CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

STRATÉGIE CYBERSECURITÉ BELGIQUE 2.0 2021-2025

MAI 2021

.be


Security

Synopsis

La présence et la croissance des services et technologies numériques offrent à la population et aux organisations belges de nombreuses opportunités de développement. Or, les autorités publiques, les citoyens et les organisations doivent également faire de plus en plus souvent face à des cybermenaces (avancées), susceptibles d'accroître les risques et de compromettre les possibilités que présentent les services et technologies numériques. L'objectif de cette stratégie nationale actualisée de cybersécurité est de préserver les capacités des services, des biens, des personnes et des capitaux au-delà de nos frontières.

Cette stratégie vise à proposer une vision prospective d'un cyberespace ouvert, libre et sécurisé qui offre une réponse aux cybermenaces qui ciblent ou pourraient cibler la Belgique. Ce document identifie les différents acteurs et les principales menaces, il définit une mission claire et, sur cette base, propose des objectifs stratégiques et des priorités pour les années à venir, ainsi que les moyens nécessaires à leur mise en œuvre. La cybersécurité étant une responsabilité partagée, les différents rôles des acteurs concernés y sont également définis. Le Centre pour la Cybersécurité Belgique (CCB) étant responsable de la coordination de la cybersécurité ; il joue à ce titre un rôle clé dans la mise en œuvre de cette Stratégie de cybersécurité 2.0.

Centre pour la Cybersécurité Belgique, Bruxelles, mai 2021

Table des matières

1. Introduction

Notre société et notre économie sont en constante évolution, un processus qui est accéléré par la transformation numérique. Les personnes, les organisations, les appareils, les données et les processus se trouvent toujours plus en interconnexion et interaction via des canaux en ligne tels que l'internet, les appareils mobiles, l'internet des objets (IoT) ou l'utilisation du cloud pour le stockage de fichiers (personnels) et de photos. Cette augmentation de l'utilisation des nouvelles technologies s'accompagne d'une recrudescence des cyberattaques et d'une intensification de la gravité et du degré d'impact de ces attaques. Les données sensibles, y compris les données personnelles des clients et les données politiquement sensibles (par exemple les renseignements militaires) sont de plus en plus exposées au risque de divulgation. Il est donc de la plus haute importance de protéger ces données en sécurisant l'environnement numérique.

1.1 Contexte stratégique

En 2012, la Belgique a élaboré sa première stratégie en matière de cybersécurité, axée sur la reconnaissance de la cybermenace, l'amélioration de la sécurité et la mise en place de mesures permettant de réagir de manière appropriée aux incidents. L'évolution constante du cyberespace nous impose d'élaborer une nouvelle stratégie belge en matière de cybersécurité qui réponde aux risques et menaces actuels et émergents.

La Stratégie de cybersécurité 2.0 trace les contours de la politique belge et vise à sécuriser le cyberespace à tous les niveaux, et ce, pour tous les acteurs. Le suivi, la coordination et la supervision de la mise en œuvre de la stratégie belge de cybersécurité relèvent de la responsabilité du Centre pour la Cybersécurité Belgique (CCB). La stratégie de cybersécurité 2.0 fixe les objectifs pour l'horizon 2025 et fera périodiquement l'objet de révisions et d'ajustements.

Cette stratégie s'inscrit également dans un contexte international. L'Union européenne se penche, à cet égard, sur un certain nombre d'initiatives visant à promouvoir et à améliorer la cyber-résilience au sein de l'UE. La directive NIS (" Network and Information Security », sécurité des réseaux et de l'information) a été adoptée en juillet 2016 et transposée en Belgique dans la loi du 7 avril 2019 : *Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité*

publique. L'article 7 de cette directive (reproduit à l'article 10 de la loi belge) impose aux États membres d'élaborer une stratégie nationale pour la sécurité des réseaux et des systèmes d'information.

En outre, le Cybersecurity Act est entré en vigueur en juin 2019. Il étend notamment le mandat de l'ENISA à l'Agence européenne pour la cybersécurité. Ce règlement souligne également la nécessité de disposer d'un certificat européen de cybersécurité dans le domaine des technologies de l'information et de la communication, en vue d'améliorer la confiance envers les produits et services et leur sécurité ; des enjeux cruciaux pour le marché intérieur numérique.

Enfin, il convient par ailleurs de garder à l'esprit les engagements nationaux sur la résilience dans le contexte de l'engagement de l'OTAN baptisé *NAVO Cyber Defence Pledge*.

1.2 Cybersecurity

La cybersécurité est le résultat d'un ensemble de mesures de sécurité qui doivent minimiser le risque d'accès perturbé et non-autorisé aux systèmes d'information et de communication (TIC).

La cybersécurité englobe toutes les mesures raisonnables et acceptables destinées à protéger les TIC des citoyens, des entreprises, des organisations et des pouvoirs publics contre les cybermenaces. Il s'agit de la protection des systèmes (tels que le matériel, les logiciels et les infrastructures connexes), des réseaux, ainsi que des données qu'ils contiennent. Les mesures visant à contrer l'exploitation des TIC, par exemple à des fins de fraude, d'incitation à la violence, ou de recrutement de terroristes, ne relèvent pas, à proprement parler, de cette stratégie.

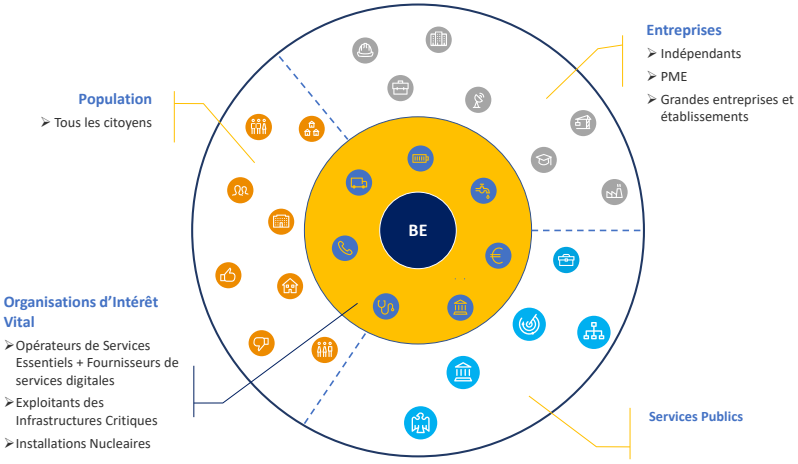
Dans cette optique, il est indispensable de développer et de renforcer les mesures techniques et organisationnelles. Tout d'abord, il convient d'identifier correctement les objectifs, ainsi que les campagnes de sensibilisation à la cybersécurité appropriées pour toutes les parties prenantes. La mise en œuvre de mesures préventives visant à protéger les données sensibles contre les cybermenaces et les cyberincidents doit également être envisagée, afin d'empêcher l'accès non autorisé à ces données. Il est

en outre nécessaire de surveiller et d'analyser les menaces potentielles. Si un incident devait tout de même se produire, l'important est d'être prêt à intervenir et à lui opposer une réaction et une solution efficaces.

Il importe de définir un cadre de gouvernance de la cybersécurité si l'on veut atteindre les objectifs de cybersécurité. Par conséquent, il est crucial de définir les rôles et les missions, ainsi que de clarifier la responsabilité de tous les acteurs concernés. La mise en place d'un cadre national de gouvernance permet le dialogue et la coordination des différentes activités.

Si le Règlement général sur la protection des données (RGPD) et la protection de la vie privée en général ne font pas partie de la cybersécurité au sens strict, ces deux dimensions sont bien évidemment étroitement impliquées dans la mission de détection du CCB. C'est pourquoi une coopération de qualité avec l'Autorité belge de protection des données s'avère nécessaire. La lutte contre les campagnes de désinformation en ligne ne relève pas non plus de la cybersécurité, mais elle y est liée. Dans ce contexte également, il est indispensable d'assurer la coopération avec les services de renseignement et de sécurité compétents.

1.3 Groupes cibles



La cybersécurité n'est pas la responsabilité unique des pouvoirs publics. Elle requiert un effort conjoint de tous les acteurs en mesure d'y contribuer. Si chacun apporte sa pierre à l'édifice, c'est la sécurité dans son ensemble qui en sortira grandie.

i. Population

Les citoyens sont les premiers responsables de la protection de leurs propres biens. Cela inclut les smartphones, les ordinateurs portables, les tablettes, mais aussi les applications qui y sont installées (comme les applications bancaires) et donc aussi les données qu'ils contiennent. En protégeant leurs propres appareils et applications et en les utilisant de manière appropriée, ils compliquent la tâche des auteurs de cyberattaques. Avec le soutien des pouvoirs publics et des médias, tels que Safeonweb.be et info-risques.be, la population peut prendre conscience des principales cybermenaces; elle se sentira aussi concernée par la sécurisation du cyberespace.

ii. Entreprises

Les entreprises jouent un rôle majeur dans la protection de leurs propres infrastructures et des données de leurs employés. Les petites et moyennes entreprises (PME, moins de 250 employés) occupent le devant de la scène, puisqu'elles représentent plus de 99 % des entreprises. Ce groupe d'acteurs comprend également des établissements d'enseignement et des fournisseurs de produits de sécurité. Les produits de sécurité tels que les pare-feu, les antivirus, le cryptage ou d'autres produits logiciels et matériels augmentent sérieusement la sécurité des systèmes informatiques et réduisent le risque d'incidents. Il est important d'investir dans ces produits de sécurité, de soutenir leurs fournisseurs et d'en faciliter l'usage par les utilisateurs des systèmes informatiques. Le développement d'une certification de base en cybersécurité permettant à l'entreprise de démontrer qu'elle se préoccupe suffisamment des cybermenaces les plus courantes est un aspect non négligeable de cette approche et peut également constituer un avantage concurrentiel. Dans cette optique, l'Union européenne a lancé en 2019 un cadre de certification en matière de cybersécurité.

iii. Services publics

Avec sa structure étatique complexe, il est difficile en Belgique d'assurer la coordination d'une politique de cybersécurité pour les services publics. Les autorités fédérales disposent de services publics fédéraux horizontaux, verticaux et de programmation. Les régions et les communautés se déclinent en ministères et en directions. Le Centre pour la Cybersécurité Belgique

(CCB) élabore des conseils et des directives qui sont à la disposition de tous les services publics.

