DOC 54 **0257/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

BUITENGEWONE ZITTING 2014

16 september 2014

VOORSTEL VAN RESOLUTIE

over de aanscherping van de cyberveiligheid in België

(ingediend door de heer Georges Dallemagne)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

SESSION EXTRAORDINAIRE 2014

16 septembre 2014

PROPOSITION DE RÉSOLUTION

visant à renforcer la *cyber*sécurité en Belgique

(déposée par M. Georges Dallemagne)

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
Open Vld	:	*Open Vlaamse liberalen en democraten*
sp.a	:	*socialistische partij anders*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
cdH	:	*centre démocrate Humaniste*
VB	:	*Vlaams Belang*
PTB-GO!	:	*Parti du Travail de Belgique – Gauche d'Ouverture*
FDF	:	*Fédéralistes Démocrates Francophones*
PP	:	*Parti Populaire*

Afkortingen bij de nummering van de publicaties:

DOC 54 0000/000:	*Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag*
CRABV:	*Beknopt Verslag*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig papier)*

Abréviations dans la numérotation des publications:

DOC 54 0000/000:	*Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral*
CRABV:	*Compte Rendu Analytique*
CRIV:	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers

Bestellingen:
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.dekamer.be
e-mail : publicaties@dekamer.be

De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier

Publications officielles éditées par la Chambre des représentants

Commandes:
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.lachambre.be
courriel : publications@lachambre.be

Les publications sont imprimées exclusivement sur du papier certifié FSC

TOELICHTING

DAMES EN HEREN,

Dit voorstel van resolutie neemt ten dele de tekst over van voorstel van resolutie DOC 53-2918/001.

De informatie- en communicatietechnologie (ICT) overheerst onze moderne samenleving. Zonder ICT kan de maatschappij niet langer doeltreffend functioneren. De keerzijde van dat alles is echter dat die ICT zeer kwetsbaar is. Dagelijks horen of lezen we berichten over informaticasystemen en digitale databanken die worden gehackt en/of aangevallen. Daarbij moeten we wel bedenken dat het merendeel van die cyberveiligheidsincidenten niet eens wordt opgemerkt of gerapporteerd. Dat blijkt althans uit een rapport van het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa). Dagelijks zouden zowat 200 miljard besmette mails (*spam*) worden verzonden; elke seconde zouden 46 nepcodes worden gecreëerd met de bedoeling onlinegegevens te stelen; jaarlijks zou de cybercriminaliteit 292 miljard euro aan inkomsten doen verloren gaan en dagelijks zou ze 1 miljoen mensen treffen.

De cyberbeveiliging bestrijkt heel wat aangelegenheden. Bedoeling is weerwerk te bieden aan alle mogelijke bedreigingen, gaande van een crimineel gebruik van het internet (cybercriminaliteit) tot aanvallen op informaticanetwerken en de gevolgen daarvan op militair en strategisch vlak (cyberdefensie en beveiliging van de informatiesystemen).

Een cyberaanval is een kwaadwillige poging om informaticasystemen te treffen, bijvoorbeeld om gegevens te stelen, om de normale werking van de informaticasystemen te verstoren, te ontregelen of teniet te doen, om de controle over informaticaprocessen in handen te krijgen of om de authentificatiesystemen te verschalken en aldus onwettige handelingen te kunnen verrichten. Door van op afstand de controle over te nemen op computers, krijgt men toegang tot alle gegevens op de harde schijf, alsook tot alle inkomende en uitgaande gegevens. Zelfs de webcam van de gehackte computers kan van op afstand worden gestuurd, waardoor de indringers kunnen zien en horen wat er in de omgeving van een aangeschakelde computer gebeurt.

Het aantal cyberaanvallen neemt hand over hand toe. Denken we maar aan de aanval tegen Estland in 2008, aan de inzet van het Stuxnet-virus tegen de Iraanse nucleaire installaties in 2010 (die ook andere landen, zoals Indië, besmette), of nog aan de cyberaanvallen die het Chinese leger uitvoert. Een ander voorbeeld is

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

La présente proposition de résolution reprend en partie le texte de la proposition de résolution DOC 53 2918/001.

