européenne (UE) en vue d'établir et renforcer le marché unique numérique. Sécuriser le cyberespace participe ainsi de la politique européenne qui vise à supprimer les entraves empêchant d'exploiter pleinement les possibilités offertes par Internet. « *Une fois le marché unique numérique totalement opérationnel,* écrit la Commission européenne [13]*, il y aura moins d'obstacles et plus de possibilités : les citoyen·ne·s et les entreprises pourront faire du commerce et innover sans entraves. Ils pourront le faire en toute légalité, en toute sécurité et à des prix abordables, ce qui leur facilitera la vie.* » En tant que telle, la politique de cybersécurité de l'UE dessert des objectifs de maintien de l'activité économique et de préservation de la prospérité.

LES NORMES, PRINCIPES ET VALEURS QUE L'UNION EUROPÉENNE DÉFEND HORS LIGNE DOIVENT AUSSI S'APPLIQUER EN LIGNE.

À cette fin, l'Europe a entrepris, en septembre 2017, de renforcer sa stratégie définie en 2013, à l'aide d'un paquet cybersécurité en trois axes : résilience, dissuasion et défense. Parallèlement, l'UE s'est dotée d'un cadre réglementaire modernisé en vue de soutenir le marché unique numérique. Deux textes fondamentaux entretiennent à cet égard un lien avec les questions de cybersécurité : le règlement européen GDPR (pour General Data Protection Regulation) et la toute première législation visant la sécurité des réseaux et des systèmes d'informations des États membres (ou directive NIS).

3.1.1. La stratégie de cybersécurité de l'Union européenne

La **Stratégie de cybersécurité de l'Union européenne**, présentée en 2013 et amendée en 2017, constitue le cœur de l'approche prônée par la Commission européenne pour protéger l'espace numérique, ses entreprises et ses utilisateurs·trices. D'envergure globale, elle se complète de textes et mesures complémentaires ciblant des aspects particuliers.

A. Approche globale : la stratégie de cybersécurité

En 2013, la Commission et la haute représentante de l'UE pour les affaires étrangères et la politique de sécurité ont présenté conjointement la Stratégie de cybersécurité de l'Union européenne. Cette stratégie visait à offrir un cyberespace ouvert, sûr et sécurisé à ses utilisateurs [14], tout en attribuant à cet égard un rôle important aux pouvoirs publics.

Quatre ans plus tard, le président de la Commission européenne, dans son discours sur l'état de l'Union prononcé en septembre 2017, diagnostiquait que malgré « d*es progrès dans la sécurisation de l'Internet [...] l'Europe reste mal équipée face aux cyberattaques* [15] », et appelait en conséquence à mieux protéger les Européen·ne·s à l'ère du numérique.

13 Commission européenne. Marché unique numérique - Supprimer les entraves pour exploiter pleinement les possibilités offertes par interne. Site Internet de la Commission européenne, en ligne (consulté le 16/02/2018). Disponible sur https://ec.europa.eu/commission/priorities/digital-single-market_fr.

14 Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé. Déjà cité.

15 JUNCKER, Jean-Claude. Discours sur l'état de l'Union 2017. Discours. Présidence, Commission européenne, Bruxelles, 13 septembre 2017, en ligne (consulté le 16/02/2018). Disponible sur http://europa.eu/rapid/press-release_SPEECH-17-3165_fr.htm.

Sur base de cet appel, la Commission européenne a présenté un nouveau paquet cybersécurité, actualisant et renforçant sa stratégie de 2013 dans trois secteurs clés :

- la consolidation de la **résilience** de l'UE face aux cyberattaques et le renforcement de sa capacité de réaction en matière de cybersécurité ;
- la **dissuasion** par la mise en œuvre d'une répression efficace par le droit pénal ;
- la **défense** par le renforcement de la stabilité à l'échelle mondiale grâce à la coopération internationale.

Dans cette perspective, la Commission a annoncé les mesures suivantes :

- le renforcement du mandat de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour la transformer en véritable Agence de l'UE pour la cybersécurité [16] ;
- l'instauration d'un système de certification de cybersécurité à l'échelle de l'UE ;
- la mise en place d'un plan d'action relatif aux modalités de réaction aux crises et incidents de grande ampleur en matière de cybersécurité ;
- la création d'un Centre européen de recherche et de compétences en matière de cybersécurité ;
- la mise en œuvre rapide de la directive européenne sur la sécurité des réseaux et des systèmes d'informations (ou directive NIS [17]).

Ces nouvelles mesures s'ajoutent aux **priorités et principes initiaux de la Stratégie de cybersécurité de l'UE** résumés dans notre tableau ci-dessous :

LES LIGNES DE FORCE DE LA STRATÉGIE DE CYBERSÉCURITÉ DE L'UNION EUROPÉENNE, EN RÉSUMÉ

5 PRIORITÉS STRATÉGIQUES	5 PRINCIPES DE CYBERSÉCURITÉ
• parvenir à la cyber-résilience ; • faire reculer considérablement la cybercriminalité ; • développer une politique et des moyens de cyberdéfense liés à la politique de sécurité et de défense commune (PSDC) ; • développer les ressources industrielles et technologiques en matière de cybersécurité ; • instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE.	• les valeurs essentielles de l'UE prévalent dans le monde virtuel autant que dans le monde réel ; • la protection des droits fondamentaux, de la liberté d'expression, des données personnelles et de la vie privée ; • l'accès pour tous ; • la gouvernance participative, démocratique et efficace ; • une responsabilité partagée pour assurer la sécurité.

16 Lire à ce propos page 32.
17 Nous revenons plus en détail sur la directive NIS ci-après en page 26.

B. Approches ciblées : textes et mesures complémentaires à la Stratégie de cybersécurité de l'UE

En avril 2015, la Commission européenne a communiqué son **programme de sécurité pour la période courant jusqu'en 2020** [18]. Le programme apporte notamment une réponse à l'inquiétude croissante des citoyen·ne·s européen·ne·s face au terrorisme. Le programme pose comme objectif de travailler mieux et plus étroitement entre États membres, en fonction de trois priorités dont la cybercriminalité. Parmi ses actions clés, il prévoit de renforcer les outils de lutte contre ce phénomène en s'attaquant « *aux obstacles à la conduite des enquêtes pénales en ligne, en résolvant notamment la question de la compétence territoriale et en arrêtant des règles pour l'accès aux preuves et aux informations sur l'Internet* ».

En mai 2015, la Commission européenne a lancé sa **Stratégie pour un marché unique numérique** [19] (ou Digital single market) qui vise à supprimer les obstacles pour exploiter pleinement les possibilités offertes par Internet. Les cybermenaces figurent au rang de ces obstacles.

Pour la Commission, il s'agit à ce niveau de défendre l'économie en ligne et, plus largement, la prospérité. Les objectifs clés fixés par la Commission sur ce plan sont :

- accroître les capacités et la coopération ;
- faire de l'Union européenne un acteur de poids ;
- intégrer la cybersécurité dans les politiques de l'UE.

Enfin, en juillet 2016, la Commission européenne a annoncé le lancement d'un **partenariat public-privé (PPP) axé sur la cybersécurité** [20], dans le cadre de la stratégie pour le marché unique numérique. L'UE investirait à ce titre 450 millions d'euros dans le PPP puisés dans le budget du programme pour la recherche et l'innovation Horizon 2020. Le secteur privé, représenté dans le PPP par l'Organisation européenne pour la cybersécurité (ECSO [21]) apporterait pour sa part une contribution trois fois plus élevée au PPP. Celui-ci devrait recruter ses membres parmi les centres de recherches, les universités ainsi que les administrations publiques nationales, régionales et locales. L'objectif du partenariat est de stimuler la coopération à un stade précoce du processus de recherche et d'innovation et de forger des solutions de cybersécurité applicables à différents secteurs tels que l'énergie, la santé, les transports et la finance. Les premiers appels à propositions ont été lancés dès la fin 2016.

18 Commission européenne. La Commission prend des mesures pour renforcer la coopération au sein de l'UE contre le terrorisme, la criminalité organisée et la cybercriminalité. Communiqué de presse. Communiqués de presse, Commission européenne, 28 avril 2015, Strasbourg, en ligne (consulté le 22/12/2017). Disponible sur http://europa.eu/rapid/press-release_IP-15-4865_fr.htm.

19 Commission européenne. Digital Single Market. Site Internet de la Commission européenne, en ligne (consulté le 16/02/2018). Disponible sur https://ec.europa.eu/digital-single-market.

20 Commission européenne. La Commission signe un accord avec le secteur de la cybersécurité et redouble d'efforts pour lutter contre les cybermenaces. Communiqué de presse. Communiqués de presse, Commission européenne, 5 juillet 2016, Bruxelles, en ligne (consulté le 22/12/2017). Disponible sur http://europa.eu/rapid/press-release_IP-16-2321_fr.htm.

21 Pour plus d'informations sur l'Organisation européenne pour la cybersécurité, consulter le site www.ecs-org.eu.

3.1.2. Le nouveau cadre réglementaire de l'Union européenne : directive NIS et règlement GDPR

Deux textes fondamentaux de l'UE [22] ont récemment établi un nouveau cadre en matière de sécurité de l'information et entretiennent de ce fait un lien étroit avec la cybersécurité :

A. la directive NIS du 6 juillet 2016 [23] (pour « Network and Information systems » ou SRI dans l'espace francophone : « sécurité des réseaux et de l'information »), toute première législation commune en matière de cybersécurité qui contribuera à préserver la sécurité des réseaux et des systèmes d'informations des États membres de l'UE ;

B. le règlement européen GDPR (pour « General Data Protection Regulation » aussi désigné, dans l'espace francophone, sous les initiales RGPD pour « Règlement général sur la protection des données ») qui unifie et amplifie la protection des données à caractère personnel et le respect de la vie privée notamment dans les communications électroniques avec comme objectif de rendre aux citoyen·ne·s la maîtrise de ces données.

Ces réglementations européennes concernent une très large communauté d'acteurs, des consommateur·rice·s aux fournisseurs de services en ligne, en passant aussi par les services publics [24].

A. La directive NIS, le cadre européen d'organisation de la sécurité des réseaux et des systèmes d'information

La directive européenne [25] NIS sur la sécurité des réseaux et des systèmes d'information crée le **cadre légal permettant aux États membres de hisser le niveau général de la cybersécurité dans l'UE.**

La directive NIS s'articule autour de 3 axes :

- stimuler la préparation des États membres par l'obligation de se doter des instruments adaptés, notamment une Computer security incident response team (ou CSIRT, c'est-à-dire une équipe de réponse aux incidents de sécurité informatique) et une autorité nationale compétente en matière de cybersécurité ;
- faire coopérer les États membres en créant un groupe de coopération et un réseau des CSIRT afin de faciliter cette coopération ;

22 Commission européenne. Marché unique numérique : bénéficier au mieux du numérique en Europe. Fact sheet. Infographie. News, Digital Market, Commission européenne, 24 février 2017, en ligne (consulté le 22/12/2017). Disponible sur https://ec.europa.eu/digital-single-market/en/news/digital-single-market-making-most-digital-opportunities-europe.
23 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. La directive est entrée en vigueur le 8 août 2016. Les États membres étaient tenus de la transposer dans leur ordre juridique avant le 9 mai 2018 au plus tard. Disponible sur http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148&qid=1497256687970.
24 Sur les obligations des services publics, lire en page 31 l'encadré « Se conformer aux règlementations : quelle aide au niveau du CIRB ? ».
25 Une directive est l'un des « *instruments juridiques dont disposent les institutions européennes pour mettre en œuvre les politiques de l'Union européenne (UE). Il s'agit d'un instrument flexible essentiellement utilisé pour harmoniser les législations nationales. Elle instaure une obligation de résultat mais laisse les pays de l'UE libres quant aux moyens à prendre pour y parvenir* ». Source : EUR-LEX, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Al14527.

- développer une culture de la sécurité au sein des secteurs vitaux pour l'économie et, plus encore, parmi les secteurs dont l'activité utilise intensivement les TIC, avec une obligation pour les entreprises des États membres considérées comme des opérateurs de services essentiels ainsi que les fournisseurs de services numériques de respecter des exigences en matière tant de sécurité face aux incidents que de notification des incidents les plus graves.

