ÉCOLE DE GUERRE

PROMOTION *GÉNÉRAL GALLOIS*

2016 -2017

LA BELGIQUE ET SA CYBERSTRATÉGIE

Maj d'Avi Karl SAMYN, ir

Sous la direction de :

M. Joseph HENROTIN, PhD

Rédacteur en chef DSI, DSI HS

Chargé de recherche CAPRI

Avant-propos

Ce travail est basé sur de l'information provenant de sources ouvertes, non-classifiées. Certains aspects, traités de façon superficielle dans ce travail, sont traités de façon plus approfondie au sein des différents services et agences nationales mais, de par leur contenu sensible, ne se trouvent pas dans le domaine public et ne seront donc pas discutés ici.

Résumé

Notre société actuelle est, socialement et économiquement, hyper-connectée, évoluant dans un cyberespace constitué de systèmes physiques et d'informations virtuelles qui est le cinquième milieu reconnu par l'OTAN, aux côtés de la terre, la mer, l'air et l'espace.

Afin de contrer les vulnérabilités que ce milieu nous crée, l'Etat, puis la Défense belge, ont tour à tour lancé leur stratégie de cybersécurité, chacune présentant des lignes directrices communes avec l'autre, mais également des différences notables. Leur mise en œuvre par plusieurs organismes nationaux différents renforce parfois ces divergences, sans que le fil rouge de la protection des intérêts du pays, infrastructures critiques et systèmes publics inclus, ne soit perdu.

L'organisme d'Etat BelNIS aplanit ces différences en assurant partiellement le C2 commun, à défaut d'un centre multidisciplinaire et interdépartemental qui unifierait intégralement la structure C2 et la Cyber Picture nationale.

Entretemps, les projets et initiatives se sont succédés, autant pour augmenter le niveau de protection des secteurs vitaux que pour éduquer la population et ainsi réduire la faiblesse du maillon que constitue l'humain en matière de cybersécurité.

Le pouvoir législatif appuie cette évolution en adaptant peu à peu le cadre légal aux nouveaux acteurs et méthodes émergeant du cybermonde, même s'il lui reste du travail à faire.

Le focus de la Défense s'oriente plus vers le cyberdéfensif, accordant moins d'attention au cyberoffensif et aux possibilités qu'il présente en matière d'information. L'aspect multiple des cyberopérations offre pourtant un large choix d'effets et est loin d'être limité aux *Computer Network Operations*.

Cette variété dans la cybermenace requiert d'ailleurs que le panel de spécialistes impliqués dans la cyberdéfense soit pareillement diversifié, comportant aussi bien des geeks en informatique que des politologues, et que ce personnel hautement qualifié puisse rester suffisamment de temps en place que pour acquérir les connaissances, compétences et expérience nécessaires à leur rôle de conseiller des dirigeants civils et militaires.

Parce que ce n'est qu'en créant une vision large mais cohérente, en pensant à la cybersécurité dès le début de chaque projet, en investissant dans les moyens humains et matériels, qu'une cyberdissuasion forte et crédible pourra garantir l'équilibre entre les libertés individuelles et la protection des intérêts communs.

Executive summary

From both a social and economic point of view, our current hyper connected society evolves in cyberspace. It is built up from physical systems and virtual information and was recently recognized as the fifth domain by NATO besides land, sea, air and space.

In order to counter the vulnerabilities created by this domain, the Belgian government, and later her Ministry of Defence, created their own cyber security strategy. Each has common guidelines, but also notable differences. Their implementation by several national organisations has reinforced these differences, but has always assured the protection of national interests, i.e. critical infrastructure as well as public systems.

In the absence of a multidisciplinary and interdepartmental cyber centre that integrates a complete C2 structure together with a national Cyber Picture, the federal government body BelNIS acts to level the differences in the strategies, by assuring a common C2 structure. Meanwhile, a number of projects and initiatives have come to light, both aimed at improving the level of protection of the critical infrastructures as well as for educating the population in regard to cyber security, since the human is considered the weakest link to this matter.

The legislative power supports this evolution, by modifying the legal framework to new actors and methods that continue to emerge from cyberspace. But there is still work to do.

Belgian Defence is focus is oriented more towards cyber defence, thus paying less attention to the offensive possibilities within the information domain. However, the multiple aspects of cyber operations provide a vast number of choices to the effects that can be achieved and are far from being limited to Computer Network Operations.

The variety of cyber threats requires an even distribution amongst the cyber defence specialists, ranging from computer geeks to political scientists. Furthermore these specialists should remain in place long enough to obtain the necessary knowledge, competences and experience to allow them to be able to advise both civil and military leaders.

It is only by creating a general but coherent vision; by thinking about cyber security at the very start of each project; and by investing in the human and material resources that a powerful and credible cyber deterrence can guarantee the balance between individual freedoms on the one hand and the protection of the common interests on the other.

Table des matières

> “True CyberSecurity is preparing for what’s next, not what was last”
>
> Neil Rerup

1 Introduction

A l'heure actuelle, la connectivité et, d'un point de vue plus large, le cyberespace, ont pris une place très importante dans notre vie quotidienne, aussi bien sur le plan social que sur le plan économique. Des menaces contre ce domaine cyber peuvent avoir des répercussions importantes pour les individus, les entreprises et même la société en général. C'est la tâche du gouvernement et de ses organismes d'assurer la sécurité des fonctions vitales et donc des secteurs essentiels du pays en toute circonstance.

Pour répondre aux menaces que le domaine cyber engendre et afin de déterminer des objectifs, une approche et des domaines d'actions, il est nécessaire de définir une cyberstratégie. En effet, chaque pays, organisation, entreprise, ou autre un tant soit peu sérieux est convaincu de l'importance que ce domaine cybernétique revêt et de l'impact qu'une dégénérescence de cet environnement pourrait avoir sur ses propres moyens (civils et militaires). C'est en tout cas le point de vue de l'Union Européenne, qui a vite été suivie par plusieurs de ses pays membres.

C'est aussi dans cet élan que la Belgique a écrit son *Cyber Security Strategy* en 2012 et, un peu plus tard, son *Cyber Security Strategy for Defence*.

La problématique abordée dans ce travail se place à ce niveau. Certes, en matière de cybersécurité belge, différents documents décrivant soit une stratégie, soit reprenant des éléments relevant d'une stratégie, existent. Mais existe-t-il une cohérence entre tous ces documents et initiatives ? Autrement dit, quelles sont les interactions entre l'Etat (le gouvernement) et l'armée (la Défense) au niveau des différentes stratégies de cybersécurité ? Analyser en parallèle ces documents et stratégies permet d'établir une bonne vue d'ensemble de toutes ces initiatives, ce qui constitue une condition sine qua non si l'on veut être capable de tirer des conclusions, et, le cas échéant, d'identifier les lacunes qui existeraient et de faire les propositions ou les recommandations adéquates.

Dans chacune de ces cyberstratégies, les relations entre individus d'un côté et entre organismes nationaux ou internationaux d'un autre côté, les perceptions d'autres agences, organisations et pays, le climat économique et politique, les intérêts propres, et d'autres éléments organisationnels se retrouvent au fil des chapitres, comme il se doit. Ne pas les y voir aurait été vraiment surprenant, et un peu préoccupant[1].

[1] F.-B. Huyghe, O. Kempf et N. Mazzuchi, *Gagner les cyberconflits: Au-delà du technique*, Economica (Collection Cyberstratégie), 2015, p.65

Quoi qu'il en soit, la cybersécurité doit faire intégralement partie de la culture d'entreprise. Pour en arriver là, il faut assurer un suivi permanent des risques et des mesures mises en place dans l'organisation.

La technologie occupe une place importante dans ce monde du cyberespace. Les systèmes d'information et de communication font de plus en plus partie de notre vie quotidienne. De plus, cette technologie évolue très vite. On peut même parler d'une révolution, au même titre que la révolution industrielle ou la révolution numérique. Mais il est impératif de regarder au-delà de la technologie, car le cyber, ce n'est pas seulement le matériel physique, c'est également l'aspect immatériel de l'information, cette information qui est devenue, au fil des années, un bien très précieux. Tout ceci engendre une augmentation de la rapidité avec laquelle l'environnement de la sécurité de l'information se renouvelle.

En effet, nous vivons dans un monde où tout est connecté, ce que l'on appelle communément « l'Internet des Objets ». C'est une ère où chaque objet présente un risque potentiel au niveau de la cybersécurité[2] et où même les systèmes qui ne sont pas directement connectés à l'Internet courent des risques de plus en plus élevés, comme le virus Stuxnet l'a démontré. Effectivement, en 2010, la découverte de ce malware attaquant les systèmes de contrôle (SCADA), avait déjà fortement contribué au développement de la perception actuelle et à la mise en évidence de la sophistication des menaces cyber, ainsi que des dégâts que ces menaces peuvent engendrer au sein des gouvernements, des organisations et de leurs infrastructures critiques.

Par conséquent, la cybersécurité, et la sécurité des informations en particulier, est devenu un souci majeur pour chacun d'entre-nous, car cette problématique grandissante est intrinsèquement liée à la façon dont nous vivons notre vie au quotidien.

Il est d'ailleurs remarquable de voir avec quelle rapidité la situation a évolué dans les quatre années qui ont suivi la publication du document belge *Cyber Security Strategy*. Les risques sont devenus plus sérieux, plus répandus et plus globaux. Les cyberattaques contre les institutions gouvernementales et les infrastructures nationales critiques sont devenues des sujets de sécurité nationale[3,4].

[2] « Hacker lassen Finnen frieren », Der Spiegel Online, 08 novembre 2016, http://www.spiegel.de/netzwelt/web/finnland-hacker-schalten-heizungen-aus-a-1120234.html

[3] Erwin Sandra, Magnuson Stew, Parsons Dan (et al.), « Top Five Threats to National Security in the Coming Decade », National Defense Industrial Association, November 2012,

Mais le cyberespace est devenu un outil fondamental pour soutenir la croissance d'une organisation, voire même d'un pays. L'Internet s'est peu à peu imposé en tant que moteur majeur de l'économie internationale, de la croissance et des innovations[5].

Tout doit donc être mis en œuvre pour que les organismes étatiques et les différentes organisations d'importance nationale, chacun à son niveau, soient formés et équipés des meilleurs moyens possibles dans le but d'assurer la protection des différentes institutions gouvernementales ainsi que des infrastructures critiques pour le pays et sa population.

Après une série de définitions de termes et de concepts employés, un passage en revue des différents documents de base de la cyberstratégie belge ainsi que d'autres documents également pertinents et une analyse des organismes en lien avec cette cyberstratégie nationale, une lecture transversale ainsi qu'une présentation des enjeux et des défis que représente l'implémentation d'une cyberstratégie efficiente dans notre pays nous amènerons à la conclusion de ce travail.

http://www.nationaldefensemagazine.org/archive/2012/november/pages/topfivethreatstonationalsecurityinthecomingdecade.aspx

[4] « Cyberaanval via beveiligingscamera's en babyfoons », deredactie.be, 21 octobre 2016 – 21:37, http://deredactie.be/cm/vrtnieuws/cultuur%2Ben%2Bmedia/media/1.2799653#

[5] *G8 Declaration, Renewed commitment for freedom and democracy*, G8 Summit of Deauville, May 26-27, 2011, Preamble - §5.

2 Le « cyber »

2.1 Le milieu

Avant de rentrer plus en détails dans les différents documents, de distinguer les intervenants et d'analyser leurs implications dans le domaine cyber belge, certaines notions doivent être clarifiées afin d'éviter toute confusion sémantique.

En effet, différentes écoles existent pour interpréter, expliquer et cataloguer les mots portant le préfixe cyber, ce qui peut mener à des malentendus.

Mais avant même de commencer à parler de cyberstratégie, cybersécurité, cyberdéfense, cyberattaque, etc..., une définition du mot « cyberespace » est nécessaire. Utilisé pour la première fois dans la nouvelle de science-fiction *Burning Chrome* (en français renommé « Gravé sur chrome ») de William Gibson, publié en 1982, ce n'est qu'en 1984, avec la sortie du roman de science-fiction *Neuromancer* (en français renommé « Neuromancier ») du même auteur, que le terme devient populaire.
Trop souvent confondu, à tort, avec le terme Internet, il est actuellement défini de plusieurs façons.