Les technologies de l'information et de la communication (TIC) dominent nos sociétés modernes. Indispensables à une société performante, elles sont également très vulnérables. Des intrusions et des attaques sur les systèmes informatiques ou les bases de données digitales sont mentionnées quotidiennement. Et pourtant la plupart des incidents de *cyber*sécurité ne sont ni détectés ni rapportés, comme le signale un rapport de l'Agence européenne chargée de la sécurité et des réseaux de l'information. Il y aurait deux cent milliards de courriels pourris (*spams*) envoyés chaque jour, quarante-six codes malveillants créés chaque seconde afin de voler des données en ligne, 292 milliards d'euros de revenus annuels perdus et un million de victimes chaque jour.

La *cyber*sécurité est un domaine très vaste qui vise à répondre à toutes ces menaces, qui vont de l'utilisation criminelle d'internet (*cyber*criminalité) aux attaques contre les réseaux informatiques et leurs conséquences militaires et stratégiques (*cyber*défense et sécurité des systèmes d'information).

Une *cyber*attaque est une tentative d'atteinte à des systèmes informatiques réalisée dans un but malveillant. Elle peut avoir comme objectif de voler des données, de détruire, endommager ou altérer le fonctionnement normal des dispositifs informatiques, de prendre le contrôle de processus informatique ou de tromper les dispositifs d'authentification pour effectuer des opérations illégitimes. La prise de contrôle d'ordinateurs à distance permet d'avoir accès à toutes les informations du disque dur ainsi qu'à tous les flux entrants et sortants. Même la webcam située sur les PC peut être actionnée à distance et permet à un intrus de voir et d'entendre ce qui se passe autour d'un ordinateur allumé.

Les cas de *cyber*attaques se multiplient, de l'attaque contre l'Estonie en 2008 à l'utilisation du virus Stuxnet contre les installations nucléaires iraniennes en 2010 (lequel a aussi infecté d'autres pays, comme l'Inde) ou encore les *cyber*attaques menées par l'armée chinoise. On rappellera aussi l'attaque massive dont a été victime

de massale aanval die Zuid-Korea op 20 maart 2013 te verwerken kreeg. Wat België betreft, kan worden verwezen naar de recente aanvallen tegen Belgacom en de FOD Buitenlandse Zaken. Het aantal gerichte cyberaanvallen is in 2013 wereldwijd zowat verdubbeld, zo blijkt uit het jaarverslag van het Amerikaanse bedrijf Symantec. Terwijl dat aantal tussen 2011 en 2012 met 42% was toegenomen, werden alleen al voor 2013 91% meer aanvallen genoteerd. Verschillende ministers van Defensie van OESO-lidstaten beschouwen cyberaanvallen en terrorisme als even gevaarlijk. Zo komt cyberbeveiliging ruimschoots aan bod in het recente Franse *Livre blanc sur la défense et la sécurité nationale*. Een ander voorbeeld is uiteraard het elektronisch bewakingsprogramma PRISM.

De indiener van dit wetsvoorstel vindt dat de vitale infrastructuur van ons land gevaar loopt. Het is immers niet ondenkbeeldig dat de controle erop van op afstand wordt overgenomen of dat die infrastructuur wordt vernietigd. Tal van bronnen maken melding van geregelde aanvallen of inbraken die zijn gericht tegen overheidsinstellingen of privéondernemingen in België. Enkele maanden geleden nog werd België in het Amerikaanse Mendiant-rapport genoemd als een doelwit van cyberaanvallen. Een Belgisch militair expert beweert dan weer dat de kritieke infrastructuur van ons land (energie, transport, telecommunicatie, ruimtevaart, biochemie, landsverdediging, buitenlandse zaken enzovoort) haast dagelijks met cyberaanvallen te maken krijgt. De detectie van dergelijke aanvallen is er fors op vooruitgegaan, maar daar staat tegenover dat de particuliere gebruikers en de ondernemingen, inzonderheid de kmo's, de bedreiging danig onderschatten en over weinig middelen beschikken om ze te detecteren, laat staan te pareren.