Plus en détail, on retient des définitions posées par la directive ainsi que des obligations qu'elle crée, par exemple que :

- la sécurité des réseaux et des systèmes d'information désigne la « *capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité, ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles* » ;
- les opérateurs de services essentiels (parmi lesquels se trouvent, le cas échéant, des entités publiques), prennent :
  - « *les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités* » ;
  - « *les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services* ».

LES SECTEURS D'INFRASTRUCTURES CRITIQUES SELON LA DIRECTIVE NIS

SECTEURS	SOUS-SECTEURS
Énergie	Électricité
	Pétrole
	Gaz
Transports	Transport aérien
	Transport ferroviaire
	Transport par voie d'eau
	Transport routier
Banques	
Infrastructures de marchés financiers	
Secteur de la santé	Établissements de soins de santé (y compris les hôpitaux et les cliniques privées)
Fourniture et distribution d'eau potable	
Infrastructures numériques	

La directive NIS en Belgique

AU NIVEAU FÉDÉRAL

Le **Centre pour la Cybersécurité Belgique (CCB)** [26] a reçu du Gouvernement fédéral la mission de préparer la législation transposant la directive NIS dans le droit national. Le CCB a dès lors élaboré un cadre général de transposition de la directive en Belgique, soumis le 30 mars 2018 au Conseil des ministres fédéral sous la forme d'un avant-projet de loi [27].

L'avant-projet de loi, approuvé par le Gouvernement fédéral et transmis pour avis au Conseil d'État, prévoit de désigner des « *autorités compétentes à plusieurs niveaux aves des rôles distincts* », à savoir une autorité nationale et des autorités sectorielles. Les autorités sectorielles auraient la charge d'identifier, pour leur secteur spécifique, les opérateurs de service essentiel (OSE) relevant de la directive NIS.

Dans ses travaux préliminaires [28], le CCB avait:

- défini la notion d'OSE comme suit : « *une entité qui fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques* », la fourniture de ce service étant « *tributaire des réseaux et des systèmes d'information* » et un incident dans ce cadre étant un événement qui « *aurait un effet disruptif important sur la fourniture dudit service* » ;
- proposé :
  - que le **secteur public** soit inclus dans la liste des OSE ;
  - d'avoir **recours à des autorités sectorielles** pour chaque secteur concerné, avec la charge pour ces autorités de collaborer avec le CCB pour identifier, déterminer des normes de sécurité et de contrôler des opérateurs de services essentiels ou des fournisseurs de services numériques ;
  - que le CCB consulte les autorités sectorielles désignées, les **autorités régionales et communautaires**, la Direction générale du Centre de crise du Service public fédéral Intérieur, en vue de déterminer des critères communs à tous les secteurs (transectoriels) permettant d'identifier des opérateurs de services essentiels, avec la possibilité pour chaque autorité sectorielle d'ajouter des critères propres à son secteur ;
  - qu'un socle commun et générique de mesures de sécurité des réseaux et systèmes d'information, basé sur des **standards internationaux et des règles spécifiques** acceptés comme telles dans le monde de la sécurité des technologies de l'information (ISO2700X et autres normes) ;
  - que des **contrôles des obligations des OSE** soit assurés par un organisme indépendant et que les autorités sectorielles pourraient également prononcer des demandes de mise en conformité dans un certain délai et/ou infliger des sanctions.

26 Sur le rôle et l'action du Centre pour la Cybersécurité Belgique, lire en page 34 la section 3.2.2. « Au niveau belge ».
27 Royaume de Belgique, SPF Chancellerie du Premier ministre. Cadre pour la sécurité des réseaux et des systèmes d'information pour la sécurité publique. Communiqué de presse. Conseil des ministres du 30 mars 2018, Presscenter.org, en ligne (consulté le 30/04/2018). Disponible sur http://www.presscenter.org/fr/pressrelease/20180330/cadre-pour-la-securite-des-reseaux-et-des-systemes-dinformation-pour-la-securi.
28 Royaume de Belgique, SPF Chancellerie du Premier ministre. Cadre général de transposition de la directive NIS en Belgique. Communiqué de presse. Conseil des ministres du 20 juillet 2017, Presscenter.org, en ligne (consulté le 16/02/2018). Disponible sur http://www.presscenter.org/fr/pressrelease/20170720/cadre-general-de-transposition-de-la-directive-nis-en-belgique.

La directive NIS en Belgique

AU NIVEAU DE LA RÉGION DE BRUXELLES-CAPITALE

La Région de Bruxelles-Capitale se doit de collaborer aux travaux de transposition de la directive NIS. Le CIRB et BPS constituent les acteurs clés à ce niveau, pour être les interlocuteurs régionaux du CCB. Les mesures présentées au chapitre 3 de ce Cahier s'inscrivent déjà dans cette logique [29].

B. Le règlement général sur la protection des données (ou règlement GDPR)

Le **règlement** [30] **européen GDPR** répond au vœu de l'UE d'établir un climat de confiance parmi les citoyen·ne·s européens à l'égard de l'utilisation qui est faite de leurs données personnelles, c'est-à-dire toutes les informations qui identifient une personne physique [31]. Il poursuit en cela une finalité économique : faciliter l'activité des entreprises dans le cadre du marché unique numérique. Cependant, le règlement se pose également en rempart contre les cyberattaques par les obligations qu'il crée en termes de collecte, de conservation ou de traitement des données.

Les évolutions des technologies justifiaient une réforme en profondeur d'une législation vieillissante, voire obsolète, face à un grand marché dont Internet a aboli les frontières. Sont concernées aussi bien la directive de 1995 relative à la protection des données pour garantir le droit à la vie privée que la décision-cadre de 2008 traitant cette problématique sous l'angle de la coopération policière et judiciaire.

Avec le règlement GDPR, l'UE dispose désormais d'un cadre légal uniforme selon le principe « un continent, une législation », avec des mesures applicables à tous les gestionnaires de données, quel que soit le lieu où ils sont implantés, y compris hors d'Europe. Entré en vigueur le 27 avril 2016, le règlement GDPR laissait aux parties concernées un délai de deux ans pour s'adapter à ses exigences. Cette période est arrivée à son terme le 25 mai 2018.

Les données personnelles et leur protection selon le GDPR

La définition des données personnelles reprise par le règlement GDPR est large. Sont concernées toutes les informations se rapportant à une personne physique identifiée ou identifiable en vie, incluant les informations relatives à l'état physique, physiologique, mental, les données génétiques, biométriques, médicales, économiques, culturelles et sociales. Les adresses IP, cookies ou encore tags RFID sont à inclure dans cette définition.

29 Lire pages 44 et suivantes.
30 Le règlement est un acte juridique de portée générale, obligatoire dans tous ses éléments et directement applicable dans tous les pays de l'Union européenne. Source : EUR-LEX, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM:l14522.
31 Le règlement GDPR englobe dans définition des données personnelles toutes les données se rapportant à une personne physique identifiée ou identifiable en vie, incluant les informations relatives à l'état physique, physiologique, mental, les données génétiques, biométriques, médicales, économiques, culturelles et sociales.

Concrètement, le règlement consacre les droits des citoyen·ne·s à différents niveaux intéressant la cybersécurité :

- la **protection des données par défaut et dès la conception** (ou « privacy by default » et « privacy by design ») constitue un principe général du règlement et garantit respectivement que :
  - tout service utilisant des données personnelles leur applique d'emblée le niveau de protection le plus élevé ;
  - la législation s'applique de manière préventive et proactive à toute nouvelle technologie ;
- l'**obligation d'informer** le·la citoyen·ne et les autorités, dans les meilleurs délais, lorsque des données sont accidentellement ou illégalement détruites, perdues, altérées, consultées par des personnes non autorisées ou divulguées à de telles personnes et lorsque les droits des personnes sont menacés ;
- des **limitations étroites en termes de collecte, de traitement et de conservation des données** réduisent de facto les risques :
  - les données à caractère personnel sont collectées pour une finalité légitime et spécifique et ne peuvent pas être utilisées à d'autres fins ;
  - seules les données nécessaires aux fins prévues peuvent être collectées ;
  - les données à caractère personnel ne peuvent pas être conservées plus longtemps que le temps nécessaire pour répondre à l'objectif visé ;
  - les données à caractère personnel doivent être protégées contre tout accès non autorisé, perte ou destruction.

La cybersécurité, en particulier la détection des cybermenaces et la réponse à celles-ci en termes de cyber-résilience, s'inscrivent en filigrane du règlement GDPR. L'obligation d'informer le·la citoyen·ne et les autorités en cas de violation des données fait le lien avec les cybermenaces. À ce niveau, les obligations des détenteurs de données ne s'arrêtent pas aux dispositions énumérées ci-dessus. Le règlement définit également le principe de responsabilité (ou « accountability »), à savoir que l'entité responsable des données doit :

- mettre en place des mesures de protection des données contre tout accès non autorisé, perte ou destruction ;
- pouvoir démontrer qu'elle agit en conformité avec le règlement GDPR.

Autrement dit, ce sont bien des obligations en termes de cyber-résilience qui sont ainsi formulées par le règlement GDPR.

Se conformer aux règlementations : quelle aide au niveau du CIRB ?

Au même titre que d'autres législations, tant la directive NIS que le règlement GDPR ont un impact, direct ou indirect, sur l'organisation des services publics. C'est pourquoi le CIRB propose aux administrations et organismes publics une palette de services en vue de les assister dans la mise en conformité avec ces législations.

- **NIS et sécurité de l'information (IS)** : sans attendre que soit déterminés le champ d'application de la directive NIS et, notamment, quelles organisations seront identifiées comme OSE, les services publics doivent se soumettre à diverses obligations ou bonnes pratiques en matière d'IS.

  Depuis 2010, le CIRB s'est doté d'un service dédié à l'IS et à la mise en conformité aux prescrits légaux, notamment en matière de protection des données à caractère personnel. **Les clients du CIRB peuvent faire appel à l'expertise de cette équipe dans le cadre de missions d'Information Security as a Service (ISaaS).**

  Le service ISaaS englobe une large variété de prestations, comme des conseils en matière d'IS, l'analyse de la politique IS de l'organisation, le suivi et la mise en place d'un plan de mesures dans ce cadre, l'analyse continue de la politique IS selon un processus d'amélioration continue (plan – do – check – act) assortie de recommandations et de propositions d'amélioration.

  Les analyses IS du CIRB se basent sur le cadre de référence des normes ISO 27001 et suivantes et se combinent à des analyses de risques. En l'absence d'un plan de sécurité formel, le service ISaaS peut débuter par une analyse de la sécurité et des risques liés à l'information auprès de son client, avec l'objectif de remédier à cette carence.

  Les personnes intervenant dans le cadre ISaaS sont enfin compétentes pour remplir les fonctions de **conseiller en sécurité de l'information (CSI)** externe si le client ne souhaite pas confier ce rôle à une ressource interne. En conformité avec l'arrêté royal du 17 mars 2013 [32], le CSI s'assure que l'organisation accorde l'attention nécessaire à la sécurité de l'information via des mesures structurelles, organisationnelles, physiques et techniques.

- **GDPR** : les organisations publiques sont concernées par l'application du GDPR. C'est pourquoi le CIRB a lancé, dès le printemps 2017, une campagne de sensibilisation à la **mise en conformité vis-à-vis du GDPR** par les instances publiques, en parallèle au lancement d'une offre de services dédiée à cette mise en conformité.

  L'offre de services GDPR du CIRB met l'accent sur l'aspect transversal du GDPR (ses implications dépassent de loin les seuls processus informatiques). Elle se décline en quatre niveaux de services :

1. La formation : depuis la session d'information sur les enjeux du GDPR dédiée aux responsables des partenaires du CIRB jusqu'à la formation approfondie de plusieurs jours englobant tous les éléments juridiques et techniques en passant par la sensibilisation du personnel au respect du GDPR au quotidien ;

32 Royaume de Belgique, SPF Technologie de l'Information et de la Communication. Arrêté royal relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral - 17 mars 2013. Moniteur belge, 183e année, n° 89, 22 mars 2013, Bruxelles, en ligne (consulté le 16/02/2018). Disponible sur http://www.ejustice.just.fgov.be/mopdf/2013/03/22_1.pdf#Page6.

