5 - 1855/1

SÉNAT DE BELGIQUE

SESSION DE 2012-2013

28 NOVEMBRE 2012

Proposition de résolution visant à sécuriser les informations électroniques et à lutter contre les cyberattaques

(Déposée par M. Karl Vanlouwe)

DÉVELOPPEMENTS

La présente proposition de résolution vise à faire en sorte que le Parlement prenne à bras-le-corps la problématique actuelle de la cybercriminalité. L'auteur observe que sur ce plan, le gouvernement fédéral a accumulé un retard énorme par rapport à nos voisins. Ainsi, la cybersécurisation des informations et des infrastructures critiques n'a jamais été une priorité du gouvernement. Cela rend toutes les organisations internationales, les entreprises et les citoyens établis dans ce pays d'autant plus vulnérables face à des groupes et à des pays utilisant activement des cyberarmes pour en tirer un avantage concurrentiel.

L'objectif de la présente proposition de résolution est d'aboutir à un engagement concret en vue de sécuriser et de défendre nos informations sensibles et infrastructures critiques.

Situation actuelle

L'Internet est le plus grand réseau informatique au monde. Il est prévu que d'ici 2020, il reliera plus de 50 milliards d'entités, qu'il s'agisse de personnes, d'entreprises ou de systèmes informatiques. Il est tout simplement impossible d'imaginer notre quotidien sans l'Internet.

Le cyberespace ne connaît pas de frontières et relie entre eux plus de 2,25 milliards d'individus (1). Il crée de nouvelles méthodes de travail, comme c'est déjà le cas pour les soins de santé et l'enseignement, met de

(1) *Internet World Statistics 2011.*

BELGISCHE SENAAT

ZITTING 2012-2013

28 NOVEMBER 2012

Voorstel van resolutie ter beveiliging van elektronische informatie en bescherming tegen cyberaanvallen

(Ingediend door de heer Karl Vanlouwe)

TOELICHTING

Dit voorstel van resolutie wenst het actuele probleem van cybercriminaliteit aan te kaarten in het Parlement. Indiener merkt op dat de federale regering op dit vlak een enorme achterstand heeft tegenover de buurlanden. Zo is de cyberbeveiliging van informatie en kritieke infrastructuren nooit een prioriteit van de regering geweest. Hierdoor zijn alle in dit land gevestigde internationale organisaties, bedrijven en burgers des te kwetsbaarder tegenover groepen en landen die actief gebruik maken van cyberwapens om een competitief voordeel te halen.

De bedoeling van deze resolutie is tot een concreet engagement te komen om onze gevoelige informatie en kritieke infrastructuren te beschermen en verdedigen.

Een situering

Het internet is het grootste computernetwerk ter wereld, tegen 2020 wordt verwacht dat er meer dan 50 miljard entiteiten met elkaar verbonden zijn, gaande van personen, bedrijven tot computersystemen. Het is onmogelijk om het dagelijks leven zonder internet in te beelden.

Cyberspace kent geen grenzen en verbindt meer dan twee en een kwart miljard individuen (1). Cyberspace introduceert nieuwe manieren van werken, zoals bij de gezondheidszorg en onderwijs, brengt nieuwe afzet-

(1) *Internet World Statistics 2011.*

nouveaux débouchés commerciaux à portée de clic et stimule de nouvelles méthodes de production. Mais en même temps, il est aussi devenu plus sensible aux pannes, lesquelles offrent de nouvelles perspectives aux cybercriminels.

Ces vingt dernières années, le monde s'est de plus en plus interconnecté grâce à la cyberdimension. Cette évolution a eu un impact énorme sur notre vie quotidienne, ainsi que sur l'économie et la société en général. À l'époque, des visionnaires et des analystes du marché avaient pu prévoir la rapidité de cette évolution et l'ampleur de cet impact de l'Internet, mais seuls quelques-uns en avaient entrevu les risques, les menaces et les défis potentiels.

Aujourd'hui, l'Internet offre à la population mondiale un moyen inédit de disposer d'informations et de les diffuser, d'interagir socialement, de faciliter les transactions et de coopérer à l'échelle internationale. Mais nous ne nous interrogeons pas suffisamment sur les technologies qui le sous-tendent et sur les évolutions technologiques rapides qui le caractérisent. La convivialité de la toile a pour inconvénient qu'elle nous fait parfois ignorer les risques potentiels liés à la complexité de ces structures sous-jacentes.

Pour ceux qui s'y connaissent, exploiter ces failles est un véritable jeu d'enfant. De nos jours, les pirates informatiques utilisent l'Internet pour organiser des actions criminelles, espionner des flux d'informations et les écouter en ligne, provoquer intentionnellement ou non la défaillance de systèmes et d'applications ou usurper des identités électroniques.

Du fait de la méconnaissance du fonctionnement de l'Internet, la cyberdimension risque de plus en plus de se transformer en un véritable Far-West où les criminels pourront agir sans entrave.

Aujourd'hui, la cybercriminalité revêt mille et une formes et le phénomène est en constante évolution. La caractéristique de ces criminels est qu'ils ne cessent d'innover et qu'ils ont toujours une longueur d'avance sur la surveillance informatique et la cybersécurité. On peut classer les menaces contre la cybersécurité en quatre types, en fonction de l'intention des criminels :

1. Le pirate « ordinaire » : il s'agit principalement d'étudiants et d'ingénieurs en informatique qui se lancent le défi de pirater un système informatique et qui ont pour objectif principal le piratage en lui-même, sans mauvaise intention, mais qui peuvent parfois occasionner des dommages considérables. Cela peut aller du piratage de réseaux d'écoles pour pouvoir changer des notes à la modification de la page d'accueil d'un site Web. Ils agissent pour asseoir la réputation et la gloire de leur nom ou de leur communauté de pirates, ou simplement par plaisir.

markten dichterbij en ondersteunt nieuwe productiemethodes. Maar tegelijk is het ook gevoeliger geworden voor onderbrekingen, wat nieuwe mogelijkheden voor cybercriminelen biedt.

De laatste twintig jaar is de wereld in toenemende mate verweven met de cyberdimensie. Deze ontwikkeling heeft een enorme impact gehad op ons dagdagelijkse leven, evenals de economie en samenleving in het algemeen. De snelheid en omvang van deze impact op het internet kon destijds werden voorspeld door visionairs en marktanalisten, maar de potentiële gerelateerde risico's, bedreigingen en uitdagingen werden slechts door enkelen aangekaart.

Het internet biedt de wereldbevolking vandaag een nooit eerder geziene manier om over informatie te beschikken en te verspreiden, om sociaal te interageren, transacties te faciliteren en internationaal samen te werken. We stellen ons echter te weinig vragen over de onderliggende technologieën die het internet rechthouden en de snelle technologische evolutie die het meemaakt. De nevenwerkingen van de « gebruiksvriendelijkheid » is dat we ons niet altijd bewust zijn van de potentiële risico's die meekomen met de complexiteit van deze onderliggende structuren.

Voor zij die hier wel kennis van hebben, is het uitbuiten van zwakheden een koud kunstje. Hackers gebruiken tegenwoordig het internet om misdrijven te organiseren, informatiestromen te bespioneren en af te luisteren, al dan niet intentioneel systemen en applicaties te doen falen of elektronische identiteiten te misbruiken.

Door de slechte kennis over de werking van het internet, riskeert de cyberdimensie steeds verder in een soort van Wilde Westen te vervallen, waar misdadigers zonder veel hinder hun gram kunnen halen.

Tegenwoordig is cybercrime aanwezig in allerhande formaten en blijft het fenomeen constant evolueren. Typisch is dat de criminelen zeer innovatief zijn en steeds een aantal stappen voor zijn op orderhandhavers en cybersecurity. Er is een onderscheid tussen vier soorten bedreigingen in cybersecurity, gebaseerd op de intentie van de criminelen :

1. De « gewone » hacker : voornamelijk studenten en computeringenieurs die de uitdaging aangaan om een computersysteem te hacken, waarbij de intentie voornamelijk het hacken zelf is, zonder hierbij een slechte bijbedoeling te hebben maar soms verregaande schade kan veroorzaken. Dit kan gaan van het hacken van schoolsystemen om de toetsresultaten te manipuleren of het uitzicht van een website aan te passen. Ze werken voor de faam en glorie van hun naam of hun hackersgemeenschap of louter voor hun plezier.

2. Le pirate criminel : son intention est de tirer de l'argent de son activité en piratant directement des systèmes et en volant des données de transaction pour les vendre au plus offrant ou demander une rançon. Il s'agit en l'occurrence du vol de mots de passe, de l'imitation de données d'identité électroniques, du vol ou du détournement de propriété intellectuelle. Le pirate criminel est étroitement lié au crime organisé.

3. « L'hacktivisme » : il s'agit d'une forme moderne d'activisme qui consiste à pirater des systèmes pour effectuer une déclaration dont la portée pourra être aussi bien politique que sociale. *WikiLeaks* en a été le fondateur, après s'être inspiré de l'activisme traditionnel, comme celui de Greenpeace, qui luttait contre les centrales nucléaires ou la pêche à la baleine. Il existe des collectifs d'activistes comme *Anonymous* ou *LulzSec*, qui cherchent à dénoncer la protection des systèmes et estiment que les autorités n'ont pas à réguler le cyberespace au détriment de la liberté.

4. L'espionnage, la cyberguerre et le terrorisme : il s'agit de la variante politique, qui met aux prises des États-nations, des terroristes ou des entreprises. Cela peut aller du vol de secrets industriels, de découvertes scientifiques et de droits de propriété intellectuelle jusqu'au détournement de secrets d'État. Nier la réalité de telles formes d'espionnage peut entraîner des pertes massives d'emplois à cause de la réduction de la compétitivité économique. Certains pays sont capables de bloquer l'accès à Internet d'autres pays, et même de contrôler, voire de neutraliser à distance, des systèmes critiques tels que les transports et la distribution d'électricité.

La cybercriminalité peut adopter différentes formes qui continuent d'évoluer parallèlement à l'objectif qu'elles poursuivent : logiciels malveillants, virus, phishing, enregistrement de frappes, injection de commandes sql, « reniflage », chevaux de Troie, etc. En recherchant sans cesse des failles encore inconnues dans des systèmes, réseaux et applications, en les combinant et en les adaptant, les cybercriminels veillent à être indétectables par les scanners automatiques de logiciels malveillants.

Les *botnets* (réseaux d'ordinateurs zombies) illustrent parfaitement à quel point les cyberattaques peuvent être massives et sont à même de ralentir ou même de bloquer des géants de l'Internet tels que *Google* et *Twitter*. Dans le cas d'une attaque par déni de service (DDOS), un grand nombre d'ordinateurs infectés, pilotés par un point de commande central, accèdent simultanément au serveur (Web) d'une entreprise. Conséquence : le serveur n'est temporairement plus disponible ou se bloque (*Distributed Denial of Service*). Les *botnets* sont des réseaux de dizaines ou de millions d'ordinateurs infectés qui envoient des pourriels (*spams*) en masse, répandent des virus,

2. De criminele hacker : de intentie is hier om geld te slaan uit hun activiteiten, door direct systemen te hacken en transactiegegevens te stelen en deze te verkopen aan de hoogste bieder of losgeld te vragen. Het gaat hier over het stelen van paswoorden, het imiteren van elektronische identiteitsgegevens, het stelen of compromitteren van intellectueel eigendom. De criminele hacker is nauw verbonden met de georganiseerde misdaad.

3. Hacktivisme : een moderne manier van activisme door systemen te hacken om een statement te maken, dat zowel politiek als maatschappelijk kan zijn. *Wikileaks* was hiervan de grondlegger en bouwt voort op het traditionele activisme zoals Greenpeace dat vocht tegen nucleaire centrales of walvisvangst. Er bestaan hacktivisme-collectieven zoals *Anonymous* of *LulzSec* die de beveiliging van systemen aan de kaak willen stellen en vinden dat de overheden cyberspace niet mogen reguleren ten koste van de vrijheid.

4. Spionage, cyberoorlog en terrorisme : de politiek gemotiveerde variant die plaats vindt tussen natiestaten, terroristen of bedrijven. Dit kan gaan van het stelen van industriële geheimen, wetenschappelijk onderzoek, intellectueel eigendom, tot staatsgeheimen. Het ontkennen van deze vormen van spionage kan resulteren in een massaal banenverlies door verlies aan economische competitiviteit. Sommige landen zijn in staat de internettoegang van bepaalde landen te blokkeren en zelf de kritieke systemen, zoals transport en elektriciteitsvoorziening, te controleren of zelfs te neutraliseren vanop afstand.

Er zijn verschillende manieren om aan cybercriminaliteit te doen, die blijven evolueren parallel met het doel : malware, virussen, phishing, keylogging, sql-injectie, afluisteren, Trojaanse paarden, ... Door telkens nog onbekende zwakheden in systemen, netwerken en applicaties te ontdekken, te combineren en aan te passen, zorgen cybercriminelen dat ze niet kunnen onderschept worden door automatische malware scanners.