Cybercriminaliteit kost de Belgische economie vandaag al handenvol geld, al valt het exacte bedrag moeilijk te becijferen. De kostprijs zou echter torenhoog kunnen oplopen als de regering geen werk maakt van drastische en aan de omvang van het risico aangepaste maatregelen.

Op Europees vlak hebben de Europese Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid in februari 2013 een EU-strategie voor cyberbeveiliging voorgesteld, onder het motto: "een open, veilige en beveiligde cyberspace". Tevens werd een voorstel voor een richtlijn ingediend, houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.

la Corée du Sud le 20 mars 2013. En Belgique, nous citerons les récentes attaques dont ont été victimes l'entreprise Belgacom et le SPF Affaires étrangères. Les *cyber*attaques ciblées ont pratiquement doublées dans le monde en 2013, selon le rapport annuel de la société américaine Symantec. Alors qu'elles avaient progressé de 42 % entre 2011 et 2012, on enregistre une croissance de 91 % pour la seule année 2013. Plusieurs ministres de la Défense de pays membres de l'OCDE considèrent les *cyber*attaques comme un risque du même niveau que le terrorisme. Par exemple, le Livre blanc de la Défense française paru récemment mentionne abondamment la *cyber*sécurité, sans parler du programme de surveillance PRISM.

L'auteur de la présente proposition de résolution estime que la capacité de prise de contrôle à distance ou de destruction d'infrastructures vitales pour notre pays est en jeu. De nombreuses sources font état d'attaques ou d'intrusions régulières dont seraient victimes des départements publics ou des entreprises privées en Belgique. Il y a quelques mois, le rapport américain Mendiant mentionnait la Belgique comme cible de *cyber*attaques. Selon un expert militaire belge, les infrastructures critiques en Belgique (énergie, transport, télécom, aérospatial, biochimie, défense, affaires étrangères…) feraient l'objet de *cyber*attaques de manière quasi quotidienne. La détection s'est nettement améliorée, même s'il faut reconnaître que les utilisateurs particuliers et les entreprises, notamment les PME, sous-estiment gravement la menace et qu'ils ne disposent que de peu de moyens pour la détecter et encore moins pour la contrer.

Le coût pour l'économie belge est déjà substantiel, même s'il est difficilement chiffrable. Il deviendra vite exorbitant si le gouvernement ne prend pas des mesures drastiques à la mesure des enjeux.

Au niveau européen, la Commission européenne et la Haute représentante de l'UE pour les affaires étrangères et la politique de sécurité ont présenté en février 2013 une "Stratégie de *cyber*sécurité de l'UE: un *cyber*espace ouvert, sûr et sécurisé" ainsi qu'une proposition de directive concernant "des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (SRI)".

Dat voorstel voor een richtlijn strekt ertoe de netwerk- en informatiebeveiliging (NIB) in de EU grondig te herzien. Het behelst bijvoorbeeld de verplichting dat overal dezelfde regels zouden gelden en dat de bestaande leemten in de wetgeving worden aangevuld. Meer concreet wordt met het voorstel voor een richtlijn het volgende beoogd:

1° alle EU-lidstaten verplichten te voorzien in "een minimale nationale capaciteit", door "voor NIB bevoegde autoriteiten aan te wijzen, computercrisisteams op te zetten (*Computer Emergency Response Teams* — CERT's) en nationale NIB-strategieën en -samenwerkingsplannen vast te stellen";

2° ervoor zorgen dat "de nationale bevoegde autoriteiten samenwerken in het kader van een netwerk dat beveiligde en doeltreffende coördinatie, inclusief gecoördineerde informatie-uitwisseling, alsmede opsporing en reactie op EU-niveau mogelijk maakt". De lidstaten moeten via dit netwerk, en met de permanente steun van het Enisa, informatie uitwisselen en samenwerken om NIB-dreigingen en -incidenten aan te pakken en er aldus voor te zorgen dat de richtlijn in de hele EU op convergente wijze wordt toegepast.

