Cyber Security Strategy

BELGIUM BELGIQUE BELGIE BELGIEN

23-11-2012	Securing Cyberspace

Identifier la cybermenace
Améliorer la sécurité
Pouvoir réagir à des incidents

SYNTHESE

Notre société, de même que notre économie, sont devenues fortement dépendantes de la technologie de l'information et de la communication, base actuelle du fonctionnement de nombreux processus professionnels, y compris dans les secteurs vitaux. La disponibilité de ces systèmes informatiques n'en est que plus cruciale, de même que leur fonctionnement intègre et de bonne qualité.

Société de connaissances, la Belgique est devenue plus vulnérable du fait de la rapidité de l'évolution technologique. L'espionnage économique et politique dans le cyberespace met en danger le potentiel économique et scientifique de notre pays. Mais l'intrusion dans l'infrastructure ICT, sa mise hors service menacent également la pérennité des activités sociales dans le cyberespace.

La cybermenace est réelle. Les criminels continuent à viser d'abord l'argent et le pouvoir. Chaque jour, les possibilités d'atteindre leur objectif augmentent. Les connaissances et outils nécessaires deviennent de plus en plus accessibles, ce qui augmente de façon inquiétante le nombre d'incidents.

Avec sa stratégie nationale de cyber security, la Belgique aligne trois objectifs stratégiques pour garantir la cybersécurité dans notre pays:

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

L'approche nécessaire à la réalisation des objectifs stratégiques précités se traduit par différentes lignes d'action.

L'approche de la cybersécurité doit être centralisée et intégrée par un organe central. D'où la nécessité d'accords clairs entre les différents partenaires nationaux publics, privés et académiques, de même qu'un engagement important de leur part. Tous les aspects de la sécurité doivent être abordés dans le cadre d'une coopération nationale et internationale optimale.

Partant de la législation existante, un cadre légal doit être créé pour trouver un équilibre entre les droits et libertés du citoyen et les interventions indispensables de l'autorité.

La cybermenace en général, mais également celle visant les systèmes publics et les infrastructures critiques, doivent faire l'objet d'un suivi permanent. Les incidents sécuritaires doivent être traités de façon conséquente et coordonnée. La capacité doit pour cela être renforcée.

Des normes et directives sécuritaires seront établies pour améliorer la protection des systèmes ICT. Il est impératif d'informer les citoyens, les entreprises, les importantes infrastructures nationales, mais aussi les autorités.

Une action conjointe des différents acteurs est également indispensable en cas d'incidents de nature criminelle ou de cybercriminalité, car ainsi, l'impact de l'incident restera le plus limité possible, et les auteurs pourront être retrouvés pour ensuite être traduits en justice.

Grâce aux formations et campagnes d'information nécessaires, l'expertise et les connaissances des différents acteurs du cyberespace relatives à la cybersécurité doivent s'améliorer. Le développement technologique doit être stimulé, pour pouvoir offrir un accès sécurisé au cyberespace.

TABLE DES MATIERES

1 LA CYBERMENACE

1.1 Notre société et notre économie dépendent de l'ICT

Notre société, de même que notre économie, dépendent fortement de la technologie de l'information et de la communication (ICT). Cette dépendance augmente car souvent, les processus économiques n'ont **aucune solution en dehors du cyberespace**.

A côté de **l'enregistrement et le traitement administratif** de données, L'ICT contrôle et administre aussi des **processus industriels**. Ces systèmes SCADA[1] sont utilisés notamment dans des secteurs vitaux et sont de plus en plus souvent reliés à Internet. La progression des applications 'the Internet of things' ou 'machine-to-machine'[2] notamment dans les transports, l'aéronautique et la santé, augmentent également la dépendance à l'ICT, allant de paire avec sa vulnérabilité.

La **disponibilité** et le **fonctionnement intègre et de bonne qualité** de tous ces systèmes sont essentiels. En effet, ils constituent la base du fonctionnement de secteurs vitaux tels que la fourniture d'énergie, les transports, le secteur financier, les soins de santé et les services publics. Si l'infrastructure ICT de ces secteurs est perturbée ou mise hors service, intentionnellement ou non, les dégâts peuvent être très graves, voire fatals.