D'après le dictionnaire Petit Robert, édition 2010, le terme désigne

> « un ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs »[6].

L'ANSSI définit le cyberespace comme suit :

> « Un espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques »[7].

Le département de la défense américaine (DOD) utilise la définition ci-dessous :

> « *A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer*

[6] Source http://fr.wikipedia.org/wiki/cyberespace/
[7] Glossaire, https://www.ssi.gouv.fr/entreprise/glossaire/c/

systems, and embedded processors and controllers »[8].

Selon la *Cyber Security Strategy* belge, le cyberespace est[9] :

> « L'environnement global né de l'interconnexion des systèmes d'information et de communication. Le cyberespace est plus large que le monde informatique et contient également les réseaux informatiques, systèmes informatiques, médias et données numériques, qu'ils soient physiques ou virtuels. »

La même définition est retrouvée dans la *Belgian Defense Cyber Security Strategy*:

> « *The global environment that is created through the interconnection of communication and information systems. The cyberspace includes the physical and virtual computer networks, computer systems, digital media and data* »[10],

Un grand nombre de variantes, donc, mais toutes ces définitions de cyberespace ont ceci de commun qu'elles mettent en valeur les aspects du matériel et de l'infrastructure. Elles reprennent aussi le fait que le cyberespace présente un aspect immatériel dont nous avons déjà parlé plus haut, c'est-à-dire l'information. Par contre, parmi les définitions citées ici, la définition belge est la seule qui tienne compte de l'aspect typiquement virtuel de ce milieu. En effet, on doit faire abstraction de la couche physique et des données transitant sur cette couche physique doit être faite afin de bien comprendre ce que recouvre le cyberespace. La virtualité ne se situe pas uniquement dans le fait que les données ne se trouvent pas nécessairement dans un endroit physique unique, avec comme conséquence qu'elles peuvent exister simultanément dans plusieurs lieux physiques en même temps, mais aussi dans le fait que les données peuvent être perçues différemment par des individus ou des entités différentes. De plus, il n'y a plus de frontière physique dans le cyberespace.

[8] DOD, *Joint Publication 3-12 (R)*, 05 février 2013, p. GL-4
[9] Belgische Federale regering, *Cyber Security Strategy*, 2012, p 12
[10] Belgische Defensie – ACOS Strat, *Cyber Security Strategy for Defence*, 2014, p 18

Le cyberespace peut dès lors être considéré comme un cinquième milieu[11], à côté des milieux physiques déjà existant : terre, air, mer, espace extra-atmosphérique, comme illustré dans le schéma représenté ci-dessous.

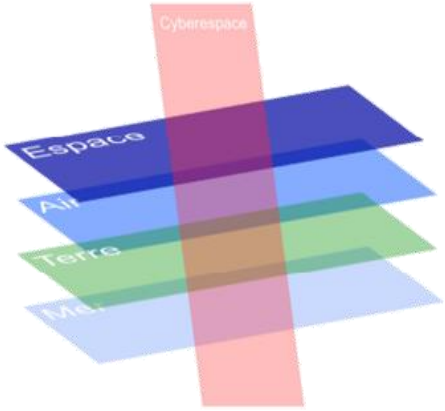

Figure 1
Illustration extraite de : Daniel Ventre, Cyberespace et acteurs du cyberconflit, éditions Hermès Lavoisier, Paris, 2011

2.2 La stratégie

« La » stratégie contemporaine englobe bien plus que des éléments strictement militaires. Au début du XXe siècle, de nouveaux concepts ont émergé : stratégie générale, stratégie élargie, stratégie totale ou encore grande stratégie comme Liddell Hart avait nommé sa théorie en la matière. La concernant, il dit d'ailleurs ceci[12] :

> « *The role of grand strategy – higher strategy – is to co-ordinate and direct all the resources of a nation, or band of nations, towards the attainment of the political object of the war – the goal defined by fundamental policy.* »

Dans un registre plus récent, la grande stratégie, selon Colin Gray, comprend[13]

> « l'emploi délibéré de tous les instruments de pouvoir dont dispose une communauté de sécurité. »

Peu importe la dénomination employée pour « la » stratégie contemporaine, celle-ci combinera toujours plusieurs stratégies sectorielles afin d'atteindre les objectifs fixés. L'une de ces stratégies sectorielles est la stratégie générale militaire, qui repose sur quatre piliers[14]. Dans l'un de ces piliers, on retrouve les stratégies de milieu,

[11] Pierluigi Paganini, « NATO officially recognizes cyberspace a warfare domain », 18 juin 2016, http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html
[12] B. H. Liddell Hart, *Strategy*, 2nd rev. ed., London: Faber & Faber, 1967, p. 322
[13] Colin Gray, *War, Peace and International Relations: An Introduction to Strategic History*, Abingdon and New York City: Routledge 2007, p. 283.
[14] J. Henrotin, Introduction à la stratégie Syllabus des conférences données à l'ESIG, 2014, p. 12-13

comme la stratégie maritime, la stratégie aérienne et plus récemment la stratégie aérospatiale.

Si l'on se tient au principe que le cyberespace est considéré comme le cinquième milieu, la cyberstratégie devient donc la stratégie de milieu la plus récente. Plusieurs similitudes peuvent d'ailleurs être établies entre elle et les autres stratégies de milieu. Exactement comme dans le milieu aérien, les différents modes d'actions sont rapides -encore plus rapides, même- et les actions entreprises peuvent aussi bien toucher des objectifs militaires que civils. Mais les principes de la stratégie maritime peuvent également s'appliquer à la cyberstratégie. Ainsi, les modes d'opération cyber peuvent avoir un effet direct dans un milieu différent du leur (on parlerait ici de guerre littorale dans un cadre maritime), ils peuvent détruire des infrastructures (semblable aux principes de la frappe terrestre depuis la mer) ou même interrompre les flux d'informations (comme dans les guerres d'escadre et de course).

Le milieu cyber, en grande partie virtuel donc, englobe également le spectre électromagnétique dont Boeing[15] avait déjà souligné l'importance en 1976, en même temps que celle du contrôle de l'information.

A la base, le milieu cyber est essentiellement destiné à appuyer les opérations dans les autres milieux (terre, air, mer, espace extra-atmosphérique). C'est en réalité de ça que la cyberstratégie tire toute sa puissance, puisque les opérations cybers peuvent ainsi agir dans n'importe quel autre milieu au départ du leur, dès lors qu'ils sont interconnectés entre eux, ce qui est presque toujours le cas aujourd'hui vu le niveau technologique des moyens de communications modernes mis en œuvre et le type d'informations échangées.

2.3 Cyber : -sécurité / -défense / -attaque

Une cyberstratégie cohérente implique de pouvoir faire face de la façon la plus efficace qui soit aux menaces émanant du cyberespace. Dans cette optique, une bonne cybersécurité doit être garantie en tout temps et en tout lieu.

[15] T. Rona, *Weapon Systems and Information War*, The Boeing Aerospace Company, juillet 1976

Selon la *Cyber Security Strategy* belge et la *Belgian Defense Cyber Security Strategy*, la cybersécurité est définie comme suit[16] :

> *« The desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks. »*

C'est l'état dans lequel les systèmes peuvent résister à des événements issus du cyberespace, le fait de pouvoir rester hors de toute atteinte ou dégâts lié à une attaque, une perturbation ou une mauvaise utilisation des TIC.

La *Belgian Defense Cyber Security Strategy* définit la cyberdéfense comme[17] :

> *« The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. »*

Au niveau national, la cyberdéfense n'a pas été définie. Néanmoins, si l'on procède suivant la logique de la Défense Belge, ce serait l'application de l'ensemble des mesures de protection contre les menaces cybers qui permettraient à l'État belge de défendre ses systèmes jugés les plus essentiels. En effet, la cybersécurité comprend la Sécurité des Systèmes d'Information (SSI), c.-à-d. la cyberprotection, et la cyberdéfense (défense active, actions offensives).

L'Etat doit donc pouvoir se défendre contre les cyberattaques, ces dernières pouvant être définies comme des actions volontaires, offensives ou malveillantes, menées au travers du cyberespace et ayant comme but d'endommager les systèmes qui traitent des informations ou d'affecter ces informations elles-mêmes.

[16] Belgische Defensie – ACOS Strat, *Cyber Security Strategy for Defence*, 2014, p. 18
[17] *Ibid.*

3 La cyberstratégie belge

3.1 Les documents

3.1.1 Cyber Security Strategy

En 2012, le gouvernement belge a officiellement adopté sa stratégie de cybersécurité en publiant le document *Cyber Security Strategy*.

Vu l'importance que revêtent les technologies d'information et de communication dans notre société actuelle, leur disponibilité et leur bon fonctionnement, c'est-à-dire intègre et de bonne qualité, sont cruciaux.

Il en découle que, parmi les acteurs concernés, tout le monde est convaincu de la nécessité de l'établissement d'une cyberstratégie, ne fut-ce que parce que le cyberespace est un outil fondamental pour appuyer la croissance et qu'à ce titre, il doit être préservé le plus complètement possible.

Dans cet esprit, les objectifs suivants, ont été définis dans la stratégie nationale de cybersécurité[18] :

1. viser un cyberespace sûr et fiable qui respecte les valeurs et droits fondamentaux d'une société moderne ;
2. veiller à une protection optimale contre la menace cyber des systèmes publics et infrastructures critiques ;
3. développer nos propres capacités de cybersécurité pour une politique de sécurité autonome et une réaction aux incidents sécuritaires adaptée.

Afin de réaliser les trois objectifs repris ci-dessus, la Belgique s'est tracé un certain nombre de lignes d'actions concrètes. Quelques-unes d'entre-elles méritent d'attirer notre attention. En effet, elles se rapportent à une approche centralisée et intégrée de la cybersécurité et, de par leur application, la menace cyber se retrouve continuellement suivie. De plus, dans le futur, des normes et directives de sécurité standard seront édictées dans le but d'améliorer la protection des systèmes TIC. Et, si malgré tout cela, des incidents se produisaient quand même, alors la réaction à y apporter serait adaptée et menée avec les moyens adéquats, et tout ceci à l'intérieur d'un cadre légal correct et avec les stimulants nécessaires afin d'élargir les connaissances en matière de cybersécurité et de promouvoir les développements

[18] Belgische Federale regering, *Cyber Security Strategy*, 2012, p. 2.

technologiques dans le domaine cyber.

3.1.2 Belgische Gids voor Cyber Veiligheid / Guide belge de la cybersécurité

Partout dans le monde, chaque jour, des entreprises et des organisations sont confrontées à des formes de cybercriminalité ou de cyber-infractions. En Belgique aussi, ces faits deviennent un vrai souci pour un grand nombre d'entre-elles. Un petit guide a dès lors été conçu dans le but que le monde des affaires comprenne les risques et la façon de les gérer en pratique. C'est un guide simple et pragmatique conçu pour aborder la problématique de la cybersécurité dans les entreprises. Et, lorsque l'on sait que la cybersécurité est l'un des grands challenges auxquels sont confrontées un grand nombre d'entreprises, on comprend toute l'importance que peut revêtir ce petit manuel en matière de prévention et de protection des problèmes de ce genre.

3.1.3 Cyber Security Strategy for Defence

En 2014, la *Cyber Security Strategy for Defence* a été publiée. Ce document définit le cadre stratégique pour la Défense, articulée autour de trois piliers : cyberdéfense, cyberintelligence et cyber contre-offensive.

En plus de ce cadre, le document met en avant une vision claire du futur dans le domaine cyber. Dans cette vision, l'élaboration de capacités propres est orientée suivant les activités journalières, aussi bien territoriales qu'expéditionnaires, et ceci depuis le niveau stratégique jusqu'au niveau tactique, en passant par le niveau opératif. De plus, la continuation et le développement à long terme de la coordination et de la collaboration interdépartementale au niveau national, ainsi que la possibilité de profiter d'opportunités au niveau international, sont également prises en compte.