3° bewerkstelligen dat "een cultuur van risicobeheer ingang vindt en dat de particuliere en de openbare sector onderling informatie uitwisselen". Zowel bedrijven uit de kritieke sectoren (banken, effectenbeurzen, energieproducenten, -transporteurs en -distributeurs, transporteurs via de lucht, het spoor of over zee, gezondheidssector, internetdienstverlening) als de overheden zouden ertoe worden verplicht:

— "de risico's waarmee zij worden geconfronteerd, te beoordelen, passende en evenredige maatregelen te nemen om NIB te waarborgen", en

— "aan de bevoegde autoriteiten verslag uit te brengen over incidenten die hun netwerken en informatiesystemen ernstig in gevaar brengen en de continuïteit van kritieke diensten en de levering van goederen significant beïnvloeden".

Op Belgisch niveau heeft de eerste minister op 21 december 2012 een *cyber security strategy* voorgesteld, die België moet voorzien van een federale strategie ter beveiliging van de informatienetwerken en -systemen, met inachtneming van de persoonlijke levenssfeer. In het document worden de drie strategische doelstellingen toegelicht die de *cyber*beveiliging in België moeten waarborgen: de *cyber*dreiging identificeren, de veiligheid verbeteren en het reactievermogen versnellen.

La proposition de directive vise à revoir en profondeur la manière dont la SRI est abordée dans l'UE. Elle prévoit d'imposer des obligations réglementaires afin que les règles soient les mêmes partout et que les lacunes législatives existantes puissent être comblées. Les objectifs de la directive proposée sont les suivants:

1° exiger de tous les États membres qu'ils mettent en place un minimum de moyens au niveau national en établissant des autorités compétentes dans le domaine de la SRI, en mettant sur pied des équipes d'intervention en cas d'urgence informatique (CERT) et en adoptant des stratégies et des plans de coopération nationaux en matière de SRI;

2° prévoir que les autorités compétentes coopèrent au sein d'un réseau permettant une coordination sûre et efficace, un échange coordonné d'informations ainsi que la détection et l'intervention au niveau de l'UE. Au sein de ce réseau, les États membres échangeraient des informations et coopéreraient avec le concours permanent de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour faire face aux menaces et incidents en matière de SRI et pour faciliter une application convergente de la directive dans toute l'UE;

3° créer une culture de gestion des risques et favoriser le partage d'informations entre le secteur privé et le secteur public. À cet égard, les entreprises des secteurs critiques — à savoir les secteurs de la banque, des bourses de valeurs, de la production, du transport et de la distribution d'énergie, des transports (aérien, ferroviaire, maritime), de la santé, des services internet — ainsi que les administrations publiques seraient tenues:

— d'évaluer les risques qu'elles courent et d'adopter des mesures appropriées et proportionnées pour garantir la SRI, et

— de signaler aux autorités compétentes tout incident de nature à compromettre sérieusement leurs réseaux et systèmes informatiques et ayant un impact significatif sur la continuité des services critiques et la fourniture des biens.

Au niveau belge, la "*cyber security strategy*" qui vise à pourvoir la Belgique d'une stratégie fédérale de sécurité des réseaux et systèmes d'information, dans le respect de la vie privée, a été présentée par le premier ministre le 21 décembre 2012. Le document présente les trois objectifs stratégiques pour garantir la *cyber*sécurité en Belgique, à savoir: identifier la *cyber*menace, améliorer la sécurité et pouvoir réagir aux incidents. Ce projet est né du travail de la plate-forme de concertation pour

