Le **centre national** pour la **cybersécurité**

Le chef d'orchestre tant attendu parviendra-t-il à accorder les violons ?

Depuis quelque temps, la cybersécurité est devenu un thème incontournable. In extremis, le gouvernement Di Rupo 1er est parvenu à créer un cybercentre national. Dans la présente contribution, Piet Pieters décrit le long et difficile processus de décision qui a permis d'aboutir à ce résultat. Au bout de plusieurs années de dissonances, de grands espoirs reposent sur ce nouveau chef d'orchestre.

INTRODUCTION

Le 25 avril 2014, le Conseil des ministres approuvait, en deuxième lecture, un projet d'arrêté royal « portant création du Centre pour la cybersécurité Belgique », en un mot le CCB[1].

Ceux qui liront ce texte fondateur en apprendront plus sur le statut du directeur et du directeur-adjoint de ce nouveau service placé sous l'autorité du Premier ministre, que sur les défis que l'institution devra affronter. Sa création n'arrive d'ailleurs pas trop tôt : ces dernières années se résument à une longue succession d'obstacles et d'indécisions. Mais voilà que, fin 2013, le dossier finalement accélère, probablement entraîné dans le sillage des affaires Snowden et de Belgacom.

Alors que fin mars 2013, il était encore question d'un énième groupe de travail[2], le gouvernement Di Rupo 1er faisait l'effort d'un rattrapage lors de la dernière Déclaration du gouvernement du 15 octobre 2013 : « *Enfin, la sécurité, c'est aussi la protection de la vie privée, de nos intérêts économiques et de l'appareil de l'État. C'est pour cette raison que nous accélérons la mise en œuvre de la stratégie de cybersécurité en mettant sur pied un centre belge de cybersécurité.* »[3]

LA CYBERMENACE : INVISIBLE MAIS RÉELLE

Virus, chevaux de Troie, vers informatiques, ... Nous les connaissons comme le revers de notre société d'information actuelle. Néanmoins, il reste à savoir si chaque utilisateur Internet, qu'il soit citoyen, entreprise ou autorité publique, est aussi toujours conscient des dangers. Le hameçonnage[4], l'ingénierie sociale et le canular informatique[5] sont déjà plus largement connus.

Néanmoins, sommes-nous tous suffisamment alertes face aux logiciels malveillants et autres logiciels espions ou « advanced persistent threats » moins évidents[6] ? Le spam dans notre boîte de réception saute aux yeux, comme une vitre brisée. Mais le cyber-voyou, mieux organisé, préfère se tapir plus longtemps, pour préparer son action ou en profiter le plus longtemps possible. Nous sommes plus que jamais dépendants de l'ICT et donc vulnérables à leurs failles. Pourtant, nous ne nous en apercevons peut-être même pas. Il en va de même pour le vol de secrets industriels, où il n'est plus nécessaire (et depuis longtemps!) de forcer une porte en acier. Et que dire des « hacktivistes » qui, derrière leur ordinateur, déstabilisent des processus d'entreprises, face auxquels les services de police traditionnels sont impuissants ? Les cyber-risques sont réels, les cybermenaces tout autant.

VULNÉRABILITÉS

Analysons brièvement trois vecteurs par lesquels peuvent se manifester les cybermenaces : les vulnérabilités liées au système, celles liées aux données et les vulnérabilités indirectes[7].

Attaques du réseau

Les attaques liées au système ciblent la prestation de services ou la gestion d'une organisation. Comme exemple extrême dans cette catégorie, citons la mise au jour du virus Stuxnet qui, en 2010, sabota les centrifugeuses de centrales nucléaires iraniennes. De cette même année, date aussi l'attaque DDoS d'Anonymous à l'encontre des sites Internet de Paypal et Mastercard[8],

(1) Le projet a dû ensuite être remis au Conseil d'État. Il n'avait pas encore été publié lors de la rédaction de cette contribution.

(2) *Questions et Réponses* Sénat 2012-2013, le 19 février 2013 (Question n° 5-8212 K. VANLOUWE) : « *Le Comité ministériel et le Collège du renseignement et de la sécurité suivront la mise en œuvre de la stratégie et plus particulièrement la création d'un Centre pour la cybersécurité en Belgique, qui serait l'autorité nationale compétente pour la cybersécurité. Un groupe de travail ad hoc sera mis en œuvre dans les prochaines semaines, afin d'appuyer techniquement le collège.* »

(3) www.lachambre.be ou www.presscenter.org.

