DOC 53 **1289/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

15 mars 2011

PROPOSITION DE RÉSOLUTION

concernant la lutte contre les cyberattaques et les cyberguerres

(déposée par MM. Denis Ducarme
et David Clarinval)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

15 maart 2011

VOORSTEL VAN RESOLUTIE

over de strijd tegen cyberaanvallen en cyberoorlogen

(ingediend door de heren Denis Ducarme
en David Clarinval)

N-VA	:	*Nieuw-Vlaamse Alliantie*
PS	:	*Parti Socialiste*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
sp.a	:	*socialistische partij anders*
Ecolo-Groen!	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
VB	:	*Vlaams Belang*
cdH	:	*centre démocrate Humaniste*
LDD	:	*Lijst Dedecker*
INDEP-ONAFH	:	*Indépendant - Onafhankelijk*

Abréviations dans la numérotation des publications:

DOC 53 0000/000:	*Document parlementaire de la 53ème législature, suivi du n° de base et du n° consécutif*
QRVA:	*Questions et Réponses écrites*
CRIV:	*Version Provisoire du Compte Rendu intégral (couverture verte)*
CRABV:	*Compte Rendu Analytique (couverture bleue)*
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: couverture blanche; COM: couverture saumon)*
PLEN:	*Séance plénière*
COM:	*Réunion de commission*
MOT:	*Motions déposées en conclusion d'interpellations (papier beige)*

Afkortingen bij de nummering van de publicaties:

DOC 53 0000/000:	*Parlementair document van de 53e zittingsperiode + basisnummer en volgnummer*
QRVA:	*Schriftelijke Vragen en Antwoorden*
CRIV:	*Voorlopige versie van het Integraal Verslag (groene kaft)*
CRABV:	*Beknopt Verslag (blauwe kaft)*
CRIV:	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen) (PLEN: witte kaft; COM: zalmkleurige kaft)*
PLEN:	*Plenum*
COM:	*Commissievergadering*
MOT:	*Moties tot besluit van interpellaties (beigekleurig 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
e-mail: publications@lachambre.be

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

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Une cyberattaque consiste en un acte malveillant envers un dispositif informatique, via l'accès à un réseau Internet. Pendant longtemps, la guerre informatique, ou cyberguerre, est souvent restée cantonnée aux scénarios de certains films ou du monde de la science-fiction. Force est de constater que, actuellement, le blocage des moyens informatiques, et donc des centres de commandement ou de transmission d'information, est une pratique redoutée par les personnes préoccupées par la sécurité informatique. Les virus informatiques ont été les premières armes de ce type.[1] Au vu de la multiplication des cas, le cyberespace semble devenir un véritable espace de confrontation, au même titre que les espaces terrestre, aérospatial ou maritime. La cyberguerre pourrait-elle devenir le prélude à une attaque conventionnelle, voire d'une attaque asymétrique stratégique?[2]

La première cyberattaque visant une structure étatique durant plusieurs semaines, avec des moyens suffisants pour saturer durablement les sites visés, a émané de sites russes contre des sites de l'administration estonienne. Banques, administrations, hôpitaux et les sites de journaux de ce pays balte furent piratés au printemps 2007.[3]

L'attaque survint suite au conflit diplomatique généré autour du projet de déplacement du Soldat de Bronze, planifié par le gouvernement estonien en avril 2007 mais ayant abouti à des nuits d'émeutes, émanant d'une forte minorité de nationalistes russophones implantée dans le pays. La majorité des institutions estoniennes ayant adopté une bureaucratie sans papier, entièrement informatique et reliées entre elles par Internet, ce pays fut une cible de choix, car particulièrement vulnérable à ce type d'attaques.[4]

Dès avril 2007, les sites de journaux, des principales banques ou des institutions gouvernementales ont subi des bombardements massifs de spams ou ont été victimes de défacement (changement de page de garde), de déni de service.[5]

Pour les Estoniens, il ne fait aucun doute que ces attaques étaient le fait de la Russie. *"Nous n'avons pas de*

1 http://fr.academic.ru/dic.nsf/frwiki/73990.
2 Rapport sur la criminalité virtuelle 2009, McAffee.
3 In *Le Monde* 26 mai 2008.
4 http://fr.wikipedia.org/wiki/Cyberattaque.
5 In *Le Monde* 26 mai 2008.