Dit project vloeit voort uit het werk van BelNIS (*Belgian Network Information Security*), een overlegplatform voor informatieveiligheid. BelNIS is het enige forum waarop de mensen uit het veld elkaar kunnen ontmoeten. De leden van BelNIS zijn vertegenwoordigers van de volgende overheidsspelers: de beleidscel van de minister/staatssecretaris die bevoegd is voor de informatisering van de overheid, de Commissie voor de bescherming van de persoonlijke levenssfeer, de Nationale Veiligheidsoverheid (NVO), de Kruispuntbank van de Sociale Zekerheid, het Belgisch Instituut voor postdiensten en telecommunicatie, de *Federal Computer Crime Unit*, de Algemene Dienst inlichting en veiligheid (ministerie van Defensie), de FOD Economie, Fedict, het Crisiscentrum (FOD Binnenlandse Zaken), de Veiligheid van de Staat, de POD Wetenschapsbeleid (waaronder het *Computer Security Incident Response Team* (CERT.be) ressorteert), de FOD Justitie, het Federaal Parket, het College van procureurs-generaal, het OCAD-OCAM en de FOD Buitenlandse Zaken. BelNIS kan zo nodig externe deskundigen bij zijn werkzaamheden betrekken en komt eenmaal per maand samen.

Het platform mag dan al de verdienste hebben te bestaan en de verschillende betrokken overheidsspelers met elkaar te doen samenwerken, dat neemt niet weg dat het geen eigen middelen heeft en dat niemand er echt aan het hoofd van staat. Overigens ontbeert het platform ook maar enige wettelijke basis die de taken en actiemiddelen ervan vastlegt. Om die redenen moet het platform wettelijk worden verankerd, door het om te vormen tot een Centrum voor cyberbeveiliging in België (CCB), dat de nodige specifieke middelen krijgt om zijn taak naar behoren te kunnen uitvoeren. Het Centrum zou moeten zorgen voor een betere sturing en opvolging van de cyberbeveiliging in ons land. Bedoeling is dat het voorstellen formuleert om het wettelijk raamwerk aan te passen, alsook ervoor zorgt dat gecoördineerd wordt gereageerd op incidenten en dat gestandaardiseerde praktijken worden toegepast. Voorts zou het CCBB informatie moeten verspreiden en participeren aan de sensibilisering van de diverse betrokken instanties. In al onze buurlanden (Frankrijk, Duitsland, Nederland en het Verenigd Koninkrijk) bestaat een dergelijk centrum al. Van zijn kant heeft de Amerikaanse president Barack Obama onlangs nog beklemtoond dat cyberdefensie voor de veiligheid van de Verenigde Staten een even grote uitdaging vormt als de strijd tegen het terrorisme. Overigens werd in de VS een *cybercommand* opgericht en werden duizenden *cyberwarriors* gerekruteerd.

Het Chinese leger heeft dan weer een departement in het leven geroepen dat zich specifiek met de cyberoorlog bezighoudt. Dat departement wordt verantwoordelijk geacht voor heel wat cyberaanvallen in de VS en in tal van andere landen, waaronder België.

la sécurité de l'information, appelée BelNIS (*Belgian Network Information Security*). BelNIS est la seule instance permettant aux acteurs de terrain de se rencontrer. Les membres de BelNIS sont des représentants des acteurs publics suivants: Cellule stratégique du ministre/secrétaire d'État en charge de l'informatisation de l'État, Commission de la protection de la vie privée, Autorité Nationale de Sécurité, Banque Carrefour de la Sécurité Sociale, Institut Belge des Postes et des Télécommunications, *Federal Computer Crime Unit*, Service général du renseignement et de la sécurité (Ministère de la Défense), SPF Économie, Fedict, Centre de crise (SPF Intérieur), Sûreté de l'État, SPP Politique scientifique, dont dépend le *Computer Security Incident Response Team* (CERT.be), SPF Justice, Parquet fédéral, Collège des procureurs généraux, OCAD-OCAM, SPF Affaires étrangères. BelNIS peut inviter des experts extérieurs en fonction des besoins. BelNIS se réunit une fois par mois.