Un internet sûr et disponible **constitue l'épine dorsale de notre économie**. L'espionnage économique sur Internet menace directement la compétitivité de nos entreprises. Notre économie a besoin de systèmes de communication fiables pour pouvoir être performante.

1.2 Notre pays est vulnérable

La Belgique est aujourd'hui plus que jamais une **société de connaissance**, dont le capital est justement formé de l'information (information de politique stratégique, procédés industriels, patentes et brevets).

Ces dernières années, divers incidents ont démontré que des infections ciblées des entreprises et des organisations avec des logiciels malveillants constituent la base de l'espionnage économique et politique, d'où la menace sur le **potentiel scientifique et économique** de notre pays.

Divers **facteurs** déterminent la vulnérabilité de la Belgique:

(1) Tout d'abord, l'**accessibilité** à l'internet à large bande de tous les systèmes ICT importants. Cet avantage économique indéniable est également synonyme de vulnérabilité car ces larges bandes peuvent également être utilisées pour infecter d'autres serveurs par des 'attaques DDoS[3].

(2) Pour leurs systèmes d'information, les organisations font généralement appel à la **technologie commerciale standard**. Ces technologies font sans cesse l'objet de découvertes et de publications de

---

[1] SCADA ou Supervisory Control And Data Acquisition: collecte, transmission, traitement et visualisation de signaux de mesure et de réglage de différentes machines ou appareils dans des systèmes de contrôle de processus industriels. Ces systèmes SCADA sont souvent reliés directement ou indirectement (par ex. avec ces clés USB) à Internet.

[2] 'The Internet of things' ou 'machine-to-machine' (m2m) consiste à utiliser des capteurs et des modules de commande pour contrôler et éventuellement mettre à jour des appareils (par ex. compteurs intelligents, électroménager, containers, camions, surveillance médicale), par transmission de données sans fil.

[3] DDoS ou Distributed Denial of Service est le nom d'un type d'attaque rendant un service inaccessible aux bénéficiaires habituels du service. Il s'agit d'une technique perturbant fortement le fonctionnement normal du système par un grand nombre de Requêtes.

nouvelles vulnérabilités. Les cybercriminels réagissent plus rapidement que la plupart des gestionnaires système.

(3) La concentration de données et d'applications de plusieurs entreprises et organisations dans des centres de données du '**Cloud**' fait de ces centres et réseaux le talon d'Achille de notre cybersociété. En outre, ces infrastructures ne sont souvent plus sur le territoire belge et il n'est donc pas toujours possible à l'autorité belge de garantir la sécurité des entreprises et organisations.

(4) Les grandes banques de données personnelles menacent également la **vie privée** des citoyens.

(5) Souvent, les entreprises, services publics et organisations ne disposent pas encore de **mesures de protection et de détection** adéquates, ce qui empêche une réaction adéquate aux incidents touchant leur infrastructure.

(6) Enfin, les alliances Internationales de protection de la sécurité de l'Etat ne sont pas nécessairement valables ou applicables dans le cyberespace. La stratégie de cyber security devra donc s'axer principalement sur l'**aspect national**.

Ces vulnérabilités créent donc un danger d'une part d'intrusion et d'utilisation illégale de l'infrastructure ICT, d'autre part de mise en hors service de cette infrastructure. C'est donc non seulement le potentiel scientifique et économique qui est menacé, mais aussi la **protection d'intérêts essentiels et vitaux**.

1.3 La cybermenace est réelle

Les **intentions** des criminels demeurent **inchangées:** s'enrichir et accroître leur pouvoir économique, scientifique, politique ou militaire. Les **possibilités** de le faire ont quant à elles fortement **augmenté.** L'évolution d'Internet avec des moyens limités facilite donc le sabotage, l'espionnage, la subversion, le terrorisme, le commandement et la direction, la propagande et les cyberopérations militaires.

Depuis le printemps 2012, des milliers de PC en Belgique, principalement de particuliers, sont bloqués par un maliciel "ransomware" qui demande à la victime de payer pour débloquer son PC.