Botnets zijn een goed voorbeeld van hoe cyberaanvallen op grote schaal kunnen plaatsvinden en in staat zijn internetgiganten zoals *Google* en *Twitter* te vertragen of zelfs af te sluiten. Bij een DDOS-aanval maakt een groot aantal besmette computers, aangestuurd door een centraal commandopunt, gelijktijdig een verbinding met een (web)server van een bedrijf. Daardoor wordt de server tijdelijk niet meer beschikbaar of crasht hij (*Distributed Denial of Service*). *Botnets* zijn netwerken van tientallen of miljoenen besmette computers die massaal spam versturen, virussen verspreiden, ongemerkt data doorsturen en aanvallen op computersystemen uitvoeren. Slechts een

transmettent sournoisement des données et exécutent des attaques sur des systèmes informatiques. Seule une partie des botnets actuels ont pu être détectés et neutralisés efficacement.

Aperçu des principaux cyberincidents des dernières années :

En 2007, l'infrastructure internet de l'Estonie a été attaquée par un *botnet* qui a privé le pays de connexion pendant une semaine. L'attaque dirigée contre l'Estonie a duré trois semaines et n'a cessé que parce que les pirates y ont eux-mêmes mis un terme. Il s'agissait d'une attaque massive par déni de service (DDOS) menée contre les sites des autorités après qu'un différend entre la Russie et l'Estonie concernant le déplacement d'un monument aux morts militaire se soit envenimé.

Janvier 2009 : le virus *Conficker* est répandu au moyen d'une clé USB infectée et l'hôpital Imelda à Bonheiden est gravement touché.

En 2010, *WikiLeaks* publie des millions de documents de l'armée américaine après les avoir reçus d'un soldat mécontent possédant les habilitations de sécurité adéquates. La communication interne de diplomates et d'officiers est disponible en ligne et apporte un éclairage tout à fait différent sur les guerres d'Irak et d'Afghanistan.

Stuxnet, un virus informatique destiné à retarder le programme d'enrichissement nucléaire iranien, fait également son apparition en 2010. Ce virus incroyablement sophistiqué (*multilayered*) est spécialement conçu pour manipuler des systèmes de contrôle industriels, comme les systèmes SCADA qui commandent une centrale nucléaire. *Stuxnet* serait l'œuvre d'une équipe restreinte mais particulièrement professionnelle, disposant d'un budget très considérable.

En 2011, plusieurs millions de données de cartes de crédit d'utilisateurs du réseau de PlayStation Sony en ligne sont dérobées. Ces dernières ont probablement été proposées par la suite, contre paiement, au crime organisé.

6 janvier 2012 : le collectif *Anonymous* pirate le site Internet d'ArcelorMittal après l'annonce, par ce groupe industriel, de la fermeture de la phase à chaud de Liège. Les pirates affirment que plusieurs organisations belges (des hôpitaux notamment) utilisent le même script vulnérable *Perl* et peuvent recourir à la même méthode si elles le souhaitent.

Avril 2012 : le SPF Finances met en garde contre un site Internet qui utilise le logo officiel du service public pour subtiliser les données de la carte de crédit de contribuables à leur insu.

fractie van de botnets die bestaan worden succesvol opgespoord en geneutraliseerd.

Een overzicht van de belangrijkste cyberincidenten van de voorbije jaren :

In 2007 werd de internetinfrastructuur van Estland aangevallen door een *botnet*, waardoor het land gedurende een week niet verbonden was. De aanval tegen Estland duurde drie weken en is enkel gestopt omdat de hackers de aanval hebben stopgezet. Het ging om een massale DDOS-aanval op de overheidswebsites nadat een rel tussen Rusland en Estland over de verplaatsing van een oorlogsmonument escaleerde.

Januari 2009 : via een besmette USB-stick wordt het *Conficker*-virus verspreid en wordt het Imelda-ziekenhuis te Bonheiden zwaar getroffen.

In 2010 maakte *WikiLeaks* miljoenen documenten van het Amerikaanse leger openbaar, nadat een misnoegde soldaat met de juiste veiligheidsmachtigingen deze had doorgespeeld aan de klookkenluiderswebsite. De interne communicatie van diplomaten en officieren komt online te staan en werpt een heel ander licht op de oorlogen in Irak en Afghanistan;

Eveneens in 2010 dook *Stuxnet* op, een computervirus dat het atoomverrijkingsprogramma van Iran trachtte te vertragen. Het virus heeft een ongeziene sofisticatie (*multilayered*), speciaal om industriële controlesystemen te manipuleren, bijvoorbeeld zoals de SCADA-systemen die een nucleaire centrale regelen. *Stuxnet* zou het werk zijn van een klein maar bijzonder professioneel team met een zeer groot budget.

In 2011 werden miljoenen creditcardgegevens gestolen van gebruiker van het online Sony PlayStation netwerk. Vermoedelijk werden deze daarna te koop aangeboden aan de georganiseerde misdaad.

6 januari 2012 : *Anonymous* hackt de website van ArcelorMittal nadat deze aangekondigd had de warme lijn te Luik te gaan sluiten. De hackers stellen dat menige Belgische organisaties hetzelfde zwakke *Perl*-script gebruiken, onder meer ziekenhuizen, en ze daarmee hetzelfde trucje kunnen uithalen indien ze willen.

April 2012 : de FOD Financiën waarschuwt voor een website die het officiële logo van de dienst gebruikt om de kredietkaartgegevens van nietsvermoedende belastingplichtigen te ontfutselen.

2 mai 2012 : des pirates menacent de divulguer des informations confidentielles sauvegardées sur le serveur du site du prêteur Elantis. Les pirates réclament 150 000 euros en échange des données. Il s'agit en l'occurrence d'hacktivistes qui dénoncent le manque de sécurisation de certaines informations confidentielles.

31 mai 2012 : un reportage de l'émission Panorama montre comment un pirate peut facilement avoir accès au système d'exploitation d'une école de Lommel pour y manipuler la température dans la salle d'étude, comment il parvient à ouvrir des cellules dans une prison américaine ou des écluses, et à accéder aux ordinateurs de centrales nucléaires.

15 juin 2012 : un pirate se faisant appeler Rex Mundi menace de divulguer les profils volés de la société d'intérim AGO si cette dernière ne lui verse pas une rançon. Le pirate prouve sa détermination en diffusant des documents internes contenant des adresses électroniques, des noms et des rapports d'entretiens d'intérim, dont certains sont très dénigrants.

25 juin 2012 : quatre personnes suspectées de piratage de sites bancaires sont arrêtées. Un montant total de plus de 0,8 million d'euros est dérobé.

En octobre 2012, on apprend qu'au cours des dix premiers mois de l'année, quatre cent quatre-vingt clients de banques ont déjà été victimes de vols via l'Internet, pour un préjudice total de près d'un million d'euros.

En 2012, le nombre d'intrusions réussies dans des systèmes informatiques d'entreprises établies en Belgique est en forte hausse par rapport aux années précédentes. Les entreprises éprouvent toujours une certaine réticence à déclarer des cyberincidents, par peur de perdre la face; c'est pourquoi ces incidents sont généralement rendus publics par les pirates eux-mêmes.

En 2012, un virus encore plus sophistiqué fait son apparition, de nouveau en Iran. Baptisé « Flame », il permettrait d'espionner toutes les activités des ordinateurs et de les transmettre à un centre de commandement et de contrôle.

Le cyberespace est d'une complexité telle qu'on ne peut parler aujourd'hui que de solutions fragmentaires et partielles. Les innombrables anti-virus, sécurisations de réseau et techniques de gestion d'identité sont, dans certains cas, déjà dépassés après une semaine à peine. Même si l'on décidait de se passer de l'Internet, cela ne serait pas suffisant pour suivre l'évolution permanente des applications sans fil. L'internet est devenu incontournable, il est ouvert à tous et la sécurité de son utilisation doit être garantie. La collectivité ne pourra trouver une manière efficace d'identifier et de combattre la cybercriminalité qu'en

2 mei 2012 : hackers dreigen ermee vertrouwelijke informatie openbaar te zullen maken die op de server van de website van de kredietverlener Elantis bevindt. De hackers eisen 150 000 euro in ruil voor de gegevens. Hier gaat het over hacktivisten die de zwakke beveiliging van vertrouwelijk informatie op de korrel nemen.

31 mei 2012 : in een reportage van Panorama wordt getoond hoe een hacker gemakkelijk toegang kan krijgen het besturingssysteem van een Lommelse school en de temperatuur in de studiezaal manipuleert, celdeuren weet te openen in een Amerikaanse gevangenis, sluizen kan openen en toegang kan krijgen tot de computers van nucleaire centrales.

15 juni 2012 : een hacker die zich Rex Mundi noemt dreigt ermee de gestolen profielen van het interimkantoor AGO-interim vrij te geven tenzij ze losgeld geven. Als bewijs worden er interne documenten gelekt zoals e-mailadressen, namen en verslagen van interimgesprekken die soms zeer denigrerend zijn.

25 juni 2012 : er worden vier personen aangehouden die verdacht worden van hacking van bankenwebsites. In totaal werden bedragen gestolen voor meer dan 0,8 miljoen euro.

In oktober 2012 raakte bekend dat in de eerste tien maanden van dit jaar reeds vierhonderdtachtig cliënten van banken bestolen werden via het internet voor een totale som van bijna één miljoen euro.

In 2012 zijn in België het aantal succesvolle inbraken in computersystemen van bedrijven sterk gestegen in vergelijking met de vorige jaren. Er heerst bij de bedrijven nog altijd een taboe om cyberincidenten aan te geven om geen gezichtsverlies te leiden, daarom worden ze meestal wereldkundig gemaakt door de hackers zelf.

In 2012 duikt een nog gesofisticeerder virus op, opnieuw in Iran. Het wordt *Flame* genoemd en zou alle activiteiten op computers kunnen bespioneren en doorsturen naar een commando-en controlecentrum.

Door de complexiteit van cyberspace is er vandaag slechts sprake van gefragmenteerde en gedeeltelijke oplossingen. De ontelbare antivirussen, netwerkbeveiligingen, identiteitsbeheertechnieken zijn na een week of dag al achterhaald. Zelfs indien men kiest om geen gebruik meer te maken van het internet, zou dit zelf niet genoeg zijn om met de steeds evoluerende draadloze toepassingen te kunnen meegaan. Het internet is een must geworden, is er voor eenieder en de vrijheid om het in veiligheid te gebruiken moet worden verrrekend. Opdat de gemeenschap een effectieve manier zou vinden om cybercrime te

passant par une approche holistique et globale, dans le cadre de laquelle tous les aspects des systèmes et des programmes, ainsi que le facteur humain, seraient mis au service de la sécurisation des technologies, à tous les niveaux. L'accent doit être mis sur la gestion du risque, afin que la relation entre sécurité, convivialité et fonctionnalité reste optimale pour l'utilisateur.

La fragmentation et l'inefficacité sautent aux yeux dès l'instant où l'on examine les modalités organisationnelles de la lutte contre la cybercriminalité et la façon dont la cybersécurité est assurée. Comme la lutte doit être menée par des individus, des services de sécurité, les CERT, la Justice, des départements de services publics, des autorités locales et internationales et des ministres qui n'ont pas ou guère harmonisé leur politique, il est de plus en plus aisé pour les pirates de déceler les failles dans les systèmes de sécurisation.

Cybercriminalité

Dans son rapport « *Organized Crime Threat Assessment* » publié en 2011 (1), Europol note que le modèle organisationnel de la cybercriminalité, qu'il a analysé, a évolué d'une organisation hiérarchique vers un modèle horizontal. Celui-ci se caractérise par l'absence d'un *leadership* clair, mais aussi par la répartition du travail en fonction des spécialités techniques et par le fait que la majorité des membres ne se connaissent que par leurs contacts en ligne. Selon le rapport, la cybercriminalité tient sa spécificité de son degré d'automatisation, qui permet d'opérer sans plus devoir se rencontrer physiquement. Dans ce contexte, les *botnets*, c'est-à-dire des réseaux d'ordinateurs zombies infectés, sont cruciaux pour la rentabilité de la cybercriminalité. Grâce à un botnet, les cybercriminels peuvent utiliser des milliers d'ordinateurs compromis pour lancer simultanément des attaques automatisées contre des systèmes de particuliers et d'entreprises, envoyer des *spams*, héberger des sites web de *phishing*, distribuer des crimeware, lancer des attaques DDOS (*distributed denial of service*) et analyser des systèmes dans le but d'en détecter les failles.

Le degré d'automatisation atteint peut permettre à un petit groupe d'individus de construire un botnet avec succès. La rapidité avec laquelle un botnet permet d'opérer au-delà des frontières étatiques conventionnelles et l'anonymat qu'il confère posent des défis de taille. En l'occurrence, il est surtout important de pouvoir compter sur des méthodes de détection rapides, de bien comprendre le contexte légal et juridique et d'établir un niveau de coopération inédit entre pays et entre acteurs privés et publics.

(1) *Internet Facilitated Organized Crime Threat Assessment.*

identificeren en te bestrijden is een holistische, alomvattende benadering nodig, waarin alle aspecten van systemen, programma's en de menselijke factor in kaart worden gebracht om alle niveaus van technologie te beveiligen. De nadruk moet hier gelegd worden op *riskmanagement*, zodat de relatie tussen veiligheid, bruikbaarheid en functionaliteit optimaal behouden blijft voor de gebruiker.