Si cette plate-forme a le mérite d'exister et de faire travailler ensemble les différents acteurs publics concernés, elle ne dispose pas de ressources propres et aucun acteur n'assure la direction. Cette plate-forme n'a d'ailleurs aucune base légale qui définit ses missions et ses moyens d'action. Elle devrait donc être institutionnalisée sous forme d'un Centre pour la *cyber*sécurité en Belgique (CCB) et dotée de moyens spécifiques à la hauteur des enjeux. Ce Centre permettrait d'avoir un meilleur pilotage et suivi de la *cyber*sécurité en Belgique. Il formulerait des propositions d'adaptation du cadre légal, permettrait de coordonner la réponse aux incidents, de diffuser des standards et des informations et de participer à la sensibilisation des autres entités concernées. Une institution similaire existe chez chacun de nos voisins (France, Allemagne, Pays-Bas, Royaume-Uni). De son côté, le président Barack Obama a récemment estimé que la *cyber*défense était un enjeu encore plus important que le terrorisme pour la sécurité des États-Unis. Un *cybercommand* a d'ailleurs été créé et des milliers de "*cyberwarriors*" ont été recrutés.

L'armée chinoise a, quant à elle, aussi développé un département consacré à la *cyber*guerre. Ce département a été accusé de nombreuses attaques aux États-Unis et dans plusieurs autres pays du monde, dont la Belgique.

De Ministerraad heeft op 19 december 2013 een ontwerp van koninklijk besluit aangenomen betreffende de oprichting van het Centrum voor *Cyber*security België (CCB). Dat centrum wordt opgericht bij de FOD Kanselarij van de eerste minister en is bevoegd voor de tenuitvoerlegging van de *cyber*veiligheidsstrategie. Het CCB zal een tiental medewerkers tellen, en worden geleid door een directeur en een adjunct-directeur.

De regering heeft in het kader van de begroting 2014 een bedrag van 10 miljoen euro vrijgemaakt om de cyberveiligheid in België te versterken. De Ministerraad is het op 13 mei jongstleden eens geworden over de verdeling van dat bedrag: twee miljoen euro wordt aangewend om de integriteit van de netwerken te herstellen en om de *cyber*veiligheid te verbeteren op grond van de veiligheidsanalyse van de *task force* die belast is met het oplossen van de problemen die bij de FOD Buitenlandse Zaken zijn gerezen, alsook met het controleren van de integriteit van de netwerken van de overheidsdiensten; de overige acht miljoen euro zullen worden aangewend voor de indienstneming van extra personeel en voor aanvullende investeringen inzake opsporing en bescherming, waaronder de oprichting van het CCB.

Die bedragen moeten volgens de indienster van dit voorstel van resolutie snel aan de betrokken diensten worden toegekend. Inzake *cyber*veiligheid moeten immers dringend doortastende en doeltreffende maatregelen worden genomen.

In de huidige stand van de Belgische wetgeving mogen de bevoegde diensten, bijvoorbeeld Landsverdediging, trouwens geen sites en computers neutraliseren die cyberaanvallen uitvoeren, tenzij die zich in een land bevinden waarmee België in staat van oorlog verkeert. Ons land kan dus enkel antihackingsystemen opzetten, zonder echter cyberaanvallen een halt te kunnen toeroepen. De Belgische politiediensten beschikken al evenmin over een wettelijke hefboom om het IP-adres dat achter een aanval schuilgaat, te neutraliseren of zelfs maar te achterhalen.

Een van de moeilijkheden in verband met cyberbeveiliging is dat de meeste cyberincidenten worden verzwegen wanneer ze worden ontdekt. De overheid en de privésector moeten de krachten bundelen om die dreiging het hoofd te bieden cybercriminaliteit treft immers iedereen: niet alleen alle landen en de kritieke infrastructuur ervan, maar ook de financiële wereld en de banken als hoekstenen van onze economie, en de bedrijven, zowel de grote als de kmo's. Die kmo's zijn bijzonder kwetsbaar omdat het hen ontbreekt aan middelen om de cyberdreiging op te vangen.

Le 19 décembre 2013, le Conseil des ministres a adopté un projet d'arrêté royal portant création du Centre pour la *Cyber*sécurité en Belgique (CCB). Ce centre est créé auprès du SPF Chancellerie du premier ministre et il est compétent pour la mise en œuvre de la stratégie de *cyber*sécurité. Le CCB sera composé d'une dizaine de collaborateurs et dirigé par un directeur et un directeur adjoint.