2. L'évaluation préalable dont le but est d'effectuer un diagnostic de la maturité de l'organisation du partenaire du CIRB en identifiant les principaux types de traitements de données personnelles ainsi que les problèmes clés de non-respect du GDPR, et se conclut par un rapport identifiant les principales zones de risque et un premier plan d'actions de haut niveau en vue de la mise en conformité au GDPR ;

3. L'accompagnement à la mise en conformité via un chef de projet formé au GDPR, secondé par une équipe spécialisée dans le rôle de Data Protection Officer, GDPRafin d'assurer que les éléments de non-respect du GDPR soient priorisés et traités ;

4. Le Data Protection Officer (DPO) « as a service » [33] : le CIRB peut jouer le rôle de DPO pour ses partenaires et en porter toutes les responsabilités en matière d'information et de coaching, conseil, de formation, de vérification du respect du GDPR ainsi que de point de contact avec les autorités de contrôle. Ce rôle de DPO est en effet un rôle obligatoire pour chaque administration. Les DPO du CIRB travaillent au sein d'une équipe pluridisciplinaire en collaboration avec des juristes, des experts de la sécurité de l'information et des experts informatiques. Ils bénéficient d'outils et d'une expérience déclinables d'une organisation à l'autre parmi les différents partenaires du CIRB.

À ce jour, plusieurs administrations régionales et locales ont déjà bénéficié des sessions de sensibilisation et de formation en matière de GDPR. Des évaluations préalables sont également en cours.

En savoir plus : le CIRB a publié une brochure « Règlement général sur la protection des données (RGPD) - Guide pratique à l'attention des institutions locales et régionales de la Région de Bruxelles-Capitale », à télécharger sur son site [34].

3.2. Les acteurs clés de la cybersécurité :

3.2.1. Au niveau européen :

Différents acteurs interviennent à l'échelon européen en matière de cybersécurité au bénéfice des Etats membres de l'UE. Il s'agit :

- de l'European Network and Information Security Agency (ENISA) ;
- du réseau des centres nationaux de réponse aux incidents de sécurité informatique (réseau CSIRT) ;
- du Centre européen de lutte contre la cybercriminalité (EC3).

Par ailleurs, l'Union européenne dispose d'une CERT interne (CERT-EU) qui vient en aide aux différentes institutions européennes en cas de cyberattaque de manière à protéger l'intégrité de infrastructures informatiques.

33 Pour plus d'informations, consultez la page http://cirb.brussels/fr/quoi-de-neuf/actualites/reglement-europeen-relatif-a-la-protection-des-donnees-a-caractere-personnel-gdpr.
34 Pour en savoir plus sur l'application du RGPD par les pouvoirs publics, consulter la brochure du CIRB, Règlement général sur la protection des données (GDPR) - Guide pratique à l'attention des institutions locales et régionales de la Région de Bruxelles-Capitale. Disponible sur : http://cirb.brussels/guide-gdpr.

L'ENISA, future Agence de l'Union européenne pour la cybersécurité

En septembre 2017, la Commission européenne a annoncé sa volonté de créer une véritable Agence de l'Union européenne pour la cybersécurité, en élargissant les statuts et les missions de l'European Network and Information Security Agency (ou ENISA en abrégé) fondée en 2004.

Présentée comme l'une des mesures du paquet cybersécurité [35] de la Commission européenne, la création de cette future Agence pour la cybersécurité doit permettre à l'UE de prendre une part plus active dans la lutte contre les cybermenaces. Le mandat de l'ENISA s'est en effet avéré trop restreint, face notamment à l'évolution des besoins en cybersécurité, en particulier dans la lutte contre les cyberattaques massives.

L'ENISA a jusqu'à présent apporté « *son soutien aux institutions européennes, aux États membres et aux entreprises en traitant les problèmes de sécurité des réseaux et de l'information, en y réagissant et, surtout, en les prévenant* » [36]. En pratique, elle a essentiellement joué un rôle d'expert et de facilitateur développant une culture de la sécurité des réseaux d'information dans toute l'Union, en mettant en commun les bonnes pratiques ainsi qu'en mettant en relation les parties prenantes. C'est ainsi que, chaque année, l'ENISA publie son rapport « ENISA Threat Landscape » qui fait le point sur les principales cybermenaces dans l'espace européen.

Le **périmètre d'action de la future Agence pour la cybersécurité** en ferait le « *point de référence dans l'écosystème de cybersécurité de l'UE, œuvrant en étroite coopération avec tous les autres organismes compétents dudit écosystème* ». La Commission européenne fait à nouveau le constat que « *pour accroître la cyber-résilience collective de l'Union, les actions individuelles des États membres de l'UE et une approche parcellaire de la cybersécurité ne [sont] pas suffisantes* » [37] .

Parmi les nouveaux domaines d'actions de la future Agence pour la cybersécurité, citons en particulier :

- l'élaboration et la mise en œuvre de la politique de l'UE, dont le réexamen de la stratégie de cybersécurité de l'UE ;
- la réponse aux crises de cybersécurité via la coopération entre les États membres ;
- le soutien à la directive NIS ;
- le soutien au marché de la cybersécurité par l'harmonisation des certifications nationales de produits et services de sécurité en matière de TIC ;
- le perfectionnement des moyens et des compétences dont disposent les autorités publiques nationales et de l'UE en termes de réponses aux incidents et de réglementation ;
- le partage des connaissances et informations ainsi que la sensibilisation en coordination avec les autorités des États membres ;
- la fixation des priorités de recherche et développement, y compris dans le cadre du partenariat public-privé contractuel sur la cybersécurité.

35 Lire plus haut, page 23
36 Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité. Déjà cité.
37 Proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité. Déjà cité.

Le Réseau CSIRT

Créé en vertu de la directive NIS, le réseau CSIRT répond au vœu de la Commission européenne d'établir un cadre de coopération volontaire entre Etats membres de l'UE. Le réseau a pour objectif de faciliter le partage d'informations techniques sur les risques et les vulnérabilités. Il doit, pour cela, bénéficier de la coopération effective, efficace et sécurisée des CSIRT nationaux de tous les États membres de l'UE.

La cyberattaque WannaCry en mai 2017 a constitué le premier incident à l'occasion duquel le réseau a été activé, avec cependant peu d'efficacité comme l'a analysé la Commission remarquant que « *cet incident a démontré que le système n'était pas encore pleinement opérationnel* » [38].

Le Centre EC3

Le Centre européen de lutte contre la cybercriminalité (European Cybercrime Centre - EC3) a été créé en 2013 au sein d'Europol, l'agence européenne spécialisée dans la répression de la criminalité. La cybercriminalité fait en effet partie des neuf thématiques prioritaires d'Europol (aux côtés de la lutte contre le trafic de drogues ou de la traite des êtres humains).

L'EC3 a pour mission d'apporter son renfort à la réponse policière à la cybercriminalité dans l'Union européenne. Le Centre doit permettre aux États membres et aux institutions de l'UE de développer des moyens opérationnels et d'analyse aux fins des enquêtes et de la coopération avec les partenaires internationaux [39].

3.2.2. Au niveau belge :

En Belgique, différentes organisations officielles prennent en charge les questions de cybersécurité en fonction de compétences ou de niveaux d'action spécifiques pour chacune d'entre elles.

Il s'agit :

- du Centre pour la Cybersécurité Belgique (CCB) ;
- de la Cyber emergency team fédérale (CERT.be) ;
- de la Federal Computer Crime Unit (CFFU) et des cinq Regional Computer Crime Units (RCCU) au sein de la Police fédérale belge.

En outre, la Cyber Security Coalition est une plateforme de collaboration entre acteurs publics, privés et académiques en vue de promouvoir dans notre pays la cybersécurité et les bonnes pratiques dans ce domaine.

38 Commission européenne. Union de la sécurité : la Commission prend de nouvelles mesures pour prévenir la radicalisation et les cybermenaces. Communiqué de presse. Communiqués de presse, Commission européenne, 29 juin 2017, Bruxelles, en ligne (consulté le 22/12/2017). Disponible sur http://europa.eu/rapid/press-release_IP-17-1789_fr.htm. + Commission européenne. Huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective. Communication de la Commission au Parlement européen, au Conseil européen et au Conseil. 29 juin 2017, Bruxelles, en ligne (consulté le 22/12/2017). Disponible sur http://ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-354-F1-FR-MAIN-PART-1.PDF.

39 Commission européenne. La stratégie de sécurité intérieure de l'UE en action. Communication de la Commission au Parlement européen et au Conseil. 22 novembre 2010, Bruxelles, en ligne (consulté le 22/12/2017). Disponible sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:FR:PDF.

Le Centre pour la Cybersécurité Belgique

En 2015, la Belgique s'est dotée d'un nouvel organe, le Centre pour la Cybersécurité Belgique (CCB) [40], placé sous l'autorité du Premier ministre.

Le CCB, au titre d'autorité nationale, a pour mission de :

- superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité ;
- gérer par une approche intégrée et centralisée les différents projets en la matière ;
- assurer la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique ;
- formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité ;
- assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du Gouvernement fédéral ;
- élaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics ;
- coordonner la représentation belge dans les forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière ;
- coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication ;
- informer et sensibiliser les utilisateurs des systèmes d'information et de communication.

En ce qui relève de la gestion de crise en cas de cyberincidents, le CCB est l'auteur du **Cyberplan national d'urgence** belge qui vise à « *prévoir une structure de réponse aux crises et incidents dans le domaine de la cybersécurité qui exigent une coordination et/ou une gestion à l'échelon national* ». Ce plan crée le mécanisme « *d'escalade de base permettant aux différents services actifs dans le cyberdomaine de coordonner leurs actions afin de faire face aux cyberincidents au niveau national. L'accent est nettement placé sur l'échange rapide et correct d'informations entre les services* ».

De manière pratique, le CCB est devenu en janvier 2017 le gestionnaire de la **cyber emergency team fédérale** (ou CERT.be) en vertu de son rôle de coordination en matière de cybersécurité en Belgique (lire ci-après).

Le CCB a lancé divers projets afin de renforcer la cybersécurité dans les secteurs vitaux de la Belgique. Ces secteurs, qui revêtent une importance cruciale pour la sécurité de la population belge, ont été identifiés dans la ligne de directive NIS : l'énergie, la mobilité, les télécoms, la finance, l'eau potable, la santé publique, le gouvernement. Ces secteurs vitaux ont accès, par le biais d'une plateforme partagée, aux avertissements filtrés faisant état d'intrusions ou de cybermenaces. Ils reçoivent de cette manière des informations d'une source fiable leur permettant de rapidement adopter les mesures nécessaires pour contrer ces attaques.

40 Le CCB (www.ccb.belgium.be) a été créé en vertu de l'arrêté royal du 10/10/2014.

L'action du CCB est donc large et s'étend au-delà du niveau fédéral.

Le présent plan régional de cybersécurité, en particulier, se place dans cette sphère d'influence. Il est essentiel pour la Région bruxelloise d'y être pleinement associée, d'en coordonner et en assurer la diffusion.

La Cyber emergency team fédérale, CERT.be

Créée en 2009, la Cyber emergency team fédérale (ou CERT.be, www.cert.be) a la charge de coordonner la gestion et la réponse aux incidents et crises d'ampleur nationale auprès d'opérateurs d'infrastructures critiques ou de services essentiels.

Les rôles de la CERT.be sont de :

- rassembler et fournir des informations sur les incidents de sécurité ;
- apporter un soutien en cas d'incident ;
- coordonner la gestion d'incidents à grande échelle ;
- contribuer à la mise en place des activités de CERT au sein des entreprises ;
- partager des données et connaissances par le biais de publications et des événements.

En pratique, la CERT.be sert de point de contact central aux entreprises et organisations gouvernementales belges pour leurs problèmes liés à la cybersécurité. Ces entreprises et organisations peuvent s'adresser à la CERT.be pour signaler un cyberincident et/ou demander conseil sur la cybersécurité.