De fragmentatie en inefficiëntie wordt zeer duidelijk wanneer we kijken naar de organisatorische manieren waarop cybercrime wordt bestreden en de manier waarop in cyberveiligheid wordt voorzien. Omdat de bestrijding dient te gebeuren door individuen, veiligheidsdiensten, de CERTs, justitie, overheidsdepartementen, lokale en internationale overheden, en ministers die hun beleid niet of amper op elkaar hebben afgestemd, wordt het voor de hackers alleen maar makkelijker wordt om zwakheden in de beveiliging te ontdekken.

Cybercrime

In het iOCTA (1) rapport van 2011, heeft Europol na een analyse van het cybercrimineel businessmodel een verschuiving vastgesteld van een hiërarchische organisatie naar een flat model. Dit wordt gekenmerkt doordat er geen duidelijk leiderschap te onderscheiden valt, maar ook doordat arbeid verdeeld wordt volgens de technische specialiteiten, en de meeste leden elkaar enkel kennen van hun online contacten. Het rapport identificeert verder dat de eigenheid van cybercrime ligt in haar mate van automatisatie, waarin de nood om fysiek samen te komen niet langer noodzakelijk is om te opereren. In deze context zijn botnets — een netwerk van geïnfecteerde zombie-computers — cruciaal voor de rendabiliteit van cybercrime. Door middel van een botnet kunnen cybercriminelen gebruik maken van duizenden gecompromitteerde computers tegelijkertijd om geautomatiseerde aanvallen uit te voeren op systemen van particulieren en bedrijven, *spam* rond te sturen, *phishing*-websites te hosten, crimeware te distribueren, DDOS-aanvallen uit te voeren en systemen te scannen op zwakheden.

Deze mate van automatisering kan ervoor zorgen dat een kleine groep van individuen met succes een botnet kunnen opzetten. De snelheid waarmee een botnet over de conventionele landsgrenzen kan opereren en de anonimiteit dat hiermee gepaard gaat stelt ons voor grote uitdagingen. Dit gaat vooral over snelle detectiemethoden, het verstaan van de legale en juridische context en de noodzaak om tot een nieuw niveau van samenwerking te komen tussen landen en tussen private en publieke actoren.

(1) *International Assessment of Internet Facilitated Organized Crime.*

Impact sur les citoyens et les infrastructures critiques

Selon un rapport de PricewaterhouseCoopers, pas moins de 44 % des entreprises belges ont été victimes de la cybercriminalité en 2011 (1). C'est la deuxième forme la plus fréquente de criminalité économique dans notre pays. En général, les entreprises ne sont pas promptes à signaler les cyberattaques dirigées contre leurs systèmes informatiques, par crainte que cela nuise à leur image de marque. Il est dès lors difficile d'estimer à leur juste valeur les dommages causés par la cybercriminalité. On pourrait contribuer à y remédier en imposant aux entreprises l'obligation de signaler les cyberincidents, comme cela se fait déjà dans un certain nombre d'États des États-Unis ainsi qu'en Grande-Bretagne.

Sur la base d'entretiens réalisés avec des clients et des partenaires en Belgique, *Trend Micro* conclut que les entreprises sont conscientes des dangers et menaces liés à l'Internet mais sont prêtes à courir le risque d'être victimes de cybercriminalité (2). Ce risque s'accroît cependant avec des technologies populaires, liées par exemple à la mobilité, la consumérisation de l'IT (CoIT), la virtualisation et l'informatique en nuage (« *cloud computing* »), pour lesquelles il n'existe actuellement pas de solutions satisfaisantes. Ces tendances (mobiles) créent un contexte de coopération en perpétuelle mutation et exigent un autre mode de sécurisation.

Même les pouvoirs publics ne sont pas épargnés. Selon le CERT, le SPF Politique scientifique a déjà essuyé à quatre reprises une cyberattaque. Dans un des cas, le serveur du Conseil d'État avait été utilisé pour l'envoi de *spams*. Dans un autre cas, un logiciel malveillant (« *malware* ») s'était introduit et avait réussi à dérober les données d'accès d'un utilisateur et à les transmettre à une partie externe. Enfin, un mot de passe lié au quartier général de l'Agence spatiale européenne (ESA) à Frascati en Italie aurait également été volé.

Le gouvernement étant avare de commentaires sur ces cas, il est difficile d'estimer dans quelle mesure les failles en question ont pu être exploitées pour commettre des abus. Par ailleurs, d'autres cyberincidents n'ont pas été rendus publics pour des raisons de sécurité. Quoi qu'il en soit, les sites internet des pouvoirs publics doivent tous faire l'objet d'un monitoring permanent en phase avec les dernières évolutions dans le domaine des TIC, et les connaissances y afférentes devraient de préférence être transmises aux États membres de l'Union européenne.

(1) *http://www.pwc.be/fr/press/2011-11-29-crime-survey.jhtml.*

(2) *http://www.trendmicro.nl/newsroom/pr/trend-micros-q-security-roundup-report-cybercrime-is-big-business-en-wordt-steeds-persoonlijker/.*

Impact op de kritieke infrastructuren en burgers

Volgens een rapport van PricewaterhouseCoopers was in 2011 maar liefst 44 % van de Belgische bedrijven het slachtoffer van cybercriminaliteit (1). Het is de tweede meest voorkomende vorm van economische criminaliteit in ons land. Bedrijven zijn meestal afwachtend om cyberaanvallen op hun computersystemen bekend te maken uit angst voor imagoschade. Hierdoor is het ook moeilijk om de ware schade van cybercriminaliteit te kunnen inschatten. De verplichting voor bedrijven om cyberincidenten te melden, zoals nu al in een aantal staten van de VS en in Groot-Brittannië geldt, zou hiertoe kunnen helpen.

Uit gesprekken met klanten en partners in België concludeert *Trend Micro* dat bedrijven zich bewust zijn van de internetgevaren en bedreigingen, maar dat ze bereid zijn het risico te nemen het slachtoffer te worden van een cybercrimineel (2). Dat risico wordt echter almaar groter door populaire technologieën als mobiliteit, CoIT (*consumerisation of IT*), virtualisatie en *cloud computing* waarvoor bestaande oplossingen tekortschieten. Deze (mobiele) trends creëren een steeds veranderende samenwerkingscontext en vragen om een andere manier van beveiligen.

Zelfs de overheid wordt niet gespaard. Volgens CERT is de FOD Wetenschapsbeleid reeds vier keer het slachtoffer geweest van een cyberaanval. In één geval ging het over het gebruik van de server van de Raad van State voor het versturen van *spam*. In een ander geval ging het over een intrusie van *malware* die de inloggegevens van een gebruiker heeft kunnen ontvreemden en dit heeft kunnen doorsturen naar een externe partij. Ten slotte zou er ook nog een paswoord gestolen zijn dat te maken zou hebben met het hoofdkwartier van het Europees Ruimteagentschap ESA te Frascati in Italië.

Omdat de regering karig blijft met commentaar omtrent deze gevallen is het ook moeilijk in te schatten in hoeverre misbruik werd gemaakt van deze « openstaande achterpoortjes ». Ook worden andere cyberincidenten niet bekend gemaakt omwille van veiligheidsredenen. Zeker is wel dat alle overheidswebsite constante monitoring nodig hebben die up-to-date is met de recentste ontwikkelingen op ICT-gebied, en deze kennis het best op Europees niveau moet worden verspreid naar de lidstaten.

(1) *http://www.pwc.be/nl/press/2011-11-29-crime-survey.jhtml.*

(2) *http://www.trendmicro.nl/newsroom/pr/trend-micros-q-security-roundup-report-cybercrime-is-big-business-en-wordt-steeds-persoonlijker/.*

Les ministres s'accordent à dire que des incidents de sécurité ont lieu en permanence, mais que ceux-ci ne présentent pas tous la même ampleur ni la même complexité (1). Les pouvoirs publics sont cependant incapables de dire actuellement si les incidents de sécurité débouchent sur des abus, pas plus qu'ils ne savent quelle est l'identité de la partie externe ou la durée d'un incident.

On sait néanmoins que la plupart des cyberintrusions viennent de pays émergents tels que la Chine, la Russie et l'Inde, sans pouvoir pour autant identifier les commanditaires parce que les pirates informatiques savent bien dissimuler leurs traces.

Partie de l'agenda européen

Une évolution technologique s'opère actuellement dans les domaines de l'informatique en nuage (« *cloud computing* ») et du développement d'appareils électroniques appelés à être connectés à l'Internet à tout moment et en tout lieu. C'est la raison pour laquelle quelques projets mettant l'accent sur la nécessité d'une coopération mutuelle existent déjà au niveau européen. Le septième programme-cadre (7e PC) et le programme d'appui stratégique en matière de technologies de l'information et de la communication du programme-cadre pour la compétitivité et l'innovation (CIP ICT PSP), publiés récemment par la Commission européenne, sont entièrement consacrés à la cybersécurité et appellent à la réalisation de davantage de recherches et à l'adoption d'une approche plus ciblée en la matière.

Le 30 mars 2009, la Commission européenne a publié sa communication relative à la protection des infrastructures d'information critiques (PIIC (2)), par laquelle l'Europe entend se protéger contre les cyberattaques et les coupures de réseau à grande échelle. L'objectif poursuivi est d'améliorer la préparation, la sécurité et la résilience des États membres et de proposer un plan visant à renforcer la sécurité et la résilience des infrastructures d'information critiques (plan d'action PIIC). Ce plan d'action s'articule autour des cinq axes suivants : la préparation et la prévention, la détection et la réaction, l'atténuation et la récupération, la coopération internationale et les critères concernant les infrastructures critiques européennes dans le secteur des TIC. Il indique les tâches à accomplir, au titre de chacun de ces axes, par la Commission, les États membres et/ou les entreprises, avec le soutien de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

(1) Réponse du ministre des Affaires étrangères Steven Vanackere à la question écrite no 5-4302.

(2) *http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.*

De ministers zijn het er over eens dat er constant veiligheidsincidenten plaatsvinden, maar dat deze verschillen in omvang en complexiteit (1). Op dit moment blijft het voor de overheid echter onbekend of er misbruik wordt gemaakt van veiligheidsincidenten, wie de externe partij is en hoelang een incident duurde.

Men kan wel leren dat de meeste cyberintrusies afkomstig zijn uit groeilanden zoals China, Rusland en India, maar het is niet te achterhalen wie de opdrachtgevers zijn omdat hackers hun sporen goed kunnen camoufleren.

Deel van de Europese agenda

Op dit ogenblik vindt er een technologische evolutie plaats op de vlakken van *cloud computing* en de ontwikkeling van elektronische toestellen die altijd en overal verbonden zullen zijn met het internet. Daarom lopen er op Europees niveau reeds enkele projecten die de nood voor wederzijdse samenwerking benadrukken. De recente bekendmaking door de Europese Commissie van het *7th Framework Programme* (FP7) en het *Information Communication Technologies Policy Support Programme in Competitiveness and Innovation Framework Programme*(CIP PSP) draaien volledig om cybersecurity en roept op tot meer research en een meer doelgerichte aanpak.

Op 30 maart 2009 stelde de Europese Commissie het (CIIP (2)) voor, waarmee Europa zich wil beschermen tegen grootschalige cyberaanvallen en netwerkonderbrekingen. De doelstelling is om de voorbereiding, beveiliging en slagkracht van de lidstaten te versterken en een plan voor te stellen om de beveiliging en slagkracht van vitale ICT-infrastructuren te versterken (CIPP-actieplan). Het CIIP-actieplan is gebouwd op vijf pijlers : paraatheid en preventie, detectie en respons, afzwakking en herstelling, internationale samenwerking en het vaststellen van criteria voor Europese kritieke infrastructuren op ICT-vlak. Het benadrukt het werk dat onder elke pijler moet gedaan worden door de Europese Commissie, de lidstaten en/of industrie, met de steun van het Europees Netwerk en Informatieveiligheidagentschap (ENISA).

(1) Antwoord van minister van Buitenlandse Zaken Steven Vanackere op schriftelijke vraag nr. 5-4302.

(2) *http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.*

La confiance et la sécurité sont les conditions fondamentales à la mobilisation de programmes TIC. La stratégie numérique pour l'Europe 2010-2020 (1) propose à cet égard que toutes les parties concernées allient leurs forces pour développer plus avant la sécurité et la résilience des infrastructures TIC en mettant l'accent sur la prévention, la préparation et la conscientisation.

Des menaces inédites et sophistiquées se font jour sans cesse, affichant également une dimension géopolitique de plus en plus claire. Nous devons faire face à un courant qui considère les TIC comme un moyen de prendre le contrôle dans les domaines politique, économique et militaire, y compris par des options offensives.

L'expérience nous montre qu'une approche exclusivement nationale de ce problème n'est pas suffisante. Au terme du *Cyber Exercise 2010*, auquel seuls les États membres européens ont participé, il a été admis ouvertement que la participation du secteur privé aurait été tout aussi importante. C'est pourquoi les banques et fournisseurs d'accès à Internet (ISP) ont, eux aussi, été conviés à participer au cyberexercice paneuropéen suivant, au cours duquel ont été simulés mille deux cents cyberincidents différents faisant partie d'une attaque DDOS dirigée contre des sites internet de pouvoirs publics et des systèmes informatiques de grandes banques européennes.