Cette vision permet de concevoir l'amélioration des capacités cyber au sein de la Défense d'une façon cohérente et ce, avec une implémentation réalisable. Mais la création d'une culture de la cybersécurité n'en devient que plus nécessaire.

3.1.4 De strategische visie voor Defensie / La vision stratégique pour la Défense

La vision stratégique pour la Défense, publiée le 29 juin 2016, se base sur l'Accord de Gouvernement du 9 octobre 2014, dans lequel il est clairement établi que le besoin sécuritaire est grand et que la cybersécurité doit constituer une priorité.

> « Le besoin de sécurité est élevé. »[19]
>
> « Considérant les dangers auxquels sont confrontés nos institutions, nos entreprises et nos citoyens, la cybersécurité constituera une priorité. »[20]

Le secteur économique est d'une importance vitale pour le pays. Or, de grands pans de l'économie sont basés sur, entre autres choses, les flux de services et d'information, dont une grande partie transite par le cyberespace.

Dans le même esprit, la Défense est une organisation qui s'appuie fortement sur la technologie, ce qui la rend donc particulièrement dépendante du milieu cyber. Cette dépendance, que ce soit pour l'économie ou la Défense, représente une vulnérabilité en matière de cybersécurité, et ce d'autant plus que sécurité interne et externe sont de plus en plus étroitement entremêlées.

La Défense doit donc disposer de ses propres capacités cyberinformatiques, qui devront pouvoir lui permettre d'accomplir jusqu'à des missions offensives[21] et qui pourront être déployées en temps de crises nationales. Ainsi, elle sera en mesure de prendre elle-même l'initiative et de fournir des spécialistes, le tout en collaboration avec d'autres acteurs nationaux de sécurité ainsi qu'avec des entreprises privées.

Ainsi donc, la Défense de demain sera basée sur quatre dimensions capacitaires : renseignement-cyber-influence, terre, air, maritime. Le cyber occupe une place de premier plan dans le Service de Renseignement Militaire, ce qui est d'autant plus justifié que l'environnement cybernétique mérite une attention particulière dans l'optique d'un renforcement des capacités de renseignement et d'influence de la Défense. Il est ainsi aisé d'imaginer une riposte à des menaces hybrides au moyen de notre capacité d'influence, dont l'un des points de départ et d'action est le cyberespace.

Ce pilier du cyber-renseignement garantit également le *situational understanding* (ou compréhension de la situation) nécessaire qui protègera notre liberté d'action au sein de cette dimension militaire essentielle. Le fait d'aller plus loin dans la mise en œuvre du CSOC (*Cyber Security Operations Center*) sera également la garantie d'une plus grande cohérence pour la cyberdéfense des systèmes de technologie de

[19] Belgische Defensie, *La vision stratégique pour la Défense*, 29 Jun 2016, p. 19.
[20] *Ibid.* p. 61.
[21] *Ibid.* p. 61.

l'information et de la communication (TIC) de nos forces armées.

3.2 Les organismes

3.2.1 CERT.be

La Belgique dispose d'une équipe d'intervention d'urgence en sécurité informatique (Computer Emergency Response Team ou CERT.be). Cette équipe fédérale d'urgence cyber est un spécialiste neutre en matière d'Internet et de sécurité des réseaux, qui est à même d'assister les entreprises et les organisations belges dans les matières suivantes :

- coordination lors d'un incident cyber ;
- avis concernant la recherche d'une solution lorsqu'un incident cyber survient ;
- appui afin de prévenir que ces incidents de sécurité ne surviennent.

En plus de tout ceci, il existe une structure bien définie pour rapporter les incidents de cybersécurité.

Il est à remarquer que, depuis le 1er Janvier 2017, le CERT a été intégré au CCB (voir point suivant).

3.2.2 CCB

« L'approche de la cybersécurité doit être centralisée et intégrée par un organe central. »[22]

En réponse à ce domaine d'action décrit dans le document *Cyber Security Strategy*, le Centre pour la Cybersécurité Belgique (CCB) a été fondé par l'arrêté royal du 10 octobre 2014.

Le CCB relève de l'autorité du Premier Ministre et est en charge de la cybersécurité en Belgique. Il devra dès lors élaborer la politique nationale en matière de cybersécurité et encourager tous les services concernés de Belgique à faire des efforts de façon appropriée et intégrée. De plus, depuis le 1er janvier 2017, le CCB a repris la direction des services du CERT.be des mains du SPF (Service Public Fédéral, soit un ministère au niveau fédéral) Technologie de l'information et de Communication. La recherche, l'observation et l'analyse des problèmes de sécurité en ligne, ainsi que l'information permanente des utilisateurs à ce sujet, tombent maintenant également sous sa compétence.

[22] Belgische Federale regering, *Cyber Security Strategy*, 2012, p. 2.

Le CCB s'adresse à tous les utilisateurs domestiques, mais offre aussi des informations et des avis aux entreprises et initie des informations, des formations, de l'entraînement, des cours et de la recherche académique afin d'améliorer le niveau de connaissances en matière de cybersécurité en Belgique.

A côté de cela, différentes initiatives ont été prises afin de renforcer la cybersécurité dans les secteurs vitaux belges. Ceux-ci sont les secteurs qui sont cruciaux pour la sécurité de la population belge et sont identifiés comme suit : énergie, mobilité, télécom, secteur financier, eau potable, santé publique, gouvernement.

Dans ce cadre, un Cyberplan d'urgence a été mis en place. Ce plan doit permettre d'organiser une structure de réponse aux crises et incidents cyber-sécuritaires qui demanderaient une coordination et/ou une gestion à un niveau national, afin que les différents services belges actifs dans le domaine cyber puissent collaborer de façon efficiente, dans le but de reprendre la situation sous contrôle le plus rapidement possible.
De plus, dans le but de pouvoir avertir les secteurs vitaux d'une façon rapide et standardisée lorsqu'une nouvelle menace cyber ou cyberattaque se profile, un système d'*Early Warning* a aussi été mis en place.

3.2.3 BelNIS

Une plateforme de concertation fédérale pour la sécurité de l'information existe. Cette plateforme, sous la présidence du directeur du CCB, réunit chaque mois les différents organismes actifs en matière de sécurité de l'information en vue d'énoncer des recommandations sur les différents sujets qui touchent à la sécurité de l'information.

Par le biais de BelNIS, un soutien actif pour promouvoir un partenariat public-privé existe, puisque cet organisme gouvernemental travaille en collaboration étroite avec des entités privées et semi-privées.

3.2.4 La Défense

La Défense dispose de ses propres capacités cyber afin de pouvoir offrir une réponse adéquate et rapide à une menace cyber de type militaire. Ces capacités continueront à être développées pour, à terme, être capable de détecter et de neutraliser des cyberattaques contre les systèmes d'information de la Défense. Cette évolution se continuera également dans l'idée de pouvoir appuyer aussi bien les opérations

militaires expéditionnaires que la protection du personnel durant ces opérations.

Les capacités actuelles de cybersécurité se trouvent sous l'autorité d'ACOS IS et de DG MR, la Direction Générale *Material Resources*, qui est en charge de l'ensemble des ressources matérielles de la Défense, dont les équipements de communications et d'information font partie. Les capacités futures devront être bâties sur base des capacités existantes, qui seront agrandies et renforcées.

3.2.4.1 ACOS IS

ACOS IS est le Département d'Etat-Major de Renseignement et de Sécurité. Ce service analyse la menace cyber contre les TIC de la Défense, en Belgique mais également à l'étranger lors d'opérations militaires. Il analyse aussi celles concernant les entreprises, organisations et institutions qui sont en lien direct avec le Défense et ses missions.

Afin d'avoir une image plus claire des menaces cybers contre des infrastructures d'organisations internationales situées en Belgique, ACOS IS travaille avec son propre service de renseignement ainsi que son propre service de sécurité, à savoir le Service Général du Renseignement et de la Sécurité (SGRS).

3.2.4.2 InfoOpsGp

L'Information Operations Group est une unité opérationnelle qui appuie les unités de combat. Les tâches premières de cette unité sont d'assurer la communication avec les populations et autorités du théâtre d'opération, de réagir à une éventuelle propagande anti-belge et d'analyser tous les facteurs humains qui pourraient influencer les missions.

Il paraît évident que toutes ces tâches sont effectivement en lien direct avec la gestion de l'information et la capacité d'influence.

4 Analyse

4.1 Comparaison des documents

Une stratégie cohérente se base sur des objectifs stratégiques réalisables. Cependant, peut-on considérer qu'aussi bien les objectifs qui ont été définis politiquement que les objectifs militaires qui en découlent sont suffisamment réalistes ? Existe-t-il des contradictions entre ces objectifs, ou bien se complètent-ils entre eux ?

Dans sa *Cyber Security Strategy*, la Belgique aligne trois objectifs stratégiques (cf §3.1.1). La Défense belge a alors pris en compte ces trois objectifs lorsqu'elle a rédigé le document suivant, le *Cyber Security Strategy for Defence*, afin d'en extraire des objectifs stratégiques applicables à son propre niveau. Elle a, en plus de cela, identifié les effets à obtenir au niveau stratégique militaire[23].

Une approche différente entre la stratégie générale et celle de la Défense belge peut quand même être observée. Le droit à la légitime défense, ainsi que la riposte immédiate par une cyberattaque, dans le respect des dispositions du droit des conflits armés[24], sont des éléments qu'on ne retrouve que dans la stratégie de la Défense, et pas dans la stratégie générale, par exemple.

L'un des piliers de la capacité de cybersécurité de la Défense est ainsi la *Cyber Counter-Offensive*[25].

Il faut bien être conscient que les choix à prendre après une cyberattaque sont difficiles et également très coûteux, que ce soit financièrement ou structurellement. Dans le but d'atténuer les facteurs de risque opérationnel, on pourrait imaginer d'anticiper sur les cyberattaques visant les systèmes et infrastructures critiques nationaux. C'est ici que le concept de cyberdéfense proactive est introduit[26]. La connaissance anticipée des risques fait déjà partie de la stratégie chez Sun Tzu[27]. Selon lui il est important de ne pas rester dans l'ignorance de l'état d'un ennemi, mais on doit connaître la véritable menace, afin de pouvoir l'anticiper. Ces principes intemporels sont pleinement d'application lorsque l'on parle du monde cyber. En effet, il est nettement préférable d'agir avant qu'une situation menaçante ne devienne

[23] Belgische Defensie – ACOS Strat, *Cyber Security Strategy for Defence*, 2014, p. 9.
[24] MONITEUR BELGE, *30 Novembre 1998 - Loi organique des services de renseignement et de sécurité*, Section 2 Art 11 §1 2°.
[25] Belgische Defensie – ACOS Strat, *Cyber Security Strategy for Defence*, 2014, § 8.a.(3), p10.
[26] Seyed Hossein Ahmadpanah, *Proactive Cyber Defense: Security For Government*, CreateSpace Independent Publishing Platform, 2015, 138 p.
[27] *L'art de la guerre* – Chapitre XIII

vraiment un point d'affrontement ou même une crise, avant qu'une cyberattaque ne détruise certaines des infrastructures critiques nationales et que la nation n'ait peut-être plus les capacités de réagir, c.-à-d. de mener à bien une contre-attaque, dans le domaine cyber ou autre.

D'un point de vue diplomatique, il est pourtant difficile de justifier l'emploi proactif de la cyberdéfense. La diplomatie fait d'ailleurs partie des moyens qui doivent être épuisés avant de se lancer dans un conflit.

D'un point de vue juridique, l'usage même des opérations contre-offensives dans le domaine cyber ne sera pas toujours légalement possible. Ce genre d'actions est en effet très délicat et complexe à défendre en regard du droit international, ce qui est principalement dû à l'absence de frontières dans le cyberespace et à l'anonymat relatif des utilisateurs.