La sécurité et la cybersécurité en particulier relèvent de la compétence fédérale et sont traitées au niveau national.

iv. Organisations d'Intérêt Vital

Les Organisations d'Intérêt Vital (OIV) pour notre pays doivent bénéficier d'une protection optimale contre les cyberattaques, car les incidents liés à ces organisations peuvent avoir un impact national à grande échelle.

Dans ce contexte, on entend par « Organisations d'Intérêt Vital » les entités publiques et privées qui fournissent un service essentiel à la population belge, en utilisant les réseaux et les systèmes d'information. Sont au moins visés les exploitants d'infrastructures critiques, les opérateurs de services essentiels et les fournisseurs de services numériques, ainsi que les infrastructures nucléaires (comme prescrit dans leurs cadres juridiques respectifs)[1].

A priori, les autorités sectorielles, en concertation avec le Centre de crise national (NCCN) et le CCB, identifient les Organisations d'Intérêt Vital. Le terme est destiné à évoluer et couvre les secteurs de l'énergie, de la mobilité, des télécommunications, le secteur financier, celui de l'eau potable, de la santé publique, des fournisseurs de services numériques et les autorités publiques.

1.4 Vision

La Belgique plaide en faveur d'un cyberespace ouvert, libre et sûr qui permette à nos citoyens et entreprises de s'épanouir pleinement et de s'engager sur la scène internationale, et qui sauvegarde et protège les droits fondamentaux. Afin de construire et d'assurer la confiance essentielle de la société dans le cyberespace, la cybersécurité joue un rôle inévitable et décisif. Il s'agit là d'une responsabilité partagée par tous les acteurs, qui exige une approche globale.

1 *Bien que le potentiel scientifique et économique du pays et les organisations fournissant des services essentiels au sein du secteur public entrent dans le champ d'application visé par le concept d'« Organisations d'Intérêt Vital », un cadre clair de cybergouvernance pour ces secteurs doit d'abord être développé.*

1.5 Mission

À l'horizon 2025, la Belgique doit être l'un des pays les moins vulnérables d'Europe dans le domaine de la cybersécurité.

La Stratégie Cybersécurité 2.0 ambitionne de faire de la Belgique l'un des pays les moins vulnérables d'Europe dans le domaine de la cybersécurité à l'horizon 2025. Elle s'articulera autour de plans d'action destinés à protéger tous les acteurs, qu'ils évoluent dans la population au sens large, dans des organisations privées ou dans des Organisations d'Intérêt Vital. La stratégie s'inscrit dans la lignée des stratégies d'investissement du gouvernement et du secteur privé pour des développements futurs et garantit ces investissements ainsi que la création de nouvelles opportunités et de nouveaux emplois. En outre, les objectifs stratégiques permettent de se préparer à l'apparition de nouvelles évolutions technologiques et de risques potentiels.

2. Évaluation des risques

L'évaluation nationale des risques 2018-2023 du Centre de crise national considère le cyberespace comme l'un des plus importants groupes de risques auxquels notre pays sera confronté au cours des prochaines années. Au sein de ce groupe, la cybercriminalité et l'hacktivisme visant les entreprises et les infrastructures critiques sont identifiés comme des risques nationaux prioritaires.

En 2017, nous avons assisté à la propagation fulgurante du ransomware WannaCry dans plus de 150 pays qui a interrompu de nombreuses opérations commerciales. Le malware NotPetya s'est, quant à lui, rapidement fait connaître comme le cyberincident le plus coûteux jamais connu.

En outre, l'évolution de la cybermenace, passant d'une menace financière à une menace géopolitique, est extrêmement préoccupante. Les pays occidentaux sont confrontés à une menace dans le cyberespace qui dépasse le danger des attaques physiques. Ces cybermenaces peuvent avoir de graves conséquences directes, par exemple sur notre distribution d'électricité, nos systèmes bancaires ou la disponibilité de tous les services en ligne. En signalant sans cesse des cyberincidents, même de moindre gravité, l'on risque de saper la confiance de la population dans l'environnement et les services numériques, avec de potentielles conséquences néfastes pour l'économie.

La cybermenace peut être utilisée dans le cadre de la menace hybride pour amplifier les effets d'autres méthodes d'attaque. En cas de menace, la combinaison, par exemple, d'une attaque physique et d'une série de cyberattaques peut sérieusement augmenter l'impact et semer temporairement une atmosphère de chaos.

Cette stratégie fixe les objectifs nationaux pour la période 2021-2025 pour faire face à l'évolution constante du cyberespace. Afin que les bonnes priorités soient posées à l'heure d'élaborer ces objectifs, il est nécessaire d'avoir une vision claire des différents risques et cybermenaces auxquels la Belgique peut être confrontée durant cette période. Ce chapitre donne un aperçu concis des principaux acteurs de la menace et des risques technologiques.

Toutefois, il convient de noter que l'évaluation des risques est un processus continu. Des plateformes de concertation appropriées, telles que le

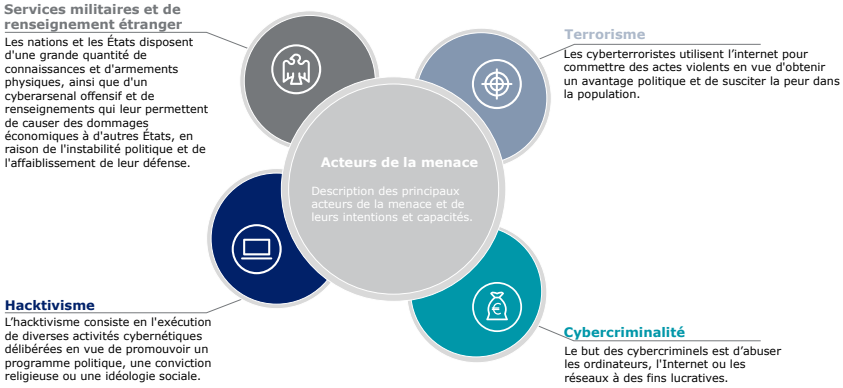
Comité de coordination du renseignement et de la sécurité et sa plateforme 4 Cyber, devront donc continuer à évaluer les mesures prises, à suivre les tendances de la cybercriminalité et à ajuster les objectifs si nécessaire. La préparation d'une contribution belge à l'analyse de risque européenne 5G en 2019 en est un exemple.

En outre, dans le cadre du suivi de l'évaluation nationale des risques 2018-2023, le Centre de crise national prévoit une analyse plus approfondie des principaux groupes à risques (dont le cyberespace fait partie) avec l'ensemble des acteurs concernés. Son objectif est de mieux identifier les causes et les conséquences sous-jacentes afin de fournir une vue d'ensemble claire aux décideurs.

Enfin, certains événements comportant un cyberrisque accru (sommets internationaux, élections, etc.) sont régulièrement organisés sur le territoire belge. Pour ce type d'événement, il peut s'avérer nécessaire de procéder à une évaluation des risques exceptionnelle afin d'identifier les risques accrus et de recommander des mesures appropriées.

2.1 Acteurs de la menace

Vu que les motivations et les capacités des acteurs de la menace changent constamment, il est crucial de comprendre qui en sont les principaux représentants et de les surveiller. Cela permet également d'appréhender le futur développement du cyberespace. La Belgique considère que les acteurs suivants sont ceux qui représentent la plus grande menace pour l'État belge et la population: les hacktivistes, les cybercriminels, les services militaires et de renseignement étrangers et les groupements terroristes.



2.1.1 Cybercriminalité

Ces dernières années, l'impact (potentiel) des cybermenaces émanant de cybercriminels est devenu chaque jour de plus en plus évident. Ces menaces sont non seulement capables de perturber notre cyberinfrastructure, elles détruisent également l'intégrité, la disponibilité et la confidentialité des informations que nous enregistrons, analysons et échangeons sous forme numérique. La numérisation d'objets ou de biens (*Internet of Things*) implique qu'ils sont " piratables », avec un impact direct sur la sécurité générale de chaque citoyen. Mais cela signifie aussi qu'elles peuvent générer des indices numériques susceptibles de s'avérer utiles dans le cadre des enquêtes criminelles.

L'objectif premier des cybercriminels, tant à titre individuel que dans le contexte de la criminalité organisée, est souvent de générer de l'argent et des profits, par exemple via le phishing, le vol de données ou le ransomware. Dans d'autres cas, ils peuvent également nourrir des ambitions plus destructrices, comme le sabotage de données ou les cyberattaques. Les cybercriminels peuvent également se spécialiser dans des services spécifiques qu'ils proposent ensuite contre paiement sur le *Dark Web*. Un criminel peut, par exemple, s'abonner à un exploit kit qui lui permet d'utiliser les méthodes d'intrusion numériques les plus récentes sans aucune connaissance technique.

Ainsi, les cybercriminels offrent leurs services à quiconque veut bien les payer. Outre le cyberterrorisme, les organisations criminelles (ou les

individus) qui souhaitent causer des dommages matériels et/ou physiques devraient donc également être pris en compte comme acteurs potentiels de la menace au niveau national. Après tout, l'impact potentiel des cyberattaques sur les infrastructures critiques peut être de nature telle que la stabilité des institutions publiques est mise sous pression.

2.1.2 Services militaires et de renseignement étrangers

Les nations et les états disposent d'une grande quantité de connaissances et d'armements physiques, ainsi que d'un cyberarsenal offensif. Cependant, il est toujours possible qu'ils souhaitent les affecter à d'autres fins que la protection de leurs propres citoyens. C'est ainsi que les services militaires et les services de renseignement peuvent utiliser ces connaissances et ces armements pour causer des dommages économiques à d'autres États, pour provoquer l'instabilité politique et/ou pour affaiblir leur défense. Les services militaires et de renseignement étrangers ne se livrent pas seulement à des cyberattaques pour obtenir un avantage concurrentiel dans le domaine du renseignement: de plus en plus de techniques avancées sont utilisées pour perturber le fonctionnement des organisations - et indirectement aussi des pays dans lesquels elles se trouvent – par exemple, en divulguant des informations confidentielles.