Mais les entreprises font également l'objet d'extorsions. *Ainsi par exemple, une banque belge a été victime de cybercriminels en mai 2012.* Si la banque n'exécutait pas le paiement d'une grosse rançon*, les données de milliers de clients obtenues par hacking seraient divulguées sur Internet.*

Dans le domaine cyber, il est plus simple, plus rapide et moins cher de s'introduire dans les systèmes ou de les attaquer que de les protéger.

Les **connaissances et outils** nécessaires à ces cyberattaques sont **accessibles** à tous sur internet. En outre, grâce à la technologie, les opposants peuvent communiquer de façon sécurisée et ainsi masquer leur identité. Il est donc devenu difficile, voire impossible de les surveiller.

La rapidité du développement technologique fait que **la protection** de nombreux systèmes n'est **pas à jour**, les rendant ainsi vulnérables à leur prise de contrôle par des criminels

Uniquement intéressées par l'argent, les organisations criminelles ont utilisé durant cette décennie les facteurs susmentionnés pour créer des réseaux de serveurs et de postes de travail piratés. Souvent, ils utilisent pour ce faire des logiciels malveillants, à l'insu de l'utilisateur, tels que les chevaux de Troie qu'ils introduisent dans les systèmes pour prendre leur contrôle. Les réseaux établis sont appelés ***botnets*** et servent à de nombreuses activités illégales: diffusion de spam et de logiciels malveillants, espionnage d'entreprises et de particuliers, transactions financières frauduleuses, extorsion d'entreprises après sabotage de serveurs et de postes de travail et mise hors service de système par envoi massif de données (attaque DDoS).

Depuis 2007, différentes vagues d'attaques ont été constatées dans l'e-banking de notre pays. Pour les cas les plus récents de 2012, des chevaux de Troie et des botnets ont été utilisés, mais aussi des sites de hameçonnage

et de l'ingénierie sociale (le hacker téléphone à la victime et l'incite, sous différents prétextes, à collaborer à son insu au hacking et aux transferts illégaux d'argent).

La force des botnets et des chevaux de Troie n'a pas échappé à l'attention de certains groupes dans notre société qui, ces dernières années, ont trouvé en ces moyens de **nouvelles motivations** devenues la base de nouvelles menaces.

Tout d'abord, le **hacktivisme** par la masse. Ce hacktivisme consiste en une cybercriminalité d'inspiration politique ou idéologique, rendant publiques des 'informations secrètes'. Les actions touchent les autorités mais aussi les entreprises commerciales et débouchent souvent sur des attaques et contre-attaques. Les actions sont dirigées depuis les médias sociaux, ce qui laisse peu (ou pas) de temps aux autorités pour réagir, ou encore moins éviter les incidents. Les hacktivistes sont généralement peu structurés mais récolte l'attention des médias par la réutilisation du pseudonyme 'Anonymous' comme signature.

Une entreprise mondiale de l'acier fut, début 2012, la première victime d'envergure du mouvement de hackers 'Anonymous Belgium'. Depuis, de plus en plus de cybercriminels commettant leurs méfaits sous la même bannière et s'attaquent aussi bien au secteur public qu'à l'industrie.

Ensuite, on voit des groupes et états organisés coupables de **cyberespionnage** pour des motifs économiques et politiques. Leur objectif est de connaître les stratégies, patentes, stocks, etc. de grandes entreprises (actives dans le pétrole ou l'énergie, institutions financières) et de divers départements publics dans tous les pays. Souvent, cet espionnage passe inaperçu pendant des mois, voire des années et personne ne sait exactement quelles informations arrivent entre les mains de l'opposant.

Les incidents sécuritaires constatés en Belgique diffèrent substantiellement en matière d'ampleur et de degré de complexité. Ainsi, certains incidents ayant touché le ministère des Affaires étrangères peuvent être qualifiés très certainement de cyberattaques.[4]

Un troisième développement consiste à déstabiliser ou à paralyser des infrastructures critiques et essentielles, avec des conséquences parfois fatales. Des maliciels spécifiques permettent de prendre ou de saboter le contrôle de certaines facilités industrielles. Cette forme de **cyberwarfare** est clairement dirigée vers un état.

Le virus informatique persistant Sality.gen, virus, a paralysé pendant une semaine et demie en 2012 des parties de l'administration centrale et des bureaux de contrôle et de recettes du SPF Finances. L'origine de l'infection ou ses objectifs restent flous.