Dans le cadre du budget 2014, le gouvernement a dégagé un budget de 10 millions d'auros pour renforcer la *cyber*sécurité en Belgique. Le 13 mai dernier, le Conseil des ministres s'est accordé sur la répartition de ce montant. Deux millions d'euros sont réservés pour restaurer l'intégrité des réseaux et pour renforcer la *cyber*sécurité sur la base de l'analyse de sécurité menée par la *task force* chargée de résoudre les problèmes survenus aux SPF Affaires étrangères et de contrôler l'intégrité des réseaux des services publics. Les 8 millions d'euros restants seront utilisés pour l'engagement de personnel supplémentaire et pour des investissementes additionnels sur le plan de la détection et de la protection, dont la création du CCB.

L'auteur de la présente proposition de résolution estime que ces budgets doivent être rapidement alloués aux services concernées. Il est, en effet, urgent de prendre des décisions fortes et efficaces en matière de *cybersécurité*.

Par ailleurs, la loi belge ne permet pas aux services compétents, par exemple ceux de la Défense nationale, de neutraliser les sites et ordinateurs qui mènent des *cyber*attaques, à moins que ces sites ne soient situés dans un pays avec lequel la Belgique est en guerre. La Belgique ne peut donc que mettre en place des systèmes anti-intrusion, sans possibilité de faire cesser l'attaque. La police belge non plus ne dispose pas de moyens légaux pour neutraliser ni même pour identifier une adresse IP à l'origine d'une attaque.

Une des difficultés en matière de *cyber*sécurité est que la plupart des incidents *cyber*nétiques sont tus lorsqu'ils sont découverts. Secteur public et privé doivent unir leurs efforts pour faire face à cette menace. En effet, le *cyber*crime touche les États et ses infrastructures critiques, mais aussi le domaine financier et bancaire, clé de voûte du système économique, ainsi que les entreprises, tant les grandes que les PME. Les PME sont particulièrement vulnérables par manque de moyens pour faire face aux *cyber*menaces.

Georges DALLEMAGNE (cdH)

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. wijst op het belang van de informatie- en communicatietechnologie in onze moderne samenlevingen;

B. stelt vast dat er heel wat cyberaanvallen plaatsvinden, met vernietigende gevolgen voor het welzijn van de bevolking, voor de economie en voor de veiligheid van het land;

C. attendeert op de kwetsbaarheid van de informatiesystemen, inclusief de meest strategische en de best beschermde;

D. herinnert aan de strategie van de federale regering inzake cyberveiligheid (21 december 2012);

E. wijst op de Europese strategie voor cyberbeveiliging, "Een open, veilige en zekere cyberspace", evenals op het voorstel voor een richtlijn van de Europese Commissie houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen;

F. stelt vast dat binnen de NAVO werk wordt gemaakt van cyberdefensie;

G. wijst erop dat de regering in het raam van de begroting 2014 heeft beslist 10 miljoen euro te investeren, alsook extra personeel aan te trekken om de cyberveiligheid in België aan te scherpen;

H. geeft aan dat de Ministerraad op 19 december 2013 een ontwerp van koninklijk besluit heeft aangenomen betreffende de oprichting van het Centrum voor Cybersecurity België (CCB), ter uitvoering van de Belgische strategie inzake cyberveiligheid;

I. acht het noodzakelijk de wetgevingsinstrumenten tot beveiliging van het grondgebied en de kritieke infrastructuur te versterken, teneinde te kunnen optreden tegen cyberaanvallen;

verzoekt de regering:

1. inzake cyberbeveiliging een gecentraliseerde en geïntegreerde aanpak te ontwikkelen, op grond van een wettelijk raamwerk dat een efficiënt optreden in verhouding tot de ernst van de dreiging mogelijk maakt en dat tegelijk de fundamentele rechten en vrijheden in acht neemt;

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. considérant l'importance des technologies de l'information et de la communication dans nos sociétés modernes;

B considérant le nombre élevé des *cyber*attaques et leurs conséquences néfastes pour le bien-être de la population, l'économie et la sécurité du pays;