Les capacités des divers services militaires et de renseignement nationaux sont de plus en plus sophistiquées. C'est pourquoi, il devient de plus en plus difficile de détecter et de prévenir de telles cyberattaques. En conséquence, l'activité réelle de ces acteurs de la menace est beaucoup plus importante que ne le montrent les statistiques.

2.1.3 Hacktivisme

L'hacktivisme consiste en l'exécution de diverses cyberactivités délibérées en vue de promouvoir un programme politique, une conviction religieuse ou une idéologie sociale. Un mouvement politique peut par exemple mener ce type d'activités. Les méthodes d'attaque les plus couramment utilisées à l'heure actuelle sont *Doxing*[2], *DDoS*[3], le *Web defacement*[4], et la prise de contrôle illégale des identités et des canaux de médias sociaux.

2 *Doxing : le terme Doxing désigne la diffusion publique généralement illégale d'informations ou de documents provenant d'une personne.*
3 *DDoS est l'abréviation anglaise de « distributed-denial-of-service » ; il s'agit d'attaques dans lesquelles un grand volume de données est envoyé à un système spécifique afin de perturber son fonctionnement normal.*
4 *Web defacement : une dégradation de site ou de page Internet qui consiste en la modification non autorisée de son contenu.*

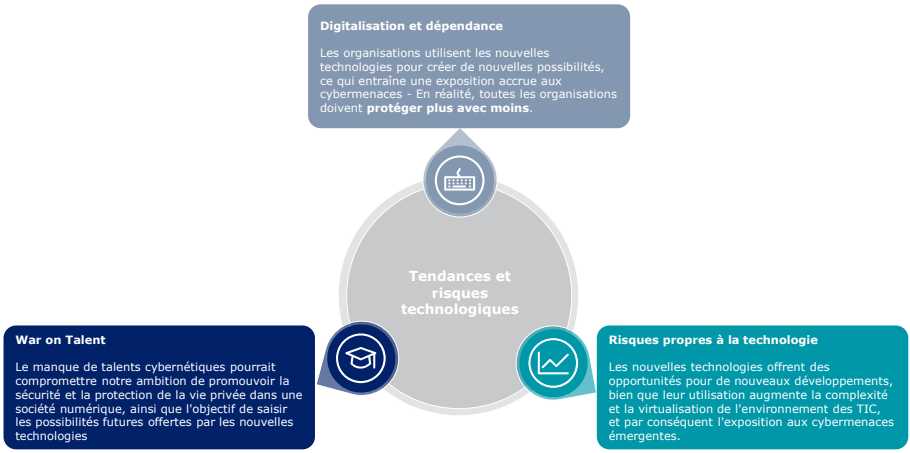
2.1.4 Terrorisme

Le cyberterrorisme couvre l'exercice d'activités violentes par le biais d'internet, dans le but sous-jacent d'obtenir un avantage politique par l'intimidation et l'incitation à la peur. Ces actes peuvent entraîner la destruction, la perte de vies humaines et/ou des dommages physiques. Les cibles les plus évidentes des cyberterroristes sont les services publics, les industries, les infrastructures critiques, etc.

Par exemple, certains groupes terroristes utilisent l'internet comme principal canal de propagande et de recrutement. Depuis 2016, l'utilisation de Twitter et de Facebook est toutefois clairement délaissée au profit de canaux de communication plus chiffrés. Les derniers développements font également apparaître une utilisation croissante de cyberoutils pour le financement du terrorisme, par exemple par le biais de ransomware, des techniques de cryptomining ou même de crowdfunding. Dans ce contexte, on craint sérieusement que les organisations terroristes ne multiplient leurs cyberattaques. Cependant, il semble que ces techniques d'attaque restent assez limitées. Pour l'exécution d'attaques DDOS, les groupes achètent toujours des services d'hébergement de domaines, téléchargent des logiciels et louent des botnets, au lieu de développer leurs propres cyberarmes.

2.2 Tendances et risques technologiques

Le paysage technologique évolue et de plus en plus de nouveaux produits ne cessent d'affluer sur le marché. Les organisations utilisent ces nouvelles technologies pour maintenir leur compétitivité et développer de nouvelles opportunités. Toutefois, ces évolutions technologiques comportent des risques, notamment parce qu'elles contribuent à développer de nouvelles opportunités pour les acteurs de la menace. Il est donc essentiel d'être toujours au courant de l'évolution des technologies et d'être conscient des risques y associés.



2.2.1 Dépendance

Les organisations utilisent les nouvelles technologies pour créer de nouvelles possibilités et accroître leur productivité ou leur efficacité. En utilisant de manière accrue ces technologies, elles deviennent de plus en plus dépendantes des TIC et, de ce fait, de plus en plus exposées aux cybermenaces. On peut également observer de manière générale que l'adoption des technologies augmente plus vite que leur sécurisation.

En effet, les organisations se concentreront davantage sur la fourniture et l'utilisation des nouvelles technologies plutôt que sur l'allocation de budgets à leur sécurité. L'on oublie souvent que les nouvelles technologies ne sont pas d'emblée soumises à des tests approfondis. Il est donc très risqué de supposer qu'elles ne seront pas la cible d'attaques ou qu'il est sûr d'implémenter et de sécuriser la technologie selon les méthodes habituelles. Après tout, il faut souvent plusieurs mois ou années avant que la plupart des attaques et des vecteurs sur une technologie particulière ne deviennent publics et qu'elle ne soit correctement sécurisée. Le *Secure Development* - en mettant l'accent sur la sécurité – devrait donc être inclus dans le processus de développement de nouveaux logiciels et de nouvelles technologies.

A chaque étape du processus de développement, de production, de maintenance et de traitement, l'on relève aussi de plus en plus de dépendance à des *Third Party Providers*. Cela augmente le risque et l'impact critique potentiel des *supply chain attacks*.
L'interconnexion des produits peut également conduire à une *hazardisation*.

C'est la situation qui se présente lorsqu'un produit est sûr au moment où il est acquis par un consommateur, mais devient dangereux une fois connecté à un réseau en raison de modifications malveillantes, incorrectes ou négligentes du code opérationnel.

2.2.2 Risques propres à la technologie

Les nouvelles applications issues des technologies émergentes offrent souvent des avantages significatifs par rapport aux méthodes traditionnelles, par exemple en termes d'efficacité et d'économies d'échelle. Cependant, elles génèrent aussi des risques de sécurité spécifiques.

Le *Cloud Computing* en est un bon exemple. L'avantage majeur est que l'infrastructure n'a plus besoin d'être entretenue et que l'évolution suit le rythme de croissance de l'organisation. Une infrastructure Cloud centrale peut dès lors être adéquatement sécurisée de manière professionnelle. Cependant, demeure le risque que l'accès non autorisé mette en péril soudainement une très grande quantité d'informations.

Deux menaces économiques doivent à cet égard être épinglées. Premièrement, le monde des applications basées sur le cloud se caractérise par la présence d'un nombre limité d'acteurs internationaux, avec des économies d'échelle qui peuvent être exploitées, entraînant un risque de concentration. Deuxièmement, ce sont souvent de nouveaux acteurs beaucoup plus petits qui proposent les innovations sur ce marché. Et ces jeunes organisations ne sont souvent pas au même niveau en termes de performance et de maturité des processus, ce qui peut créer à tort de la confiance dans ces applications.

Le développement technologique sans cesse croissant de nouveaux (types de) produits et services basés sur les TIC dans de nombreux secteurs économiques exige également une évolution rapide des autorités de surveillance en matière de surveillance du marché et de capacités d'inspection. En revanche, il faut reconnaître que ces technologies offrent parfois aussi des avantages pour développer plus efficacement la surveillance du marché.

Les autorités accordent déjà beaucoup d'attention aux aspects personnels de la sécurité et de la protection de la vie privée. Par contre, les autorités de surveillance ne couvrent pas encore ou peu les aspects liés aux produits de ces thèmes, comme la réglementation et le contrôle. Il est donc nécessaire d'adapter le cadre juridique existant. L'idéal serait d'intégrer ces aspects dans un cadre européen/international. Le *Cybersecurity Act*

européen constitue un pas important dans cette direction et nécessite une implémentation belge claire.

La protection individuelle des appareils connectés à Internet figure aussi parmi les risques courants. Le plus grand défi récent dans ce domaine est l'Internet des objets (IoT).

Il est primordial d'évaluer les risques et de mettre en place la sécurité nécessaire avant d'utiliser les nouvelles technologies. Vu la vitesse de développement et d'adoption de nouvelles technologies comme l'intelligence artificielle, le *Quantum Computing*, le *Blockchain* et les *Smart Meters&Grids*, l'enjeu réside dans l'évaluation appropriée de l'ensemble des risques (et la protection contre ces risques).

2.2.3 War On Talent

La transformation numérique et l'application des nouvelles technologies se sont traduites par une recrudescence des abus de ces systèmes. C'est pourquoi il est important pour une organisation d'investir dans le recrutement de profils informatiques et de profils de sécurité informatique. Or, le marché du travail souffre d'une pénurie de talents en cybersécurité. Les formations qui consacrent une part (importante) à la cybersécurité se font rares. Cette matière est souvent enseignée à titre optionnel, de sorte qu'en pratique, peu de connaissances sont acquises ou transférées à ce sujet.

Résultat: les professionnels de la cybersécurité sont une profession en pénurie. Nombreuses seront dès lors les organisations qui ne seront pas en mesure de pourvoir ces postes ou qui les remplaceront par d'autres profils. De plus, engager des profils non compétents ne ferait qu'augmenter la menace interne (" *insider threat* »).

3. Objectifs stratégiques et approche

La conception d'une cyberstratégie a pour ambition de répondre aux évolutions technologiques et au besoin criant de protéger la population, le secteur privé et public et les secteurs vitaux. La cyberstratégie 2.0 comporte six objectifs stratégiques pour les quatre prochaines années. Cette stratégie énonce un certain nombre de mesures pour réaliser ces objectifs stratégiques. C'est en partie grâce à l'aide de diverses parties prenantes qu'ils pourront être atteints.