En avril 2009, des hackers ont réussi à s'introduire dans le réseau électrique des Etats-Unis et à le perturber. En juin 2010, le virus Stuxnet a saboté les centrifuges des centrales nucléaires iraniennes, occasionnant un retard de 2 ans à leur programme nucléaire. En mai 2012, le gigantesque virus d'espionnage Flame a été découvert. Flame a infecté plus de 1000 ordinateurs au Moyen-Orient et pouvait notamment voler des mots de passe, mettre des PC sur écoute par microphone et enregistrer des conversations Skype.

Des éléments indiquent que des groupes de hackers étrangers mettent au service des autorités et des entités militaires leurs capacités et botnets en échange de sponsoring, de tolérance ou de protection. La spécialisation et la capacité des cybercriminels peuvent également être facilement mobilisées via l' « économie souterraine ». Dans le futur, il faudra tenir compte avec une menace de terroristes qui se serviraient également de ces moyens et techniques pour leurs actions. Jusqu'à ce jour, aucun fait de véritable cyberterrorisme constituant un danger pour des vies humaines n'a été constaté.

---

[4] Réponse à la question écrite n° 5-4302 de Karl Vanlouwe d.d. 23 décembre 2011 au Vice Premier Ministre et ministre des Affaires étrangères, 'Cyberattaques et cybercrime – Cyberdéfense – UE – OTAN – Situation spécifique Service Public Fédéral Extérieur.

2 OBJECTIFS STRATÉGIQUES

La Belgique visera un cyberespace sûr et fiable qui respecte les valeurs et droits fondamentaux de la société moderne.

Un **cyberespace sûr et fiable** garantit les principes fondamentaux de la sécurité de l'information, en particulier la disponibilité, l'intégrité, la confidentialité et la non-répudiation des données et systèmes d'enregistrement et/ou de traitement.

Il faut protéger notre société et ses citoyens des abus, des contenus indésirables et autres menaces en tenant compte de l'**équilibre** entre l'importance de la sécurité (nationale) et l'importance des valeurs de base de notre société moderne telles que la vie privée, la liberté d'expression, le droit à la libre collecte d'informations et le respect d'autrui.

Cette quête de plus de cybersécurité est **essentielle** pour réduire la vulnérabilité de la Belgique et répondre aux besoins réels d'une société et d'une économie ancrées profondément dans le cyberespace.

L'autorité donne aux entreprises et à la population **des conseils et des indications de sécurité** sur la façon dont elles peuvent améliorer la protection de leurs ordinateurs et réseaux et comment réagir en cas de problème. Ainsi, les citoyens et entreprises peuvent continuer à profiter des avantages et opportunités que peut offrir un Internet sûr et public dans un cyberespace fiable.

La Belgique visera une protection et une sécurisation optimales des infrastructures et systèmes publics critiques contre la cybermenace.

Les **infrastructures critiques** fournissent à la société des biens ou des services à ce point essentiels qu'il convient d'éviter au maximum toute interruption ou perturbation de leur fonctionnement.

Compte tenu de l'apparition récente et de l'augmentation constante des cybermenaces, l'objectif est de faire en sorte que la **sécurité informatique** de ces infrastructures critiques soit assurée de la manière la plus optimale possible et soit adaptée aux types de menaces existant à leur encontre.

Les **systèmes ICT des autorités** doivent également être suffisamment protégés et contrôlés.

La Belgique désire développer ses propres capacités en cyber security.

Grâce à ses propres **capacités** en cybersécurité, la Belgique pourra, en toute autonomie, mener une politique sécuritaire et réagir aux incidents.

La reconnaissance internationale d'une cyberattaque comme une attaque armée n'est pas évident et donc, un soutien externe peut rarement être escompté. Le rôle d'organisations Internationales de sécurité reste très limité et les alliances de cybersécurité doivent être redéfinies. La Belgique désire élargir suffisamment ses propres capacités en cybersécurité pour pouvoir mettre sur pied **d'importantes coopérations au niveau international**.

Un niveau respectable d'expertise et de moyens en cybersécurité favorisera la coopération internationale. La Belgique désire appuyer le développement de nouvelles technologies dans le domaine de la cybersécurité et ainsi, stimuler les **initiatives académiques** nationales et la **prospérité économique**.