(4) Par exemple, les courriels qui circulaient au mois d'avril 2012, provenant de l'adresse « fiscus@administration.be » et qui usurpaient le logo du SPF Finances. Ces courriels d'hameçonnage demandaient au récepteur de remplir ses données de carte de crédit sur leur site.

(5) L'ingénierie sociale est une technique de hackers utilisée pour exploiter la crédulité de l'utilisateur afin de lui soustraire des informations confidentielles concernant un certain système informatique qu'ils tentent d'infiltrer. Un canular informatique (ou hoax) est un faux message ou une fausse information qui a pour but d'être transmis le plus possible (www.cert.be).

(6) Les criminels tentent d'infiltrer discrètement des systèmes d'entreprise et d'y rester le plus longtemps possible pour voler un maximum : droits de propriété intellectuelle, secrets d'entreprise, informations sur des processus internes… (www.cert.be).

(7) Cybersecuritybeeld Pays-Bas, décembre 2011 (www.govcert.nl), juin 2012 et juin 2013 (www.ncsc.nl).

(8) Une attaque DDoS (*Distributed Denial of Service attack*) est un type d'attaque venant d'un botnet. Un grand nombre d'ordinateurs infectés, dirigé par un lieu de commande central, se connecte simultanément au serveur (web) d'une entreprise. Ce qui le rend temporairement non disponible ou le fait crasher (www.cert.be).

en raison de la décision de ces derniers de ne plus traiter les transactions de paiement de WikiLeaks. Au début de l'année 2012, le géant de l'acier ArcelorMittal eut la mauvaise surprise de devenir la première victime importante de hackers qui opèrent sous le nom d'« Anonymous Belgium ».

Il s'agit donc d'attaques qui ont un impact direct sur le fonctionnement d'un système ou d'un réseau, ce qui a d'ordinaire « l'avantage » qu'elles sont très visibles et qu'une réaction immédiate est possible.

Intrusions

Les intrusions liées aux données – qui sont bien plus difficiles à détecter – permettent à l'attaquant de s'introduire discrètement[9]. C'est le cas de phénomènes comme le cyber-espionnage électronique et la fraude de l'identité. Ainsi, en 2012, fut découvert Flame, un virus espion d'État, qui au Moyen-Orient passait son temps à voler des mots de passe et enregistrer des communications vocales en ligne. Le ministre belge des Affaires étrangères avoua dans la même période que son département avait été la cible de cyberattaques : « *Il n'est pas exclu que des informations assez sensibles aient été obtenues* »[10].

Le cambriolage de hackers auprès d'un éditeur de certificats de sécurité, DigiNotar, établi aux Pays-Bas, pendant l'été 2011, permit d'écouler de faux certificats de sécurité[11]. Et plus récemment, pendant les vacances de Pâques 2014, de nombreux responsables de sécurité furent secoués par la découverte d'une faille de sécurité au sein du protocole OpenSSL, surnommée « Heartbleed », pour laquelle on ne peut qu'espérer qu'entre-temps elle n'ait pas permis que des clés privées tombent dans de mauvaises mains. Enfin, dernièrement on a également découvert un nouveau hacking au SPF Affaires étrangères et un incident au SPF Economie.

Vulnérabilités indirectes

Pour finir, on entend par menaces ou risques indirects, soit des logiciels malveillants sans cible particulière qui s'auto-propagent le plus possible, soit les effets secondaires d'une attaque ciblée, par exemple parce qu'on est client dans une entreprise concernée ou qu'on a été connecté et infecté.

Pensons par exemple au persistant virus Sality.gen, capable de s'auto-propager et qui début 2012 a tenu en haleine le fisc belge pendant une semaine et demie.

MAL CONNU, MAL AIMÉ

Nous avons déjà signalé que la cybermenace est de nature plutôt invisible, du moins jusqu'à ce que les dégâts se manifestent ou que l'intrusion soit détectée. Admettons néanmoins que les départements ICT d'importantes entreprises et gouvernements connaissent bien les pièges du monde virtuel. Néanmoins, cette problématique est-elle perçue de la même façon par les topmanagers de ces organisations et les responsables politiques ?