3.1 Renforcer l'environnement numérique et accroître la confiance dans l'environnement numérique

3.1.1 Investir dans une infrastructure réseau sécurisée

En collaboration avec les fournisseurs d'accès internet (FAI), nous œuvrerons à une infrastructure réseau de base plus sûre. De nouvelles techniques de protection suivront les évolutions technologiques telles que l'" Internet of Things » (IoT) et les nouvelles générations de réseaux fixes et mobiles.

La sécurité de l'infrastructure réseau peut être améliorée par la mise en œuvre de normes Internet plus sûres (sécurité DNS, routage sécurisé, cryptage, etc.). Ces normes offrent un moyen sûr d'échanger des données (« safe data transport layer »). Tout le processus d'échange de données en ligne se retrouverait alors sécurisé limitant ainsi le risque d'attaque à l'encontre d'un maillon faible de la chaîne.

De telles normes peuvent également fournir des identités et des publications plus fiables sur l'internet. Cela peut être fait, par exemple, en encourageant l'utilisation de technologies telles que Itsme et Extended Validation Certificates sur les sites web.

Une autre piste est de développer un environnement d'essai (" testbed ») pour l'infrastructure. Un " *testbed* » est une plateforme qui permet de tester une nouvelle infrastructure dans un environnement fiable, contrôlé et sûr, avant qu'elle ne soit utilisée de tous..

3.1.2 Créer une " Cyber Green House »

La création d'une « Cyber Green House » constituera un stimulant important pour l'innovation dans le secteur de la cybersécurité. La création d'un tel centre d'innovation vise à mettre à l'essai des cybersolutions et des

modèles commerciaux novateurs dans un environnement sécurisé ainsi qu'à diffuser les " Cybersecurity Guidelines » et les " Best Practices ».

3.1.3 Stimuler l'expertise et les connaissances

Pour répondre au besoin d'une sécurité accrue et à la demande en professionnels de la sécurité, il est inévitable d'investir davantage dans l'expertise et les connaissances. La contribution des établissements d'enseignement dans le domaine de la cybersécurité n'est pas négligeable. D'une part, ils jouent un rôle considérable dans l'amélioration des connaissances en menant des recherches et d'autre part, ils contribuent à l'élaboration et à l'organisation de formations pertinentes.

Les investissements consacrés à la recherche et au développement (R&D) dans le domaine de la cybersécurité seront poursuivis. Le secteur privé et les établissements d'enseignement comme les universités et les hautes écoles travailleront en étroite collaboration.

Les initiatives européennes dans ce contexte seront évaluées à la lumière de cet objectif.

Les responsables de la sécurité des institutions publiques doivent être formés à un niveau de sécurité adéquat au moyen de programmes de formation destinés aux agents de l'État.

Afin de remédier au manque de professionnels de la sécurité de l'information, tant dans le secteur public que dans le secteur privé, il faudrait encourager davantage de jeunes à suivre les filières STEM (Science, Technology, Engineering and Mathematics). Cela nécessite d'établir des contacts avec les communautés et de définir une politique cohérente en la matière, en coopération avec les partenaires concernés. Cette politique peut par exemple consister à fournir du matériel de sensibilisation aux écoles ou à organiser des programmes de tutorat.

3.1.4 Certification en cybersécurité et labelling des produits, services et processus

La Belgique créera un cadre permettant aux entreprises d'évaluer et de certifier la sécurité des produits, services et processus TIC.

Ce cadre sera mis en conformité avec le règlement européen de 2019 sur la cybersécurité (Cybersecurity Act) et avec les développements en cours au niveau européen. Le Cybersecurity Act vise une reconnaissance européenne

des certificats délivrés, ainsi qu'une harmonisation maximale avec les cadres de référence européens et internationaux existants.

À cette fin, la Belgique mettra en place une " National Cybersecurity Certification Authority » (NCCA), comme l'exige le Cybersecurity Act. En concertation avec entre autres les autorités de contrôle de marché, d'autres autorités sectorielles et le NCCN, cette NCCA coordonnera l'expertise nécessaire en matière de certification de la cybersécurité, octroiera les certificats comportant des exigences élevées en matière de sécurité et établira une coopération étroite avec BELAC (l'organisme belge d'accréditation) en exploitant au maximum les processus, procédures et réglementations existants.

Un mécanisme d'accréditation en matière de cybersécurité sera également mis au point pour les entreprises, en particulier les PME, qui souhaitent démontrer que les exigences de base, les meilleures pratiques et les politiques en matière de cybersécurité sont un minimum respectées. Il est également important de se pencher sur une approche intégrée pour les secteurs stratégiques qui combine les aspects informatiques, la protection physique et le screening du personnel.

Ces initiatives appuient fortement la vision de cette stratégie de cybersécurité et renforceront la confiance des clients dans la sécurité de l'environnement numérique.

3.1.5 Renforcer les cybercompétences des services de renseignement et de sécurité

Afin de répondre de manière appropriée à la menace qui s'accroît rapidement, les capacités et les compétences de nos services de renseignement et de sécurité doivent au moins évoluer au même rythme que cette menace. Le capital humain des experts techniques en cybersécurité est la meilleure arme contre ces nouvelles menaces au niveau national.

Afin de fournir à nos services les experts nécessaires, d'autres méthodes de recrutement et d'emploi seront, dans la mesure du possible, évaluées et utilisées. Après tout, nos services de sécurité ne sont pas les seuls à avoir besoin de jeunes experts de l'informatique hautement qualifiés. La « guerre des talents » fait rage entre les entreprises spécialisées, les grandes multinationales, ainsi que tous les services de sécurité en Europe et au-delà. Dans l'idée d'élargir leurs connaissances, ces experts techniques se mettent souvent en quête de nouveaux défis et ne cherchent généralement

pas à occuper le même emploi toute leur vie. Un système de recrutement suffisamment flexible et une rémunération plus compétitive devraient permettre à nos services de sécurité de faire face de manière plus saine à une telle concurrence avec le reste du marché du travail.

En outre, les pouvoirs publics doivent offrir à leurs experts techniques en cybersécurité suffisamment de formations techniques de haute qualité, formations qui auront un effet motivateur non négligeable et offriront une garantie de connaissances techniques et d'expertise suffisantes.

3.2 Armer les utilisateurs et les administrateurs d'ordinateurs et de réseaux

L'Internet se compose d'infrastructures et de systèmes qui sont presque tous entre les mains de propriétaires privés. Il est donc très important que chaque propriétaire d'un système ou d'un réseau informatique soit suffisamment armé pour le protéger contre les cybermenaces et autres cyberattaques.

3.2.1 Sensibilisation et implication

En plus d'informer les citoyens quant aux menaces possibles, les pouvoirs publics s'efforcent de davantage les sensibiliser à la façon de mieux se protéger contre les éventuels cyberrisques.

La protection des systèmes et des réseaux informatiques nécessite d'une part, des mesures techniques de protection et d'autre part, que chaque utilisateur fasse preuve de responsabilité. Les personnes suffisamment conscientes et vigilantes deviennent rapidement le meilleur système de détection des cyberattaques. Le site Internet www.safeonweb.be fournit au public toutes les informations sur les menaces spécifiques, sur la manière de les reconnaître, de s'en prémunir ou de réagir.

L'Internet appartient à tout le monde et est accessible à tout un chacun. Sa sécurité est donc également le fruit d'un effort commun. C'est pourquoi la population est encouragée à prendre part à la sécurisation. Par exemple, tout un chacun peut envoyer les e-mails considérés suspects à suspect@safeonweb.be. De telles initiatives seront élargies.

Le CCB organise une campagne annuelle de sensibilisation dans les médias. Celle-ci s'inscrit dans le cadre des initiatives européennes. L'agence

européenne ENISA organise également chaque année en octobre le Mois européen de la cybersécurité.

Le CCB veillera à faciliter les contacts entre les citoyens et les prestataires de services en cybersécurité de qualité dans notre pays. Cette facilitation devrait permettre aux citoyens de faire face aux incidents de sécurité et de neutraliser les problèmes.

La sensibilisation du public a également un impact direct au sein des entreprises et crée une culture générale de préoccupation et de sécurité. Il y a lieu de continuer à miser sur les campagnes de sensibilisation, telles que les webinaires, les guides ou kits de cybersécurité.

3.2.2 Information sur les menaces et les vulnérabilités

La mise en garde opportune contre les menaces ou vulnérabilités émergentes graves est cruciale.

Le CCB analyse en permanence toutes les informations disponibles sur les cybermenaces ou les vulnérabilités et envoie, le cas échéant, les alertes nécessaires. Le CCB communique également constamment sur ses réseaux sociaux (Facebook, Twitter) toutes les informations utiles à la population. Il entretient également une relation directe et transparente avec les principaux médias nationaux. En outre, BE-Alert du Centre de crise national (NCCN) peut soutenir la diffusion d'alertes et les envoyer dans une région spécifique.

Les entreprises et les organisations sont encouragées à publier une " politique coordonnée de divulgation des vulnérabilités » (*Coordinated Vulnerability Disclosure Policy*). Par l'intermédiaire des autorités sectorielles, des organisations professionnelles et de la Cyber Security Coalition Belgium, elles seront tenues informées des menaces ou vulnérabilités graves. Les Organisations d'Intérêt Vital recevront également des alertes ciblées et non publiques par le biais de l'" Early Warning System » (EWS) du CCB.

En collaboration avec la " *Computer Emergency Response Team* » nationale (CERT.be) et en tant que CSIRT nationale (« Computer Security Incident Response Team »), le CCB est chargé de détecter et d'analyser les problèmes de sécurité en ligne et les vulnérabilités et d'en informer les utilisateurs. Toutefois, cela ne peut se faire sans le soutien des fournisseurs de services Internet qui doivent rapidement transmettre les alertes à leurs clients vulnérables ou en danger.