3 APPROCHE ET DOMAINES D'ACTION

Pour réaliser les trois objectifs stratégiques précités, la Belgique élabore une série de lignes d'action concrètes.

3.1 Approche centralisée et intégrée de la cybersécurité

Travailler à la sécurité dans le cyberespace suppose une très bonne coopération nationale et internationale.

Cela réclame, de la part de **toutes les parties** (autorités, entreprises, fournisseurs de services ICT, opérateurs de réseau et individus), un échange mutuel d'informations fiables, structurées et un **engagement important** où des accords clairs s'imposent sur le rôle de tous les intéressés et la manière de collaborer ensemble.

En effet, ce n'est que si tous les aspects de la sécurité entrent en ligne de compte dans une stratégie nationale qu'il existe une chance de réussite. Il est par ailleurs indispensable que les différents aspects soient abordés d'une **manière intégrée**. Chaque partie doit tenir compte, dans ses actions, du rôle et des compétences des autres parties. En élaborant des accords concrets à ce sujet, il est garanti que chaque partie pourra endosser effectivement son rôle.

De nombreuses mesures de protection ne seront efficientes que si elles peuvent être projetées au niveau **international**. Tant la coopération bilatérale qu'une participation active aux initiatives des organisations internationales sont essentielles. La collaboration doit d'abord avoir lieu au sein de l'Union Européenne (p ex à l'Agenda Digital) ou de l'OTAN mais l'harmonisation avec les partenaires doit aussi se faire mondialement. De même, les différents niveaux dirigeants de notre régime doivent être pris en compte. Tant les autorités fédérales, régionales que locales doivent être impliquées dans le développement de la stratégie.

Plus que jamais, cette stratégie doit être élaborée par une **relation privé-public étroite**. Les systèmes et les infrastructures critiques à protéger sont en effet pour une grande part aux mains de parties privées sans la collaboration desquelles une politique de sécurité effective est impossible. L'implication des opérateurs internet, gestionnaires de réseaux, cloud providers et des divers secteurs d'entreprise est donc une condition sine qua non.

Le **monde académique** doit également se charger d'une tâche importante, tant pour l'exécution du *research & development* que pour la formation d'informaticiens compétents qui peuvent aussi développer technologiquement le thème de la cybersécurité.

Pour bâtir effectivement une stratégie nationale de manière intégrale et intégrée et en suivre son exécution, il faut une **supervision centrale**. Celle-ci doit se faire dans le respect des compétences de chaque partie à chaque niveau.

3.2 Création d'un cadre légal

L'élaboration d'une stratégie nationale pour la cybersécurité doit être ancrée dans un cadre légal transparent qui se porte garant d'un **équilibre** entre les **droits et les libertés** du citoyen et les **interventions** nécessaires **de l'autorité** pour garantir la sécurité.

La stratégie nationale prend pour point de départ le cadre légal national et international existant dans lequel sont fixés, pour chaque autorité, son domaine de compétence, ses obligations et ses instruments juridiques potentiels. **Une utilisation optimale** des **compétences déjà disponibles** dans une approche intégrée est en première instance suffisante comme point de départ.

Concernant la **poursuite de l'élaboration** de la stratégie nationale, il faudra veiller à prévoir également une base légale pour les nouvelles compétences ou obligations ou encore, à adapter ou élargir les compétences ou obligations existantes.

Il est aujourd'hui déjà évident que les **compétences de la police, de la justice et des services de sécurité** devront être adaptés pour continuer à intervenir de manière efficace et efficiente dans le cyberespace, où les traces se diffusent toujours plus loin sur la toile mondiale, pesant sur la limite territoriale de la juridiction. Les instruments qui protègent la cybersécurité d'une part constituent d'autre part des outils qui sont mis à profit par les criminels pour échapper aux griffes de la justice. Ici aussi, la balance doit être rééquilibrée.

3.3 Suivi permanent de la cybermenace

Tant la **cybermenace générale** contre les valeurs fondamentales et les intérêts de l'Etat que les **cybermenaces spécifiques** contre les systèmes essentiels et vitaux importants doivent être suivies et analysées en permanence. Les informations doivent être activement partagées avec les services chargés de la protection des systèmes concernés.