C. considérant la vulnérabilité des systèmes d'information, y compris les plus stratégiques et les mieux protégés;

D. considérant la stratégie en matière de *cyber*sécurité du gouvernement fédéral du 21 décembre 2012;

E. considérant la "stratégie de *cyber*sécurité de l'UE: un *cyber*espace ouvert, sûr et sécurisé" ainsi que la proposition de directive concernant "des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (SRI)" de la Commission européenne;

F. considérant le développement de la *cyber*défense au sein de l'OTAN;

G. considérant la décision du gouvernement d'investir 10 millions d'euros ainsi que d'engager du personnel supplémentaire pour renforcer la *cyber*sécurité en Belgique, dans le cadre du budget 2014;

H. considérant l'adoption, le 19 décembre 2013, par le Conseil des ministres d'un projet d'arrêté royal portant création du Centre pour la *cyber*sécurité en Belgique (CCB), compétent pour la mise en œuvre de la stratégie de *cyber*sécurité;

I. considérant la nécessité de renforcer les dispositifs législatifs permettant d'assurer la sécurité du territoire et des infrastructures critiques en cas de *cyber*attaques;

demande au gouvernement:

1. de développer une approche centralisée et intégrée en matière de sécurité, dotée d'un cadre légal qui permette une action efficace à la mesure de la menace, mais aussi soucieuse de nos droits et libertés fondamentaux;

2. de oprichting van een Centrum voor cyberbeveiliging in België te bespoedigen, teneinde onze samenleving b*eter* tegen de cyberdreiging te wapenen en meer gespecialiseerde kennis aangaande cyberbeveiliging op te doen; voorts moet het Centrum advies verstrekken over cyberveiligheidsaangelegenheden, reageren op de bedreigingen en aanvallen en zorgen voor een gecoördineerd optreden in crisissituaties;

3. te voorzien in de technische en de menselijke middelen die onmisbaar zijn om een efficiënte strategie uit te werken die het hoofd kan bieden aan de uitdagingen inzake cyberveiligheid;

4. initiatieven te nemen om privésector bewust te maken van de bestaande cyberveiligheidsrisico's, opdat die sector de nodige beschermingsmaatregelen neemt;

5. na te gaan of het opportuun is ons land uit te rusten met een offensiever instrument ter bestrijding van cyberaanvallen;

6. spoedig werk te maken van de verwezenlijking van de maatregelen die zijn vervat in voormeld voorstel voor een Europese richtlijn;

7. de samenwerking met het ENISA *(European Union Agency for Network and Information Security)* op te voeren, alsook een nauwere samenwerking te overwegen met de NAVO-gelieerde structuren NCIA *(NATO Communications and Information Agency)* en CCD COE NATO *(NATO Cooperative Cyber Defence Centre of Excellence)*.

30 juni 2014

2. d'accélérer la mise en place du Centre pour la *cyber*sécurité en Belgique afin d'augmenter la capacité de défense de la société contre la *cyber*menace, d'agrandir l'expertise sur la *cyber*sécurité, de donner des avis sur la protection, de répondre aux menaces et attaques et de coordonner la réponse en cas de crise;

3. de prévoir les moyens techniques et humains indispensables à la mise en place d'une stratégie efficace et à la hauteur des enjeux de *cyber*sécurité;

4. de prendre des initiatives afin d'encourager le secteur privé à prendre conscience des risques existants en matière de *cyber*sécurité, afin qu'ils prennent les mesures de protection nécessaires;

5. d'évaluer l'opportunité de se doter d'une capacité plus offensive en matière de *cyber*attaques;

6. de mettre rapidement en œuvre les mesures mentionnées dans le projet de directive européenne;

7. d'accentuer la coopération avec l'ENISA *(European Union Agency for Network and Information Security)* ainsi que d'envisager une collaboration accrue avec les structures liées à l'OTAN que sont la NCIA (*NATO Communication and Information Agency*) et le CCD COE *(NATO Cooperative Cyber Defence Centre of Excellence)*.

30 juin 2014

Georges DALLEMAGNE (cdH)

Centrale drukkerij – Imprimerie centrale