La Federal Computer Crime Unit et les Regional Computer Crime Units de la Police fédérale belge

La Federal Computer Crime Unit (FCCU [41]) est l'unité de la Police fédérale en charge de la lutte contre la criminalité dans le domaine des TIC. La FCCU assure notamment la protection du·de la citoyen·ne dans le cadre des nouvelles formes de criminalité dans la société virtuelle. Elle traite les cas de cybercriminalité passibles de poursuites judiciaires, par exemple les dossiers de pédophilie et de fraudes (ventes frauduleuses) sur l'Internet ainsi que des fraudes via les télécoms.

Les Regional Computer Crime Units (RCCU) sont actives au niveau des ressorts de cour d'appel du pays [42], donc en ce compris l'arrondissement judiciaire de Bruxelles. Outre la recherche des infractions liées à la criminalité sur Internet et l'identification de leurs auteurs, les RCCU effectuent également des analyses technico-légales de systèmes informatiques (PC, autres supports de données et petits réseaux).

41 Pour plus d'informations sur la Federal Computer Crime Unit, consulter le site http://www.police.be/fed/fr/a-propos/directions-centrales/federal-computer-crime-unit.
42 Anvers, Bruxelles, Gand, Liège et Mons.

La Cyber Security Coalition

L'asbl Cyber Security Coalition (www.cybersecuritycoalition.be) est une initiative commune du secteur académique, des autorités publiques et du secteur privé. Rassemblant plus de 50 acteurs clés de ces trois univers, la Coalition unit les efforts respectifs de ses membres pour renforcer la cybersécurité au niveau national. Le CIRB en est un membre actif.

Ce réseau d'experts agit selon quatre axes stratégiques :

- le partage d'expérience ;
- la collaboration opérationnelle ;
- les recommandations politiques ;
- des campagnes de sensibilisation.

En 2015, la Cyber Security Coalition a publié le Guide de gestion des incidents [43] pour aider les organisations de tous ordres à trouver la réponse à cette question : « *Votre organisation sait-elle gérer un incident de cybersécurité ?* ». On peut y lire un ensemble d'informations pertinentes et pratiques pour aider les organisations à détecter et à résoudre les incidents de cybersécurité.

La Cyber Security Coalition a par ailleurs co-initié avec le CCB la campagne « Récupérons Internet » via le site www.safeonweb.be. La campagne part du constat que 68 % de la population belge ne dispose pas d'une protection en ligne suffisante et, par conséquent, facilite la tâche des criminels. Elle encourage donc le grand public à sécuriser ses appareils par l'installation d'utilitaires de détection de virus, par la sauvegarde des données et la mise à jour des logiciels. Plus de 6,5 millions de visiteurs ont déjà effectué via ce site un test pour évaluer leur niveau de protection.

3.2.3. Au niveau de la Région de Bruxelles-Capitale :

En Région de Bruxelles-Capitale, le Centre d'Informatique pour la Région Bruxellois (CIRB) et Bruxelles Prévention & Sécurité (BPS) couvrent déjà, par la nature de leurs missions et activités, différentes facettes de la cybersécurité à l'échelle de la Région.

Ces deux administrations partenaires entendent agir notamment sur deux aspects stratégiques :

- le développement d'une culture globale de réflexion en matière de sécurité de l'information ;
- la sensibilisation des partenaires actifs sur le territoire régional.

LE CENTRE D'INFORMATIQUE POUR LA RÉGION BRUXELLOISE ET BRUXELLES PRÉVENTION & SÉCURITÉ COUVRENT DÉJÀ DIFFÉRENTES FACETTES DE LA CYBERSÉCURITÉ

Le CIRB et BPS entretiennent des liens étroits, au travers de multiples partenariats et projets concrets tels que le centre de communication régional, le centre de crise régional, la plateforme régionale de vidéoprotection ou encore la mise en place du réseau de caméras ANPR [44]. Le CIRB est par ailleurs le partenaire IT de BPS dans le cadre de ses besoins informatiques journaliers.

43 Cyber Security Coalition. Cybersécurité - Guide de gestion des incidents. En ligne (consulté le 22/12/2017). Disponible sur www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FR.pdf.
44 « Automatic number-plate recognition » ou reconnaissance automatique des plaques minéralogiques.

Le Centre d'Informatique pour la Région Bruxelloise

Le Centre d'Informatique pour la Région Bruxelloise (CIRB) [45] est le partenaire technologiquement neutre, compétitif, fiable et de qualité de toute institution publique sur le territoire de la Région bruxelloise, et qui entend en connaissance de cause et de manière proactive, introduire des TIC novatrices et cohérentes afin de maximiser d'une part, l'efficacité de son fonctionnement et d'autre part, la convivialité des services aux Bruxelloi·se·s, aux entreprises et aux visiteurs.

Dans ce cadre, le CIRB a rassemblé l'ensemble des pouvoirs locaux et régionaux autour de projets assurant leur développement numérique. La mutualisation constitue le trait commun à toute activité du CIRB et son fer de lance, qu'il décline à travers quatre axes : les infrastructures, les plateformes et services IT, les données et les ressources humaines IT.

Le CIRB assure en outre la cohérence des organes mis en place pour gérer la politique IT en Région de Bruxelles-Capitale. Il est chargé de délivrer une contribution permanente, efficace et cohérente à la préparation des politiques, notamment par :

- un rôle d'autorité et d'influence destinées à favoriser la transition numérique par l'évolution des méthodes de travail des institutions publiques ;
- un rôle de promotion et de vitrine des TIC ;
- un rôle de vigie qui implique une connaissance approfondie et une observation permanente de l'évolution des TIC, y compris en comparaison avec les autres entités fédérées et l'Union européenne.

Depuis sa création, le CIRB est un acteur majeur de la sécurité informatique. Il a une vocation naturelle à s'approprier les questions de sécurité de l'information et de cybersécurité, tant pour ses propres besoins que pour ceux des organisations qui utilisent ses services.

En termes de sécurité de l'information, le CIRB s'appuie en premier sur le Data Center Régional (DCR) et sur le réseau IRISnet. Pilier de la gouvernance IT des pouvoirs publics bruxellois, le DCR leur permet de conserver la maîtrise et la gestion de leurs données critiques et sensibles. Le DCR regroupe ainsi les équipements informatiques et les serveurs qui permettent de stocker, de traiter et de protéger les données de la grande majorité des institutions et du secteur publics bruxellois, aux niveaux local et régional. Le DCR héberge des services centraux dans le déploiement de la stratégie de smart city régionale, comme IRISbox, l'intégrateur de services Fidus ou encore la plateforme régionale de vidéoprotection servant de support aux services de sécurité et à la Low Emission Zone. Dans son rôle de responsable de la sécurité informatique du DCR, le CIRB est en contact avec le CCB qui l'informe des nouvelles menaces en cas d'alertes.

En outre, les clients du CIRB peuvent s'appuyer sur son expertise dans la résolution des incidents de sécurité. Celle-ci complète l'offre du CIRB axée sur les outils traditionnels (firewall, backup, virtual private network) qui assurent la protection des systèmes, des données et contribuent à préserver les investissements informatiques.

45 Le CIRB a été créé par la loi du 21 août 1987, modifiée par l'ordonnance du 20 mai 1999 portant sur sa réorganisation ainsi que par l'ordonnance du 29 mars 2001. L'ordonnance du 8 mai 2014 le consacre comme intégrateur de services régional.

Enfin, le CIRB joue à ce niveau un rôle de conseiller et de fournisseur de services en aidant les organisations publiques bruxelloises à se conformer aux standards et réglementations touchant directement ou indirectement les questions de sécurité de l'information.

Bruxelles Prévention & Sécurité (BPS)

La sixième réforme de l'État a redessiné l'architecture de la sécurité en Région bruxelloise. Sans toucher aux compétences et aux prérogatives des différents niveaux de pouvoir (fédéral ou local), la réforme a principalement eu pour conséquence de confier d'importantes responsabilités en matière de prévention et de sécurité à la Région bruxelloise.

Ainsi, la fonction de Gouverneur en Région de Bruxelles-Capitale a été supprimée. En conséquence, deux autorités régionales détiennent depuis 2014 des compétences dans le domaine de la sécurité :

- le·la Ministre-Président·e bruxellois·e qui « *exerce les compétences en ce qui concerne le maintien de l'ordre public* » ;
- le·la Haut·e Fonctionnaire, qui est compétent·e « *pour les missions du Gouverneur relatives à la sécurité civile et pour l'élaboration des plans relatifs aux situations d'urgence sur le territoire de Bruxelles-Capitale* ».

Les nouvelles missions de l'agglomération bruxelloise découlant de la sixième réforme sont les suivantes [46] :

- la coordination des politiques de sécurité, en ce compris l'observation et l'enregistrement de la criminalité ;
- la coordination des politiques de prévention ;
- l'élaboration d'un plan régional de sécurité.

Afin d'exécuter ces missions, le Gouvernement de la Région de Bruxelles-Capitale a décidé, dans son accord 2014-2019 [47], de mettre en place un nouvel organisme d'intérêt public (OIP) dénommé Bruxelles Prévention & Sécurité (BPS) [48].

BPS doit permettre l'organisation d'une gestion administrative centralisée et transversale de la sécurité à Bruxelles, de même que le développement d'une politique régionale en matière de sécurité s'appuyant tant sur les compétences fédérales déconcentrées que sur les compétences régionales.

46 Royaume de Belgique, SPF Chancellerie du Premier ministre. Loi relative à la Sixième Réforme de l'Etat concernant les matières visées à l'article 77 de la Constitution – 6 janvier 2014 - Modification de la loi du 26 juillet 1971 organisant les agglomérations et les fédérations de communes (Titre chapitre 2). Moniteur belge, 184e année, n° 32, 31 janvier 2014, Bruxelles, page 8720, en ligne (consulté le 16/02/2018). Disponible sur http://www.ejustice.just.fgov.be/mopdf/2014/01/31_1.pdf. L'article 14 énumère les missions de l'agglomération bruxelloise. En plus de celles mentionnées ci-dessus, l'agglomération « *exerce les compétences visées aux articles 128 et 129 de la loi provinciale, ainsi que les compétences qui, dans des lois particulières, sont attribuées au Gouverneur de province, sauf si ces lois particulières en disposent autrement* », « *exerce la tutelle sur les budgets des zones de police* », « *encourage la mutualisation de services administratifs des zones de police ainsi que le recours par celles-ci à la centrale d'achat pour l'acquisition de matériel* » et « *propose un texte d'harmonisation des règlements de police, dans le respect des spécificités communales* ».

47 Région de Bruxelles-Capitale. Gouvernement. Accord de gouvernement bruxellois 2014-2019. Chapitre 3 – Une politique qui garantit la qualité de vie dans tous les quartiers. § III – Mettre en place une politique de sécurité régionale (p. 60). En ligne (consulté le 16/02/2018). Disponible sur http://be.brussels/files-fr/a-propos-de-la-region/competences-regionales/accord-de-gouvernement-2014-2019.

48 Bruxelles Prévention & Sécurité a été créé par l'ordonnance du 28 mai 2015 publiée au Moniteur belge du 10/06/2015.

BPS joue un rôle central dans la coordination des différents opérateurs de la chaîne de prévention et de sécurité à l'échelle de la Région. Il en assure la cohérence et la complémentarité en les mettant en relation dans des domaines d'action comme :

- la gestion civile de crise (zones de police et services de sécurité civile) ;
- le soutien à la formation policière (Actiris, VDAB, Bruxelles Formation) ;
- la vidéoprotection (zones de police, STIB, Mobiris, CIRB).

Les politiques de BPS visent tout à la fois la prévention et la prise en charge des questions de sécurité dans un large spectre de matières, au niveau de l'aménagement du territoire, de la mobilité et de toute autre compétence ayant un impact sur la sécurité et sur le sentiment de sécurité en Région bruxelloise.

En tant qu'organisme centralisant les matières concernées, BPS a été chargé de la rédaction du Plan global de sécurité et de prévention (PGSP) [49] et assure la coordination de sa mise en œuvre en rendant compte des mesures exécutées aux autorités compétentes. Le PGSP s'articule autour de dix thématiques de travail, dont la cybercriminalité.

De manière générale, les mesures qui ont trait à la cybercriminalité portent sur :

- la cyberhaine (M 1.2 du PGSP) ;
- la sensibilisation aux risques liés aux TIC (M 8.11, M 8.12, M 8.13) ;
- les capacités de recherche sur le Darknet (M 8.14) ;
- l'élaboration d'une image des cybermenaces et cyberincidents (M 8.15) ;
- l'instauration, en matière de gestion de crise et de résilience, d'un groupe de veille technologique afin d'apporter une plus-value en termes d'innovation technique et technologique (M 10.13).