Les systèmes et réseaux ICT de l'autorité, et en particulier ceux qui sont importants pour le fonctionnement et l'avenir de l'Etat, doivent être surveillés et les tentatives de pénétration ou de perturbation doivent être signalées et suivies au niveau central.

Les incidents de sécurité seront traités de manière conséquente et coordonnée. Des leçons seront tirées de ces incidents et la stratégie et l'approche nationales corrigées.

Les mesures de protection nationales doivent être **en équilibre** avec la cybermenace réelle. Cela demande une coopération intensive et un échange d'informations, tant sur le plan national qu'international.

3.4 Amélioration de la protection contre la perturbation ou la violation des systèmes informatiques

Pour améliorer la protection des **systèmes ICT,** des **directives et des normes de sécurité standard** seront établies pour les différentes sortes de systèmes.

L'autorité évaluera et **approuvera** ses propres systèmes réseaux et informatiques pour l'usage en réseaux hautement sécurisés. Pour les réseaux qui traitent des informations classifiées **et sensibles, des audits de sécurité** veilleront au contrôle de la conformité.

En ce qui concerne plus spécifiquement **les infrastructures critiques**, une **évaluation des politiques de sécurité** mises en place par les exploitants sera effectuée régulièrement. Ces politiques doivent tout autant intégrer la sécurité physique que la cybersécurité des systèmes informatiques de l'infrastructure en question. Une évaluation sur la collaboration entre les exploitants et les diverses autorités compétentes en la matière aura également lieu. le cas échéant, le cadre juridique existant pourra être adapté ou complété.

Tant les citoyens, les entreprises, les infrastructures nationales importantes que l'autorité doivent être avertis de manière adéquate des nouvelles vulnérabilités, menaces et mesures de protection potentielles. Tous les utilisateurs des systèmes ICT seront correctement **informés et sensibilisés**.

L'autorité collaborera avec les fournisseurs d'accès à Internet pour veiller à ce que leurs utilisateurs puissent disposer d'un **set de base des produits et services de sécurité**. Les fournisseurs d'accès à Internet pourvoiront et veilleront à la sécurité de leurs réseaux, systèmes, services et clients.

3.5 Renforcement de la capacité à réagir aux cyberincidents

Pour pouvoir mieux réagir aux sérieux cyberincidents, un **inventaire** des **capacités existantes** en matière de cybersécurité sera réalisé en première instance dans les différents services publics.

En fonction de la cybermenace générale connue, les **processus** de traitement de tels incidents de sécurité seront **plus détaillés** et les tâches spécifiques seront cartographiées. Ces processus ont été initiés sous la procédure 'incident handling'.[5]

Cet inventaire et l'aperçu des tâches importantes indiqueront où se situent les éventuels empiètements et où les services doivent être renforcés. Les **moyens adaptés et un nombre suffisant d'experts techniques et d'enquêteurs** seront prévus par département pour exécuter et se charger effectivement des tâches et responsabilités de cybersécurité.

En cas de problèmes, une approche coordonnée et une bonne coopération, tant entre les services publics qu'avec les acteurs privés, sont d'une importance primordiale. Un **organe central et compétent** coordonnera toutes les missions des différentes parties responsables. Ainsi par exemple, il est important que les opérateurs communiquent immédiatement les menaces ou incidents spécifiques à l'autorité compétente.

3.6 Approche spécifique de la cybercriminalité

Si les mesures de sécurité n'ont pu empêcher qu'un **incident** se produise, il est important alors en premier lieu que les incidents soient **détectés et signalés** par la victime aux partenaires appropriés et compétents.

Une **action commune** est ensuite requise pour:

- Mettre en sécurité les traces de l'incident;
- Établir un diagnostic correct de l'incident ;
- Eliminer ou neutraliser l'origine de l'incident;
- Revenir le plus vite possible à une situation opérationnelle sûre.

Il revient à la **police et à la justice** de rechercher les auteurs sur base des preuves disponibles, de retracer leur méthode de travail et leurs motivations et les traduire devant le tribunal compétent. Les résultats de leur enquête doivent en outre aider à mieux comprendre les menaces et les façons dont la société peut s'en prémunir.