TOELICHTING

DAMES EN HEREN,

Een cyberaanval is een kwaadwillige daad tegen een informaticasysteem, die wordt gepleegd via een internettoegang. Lange tijd vonden informaticaoorlogen, ook cyberoorlogen genaamd, alleen maar plaats in bepaalde films of in de wereld van de *science fiction*. Vandaag is dat niet langer het geval: mensen die zich met de internetveiligheid bezighouden, zijn uiterst beducht voor acties waarmee de blokkering wordt beoogd van informaticamiddelen en dus van commandocentra of centra voor informatieoverdracht. De computervirussen waren de eerste wapens die door de aanvallers werden gebruikt[1]. Door het fors toenemende aantal aanvallen, lijkt cyberspace uit te groeien tot een heus strijdtoneel, dat in aanmerking komt voor veldslagen zoals voorheen het land, de zee en de ruimte. Is het denkbaar dat de cyberoorlog de aanzet kan zijn voor een conventionele aanval of zelfs voor een strategische asymmetrische aanval?[2]

De eerste wekenlange cyberaanval tegen een staatsstructuur, met voldoende kracht om de geviseerde websites langdurig te doen crashen, ging uit van Russische websites tegen de websites van het Estse overheidsbestuur. Op die manier werden in het voorjaar van 2007 de informaticasystemen van banken, overheidsbesturen en ziekenhuizen, alsook de websites van kranten, gehackt[3].

De aanval kwam er in de nasleep van de diplomatieke rel over de in april 2007 door de Estse regering geplande verplaatsing van het standbeeld "De Bronzen Soldaat". Die gebeurtenis gaf aanleiding tot rellen, die uitgingen van de omvangrijke minderheid van Russisch sprekende nationalisten in het land. Aangezien de meeste Estse instellingen volledig papierloos — dus geïnformatiseerd — werken en via het internet met elkaar zijn verbonden, waren zij uiterst kwetsbaar voor cyberaanvallen en bijgevolg een gedroomd mikpunt[4].

Vanaf april 2007 zijn websites van kranten, de voornaamste banken of van regeringsinstellingen massaal getroffen door spambombardementen, door *defacement* (gekraakte welkomstpagina) of door een verstoring van de dienstverlening[5].

Voor de Esten stond het vast dat Rusland achter die cyberaanvallen zat, zo meldde *Le Monde:* "*Nous n'avons*

1 Zie: http://fr.academic.ru/dic.nsf/frwiki/739906.
2 Zie het McAffee-rapport over de virtuele criminaliteit.
3 Zie: *Le Monde*, 26 mei 2008.
4 Zie: http://fr.wikipedia.org/wiki/Cyberattaque.
5 Zie: *Le Monde, op.cit.*

convention de Genève de l'Internet, explique le porte-parole du ministère de la Défense Aari Lemmik. Selon les principes de l'OTAN, une attaque armée contre un pays de l'OTAN est une attaque contre tous les pays de l'OTAN. Peut-on considérer une cyberattaque comme une attaque armée? De notre point de vue, oui, car si, aujourd'hui, quelqu'un veut lancer une attaque armée contre un pays technologiquement développé, il commence probablement par une cyberattaque."[6]

En quelques heures, ce pays, qui est le plus connecté d'Europe, fut l'objet d'une série d'attaques par déni de service (DdoS, déni de service distribué) sans précédent à l'échelle d'un pays. Les sites gouvernementaux furent les premiers visés. Puis vint le tour des banques, des médias et des partis politiques. Le numéro des urgences (ambulances, incendies) est même resté indisponible pendant plus d'une heure.

L'attaque par déni de service est devenue un classique du genre. L'opération consiste à inonder le serveur d'un site Web de requêtes jusqu'à la paralysie, ce qui entraîne inévitablement un écran noir. Ou plus précisément une page d'"erreur http 404", c'est-à-dire une fin de non-recevoir pour tout internaute désirant visiter ce site Internet.[7] Une attaque DdoS (déni de service) est une attaque relativement basique. Il s'agit de noyer la cible sous des requêtes de connexion. Elle peut être orchestrée manuellement par plusieurs centaines de pirates coordonnés, ou à plus grande échelle, en utilisant un botnet, un réseau d'ordinateurs "zombies" infectés par un ver et contrôlés par des pirates.[8]