BPS, de par son positionnement et l'élaboration du plan qui lui a été confiée, a entamé des changements en matière de coordination et de centralisation de la gestion de la politique de sécurité au sens large.w

D'autre part, BPS souhaite contribuer au développement des nouvelles technologies qui sont un levier important pour améliorer non seulement le quotidien des habitant·e·s en ville (accessibilité et disponibilité du réseau wifi, guichet électronique pour les démarches administratives, éclairage public intelligent…) mais aussi leur sécurité. Faire de la Région de Bruxelles-Capitale une smart city est une priorité. Le développement d'une recherche novatrice en ces matières est encouragé par le Plan Global de Sécurité et de Prévention, une réflexion est menée avec les différents partenaires de la chaine de sécurité pour qu'un outil adapté de partage d'informations soit créé. La mise en place d'une gestion informatique commune aux six zones de police, équipée de nouveau matériel technologique comme le système de vidéoconférence entre les différents partenaires, par le biais d'un partenariat entre BPS, le CIRB et les communes est en cours. Le déploiement du réseau ANPR (Automatic Nummer Plate Recognition) et de la Low Emission Zone sur le territoire de notre Région, est un autre projet nécessitant l'utilisation de nouvelles technologies, suivi par BPS et le CIRB.

49 Région de Bruxelles-Capitale, Bruxelles Prévention & Sécurité. Plan global de sécurité et de prévention. En ligne (consulté le 16/02/2018). Disponible sur http://www.veiligheid-securite.brussels/fr/plan.

L'instauration d'un groupe de veille technologique figure également dans les projets de BPS. Ce projet sera réalisé en collaboration du RCCU de la Police judiciaire de Bruxelles et sera composé de spécialistes chargés d'identifier les innovations techniques et technologiques susceptibles d'apporter une plus-value en matière de gestion de crise et de résilience.

Enfin, afin d'optimaliser l'utilisation de ces nouveaux outils et de pouvoir faire face aux formes de criminalité et d'insécurité qui évoluent en permanence, il est essentiel de pouvoir renforcer la formation en ces matières. L'École régionale des métiers de la sécurité en tiendra compte dans son offre de formation dans un objectif de professionnalisation des acteur·rice·s de la prévention et de la sécurité, mais également de décloisonnement des différentes approches (partage de bonnes pratiques, échanges de processus etc.). Elle veillera aussi à renforcer le transfert des savoir et pratiques entre acteur·rice·s et à optimiser la connaissance des réalités bruxelloises. Enfin, l'École appuiera les synergies avec le monde de l'enseignement, les services publics de formation professionnelle et leurs partenaires afin d'approfondir la spécialisation des différents acteur·rice·s mais aussi de susciter des vocations aux métiers de la sécurité auprès des candidat·e·s bruxellois·e·s.

4. LE CADRE MÉTHODOLOGIQUE EXISTANT EN MATIÈRE DE CYBERSÉCURITÉ

Les organisation qui cherchent à contrer les risques et les menaces en cybersécurité peuvent s'appuyer sur différents cadres méthodologiques afin de baliser les mesures techniques et managériales nécessaires à cette fin. Il s'agit notamment :

- du Cybersecurity Framework du National Institute of Standards and Technology aux États-Unis ;
- des normes 2700x de l'Organisation internationale de normalisation (ISO).

4.1. Cybersecurity Framework

Le **Cybersecurity Framework (CSF)** [50] du National Institute of Standards and Technology (NIST) est un cadre méthodologique permettant aux entreprises d'aborder et traiter les risques de cyberattaques visant leurs infrastructures stratégiques, ainsi que de pouvoir échanger leurs bonnes pratiques sur la base d'un vocabulaire commun. C'est l'un des modèles les plus avancés au niveau pratique et, à ce titre, une référence mondiale en la matière.

Le CSF tire son origine d'une série d'attaques informatiques majeures ayant touché en 2013 des grandes entreprises, des médias et des réseaux sociaux ainsi que des organismes publics des États-Unis. Ces incidents avaient à l'époque sensibilisé la Maison-Blanche aux risques de défaillance des infrastructures du pays vitales pour le bon fonctionnement de son économie.

50 United States of America government, Department of Commerce, National Institute of Standards and Technology. Cybersecurity framework. NIST, en ligne (consulté le 16/02/2018). Disponible sur https://www.nist.gov/cyberframework.

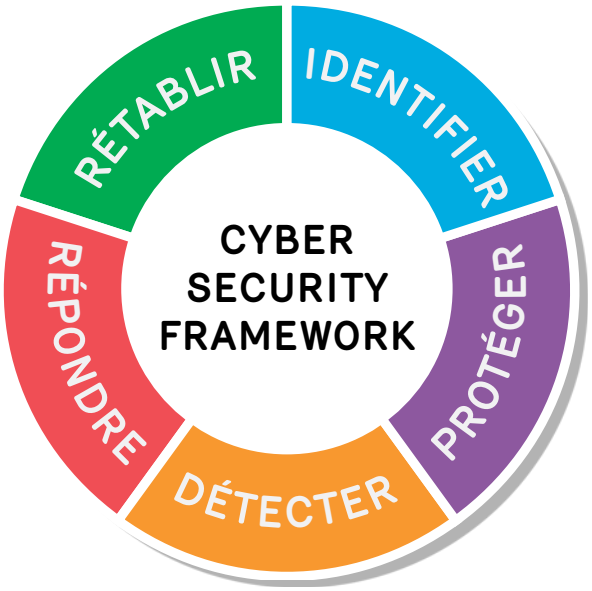
Depuis sa création en 2014, le CSF a été salué par le bureau de consultance PriceWaterhouseCooper comme « *un point charnière dans l'évolution de la cybersécurité, l'équilibre passant d'une conformité réactive à des normes proactives de gestion des risques* » [51]. Le bureau Gartner prévoit, pour sa part, que la moitié des organisations publiques et privées utiliseront le CSF d'ici à 2020 [52].

Les cinq fonctions fondamentales d'un plan de cybersécurité

Le CSF se différencie par sa vue globale de la problématique ainsi que par ses liens vers les autres normes et références. Il permet en effet à un gestionnaire ou à un technicien de puiser auprès de différentes sources tous les détails techniques nécessaires à la mise en place des mesures recommandées.

Révisé en 2017, le CSF définit les cinq fonctions fondamentales d'un plan de cybersécurité : identifier, protéger, détecter, répondre et rétablir.

- **Identifier** : développer la compréhension du point de vue organisationnel en vue de gérer la cybersécurité en termes de systèmes, ressources, données et capacités.
- **Protéger** : concevoir et déployer les mesures de protection adaptées pour assurer la continuité des services délivrés par des infrastructures critiques.
- **Détecter** : concevoir et déployer les actions adaptées pour détecter, lorsqu'ils surviennent, les événements mettant en péril la cybersécurité.
- **Répondre** : concevoir et déployer les actions nécessaires pour répondre aux événements mettant en péril la cybersécurité.
- **Rétablir** : concevoir et déployer les actions nécessaires pour tenir à jour des plans de résilience et pour restaurer des services ou infrastructures affectés par un cyberincident.



51 Price Waterhouse Cooper, Why you should adopt the NIST Cybersecurity Framework. 2014. En ligne (consulté le 16/02/2018). Disponible sur http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

52 United States of America government, Department of Commerce, National Institute of Standards and Technology. Cybersecurity «Rosetta Stone» Celebrates Two Years of Success. News, NIST, 18 février 2016, en ligne (consulté le 16/02/2018). Disponible sur https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success.

4.2. Les normes 2700x de l'Organisation internationale de normalisation (ISO)

La famille des normes ISO/IEC 2700x s'applique aux systèmes de gestion de sécurité de l'information et s'adresse à tous les types d'organismes, quelle que soit leur taille, des entreprises privées aux services publics en passant par les organismes sans but lucratif.

Regroupées sous l'intitulé commune de « Techniques de sécurité des technologies de l'information », les normes ISO 2700x aident à lutter contre les multiples formes de cybermenaces et leur expansion toujours plus rapide. Toutes les applications de la cybersécurité y sont englobées. Plus d'une douzaine de normes en font partie et entretiennent chacune à son niveau un lien avec les ressources et méthodes à déployer en vue de se prémunir ou de faire face aux dangers dans l'univers des TIC.

Les normes ISO 2700x reprennent dans leurs champs d'application : la gestion des incidents, y compris les scénarios de secours en cas de catastrophe, les défaillances de système, les interruptions des activités et les attaques de logiciels malveillants comme celles causées par les virus, les vers et les chevaux de Troie. Elles sous-tendent par ailleurs les caractéristiques de sécurité utilisées dans divers produits, technologies et applications logiciels. Il s'agit donc d'un ensemble de solutions à disposition des organisations pour protéger leurs informations sensibles et critiques ainsi que les données personnelles, quels que soient le secteur économique et la structure organisationnelle.

La norme ISO/IEC 27001, en particulier, établit les exigences relatives aux systèmes de management de la sécurité des informations. Cette norme englobe les pratiques pour une gestion optimale des risques, en vue de répondre aux problématiques de sécurité, de confidentialité, d'évaluation et de traitement des risques.

Vision à long terme et base de confiance

À l'instar du CSF, l'ISO 27001 développe une méthodologie pour implémenter et mettre en œuvre la cybersécurité. Elle applique le principe Plan, Do, Check, Act à chaque étape de l'implémentation et de l'évolution des mesures de cybersécurité. La norme se différencie donc par son accent plus prononcé sur la nécessité de penser les actions à long terme. De plus, comme toute norme ISO, elle donne lieu à des processus de certification pour le personnel en charge de ces questions, qui constituent la base d'une confiance partagée entre acteurs sur leur capacité à gérer les questions de cybersécurité.

En l'occurrence, le CIRB et son personnel concerné pratiquent les méthodologies définies par les normes ISO 2700x, en particulier pour ses services et infrastructures stratégiques propres telles que le Data Center Régional, ainsi qu'au travers de son offre Information Security Management proposée à ses partenaires. Celle-ci s'adresse notamment aux organisations qui souhaitent obtenir l'accès à des données confidentielles (sources authentiques) et se voient dès lors imposer un certain nombre d'exigences de sécurité par les autorités européennes, fédérales et régionales. Le CIRB leur propose la mise en place d'un plan stratégique de sécurité qui suit les bonnes pratiques de la norme internationale ISO 2700x. Le plan comprend des mesures de sécurité techniques ainsi que les processus pour se conformer aux lois et normes imposées par des organisations telles que le Registre national (RRN), la Banque Carrefour de la Sécurité sociale (BCSS), etc.

3.

UN PLAN DE CYBERSÉCURITÉ POUR LA RÉGION DE BRUXELLES-CAPITALE

Un plan de cybersécurité de la Région de Bruxelles-Capitale doit répondre à l'objectif de protéger, face aux cyberattaques, la capacité opérationnelle des systèmes et des infrastructures informatiques au sein de la Région, en particulier de ses infrastructures critiques. Elle suppose en amont de suivre l'évolution des cybermenaces et d'organiser une capacité régionale de réaction, dans un objectif de résilience. La Région doit choisir à ce niveau d'engager toutes les ressources nécessaires dans le cadre de règles, audits, bonnes pratiques et recommandations à partager et à mettre en œuvre au plus large niveau de collaboration avec l'ensemble des autorités compétentes.

1. 4 AXES : CYBER-RÉSILIENCE, RESSOURCES, CULTURE ET PRÉVENTION

Le plan de cybersécurité de la Région de Bruxelles-Capitale aura pour vocation d'encourager différents publics à adopter, au départ de ses principes, les comportements adéquats.

De manière synthétique, la stratégie s'articule autour de quatre axes et s'adresse à quatre publics-cibles :

4 AXES	4 PUBLICS-CIBLES
• **organiser** la cyber-résilience des infrastructures critiques ; • **développer** les ressources industrielles, technologiques et humaines ; • **sensibiliser** et **diffuser** une culture de la cybersécurité ; • **prévenir** les cyberincidents et **renforcer** la collaboration avec les acteurs compétents en matière de cybersécurité et de cybercriminalité	• les services publics ; • les entreprises ; • le secteur académique ; • le·la citoyen·ne.