La réponse à cette question semble dépendre de la mesure dans laquelle le traitement de données occupe ou non une place centrale dans le processus primaire de l'entreprise. Dans les domaines où c'est le cas, tels que la sécurité sociale et les finances, une certaine implication administrative et opérationnelle dans la cybersécurité semble exister. Dans d'autres domaines, il ne s'agirait plutôt (actuellement) que d'une lointaine préoccupation. C'est en tout cas la constatation du Conseil néerlandais « *Onderzoeksraad voor Veiligheid* », dans son rapport concernant la crise DigiNotar, mentionnée ci-dessus. Il fut ainsi déclaré que « *Le manque de connaissance en matière de cybersécurité au niveau de la direction, occasionne une transmission d'ordres faussée* »[12]. L'Inspection de la sécurité et de la Justice concluait néanmoins que la gestion de la situation de crise s'était déroulée de façon efficace[13].

COMITÉ R ET ACCORD DE GOUVERNEMENT

L'Accord de Gouvernement du 1er décembre 2011 annonçait que Di Rupo 1er rédigerait une politique de sécurité des réseaux et systèmes d'information et suivrait donc ainsi les recommandations du Comité R.

Vers la moitié de 2011, le Comité permanent R avait en effet présenté une enquête de surveillance à la Commission de suivi du Sénat, de laquelle il ressortait que les menaces qui pèsent sur les systèmes ICT belges sont susceptibles de porter atteinte à la sécurité et aux intérêts fondamentaux de l'État. « *Dans la mesure des moyens limités mis à leur disposition, les services de renseignement belges enquêtent aussi sur les attaques détectées sur les systèmes d'information des autorités, tant civiles, que militaires* », ajouta le Comité. « *Mais il s'agit encore d'une approche essentiellement défensive de détection, d'évaluation et de réaction. Force est cependant de constater que l'absence d'une politique fédérale globale en matière de sécurité de l'information (et de réelle autorité en la matière) entraîne une très grande vulnérabilité du pays en cas d'agression sur ses systèmes et réseaux vitaux d'information* »[14].

Cela amena le Comité R et la Commission de suivi à recommander au Gouvernement l'élaboration d'une stratégie fédérale en la matière, la création d'une agence chargée de coordonner les activités visant à la sécurité de l'information, ainsi que la mise à disposition des moyens nécessaires pour que la certification et l'homologation des systèmes utilisés pour le traitement d'informations classifiées en Belgique puissent se faire sans dépendre d'autorités et de services étrangers[15]. C'étaient bien ces recommandations que les négociateurs du gouvernement avaient en vue.

BELNIS

L'idée d'une autorité centrale était pourtant tout sauf nouvelle. L'appel pour la création d'une agence ou la désignation d'un service chargé de la sécurité d'information circulait déjà depuis plus d'une décennie. Déjà au début de l'an 2000, le Comité ministériel du renseignement et de la sécurité (CMRS) créa un groupe de travail, dirigé depuis 2001 par le Service général du renseignement et de la sécurité des forces armées (SGRS)[16], afin d'effectuer une recherche au sein des services et entités fédéraux existants pour évaluer s'il était possible d'élargir leur compétences concernant le cryptage et la protection de l'information. Néanmoins, aucun service ne répondant aux critères, le mandat fût reformulé,

(9) M. DE BRUYCKER, "Cyber Defence", *Revue Militaire Belge*, 2010, n° 1, 35-38.

(10) *Questions et Réponses* Sénat 2011-2012, 23 décembre 2011 (Question n° 5-4302 K. VANLOUWE).

(11) Cela alarma également les services belges, vu que l'attaquant revendiqua aussi avoir piraté la (seule) autorité de certification extérieure de l'État belge (GlobalSign). Nous avons tous une clé GlobalSign dans notre carte eID. X, "België voorbereid op rampscenario GlobalSign", *Private Veiligheid*, 2011, afl. 50, 5-6.

(12) De onderzoeksraad voor veiligheid, *Het DigiNotarincident. Waarom digitale veiligheid de bestuurstafel te weinig bereikt*, 28 juni 2012 (www.onderzoeksraad.nl).

(13) Inspectie veiligheid en justitie, *Evaluatie van de rijkscrisisorganisatie tijdens de DigiNotar-crisis*, 28 juni 2012 (www.ioov.nl).

(14) 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 (www.comiteri.be).

(15) Rapport d'activités 2011 (www.comiteri.be).

(16) Ceci fut en fait une deuxième tentative, après une première démarche – qui a échoué – début 1999, dans le cadre du « plan d'action Fedenet 1999 ». En septembre 2001, la présidence du groupe de travail passa de la Chancellerie du Premier ministre au SGRS, connu depuis sous le nom de groupe de travail (Pierre) MAURER.