Des efforts sont également déployés aux États-Unis depuis des années pour amener les pouvoirs publics, l'industrie et la recherche à harmoniser leurs initiatives. L'on refuse que la cybersécurisation du pays soit tributaire d'une confiance aveugle dans les réseaux, mais l'on veut contribuer à un État dynamique. Cet État dynamique doit reposer sur un processus permanent d'adaptations défensives et anticipatives, lequel ne doit pas se limiter à la défense militaire étant donné l'impact qu'il a également sur les pouvoirs publics, les entreprises et la compétitivité de celles-ci. En 2012, Washington a prévu un budget de pas moins de 13,1 milliards de dollars pour la cybersécurisation.

La situation en Belgique

On ne sait pas très bien au niveau gouvernemental quel service public est chargé de diriger le projet de cyberdéfense. Renseignements pris auprès des différents services publics fédéraux (SPF) concernés, il s'avère qu'il n'y a pas de vision homogène quant à la question de savoir quelles tâches doivent être effectuées et par quels services.

Ainsi, en 2005, une plate-forme de concertation sur la sécurité des réseaux informatiques — appelée plate-forme BELNIS — a été créée; elle se réunit tous les mois

(1) *http://ec.europa.eu/digital-agenda/.*

Vertrouwen en beveiliging zijn de fundamentele voorwaarden om de mobilisatie van ICT-programma's te verwezenlijken. De *Digital Agenda for Europe* 2010-2020 (1) stelt hiertoe voor dat alle belanghebbenden hun krachten bundelen om op een holistische manier de veiligheid en slagkracht van de ICT-infrastructuren verder te ontwikkelen door te focussen op preventie, paraatheid en bewustmaking.

Steeds nieuwere en gesofisticeerde bedreigingen duiken op en tegelijk wordt hun geopolitieke dimensie ook duidelijker. We zijn getuige van een trend die ICT als een middel ziet om te overheersen op politiek, economisch en militair vlak, inclusief de offensieve mogelijkheden.

Ervaring leert ons dat de exclusief nationale aanpak van dit probleem onvoldoende is. Na de *Cyber Exercise 2010*, waarin enkel de Europese lidstaten deelnamen, werd openlijk erkend dat de private sector even belangrijk zou geweest zijn. Daarom werden op de volgende pan-Europese cyberoefening eveneens de banken en internet service providers (ISP's) uitgenodigd. Tijdens deze oefening worden duizendtweehonderd verschillende cyberincidenten gesimuleerd die uitmaken van een DDOS-aanval op publieke websites en computersystemen van grote Europese banken.

Ook in de Verenigde Staten werkt men al jaren om de overheid, industrie en research op één lijn te brengen. Men wil de cyberbeveiliging van het land niet laten afhangen van blind vertrouwen in de netwerken en men wil werken aan een dynamische staat. Deze moet bestaan uit een permanent proces van defensieve en anticiperende aanpassingen. Dit moet niet beperkt worden tot militaire defensie, want het heeft eveneens een impact op de overheid, de ondernemingen en de competitiviteit van de ondernemingen. In 2012 budgetteerde Washington maar liefst 13,1 miljard dollar voor cyberbeveiliging.

De situatie in België

Binnen de Belgische regering is het onduidelijk welke overheidsdienst de leiding heeft in het cyberdefensieproject. Uit een navraag bij de verschillende betrokken federale overheidsdiensten (FOD's) blijkt dat er geen homogene visie bestaat over wie welke taak op zich neemt.

Zo werd in 2005 het BELNIS-overlegplatform opgericht dat op maandelijkse basis bij elkaar komt om antwoorden voor te stellen op de vragen met

(1) *http://ec.europa.eu/digital-agenda/.*

et a pour mission d'apporter des réponses aux questions sur la protection des infrastructures critiques. Or, malgré le fait que les SPF participent à la plate-forme BELNIS, aucun haut fonctionnaire n'a été désigné pour la diriger et aucun représentant de celle-ci ne participe à la concertation en matière de sécurité organisée au cabinet du premier ministre. Les SPF ne sont pas obligés de signaler les incidents de sécurité à BELNIS. Il en résulte que le service public fédéral Technologie de l'information et de la Communication (FEDICT), qui assure le secrétariat, n'a pas ou guère les compétences requises pour pouvoir élaborer une politique de cyberdéfense conjointement avec BELNIS. La faiblesse de BELNIS est encore accentuée par le fait que celle-ci a pour unique mission d'adresser des recommandations et qu'elle ne se réunit jamais en juillet et en août.

Au SPF Intérieur, on précise que BELNIS est chargée de faciliter la coordination entre les départements mais qu'elle n'a aucune compétence opérationnelle. L'amélioration et le renforcement de cette collaboration relèvent de la responsabilité du Premier ministre, comme le précise la ministre de l'Intérieur, Mme Joëlle Milquet (1).

Du côté de la Défense, on déclare que le département de la Justice dirige le projet de cyberdéfense et qu'il agit conjointement avec la *Federal Computer Crime Unit* (FCCU) de l'Intérieur (2).

Par ailleurs, il faut également tenir compte des accès Internet de tous les SPF qui — comme c'est le cas pour l'ensemble des universités et des parlements — sont gérés par le Service public de programmation de la Politique scientifique (BELSPO), lequel relève à son tour de la compétence du ministre Paul Magnette.

En principe, il est de la responsabilité du premier ministre de développer une politique nationale de sécurisation de l'information, mais en l'absence d'une telle politique, chaque service public fédéral doit veiller lui-même à sa propre cybersécurité. Ainsi, chaque service public prévoit des budgets à cet effet et prend des mesures de sécurisation de sa propre initiative et sans aucune concertation avec d'autres départements. Il est clair que ce n'est pas la manière la plus efficace de se prémunir contre les risques de cyberattaques.

Entre-temps, certains services publics ont désigné un conseiller spécial chargé de coordonner la politique en matière de sécurité de l'information. C'est ainsi que le SPF Affaires étrangères a confié cette tâche à un *Chief Security Officer*; la Défense, quant à elle, s'en remet dans ce domaine au SGRS et, au département de l'Intérieur, on a décidé en décembre 2011 de faire appel à la société ICT Control SA.

(1) Question écrite n° 5-4315 du sénateur Karl Vanlouwe.

(2) Question orale n° 5594 de la députée Karolien Grosemans.

betrekking tot de bescherming van kritieke infrastructuur. Ondanks dat de FOD's hierin betrokken zijn heeft BELNIS geen hoge functionaris aan het hoofd en geen vertegenwoordiger bij het veiligheidsoverleg van het kabinet van de premier. Voor de FOD's is het niet verplicht om veiligheidsincidenten te melden aan BELNIS. Dit zorgt ervoor dat FedICT, dat het secretariaat op zich neemt, weinig of geen bevoegdheden heeft om met BELNIS een cyberbeleid uit te bouwen. Het zwakke karakter van BELNIS wordt nog versterkt doordat dit overlegplatform slechts aanbevelingen kan uitwerken en tijdens juli en augustus nooit samenkomt.

Binnenlandse Zaken zegt dat het BELNIS is dat de interdepartementale coördinatie doet, maar geen enkele operationele bevoegdheid heeft. De verbetering en versterking van deze samenwerking hangt af van de eerste minister, zo stelt minister van Binnenlandse Zaken Joëlle Milquet (1).

Defensie stelt dan weer op zijn beurt dat Justitie de piloot is van het cyberproject en samen met de *Federale Computer Crime Unit* (FCCU) van Binnenlandse Zaken ageert (2).

En dan zijn er ook nog de internettoegangen van alle FOD's, die net als alle universiteiten en parlementen, beheerd worden door de overheidsdienst Wetenschapsbeleid (BELSPO) dat op zijn beurt onder de bevoegdheid valt van minister Paul Magnette.

In se is het de verantwoordelijkheid van de eerste minister om een nationaal informatieveiligheidsbeleid te ontwikkelen, maar in afwezigheid hiervan is elke federale overheidsdienst op zichzelf aangewezen voor haar cyberveiligheid. Zo stelt elke overheidsdienst haar eigen budgetten op en neemt ze op eigen initiatief, en zonder enige coördinatie met andere departementen, beveiligingsmaatregelen. Het laat zich raden dat dit niet de meest efficiënte manier is om de cyberdreiging aan te pakken.

Sommige overheidsdiensten bezitten ondertussen wel al een speciale adviseur ter coördinatie van de informatieveiligheid. Bij Buitenlandse Zaken gaat het over een *Chief Security Officer*, bij Defensie neemt ADIV deze taak op zich, en bij Binnenlandse Zaken werd in december 2011 deze taak aan het bedrijf ICT Control NV uitbesteed.

(1) Schriftelijke vraag nr. 5-4315 van senator Karl Vanlouwe.

(2) Mondelinge vraag nr. 5594 van volksvertegenwoordigster Karolien Grosemans.

Les particuliers et les exploitants de secteurs critiques en sont réduits, pour leur part, à devoir prendre eux-mêmes des mesures afin de protéger leurs logiciels. Les pouvoirs publics se contentent de diffuser des informations par le biais du site Internet du *Computer Emergency Response Team* (CERT) (un service public qui a pour mission d'informer la population belge au sujet de la sécurisation informatique).

En Belgique, les principaux intervenants dans ce domaine sont les suivants :

— les services de renseignement, à savoir le SGRS et la Sûreté de l'État :

• le SGRS (Service général du renseignement et de la sécurité) : le service de sécurité de la Défense est chargé de veiller à la sécurité des systèmes informatiques et de communications et de protéger le secret au sein de la Défense. Le SGRS fait rapport au Chef de la Défense (CHoD) et au ministre de la Défense (MoD);

• la Sûreté de l'État (VSSE) : le service du renseignement civil a pour mission de collecter, d'analyser et de traiter des informations dans le but d'identifier les menaces potentielles envers les intérêts fondamentaux de l'État et de ses citoyens, de mener des enquêtes de sécurité et de protéger les personnes;

— l'OCAM (Organe de coordination pour l'analyse de la menace) : il réalise des évaluations ponctuelles ou stratégiques sur les menaces terroristes et extrémistes en et contre la Belgique. À cet effet, il se base sur les renseignements qu'il reçoit des services d'appui. Au final, ce sont les pouvoirs publics qui devront prendre les mesures qui s'imposent afin de contrer toute menace éventuelle. L'OCAM est placé sous l'autorité conjointe du ministre de l'Intérieur et du ministre de la Justice. Il semblerait toutefois que l'OCAM se préoccupe surtout des menaces conventionnelles alors qu'aujourd'hui, nous devons aussi faire face à des défis d'une toute autre portée;

— le Comité permanent R : il est chargé de contrôler les activités et le fonctionnement de la Sûreté de l'État et du Service général du renseignement et de la sécurité. Ce contrôle doit permettre d'apprécier la légitimité, l'efficacité et la coordination des activités et donne lieu chaque année à l'établissement de rapports critiques. Ainsi, dans ses rapports annuels, le Comité R a épinglé le manque de coordination au niveau de la politique fédérale et l'absence d'une vision d'avenir;

— le Comité ministériel du renseignement et de la sécurité : il a également pour tâche de garantir la continuité de la politique en matière de sécurité. Les différents ministres responsables qui y siègent peuvent

Maar particulieren en exploitanten van kritieke sectoren moeten op eigen initiatief maatregelen inzake software nemen. De overheid beperkt zich enkel en alleen tot het verspreiden van informatie via de website van CERT (een publieke dienst met als missie de Belgische bevolking te voorzien van informatie rond computerbeveiliging).

Een opsomming van de in België relevante actoren :

— de inlichtingendiensten ADIV en VSSE :

• ADIV (Algemene Dienst van Inlichtingen en Veiligheid) : de veiligheidsdienst van Defensie, heeft de opdracht te zorgen voor het behoud van de veiligheid van informatica- en verbindingssystemen en het beschermen van het geheim binnen Defensie. ADIV rapporteert aan de Chef van Defensie (CHoD) en de minister van Defensie (MoD);

• VSSE (Veiligheid van de Staat) : de burgerlijke inlichtingendienst heeft als taak het verzamelen, analyseren en verwerken van informatie met het doel mogelijke bedreigingen voor de fundamentele belangen van de staat en zijn burgers te onderkennen, het uitvoeren van veiligheidsonderzoeken en het beschermen van personen;

— OCAD (Coördinatieorgaan voor de Dreigingsanalyse) maakt punctuele of strategische evaluaties over de terroristische en extremistische dreigingen in en tegen België. Het doet dit op basis van inlichtingen die het verkrijgt van de ondersteunende diensten. Het zijn de overheden die uiteindelijk de gepaste maatregelen zullen moeten treffen om een eventueel gedetecteerde dreiging af te wenden. Het orgaan staat onder het gezamenlijke gezag van de minister van Binnenlandse Zaken en de minister van Justitie. Dit coördinatieorgaan lijkt zich echter voornamelijk bezig te houden met conventionele dreigingen, dit terwijl we vandaag ook met heel andere uitdagingen worden geconfronteerd;

— het Vast Comité I is belast met de controle op de activiteiten en de werking van de Veiligheid van de Staat en van de algemene Dienst inlichting en veiligheid. De controle heeft betrekking op zowel de rechtmatigheid, de doelmatigheid als de coördinatie. Die controle leidt jaarlijks tot kritische rapporten. Zo werd in de jaarlijkse rapporten van het Comité I het gebrek aan een gecoördineerd federaal beleid met een toekomstvisie aangeklaagd.