1.1. Organiser la cyber-résilience des infrastructures critiques

Organiser la cyber-résilience de notre Région impose en premier lieu d'identifier leurs cibles potentielles des attaques. On a vu au premier chapitre la diversité tant des attaques que de ces cibles. La réflexion doit dont être la plus globale possible, en premier lieu lorsqu'il s'agit d'inventorier les infrastructures critiques dans la Région de Bruxelles-Capitale.

Ce premier axe de la stratégie répond à des questions essentielles : qu'est-ce qu'une infrastructure critique, quelles en sont les exemples dans la Région, pourquoi faut-il les protéger, quel rôle la Région doit-elle jouer ?

Le rôle du CIRB et de BPS dans la transposition de la directive NIS

Les actions à mettre en œuvre à ce niveau s'inscriront dans le cadre donné par le Gouvernement fédéral pour la transposition en droit belge de la directive NIS [1]. Le CCB, chargé de cette mission, a notamment proposé d'inclure le secteur public dans la liste des opérateurs de services essentiels (OSE), d'avoir recours à des autorités sectorielles et de consulter les autorités régionales.

1 Lire plus haut, l'encadré « La directive NIS en Belgique », pages 28 et 29.

Pour ces trois aspects, le CIRB et BPS se poseront comme points de contacts naturels pour représenter la Région de Bruxelles-Capitale auprès du CCB dans l'accomplissement de cette mission.

Le Gouvernement bruxellois a également marqué sa volonté qu'une attention particulière soit portée à cette matière en validant la mesure du PGSP relative à « *l'instauration d'un groupe de veille technologique composé de spécialistes chargés d'identifier les innovations techniques et technologiques susceptibles d'apporter une plus-value en matière de gestion de crise et de résilience* ». [2]

A. Réaliser et mettre à jour une étude régionale des risques en matière de cybersécurité

Selon l'adage qui veut que savoir, c'est pouvoir, la connaissance est le socle d'un plan de cybersécurité. Cette connaissance doit être centralisée et partagée. Dès lors, il serait utile de créer un registre des risques au niveau régional et d'administrer sa mise à jour régulière en fonction de l'évolution des infrastructures, d'une part, des menaces et des vulnérabilités, d'autre part. Le recensement des infrastructures critiques constituera la première mission à réaliser dans ce cadre.

Qu'est-ce qu'une infrastructure critique ?

S'agissant d'identifier les infrastructures dont les défaillances en cas de cyberattaque présentent un risque pour la délivrance de services essentiels, quelques évidences viennent immédiatement à l'esprit : les réseaux de transport, la production et la distribution de l'eau et des énergies, la sécurité, la santé…

En tant que cadre fondateur d'une politique de lutte contre la cybercriminalité à l'échelon des États membres de l'Union européenne, la directive NIS intéresse aussi la Région de Bruxelles-Capitale. Dans le cadre du plan de cybersécurité, la Région devra servir de relais au CCB fédéral dans la mise en œuvre de la directive NIS [3] sur son territoire, cela à un double niveau :

- l'adaptation éventuelle de la législation régionale ;
- le recensement sur le terrain des infrastructures critiques régionales.

Des infrastructures gérées par des pouvoirs publics bruxellois sont notamment directement concernées par la directive NIS [4], en ce sens qu'elles se rangent parmi les secteurs suivants énumérés par la directive :

- les gestionnaires de réseau de distribution et les gestionnaires de réseau de transport de gaz et d'électricité ;
- les gestionnaires des ports ;
- les autorités routières chargées du contrôle et de la gestion du trafic et les exploitants de systèmes de transport intelligents ;
- les établissements de crédit ;
- les fournisseurs et distributeurs d'eaux destinées à la consommation humaine ;
- les IXP, les fournisseurs de services DNS, les registres de noms de domaines de haut niveau.

2 Plan global de sécurité et de prévention, déjà cité. Page 49, mesure 10.13.
3 Lire plus haut, page 26.
4 Voir la liste des secteurs et sous-secteurs énumérés par la directive NIS page 27.

L'inventaire des infrastructures critiques régionales s'appuiera utilement sur les éléments de définition formulés par différents pays de l'Union européenne. C'est le cas de la France qui a adopté le concept d'opérateurs d'importance vitale (OIV). D'une portée plus large, la définition des OIV englobe :

- les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ;
- certains établissements représentant un danger environnemental ou comprenant une installation nucléaire.

Une vision globale des risques

L'étude régionale des risques en matière de cybersécurité devra par ailleurs s'étendre à certains facteurs potentiels d'aggravation des dommages, comme :

- l'interdépendance des systèmes informatiques conduit au risque d'une défaillance globale, par effet de dominos ;
- l'héritage des systèmes informatiques anciens peut retarder la parade à une attaque par exemple lorsque ces systèmes ne sont plus documentés ou que leur fournisseur n'est plus en activité ou ne supporte plus ces systèmes : c'est un point d'attention des stratégies de cybersécurité aux Pays-Bas et au Royaume-Uni [5] ;
- la dissémination des objets connectés dans notre environnement, de la maison (avec les solutions domotiques) à l'espace public (où les équipements intelligents sont en plein développement en lien avec la smart city).

COMMENT LA CYBER-RÉSILIENCE EST-ELLE ORGANISÉE, JUSQU'À QUEL POINT, PAR QUELS ACTEURS ?

Il faut par ailleurs étendre cet inventaire aux mesures déjà mises en place : comment la cyber-résilience est-elle organisée, jusqu'à quel point, par quels acteurs, selon quelles règles et procédures, avec quelle pérennité… ?

B. Établir un registre régional des personnes clés

L'efficacité d'un plan d'action en matière de cybersécurité, tant dans son élaboration que dans sa mise à jour et son exécution, repose non seulement sur une définition pertinente des risques mais aussi sur l'identification des personnes dont le rôle et l'action sont déterminants, au sein de leur organisation, en cas de survenance d'une crise à grande échelle.

Le registre régional de cybersécurité remplira cette fonction. Il collectera auprès de chaque gestionnaire d'une infrastructure critique les coordonnées de leurs référent·e·s en matière de sécurité. Ce registre sera partagé de manière sécurisée entre ces gestionnaires et sa mise à jour en continu devra bien entendu être garantie.

5 United Kingdom, Cabinet Office. National Cyber Security Strategy 2016 to 2021. Policy paper. Publications, UK government, 1er novembre 2016, en ligne (consulté le 16/02/2018). Disponible sur https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Une mesure du PGSP [6] concerne l'établissement de ce registre. Elle prévoit de sensibiliser les acteurs régionaux de la prévention et de la sécurité « *à l'importance de désigner un point de contact IT dans chaque administration régionale, zonale et communale pour relayer les informations qui seront diffusées par le Centre de Cybercriminalité belge* ».

Ce registre doit aider par ailleurs à construire une véritable communauté de la cybersécurité au niveau de la Région de Bruxelles-Capitale en tant que plateforme de partage de moyens et des informations utiles.

C. Établir les exigences minimales de sécurité par secteur

Comme énoncé plus haut, les dispositions de la directive NIS s'appliquent directement à certains opérateurs bruxellois (publics, privés ou fonctionnant sous le régime de partenariat public-privé). Elles peuvent aussi servir de référence pour les secteurs ou opérateurs qu'elle ne vise pas directement. Par ailleurs, les règles et recommandations du niveau fédéral belge devront également être prises en considération.

Nous plaidons pour que soit établi un niveau minimum de sécurité par secteur, en s'inspirant de ces normes de niveau européen ou national. L'objectif est d'harmoniser l'approche, de diffuser les bonnes pratiques ainsi qu'établir des priorités en termes d'investissements à réaliser.

D. Labelliser les infrastructures critiques

Un label régional en matière de cybersécurité donnera de la visibilité au Plan et l'aidera de ce fait à mieux produire ses effets. Le label serait de nature à créer la confiance des utilisateur·rice·s de services, qui constitue la pierre angulaire du marché unique numérique selon l'Union européenne. Il identifierait les acteurs publics, les entreprises ou les commerces qui respectent leurs obligations et appliquent les bonnes pratiques en matière de protection contre les cyberincidents.

Cette action devrait se réaliser en prolongement des initiatives menées en ce sens par le CCB dans le cadre de la transposition de la directive NIS dans le droit belge. Le Gouvernement bruxellois l'a également validée dans le cadre du PGSP sous la mesure 8.11 [7] « *Définir pour les entreprises des règles de '' bonnes conduite '' génériques en matière de sécurité ; définir une politique régionale en ce sens et délivrer un label régional (certification Sécurité IT) aux entreprises s'engageant dans ce processus* ».

E. Aider à l'implémentation des exigences de sécurité minimales par secteur

Parallèlement à la labellisation, un autre incitant à l'application du plan de cybersécurité régional consisterait à appuyer les organisations dans leurs efforts pour identifier les risques, s'en protéger et disposer des moyens de réagir aux incidents.

Nous préconisons à ce niveau de proposer aux acteurs concernés des outils les aidant dans la mise en place des directives et normes de cybersécurité standard, notamment un plan de secours et de contingence type par secteur, en identifiant des niveaux d'alerte et de crise, des responsables et des actions types.

6 Plan global de sécurité et de prévention, déjà cité. Page 43, mesure 8.12
7 Plan global de sécurité et de prévention, déjà cité. Page 43, mesure 11.

F. Créer une CERT régionale

La Cyber emergency team fédérale, CERT.be, est en charge des activités de CERT au niveau national et gouvernemental belge. Sa mission est double : d'une part, coordonner la gestion et la réponse aux incidents (« incident handling and response ») en cas d'incidents et de crises d'ampleur nationale auprès d'opérateurs d'infrastructures critiques ou de services essentiels et, d'autre part, faire office de niche d'informations.

Cependant, ce service n'est pas disponible pour les acteurs régionaux et les entreprises lorsque l'incident ne constitue pas une crise d'ampleur nationale. Une Cyber emergency team régionale sera nécessaire pour apporter une assistance aux entreprises privées ou organisations publiques confrontées à un incident important à leur échelle. Son activité s'organiserait en concertation avec la CERT fédérale.

G. Établir un plan régional de cybercontingence

De manière complémentaire à l'identification et à la gestion des risques (cfr. point A ci-avant), différents scénarios de continuité puis de reprise des activités doivent être envisagés en vue de faire face aux cybercrises potentielles.

Le plan régional de cybercontingence devra donc définir, en parallèle avec le plan national :

- les critères d'une crise à l'échelle de la Région de Bruxelles-Capitale ;
- les processus et actions clés afin de gérer cette crise ;
- les rôles et responsabilités des acteurs clés en cas de crise.

H. Organiser des exercices de cybersécurité

Le but, ici, est d'évaluer dans quelle mesure les acteurs clés sont armés contre une cyberattaque. Il s'agit en l'occurrence de tester les plans de contingence de manière à identifier des interdépendances et les faiblesses mal ou pas prises en compte, ainsi que d'améliorer la coopération entre les différents secteurs.

De tels exercices peuvent dans un premier temps se restreindre aux services informatiques des administrations, puis aux administrations dans leur ensemble, avant de s'élargir encore davantage par la suite.

1.2. Développer les ressources industrielles, technologiques et humaines

Se protéger des cyber-risques demande de pouvoir s'appuyer sur des ressources variées. Il s'agit d'utiliser les produits et services en la matière aussi bien que de disposer des connaissances et compétences pour protéger ses données et ses infrastructures.

Or, comme l'a contasté Evoliris dans son Rapport de veille 2017 « État des lieux sur la cybersécurité à Bruxelles » [8], il existe aujourd'hui un « *manque de formations liées à la cybersécurité [...] Il est important d'ouvrir un dialogue entre les institutions académiques et les entreprises. Ce sera notamment le rôle du PFE : le Pôle Formation Emploi ICT de Bruxelles [qui] devrait voir le jour d'ici la fin de l'année 2018.* » De par son rôle de sensibilisation aux métiers du secteur de l'IT, le PFE constituera à n'en pas douter un acteur à intégrer dans le futur plan régional de cybersécurité.