Dans le cas estonien, les assaillants ont utilisé des dizaines de milliers de PC zombies. Ces machines infectées malicieusement sont chargées de transmettre, à leur insu, les requêtes vers le serveur du site Web visé. La densité était telle que les experts ont enregistré une création de trafic allant jusqu'à 5 000 clics par seconde sur certains sites ciblés.[9] L'Estonie, victime d'attaques massives sur ses systèmes d'information en avril et mai 2007, a involontairement créé un sentiment d'impuissance au sein de la Communauté européenne. Face à une réalité alarmante, les autorités des États membres mesurent la vulnérabilité de leurs structures technologiques. Largement sous estimée depuis des années, la

6 In *Le Monde* 26 mai 2008.
7 *L'Estonie dénonce les* cyber-*attaques terroristes russes* 11/06/2007 in *01 Net.*
8 *L'Europe face à la criminalité numérique, Fondation Robert Schuman*, 3 septembre 2007.
9 *L'Estonie dénonce les* cyber-*attaques terroristes russes* 11/06/2007 in *01 Net.*

pas de convention de Genève de l'Internet", explique le porte-parole du ministère de la Défense Aari Lemmik. "Selon les principes de l'OTAN, une attaque armée contre un pays de l'OTAN est une attaque contre tous les pays de l'OTAN. Peut-on considérer une cyberattaque comme une attaque armée? De notre point de vue, oui, car si, aujourd'hui, quelqu'un veut lancer une attaque armée contre un pays technologiquement développé, il commence probablement par une cyberattaque."[6]

In enkele uren kreeg Estland, het Europese land dat het meest online is, een nooit geziene reeks aanvallen door verstoring van de dienstverlening (DDoS - *Distributed Denial of Service*) te verwerken. De regeringswebsites werden het eerst getroffen, gevolgd door de websites van de banken, de media en de politieke partijen. Zelfs het noodnummer voor de ziekenwagens en de brandweer viel ruim een uur lang uit.

Een aanval door verstoring van de dienstverlening is inmiddels in de cyberwereld een "klassiek" wapen geworden. De operatie bestaat erin de server van de geviseerde website te bedelven onder de aanvragen, wat leidt tot een blokkering en, onvermijdelijk, een leeg scherm — of beter de foutmelding "http 404". Die melding geeft de internetgebruiker aan dat hij geen toegang heeft tot de website die hij wil bezoeken[7]. Een DDos-aanval is behoorlijk eenvoudig van opzet. Bedoeling is het doelwit te bestoken met connectieaanvragen. Die aanval kan manueel gebeuren door verschillende honderden internauten die gecoördineerd werken, ofwel op grotere schaal via een *botnet*, een netwerk van *zombiecomputers* die werden geïnfecteerd met een wormvirus en worden gecontroleerd door de internetpiraten[8].

Voor de aanvallen tegen Estland werden tienduizenden *zombiecomputers* ingezet. Die kwaadwillig geïnfecteerde computers verzenden, zonder medeweten van de eigenaars ervan, verzoeken naar de geviseerde website. Het aantal verzoeken was zo groot dat de deskundigen op bepaalde geviseerde websites tot 5 000 clicks per seconden hebben gemeten[9]. Door die massale aanvallen van april en mei 2007 op de informaticasystemen van Estland, legde de EU-lidstaat ongewild de machteloosheid van de Europese Unie bloot. Die alarmerende toestand drukte de overheden van de lidstaten met de neus op de feiten: hun technologische structuren zijn kwetsbaar. Na jaren van een gebrek aan aandacht

6 *Idem*.
7 Zie: *L'Estonie dénonce les* cyber-*attaques terroristes russes*, in: *01 Net*, 11 juni 2007.
8 *L'Europe face à la criminalité numérique*, *Fondation Robert Schuman*, 3 september 2007.
9 *L'Estonie dénonce les* cyber-*attaques terroristes russes*, *op.cit.*

sécurité informatique devient une priorité absolue devant les menaces existantes et émergentes.[10]

Les experts de l'OTAN, chargés d'enquêter sur les bugs répétés des principaux sites Internet estoniens pendant plusieurs semaines, se sont très vite alarmés devant l'ampleur de cette attaque.*"Actuellement, l'OTAN ne définit pas les* cyber*attaques comme un acte de guerre",* a précisé à l'époque le ministre de la Défense estonien, Jaak Aaviksoo, soulignant que "l'article V du traité nord-atlantique, c'est-à-dire la défense collective, n'est pas applicable".