3.2.3 Diffusion des directives et des meilleures pratiques en matière de cybersécurité

Les cybermenaces et les techniques d'attaque utilisées évoluent très rapidement. Le partage des connaissances et des meilleures pratiques est dès lors très précieux. Ce partage enrichit les connaissances et génère de nouvelles idées pour faire face aux menaces, tout en facilitant la prise de décision. Le partage des connaissances en matière de cybersécurité se fait via des plateformes existantes ou futures.

Le CCB tient à jour un guide de référence en ligne sur la cybersécurité afin d'aider les organisations à élaborer une stratégie en matière de cybersécurité. Le guide fournit des " recommandations de base » ainsi que des " recommandations plus avancées » en termes de planification, de gestion des risques, de mesures de sécurité et d'évaluations dans le domaine de l'utilisation des ordinateurs et des réseaux informatiques. L'identification et la gestion des risques sont dès lors cruciales à cet égard. Les directives proposées sont fondées sur des normes internationales et sont continuellement mises à jour par le CCB. Les entreprises sont donc vivement encouragées à appliquer ces directives dans leurs politiques de cybersécurité.

3.3 Protéger les Organisations d'Intérêt Vital contre toutes les cybermenaces

Aux quatre coins du globe, les Organisations d'Intérêt Vital sont confrontées à des cybermenaces de plus en plus fortes et sophistiquées. Étant donné que les cyberattaques contre ces organisations peuvent avoir un impact significatif sur notre société et sur la sécurité nationale, il est crucial de les soutenir dans leur protection de manière adéquate.

3.3.1 Optimiser l'échange d'informations et envoyer des alertes

En tant qu'autorité nationale chargée de la cybersécurité, le CCB reçoit de ses partenaires toutes les informations pertinentes concernant les menaces. Il analyse en permanence les informations reçues et envoie des alertes via son " Early Warning System » (EWS) ou d'autres canaux.
Ainsi, les Organisations d'Intérêt Vital seront informées en permanence des menaces, vulnérabilités ou incidents en matière de cybersécurité pertinents (via l'« Early Warning System » – EWS – du CCB).

En Belgique, les autorités sectorielles ont une responsabilité cruciale dans

l'identification, la régulation et le contrôle des Organisations d'Intérêt Vital. Une plateforme de concertation qui réunit les autorités sectorielles en matière de cybersécurité (" Cyber Security Sectoral Authorities Platform » ou CySSAP) est conçue pour aider à optimiser la gestion des échanges d'informations avec les Organisations d'Intérêt Vital, y compris dans le contexte des dépendances transfrontalières.

3.3.2 Améliorer la protection des institutions internationales

La Belgique héberge un grand nombre d'institutions internationales, dont l'OTAN (Organisation du Traité de l'Atlantique Nord) et des institutions de l'Union européenne. Les Organisations d'Intérêt Vital belges qui soutiennent ces institutions seront identifiées afin d'en assurer une protection appropriée.

En outre, un dialogue et une coopération de qualité avec les institutions internationales de notre pays sont primordiaux et nécessaires si l'on entend accroître l'efficacité de la protection et de la réponse aux cyberattaques.

3.3.3 Traiter les incidents aux répercussions nationales

L'opérationnalisation du Cyberplan d'urgence national sera poursuivie. Une coopération optimale entre la *Computer Emergency Response Team* nationale (CERT.be) du CCB, les services de police intégrés et le Centre de crise national (NCCN), permettra de traiter rapidement et efficacement les incidents et d'amorcer immédiatement l'enquête juridique.

Les incidents aux répercussions nationales sont portés au niveau approprié et traités par des " Rapid Reaction Teams » *ad hoc*, qui font également intervenir efficacement d'autres services et partenaires.

3.3.4 Exercices

Approuvé par le Conseil des ministres en 2017, le Cyberplan d'urgence national décrit les procédures que les différents services doivent suivre en cas de cyberévénement. Ce plan doit faire l'objet d'une évaluation chaque année et être ajusté si nécessaire. Dans ce cadre, le CCB joue un rôle de coordination. La tenue régulière d'exercices revêt dès lors une importance non négligeable si l'on entend renforcer la résilience face aux incidents et tester l'efficacité du plan d'urgence. Les leçons tirées de ces exercices peuvent ensuite alimenter les évaluations annuelles de ce plan.

La participation des services de sécurité belges, d'autres services publics et d'Organisations d'Intérêt Vital aux exercices internationaux et nationaux

est donc hautement souhaitable. La coordination de la participation belge à ces exercices est assurée par une concertation entre le CCB, le SPF Affaires étrangères, le NCCN et la Défense.

3.4 Répondre à la cybermenace

Pour lutter rapidement contre la cybercriminalité croissante et les menaces à l'encontre des autorités, il convient d'investir dans l'identification rapide des menaces qui pèsent sur notre population, notre économie ou les Organisations d'Intérêt Vital.

3.4.1 Répertorier la menace internationale

Il est essentiel de surveiller et d'évaluer en permanence la cybermenace internationale afin de limiter les risques de cyberattaques et de cyberincidents. C'est la première mesure à prendre pour toute défense.

Il importe d'identifier les cyberintentions et les capacités des " acteurs » face à nos intérêts essentiels et vitaux ainsi que de suivre de près les sources potentielles. Afin de protéger nos réseaux informatiques, il est indispensable de connaître au mieux l'évolution de leurs tactiques, techniques et procédures et d'évaluer nos moyens de protection en fonction.

3.4.2 Perturber les cyberinfrastructures des criminels

Les cybercriminels se spécialisent et réutilisent les techniques et logiciels d'attaque qui circulent sur le Dark Web. Afin de pouvoir mener à bien leurs cyberattaques de haute technologie ou à grande échelle et de rester anonymes, ils utilisent leurs propres systèmes informatiques ainsi que des systèmes informatiques compromis qu'ils trouvent sur Internet.

C'est en perturbant les cyberinfrastructures des criminels que l'on mettra partiellement en péril leur *business model,* notamment au moyen de:

- la détection et la neutralisation par la voie juridique des infrastructures ;
- la détection de systèmes compromis et la notification au propriétaire ;
- la protection de la communication de la population et des entreprises contre les infrastructures malveillantes connues ;

- le partage national et international des informations.

Cette perturbation sera impossible si tous les services de renseignement et de sécurité ne coopèrent pas étroitement.

3.4.3 Développer une capacité répressive appropriée

Pour réduire la vulnérabilité de la Belgique dans le cyberespace, il est indispensable de prendre des mesures préventives. Des citoyens, des entreprises et des autorités bien informés et résilients repousseront les cybercriminels et les décourageront pour l'avenir. Les investissements dans la prévention permettent de réduire l'afflux de dossiers pénaux, grâce à quoi la police et la justice ne devront plus seulement se borner à combattre les symptômes et seront en mesure de s'attaquer aux causes profondes.

Dans le même temps, il est clair que la cybercriminalité continuera d'exister. Il demeure dès lors capital de développer un système de répression performant pour s'attaquer au mieux à la catégorie résiduelle des délits informatiques. Les auteurs de délits informatiques doivent être identifiés et arrêtés et les preuves de leur participation recueillies. Comme indiqué plus haut, l'infrastructure criminelle doit être identifiée et démantelée, les avoirs illicites saisis et confisqués et les suspects poursuivis et punis correctement. Les cybercriminels opérant typiquement dans un contexte international, il s'agit également de veiller à une coordination de qualité avec d'autres pays concernés.

Ce plan stratégique a pour ambition de soutenir le développement d'une capacité répressive appropriée. Cette capacité répressive doit être en mesure de détecter, de rechercher, de poursuivre et de sanctionner la cybercriminalité de manière adéquate et experte.

Le premier objectif consiste ici à mettre en place les capacités et l'expertise appropriées à tous les niveaux de la police intégrée (tant la police locale que les services déconcentrés et centraux de la police fédérale) afin que les capacités d'imagerie et d'enquête attendues à chaque niveau puissent être déployées efficacement et rapidement dans un environnement numérique.

Il s'agit ensuite de veiller à ce que les parquets et les tribunaux de tous les arrondissements et ressorts judiciaires disposent d'un nombre suffisant de procureurs, de magistrats instructeurs et de magistrats du siège intéressés par la cybersécurité et la cybercriminalité et que ceux-ci suivent une formation coordonnée. Ces magistrats recevront le soutien de réseaux

internes spécialisés où ils pourront échanger et discuter au sujet de leurs expériences, problèmes et meilleures pratiques. Une politique pénale élaborée dans le domaine du cyberespace viendra encadrer les activités de recherche et de poursuite de la justice.

3.4.4 Développer une capacité de défense appropriée

Internet devient de plus en plus une cible et un outil dans les conflits internationaux.

Tous les chefs d'État et de gouvernement de l'OTAN ont déclaré que le cyberespace devait être considéré comme un nouveau domaine opérationnel (outre les domaines terrestre, aérien et maritime traditionnels) dans lequel des opérations militaires et de renseignement peuvent être menées.

Les opposants saisissent toutes les occasions qui se présentent dans le cyberespace et au moyen du cyberespace pour renforcer leur position d'information, pour perturber nos systèmes civils et militaires et pour saper la confiance en les informations qui soutiennent nos opérations. La poursuite du développement des capacités cyber au sein du Service Général de Renseignement et de la Sécurité (SGRS) et de la Défense est donc l'une des priorités de la note de politique générale de la ministre de la Défense et du plan stratégique de la Défense. À terme, elle devrait également conduire à la création d'une cinquième composante qui se concentrera spécifiquement sur la cybermenace. L'objectif est double: une meilleure compréhension et une meilleure protection contre la cybermenace, ainsi qu'une meilleure compréhension des opportunités. La cyberstratégie de la Défense énonce ces objectifs en termes concrets. En plus de la réponse aux cybermenaces, cette capacité pourra fournir un soutien important à la société en cas de crise (hybride).