Le centre pour la cybersécurité est créé fin 2013, probablement suite aux affaires Snowden et Belgacom

afin de permettre la création éventuelle d'une nouvelle agence. Mais cela s'avéra si onéreux que cette piste fut également abandonnée et le secrétaire d'État à l'informatisation de l'État[17] de l'époque fut prié de chercher une alternative. Cette alternative se concrétisa par la création, par le Conseil des ministres du 30 septembre 2005, de la plate-forme de concertation sur la sécurité de l'information, aujourd'hui couramment désignée par l'acronyme BelNIS (*Belgian Network Information Security*)[18].

Le sens ou le non-sens de BelNIS est discutable. La plate-forme de concertation ne dispose d'aucune mission opérationnelle et ne peut, ni se placer au-dessus des entités existantes, ni imposer ses recommandations aux institutions et autorités politiques dont proviennent ses membres. Par contre, les experts se rencontrent régulièrement et échangent de l'information. *A priori*, cela paraît être donc une bonne chose que BelNIS n'ait pas été supprimé lors de la création du CCB. En effet, elle est au contraire intégrée dans la nouvelle configuration en en confiant la présidence au CCB.

LE LIVRE BLANC

La première contribution à mettre au bénéfice de la plate-forme BelNIS fut le *Livre blanc « Pour une politique nationale de sécurité de l'information »* de mai 2007, actualisé en septembre 2010 sous la forme d'une note, à l'intention du formateur, au sujet des priorités d'une politique nationale de sécurité de l'information. En septembre 2008, des représentants du monde académique et d'associations professionnelles publiaient leur propre *Livre blanc « Vers une Stratégie belge pour la sécurité de l'information »*[19].

Chacun de ces textes reprend, à chaque fois, les mêmes priorités : la nécessité d'une définition de normes et d'une certification, ainsi que le besoin de coordination et de maintenance. L'importance d'une équipe nationale et bien encadrée, telle que le *Computer Emergency Response Team* (CERT) fut systématiquement soulignée.

CERT.BE

L'importance d'un CERT national n'était (et n'est) pas uniquement à l'ordre du jour en Belgique, mais partout en Europe. « *La sécurité est une responsabilité partagée par tous, par conséquent tous les États-membres doivent veiller à adopter des mesures* », argumentait la Commission. « *Les efforts qu'ils déploient contribuent collectivement à une approche européenne coordonnée visant à prévenir, détecter et atténuer toutes les formes de perturbations et attaques informatiques et à y apporter une réponse. À cet égard, les États membres devraient s'engager à améliorer l'état de préparation de l'UE en mettant en place un réseau de CERT nationales/gouvernementales opérationnelles d'ici à 2012* »[20].

La création du CERT belge se déroula plutôt facilement. Lorsque le gouvernement fédéral souhaita créer en 2009 cette sorte de « pompiers de l'Internet[21] », il a rapidement abouti à BELNET, le réseau national belge de recherche et de l'enseignement. BELNET disposait alors d'un propre CERT au bénéfice de ses utilisateurs. Sur l'ordre du SPF technologie de l'information et de la communication (Fedict) et sous son impulsion financière, ce CERT de BELNET se transforma à court terme en l'actuel CERT.be. L'institut belge des services postaux et des télécommunications (IBPT) participa également à ce processus, histoire d'éviter les conflits de compétences.

Tout cela se fit de façon assez informelle, jusqu'au moment où l'inspecteur des finances de Fedict remit l'une et l'autre chose en question, surtout lorsqu'il y eut à nouveau un gouvernement bénéficiant de la plénitude de compétences. Ce dernier résolut habilement la question en confiant, par arrêté royal, la gestion (financière) du CERT.be à Fedict. De plus, cela permit par la même occasion d'arrêter formellement une description de mission pour le CERT national, à savoir « *détecter, observer et analyser les problèmes de sécurité en ligne ainsi que d'informer en permanence les utilisateurs à ce sujet* »[22].

Les possibilités du CERT.be étaient et sont (trop) restreintes, cependant le service fonctionne(dumoins, lorsqu'il est sollicité). Ainsi, DNS.be constata, début avril 2011, jusqu'à six fois plus de trafic sur les « .be name servers » qu'en temps normal. Deux serveurs de DNS.be ont saturé durant environ quatre heures. L'analyse du CERT.be nous apprit qu'il ne s'agissait pas d'une attaque orchestrée par des cybercriminels, mais d'une action de spam mal exécutée par quelques botnets provenant principalement d'Europe de l'Est et d'Amérique du Sud. D'autres services CERT européens remarquèrent eux aussi des augmentations semblables dans leur pays. Une autre belle action du CERT belge fut le site *dns-ok.be* qui permettait à tous au cours du premier semestre 2012 de tester si son ordinateur était ou non infecté par le virus *DNSchanger*.