Si, dans les grandes lignes, les objectifs et l'ambition de la Défense d'un côté, et ceux du gouvernement de l'autre, se rejoignent sur l'essentiel, à savoir la volonté de protéger la Belgique contre les cybermenaces, ils restent malgré tout concurrentiels, voire même antinomiques dans certains cas. Par exemple, suivant la situation, il pourrait être dans l'intérêt de la Défense de contre-attaquer, mais pas de celui des Affaires étrangères, ce qui laisse présager de longues discussions si ce cas de figure devait se présenter un jour.

4.2 Une arme classique

Mais en évitant, dans son document de stratégie générale, de s'engager dans la réflexion sur le cyberoffensif, la Belgique ne rate-t-elle donc pas une belle opportunité d'élargir son horizon des possibles ?

Ne pas vouloir faire usage d'une cyberdéfense offensive ou proactive, revient à dire qu'il n'y a pas de place et pas de rôle à jouer pour les cybercapacités dans le monde diplomatique. En ce en dépit du fait que, de par le principe de non-imputabilité qui leur est propre, elles autorisent justement plus de flexibilité et offrent une plus grande liberté de manœuvre – ce qui peut être d'une grande utilité dans les négociations (y compris lors des processus de paix).

Mais d'un point de vue étatique, la volonté au niveau militaire d'exécuter des

cyberopérations pourrait influencer les décisions politiques[28]. Il en ressort que, pour les Etats, le facteur limitatif empêchant l'utilisation d'armes cyber est bien la « peur », parce qu'il y a trop d'effets négatifs à redouter. Tout d'abord, les cyberopérations peuvent rapidement avoir un impact sérieux sur la population civile. Ensuite, le risque de dommages collatéraux est élevé. Une attaque directe contre une cible économique d'un adversaire pourrait toucher la propre économie de l'attaquant. Il suffit de se représenter ce que donnerait une attaque contre l'entreprise SWIFT, qui a son bureau principal en Belgique : la grande majorité des transactions financières mondiales ne seraient tout simplement plus exécutées. Et dans le pire des cas, nous ne pouvons certainement pas perdre de vue qu'un cyberincident, s'il était considéré comme un acte relevant de la déclaration de guerre, pourrait facilement conduire à une réplique menée au moyen d'un armement conventionnel.

Dès lors, on peut comprendre que des hésitations subsistent quant à l'utilisation d'armes cyber. Selon Mike McConnel, ancien espion, les effets d'une cyberguerre à grande échelle seraient tout à fait comparables à ceux engendrés par une guerre nucléaire, à savoir la destruction de la civilisation telle que nous la connaissons[29].

Tout doit naturellement être replacé dans une perspective correcte. La menace cyber est réelle et constitue pour tous une donnée importante mais, dans la dernière décennie, à peine vingt des cent-vingt-six Nations et groupes rivalisant entre eux se sont engagés sur la voie des cyberconflits. De plus, leurs actions sont restées assez limitées en termes d'amplitude et de fréquence[30]. Les plus grosses opérations cyber menées jusqu'ici ont été basées sur des attaques de type DDoS (Distributed Denial of Service), avec parfois, il est vrai, un volume et une complexité remarquables.

Tout ceci ne veut certainement pas dire que nous devons ignorer ce qui se trame dans le cyberespace. Une grande partie des activités récentes menées par la Russie, mais et surtout par la Chine, peuvent sans hésitation être classées en tant que cyberespionnage[31]. Toutefois, ici aussi, un changement se profile. Le fait que l'on puisse de mieux en mieux retracer le lien entre les faits et leurs auteurs présumés – le

[28] Brandon Valeriano, Ryan C. Maness, *Cyber War vesrsus Cyber realities : Cyber conflict in the International System*, Oxford University Press, 2015, p. 16.
[29] « War in the fifth domain : Are the mouse and keyboard the new weapons of conflict ? », The Economist, 2010, http://www.econimist.com/node/16478792
[30] Brandon Valeriano, Ryan C. Maness, *Cyber War vesrsus Cyber realities : Cyber conflict in the International System*, Oxford University Press, 2015, p. 18.
[31] *Redline drawn : China recalculates its use of cyber espionage*, Fireeye iSight Intelligence, 2016, p. 3.

principe de non-imputabilité perdant du coup une partie de sa valeur – permet d'exposer ces derniers au grand jour.

Dans ce cadre, la diplomatie pourrait avoir un effet dissuasif en abordant le sujet de ces cyberincidents par les voies diplomatiques et politiques[32], bien que sans l'attention médiatique nécessaire. Suite à cela, ces Nations seraient, d'un côté, montrées du doigt par le monde entier, et se rendraient compte qu'elles ne peuvent pas toujours se tirer indemnes de tout, et, d'un autre côté, ça permettrait de ne pas trop faire monter la tension et de ne pas miner les efforts de coopération existants, comme dans le domaine spatial ou par exemple en Syrie, où la Russie est autant un partenaire qu'un opposant.

Entretemps, de grandes quantités de données sensibles ont quand même été détournées et, encore une fois, cela nous a prouvé que nos systèmes ne sont pas si étanches que nous voudrions le croire.

Au final, le rôle qui devrait être réservé à d'éventuelles cybercapacités offensives au sein de nos organismes étatiques devrait principalement être celui de la collecte de renseignements et de l'espionnage. Cependant, il ne faudrait pas en sous-estimer, voire en oublier, l'importance de la place qu'occupe le cyberespace dans le mécanisme des opérations de propagande. Là non plus, nous ne devons pas rester inactifs.

Et tout ceci n'enlève rien au fait que nous devons être capables de réagir – bien que de façon non-offensive – contre des cyber-hackers isolés ou même contre des groupes organisés de cybercriminels.

[32] « Obama hints at sanctions against China over Cyberattacks », The New York Time, 16 Sep 2015, http://www.nytimes.com/2015/09/17/us/politics/obama-hints-at-sanctions-against-china-over-cyberattacks.html

5 Les enjeux et les défis

5.1 Commandement et Conduite

Il devient clair, à la lecture du document *Cyber Security Strategy for Defence*, qu'une structure de C2 (Commandement et Conduite) est nécessaire.

La Belgique possède-t-elle déjà une structure C2 de ce type ? Sinon, est-il planifié d'en créer une ? Et si oui, où y a-t-il des possibilités d'amélioration ?

Lorsque nous parlons d'une structure C2 en matière de cybersécurité, nous avons à l'esprit une structure qui tient compte autant des objectifs militaires que des objectifs civil/politiques.

Nous avons donc besoin d'une structure de commandement commune au sein d'une approche intégrée prenant en compte le monde militaire et civil, et qui inclut les menaces contre les infrastructures civiles. Sur ce plan, la Belgique a bien travaillé, et un organe C2 commun a été identifié en la plateforme BelNIS. Mais en pratique, cet organe ne résout pas tout, car on réfléchit encore trop « en silo », ce qui occasionne une possibilité que des lacunes persistent dans nos défenses ainsi que dans la sécurité.

Au niveau militaire également, une approche commune entre les différentes composantes et les services est d'une importance majeure. Au jour d'aujourd'hui, les décideurs militaires croient en une infrastructure de TIC résiliente et robuste, afin que les décisions puissent continuer à être prises dans les plus brefs délais, même et surtout lors de crises. Un dérangement ou une coupure dans le réseau de communication, dans les systèmes TIC ou même dans les informations qui circulent au travers et qui y sont traitées, peut avoir des conséquences catastrophiques. Et à ce sujet, nous ne devons plus uniquement penser aux réactions à avoir lorsqu'un missile balistique à longue portée est tiré, mais également à celles à avoir lorsque, par exemple, le système ADS-B, utilisé par les avions afin d'éviter les collisions en vol, se retrouve brouillé ou même désactivé suite à des actions extérieures.

A côté d'une structure C2 commune, des processus de collaboration doivent être mis en œuvre. Par conséquent, et au risque de nous répéter, cette structure devra tenir compte aussi bien des objectifs militaires que des objectifs civils et politiques. Une bonne collaboration entre tous les services concernés est nécessaire, et ceci est

valable aussi bien pour les services militaires responsables de la cyberdéfense, que pour le CCB fédéral, ou même pour les services de la police fédérale (Computer Crime Unit, l'unité fédérale en charge des crimes et délits liés au cyberespace). Ce niveau de collaboration est atteint de façon partielle grâce à la plateforme BelNIS, mais celle-ci ne prévoit ni une Recognized Cyber Picture unique, ni une unité de commandement. Un centre multidisciplinaire et interdépartemental, suivant les modèles du MIK (Marietiem Informatie Kruispunt – carrefour d'information maritime) ou du LInK (Luchtvaart Informatie Kruispunt – Carrefour d'information aéronautique), et dédié à la cybersécurité, pourrait permettre de mener à bien la création de cette Cyber Picture unifiée et l'adoption d'une vision commune sur les problèmes et les mesures à y apporter. Un tel centre devrait cependant opérer selon des directives claires et des objectifs précis, établis par le monde politique, et qui seraient continuellement adaptés en fonction des analyses de l'environnement et de la menace.

5.2 Infrastructures critiques

Dans la même optique, la nécessité de garder une chaîne de commandement et de contrôle ininterrompue s'impose donc. Dès lors, les réseaux de communication sont certainement à considérer comme faisant partie des infrastructures critiques. Ceci dit, avons-nous une bonne définition de ces infrastructures critiques ? Et est-ce que ces infrastructures critiques peuvent être protégées de façon efficace ?

La définition légale des infrastructures critiques se retrouve dans la loi relative à la sécurité et la protection des infrastructures critiques[33], et est formulée comme suit :

> « "infrastructure critique" : installation, système ou partie de celui-ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions. »

On peut ainsi en déduire que le secteur des communications électroniques est bien repris légalement comme l'une des infrastructures critiques belges.

[33] MONITEUR BELGE, *1 Juillet 2011 - Loi relative à la sécurité et la protection des infrastructures critiques*, Art 3 4°.

La protection des réseaux de communication critiques n'est pas seulement importante du point de vue du C2, mais également du point de vue économique, car l'accès à internet est devenu vital dans notre monde hyperconnecté.

D'une façon générale, on peut considérer la Belgique comme un pays « numérique ». Plus concrètement, les technologies de l'information et de la communication (TIC), mises ensemble avec la connectivité à haut débit, jouent un rôle important dans le pays. La Belgique est le premier de la classe au sein de l'UE des 15 en ce qui concerne le degré de couverture des réseaux ayant une capacité de téléchargement vers l'aval de 30 Mbps ou plus, les réseaux qu'on appelle *Next Generation Acces* (NGA)[34]. Cette bonne prestation au niveau de la rapidité et de la couverture de l'infrastructure à haut débit fait que la Belgique se classe bien en matière de performance numérique, par rapport aux autres pays européens. De plus, le secteur des télécommunications contribue considérablement à l'économie et à la société. Malgré le fait que les secteurs des TIC[35] ne représentent que 3,7% dans l'économie, ils sont responsables de 7,7% de la croissance économique depuis 1995[36].

En tenant compte du fait que la Belgique est actuellement un pays fortement numérisé, et que donc l'infrastructure télécom à haut débit est un atout pour le pays, ainsi que du fait que les secteurs TIC apportent autant au niveau de la croissance de l'économie, la Belgique a tout intérêt à continuer à investir dans la numérisation et les développement numériques.

Mais toute médaille a un revers : une infrastructure à haut débit performant entraîne une augmentation proportionnelle des risques au niveau cyber. Ces risques doivent être rapportés aux autorités gouvernementales, qui doivent dès lors être capable d'y réagir sans pour autant sortir du cadre légal existant, le tout avec les moyens alloués et dans les plus brefs délais.

Les projets démarrés par le CCB, c'est à dire le Cyberplan d'urgence et l'*Early Warning*, afin de renforcer la cybersécurité dans les secteurs vitaux de la Belgique et donc cruciaux pour la sécurité de la population belge, forment un bon point de départ. Malgré cela, le Cyberplan d'urgence reste pour l'instant limité à des réactions

[34] Belgische Federale Regering - Centrale Raad voor het Bedrijfsleven, *Belgium 2.0 – Naar een succesvolle digitale transformatie van de economie : de rol van breedbandinfrastructuur en andere elementen*, 2015, graphique 2-2
[35] *Ibid.* - définition des secteurs des TIC, p. 19.
[36] *Ibid.*

après coup. Une analyse continuelle des menaces est nécessaire, mais ne peut se faire que si les informations concernant les vulnérabilités, les cyberattaques repérées, etc... sont partagées avec les opérateurs des infrastructures critiques et les organes fédéraux concernés.