Toutefois, pour lutter effectivement contre les cybercriminels dans la cybersociété, l'action conjointe devra être menée plus **anticipativement** contre les organisations de cybercriminels et contre l'infrastructure criminelle ICT qu'ils ont élaborée pour leurs activités. L'attention se portera surtout sur les actions qui peuvent prévenir l'apparition de botnets, les démanteler ou perturber leur fonctionnement.

3.7 Contribution à l'élargissement de l'expertise et la connaissance en cybersécurité

De même que la sécurité routière n'est pas seulement l'affaire des autorités, la sécurité du cyberespace implique une **multitude d'acteurs** : les simples internautes, les fournisseurs de produits et de services, les organisations utilisatrices, les autorités, …

[5] Processus décrits dans un document élaboré par un groupe de travail de la plateforme de concertation pour la sécurité de l'information BeINIS.

Il est donc essentiel que tous les intervenants soient **sensibilisés** aux risques courus et disposent de connaissances conformes à leur rôle.

Il faut établir des **profils de connaissance** adaptés aux différentes catégories d'acteurs, et dispenser au mieux les **formations nécessaires** en concertation avec les pouvoirs organisateurs, depuis l'enseignement fondamental jusqu'aux différentes études universitaires.

Ces formations doivent être épaulées par des **campagnes de sensibilisation** adaptées au public visé (via les médias grand public, les fournisseurs d'accès internet, les revues spécialisées, …) qui doivent régulièrement être répétées.

3.8 Stimulation du développement technologique

Dans tous les secteurs économiques, le marché est demandeur de produits et services non seulement performants, mais également fiables, c'est-à-dire dont la qualité et la sécurité sont certifiées par des organismes agréés.

Après des décennies de produits non certifiés, le secteur informatique est lui aussi touché par cette tendance de fond.

L'accès aux grands projets 'high tech' (défense, industrie spatiale, systèmes financiers, appareils médicaux, …) nécessite des fournisseurs informatiques et des autorités de contrôle un saut qualitatif présentant de multiples facettes : maîtrise des **méthodologies** de génie logiciel et des **standards** internationaux d'évaluation sécuritaire, mise en place des **organes de contrôle et d'homologation**, …

La **collaboration** de tous les acteurs impliqués est essentielle à la réussite du processus : centres de recherche académiques, services de recherche et développement des fournisseurs, organismes de contrôle, autorités d'accréditation et d'homologation, administration de la politique scientifique, …

ANNEXE 1: DEFINITIONS

BOTNET

Un botnet est un ensemble d'ordinateurs infectés de logiciels malveillants, commandés à distance à l'insu de l'utilisateur à partir d'un point central. Ces botnets constituent généralement l'infrastructure nécessaire à des actions malveillantes dans le cyberespace.

CLOUD

Cloud computing est un service de l'Internet basé sur l'hébergement et le traitement de données via un réseau de serveurs rendus accessibles partout dans le monde aux entités inscrites pour ce service.

CYBERCRIMINALITE

La Cybercriminalité ou le cybercrime est un délit d'utilisation abusive, en tant que moyen, de l'automatisation et de données automatisées, pouvant viser également les systèmes informatiques ou les données y étant enregistrées.

CYBERSÉCURITÉ

La cybersécurité est la situation souhaitée où la protection du cyberespace est proportionnelle à la cybermenace et aux conséquences possibles de cyberattaques. Dans une situation de cybersécurité, la perturbation, l'attaque ou l'utilisation abusive de l'ICT ne provoque aucun danger ni dommage. Les conséquences de l'abus, de la perturbation ou de l'attaque peuvent consister en la restriction de la disponibilité et de la fiabilité de l'ICT, en la violation de la confidentialité des informations ou en des dommages causés à l'intégrité de ces informations (ajout, effacement ou modification illégaux).

CYBERESPACE

Le Cyberespace est 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.

CYBERWAR(FARE)

L'utilisation de cybercapacités à une échelle suffisante, durant une période déterminée et à haut débit, en vue d'atteindre certains objectifs ou effets dans ou au travers du cyberespace, ces actions étant considérées comme une menace pour les intérêts nationaux de l'Etat visé.