— het ministerieel Comité voor Inlichtingen en Veiligheid : heeft eveneens de doelstelling de continuïteit van het veiligheidsbeleid te garanderen. Door het samenbrengen van de verschillende verantwoorde-

ainsi collaborer par-delà les limites de leurs compétences respectives. Le Comité définit les lignes de la politique à mettre en œuvre et intervient comme relais entre le Collège du renseignement et de la sécurité (CRS) et les services qui doivent concrétiser la politique de renseignement sur le terrain. Toutefois, le Comité émet plutôt des avis et considère la cyberdéfense comme un petit élément parmi d'autres dans une stratégie globale;

— CERT.be : la *Computer Emergency Response Team* donne des directives et des informations en matière de sécurité informatique et de prévention, et il élabore des solutions visant à limiter les répercussions des cyberincidents. Il emploie des ingénieurs de BELNET, le réseau national belge de la recherche, pour le compte de FedICT (SPF Technologie de l'Information et de la Communication) et collabore avec l'IBPT (Institut belge des services postaux et des télécommunications). Il a un rôle d'information et n'a pas la compétence de prendre des initiatives. Par ailleurs, il fait office d'interlocuteur pour les personnes, les entreprises ou les autorités qui sont la cible de cyberattaques;

— le CERT militaire : petite équipe de spécialistes en sécurité informatique qui aide la Défense à sécuriser les informations et les réseaux de communication (structure secrète);

— la FCCU : (*Federal Computer Crime Unit*) : service central faisant partie de la direction de la lutte contre la criminalité économique et financière de la police judiciaire fédérale, qui est le point de contact national et international pour la cybercriminalité, avec une permanence ving-quatre heures sur vingt-quatre. Ce service est chargé, au sein de la police fédérale, d'une mission de conception, de coordination et de contrôle dans le domaine de la cybercriminalité et des enquêtes légales informatiques;

— BELNIS : plateforme de coopération entre les services publics fédéraux, créée sur la base d'un Livre blanc commun de 2007 qui met l'accent sur une collaboration coordonnée dans le but d'identifier les infrastructures critiques. Cette initiative, qui n'est pas institutionnalisée, se présente comme un forum mensuel présidé par FedICT. Chaque mois, ce forum réunit les différentes instances actives dans le domaine de la sécurité informatique en vue de formuler des recommandations sur divers sujets concernant la sécurité informatique. En ce moment, la plateforme Belnis rédige aussi une note sur les priorités de la politique nationale de sécurité;

— FedICT : le Service public fédéral TIC se charge de l'élaboration et du suivi de l'e-gouvernement, et assiste les services publics fédéraux afin qu'ils améliorent leurs services aux citoyens, aux entreprises et aux fonctionnaires à l'aide des technologies de

lijke ministers wordt er over de bevoegdheidsdomeinen heen samengewerkt. Het comité zet de beleidslijnen uit en treedt op als tussenschakel tussen het College voor Inlichtingen en Veiligheid en de diensten die op het terrein het inlichtingenbeleid vorm moeten geven. Het Comité geeft echter veeleer advies en behandelt cyberdefensie slechts als één klein onderdeel van een grote strategie;

— CERT.be : het *Computer Emergency Response Team* biedt richtlijnen en informatie aan op gebied van informaticabeveiliging en preventie en werkt oplossingen uit met als doel de gevolgen van cyberincidenten te beperken. Het wordt bemand door ingenieurs van BELNET, het Belgisch nationaal onderzoeksnetwerk, in opdracht van FedICT (FOD Informatie en Communicatietechnologie) en het werkt samen met het BIPT (Belgisch instituut voor postdiensten en telecommunicatie). Het heeft een informatieve rol, maar niet de bevoegdheid om initiatief te nemen. Daarnaast fungeert het ook als aanspreekpunt voor personen, bedrijven of overheden die te maken krijgen met cyberaanvallen.

— de militaire CERT : een klein team van IT-veiligheidsspecialisten die Defensie ondersteunen in de beveiliging van informatie en de communicatienetwerken (geheime structuur);

— de FCCU (*Federal Computer Crime Unit*) : is als centrale dienst binnen de directie economische en financiële criminaliteit van de Federale gerechtelijke politie het nationaal en internationaal invalspunt voor cybercriminaliteit met een 24 uur-permanentie. Deze dienst is binnen de Federale politie belast met de opdracht van conceptie, coördinatie en controle in het domein van cybercriminaliteit en forensisch ICT-onderzoek;

— BELNIS : een samenwerking tussen de federale overheidsdiensten volgend uit een gecoördineerde *White Paper* uit 2007 waarin de nadruk ligt op een gecoördineerde samenwerking om de kritieke infrastructuren te identificeren. Dit initiatief is niet geïnstitutionaliseerd, maar is een maandelijks forum onder voorzitterschap van de FedICT. Hier komen maandelijks de verschillende instellingen bijeen die actief zijn op het vlak van informatieveiligheid om aanbevelingen uit te werken over verschillende onderwerpen in het kader van de informatieveiligheid. Het Belnisplatform houdt zich momenteel ook bezig met het opstellen van een nota over de prioriteiten van het nationaal veiligheidsbeleid;

— FedICT : de federale ICT-overheidsdienst die instaat voor de uitwerking en opvolging van e-government en bijstand geeft aan federale overheidsdiensten om hun dienstverlening aan burgers, ondernemingen en ambtenaren te verbeteren met behulp van

l'information et de la communication (TIC). Il dote aussi la plupart des SPF de systèmes de gestion et de sécurisation de leur réseau informatique (*e-ID*, par exemple);

— l'ANS : l'Autorité nationale de sécurité est compétente pour délivrer ou retirer les habilitations, les attestations et les avis de sécurité. Elle est composée de représentants de plusieurs autorités fédérales et est présidée par le SPF Affaires étrangères;

— SPF Justice : enquête et poursuites des auteurs de cyberincidents par la magistrature, plus précisément le collège des procureurs généraux, le ministère public et les tribunaux, sur la base des informations fournies par la FCCU, le CERT, FedICT et les services de renseignements. Le Service de la politique criminelle, qui est le service d'appui et de coordination du ministre, estb responsable de la politique criminelle en Belgique;

— l'IBPT : l'Institut belge des services postaux et des télécommunications, qui relève de la compétence du SPF Économie, est chargé d'effectuer des missions de régulation sur les marchés libéralisés des télécommunications et d'exercer une autorité souveraine dans certains domaines techniques spécifiques;

— Belnet : réseau relevant du SPF Politique scientifique, qui fournit une connexion internet à tous les services publics, ainsi qu'à des organismes publics et universitaires;

— B-CCENTRE : le *Belgian Cybercrime Centre of Excellence for Training, Research and Education* propose une plateforme de coordination et de coopération pour tous les acteurs concernés par la lutte contre la cybercriminalité en Belgique. Le B-CCENTRE mène des recherches interdisciplinaires et organise des formations et des séances de sensibilisation en matière de cybercriminalité (en collaboration avec la Justice (IFJ, INCC), l'Intérieur (FCCU), FedICT, l'IBPT, l'industrie et le monde universitaire (KUL)). Le B-CCENTRE collabore étroitement avec des centres du même type au sein de l'UE et est sponsorisé par les fonds ISEC de l'Union européenne;

— Organisations d'utilisateurs : les organisations ISSA, ISACA et BELTUG représentent environ trois cent cinquante professionnels de la sécurité informatique. Le CLUSIB était une association active, attachée à la FEB, dont l'objectif était d'améliorer la sécurité informatique dans les entreprises;

— Associations professionnelles : LSEC rassemble plus de cent organisations du secteur universitaire et de l'industrie de la sécurité, y compris trois mille professionnels de la sécurité en Belgique. L'organisation a pour but de sensibiliser davantage le marché et tente de développer des projets internationaux en

informatie- en communicatie technologie (ICT). De dienst voorziet het merendeel van de FOD's van beheer en beveiliging van hun informatienetwerk, zoals e-ID;

— de NVO (Nationale Veiligheidsoverheid) is de overheid die bevoegd is voor de afgifte of de intrekking van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. De NVO is samengesteld uit vertegenwoordigers van verschillende federale overheden onder leiding van de FOD Buitenlandse Zaken;

— de FOD Justitie : onderzoek en vervolging van de plegers van cyberincidenten door de magistratuur, meer specifiek het College van procureurs-generaal, het Openbaar Ministerie en de rechtbanken op basis van de informatie van de FCCU, CERT, FedICT en de inlichtingendiensten. De Dienst Strafrechtelijk Beleid (DSB) is de beleidsondersteunende- en coördinerende dienst van de minister en is verantwoordelijk voor eht strafrechtelijk beleid in België;

— het BIPT (Belgisch Instituut voor postdiensten en telecommunicatie) valt onder de bevoegdheid van de FOD Economie en is bevoegd voor het uitvoeren van regulerende opdrachten op de geliberaliseerde telecommunicatiemarkten en het uitoefenen van een soeverein gezag op specifieke technische gebieden;

— Belnet biedt alle overheidsdiensten, net als openbare en academische instellingen internettoegang aan, en valt onder de FOD Wetenschapsbeleid;

— BCCENTRE : *Belgian Cybercrime Centre of Excellence for Training, Research and Education* : biedt een coordinatie- en samenwerkingsplatform voor alle actoren die betrokken zijn bij het bestrijden van cybercriminaliteit in België. Het B-CCENTRE leidt interdisciplinair onderzoek en organiseert training en bewustmaking rond cybercrime (i.s.m. : Justitie (IGO, NICC), Binnenlandse Zaken (FCCU), FedICT en BIPT, industrie en academia (KUL)). B-CCENTRE werkt nauw samen met gelijkaardige centra in de EU en wordt gesponsord met EU ISEC-fondsen;

— Gebruikersorganisaties : ISSA, ISACA en BELTUG, vertegenwoordigen circa driehonderdvijftig *IT Security professionals*. BELCLIV was de actieve associatie geliëerd aan het VBO dat probeerde IT beveiliging in ondernemingen te verbeteren;

— Beroepsverenigingen : LSEC brengt meer dan honderd organisaties samen van de academische sector en de veiligheidsindustrie, inclusief drieduizend *security professionals* in België. De organisatie heeft de bedoeling om de bewustmaking in de markt te vergroten, en probeert internationale projecten in

Belgique en mettant à profit l'expertise locale. LSEC fait appel à des fonds européens, tels que SIGNATURE, FIRE, etc.;

— BISSI : la *Belgian Information Security Initiative* est un projet mis sur pied par l'ISACA, LSEC, la représentation belge ISO 27000, ISSA et des représentants du monde universitaire, afin de soutenir le développement d'une initiative belge en matière de sécurité informatique.

À l'heure actuelle, la Belgique est un des rares pays d'Europe occidentale qui ne disposent pas d'une stratégie en matière de sécurité informatique. La Belgique était déjà le dernier pays d'Europe occidentale à créer un CERT national et elle reste à la traîne aujourd'hui pour adopter une stratégie en matière de sécurité informatique, alors qu'elle héberge toute une série de grandes organisations internationales telles que la Commission européenne, le Conseil européen, le Parlement européen et l'OTAN.

La situation chez nos voisins

Aux Pays-Bas, le NCSC (*Nationaal Cyber Security Centrum*) qui est opérationnel depuis le 1er janvier 2012, élabore la cyberpolitique nationale. La CPNI (plateforme néerlandaise de cybersécurité), ainsi que le centre nodal d'informations Cybercrime, font partie du partenariat de recherche néerlandais public-privé TNO. Le partage des connaissances en est la pierre angulaire, l'objectif poursuivi étant de garantir la pérennité des organisations/entreprises et de protéger les sociétés néerlandaises des incidents malveillants et des menaces. Les bases en avaient été jetées six ans auparavant et le projet a pris forme en 2011 avec la création de la plateforme NICC dans le cadre de ce partenariat public-privé. Dans un avenir proche, la CPNI sera intégrée au NCSC.

En Allemagne, le BSI (*Bundes Sicherheitsinstitut*), avec à sa tête le ministre de l'Intérieur, est responsable de la cyberpolitique; en France, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) relève de la compétence du premier ministre; et au Royaume-Uni, le premier ministre a créé l'OCS (*Office of Cyber Security*) et la plateforme CPNI, et a défini une stratégie pour résoudre les problèmes de cybersécurité. Ces institutions ont donc pu développer leurs propres méthodes de travail et stratégies. Elles fournissent aux citoyens et aux organisations une plateforme de recherche et de développement, d'entraînement et de formation, de stratégies de protection et de simulations.

Mais surtout, elles sont en mesure de servir de trait d'union avec des plateformes internationales similaires et différents partenaires tant publics que privés. Ainsi, la Microsoft DCU (*Digital Crimes Unit*) a pour mission de rechercher dans chaque État membre les

België uit te bouwen met lokale expertise. LSEC gebruikt Europese fondsen van, onder andere, SIGNATURE, FIRE, enz.;

— BISSI : *Belgian Information Security Initiative* : initiatief van ISACA, LSEC, de Belgische ISO 27000 vertegenwoordiging, ISSA en academische vertegenwoordigers, die de ontwikkeling van een Belgisch Informatieveiligheidsinitiatief ondersteunen.