C'est également dans le cadre de ce Cyberplan d'urgence que la Défense belge peut assister et soutenir d'autres organes fédéraux. Cette assistance ne consiste pas uniquement en une expertise sur le plan cyber mais couvre également d'autres actions, et ce, dans une optique plus vaste d'aide à la Nation, comme par exemple déjà prévu si le plan de délestage[37] devait un jour être activé.

Tout ceci rend les informations sur la mise en œuvre d'une stratégie ou d'un plan concernant la protection des infrastructures critiques assez sensibles. De ce fait, leur publicité est très limitée.

5.3 Aspect légal

Mais où en est-on avec l'aspect légal et le cadre juridique?

« *Le cadre juridique belge manque de clarté et les informations sur sa mise en œuvre restent lacunaires* », relève l'étude de l'entreprise « BSA *The Software Alliance* » menée en 2015[38].

Effectivement, le cadre juridique autour de la cybersécurité en Belgique apparaît comme un peu flou.

Suivant ce qu'il est défini dans la loi relative à la sécurité et la protection des infrastructures critiques[39], chaque exploitant d'une infrastructure critique doit élaborer un plan de sécurité de l'exploitant (PSE), qui prend notamment en compte le cyber risque. Mais ce cadre législatif devrait aller plus loin. Il devrait mettre en place une obligation de déclaration pour les opérateurs des infrastructures critiques, et définir un cadre légal afin que les services concernés puissent prendre les actions nécessaires, de façon à ce que :

[37] Le délestage est l'arrêt temporaire de la fourniture d'électricité à une partie des clients finaux dans certaines parties du pays. Le plan de délestage du réseau de transport d'électricité est établi dans l'arrêté ministériel du 13 novembre 2015 modifiant l'arrêté ministériel du 3 juin 2005.
[38] « L'arsenal juridique belge contre la cybercriminalité positivement évalué », Belga, 03 mars 2015 – 20:46, https://www.rtbf.be/info/medias/detail_l-arsenal-juridique-belge-contre-la-cybercriminalite-positivement-evalue?id=8921607
[39] MONITEUR BELGE, *1 Juillet 2011 - Loi relative à la sécurité et la protection des infrastructures critiques*, Art 13

- Les services de l'État soient autorisés à identifier l'origine et à neutraliser les effets d'une menace cyber.
- Les opérateurs d'importance vitale et les compagnies stratégiques doivent mettre en œuvre les mesures de cybersécurité adéquates et notifier les incidents cyber.
- Les services de l'État soient autorisés à accéder aux métadonnées pour alerter les Fournisseurs d'Accès à Internet (FAI) et les opérateurs en cas de menace cyber sérieuse.

Une législation exigeant une inventorisation des systèmes et un niveau de classification des informations traitées existe effectivement, ainsi que, pour chaque niveau, l'établissement d'un lien avec le risque qu'il représente pour l'un de nos intérêts[40]. Par contre, la Belgique n'a pas encore de mesures obligeant à un audit annuel au niveau de la cybersécurité, même si l'exécution de ce genre d'audit fait pourtant partie des lignes fortes du *Cyber Security Strategy*[41].

En ce qui concerne la Défense belge, la classification des systèmes ainsi que les audits de sécurité sont des choses qui font partie de la vie courante. Les formats d'audits qu'elle utilise pourraient dès lors servir de modèles pour la suite.

Cependant, on peut noter des avancées à l'intérieur même de ce cadre légal. C'est sur le plan de l'investigation numérique légale qu'elles sont le plus remarquable. Il y a peu, la loi concernant les méthodes particulières de recherche et d'investigation (dite BOM, du néerlandais « *Bijzondere Opsporings Methodes* ») a été adaptée aux évolutions technologiques actuelles[42]. Ainsi, les règles concernant les écoutes de conversations menées via des applications mobiles (telles que WhatsApp ou Skype), le piratage d'ordinateurs et d'autres appareils liés à internet, la copie et la conservation de données dans le cadre d'une enquête, ont été modernisées et mieux adaptées au 21^{e} siècle.

Un avant-projet de loi, daté du 17 mars 2016, élargit également les méthodes particulières de renseignements (dite BIM, du néerlandais « *Bijzondere Inlichtingen Methodes* ») pour les services de renseignements nationaux, soit la Sûreté de l'Etat, (le service de renseignement civil), et le service de renseignement militaire SGRS.

[40] MONITEUR BELGE, *11 Décembre 1998 - Loi relative à la classification et aux habilitations de sécurité*
[41] Belgische Federale regering, *Cyber Security Strategy*, 2012, p. 12 § 3.4
[42] Het journaal 1, VRT, 23 février 2017 13:13

5.4 **Hackers éthiques**

Comment devrions-nous considérer les hackers : comme des auxiliaires de l'Etat ou comme de simples criminels ?

Différentes formes de criminalité informatique sont décrites dans la législation[43]. Elles sont toutes punissables par la loi, y compris dans le cas de hackers animés de « bonnes » intentions[44]. Chaque cyberexpert qui, au jour d'aujourd'hui, tombe sur une faille dans un système TIC officiel – de façon délibérée ou pas, mais sans autorisation préalable– et en avertit les autorités, risque d'être poursuivi judiciairement. Mais une amélioration est en vue pour ces hackers qui se disent éthiques, qui considèrent qu'ils travaillent au profit de la communauté. Un hacker éthique est bien différent d'un pirate informatique, ce dernier étant un cybercriminel. Le gouvernement voudrait d'ailleurs mettre au point une politique par laquelle ces hackers éthiques seraient, dans une certaine mesure, protégés contre les conséquences légales de leurs actes[45]. Au lieu de se placer dans une position défensive par rapport à eux, l'idée serait d'utiliser leurs connaissances et compétences d'une façon optimale, afin de détecter les failles dans les réseaux, qui sont loin d'être aussi sécurisés que ce que l'on pense. Cependant, pour l'instant, selon la législation belge, une cyber-intrusion est toujours mise sur le même pied qu'une intrusion physique. Le gouvernement, avec le CCB, est donc occupé à mettre au point un « code de conduite » pour hackers éthiques. Ainsi, il pourrait malgré tout profiter des connaissances et des compétences de ces hackers, mais sans ouvrir la porte à tout et n'importe quoi. Une proposition de texte a été faite fin de l'année passée, et, comme le dit Michel de Bruycker, directeur du CCB : "*Notre texte a été positivement accueilli par la communauté des pirates informatiques*"[46].

En regardant plus en détail la cybercriminalité, celle-ci est actuellement effectivement considérée comme une priorité par le gouvernement belge, les entreprises et autres organisations nationales et internationales car, même si la cybercriminalité ne laisse pas de trace de sang et par conséquent semble moins une

[43] Computercriminaliteit, Belgium.be - Justitie, http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/
[44] Computercriminaliteit - hacking, Belgium.be - Justitie, http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/hacking
[45] « Digitale klokkenluiders krijgen wettelijk kader om te hacken », standaard.be, 08 janvier 2016 - 03:00, http://www.standaard.be/cnt/dmf20160107_02055042
[46] « Un cadre juridique pour autoriser les hackers éthiques », Belga, 08 décembre 2016, http://fr.metrotime.be/2016/12/08/news/un-cadre-juridique-pour-autoriser-les-hackers-ethiques/

problématique criminelle, en Belgique, elle constituait en 2015 environs 65% de la criminalité économique rapportée. Même si toutes les victimes ne se signalent pas, les chiffres belges pour ce type de criminalité sont le double de la moyenne mondiale[47,48].

Paradoxalement, c'est là la preuve que la Belgique a pris plusieurs bonnes initiatives en matière de cybersécurité, notamment par l'adoption de sa stratégie de cybersécurité et l'ouverture du Centre pour la Cybersécurité Belge[49]. Effectivement, la hauteur des chiffres peut être clairement imputée au plus grand nombre de cas découverts et déclarés dans le cadre des mécanismes découlant de ces initiatives.

« *Il n'y a pas de frontière au hacking* »[50], nous dit Inti de Ceukelaire, un hacker éthique flamand. D'après lui, le phénomène (de hacking) est encore et toujours sous-estimé : «Je trouve que, pour l'instant, ça va encore. Mais je parie que, dans cinq ans, les premiers meurtres par hacking seront commis. Pensez donc aux pacemakers. Ce seront des meurtres à distance, il n'y aura plus besoin de se promener avec une arme. » En effet, fin 2016, un groupe d'ingénieurs de la KU Leuven (Université Catholique de Louvain) a prouvé qu'il était possible de pirater des pacemakers et des défibrillateurs[51]. Déjà en 2015, deux hackers avaient déjà démontré que le piratage d'une voiture à distance était possible, et qu'il y avait donc moyen de prendre le contrôle de plusieurs fonctions du véhicule sans même le toucher[52]. Ceci, mis en parallèle avec les cyberattaques lancées contre des centaines de foyers finnois à la fin de l'an passé[53], n'est qu'un avant-goût de ce qui est possible et de ce qui pourrait nous attendre dans le futur si nous ne réagissons pas de façon drastique contre ces menaces cybers.

[47] « Quand prendra-t-on la cybercriminalité au sérieux? », Benoît Gagnon, 14 septembre 2016 – 10:46, http://branchez-vous.com/2016/09/14/quand-prendra-t-on-la-cybercriminalite-au-serieux/

[48] « La cybercriminalité représente 65% des cas de criminalité économique signalés en Belgique », Belga, 25 février 2016 – 15:57, http://www.lalibre.be/actu/belgique/la-cybercriminalite-represente-65-des-cas-de-criminalite-economique-signales-en-belgique-56cf15423570ebb7a8ba086c

[49] « Lutte contre la cybercriminalité: la Belgique est performante », Belga, 3 mars 2015 – 19:55, http://www.lavenir.net/cnt/dmf20150303_00610787

[50] « Ethische hacker: "Koude Oorlog is nooit gestopt, maar gaat online verder" », deredactie.be, 11 janvier 2017 – 15:52, http://deredactie.be/cm/vrtnieuws/buitenland/1.2863877#

[51] « Pacemaker hacken ? Geen fictie zo blijkt », Het Laatste Nieuws, 16 novembre 2016 – 19:59, http://www.hln.be/hln/nl/957/Binnenland/article/detail/3006452/2016/11/26/ Pacemaker-hacken-Geen-fictie-zo-blijkt.dhtml

[52] « Hackers Remotely Kill a Jeep on the Highway—With Me in It », WIRED on YouTube, 21 juillet 2015, https://www.youtube.com/watch?v=MK0SrxBC1xs

[53] « Hacker lassen Finnen frieren », Der Spiegel Online, 08 novembre 2016 http://www.spiegel.de/netzwelt/web/finnland-hacker-schalten-heizungen-aus-a-1120234.html

5.5 Meilleure cybersécurité

Avec toutes ces cybermenaces et les perspectives d'avenir actuelles, comment pouvons-nous améliorer notre cybersécurité ?

Dès la conception de nouveaux systèmes, on doit s'attarder sur l'aspect sécurité. Comme déjà mentionné dans §2.3 plus haut, la Sécurité des Systèmes d'Information (SSI) forme, avec la cyberdéfense, la cybersécurité. En tenant compte de l'aspect de SSI dès le lancement d'un projet, on peut mieux orienter certains choix. Ainsi, on peut directement trouver un juste milieu entre une sécurité optimale et les frais qui y sont liés, même si des failles sont toujours possibles. Une forteresse cyber dans un monde connecté est irréalisable.

Nous devons même aller plus loin. Chacun doit penser quotidiennement à la sécurité. C'est un très grand changement de mentalités qui devrait se produire chez tout un chacun et qui est important, l'utilisateur étant considéré comme le maillon le plus faible. Les autorités belges accordent donc beaucoup d'importance au fait d'informer la population à propos de la cybersécurité, en collaboration avec les institutions académiques dans le but que ces dernières élargissent leur offre en matière de formations portant sur le cyber en général, et plus particulièrement sur les aspects de cybersécurité et des menaces cybers.