3.4.5 Attribution

L'identification et l'attribution d'une cyberattaque à une personne, un groupe ou un État en particulier jouent un rôle de plus en plus important dans la politique mondiale. La discussion sur la nécessité et l'éventualité d'une coordination internationale de l'attribution d'une cyberattaque constitue l'une des priorités internationales de l'OTAN, de l'UE et de l'ONU. Cependant, l'attribution demeure une décision politique et souveraine qui a un impact majeur sur la politique étrangère. Toute attribution éventuelle fera dès lors l'objet d'une analyse approfondie et sera décidée au moyen

d'une procédure nationale coordonnée. Ici aussi, le renforcement des capacités s'avère crucial.

3.5 Améliorer les collaborations publiques, privées et universitaires

Lorsqu'il s'agit de prévention, de réduction, de traitement et de surveillance des cybermenaces et des cyberincidents, la coopération entre les acteurs concernés, tant au niveau national qu'international, est un facteur de succès non négligeable.

3.5.1 Promouvoir la coordination et la collaboration

Chaque acteur qui joue un rôle dans la cybersécurité en Belgique endosse des responsabilités spécifiques. Cependant, il est crucial de coordonner toutes les initiatives de manière centralisée. Le CCB, en tant qu'autorité nationale, assure la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique.

Les connaissances en matière de cybersécurité et l'évolution de la cybermenace sont partagées via des plateformes existantes ou nouvelles entre les services de sécurité concernés, les pouvoirs publics, le secteur privé et le secteur scientifique. Les experts partagent des informations et des expériences *de visu* et nouent des contacts à l'occasion de réunions périodiques. Le dialogue ouvert et structurel devrait permettre au CCB de mieux comprendre les besoins les plus pressants de notre société.

3.5.2 Soutenir la Cyber Security Coalition

La Cyber Security Coalition est un partenariat unique au sein duquel des acteurs du monde universitaire, des pouvoirs publics et du secteur privé unissent leurs forces dans le domaine de la cybersécurité. En 2021, plus de 100 organisations clés de trois secteurs étaient membres actifs et contribuaient à la mission et aux objectifs de la coalition.

La coalition répond au besoin urgent de coopération intersectorielle afin de:
- partager les connaissances et l'expérience ;
- lancer, organiser et coordonner des initiatives intersectorielles concrètes ;
- sensibiliser les citoyens et les organisations ;
- promouvoir le développement de l'expertise ;
- formuler des recommandations en faveur de politiques et d'une réglementation plus efficaces.

Les autorités, et le CCB en particulier, soutiendront activement la Cyber Security Coalition et y joueront un rôle concret.

3.6 Un engagement international clair

La cybermenace est d'envergure mondiale et ne peut être combattue au seul niveau national. La coopération internationale représente un pilier primordial d'une politique nationale forte en matière de cybersécurité. La cybersécurité doit s'articuler autour d'une perspective holistique qui s'applique aux différents vecteurs de la coopération internationale (diplomatique, militaire, économique, etc.). Il est donc indispensable que les différentes autorités concernées travaillent en étroites collaboration et concertation et ce, dans le respect de leurs compétences respectives.

La Belgique soutient le rôle législatif et diplomatique de l'UE, de l'OTAN et d'autres organisations internationales pertinentes dans leur contribution à créer un cyberespace ouvert, libre et sûr et y participera activement dans la mesure du possible. Une attention particulière est accordée à l'ENISA, l'agence pour la cybersécurité en Europe. Depuis sa création en 2004, l'ENISA a développé une culture générale et une sensibilisation à la sécurité des réseaux et des informations au sein de l'Union. Le CCB continuera à représenter la Belgique dans les différents organes et plateformes de l'ENISA.

La coopération bilatérale entre toutes les autorités compétentes en Belgique et leurs homologues étrangers permettra également d'optimiser la coopération internationale et de renforcer la confiance mutuelle.

4. Responsabilités

La collaboration et le partage des responsabilités sont des facteurs de succès critiques dans le développement d'une cybersécurité efficace. La défense de l'environnement numérique en Belgique contre les menaces (émergentes) ne relève pas de la seule responsabilité des autorités. Les autres acteurs peuvent également apporter une contribution pertinente aux différents objectifs et plans d'action connexes, notamment les citoyens, les entreprises et les Organisations d'Intérêt Vital.

À l'instar du monde réel, il est de la responsabilité de chaque propriétaire d'un système de TIC de le sécuriser correctement, ainsi que de le gérer et de l'utiliser de manière responsable. Chaque citoyen doit être informé et sensibilisé à propos des principaux risques liés à l'utilisation des TIC et d'Internet et se doit de tenir compte des conseils prodigués en matière de sécurité. Concrètement, cela signifie que chaque utilisateur doit veiller à la sécurité technique de ses systèmes et les utiliser de manière responsable. Les entreprises et les institutions publiques doivent protéger leur environnement et comprendre qu'elles ont des responsabilités si elles sont victimes d'une cyberattaque.

4.1 Le Centre pour la Cybersécurité Belgique (CCB)

Le CCB supervise la politique belge en matière de cybersécurité, coordonne et surveille sa mise en œuvre. Par une approche intégrée et centralisée, il gère les différents projets relatifs à la cybersécurité et assure la coordination entre les services et autorités concernés mais aussi entre les autorités et le secteur privé ou le monde scientifique.

En collaboration avec le Centre de crise national, le CCB assure la gestion des crises en cas de cyberincident. Il diffuse des standards, directives et normes de sécurité pour les administrations et organismes publics.

Le CCB sensibilise la population aux principales cybermenaces et aux moyens de s'en prémunir. Des programmes spécifiques avec des entités publiques et privées doivent renforcer les compétences dans le domaine de la cybersécurité.

Le CCB a également pour mission de coordonner la représentation belge aux forums internationaux sur la cybersécurité, d'assurer le suivi des

obligations internationales et de présenter le point de vue national en la matière. Le but étant de permettre une action internationale cohérente, en étroite concertation avec le SPF Affaires étrangères et la Défense.

Le CCB présente la position belge au sein des institutions européennes, notamment en matière de certification et d'étiquetage des produits et services.

4.1.1 CERT.BE

En tant que CSIRT national (« Computer Security Incident Response Team »), le CCB endosse en outre une importante tâche de détection et d'alerte. La *Computer Emergency Response Team* (CERT.be) fait partie intégrante du CCB et a pour mission de détecter, d'observer et d'analyser les problèmes de sécurité en ligne tels que les cybermenaces, les vulnérabilités des systèmes des TIC ou les cyberincidents. Le CERT.be informera en permanence la population, les entreprises, les services publics et les Organisations d'Intérêt Vital à ce sujet. En ce sens, CERT.be est la plaque tournante de l'échange d'informations en matière de cybersécurité.

4.2 La Police fédérale

Les services de police intégrés, en coopération avec leurs partenaires, sont chargés de lutter contre la criminalité informatique.

En tant que service de police de première ligne, la police locale représente le premier point de contact des citoyens, des entreprises et des services publics. Dans ce rôle, elle fait appel aux services spécialisés (RCCU/FCCU) en cas de besoin.

Au sein de la police fédérale judiciaire, les Computer Crime Units régionales (RCCU) et la Computer Crime Unit fédérale (FCCU) sont responsables de l'approche judiciaire de la criminalité informatique.

Les RCCU sont chargées d'apporter une assistance spécialisée dans le cadre d'enquêtes dans un environnement informatisé – principalement à l'appui de l'analyse légale du matériel informatique (PC, smartphones) – pour les dossiers relatifs à toutes sortes de phénomènes criminels et ce, tant pour la police locale que pour la police judiciaire fédérale de l'arrondissement dont elles relèvent. Elles traitent également de manière autonome l'approche judiciaire des dossiers relatifs à la criminalité informatique liée à

son fonctionnement en arrondissement. Dans ce contexte, la collecte de traces numériques est primordiale si l'on entend identifier les auteurs et les traduire en justice.

En tant que service opérationnel, la FCCU fait partie de la direction centrale de la lutte contre la criminalité grave et organisée. En plus d'un rôle d'analyse légale de soutien, principalement des services centraux, elle est chargée, en toute autonomie, du traitement judiciaire des dossiers criminels liés aux attaques contre l'infrastructure informatique des infrastructures critiques ou des secteurs vitaux. Lorsqu'il s'agit d'autres attaques complexes qui ne peuvent être liées à un arrondissement ou qui concernent plusieurs arrondissements, la FCCU joue un rôle de coordination. La FCCU intervient également comme point de contact national dans la bataille internationale contre la cybercriminalité.

4.3 Le Ministère public

Dans chaque arrondissement judiciaire, les enquêtes en général, et cela vaut aussi pour la cybercriminalité en particulier, sont menées sous la direction du procureur du Roi compétent. Celui-ci donne aux services de police intégrés et, le cas échéant, à d'autres services d'enquête, les mandats nécessaires pour collecter des indices et faire la lumière sur les faits. À l'issue de la procédure, c'est aussi le procureur du Roi qui traduira ou non en justice les cybercrimes. Le procureur du Roi dispose généralement d'un ou plusieurs magistrats de référence en matière de cybercriminalité qui se chargent en priorité des enquêtes sur les cybercrimes.

Le procureur fédéral fait partie du ministère public et il est notamment chargé de l'exercice de l'action publique pour des crimes spécifiques (par exemple terrorisme, violations du droit humanitaire, etc.). Le Parquet fédéral peut aussi se voir charger de coordonner, en concertation avec le procureur du Roi, des enquêtes pénales couvrant plusieurs ressorts ou ayant une dimension internationale. Le parquet fédéral dispose d'une Cyberunit composée de magistrats fédéraux qui se chargent en particulier des enquêtes concernant les cybercrimes. Il peut s'agir notamment de cybercrimes complexes à forte résonance internationale, commis par des réseaux criminels organisés au moyen de techniques de pointe, menaçant les infrastructures informatiques critiques nationales. Enfin, le parquet fédéral est également chargé de promouvoir la coopération opérationnelle internationale et représente le ministère public auprès d'EUROJUST et de

l'" European Judicial Cybercrime Network ». Si un cybercrime ne peut être localisé immédiatement dans un arrondissement spécifique, le parquet fédéral peut déjà ordonner les enquêtes les plus urgentes.

Le Cyberplan d'urgence fait intervenir le ministère public dans la gestion des cyberincidents et des cybercrises.