8 Evoliris. État des lieux sur la Cybersécurité à Bruxelles. Les cahiers d'Evoliris, N° 2, 2017, en ligne (consulté le 16/02/2018). Disponible sur http://www.evoliris.be/fr/content/cahier-2017-apres-la-sensibilisation-etat-des-lieux-sur-la-cybersecurite-a-bruxelles.

À ce niveau, le plan poursuivra l'objectif de faire émerger en Région de Bruxelles-Capitale un véritable écosystème de la cybersécurité dont les acteurs clés seront les entreprises du secteur des TIC et les milieux académiques ainsi que l'École régionale des métiers de la sécurité.

A. Encourager les entreprises actives dans le secteur de la cybersécurité

La montée en puissance des multiples formes de cybermenace constitue une opportunité de croissance pour le secteur bruxellois des TIC, en vue d'offrir ses services aux entreprises et aux autorités publiques. Le plan régional de cybersécurité doit encourager les entreprises des TIC au sein de la Région à se développer sur ce créneau d'activités.

Cette mobilisation trouvera un relais utile et efficace auprès de différents interlocuteurs comme la fédération sectorielle AGORIA, les clusters d'entreprises ou encore les milieux académiques et de la recherche. Elle pourrait se concrétiser par exemple par la mise au point d'outils, tels qu'une charte, en vue d'organiser et promouvoir le secteur.

Le plan de cybersécurité pourrait de la sorte aider la Région de Bruxelles-Capitale et son secteur des TIC à forger une image d'excellence et d'innovation.

B. Promouvoir les échanges au niveau académique et de la recherche

Une région qui veut se protéger des cyber-risques doit développer son économie de la connaissance donc, en premier lieu, soutenir dans ce domaine un enseignement de qualité ainsi que dynamiser la recherche au plus haut niveau.

La Région de Bruxelles-Capitale gagnerait à s'organiser en pôle de savoir, en commençant par inventorier les centres académiques et de recherche en lien avec la cybersécurité, de manière à les encourager dans la voie de la collaboration et de l'échange, par exemple sur des projets communs ou ciblés.

Une part importante de ce travail d'inventaire a été réalisée par Evoliris dans son « État des lieux sur la cybersécurité à Bruxelles » qui recense les formations proposées dans l'enseignement supérieur bruxellois (tant dans les universités que dans les hautes écoles) ainsi que les filières de certification et de formation continue.

Le soutien de la Région dans le cadre du plan pourrait, à ce niveau, passer par la mise à disposition de fonds, de bourses…

C. Soutenir la recherche et développement de produits et services de cybersécurité

En complément du point précédent, le plan régional de cybersécurité doit faciliter le passage de la connaissance scientifique ou technique aux applications concrètes.

Deux volets d'action sont à prévoir :

- la mise à disposition de fonds publics d'aide à la recherche et développement, au bénéfice notamment de start-up ou spin-off ;
- la création d'outils de promotion et d'incitants pour les entreprises, en vue de renforcer leur visibilité, de communiquer leurs recherches, de commercialiser leurs produits ou services.

D. Couvrir les besoins de base des différents acteurs en produits et services de sécurité

Il est essentiel que les citoyen·ne·s, les entreprises ou encore les administrations disposent d'un arsenal de cybersécurité adapté à leurs besoins et leurs usages. Si leurs risques ne peuvent être totalement couverts par les produits et services du marché, il est impératif que des solutions soient mises en place.

E. Encourager le développement de cursus académiques

La Région de Bruxelles-Capitale, ses entreprises, ses administrations ont besoin de personnes formées aux différentes facettes de la cybersécurité. Celle-ci ne touche en effet pas seulement l'informatique mais aussi les réseaux de télécommunication (mobile notamment) ou d'objets connectées.

C'est le rôle de l'enseignement, spécialement au niveau supérieur, que de couvrir toutes ces facettes. Le plan régional de cybersécurité, dans l'intérêt stratégique de la Région, établira un inventaire des formations touchant la cybersécurité, analysera leur étendue – en termes de matières abordées comme de publics touchés – et leur cohérence. Au besoin, des actions spécifiques seront entreprises pour promouvoir l'une et l'autre.

IL EST ESSENTIEL QUE LES CITOYEN·NE·S, LES ENTREPRISES OU ENCORE LES ADMINISTRATIONS DISPOSENT D'UN ARSENAL DE CYBERSÉCURITÉ

L'École intégrée des métiers de la sécurité, de la prévention et du secours

Dans sa **note stratégique** relative à l'exercice des compétences régionales bruxelloises en matière de prévention et de sécurité du 28/4/2016, le Gouvernement bruxellois a décidé de créer une École intégrée des métiers de la sécurité, de la prévention et du secours (ou École régionale des métiers de la sécurité, abrégée en ERMS).

Les missions de l'ERMS seront entre autre de :

- mettre en œuvre une vision intégrée et multidisciplinaire de la sécurité publique au sens large ;
- soutenir les différentes écoles impliquées dans la formation des acteurs de prévention et sécurité par la mutualisation de processus communs (cellule pédagogique, appui en matière de TIC, logistique…) ;
- soutenir ces écoles par la mise à disposition d'une infrastructure commune, multidisciplinaire permettant d'accueillir les différents apprenants et d'organiser des exercices intégrés et/ou spécifiques à chaque discipline ;
- mettre ses connaissances et infrastructures à disposition d'organisations publiques, voire privées, pour autant que les activités de celles-ci soient compatibles avec les missions de l'école.

En s'inspirant de la vision du PGSP [9], l'ERMS proposera également dans son programme, outre le cadastre régional des écoles et types de cours disponible :

- l'usage de nouvelles technologies d'apprentissage et techniques de l'information pour promouvoir le travail en réseau mais aussi la sécurisation des outils numériques et des usages du web ;
- en matière de gestion de crise et de résilience, en complément de l'organisation des exercices réguliers et communs sur base de scénarios réels pour les acteurs de sécurité et de secours, de former le personnel à la maîtrise des outils de communication (Astrid, plateforme digitale) et de gestion des crises.

Afin de traduire la volonté du Gouvernement bruxellois, l'une des missions de l'ERMS sera de renforcer la spécialisation en matière de formation, d'intégrer des partenariats existants et de développer de nouveaux accords. À cet égard, des collaborations avec des universités seront développées notamment dans le cadre de formations spécifiques liées à la cybercriminalité ou à la sécurité informatique.

F. Encourager et faciliter l'accès à la formation

Les filières de formation tout au long de la vie ont également leur rôle à jouer dans la généralisation des compétences et de la vigilance dans le domaine de la cybersécurité, tant dans les usages domestiques que professionnels.

Spécifiquement, des incitants à la formation peuvent être créés pour aider les indépendant·e·s, PME et grandes entreprises à renforcer leur cybersécurité.

1.3. Diffuser la culture de la cybersécurité

Une économie florissante repose sur la confiance des entreprises et des citoyen·ne·s à propos des services en ligne. Il est du ressort du Gouvernement d'assurer une prise de conscience de tous les acteurs afin d'amener des comportements responsables afin que les entreprises de toutes tailles et les citoyen·ne·s se protègent, et protègent de manières adéquate ceux dont ils sont responsables (par exemple leurs client·e·s pour les premières, leurs enfants pour les seconds).

A. Sensibiliser les indépendant·e·s, artisan·e·s et entreprises

L'économie et l'emploi en Région de Bruxelles-Capitale reposent notamment sur les activités d'un très grand nombre d'indépendant·e·s, d'artisan·e·s et de TPE ou PME qui, indépendamment de leur taille ou de leur secteur, intègrent inévitablement les TIC comme outils professionnels (logiciels comptables, métier, sites Internet, boutiques en ligne).

Il est donc primordial que la Région de Bruxelles-Capitale aide ces acteurs essentiels à sa prospérité à se protéger des cyber-risques et à y faire face. Il en va de la permanence de leur activité comme de la confiance des tiers en leur endroit.

Le plan de cybersécurité veillera donc à mettre en place ou accompagner des campagnes de communication et de sensibilisation à l'attention de cette cible stratégique pour la Région. Les acteurs régionaux de la cybersécurité et de l'économie s'emploieraient à rechercher des partenariats à ce niveau avec les interlocuteurs de référence de ces publics, les fédérations sectorielles par exemple.

9 Plan global de sécurité et de prévention, déjà cité. Objectifs transversaux - La formation des acteurs de la prévention et de la sécurité. Pages 7 et 8.

B. Encourager l'adoption de bonnes pratiques par les indépendant·e·s et les entreprises

De manière complémentaire à la sensibilisation à l'acuité des cyber-risques, les indépendant·e·s et les entreprises devraient être encouragé·e·s à mettre en œuvre les bonnes pratiques de cybersécurité, en réponse le cas échéant à leurs obligations en la matière.

L'action de la Région de Bruxelles-Capitale à ce niveau consisterait par exemple, de sa propre initiative ou en relais d'autres acteurs :

- à simplifier l'accès à ces bonnes pratiques ;
- à aider à appliquer ces bonnes pratiques ;
- à s'assurer que l'information d'autres instances (comme le CCB ou l'ENISA) leur parvienne de manière utile.

Outre les moyens traditionnels de communication, la Région de Bruxelles-Capitale utiliserait les outils les plus adaptés à la propagation de bonnes pratiques. Une charte bruxelloise de cybersécurité et d'éthique en matière des données servirait par exemple de signe de confiance pour les client·e·s des indépendant·e·s, artisan·e·s et entreprises.

C. Promouvoir les bons réflexes des acteurs économiques en cas d'incident

Corollairement à la diffusion des bonnes pratiques parmi les indépendant·e·s, artisan·e·s ou PME, la Région de Bruxelles-Capitale devra les aider à adopter de bons réflexes en cas d'incident. À l'instar des campagnes grand public visant à faire connaître le bon numéro d'appel pour joindre la police ou les pompiers, le rôle du plan de cybersécurité sera de faire connaître les adresses utiles à contacter en cas de cyberincidents. Ce sera notamment le rôle d'une CERT régionale de servir de point de contact à cet égard.

D. Sensibiliser le·la citoyen·ne

Le grand public constitue une cible à part entière des campagnes de promotion de la cybersécurité car il est souvent lui-même la victime et le relais de cyberattaques. Le rôle du plan de cybersécurité sera d'éveiller la conscience et la vigilance des citoyen·ne·s face au cyber-risque, tant par des actions spécifiques qu'en relais d'actions entreprises par d'autres acteurs. Ces actions font également l'objet de la mesure 8.11 du PGSP qui préconise de développer une campagne de sensibilisation du public à la cybersécurité [10].

E. Faire adopter les bonnes pratiques de cybersécurité par le·la citoyen·ne

Le·la citoyen·ne doit devenir le propre acteur de sa cybersécurité. Il·elle doit pour cela connaître les bonnes pratiques dont certains réflexes essentiels dans son usage quotidien des TIC. De nombreux acteurs travaillent déjà à diffuser les bonnes pratiques en la matière. Le rôle de la Région de Bruxelles-Capitale à ce niveau sera d'aider à relayer ces informations et d'analyser leur mise en pratique. En particulier, la Région de Bruxelles-Capitale veillera, dans le droit fil de sa politique de réduction de la fracture numérique, à ce que chaque citoyen·n·e ait non seulement accès aux TIC et notamment aux ressources offertes par Internet mais, aussi, les utilise de manière sûre pour soi-même et pour les autres.

10 Plan global de sécurité et de prévention, déjà cité. Page 43, mesure 11.

F. Promouvoir les bons réflexes du·de la citoyen·ne en cas d'incident

Pareillement aux entreprises, le·la citoyen·ne doit savoir à qui s'adresser lorsqu'il·elle est la victime d'une cyberattaque, ceci afin de réduire ses dommages éventuels, enrayer la propagation de l'attaque, faciliter la poursuite des cybercriminels. Le plan régional de cybersécurité, en cohésion avec l'action d'autres institutions, veillera donc à diffuser les bonnes adresses à contacter en cas d'incident.