Dans la même optique, informer et sensibiliser tous les intervenants aux dangers d'internet est une ligne d'action clairement identifiable dans les différentes stratégies belges, car, de nouveau, l'homme reste le maillon le plus faible. Ces personnes doivent être encouragées à surfer sur le net de façon sécurisée. Elles doivent savoir résister à leur curiosité pour éviter le clic de trop, celui qui va ouvrir leur porte digitale au hameçonnage et aux « rançongiciels ». L'initiative de *safe on web*, (disponible sur safeonweb.be), mise en œuvre par le CCB, démontre une bonne capacité à atteindre cet objectif de prévention, et offre en plus des propositions et des solutions aux problèmes éventuellement déjà rencontrés.

Ce changement dans les mentalités doit également se produire au sein même de la Défense. Au vu de la technicité et de l'interconnexion de tous les systèmes d'armes, chaque projet doit être soigneusement étudié, en tenant certainement compte des aspects du SSI en particulier, et de la cybersécurité en général. C'est pour cela que la cybersécurité, et plus basiquement la sécurité, devraient être pris en compte comme

ligne de développement lors du *capability definition process* DOTMLPFI[54] (*Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, Interoperability*) en usage à la Défense.

5.6 Formation et éducation

La Belgique commence elle aussi à mettre sur pied ses propres cybercapacités. Mais dispose-t-elle déjà de l'expertise nécessaire ?

Début 2016, la Belgique comptait à peine 2000 experts du cybercrime, selon Kurt Callewaert, maître de conférence à l'université *Hogeschool West-Vlaanderen* (HoWest)[55]. HoWest fournit depuis peu des hackers éthiques, étant pour l'instant la seule université reconnue en Belgique qui puisse le faire. C'est un grand pas en avant, et, mis en lien avec le *Cyber Security Challenge Belgium*[56], constitue un pas dans la bonne direction afin d'élargir l'expertise dans le domaine cyber en collaboration avec le monde académique.

Comme déjà mentionné dans les différents documents belges concernant la cyberstratégie, l'éducation constitue l'une des pierres angulaires d'une politique cohérente en la matière. Formation, connaissance et compétences sont complémentaires et forment ensemble la base nécessaire afin de pouvoir appréhender la problématique cyber dans sa globalité et ainsi de pouvoir conseiller correctement les plus hauts niveaux. Cependant, pour atteindre cet objectif, il faudrait avoir la possibilité de faire carrière dans ce métier, ce qui est loin d'être le cas actuellement. De plus, il est conseillé de laisser en place le personnel ayant un pouvoir décisionnaire pour une période d'au moins six ans, et ce en raison des technicités et spécificités du métier et de la nécessité d'assurer une continuité du commandement mais également d'obtenir une maîtrise plus complète de la problématique. A l'heure actuelle, la politique de gestions des mutations ne permet pas non plus de suivre cette recommandation.

Et par-dessus tout cela, il est nécessaire que la qualité d'expertise dans le cyberdomaine soit suffisamment diversifiée. De fait, afin de bien saisir l'étendue des risques et des menaces cyber dans leur globalité, on a besoin de plus qu'uniquement

[54] Belgian Defence – ACOS Strat, *ACST-APG-CGEN-SXX-001 / DTATL Transformation from Strategic Orientations to Capabilities for Operations*, 2007, p. 5.
[55] « Studenten willen Robin Hood zijn », standaard.be, 08 janvier 2016 – 03:00, http://www.standaard.be/cnt/dmf20160107_02055046
[56] https://www.cybersecuritychallenge.be/

des « *geeks* » en informatique : on a aussi besoin de sociologues, de linguistes et de politologues pour pouvoir répondre aux différentes facettes du problème cyber.

5.7 Computer Network Operations

Mais pourquoi aurions-nous besoin d'une expertise aussi diversifiée ? Le cyberdomaine comprendrait donc tellement plus que juste les *Computer Network Operations* ?

En élargissant notre réflexion, on peut se rendre très vite compte que la problématique est bien plus vaste que cela. Le cyberespace est constitué de trois couches dans lesquelles les opérations cyber peuvent être effectuées. Ces trois couches sont représentées dans le tableau suivant[57].

	Composants	Forme d'attaque possible
Couche physique	matériel, serveurs, ordinateurs, réseaux, câbles, satellites, infrastructures connectées	Couper des câbles sous-marins, détruire des satellites, détruire les bâtiments accueillant les serveurs, utilisation de bombes EMP
Couche logique	Protocoles (communication, adressage, transport), systèmes d'exploitation, logiciels, données, contenus	Attaques via le code : hacking, introduction des virus
Couche cognitive et humaine	Perception, sémantique, usages (réseaux sociaux, commerce, recherche, communication, partage de connaissance, désinformation, propagande, renseignements, …), Culture (langue, politique, liberté, …), identités réelles	• introduire des messages modifiant les perceptions • mener des opérations de propagande, opération d'information • hacking cognitif

La cyberguerre ne se limite donc pas qu'aux *Computer Network Operations*, loin de là. La guerre électronique appartient également au spectre de la cyberguerre. Et dès que l'on effectue des opérations dans la couche cognitive et humaine, on se retrouve vite dans des opérations psychologiques et dans de la guerre d'information.

Nous reviendrons sur cette dernière au point suivant, car elle est importante, d'autant plus que la guerre du futur a de grandes chances d'être un conflit où l'un des enjeux principaux sera le déni d'information.

[57] Basé sur le tableau de Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, (Collection Cyberconflits et Cybercriminalité), éditions Hermès Lavoisier, Paris, 2011

Avant cela, penchons-nous d'abord sur l'information : dans notre société moderne, ce sont principalement l'accès au flux d'information, ainsi que le flux d'information en lui-même, que ce soit à l'intérieur ou entre les nations, qui ont un intérêt pour l'économie, les relations internationales et la vie sociale. De la même façon, l'information est importante pour la capacité à combattre des forces armées actuelles. Une grande partie des communications passent maintenant par des connections filaires ou électromagnétiques, comme la radio et le satellite. Chacun de ces types de connections a ses faiblesses, et il est toujours possible de les perturber – via le brouillage – ou même de les couper complètement.

En effet, chaque flux d'information, qu'il soit physique ou virtuel, fournit des opportunités aux adversaires.

Les contre-mesures visant à dégrader le flux d'information ennemi et, à l'inverse, à protéger notre propre information contre toute intrusion ou ruse ennemies, et l'exploitation, pour notre propre profit, des renseignements obtenus hors des canaux d'information ennemis, tout cela fait partie de la guerre d'information qui se superpose au reste des opérations militaires.

Comme déjà mentionné par Boeing en 1976[58], dans le futur, les contre-mesures visant le flux externe d'information des systèmes d'armes deviendront si cruciales qu'elles pourront influencer le résultat des engagements[59].

En fait, les premières actions de guerre de l'information peuvent être entreprises plusieurs années avant que les hostilités n'éclatent ouvertement. Elles peuvent également rester longtemps dissimulées à l'opposant. Dans cette optique générale assez large, la guerre d'information infiltre et impacte complètement l'attitude des belligérants en devenir. Cet impact pourrait aller depuis la redéfinition des nécessités des missions jusqu'à l'influence des résultats d'engagements spécifiques, en passant par la modification des schémas de développement et de déploiement des systèmes d'armes.

Par conséquent, si nous tenons compte des cyberopérations qui sont menées au niveau de la couche cognitive, il devient clair que nous avons besoin de bien plus que simplement des *geeks* qui resteraient derrière leurs ordinateurs. Pour effectuer

[58] T. Rona, *Weapon Systems and Information War*, The Boeing Aerospace Company, julliet 1976, chapitre 2
[59] *Ibid.*

une analyse correcte de la cybermenace, nous devons pouvoir comprendre de façon complète le contenu des communications cyber. C'est pour cela qu'au sein des groupes concernés, nous avons également besoin de la connaissance qui nous permette de comprendre de façon approfondie le groupe sociétal qui est à l'origine de chaque menace, et ce, d'un point de vue idéologique, linguistique et culturel. Tant au niveau fédéral qu'au niveau de la Défense, une attention suffisante doit être portée à ce dernier point.

5.8 Guerre de l'information

En 2001, le grand public a fait connaissance avec l'expression « guerre asymétrique », en lien avec les agissements d'Al Qaïda. Maintenant, il découvre la « cyberguerre » au travers des actions, entre autres, de la Chine et de la Russie. Mais que recouvre ce type de guerre en réalité, et sommes-nous prêts pour ça ? Quels sont nos points forts et à quoi devons-nous accorder plus d'attention ?

Dans le cyberespace, les opérations sont fortement liées au contrôle de l'information. Désinformation, déception et fausses informations font partie de cette guerre de l'information. Ensemble avec les opérations psychologiques, la guerre cyber et la guerre d'information sont combiné en une seule organisation de combat, qui sera au cœur de toute guerre dans l'avenir.

Cette façon de combattre a déjà été utilisée ouvertement par la Russie. D'un côté, nous méprisons les Russes pour leur machine de propagande basée sur des informations tronquées ou manipulées. Ils utilisent de fausses nouvelles, des documents falsifiés, et pratiquent la désinformation dans le cadre de campagnes coordonnées qui ont pour but d'influencer aussi bien leur population nationale que la société internationale. La Belgique a d'ailleurs déjà été victime de ce genre de propagande lors des bombardements en Syrie. Les F-16 belges avaient alors été accusés d'avoir bombardé des cibles civiles[60]. D'un autre côté, nous devrions admirer la Russie pour ces mêmes raisons. Aucune nation au sein de l'OTAN n'a une machinerie d'influence équivalente et aussi bien rôdée.

Et pourtant, c'est quelque chose sur lequel nous devrions porter nos efforts, non pas tellement pour la diffusion de fausses informations mais bien pour arriver à

60 « Defensie ontkent dat Belgische F-16s bombardementen hebben uitgevoerd in Aleppo », de redactie.be, 19 octobre 2016 – 07:24, http://deredactie.be/cm/vrtnieuws/buitenland/1.2797185

contrebalancer la désinformation (de quelque origine qu'elle soit) de façon cohérente et construite, et à informer le public en lui présentant les actions et les faits tels qu'ils se sont réellement produits. Le Parlement Européen en a déjà pris conscience, comme l'a démontré l'adoption fin 2016 d'un texte sur la communication stratégique de l'Union, qui vise à contrer toute propagande dirigée contre elle[61]. Dans le même élan, l'OTAN mène aussi des actions dans ce domaine, la plus visible étant la création d'un centre d'excellence OTAN dans le domaine de la communication stratégique, le *NATO Strategic Communications Centre of Excellence* à Riga[62].

Pour l'instant, plusieurs nations occidentales sont en train d'investir des millions d'euros afin d'amener leurs capacités de guerre d'information au niveau des chinois et des russes. La cyberdéfense fait partie de cet effort, spécifiquement quand on parle des réseaux électronique de communication.

Pour la Belgique, c'est l'InfoOpsGp qui devrait tenir ce rôle dans lequel leurs connaissances, compétences et systèmes, actuellement affectés principalement à des tâches tactiques, pourraient être employés dans un but de contre-déception et d'influence à notre profit, en collaboration avec d'autres services tels que DG COM (Direction Générale Communications), ACOS IS et ACOS Strat, et ce, dans le cadre de la cyberguerre. On pourrait même aller jusqu'à dire que l'influence est la forme douce de la cyberguerre, le « *soft* »-cyber.

Il y a une forte interaction entre la guerre d'information d'un côté, c'est-à-dire la propagande civile et les opérations psychologiques, et la guerre cyber de l'autre côté. Les deux sont mêmes étroitement liées. Comme déjà souligné au § 5.7, la prochaine guerre sera très probablement un combat qui se jouera autour de l'information. Et, actuellement, nous ne sommes pas prêt à pour ce genre de conflit.