La politique pénale et le bon fonctionnement général et coordonné du ministère public sont du ressort du Collège des procureurs généraux. Ce collège peut donner des instructions contraignantes pour tous les membres du ministère public. Les procureurs généraux sont assistés par des réseaux nationaux d'expertise (REN), composés d'une multitude de partenaires pertinents. En ce qui concerne la cybercriminalité, il s'agit du REN CYBERCRIME, dont la coordination principale est assurée par le parquet général d'Anvers. En ce sens, le REN CYBERCRIME est le point de contact désigné pour les questions stratégiques.

4.4 La Défense

La Défense développe une cyberstratégie, un plan d'action et les capacités nécessaires pour appuyer les opérations militaires et de renseignement à partir du cyberespace et au sein de celui-ci. Ces investissements permettront à la Belgique de disposer de capacités techniques / technologiques à long terme lui permettant de protéger les infrastructures indispensables contre les cyberattaques et si nécessaire, de mener une contre-attaque.

La Défense disposera d'une cybercapacité technologique de haut vol pour conserver sa liberté d'action lors d'opérations militaires au sein du cyberespace et via celui-ci.

La Défense soutient en outre la politique nationale de cybersécurité par les actions suivantes:

- elle respecte loyalement des engagements pris dans le cyberplan d'urgence national;

- elle engage, si nécessaire, ses capacités en sa qualité d'expert technique pour soutenir des dossiers juridiques spécifiques ou en tant que support technique à des dossiers spécifiques du CERT.be;

- elle propose aux parties prenantes nationales un niveau d'expertise avancé en analyse des logiciels malveillants;

- elle intègre l'intelligence pertinente en matière de cybermenace à la plateforme nationale de renseignement sur la cybermenace ;

- elle assure le suivi des acteurs montrant des intentions ou risquant de mener des cyberattaques contre des structures et des intérêts vitaux nationaux;

- elle coordonne, le cas échéant en consultation avec les Affaires étrangères et le CCB, la participation belge aux exercices internationaux de cybersécurité;

- elle met à disposition l'infrastructure mil.cert comme site de back-up pour la gestion des incidents du CERT.be dans les situations de crise où l'infrastructure nationale est indisponible;

- elle engage, lors des situations de crise nationale, ses capacités intrusives et offensives pour réagir par une cyberattaque propre afin de neutraliser l'attaque et d'en identifier les auteurs.

4.5 Le Centre de crise national (NCCN)

En collaboration avec le CCB, le NCCN assure l'organisation et la coordination du Cyberplan d'urgence au niveau national. Le NCCN et le CCB sont conjointement responsables de la gestion des crises.

La gestion des conséquences directes et indirectes d'une crise sur la société demeure la prérogative du NCCN, des autorités sectorielles et des membres des autorités concernées. Le NCCN organise et gère la communication en cas de cybercrise nationale (voir Cyberplan d'urgence national).

Le service de permanence du NCCN assure 24 heures sur 24 et 7 jours sur 7 la disponibilité de CERT.be, qui fournit un soutien de première ligne en cas d'incidents et de crises nationales.

Le NCCN fournit un appui juridique et organisationnel aux autorités sectorielles pour l'identification des infrastructures critiques et des opérateurs de services essentiels. Il contribue également à la réalisation d'analyses

de cyberrisques qui peuvent perturber le fonctionnement d'organisations vitales ou de certains événements (voir chapitre 3).

Le NCCN gère la liste des Organisations d'Intérêt Vital et est responsable de la coordination du suivi et de l'adaptation des réglementations y afférent.

Enfin, le NCCN analyse en permanence les principaux risques nationaux (y compris les cyberrisques) et effectue des analyses de risques *ad hoc* lors d'occasions spéciales à haut risque, en coopération avec tous les partenaires concernés.

4.6 La Sûreté de l'État (VSSE)

Le Service pour la Sûreté de l'État (VSSE) a pour mission de collecter, d'analyser et de traiter des renseignements sur les activités qui menacent ou pourraient menacer la sécurité intérieure de l'État, la sécurité extérieure de l'État ou le potentiel scientifique et économique du pays.

Dans le cadre de ce mandat, la VSSE entretiendra les contacts appropriés avec les services des filiales étrangères et collectera les renseignements nécessaires à leur sujet. Elle partagera par ailleurs autant que possible les informations reçues avec CERT.be et les autres partenaires concernés.

4.7 Le Service public fédéral Affaires étrangères

Dans le contexte de la cybersécurité, les missions du service public fédéral Affaires étrangères de la cybersécurité peuvent être décrites comme suit:

- faire office de point de contact unique international au niveau diplomatique, tant au niveau bilatéral qu'au sein des organisations multilatérales pertinentes (y compris l'UE, l'OTAN et l'OSCE), en particulier en période de crise ;

- définir, en concertation avec les autorités belges compétentes, la représentation de la Belgique dans les négociations et dialogues internationaux ;

- informer les autorités belges compétentes des développements internationaux pertinents ;

- définir, en accord avec toutes les autorités belges concernées, une position dans les dossiers internationaux ;

- attribuer, de manière coordonnée ou non au niveau international, les cyberactivités malveillantes ;

- mettre au service des autorités compétentes (CCB) tant son expérience que l'environnement d'un réseau international pour l'observation et l'analyse des problèmes de sécurité en ligne, tels que les cybermenaces, les vulnérabilités des systèmes des TIC ou les cyberincidents.

4.8 L'Autorité nationale de sécurité (ANS)

L'Autorité nationale de sécurité est typiquement active dans le domaine de la sécurité de l'information, que ce soit des données les plus sensibles ou des informations " classifiées ».

La stratégie de cybersécurité de ce document se concentre sur quatre groupes cibles différents. Trois de ces groupes cibles font également partie des groupes cibles auxquels l'Autorité de sécurité nationale s'adresse:

· Les entreprises
· Les services publics
· Les Organisations d'Intérêt Vital

L'ANS développe un certain nombre de produits qui permettent aux entreprises et aux services publics de mieux protéger les informations classifiées dans un cyberdomaine. L'utilisation du cryptage des données développé par l'ANS peut améliorer le niveau de sécurité des informations classifiées dans le cyberespace, tant dans la sphère privée que publique. C'est ainsi que le réseau national classifié, dont le déploiement et l'organisation doivent encore être développés, facilitera l'échange sécurisé d'informations entre administrations publiques, réduisant ainsi les cyberrisques.

Pour certaines Organisations d'Intérêt Vital, l'ANS peut également effectuer des vérifications de sécurité (conseils de sécurité ou screening des professions sensibles). Pour ce faire, elle exige de ces organisations qu'elles

procèdent d'abord à une analyse des risques, une analyse des menaces et une analyse d'impact et qu'elles répertorient les mesures de sécurité de leurs systèmes informatiques. Ce processus permet tant de sensibiliser que de renforcer les mesures prises par ces organisations dans le domaine du cyberespace en matière de TIC.

4.9 L'Organe de coordination pour l'analyse de la menace (OCAM)

L'Organe de coordination pour l'analyse de la menace est notamment chargé d'évaluer la menace posée par le terrorisme et l'extrémisme. L'OCAM, en collaboration avec ses services partenaires, peut effectuer une analyse des menaces pour le compte du Centre de crise national en cas de cybermenaces ou de cyberincidents (potentiellement) liés à des groupes terroristes ou extrémistes ou à des hacktivistes d'inspiration idéologique ou religieuse.

4.10 Les Autorités sectorielles

La loi NIS du 7 avril 2019 (loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique) et l'arrêté royal d'exécution du 12 juillet 2019 précisent comment, en Belgique, les autorités sectorielles sont chacune responsables de l'identification, de la normalisation et des inspections des opérateurs de services essentiels dans leur secteur. Le CCB et le Centre de crise national jouent un rôle consultatif important à cet égard. La loi NIS identifie six secteurs différents de opérateurs de services essentiels: énergie, transports, finances, infrastructures numériques, santé et eau potable, ainsi que les services numériques (tels que les services de cloud computing, les moteurs de recherche en ligne et les commerces en ligne).

4.11 L'Institut Belge des services postaux et des télécommunications (IBPT)

L'Institut belge des services postaux et des télécommunications (IBPT) veille à la sécurité des réseaux et services de communications électroniques fournis par les opérateurs de télécommunications. L'IBPT contrôle le respect par les opérateurs de la législation (par exemple, les analyses de risques et les

mesures de sécurité connexes) et de ses décisions, il traite les notifications d'incidents de sécurité (y compris les incidents constituant une violation de données à caractère personnel, conjointement avec l'ACS) et il dispose de divers pouvoirs pour faire son travail (notamment celui de donner des instructions contraignantes à un opérateur). Il dispose également d'une équipe de réponse aux crises en cas d'incidents mentionnés ci-dessus.

L'IBPT est également l'autorité sectorielle et l'organisme de contrôle pour le secteur des infrastructures numériques (points d'échange Internet, fournisseurs de services DNS et registres de noms de domaine de premier niveau) dans le cadre de la loi NIS et pour les secteurs des communications électroniques et des infrastructures numériques dans le cadre de la loi «Infrastructures critiques».

L'IBPT est également chargé de contrôler l'application des dispositions légales transposant la directive relative aux équipements radioélectrique [RED (2014/53/EU)] concernant les produits contenant une fonctionnalité radio.

4.12 Le Service Public Fédéral Economie

Le Service public fédéral Economie, PME, Classes moyennes et Energie a pour mission de créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. Face à la numérisation croissante de notre société et de nos entreprises, le SPF Economie s'implique dans différents domaines de la cybersécurité.

Il s'agit de l'administration compétente pour l'identification, la normalisation et la supervision des secteurs de l'énergie et des fournisseurs de services numériques en vertu de la loi NIS.

Les victimes de divers types de cybercriminalité peuvent signaler les cas de cybercriminalité à Meldpunt, un service du SPF Economie, qui partage les données pertinentes de ces signalements avec le CCB et renvoie les victimes de cybercriminalité à la police.