België is momenteel een van de weinige West-Europese landen die geen cyberveiligheidsstrategie hebben. Ons land was reeds het laatste land in West-Europa om een nationale CERT op te richten en blijft achterop bengelen inzake een informatiebeveiligingsstrategie terwijl het een hele reeks aan belangrijke internationale organisatie huisvest, zoals de Europese Commissie, de Europese Raad, het Europees Parlement en de NAVO.

Ondertussen in de buurlanden

In Nederland is het NCSC (Nationaal Cyber Security Centrum) sinds 1 januari 2012 operationeel bij het uitstippelen van het nationaal cyberbeleid. Het CPNI (Nederlandse platform voor cybersecurity) inclusief de informatiehub Cybercrime, maakt deel uit van het Nederlandse publiek-private researchorganisatie TNO. Centraal staat de *knowledge sharing*, teneinde de continuïteit van organisaties/ondernemingen en het Nederlandse « corp » tegen malicious incidenten en bedreigingen. De basis hiervan werd reeds zes jaar geleden gelegd en is daarna via het NICC-platform geformaliseerd geworden in 2011 in dit publiek-private partnerschap. In de nabije toekomst zal het CPNI ondergebracht worden bij het NCSC.

In Duitsland heeft de BSI (*Bundes Sicherheitsinstitut*) onder leiding van de minister van binnenlandse zaken de verantwoordelijkheid over het cyberbeleid, in Frankrijk ressorteert de ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*) onder de eerste minister, en in het Verenigd Koninkrijk heeft de eerste minister het OCS (*Office of Cyber Security*) het CPNI-platform opgericht en een strategie opgesteld om met cyberveiligheidsproblemen om te gaan. Deze instellingen hebben dan ook hun eigen werkmethodes en strategieën kunnen ontwikkelen. Ze voorzien de burgers en organisaties van een platform voor research en ontwikkeling, training en opleiding, beveiligingsstrategieën en simulaties.

Belangrijker nog, zij zijn ook in staat te functioneren als de tussenschakel met soortgelijke internationale platformen en partners, zowel publiek als privaat. Microsoft DCU (*Digital Crimes Unit*) bijvoorbeeld, heeft als opdracht de partners per lidstaat te

partenaires capables de relayer les informations pertinentes vers des partenaires dans les autres États membres.

Quels sont les besoins ?

Comme nous l'avons vu, l'actualité montre clairement que la Belgique ne peut plus se permettre d'avancer en ordre dispersé dans le cybermonde. Tout d'abord, il est temps de mener un débat sérieux sur la définition de la notion de « cyberattaque » et sur le rôle que les autorités belges entendent jouer sur l'ensemble de la cyberscène. Vont-elles se contenter d'informer (awareness raising) ou iront-elles plus loin, en procédant aussi à des contrôles, des certifications, des simulations, ou même à des contre-attaques ?

À l'instar du Comité R qui, à plusieurs reprises, s'est dit préoccupé par la politique de personnel défaillante des pouvoirs publics, les SPF sont eux-mêmes demandeurs de pouvoir attirer davantage de spécialistes. Mais en raison des difficultés budgétaires du gouvernement fédéral, la quasi-totalité des experts en TIC sont recrutés dans le secteur privé. Idéalement, le CERT et BELNET devraient pouvoir disposer d'une équipe de cyberréservistes travaillant dans le secteur privé, mais susceptibles de suivre régulièrement des formations auprès des autorités fédérales ou même supranationales, et de participer à des cyberexercices internationaux. Pour le moment, cette synergie est inexistante, mais il est clair que le secteur privé et le secteur public doivent travailler main dans la main s'ils veulent pouvoir apporter une réponse efficace aux cyberattaques. S'ils collaborent ensemble et instaurent un climat de confiance mutuelle, la cyberpolitique fédérale sera capable de résister à bien davantage de menaces du cyberespace.

La certification et l'homologation de systèmes informatiques occupent une place importante dans la lutte contre la cybercriminalité. Le Comité R considère « la faiblesse des moyens techniques de certification et d'homologation comme très problématique sur le plan de la sécurité informatique ». À cet égard, il recommande formellement de prévoir les moyens nécessaires pour que la certification et l'homologation des systèmes utilisés pour le traitement d'informations classifiées en Belgique puissent enfin se faire sans dépendre d'autorités et de services étrangers (1).

En outre, il est aussi primordial de faire preuve de prudence dans le choix des équipements techniques sécurisés nécessaires au traitement d'informations sensibles et classifiées, et de leurs fournisseurs. Les

(1) Comité R : « Conclusions et recommandations de l'enquête sur la manière dont les services belges de renseignement envisagent la nécessité de protéger les systèmes d'information contre des interceptions et cyberattaques d'origine étrangère (2011) ».

zoeken die in staat zijn om de relevante informatie door te spelen naar partners in de respectieve lidstaten.

Wat zijn de noodzaken ?

De actualiteit maakt zoals gezegd duidelijk dat België niet langer in gespreide slagorde de cyberwereld tegemoet kan treden. Zo moet nu in eerste instantie een ernstig debat plaatsvinden over hoe we een cyberaanval nu exact definiëren en welke rol de Belgische overheid in heel het cyberverhaal wil spelen. Gaat men louter informeren (*awareness raising*) of gaat men verder en dus ook controleren, certifiëren, simuleren of zelfs tot terugslaan ?

Net als het Comité I reeds meermaals haar bezorgdheid uitte over het tekortschietende personeelsbeleid van de overheid, zijn de FOD's zelf vragende partij om meer specialisten te kunnen aantrekken. Maar door de budgettaire krapte van de federale regering komen bijna alle ICT-experten in de privésector terecht. Idealiter zouden CERT en BELNET kunnen beschikken over een *pool* van cyberreservisten die in de privésector werken, maar geregeld bij de federale, of zelf supranationale, overheden opleidingen kunnen volgen en deelnemen aan internationale cyberoefeningen. Deze synergie is momenteel nog onbestaande, maar het is duidelijk dat zowel de privésector als de publieke sector elkaar nodig hebben om slagkrachtig te kunnen reageren op cyberaanvallen. Indien de publieke sector en de private sector samenwerken en wederzijds vertrouwen opbouwen zal het federaal cyberbeleid bestand zijn tegen veel meer gevaren die in cyberspace bestaan.

De certificatie en homologatie van computersystemen neemt een belangrijke plaats in in de strijd tegen cybercriminaliteit. Het Comité I stelt dat « het tekort aan technische certificatie- en homologatiemiddelen als een ernstig probleem wordt gezien ». Het maakt daarbij de formele aanbeveling om in de noodzakelijke middelen te voorzien opdat de certificatie en homologatie van de systemen die in België worden gebruikt om geclassicifeerde informatie te verwerken eindelijk kunnen plaatsvinden zonder dat men afhankelijk is van buitenlandse overheden en diensten (1).

Daarnaast is het ook zeer belangrijk dat de keuze van beveiligde technische uitrustingen en leveranciers voor de verwerking van gevoelige en geclassificeerde informatie op een voorzichtige manier gebeurt. De

(1) Comité I : « Besluiten en aanbevelingen van het onderzoek naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om de informatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland, 2011 ».

systèmes doivent faire l'objet d'une évaluation, d'une certification et d'une homologation dans le respect des normes européennes. Il convient d'identifier clairement les fournisseurs de pays tiers de réputation douteuse ou entretenant peut-être des liens avec certains services de renseignement étrangers.

Par ailleurs, il est nécessaire de transposer intégralement les recommandations du « Plan d'action pour lutter contre les cyberattaques » de l'Union européenne, ce qui signifie qu'il faut aussi envisager un premier exercice de simulation d'un incident de grande envergure à l'échelon national.

Il importe également d'élaborer un « *Disaster Recovery Plan* » réaliste, qui puisse servir de « plan B » au cas où les infrastructures cruciales et les autorités seraient victimes d'une cyberattaque. On se limite actuellement à des copier-coller, sans que les services publics fédéraux suivent une procédure commune.

Enfin, il semble aussi utile de continuer à informer correctement la population à propos des risques et nouveaux dangers de la cybercriminalité. Chaque année depuis 2004, les États-Unis et le Royaume-Uni font du mois d'octobre le « *Cyber Awareness Month* » (mois de sensibilisation à la cybersécurité) (1). Durant cette période, la population et les entreprises sont sensibilisées aux risques liés à la cybercriminalité et aux méthodes pour s'en protéger. Depuis lors, plusieurs pays européens ont adopté la même tradition et l'ENISA essaie de coordonner cette initiative à l'échelle européenne et de l'étendre chaque année à de nouveaux pays (2).

Une approche ciblée

Pour faire évoluer la collaboration entre le secteur public et le secteur privé dans le domaine de la sécurisation de l'information, il faudrait lancer des actions concrètes fondées sur les expériences d'autres pays et sur leurs modèles de référence, sans pour autant pécher par excès d'ambition et en avançant par étapes :

1. réunions mensuelles d'un groupe de travail public-privé;

2. activités publiques bimestrielles;

3. développement d'un système d'échange d'informations;

4. développement d'un centre public *Bot Free Belgium* chargé de traquer les réseaux de machines

(1) *http://www.staysafeonline.org/.*

(2) *http://www.enisa.europa.eu/media/press-releases/le-premier-mois-europeen-de-securite-cybernetique-commence-aujourd-hui-a-travers-toute-leurope.*

systemen moeten volgens Europese standaarden geëvalueerd, gecertifieerd en gehomologeerd worden. Leveranciers uit derde landen met een twijfelachtige reputatie of met eventuele banden met firma's van sommige buitenlandse inlichtingendiensten moeten duidelijk geïdentificeerd worden.

Daarnaast is er nood om de aanbevelingen uit het « Actieplan voor Cyberaanvallen » van de Europese Unie volledig om te zetten, dat wil zeggen dat er ook nagedacht moet worden over een eerste rampenoefening op nationaal niveau.

En er is eveneens nood aan een realistisch « *Disaster Recovery Plan* », zijnde een « plan B » indien de cruciale infrastructuren en de overheid het slachtoffer zou worden van een cyberaanval. Voorlopig blijft het bij knip-en-plakwerk zonder dat de federale overheidsdiensten een gemeenschappelijke handleiding volgen.

Ten slotte lijkt het ook nuttig om de bevolking gepast te blijven informeren over de risico's en nieuwe gevaren van internetcriminaliteit. In de Verenigde Staten en het Verenigd Koninkrijk wordt sinds 2004 elk jaar in oktober een zogenaamde « *Cyber Awareness Month* » gehouden (1) waar de bevolking en ondernemingen gesensibiliseerd worden over de risico's van internetcriminaliteit en de methodes om er zich tegen te beveiligen. Ondertussen hebben meerdere Europese landen dit gebruik overgenomen en probeert ENISA dit op Europees niveau te coördineren en elk jaar uit te breiden naar nieuwe landen (2).

Een gefocuste benadering

Opdat de publiek-private samenwerking zou evolueren bij de informatiebeveiliging, zouden enkele praktische stappen genomen kunnen worden, gebaseerd op de ervaringen van andere landen en hun referentiemodellen, maar tegelijk niet overambitieus en stap per stap :

1. maandelijkse bijeenkomsten van een publiek-private werkgroep;

2. tweemaandelijkse publieke activiteiten;

3. ontwikkeling van een informatiesysteem;

4. ontwikkeling van een *Bot Free Belgium* — centrum van de overheid om botnetten die zich op het

(1) *http://www.staysafeonline.org/.*

(2) *http://www.enisa.europa.eu/media/press-releases/the-first-european-cyber-security-month-starts-today-across-europe-be-aware-be-secure.*

zombies présents sur le territoire, de distribuer gratuitement un logiciel anti-botnet et de mettre en place une ligne d'assistance téléphonique.

1. Réunions mensuelles d'un groupe de travail public-privé

L'objectif de ces réunions est de mettre en place un partenariat sur la cybersécurité, où les représentants des autorités et d'institutions universitaires pourront rencontrer des experts de l'industrie, s'échanger des informations et discuter d'actions communes. Ce forum contribuera en même temps à l'établissement d'une relation de confiance et au partage de connaissances et d'une expertise. Le groupe de travail pourra aussi inviter des experts nationaux et internationaux à tenir des exposés. Idéalement, cet organe pourrait mener, à terme, à la création en Belgique d'un groupe d'expertise en matière de cybersécurité.

2. Activités publiques bimestrielles

Des particuliers et des entreprises seront invités à participer à cette plate-forme de discussion et pourront ainsi partager leurs expériences en matière de cybersécurité, mais aussi se tenir au courant des incidents enregistrés et des derniers développements.

3. Système d'échange d'informations

Il s'agit d'un élément capital pour lutter contre le cybercrime et améliorer la qualité de la cyberpolitique. Un tel système n'existe pas encore en Belgique et devrait systématiquement répondre à tous les standards de qualité. Le CERT dispose d'un système mondial de diffusion de l'information, mais cette plate-forme n'est utilisée ni par les entreprises ni par les institutions publiques, et elle ne dispose pas de plusieurs instruments spécifiques (*warning qualification and anonymisation*). Il faudra aussi que la Justice puisse profiter en parallèle des services de cette plate-forme, en complément à la sienne (la FCCU). Un système similaire existe déjà au Royaume-Uni : il s'agit du système WARP (*Warning, Advice and Reporting Points*), dont l'efficacité est reconnue, tout comme l'infrastructure NEISAS.