5.9 Organisation

Mais où devrions-nous placer le cyber dans notre organisation militaire ? Faudrait-il l'intégrer dans une nouvelle armée/composante ou service ?

Pendant la réunion des ministres de la défense de l'OTAN qui s'est déroulée du 16 au 17 février 2017, il a été convenu d'une feuille de route pour la mise en œuvre du cyberespace comme domaine opérationnel.

[61] P8_TA(2016)0441 : EU strategic communication to counteract anti-EU propaganda by third parties, Parlement européen, 23 novembre 2016
[62] NATO StraCom COE, http://www.stratcomcoe.org/history

Ceci cadre en partie avec la vision stratégique de la Belgique, où l'entièreté du Renseignement-Cyber-Influence forme le quatrième domaine capacitaire. De plus, le cyberespace est transversal par rapport aux quatre domaines conventionnels : terre, mer, air, espace. La Belgique a donc assez logiquement choisi d'incorporer le pilier cyber au sein d'ACOS IS, avec un appui assuré par d'autres DG et ACOS.

Le domaine cyber et le domaine de l'information étant liés, il est nécessaire de coupler des renseignements issus du domaine de l'information à une capacité d'analyse cohérente. Tous ces éléments sont présents dans le domaine capacitaire belge Renseignement-Cyber-Influence. Mais, ils ne constituent pas à eux seuls la clé pour l'implémentation réussie d'une bonne cybersécurité, car ils restent très différents, même en étant rassemblés au sein d'une seule capacité Pour atteindre l'efficience, ils ne doivent en aucun cas travailler chacun dans leur coin mais bien collaborer et échanger les informations entre eux. Alors seulement, ils seront en mesure d'évaluer correctement la menace cyber et de soumettre aux décideurs des avis opportuns, de façon à ce que ces derniers puissent orienter leur politique où et quand cela se révèle nécessaire

5.10 Décideurs politiques

Quel rôle doit-on alors spécifiquement réserver aux responsables politiques fédéraux ?

Pour pouvoir implémenter une cyberstratégie adéquate, les décideurs politiques doivent s'impliquer de façon active dans le processus du *Plan-Do-Check-Act*. Il est nécessaire que les décideurs définissent bien les priorités qu'ils veulent placer ainsi que leurs propres objectifs politiques, et qu'ils valident les objectifs stratégiques définis par, entre autre, la Défense belge. Mais les décideurs doivent également adapter leurs objectifs ou leurs priorités lorsque les analyses menées par les différentes agences nationales le requièrent.

Mais la Belgique a une structure politique complexe. Pour définir une politique efficace qui pourrait mettre en pratique une cyberstratégie convaincante, il faudrait une vision politique à long terme, car cela nécessite des ressources, aussi bien sur le plan personnel que sur le plan budgétaire. Il faut donc fixer des priorités, ce qui nécessite de consentir aux investissements correspondants tout en tenant compte des conséquences en découlant.

Le cœur du problème est le court terme sur base duquel on travaille. Il n'existe en Belgique que la perspective courte, une perspective qui vise jusqu'aux élections suivantes. La définition d'une vraie vision à long terme exige que tous les organismes politiques du pays s'accordent sur les objectifs stratégiques qu'ils veulent atteindre. On ne peut donc certainement pas se cantonner à une politique consistant à uniquement réagir à des situations qui se sont déjà produites. Il faut mettre au point des mesures de façon préventive, aussi bien en mode défensif qu'offensif, et le tout sans perdre de vue le cadre général de l'information. Dans le contexte belge des communautés et des régions, il n'est pas évident d'arriver à un accord et à la mise au point d'une approche politique commune claire.

Mais ne regardons pas uniquement au sein de notre pays. Une coopération internationale est nécessaire, les menaces cyber constituant un problème global. Nous devons donc maintenir une portée internationale à nos stratégies de cybersécurité tout en gardant à l'esprit les efforts que nous pouvons fournir en coopération avec des partenaires ou des alliés afin d'obtenir un partage global de l'information en ce qui concerne les menaces cyber, les solutions possibles et les moyens de protection développés.

Mais n'oublions jamais que, dans le domaine cyber, nous n'avons pas d'amis. Nous sommes tous des concurrents, et certains de ces concurrents peuvent se montrer assez agressifs[63,64].

5.11 Dissuasion cyber

Mais comment allons-nous, en tant que communauté ouverte, gérer le dilemme entre la liberté d'information et le contrôle public d'une part, et la protection de nos propres intérêts nationaux dans ce milieu mouvant, d'autre part ?

Le cyberespace doit rester un lieu sûr, que ce soit pour les entreprises de toutes tailles et les particuliers, ou pour le gouvernement et ses différents départements, ses multiples services publics et ses ministères. Pour en arriver là, la mise en place de mesures de protection et d'un ensemble de réactions adéquates est une étape obligée. Mais, pour ce faire, il faut tout d'abord identifier les vulnérabilités potentielles.

[63] « NSA bespioneert Belgische ambassade », Belga, 24 février 2016 – 13:27, http://www.gva.be/cnt/dmf20160224_02146892/nsa-bespioneert-belgische-ambassade
[64] « NSA bespioneert nog steeds Belgacom », VTM, 29 août 2014 - 19:28, http://nieuws.vtm.be/binnenland/106397-nsa-bespioneert-nog-steeds-belgacom

La mise en place d'une dissuasion cyber constitue également un jalon décisif de cette sécurisation, mais, au contraire de la dissuasion nucléaire, qui peut être arborée de façon très voyante, la dissuasion cyber est moins évidente à afficher, ce qui est surtout dû au principe de non-imputabilité qui empêche de menacer directement l'auteur d'une cyberattaque, puisque celui-ci n'est pas (ou pas entièrement) officiellement connu. En effet, une dissuasion efficiente doit être construite sur base de plusieurs éléments. L'un d'entre-eux est une communication ferme sur la posture qu'on prendra suite à une cyberattaque. Afin de soutenir cette communication et cette posture, des moyens doivent être mis en place. Certains de ces moyens ont déjà été mentionnés plus haut, puisqu'il s'agit entre autres des hackers éthiques, mais aussi de moyens de renseignements et d'influence crédibles permettant d'analyser les attaques et de mieux nous défendre. Cependant, l'aspect normatif doit aussi être travaillé. Dans un cadre international, ce dernier point pourrait être mis en application en prévoyant des listes d'objectifs protégés, et qui seraient insérées dans les textes de Droit International Humanitaire. Et, en parallèle, assouplir les normes d'attribution de faits délictueux permettrait une reconnaissance officielle facilitée des origines précises d'une cyberattaque, et donc une réaction plus décisive suite à celle-ci[65].

La mise en œuvre d'une dissuasion cyber forte et crédible offrira la possibilité de trouver un équilibre entre la liberté d'information et la protection de nos propres intérêts. Ce n'est qu'à partir de ce moment-là que nous serons réellement en mesure de protéger les valeurs de notre société. Mais cette crédibilité ne pourra se bâtir que dans un climat de confiance envers la classe dirigeante, que ce soit au niveau politique fédéral ou au niveau militaire.

[65] Brian M. Mazanec, Bradley A. Thayer, *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*, Palgrave & Macmillan, 2015, p. 51.

6 Conclusion

On peut retrouver une cohérence au niveau des stratégies de cybersécurité, et plus particulièrement de cyberdéfense, créées par le gouvernement et par la Défense.

Le cyber ne doit pas être vu dans un monde trop étroit composé de geeks et de *Computer Network Operations* (opérations ordinateurs et réseau), mais doit être étendu jusqu'à un concept de guerre d'information incluant des aspects culturels et sociologiques.

Aussi bien au niveau plus général de l'État qu'au niveau de la Défense belge, on remarque qu'une coopération internationale, mais plus important encore, une approche nationale interdépartementale et une collaboration entre tous les acteurs impliqués, sont essentielles. Une supervision centrale, de même qu'une communauté cyber nationale, constituent des points-clés qui se retrouvent dans les deux documents établissant les différentes stratégies, et qui pourraient permettre un suivi précis de l'évolution des risques du cyberespace grâce, entre autre, à l'établissement d'une *Recognised Cyber Picture* commune.

Cependant, il reste du travail, d'une part, au niveau de la mise en œuvre des doctrines et des lois spécifiques, concernant la transparence du gouvernement, et d'autre part, au niveau de l'application des recommandations spécifiques émises aussi bien par les services gouvernementaux que par les instances privées.

Mais de bonnes initiatives ont malgré tout déjà été prises afin de sensibiliser la population. Des collaborations avec le monde académique permettront peu à peu de valoriser le potentiel des personnes douées en informatique. Les hackers éthiques, enfin repris dans un cadre légal, n'opèrent plus dans une zone grise. Par contre, la possibilité de garantir aux spécialistes une carrière plus stable afin qu'ils aient le temps d'assimiler la complexité de la matière et de comprendre les problématiques cyber dans leur entièreté doit être encore beaucoup plus, et beaucoup mieux, exploitée. Cette mesure devrait permettre de doter le pays de spécialistes de valeur, qui pourront assister nos dirigeants à appréhender la globalité des problèmes auxquels ceux-ci seraient confrontés, ainsi qu'à tracer les grandes lignes d'une vision cyber enfin évolutive.

Sur le plan de sa stratégie de cybersécurité, et malgré le fait que la Belgique avait pourtant pris un bon départ, aucune mise à jour sérieuse n'a été entreprise depuis 2012 – le moment de son adoption. Dans un monde qui évolue très vite, et alors que le cyberespace est en constante mutation, les changements sont continus. Il est dès lors

fortement recommandé que la stratégie ainsi que le cadre légal suivent d'au plus près ces évolutions.

Ce qui nous permet de conclure que, d'un point de vue théorique, la Belgique n'est pas parmi les plus mauvais élèves européens en matière de cyberdéfense mais qu'il faut malgré tout bien admettre que, d'un point de vue pratique, c'est encore en chantier, certaines mesures d'application concrètes se faisant toujours attendre.

Annexe A – Définitions

Cyberespace[66]

> Le cyberespace est l'environnement global né de l'interconnexion des systèmes d'information et de communication. Le cyberespace est plus large sue le monde informatique et contient également les réseaux informatiques, systèmes informatiques, médias et données numériques, qu'ils soient physiques ou virtuels.

Cyberdéfense[67]

> *The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level.*

Cybersécurité[68]

> *The desired situation in which the protection of cyberspace is proportionate to the cyber threat and the possible consequences of cyber-attacks.*

Stratégie militaire[69]

> Composante d'une stratégie nationale ou multinationale, qui traite de la façon dont la puissance militaire doit être développée et appliquée dans l'intérêt du pays ou du groupe de pays.

[66] Belgische Federale regering, *Cyber Security Strategy*, 2012, p. 12.
[67] Belgische Defensie – ACOS Strat, *Cyber Security Strategy for Defence*, 2014, p. 18.
[68] *Ibid.*
[69] *AAP-6(2013) NATO Glossary of Terms and Definitions*, 439 p. - définition p. 3-S-6

Annexe B – Abréviations

ACOS IS	Département d'Etat-Major de Renseignement et de Sécurité
ADS-B	Automatic Dependent Surveillance-Broadcast
BelNIS	Belgian Network Information Security
CCB	Centre pour la Cybersécurité en Belgique
CERT	Computer Emergency Response Team
CSOC	Cyber Security Operations Center
DDoS	Distributed Denial of Service
DG Com	Direction Générale Communications
DG MR	Direction Générale Material Resources
DOD	Department of Defence
FAI	Fournisseurs d'Accès à Internet
FCCU	Federal Computer Crime Unit
NGA	Next Generation Access
SCADA	Supervisory Control And Data Acquisition
SGRS	Service Général du Renseignement et de la Sécurité
SPF	Service Public Fédéral
SSI	Sécurité des Systèmes d'Information
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIC	Technologies de l'Information et de la Communication

Annexe C - Bibliographie

Références des lois

[1] MONITEUR BELGE, 11 Décembre 1998 - Loi relative à la classification et aux habilitations de sécurité

[2] MONITEUR BELGE, 30 Novembre 1998 - Loi organique des services de renseignement et de sécurité

[3] MONITEUR BELGE, 1 Juillet 2011 - Loi relative à la sécurité et la protection des infrastructures critiques

Références bibliographique

[1] Belgische Defensie – ACOS Strat, Cyber Security Strategy for Defence, 2014, 18 p.