ATTAQUE DDOS

Distributed Denial of Service est le nom d'un type d'attaque rendant un service inaccessible aux bénéficiaires habituels du service. Il s'agit d'une technique perturbant fortement le fonctionnement normal du système par un grand nombre de requêtes.

HACKER

Un hacker, tout en sachant qu'il n'y est pas autorisé, accède à ou surfe dans un système informatique.

SCADA OU ICS (INDUSTRIAL CONTROL SYSTEMS)

Supervisory Control And Data Acquisition consiste à collecter, transmettre, traiter et visualiser des signaux de mesure et de régulation de différents appareils ou machines dans des systèmes de contrôle des processus industriels. Ces systèmes SCADA sont souvent directement ou indirectement (par ex. avec des clés USB) reliés à Internet.

ANNEXE 2: ACRONYMES

ANS	Autorité Nationale de Sécurité
BCSS	Banque-Carrefour de la Sécurité Sociale
Belac	Organisme belge d'Accréditation
Belnet	Belgian national research network
BelNIS	Belgian Network Information Security
CCSB	Centre pour Cyber Sécurité Belgique
CERT	Computer Emergency Response Team
CMRS	Comité ministériel du renseignement et de la sécurité
CPVP	Commission de la protection de la vie privée
DGCC	Direction Générale Centre de Crise
ESA	European Space Agency
FCCU	Federal Computer Crime Unit
Fedict	SPF Technologie de l'Information et de la Communication
IBPT	Institut belge des services postaux et des télécommunications
ICT	Information and Communication Technology
OCAM	Organe de coordination pour l'analyse de la menace
OTAN	Organisation du Traité de l'Atlantique Nord
SCADA	Supervisory Control and Data Acquisition
SGRS	Service Général du Renseignement et de la Sécurité
SPF	Service Public Fédéral

ANNEXE 3: PROTECTION DES INFRASTRUCTURES CRITIQUES

Dans le domaine de la prévention et de la sécurité, la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques transpose partiellement la directive 2008/114/CE du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

A l'heure actuelle, cette loi compte quatre secteurs dans son champ d'application. Il s'agit, pour ce qui est des infrastructures critiques européennes et nationales, du secteur de l'énergie et celui des transports, et pour ce qui est des infrastructures critiques purement nationales, du secteur des finances et celui des communications électroniques publiques.

La loi impose aux exploitants d'une infrastructure désignée comme critique de nommer un point de contact pour la sécurité mais également d'élaborer un P.S.E (plan de sécurité de l'exploitant) visant à prévenir, atténuer, et neutraliser les risques d'interruption du fonctionnement ou de destruction de son infrastructure par la mise au point de mesures matérielles et organisationnelles internes.

L'article 13 § 2 de la loi précise que ce plan contient au minimum des mesures permanentes, applicables en toutes circonstances, et des mesures graduelles, à appliquer en fonction de la menace. l'OCAM prendra en compte la cybersécurité dans l'analyse de la menace qu'il réalisera, à la demande de la DGCC, dans le cadre de la loi sur la protection des infrastructures critiques.

Ces mesures peuvent aussi bien être physiques, par exemple, le contrôle d'accès ou la surveillance des points névralgiques, que logiques, c'est-à-dire spécifiques aux systèmes ou réseaux informatiques de l'infrastructure en question (installation de logiciels de détection de malwares, …).

Il incombe à l'exploitant de prendre, d'initiative, de telles mesures logiques dès lors que son plan de sécurité est élaboré sur la base d'une analyse des risques consistant à identifier les principaux scénarios de menaces potentielles, en ce compris, les cybermenaces.

Cependant, s'il s'avère que les exploitants d'un secteur ou sous-secteur particulier ne prennent pas de telles mesures ou que celles-ci sont insuffisantes, il reste possible de contraindre l'exploitant d'inclure des mesures spécifiques dans son plan de sécurité. Si la loi en prévoit en effet le contenu minimum, elle laisse la possibilité pour le Roi, pour un secteur ou sous-secteur déterminé, d'en détailler le contenu.

Du point de vue de la réaction, en cas d'incident visant les systèmes informatiques ou réseaux de communications électroniques d'une infrastructure critique, il est prévu que l'exploitant joue un rôle particulier aux côtés des autorités en charge de gérer la crise.