Dans le modèle WARP, des communautés de confiance se réunissent pour partager des informations spécifiques sur les menaces, risques et alertes susceptibles d'affecter les réseaux électroniques. Ce modèle a déjà fait ses preuves au Royaume-Uni et en Irlande et a le potentiel pour servir de réseau pour l'Europe entière.

Le système WARP est un canal d'information, une plate-forme de partage de données qui peut en même temps être reliée à une autre plate-forme de type « cellule de crise » (*incident response*). Grâce à lui, il

grondgebied bevinden op te sporen, door onder andere gratis anti-botnetsoftware te voorzien en een telefonische hulplijn open te stellen.

1. Maandelijkse bijeenkomst van een publiek-private werkgroep

De bedoeling is dat deze bijeenkomsten een partnerschap vormt inzake cyberveiligheid, waar de vertegenwoordigers van de overheid, van academische instellingen en experten van de industrie bij elkaar komen, om elkaar te informeren en gezamenlijke acties te bediscussiëren. Dit forum zal tegelijk bijdragen tot het uitbouwen van een vertrouwensrelatie en het delen van kennis en expertise. De werkgroep kan ook nationale en internationale experten uitnodigen als gastsprekers. Idealiter zou dit orgaan op termijn kunnen evolueren tot een *cybersecurity knowledge group* in België.

2. Een tweemaandelijkse publieke activiteit

Door particulieren en bedrijven te laten deelnemen aan dit discussieplatform kunnen ook zij hun ervaringen inzake het cyberbeleid delen, maar ook op de hoogte gehouden worden over incidenten en nieuwe ontwikkelingen

3. Information sharing system

Dit is een cruciaal element in de strijd tegen cybercrime en om de kwaliteit van het cyberbeleid te verbeteren. Een dergelijk systeem bestaat momenteel nog niet in België, en zou van systematische kwalitatieve aard moeten zijn. De CERT beschikt over een wereldwijd systeem om informatie te verspreiden, maar dit platform wordt noch door ondernemingen noch door overheidsinstellingen gebruikt en mist enkele specifieke instrumenten (*warning qualification and anonymisation*). Tegelijkertijd zal het ook noodzakelijk zijn dat justitie gebruik moeten kunnen maken van dit platform, naast haar eigen platform (FCCU). Een soortgelijk systeem bestaat reeds in het Verenigd Koninkrijk en is daar succesvol bevonden, namelijk het WARP-systeem (*Warning, Advice and Reporting Points*), net als de NEISAS-infrastructuur.

In het WARP-model komen vertrouwensgemeenschappen samen om specifieke informatie te delen over bedreigingen, risico's en waarschuwingen die elektronische netwerken kunnen bedreigen. Dit model heeft reeds haar verdienste kunnen bewijzen in het Verenigd Koninkrijk en in Ierland en heeft het potentieel om te fungeren als een netwerk voor heel Europa.

WARP is een informatiekanaal, een platform waarop men gegevens kan delen en dat tegelijk ook gelinkt is aan een platform voor *incident response*. Het zal hierdoor ook mogelijk zijn om kritieke infrastruc-

sera également possible d'identifier les infrastructures critiques à partir de la base (*bottom up*), et les experts nationaux en matière de sécurité seront en mesure de réagir rapidement en cas d'incident.

Nous disposerons ainsi d'informations détaillées sur toutes les menaces, risques et alertes, avec en même temps un échange de bonnes pratiques en vue de protéger au mieux ces réseaux électroniques, ce qui permettra de stimuler le dialogue entre les différents secteurs.

Protéger les infrastructures critiques représente un défi dont la clef de voûte est entre autres la sécurisation des informations : chercher une aiguille dans une meule de foin. Il convient tout d'abord d'identifier efficacement, parmi les millions de cyberincidents comptabilisés grossièrement, les cas réellement pertinents, après quoi il faut tenter d'établir des liens entre eux afin de déterminer les priorités absolues.

4. Création/développement du projet « Bot Free Belgium »

À l'instar de la plate-forme « *Botfrei.de* » créée en Allemagne, il y a également lieu d'instaurer en Belgique une plate-forme permettant de détecter et de neutraliser efficacement les *botnets* (réseaux de machines zombies). L'initiative allemande anti-botnet est née d'un projet de l'industrie allemande de l'Internet, lancé avec le soutien financier du ministère allemand de l'Intérieur et de l'agence fédérale de la sécurité de l'information.

Les fournisseurs d'accès internet (FAI) qui participent au projet identifient les ordinateurs infectés lorsqu'ils se connectent à des réseaux suspects de botnets à l'étranger. Le FAI avertit ensuite le propriétaire de l'ordinateur qu'il est peut-être victime d'un *botnet*, et le renvoie vers un site Web national d'information (*botfrei.de*) et un centre d'appels, où il pourra recevoir l'assistance nécessaire pour désinfecter sa machine. En Allemagne, dix FAI importants participent déjà à l'initiative, de même que les trois entreprises principales de logiciels antivirus : Symantec, Kaspersky et Avira.

L'idée est particulièrement intéressante parce que les initiatives anti-*botnet* actuelles visent seulement les serveurs C&C et ne prêtent aucune attention à l'utilisateur final infecté. La clé pour lutter contre les botnets est d'offrir un accompagnement personnalisé au propriétaire de la machine infectée, plutôt que de diffuser en masse des messages d'avertissement.

*
* *

turen te identificeren van onderuit (*bottom up*) en de nationale veiligheidsexperts worden in staat gesteld om snel te reageren in geval van incidenten.

Hierdoor zullen we beschikken over gedetailleerde informatie over bedreigingen, risico's en waarschuwingen samen met een uitwisseling van *good practice advise* om deze elektronische netwerken het best te beschermen, en kan de dialoog tussen de verschillende sectoren worden bevorderd.

Een deel van de uitdaging van de bescherming van kritieke infrastructuren is informatiebeveiliging : het vinden van een naald in een hooiberg. Van de miljoenen ruwe cyberincidenten moet op een efficiënte manier eerst de relevante incidenten geïdentificeerd worden, waarna men via het zoeken van verbanden de incidenten kan identificeren die de hoogste prioriteit hebben.

4. De oprichting/ontwikkeling van het « Bot Free Belgium » project

Naar voorbeeld van het in Duitsland opgerichte « *Botfrei.de* » platform moet er in België ook een platform opgericht worden om *botnets* efficiënt te kunnen opsporen en neutraliseren. Het Duitse antibotnet initiatief is ontstaan als een project van de Duitse internetindustrie met de financiële steun van het Duitse ministerie van binnenlandse zaken en het federale agentschap van informatieveiligheid.

De deelnemende Internet Service Providers (ISP's) identificeren een geïnfecteerde computer als die met verdachte botnet-netwerken in het buitenland contacten legt. Vervolgens waarschuwt de ISP de eigenaar dat zijn computer mogelijk het slachtoffer is van een *botnet* waarop de eigenaar naar een informatieve nationale website (*botfrei.de*) en een *callcenter* gestuurd wordt waar hij de nodige steun kan krijgen om de computer te desinfecteren. In Duitsland nemen reeds tien grote ISP's deel aan het initiatief, net als de drie grote antivirussoftwarebedrijven, Symantec, Kaspersky en Avira.

Dit is een bijzonder interessant idee omdat de huidige anti-*botnet*iniatieven enkel de C&C-servers viseren en geen aandacht schenken aan de geïnfecteerde eindgebruikers. De sleutel tot de bestrijding van botnets is de eigenaar van de geïnfecteerde machine gepersonaliseerde begeleiding geven in plaats van massaberichten naar iedereen te sturen.

Karl VANLOUWE.

*
* *

PROPOSITION DE RÉSOLUTION

Le Sénat,

A. renvoyant à l'enquête de contrôle réalisée en 2011 par le Comité permanent de contrôle des services de renseignement et de sécurité sur l'attitude des services belges de renseignement face à la nécessité de protéger les systèmes d'information et de communication contre des interceptions et des cyberattaques en provenance de l'étranger;

B. se ralliant aux constatations et conclusions de l'enquête de contrôle précitée;

C. considérant :

— que les menaces qui pèsent sur les systèmes d'information et de communication sont susceptibles de porter atteinte à la sécurité et aux intérêts fondamentaux de l'État;

— que le pays est très vulnérable aux attaques potentielles contre ses systèmes et réseaux vitaux d'information et de communication;

— que l'absence d'autorité compétente et de moyens techniques de certification et d'homologation est problématique tant pour la sécurité des systèmes d'information sensibles et/ou des systèmes utilisés pour le traitement d'informations classifiées que pour la position des entreprises belges dans ce secteur;

— qu'il est nécessaire de développer une stratégie fédérale globale de sécurisation des systèmes d'information et de communication;

D. se ralliant aux conclusions du Livre blanc « Pour une politique nationale de sécurité de l'information » élaboré par la plate-forme de concertation sur la sécurité de l'information;

E. renvoyant à la note rédigée par les experts de la plate-forme BELNIS en octobre 2011, à l'intention du formateur, au sujet des priorités d'une politique nationale de sécurité de l'information;

F. renvoyant au « *Belgium Country Report* » de mai 2011 de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA);

G. renvoyant à la note du *Belgian Cybercrime Centre of Excellence for Training, Research & Education* (B-CCENTRE) intitulée « *Cybercrime. The Belgian Landscape* » du 28 mars 2012;

H. considérant que l'Internet met 2,4 milliards de personnes en contact et crée de nouveaux moyens pour obtenir et diffuser des informations, interagir socialement, faciliter les transactions et collaborer à l'échelle internationale;

VOORSTEL VAN RESOLUTIE

De Senaat,

A. verwijzend naar het toezichtonderzoek uit 2011 dat het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten voerde naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om informatie- en communicatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland;

B. zich aansluitend bij de vaststellingen en conclusies van bovengenoemd toezichtonderzoek;

C. overwegende :

— dat de bedreigingen waaraan de informatie- en communicatiesystemen bloot staan afbreuk kunnen doen aan de veiligheid en de fundamentele belangen van de Staat;

— dat het land zeer kwetsbaar is voor aanvallen tegen zijn vitale informatie- en communicatiesystemen en -netwerken;

— dat het ontbreken van een bevoegde overheid en van de technische certificatie- en homologatiemiddelen problematisch is zowel voor de veiligheid van gevoelige informatiesystemen en/of systemen die gebruikt worden om geclassificeerde informatie te verwerken, als voor de positie van de Belgische bedrijven in die sector;

— dat er nood is aan een globale federale strategie voor de beveiliging van informatie- en communicatiesystemen;

D. zich scharend achter de conclusies van het « witboek voor een nationaal beleid voor de informatieveiligheid » zoals uitgewerkt door het overlegplatform voor informatieveiligheid,

E. verwijzend naar de nota van de experts gelieerd aan BELNIS « Nota aan de Formateur. Prioriteiten van een nationaal beleid voor informatieveiligheid » van oktober 2011;

F. verwijzend naar het « *Belgium Country Report* » van mei 2011 van het Europees Netwerk en Informatieveiligheidsagentschap ENISA;

G. verwijzend naar de nota van het *Belgian Cybercrime Centre of Excellence for Training, Research & Education* (BCCENTRE) « *Cybercrime. The Belgian Landscape* » van 28 maart 2012;

H. gelet op het feit dat het internet 2,4 miljard mensen met elkaar verbindt, en nieuwe manieren introduceert om over informatie te beschikken, te verspreiden, om sociaal te interageren, om transacties te vergemakkelijken en internationaal samen te werken;

I. considérant qu'en 2011, 44 % des entreprises belges auraient été victimes d'actes de cybercriminalité et que celle-ci est la deuxième forme la plus fréquente de criminalité économique dans notre pays;

J. considérant que la dépendance croissante à l'Internet implique aussi que l'interruption et/ou les manipulations de celui-ci peuvent avoir des conséquences de grande ampleur et particulièrement dangereuses;

K. considérant, d'une part, la tendance qui consiste à utiliser les TIC comme un instrument de domination dans les domaines politique, économique et militaire — en recourant au besoin à des stratégies offensives — et, d'autre part, la dimension géopolitique des cyberattaques;

L. vu la présence en Belgique d'importantes organisations internationales comme la Commission européenne, le Conseil européen et le Parlement européen, l'OTAN et Eurocontrol, et vu le fait que notre pays a, pour cette raison même, déjà été pris pour cible à plusieurs reprises par des cyberterroristes et qu'il le sera encore dans le futur;

M. renvoyant à l'évolution technologique continue qui se produit dans le monde de l'informatique où les autorités nationales ne jouent qu'un rôle secondaire;

N. considérant qu'en raison de la complexité de l'Internet dans lequel opèrent différents programmes, les solutions mises en œuvre aujourd'hui sont fragmentées et partielles et qu'il faudrait donc développer une approche holistique et globale du problème;

O. considérant que pour lutter efficacement contre la cybercriminalité, il faut instaurer une collaboration entre des acteurs aussi bien publics que privés, notamment des experts TIC, des universitaires, des magistrats, des fonctionnaires, des organisations internationales mais aussi des citoyens, comme l'a montré le *Cyber Europe Exercise 2010*;