Vu l'importance des PME pour l'économie belge, le SPF Economie travaillera plus étroitement avec le CCB pour renforcer la cybersécurité de ce groupe d'entreprises.

4.13 Cadre de gouvernance et plateformes de consultation

Outre leurs propres responsabilités, la coopération entre les acteurs concernés est un important facteur de succès dans la prévention, la réduction, le traitement et la surveillance des cybermenaces et des cyberincidents. Les connaissances en matière de cybersécurité et l'évolution de la cybermenace sont partagées via des plateformes existantes ou nouvelles entre les services de sécurité concernés, les autorités, le secteur privé et le secteur scientifique. Les experts partagent des informations et des expériences *de visu* et nouent des contacts à l'occasion de réunions périodiques..

Au sein de la plateforme 4 Cyber du Comité de coordination du renseignement et de la sécurité (CCRS), les services de renseignement et de sécurité examinent la politique générale en matière de cybersécurité.

La concertation entre les autorités de surveillance des Organisations d'Intérêt Vital se fait par l'intermédiaire de la plateforme CySSAP (" Cybersecurity Sectoral Authority Platform »).

Le Réseau d'expertise sur la cybercriminalité (REN) réunit des experts des services publics dans le domaine de la cybercriminalité pour des concertations périodiques. La coordination principale est assurée par le parquet général d'Anvers.

La plateforme CSI/DPO (Conseillers en Sécurité de l'Information/Data Protection Officers) regroupe les conseillers en sécurité et les responsables de la protection des données de chaque service public. Une réunion spécifique sur les cyberaspects a lieu chaque trimestre dans le cadre du « Quarterly Cyber Threat Report » du CCB/CERT.

SIT (Synergy IT) est la plateforme de partage des connaissances et de concertation des responsables des TIC de tous les services publics fédéraux (services publics fédéraux, institutions publiques de sécurité sociale et organismes d'intérêt public). Le SIT se réunit tous les mois dans le but d'initier et d'assurer le suivi des initiatives informatiques conjointes, tant pour les marchés publics que pour les projets, et d'apporter une contribution technique de base aux initiatives G-Cloud.

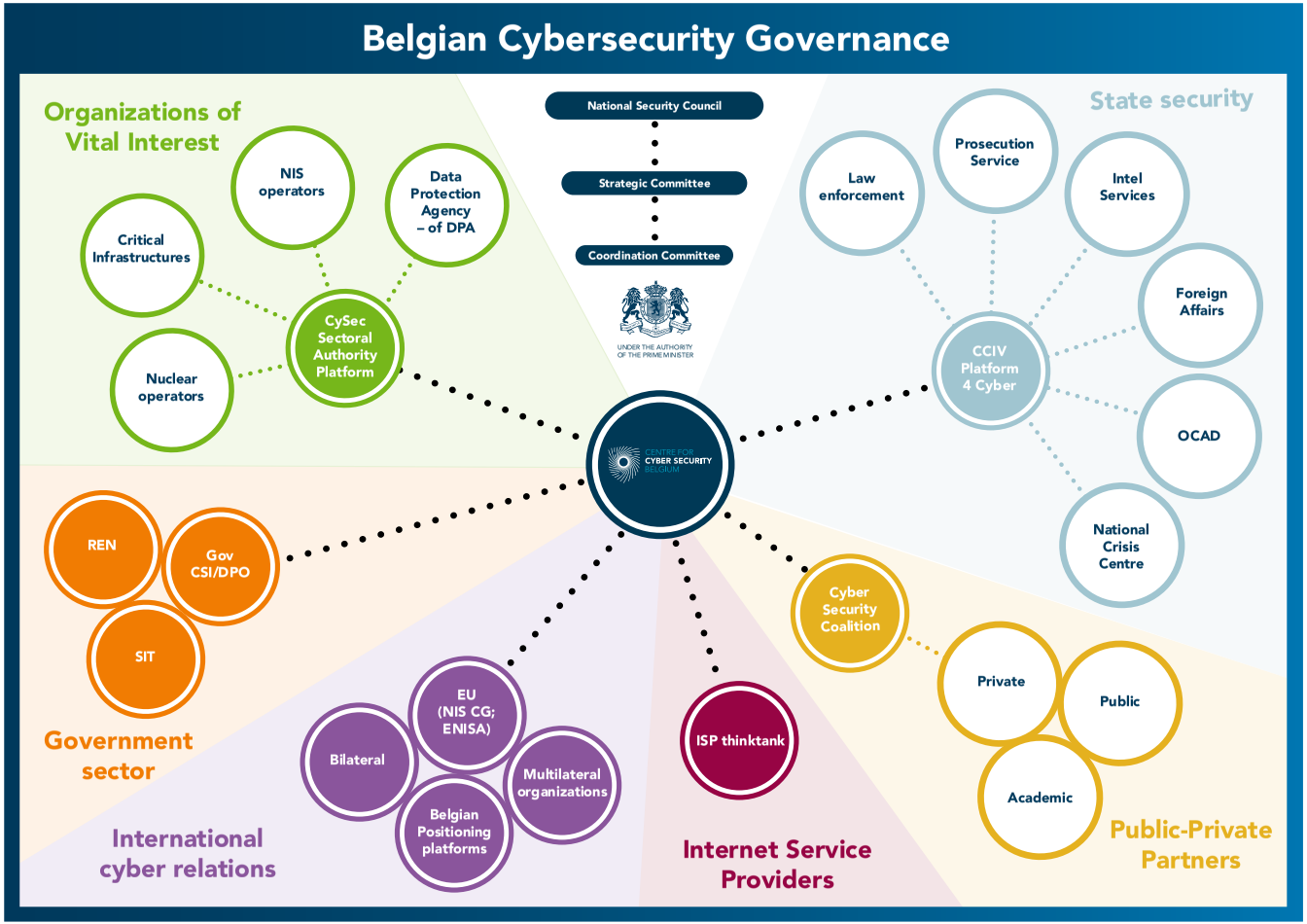
L'élaboration des positions belges formelles dans les discussions internationales passe par les voies habituelles du SPF Affaires étrangères.

La Commission économique interministérielle (CEI) est un mécanisme de coordination technico-administrative indépendant, souple et flexible au sein du SPF Economie, PME, Classes moyennes et Énergie, qui peut aider à déterminer et coordonner les positions administratives des autorités fédérales et fédérées dans les dossiers nationaux, européens et internationaux.

Dans le groupe de réflexion ISP, le CCB consulte régulièrement les plus grands fournisseurs d'accès à Internet en Belgique à propos de mesures et projets concrets susceptibles d'améliorer la cybersécurité pour les citoyens et les entreprises belges.

Les rapports trimestriels sur les cybermenaces, organisés par le CCB et CERT.be, rassemblent plusieurs de ces plateformes de concertation et informent tous les participants ainsi que les Organisations d'Intérêt Vital sur les menaces actives.

La Cyber Security Coalition Belgium réunit régulièrement des experts du domaine des secteurs privé, universitaire et public sous la forme d'événements de partage d'expériences et dans des groupes de discussion où les meilleures pratiques, les expériences ou les initiatives sont discutées autour de différents thèmes (comme la sécurité cloud, NIS, crypto, etc.).


Belgian Cybersecurity Governance
Organizations of Vital Interest
NIS operators
Data Protection Agency – of DPA
Critical Infrastructures
CySec Sectoral Authority Platform
Nuclear operators
National Security Council
Strategic Committee
Coordination Committee
UNDER THE AUTHORITY OF THE PRIME MINISTER
CYBERSECURITY BELGIUM
State security
Law enforcement
Prosecution Service
Intel Services
Foreign Affairs
CCIV Platform 4 Cyber
OCAD
National Crisis Centre
REN
Gov CSI/DPO
SIT
Government sector
Bilateral
EU (NIS CG; ENISA)
Multilateral organizations
Belgian Positioning platforms
International cyber relations
ISP thinktank
Internet Service Providers
Cyber Security Coalition
Private
Public
Academic
Public-Private Partners

5. Moyens

Afin de mettre en œuvre la vision et les six objectifs stratégiques de cette stratégie ambitieuse, des investissements supplémentaires importants, mais essentiels, sont nécessaires. Un engagement clair du gouvernement belge en faveur de ces ressources est donc l'élément final élémentaire de cette stratégie nationale de cybersécurité renouvelée. Après tout, il est essentiel d'accroître notre cybercapacité pour armer efficacement et de manière réaliste notre économie, nos services publics et nos organisations vitales contre les cybermenaces toujours plus nombreuses.

Les investissements dans la cybersécurité ont également un impact économique direct et évident. Si le gouvernement parvient à inspirer et à garantir la confiance dans la «vie digitale», les entreprises et les citoyens seront également plus confiants pour investir dans davantage d'applications numériques. Cela stimulera la productivité et la croissance économique dans notre pays, et les cyberattaques pourront plus facilement être prévenues.

Avec cet engagement d'investissement concret, la Belgique suit les initiatives importantes prises dans ses pays voisins. Ces investissements génèrent également une grande confiance dans la mise en œuvre réaliste de nos objectifs, en particulier chez nos partenaires européens et internationaux. Après tout, beaucoup d'entre eux ont un siège ou une représentation importante dans notre pays.

La mission de faire de la Belgique l'un des pays les moins vulnérables d'Europe dans le domaine de la cybersécurité d'ici 2025 est un effort collectif. Outre le CCB, d'autres services publics, les services de renseignement et de sécurité, mais aussi le monde des affaires, les Organisations d'Intérêt Vital, le monde universitaire et les citoyens ont chacun leur propre responsabilité individuelle pour atteindre les objectifs ambitieux fixés.

Le gouvernement fédéral a une responsabilité importante à cet égard, à la fois pour fixer la direction mais aussi pour donner l'exemple. Elle développera donc une cybercapacité crédible, capable de suivre le rythme des autres acteurs belges et de chercher à se connecter aux possibilités de nos pays voisins.

Prépresse et impression
Imprimerie centrale de la Chambre des représentants

Bruxelles, octobre 2020

Editeur responsable
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur, Rue de la Loi 16, 1000 Bruxelles

D/2021/14828/002