[2] Belgische Federale regering, Cyber Security Strategy, 2012, 17p .

[3] Belgische Defensie, La vision stratégique pour la Défense, 29 Jun 2016, 144 p.

[4] International Chamber of Commerce Belgium, VBO, EY (et al.), Belgische gids voor cyberveiligheid, 2014, 68 p.

[5] Belgische Federale Regering - Centrale Raad voor het Bedrijfsleven, Belgium 2.0 – Naar een succesvolle digitale transformatie van de economie : de rol van breedbandinfrastructuur en andere elementen, 2015, 51 p.

[6] US Department of Homeland Security, Blueprint for a Secure Cyber Future, 2011, 40 p.

[7] ENISA et CSCG, Definition of Cybersecurity - Gaps and overlaps in standardisation, 2016, 35 p.

[8] ENISA, National Cyber Security Strategies, 2012, 15 p.

[9] ENISA - Resilience and CIIP Unit, An evaluation framework for Cyber Security Strategies, 2014, 42 p.

[10] F.-B. Huyghe, O. Kempf et N. Mazzuchi, Gagner les cyberconflits: Au-delà du technique, Economica (Collection Cyberstratégie), 2015, 175 p.

[11] T. Rona, Weapon Systems and Information War, The Boeing Aerospace Company, Jul 1976, 71 p.

[12] Brian M. Mazanec, Bradley A. Thayer, Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace, Palgrave & Macmillan, 2015, 95 p.

[13] Martin C. Libicki, Cyberdeterrence and Cyberwar, R AND Corporation, 2009, 214 p.

[14] Brandon Valeriano, Ryan C. Maness, Cyber War vesrsus Cyber realities : Cyber conflict in the International System, Oxford University Press, 2015, 288 p.

[15] NATO, AAP-6(2013) NATO Glossary of Terms and Definitions, 2013, 439 p.

[16] Daniel Ventre, Cyberespace et acteurs du cyberconflit (Collection Cyberconflits et Cybercriminalité), éditions Hermès Lavoisier, Paris, 2011, 288 p.

[17] Belgian Defence – ACOS Strat, ACST-APG-CGEN-SXX-001 / DTATL Transformation from Strategic Orientations to Capabilities for Operations, 2007, 12 p.

[18] G8 Declaration, Renewed commitment for freedom and democracy, G8 Summit of Deauville, May 26-27, 2011

[19] DOD, Joint Publication 3-12 (R), 05 février 2013, 70 p.

[20] B. H. Liddell Hart, Strategy, London: Faber & Faber, 1967. 2nd rev. ed., 448 p.

[21] Colin Gray, War, Peace and International Relations: An Introduction to Strategic History, Abingdon and New York City: Routledge 2007, 321 p.

[22] J. Henrotin, Introduction à la stratégie Syllabus des conférences données à l'ESIG, 2014, 171 p.

[23] Sun Tzu, L'art de la guerre

[24] Seyed Hossein Ahmadpanah, Proactive Cyber Defense: Security For Government, CreateSpace Independent Publishing Platform, 2015, 138 p.

[25] Redline drawn : China recalculates its use of cyber espionage, Fireeye iSight Intelligence, 2016, 16 p.

[26] J. Henrotin, Techno-guérilla et guerre hybride, le pire des deux mondes, Nuvis, 2014, 361 p.

[27] Armistead Leigh, Information Operations Matters, best practices, Potomac Books, 2010, 152 p.

Articles scientifiques

[1] BIHAN Benoist, « Cyberespace : la nécessité d'une approche différenciée», Défense & Sécurité Internationale, Hors-série n°32, octobre-novembre 2013, 3 p., p. 27-29.

[2] CATTARUZA Amaël et DOUZET Frédérick, « Le cyberespace au cœur des tensions géopolitiques internationales », Défense & Sécurité Internationale, Hors-série n°32, octobre-novembre 2013, 3 p., p. 16-18.

[3] HENROTIN Joseph, « Cyberguerre. Un nouvel avatar de la tentation technologique ? », Défense & Sécurité Internationale, Hors-série n°32, octobre-novembre 2013, 3 p., p. 24-26.

[4] HENROTIN Joseph, « L'analogie maritime face à la stratégie organique et à la stratégie des moyens en cyberstratégie », Défense & Sécurité Internationale, n°98, décembre 2013, 5 p., p. 46-50.

[5] LIBICKI Martin C., « Cyberspace Is Not a Warfighting Domain », *I/S: A Journal of Law and Policy for the Information Society* 8, n°2, 2012, 15 p. p. 321-336.

[6] MALIS Christian, « Une révolution dans les affaires militaires ? Les paradoxes du cyberconflit », Défense & Sécurité Internationale, Hors-série n°32, octobre-novembre 2013, 5 p., p. 19-23.

[7] PAVERO Franck, « Cyberdéfense. De Stuxnet aux armes de demain », Défense & Sécurité Internationale, Hors-série n°32, octobre-novembre 2013, 5 p., p. 42-46.

[8] VENTRE Daniel et PRÉAUX Charles, « Que couvrent les dénominations cyber liées à la défense ? », Défense & Sécurité Internationale, Hors-série n°32, octobre-novembre 2013, 4 p., p. 8-11.

Articles de presse contemporaine des faits étudiés

[1] Les infos, TF1, 16 septembre 2016 22:03

[2] Het journaal 1, VRT, 23 février 2017 13:13

Congrès

[1] Conférence – la politique de défense et de sécurité nationale, le rôle du MINDEF (M. Malet, 04 octobre 2016, EdG, Paris)

Internet

[1] Glossaire, https://www.ssi.gouv.fr/entreprise/glossaire/c/,
date de consultation de la page 05 octobre 2016

[2] Quand prendra-t-on la cybercriminalité au sérieux?, Benoît Gagnon, 14 septembre 2016 – 10:46, http://branchez-vous.com/2016/09/14/quand-prendra-t-on-la-cybercriminalite-au-serieux/,
date de consultation de la page 05 octobre 2016

[3] Cyberaanval via beveiligingscamera's en babyfoons, deredactie.be, 21 octobre 2016 – 21:37, http://deredactie.be/cm/vrtnieuws/cultuur%2Ben%2Bmedia/media/1.2799653#,
date de consultation de la page 23 octobre 2016

[4] ERWIN Sandra, MAGNUSON Stew, PARSONS Dan (et al.), Top Five Threats to National Security in the Coming Decade, National Defense Industrial Association, November 2012, http://www.nationaldefensemagazine.org/archive/2012/november/pages/topfivethreatstonationalsecurityinthecomingdecade.aspx,
date de consultation de la page 30 octobre 2016

[5] Hacker lassen Finnen frieren, Der Spiegel Online, 08 novembre 2016 http://www.spiegel.de/netzwelt/web/finnland-hacker-schalten-heizungen-aus-a-1120234.html,
date de consultation de la page 08 novembre 2016

[6] La cybercriminalité représente 65% des cas de criminalité économique signalés en Belgique, Belga, 25 février 2016 – 15:57, http://www.lalibre.be/actu/belgique/la-cybercriminalite-represente-65-des-cas-de-criminalite-economique-signales-en-belgique-56cf15423570ebb7a8ba086c,
date de consultation de la page 08 novembre 2016

[7] L'arsenal juridique belge contre la cybercriminalité positivement évalué, Belga, 03 mars 2015 – 20:46, https://www.rtbf.be/info/medias/detail_l-arsenal-juridique-belge-contre-la-cybercriminalite-positivement-evalue?id=8921607,
date de consultation de la page 09 novembre 2016

[8] Lutte contre la cybercriminalité: la Belgique est performante, Belga, 3 mars 2015 – 19:55, http://www.lavenir.net/cnt/dmf20150303_00610787,
date de consultation de la page 09 novembre 2016

[9] Un cadre juridique pour autoriser les hackers éthiques, Belga, 08 décembre 2016, http://fr.metrotime.be/2016/12/08/news/un-cadre-juridique-pour-autoriser-les-hackers-ethiques/,
date de consultation de la page 16 décembre 2016

[10] Proposition de résolution visant à renforcer la cybersécurité en Belgique, déposée par M. Georges Dallemagne, 16 septembre 2014,
http://www.dekamer.be/FLWB/PDF/54/0257/54K0257001.pdf,
date de consultation de la page 05 février 2017

[11] Defensie ontkent dat Belgische F-16s bombardementen hebben uitgevoerd in Aleppo, de redactie.be, 19 octobre 2016 – 07:24,
http://deredactie.be/cm/vrtnieuws/buitenland/1.2797185,
date de consultation de la page 10 février 2017

[12] Pacemaker hacken ? Geen fictie zo blijkt, Het Laatste Nieuws, 16 novembre 2016 – 19:59,
http://www.hln.be/hln/nl/957/Binnenland/article/detail/3006452/2016/11/26/Pacemaker-hacken-Geen-fictie-zo-blijkt.dhtml,
date de consultation de la page 25 février 2017

[13] NSA bespioneert Belgische ambassade, Belga, 24 février 2016 – 13:27, http://www.gva.be/cnt/dmf20160224_02146892/nsa-bespioneert-belgische-ambassade, date de consultation de la page 19 décembre 2016

[14] NSA bespioneert nog steeds Belgacom, VTM, 29 août 2014 - 19:28, http://nieuws.vtm.be/binnenland/106397-nsa-bespioneert-nog-steeds-belgacom, date de consultation de la page 19 décembre 2016

[15] Studenten willen Robin Hood zijn, standaard.be, 08 janvier 2016 – 03:00, http://www.standaard.be/cnt/dmf20160107_02055046, date de consultation de la page 10 décembre 2016

[16] Cyber Security Challenge, https://www.cybersecuritychallenge.be/ , date de consultation de la page 03 février 2017

[17] War in the fifth domain : Are the mouse and keyboard the new weapons of conflict ? , The economist, 2010, http://www.econimist.com/node/16478792, date de consultation de la page 25 janvier 2017

[18] Computercriminaliteit, Belgium.be - Justitie, http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/, date de consultation de la page 18 janvier 2017

[19] Computercriminaliteit, Belgium.be - Justitie, http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/hacking, date de consultation de la page 18 janvier 2017

[20] Digitale klokkenluiders krijgen wettelijk kader om te hacken, standaard.be, 08 janvier 2016 - 03:00, http://www.standaard.be/cnt/dmf20160107_02055042, date de consultation de la page 17 janvier 2017

[21] Ethische hacker: "Koude Oorlog is nooit gestopt, maar gaat online verder", deredactie.be, 11 janvier 2017 – 15:52, http://deredactie.be/cm/vrtnieuws/buitenland/1.2863877# , date de consultation de la page 12 janvier 2017

[22] Hackers Remotely Kill a Jeep on the Highway—With Me in It, WIRED on YouTube, 21 juillet 2015, https://www.youtube.com/watch?v=MK0SrxBC1xs, date de consultation de la page 05 octobre 2016

[23] NATO officially recognizes cyberspace a warfare domain, Pierluigi Paganini, 18 juin 2016, http://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html, date de consulatation de la page 05 octobre 2016

[24] Obama hints at sanctions against China over Cyberattacks, The New York Time, 16 Sep 2015, http://www.nytimes.com/2015/09/17/us/politics/obama-hints-at-sanctions-against-china-over-cyberattacks.html , date de consultation de la page 16 décembre 2016

Témoins

[1] Mr HENROTIN J. – 09 Décembre 2016

[2] Mr SNOECK B. – 16 Février 2017

Films

[1] *Blackhat* (nom français : Cyber) – Etats-Unis

La cybercriminalité, la cyberguerre et les difficultés de collaborer dans le milieu du cyber.

[2] *Cyberwar* - série téléviser – Etats-Unis

Reportages de Ben Makuch avec comme but de découvrir et mieux comprendre le milieu de la cyberguerre