P. renvoyant aux initiatives de la Commission européenne dans le domaine de la cybersécurité, notamment le septième programme-cadre (7e PC), le programme d'appui stratégique en matière de technologies de l'information et de la communication du programme-cadre pour la compétitivité et l'innovation (CIP ICT PSP) et l'Agenda numérique pour l'Europe 2010-2020;

Q. renvoyant aux recommandations du plan d'action PIIC (Communication relative à la protection des infrastructures d'information critiques) de la Commission européenne de 2009, qui vise à permettre aux États membres de renforcer les infrastructures vitales TIC et SCADA et ce, en collaboration avec la

I. gelet op het feit in 2011 vermoedelijk 44 % van de Belgische bedrijven het slachtoffer was van cybercriminaliteit en het de tweede meest voorkomende vorm van economische criminaliteit is in ons land;

J. gelet op het feit dat de groeiende afhankelijkheid van het internet eveneens betekent dat onderbreking en/of manipulaties van het internet grootschalige en bijzonder gevaarlijke gevolgen kunnen hebben;

K. verwijzend naar de trend om ICT als een middel te gebruiken om te overheersen op politiek, economisch en militair vlak, inclusief offensieve mogelijkheden, en de geopolitieke dimensie van cyberaanvallen;

L. gelet op de aanwezigheid van belangrijke internationale organisaties in België, zoals de Europese Commissie, de Europese Raad en het Europees Parlement, de NAVO en Eurocontrol en het feit dat ons land hierdoor reeds meermaals een doelwit is geweest en zal blijven voor cyberterroristen;

M. verwijzend naar de constante technologische evolutie die plaatsvindt in de informaticawereld waarin de nationale overheden een secundaire rol is toebedeeld;

N. overwegende dat door de complexiteit van het internet waarin verschillende programma's opereren er vandaag slechts sprake is van gefragmenteerde en gedeeltelijke oplossingen en daarom een holistische en alomvattende benadering van het probleem nodig is;

O. overwegende dat voor een succesvol bestrijden van cybercriminaliteit de medewerking vereist is van zowel publieke als private actoren, waaronder ICT-experten, academici, magistraten, ambtenaren, internationale organisaties maar ook burgers, zoals bleek uit de *Cyber Europe Exercise 2010*;

P. verwijzend naar de initiatieven van de Europese Commissie op het vlak van cyberveiligheid, waaronder FP7 (*7th Framework Programme*), CIP PSP (*Information Communication Technologies Policy Support Programme in Competitiveness and Innovation Framework Programme*) en de *Digital Agenda for Europe* 2010-2020;

Q. verwijzend naar de aanbevelingen van het CIIP-actieplan (*Communication on Critical Infrastructure Protection*) van de Europese Commissie uit 2009 dat de lidstaten moet leiden naar een versterking van de vitale ICT- en SCADA-infrastructuren in samenwerking met de Europese Commissie, andere lidstaten, de

Commission européenne, d'autres États membres, le secteur privé et l'ENISA;

R. renvoyant au livre blanc « Vers une Stratégie belge pour la sécurité de l'information » élaboré par des représentants du monde académique et d'associations professionnelles réunis au sein du groupe BISI et par LSEC, et considérant le rôle important que ceux-ci peuvent jouer en vue de favoriser la collaboration entre le secteur public et le secteur privé;

S. considérant que l'autorité fédérale est la mieux placée pour créer les forums nécessaires et prévoir des budgets en vue de prendre la direction du projet de cyberdéfense et qu'il lui revient de définir le rôle qu'elle doit y jouer, lequel peut consister à informer, contrôler, certifier, simuler et/ou encore protéger;

T. vu la création de la plate-forme de concertation BELNIS qui assure la coordination interdépartementale mensuelle de la cybersécurité des pouvoirs publics mais n'a pas de compétences opérationnelles suffisantes et n'est pas membre à titre permanent du Comité ministériel du renseignement et de la sécurité;

U. considérant que des particuliers et des exploitants de secteurs critiques prennent, d'initiative, des mesures en matière de logiciels en vue de défendre leurs intérêts et qu'ils accueilleraient favorablement une initiative de plus grande ampleur des pouvoirs publics;

V. vu la nécessité d'amener les acteurs concernés à débattre de l'élaboration d'un *Disaster Recovery Plan*, qui servira de « plan B » au cas où les infrastructures cruciales et les autorités seraient victimes d'une cyberattaque,

Demande au gouvernement :

1. d'élaborer et de mettre en œuvre rapidement une stratégie fédérale de sécurité des systèmes d'information et de communication;

2. de procéder à la création rapide d'une agence chargée de coordonner les activités visant à la sécurité des systèmes d'information et de communication;

3. de procéder à la désignation d'une autorité chargée de la certification et de l'homologation des systèmes sensibles et/ou utilisés pour le traitement d'informations classifiées en Belgique;

4. d'associer les services de renseignement belges (SGRS et VSSE) à la mise en place de cette agence et de cette autorité en raison de l'expérience et du savoir-faire dont ils disposent en cette matière;

5. de fournir les moyens nécessaires pour lutter contre la cybercriminalité et pour dispenser une

private sector en ENISA (Europees Netwerk en Informatieveiligheidsagentschap);

R. verwijzend naar het witboek van de academische- en beroepsverenigingen BISSI « Naar een Belgische Strategie voor Informatiebeveiliging » en LSEC en de belangrijke rol die zij kunnen spelen om bij te dragen tot de samenwerking tussen publieke en private sector;

S. overwegende dat de federale overheid het best geplaatst is om de nodige fora op te richten en budgetten te voorzien om de leiding van het cyberdefensieproject te nemen, om de rol te bepalen die de overheid hierin dient te spelen : informeren, controleren, certifiëren, simuleren of verdedigen ?

T. gelet op de oprichting van het BELNIS-overlegplatform dat de maandelijkse interdepartementale coördinatie van de cyberveiligheid van de overheid op zich neemt, maar onvoldoende operationele bevoegdheden bezit en ook geen permanent lid is van het ministerieel Comité voor Inlichtingen en Veiligheid;

U. verwijzend naar het feit dat particulieren en exploitanten van kritieke sectoren op eigen initiatief maatregelen inzake software nemen om hun belangen te verdedigen en een groter initiatief van de overheid zouden verwelkomen;

V. overwegende de noodzaak om de relevante actoren er toe te bewegen de discussie op te starten omtrent een zogenaamd *Disaster Recovery Plan*, zijnde een « plan B », indien die cruciale infrastructuren en de overheid het slachtoffer zou worden van een cyberaanval,

Vraagt de regering :

1. om snel een federale strategie voor de beveiliging van informatie- en communicatiesystemen uit te werken en in werking te stellen;

2. om snel werk te maken van de oprichting van een agentschap belast met de coördinatie van de activiteiten omtrent de veiligheid van informatie- en communicatiesystemen;

3. om over te gaan tot de aanwijzing van een overheid belast met de certificatie en homologatie van gevoelige systemen en/of systemen die in België gebruikt worden om geclassificeerde informatie te verwerken;

4. om de Belgische inlichtingendiensten (ADIV en VSSE) bij de creatie van dit agentschap en deze overheid te betrekken op grond van hun expertise en kennis van zaken in deze materie;

5. de middelen te verstrekken voor de bestrijding van cybercrime en het verzorgen van aangepaste

formation adéquate aux acteurs qui y sont confrontés, et d'affiner le cadre législatif en la matière;

6. de mettre à la disposition de l'agence précitée les moyens techniques et humains nécessaires pour que la certification et l'homologation des systèmes utilisés pour le traitement d'informations classifiées en Belgique puissent enfin se faire sans dépendre d'autorités et de services étrangers;

7. de créer un organe central chargé de rassembler toutes les informations relatives aux menaces visant notre réseau informatique et d'instaurer l'obligation de signaler à cet organe certains types de menaces;

8. d'associer également le secteur académique et le secteur privé au développement et à la mise en œuvre d'une politique de sécurité de l'information, car la confiance et la coopération permettent de créer une synergie fructueuse entre tous les acteurs concernés;

9. de garantir la pérennité du B-CCENTRE lorsque le financement du projet par la Commission européenne arrivera à son terme;

10. d'élaborer un *Disaster Recovery Plan* qui puisse être utilisé pour garantir la continuité du service critique, éventuellement par le biais de CERT sectoriels qui informeront le CERT national sur les incidents et pourront instaurer des mesures nationales et internationales par secteur d'infrastructures critiques, comme le prévoit le Programme européen de protection des infrastructures critiques (EPCIP) de la Commission européenne;

11. d'envisager de déconnecter des réseaux une partie de ses ordinateurs et infrastructures pilotées par ordinateur et de les faire fonctionner en réseaux fermés;

12. d'accorder plus d'attention à la cybersécurité en octroyant à un représentant du CERT, de BELNIS ou d'un nouvel organe à créer, un siège permanent au sein du Comité ministériel du renseignement et de la sécurité;

13. de donner suite à la déclaration d'intention adoptée par les pays du Benelux, qui souligne l'importance d'une coopération étroite entre les pouvoirs publics, l'industrie et le monde académique en matière de cybersécurité et qui permet de parler d'une seule voix sur la scène internationale (1), et d'envisager de l'ouvrir à d'autres États membres de l'Union européenne;

(1) *05/04/2011http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2011/04/05/benelux-ondertekenen-intentieverklaring-cyber-security.html.*

opleiding voor de actoren die met cybercrime geconfronteerd worden en het wetgevend kader om de problematiek aan te pakken te verfijnen;

6. om de noodzakelijke technische en menselijke middelen ter beschikking te stellen van dit agentschap opdat de certificatie en homologatie van de systemen die in België gebruikt worden om geclassificeerde informatie te verwerken uiteindelijk kan geschieden zonder daarvoor van buitenlandse overheden en diensten afhankelijk te zijn;

7. een centraal orgaan op te richten dat alle informatie verzamelt over de bedreigingen van ons computernetwerk en de meldplicht ten aanzien van het orgaan verplicht maakt voor bepaalde soorten bedreigingen;

8. eveneens de academische en private sector te betrekken in het ontwikkelen van een informatieveiligheidsbeleid en de implementatie ervan, omdat vertrouwen en samenwerking een goede wisselwerking tussen alle actoren een vruchtvolle synergie tussen alle betrokken actoren teweeg brengt;

9. het voortbestaan van het B-CCENTRE te garanderen na de stopzetting van de financiering van het project door de Europese Commissie;

10. een *Disaster Recovery Plan* uit te werken dat gebruikt kan worden om de continuïteit van de kritische dienstverlening te waarborgen, eventueel via sectoriële CERT's die de nationale CERT moeten informeren over incidenten en nationale en internationale maatregelen kunnen invoeren per sector van kritieke infrastructuren, zoals beschreven in EPCIP van de Europese Commissie;

11. te overwegen een deel van zijn computers en computergestuurde infrastructuur van de netwerken los te koppelen en in gesloten netwerken onder te brengen;

12. meer aandacht te geven aan cyberveiligheid door een afgevaardigde van CERT of BELNIS of een nieuw op te richten orgaan een permanente plaats te geven in het ministerieel Comité voor Inlichtingen en Veiligheid;

13. gebruik te maken van de intentieverklaring die gesloten werd tussen de Benelux-landen waarin men het belang van nauwe samenwerking inzake cyberproblemen tussen overheid, bedrijfsleven en wetenschap benadrukt, en met eenzelfde stem kan spreken op internationaal niveau (1) en te overwegen deze open te stellen voor andere EU-lidstaten;

(1) 05/04/2011http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2011/04/05/benelux-ondertekenen-intentieverklaring-cyber-security.html.

14. d'investir davantage dans des campagnes de sensibilisation auprès de la population et d'organiser chaque année pendant le mois d'octobre un « mois international de sensibilisation à la cybersécurité », comme l'ENISA incite à le faire et comme cela se fait depuis longtemps déjà dans plusieurs États membres de l'UE ainsi qu'aux États-Unis;

15. de collaborer activement avec les experts du CERT européen, de la CDMA et du Bureau des C3 de l'OTAN;

16. de s'engager activement dans la création du Centre européen de lutte contre la cybercriminalité (EC3), qui assurera depuis La Haye la coordination européenne de la politique de lutte contre la cybercriminalité à partir de 2013;

17. de plaider au sein du Conseil de l'Atlantique Nord (CAN) pour que l'article 5 du traité de l'OTAN soit réexaminé à la lumière du nouveau contexte global de la cyberdéfense.

5 novembre 2012.

14. om meer te investeren in bewustmakingscampagnes bij de bevolking en elk jaar tijdens de maand oktober een « *international cyber awareness month* » te houden, zoals wordt aangemoedigd door ENISA en sinds lang het geval is in meerdere EU-lidstaten en de Verenigde Staten;

15. actief samen te werken met de experten van de Europese CERT, de CDMA en C3 Board van de NAVO;

16. een actief engagement aan te gaan met betrekking tot de oprichting van het Europees Cybercrime Centrum (EC3) dat vanaf 2013 de Europese coördinatie van het cyberbeleid zal verzorgen vanuit Den Haag;

17. er in de Noord-Atlantische Raad (NAC) voor te pleiten om artikel 5 van het NAVO-verdrag opnieuw te bekijken in het licht van de nieuwe globale context van cyberdefensie.

5 november 2012.

Karl VANLOUWE.

124650 - I.P.M.