Les professionnels des technologies de l'information et de la communication des entreprises et des organisations qui sont confrontés à des cyberincidents peuvent en toute confiance s'adresser au CERT.be pour obtenir un avis professionnel. Depuis le 21 mai 2013, un site proposant des conseils de sécurité pour l'utilisation d'Internet est disponible pour le grand public[23]. L'arrêté royal du CCB maintient intact – et c'est heureux – les tâches du CERT national. Seule la gestion (financière) est transférée de Fedict au CCB.

(17) Compétent pour le SPF Technologie de l'information et de la communication (Fedict). Sous Di Rupo I, cette compétence est exercée par le secrétaire d'État à la fonction publique et à la modernisation des services publics.

(18) Les membres sont : Cellule stratégique du secrétaire d'État, Fedict, Crisis Emergency Response Team (CERT), Commission de la protection de la vie privée, Autorité nationale de sécurité (ANS), SGRS, Sûreté de l'État (VSSE), Organe de coordination pour l'analyse de la menace (OCAM), Institut belge des services postaux et des télécommunications (IBPT), Police fédérale (Federal Computer Crime Unit – FCCU), SPF économie, Banque carrefour de la sécurité sociale (BCSS), SPF Intérieur – Direction générale centre de crise (DGCC), Parquet fédéral, Collège des procureurs généraux, SPF affaires étrangères.

(19) Ce dernier est un document public, disponible sur www.lsec.be.

(20) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 31 mars 2011 relative à la protection des infrastructures d'information critiques « Réalisations et prochaines étapes : vers une cybersécurité mondiale », COM(2011), 163 final. Cette question européenne apparut déjà en d'autres termes dans la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative à la protection des infrastructures d'information critiques intitulée « Protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'état de préparation, la sécurité et la résilience », COM(2009) 149 final.

(21) Terme parfaitement approprié, utilisé par le ministre pour l'entreprise et la simplification, également compétent dans le domaine de l'informatisation de l'État (et donc Fedict). Un CERT n'est décidemment pas un service de police, et ne désire surtout pas l'être.

(22) Arrêté royal du 9 mai 2012 modifiant l'arrêté royal du 11 mai 2001 portant création du Service public fédéral technologie de l'information et de la communication, *M.B.*, 4 juin 2012.

(23) www.safeonweb.be.

STRATÉGIE NATIONALE

Si l'insertion mi-2012 du CERT national dans l'arrêté royal Fedict était une manœuvre intelligente du Gouvernement. D'un point politique cela signifiait aussi prendre le risque que l'on s'en contenterait jusqu'à la fin de la législature...

Car en effet, si Di Rupo 1er voulait réellement mettre sur pied une nouvelle institution, le Premier ministre ne l'a pas clairement confirmé à ce moment-là. Le Gouvernement est conscient, répondit-il fin janvier 2012 à une question parlementaire, que les initiatives et efforts déjà livrés ne sont pas encore suffisants ; il et réservera donc à cette problématique « *toute l'attention qu'elle mérite* ». « *Vu la situation budgétaire actuelle, le gouvernement sera toutefois aussi contraint de trouver un juste équilibre entre les défis budgétaires auxquels doivent faire face l'ensemble des services ou autorités concernés et l'élaboration d'une stratégie fédérale efficace en la matière, laquelle devra se traduire dans des objectifs opérationnels réalisables* »[24].

Mais fini de se lamenter ! Plus de 10 ans après le groupe de travail MAURER, c'était à nouveau le service de renseignement militaire SGRS qui – avec la bénédiction de la Chancellerie – prit la direction (de fait) d'un groupe de travail afin d'élaborer les propositions concrètes nécessaires (groupe de travail DE BRUYCKER)[25]. Durant l'été et l'automne 2012, un projet de « cyber security strategy » fut élaboré, comptant quatre chapitres :

- cybermenace ;
- objectifs stratégiques ;
- approche et domaines d'action ;
- moyens.