1.4. Prévenir les cyberincidents

Au regard de l'évolution des nouvelles technologies, la criminalité a connu une modification d'orientation importante ces dernières années avec un déplacement et un développement des phénomènes de criminalité de l'espace public vers les espaces virtuels. La cybercriminalité fait dorénavant partie intégrante des risques du quotidien et requiert une attention grandissante de la part des autorités. À cet égard, elle nécessite un investissement important dans le développement de nouveaux moyens de recherches et d'actions.

Dans son PGSP, le Gouvernement bruxellois a déjà démontré sa volonté de faire de la lutte contre la cybercriminalité l'une de ses dix thématiques prioritaires pour les prochaines années. En phase avec la stratégie globale du PGSP, plusieurs mesures visent entre autres à « *renforcer les capacités de recherche sur le darknet afin notamment de lutter de manière proactive contre le développement de divers phénomènes criminels (trafic de stupéfiants, trafic d'armes, prévention et lutte contre le terrorisme et le radicalisme) et favoriser l'échange des informations qui en résultent entre les services compétents* »[11] (M8.14).

A. Prévenir le passage à l'acte de potentiels futurs cybercriminels

Dans la continuité de l'approche du PGSP, un Centre de cybersécurité régional va être mis en place.

La pertinence d'un tel outil a été démontrée à maintes reprises puisque les nouveaux moyens de communication ont été utilisés pour lancer des appels au rassemblement et à la violence. Une vigilance accrue de la part des autorités administratives et judiciaires et ce, tout particulièrement en matière de veille sur les réseaux sociaux est devenue incontournable.

Le Centre de cybersécurité régional comptera des représentants de la Regional Computer Crime Unit de la Police judiciaire fédérale, des six zones de police locale de la Région ainsi que des représentants de la direction de la coordination de la police fédérale. Cette collaboration sera encadrée par une convention reprenant les modalités de collaboration entre les différentes entités.

11 Plan global de sécurité et de prévention, déjà cité. Page 43, mesure 8.14.

La mise en place d'un groupe de veille technique permettra de renforcer et de concrétiser les objectifs régionaux. Ce groupe pourra bénéficier de la mise en commun de moyens techniques, tel qu'un logiciel de veille acquis par la Région de Bruxelles-Capitale. Le but à ce niveau est de prévenir l'enrôlement de Bruxelloi·se·s dans les réseaux de cybercriminalité. Le plan de cybersécurité articulera à ce niveau :

- des actions sur le terrain de l'éducation, spécialement auprès du public des cours (du niveau secondaire ou supérieur) en informatique, via le témoignage de policier·ère·s, repenti·e·s… ;
- dans la dissuasion par le renforcement des infrastructures TIC dans la Région et notamment la protection des infrastructures critiques.

La CERT régionale contribuera, quant à elle, à prévenir et limiter les risques d'incidents en cybersécurité sur le territoire régional, mais aussi à apporter un soutien lors de ceux-ci.

B. Renforcer les compétences au niveau des investigations

Par la spécificité des techniques qu'elle emploie, la cybercriminalité exige pour être combattue des ressources humaines elles-mêmes rompues à ces procédés, tant sur le plan des connaissances – y compris juridiques – que de leur utilisation concrète. Le plan régional de cybersécurité cherchera à appuyer la formation des acteurs concernés pour identifier rapidement et efficacement les techniques utilisées par les cybercriminels ou agir dans le cyberespace pour infiltrer les réseaux de la cybercriminalité et contrecarrer leurs actions. Des filières de formation en cybercriminologie doivent être prévues de même que la possibilité de faire appel à l'aide de hackers éthiques.

Le développement de nouvelles formations en partenariat avec l'École régionale des métiers de la sécurité et le monde académique en seront le moteur.

C. Coopérer au niveau fédéral et international

Le plan de cybersécurité doit intégrer ses acteurs dans les réseaux existants, tant au niveau fédéral belge qu'international, dans le domaine de la lutte contre la cybercriminalité. Des contacts et collaborations doivent être établis avec :

- au niveau belge : la Federal Computer Crime Unit et la Regional Computer Crime Unit ;
- au niveau international : des instances comme Interpol, le FBI, l'EC3 Europol ou encore l'EUCTF (European Cybercrime Task Force).

2. MISE EN ŒUVRE DU PLAN DE CYBERSÉCURITÉ

Dans une volonté d'aller au-delà de l'analyse, nous développons ci-après les étapes qui nous paraissent nécessaires en vue de couronner de résultats sa mise en place.

2.1. Mettre en place un groupe régional de réflexion

Le groupe de réflexion rassemblera les acteurs clés de la cybersécurité en Région de Bruxelles-Capitale avec comme mission d'analyser et de développer les pistes envisagées dans le plan de cybersécurité présenté dans ces pages. Il s'appuiera sur le groupe de travail déjà mis en place par BPS dans le cadre du PGSP et recrutera ses membres tant dans le secteur public que dans la sphère privée : entreprises, monde académique et de la recherche.

Les travaux du groupe de réflexion consisteront à :

- identifier les acteurs principaux jouant un rôle dans la cybersécurité de la Région, définir leurs rôles, responsabilités et droits ;
- clarifier les compétences de cybersécurité qui sont du ressort de la Région par rapport au pouvoir fédéral et autres entités fédérées ;
- définir un programme régional de cybersécurité, détaillant des projets concrets dans chacun des axes du plan de cybersécurité ;
- proposer une feuille de route de cybersécurité pour l'horizon 2020 ;
- suivre la réalisation de la feuille de route.

2.2. Mettre en place une gouvernance du programme régional de cybersécurité

La cohérence et la pérennité du plan de cybersécurité appellent à mettre en place un modèle de gouvernance à plusieurs niveaux, avec un appui fort du Gouvernement régional, tant en termes de vision que de budget :

- gouvernance du plan de cybersécurité par un comité des sages ;
- comités par secteur pour l'implémentation et le suivi de la feuille de route.

2.3. Établir des partenariats public-privé

La mise en place de la stratégie doit donc impliquer toutes les parties prenantes de la cybersécurité en Région de Bruxelles-Capitale. Des partenariats publics-privés pourraient être organisés afin d'augmenter la capacité et l'expertise des instances régionales dans la lutte contre les vulnérabilités, les incidents et les attaques dans le cyberespace.

LA CYBERCRIMINALITÉ EXIGE
POUR ÊTRE COMBATTUE
DES RESSOURCES HUMAINES
ELLES-MÊMES ROMPUES
À CES PROCÉDÉS

CONCLUSION

L'univers – bien mal nommé – virtuel ne peut offrir moins de sécurité que le monde réel. Il est donc de la responsabilité des autorités publiques de mettre en place les cadres et d'entreprendre les actions nécessaires pour assurer une sécurité et une fluidité des outils et réseaux numériques, ainsi que des informations qu'ils contiennent. Il s'agit d'instaurer un climat de confiance propice à faire profiter chacun du meilleur des technologies aujourd'hui à sa disposition, en voyant sa vie privée et ses données, spécialement ses données à caractère personnel, efficacement protégées tant contre les accidents que contre la malveillance et la cybercriminalité.

Le présent Cahier poursuit l'objectif de sensibiliser les acteur·rice·s et les décideur·euse·s publics·ques de la Région de Bruxelles-Capitale et, plus largement, les communautés économique et académique bruxelloises, aux défis de la cybersécurité dans un monde aujourd'hui largement tributaire des TIC. Il vise à orienter l'action de la Région en vue de garantir la résilience de ses systèmes d'information.

INSTAURER UN CLIMAT DE CONFIANCE PROPICE À FAIRE PROFITER CHACUN DU MEILLEUR DES TECHNOLOGIES

Au-delà de l'effet d'alerte engendré par la répétition des cyberattaques, nous avons cherché à articuler les multiples dimensions d'un futur plan régional de cybersécurité : la prévention, la réaction et la correction. Quatre axes opérationnels structurent le plan :

- organiser la cyber-résilience de nos infrastructures techniques ;
- développer les ressources industrielles, technologiques et humaines au sein de la Région ;
- diffuser la culture de la cybersécurité, notamment dans la population et les entreprises bruxelloises ;
- prévenir les cyberincidents.

L'interdépendance des systèmes d'information, comme l'ont montré les récents exemples de cyberattaques en 2017, est un facteur aggravant les risques et les menaces sur la démocratie. La Région doit donc envisager son action sous un angle transversal, en coalisant ses forces vives autour de l'objectif de résilience et en mobilisant les compétences de chaque acteur par rapport à cet objectif. Cela, en dépassant les frontières qui séparent les secteurs privé et public, le monde académique et celui des entreprises, sans oublier les citoyen·ne·s.

CONCLUSION

Des jalons essentiels d'un plan régional de cybersécurité ont déjà été posés. Qu'il s'agisse, pour le CIRB, de ses infrastructures sécurisées et de ses services en ce qui concerne la gestion de la sécurité de l'information ou la mise en conformité des administrations bruxelloises avec le GDPR ou, pour BPS, du PGSP et de ses développements, ces fondations peuvent servir à bâtir l'édifice plus global du plan régional de cybersécurité, en symbiose avec les missions assurées à l'échelon fédéral belge par le CCB.

Ce positionnement ambitieux de la Région s'inscrit aussi dans la mise en complémentarité intelligente de nos différentes compétences : que ce soit en matière de développement informatique ou en matière de coordination des politiques de sécurité.

Le moment est venu de capitaliser les bénéfices de ces premiers accomplissements. Ce sera au Gouvernement régional de prendre et mettre en application, de manière collégiale, les décisions adéquates pour donner vie au plan de cybersécurité que le CIRB et BPS appellent aujourd'hui de leurs vœux au travers de ce Cahier. Nos deux organismes se tiennent à disposition de la Région pour l'accompagner dans cette mission et donner une forme concrète à ce plan.

GLOSSAIRE

BPS	Bruxelles Prévention & Sécurité
CCB	Centre pour la Cybersécurité Belgique
CERT	Computer Emergency Response Team
CIRB	Centre d'Informatique pour la Région Bruxelloise
CSF	Cybersecurity Framework
CSI	Conseiller en Sécurité de l'Information
DCR	Data Center Régional
DNS	Domain Name System
DPO	Data Protection Officer
ENISA	European Network and Information Security Agency
FCCU	Federal Computer Crime Unit
GDPR	General Data Protection Regulation
ISaaS	Information Security as a Service
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IXP	Internet eXchange Point
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OIV	Opérateur d'Importance Vitale
OSE	Opérateur de Service Essentiel
PGSP	Plan Global de Sécurité et Prévention
PME	Petite et Moyenne Entreprise
RCCU	Regional Computer Crime Unit
TIC	Technologies de l'Information et de la Communication
TPE	Très Petite Entreprise

LES CAHIERS DU CIRB

Le Centre d'Informatique pour la Région Bruxelloise a pour rôle d'organiser, promouvoir et disséminer l'usage des TIC auprès des autorités et administrations locales de la Région de Bruxelles-Capitale.

Le Centre poursuit à cet effet une mission d'information, notamment par la publication de Cahiers faisant le point sur ses activités, ses projets ou encore sur l'évolution des technologies.

PUBLICATIONS RÉCENTES :

2017	
Guide pratique	Règlement Général sur la Protection des Données (GDPR) - Guide pratique à l'attention des institutions locales et régionales de la Région de Bruxelles-Capitale
2015	
Cahier 36	12 règles fondamentales de sécurité informatique
Cahier 35	4 projets-clés de smartcity.brussels
2014	
Livre blanc 2014-2019	Smart.brussels : une région connectée, une région durable, une région ouverte, une région sécurisante
2013	
Cahier 34	IRISnet, le maillon fort d'une *smart region*
2012	
Cahier 33	Joignez la conversation : le secteur public à l'heure des réseaux sociaux + Guide pratique Médias sociaux

Les Cahiers du CIRB sont disponibles sous format électronique, à télécharger depuis son site Internet cirb.brussels

Pour toute information sur les Cahiers du CIRB, écrire à communication@cirb.brussels

Rédaction et coordination : Service Communication du CIRB
Imprimé avec de l'encre végétale sur papier issu de forêts gérées durablement (label FSC).

cirb.brussels
IT is for you

Editeur responsable : Hervé Feuillien
CIRB Avenue des Arts, 21 - 1000 Bruxelles
T 32 2 282 47 70 F 32 2 230 31 07
cirb.brussels - communication@cirb.brussels
@CIRB_CIBG