C'est surtout le dernier chapitre qui était intéressant, vu qu'il prévoyait explicitement la création d'un « Centre pour la cybersécurité en Belgique (CCSB) », budget et missions inclus et même un nom de domaine[26]. Ce dernier chapitre décrivait également le rôle de tous les autres services pertinents en relation avec la cybersécurité, ce qui éclairait immédiatement les compétences respectives de chacun.

Mais hélas, la partie concernant les moyens ne survécut pas aux consultations suivantes entre les cabinets. Le texte qui fut présenté au Conseil des ministres n'était donc ni plus ni moins que le texte préparé par le groupe de travail DE BRUYCKER, le quatrième chapitre en moins.

Et en effet, le 21 décembre le Conseil des ministres chargeait le Premier ministre de s'occuper de la « coordination de l'exécution » de la cyberstratégie belge. Le communiqué de presse officiel nous appris à ce sujet que : « *Le Premier ministre, Elio Di Rupo, a présenté au Conseil des ministres un projet de cyberstratégie belge. Conformément à l'accord du gouvernement, ce projet vise à pourvoir la Belgique d'une stratégie fédérale de sécurité des réseaux et systèmes d'information, dans le respect de la vie privée. La cyberstratégie belge a pour objectif d'identifier la cybermenace, d'améliorer la sécurité et de pouvoir réagir aux incidents. Ce projet est né du travail de la plateforme de concertation pour la sécurité de l'information BelNIS (Belgian Network Information Security).* »

Et puis plus rien..., jusqu'à l'affaire Belgacom et les révélations sur les activités des services de renseignement américain NSA et britannique GCHQ. Elles menèrent au passage suivant dans la note de politique générale du SPF Chancellerie du Premier ministre du 6 novembre 2013 : « *Le gouvernement fédéral a décidé d'accélérer la mise en œuvre de sa stratégie de cybersécurité et d'y investir 10 millions d'euros en 2014. (...) Les moyens budgétaires serviront donc, d'une part, à la création du Centre de cybersécurité belge et, d'autre part, à renforcer en personnel des services compétents en cette matière* »[27]. Six mois plus tard et peu après la découverte du nouveau piratage aux Affaires étrangères, la véritable répartition et la destination concrète de ces moyens eu lieu lors du Conseil des ministres (électronique) du 13 mai 2014.

> Le chapitre consacré au financement du centre pour la cybercriminalité en Belgique n'a pas survécu aux consultations intercabinets

UN CHEF D'ORCHESTRE

Un propos célèbre du Lieutenant-colonel Miguel De Bruycker du SGRS disait que notre pays disposait déjà d'un orchestre modeste, mais qu'il avait surtout rapidement besoin d'un chef d'orchestre. C'était donc cet objectif que son groupe de travail se chargeât de définir et qui fut finalement repris, bien qu'en deux temps, par le Gouvernement.

La tâche du CCB consiste à élaborer des actions politiques, méthodologiques et coordinatrices, qui soient aussi bien préventives que réactives : créer des standards, des normes de sécurité et des directives pour les systèmes d'information des services publics, assurer l'exécution d'obligations et représentations internationales, formuler des propos pour de nouvelles réglementations, coordonner tous les partenaires publics et privés – y compris scientifiques – concernés, ainsi que coordonner l'évaluation et la certification des systèmes d'information et de communication, y compris sensibiliser les utilisateurs de tels systèmes. Le CCB assure également la gestion de crise lors de cyberincidents, en collaboration avec le Centre gouvernemental de coordination et de crise. Le CCB adressera ses rapports au Premier ministre, également Président du Comité ministériel du renseignement et de la sécurité, qui devra aussi déterminer les lignes d'action stratégiques dans ce domaine de sécurité spécifique.

Musique maestro.

(24) *Questions et réponses*, Sénat 2011-2012, 23 décembre 2011 (Question n° 5-4291 K.VANLOUWE, réponse fournie le 26 janvier 2012).

(25) « De fait », vu que le groupe de travail formel fut créé au sein de BelNIS. Outre le SGRS, le FCCU, Fedict, Cert.be, l'IBPT, la DGCC et l'ANS y participèrent aussi.

(26) Centre pour cyber sécurité Belgique, Centre for Cyber Security Belgium, Centrum voor cyber security België (www.ccsb.be).

(27) *Doc. parl.* Chambre 2013-2014, 3096/009.

Piet Pieters
Directeur de l'infrastructure critique,
Centre gouvernemental de coordination et de crise
L'auteur écrit uniquement en son propre nom.