Pour faire face à cette nouvelle menace, 8 pays de l'Organisation du Traité de l'Atlantique Nord (OTAN) ont créé, à la mi-mai 2008, le tout nouveau centre de cyberdéfense. Même si ce n'est qu'un début, ce centre n'a aucune fonction opérationnelle, cette tâche étant confiée dans chaque pays aux CERT (*Computer Emergency Response Team*). À Tallinn, les experts de l'OTAN ont développé des instruments pour défendre le cyberespace, qu'ils mettront à disposition des pays membres sous forme d'entraînement, d'analyse, de consultations. L'Estonie, dont l'économie est très dépendante d'Internet, militait depuis des années pour l'ouverture d'un tel centre.[11]

Au Sommet de Bucarest au printemps 2008, l'Otan réclamait plus de coopération entre ses États membres et tirait la sonnette d'alarme. Tout comme la première puissance du monde, désemparée. "*Vous n'avez besoin ni d'une armée, ni de marines, ni d'une aviation hors pair pour battre les États-Unis"*, explique le général américain William T. Lord, pour qui un ordinateur peut virtuellement être à l'origine de plusieurs 11 Septembre. Un "*hacktivisme"* qui, redonnant de la vigueur aux terrorismes de tous poils, secoue l'équilibre des forces en vigueur depuis la chute du mur de Berlin.[12]

Bien que la pratique de l'OTAN ne prenait alors pas encore en compte ce genre d'attaques, certains responsables estoniens ont considéré la cyberattaque, par son organisation et sa durée, comme un acte de guerre à part entière, car les structures visées se sont retrouvés entièrement inopérantes, de la même manière que si elles avaient été frappés par des missiles. Le président de l'Estonie, Toomas Hendrik a considéré ces actes

[10] *L'Europe face à la criminalité numérique, Fondation Robert Schuman*, 3 septembre 2007.
[11] In *Le Monde* 26 mai 2008.
[12] In *L'Express* 6 mai 2008.

wordt de informaticaveiligheid een absolute prioriteit. De dreiging is immers reëel en er komen nieuwe dreigingen bij[10].

De NAVO-experts, die ermee belast waren de herhaalde bugs te onderzoeken die gedurende verscheidene weken de belangrijkste Estse websites teisterden, maakten zich prompt bezorgd over de omvang van die aanval. Jaak Aaviksoo, de Estse minister van Defensie, preciseerde dat de NAVO de cyberaanvallen momenteel niet aanmerkt als een oorlogsdaad. Bovendien benadrukte hij dat artikel V van het Noord-Atlantisch Verdrag, namelijk de collectieve verdediging, niet van toepassing is.

Als reactie op deze nieuwe bedreiging, hebben 8 landen van de Noord-Atlantische Verdragsorganisatie (NAVO), medio mei 2008, het spiksplinternieuwe centrum van cyberverdediging opgericht. Ook al is nog maar een prille aanzet, dit centrum beschikt over geen enkele operationele functie, aangezien die taak in ieder land toevertrouwd wordt aan het CERT (*Computer Emergency Response Team*). De experts van de NAVO hebben in Tallinn instrumenten ontwikkeld die aan de NAVO-lidstaten ter beschikking gesteld zullen worden in de vorm van training, analyse en adviesverlening, om de cyberspace te beschermen. Estland, waarvan de economie zeer afhankelijk is van het internet, voert al jaren actie voor de oprichting van zo'n centrum.

Tijdens de Top van Boekarest in het voorjaar van 2008, eiste de NAVO meer samenwerking tussen haar lidstaten en trok aan de alarmbel, net als de voornaamste wereldgrootmacht trouwens, die behoorlijk ontdaan was. De Amerikaanse generaal William T. Lord verklaarde dat je geen kolossaal leger, noch een formidabele marine of luchtmacht nodig hebt om de Verenigde Staten te verslaan. Daarbij was hij van mening dat het theoretisch mogelijk is dat een computer aan de oorsprong kan liggen van verscheidene 9/11's. Dat "*hacktivisme"*, dat allerlei vormen van terrorisme een boost geeft, verstoort sinds de val van de Berlijnse Muur de bestaande machtsevenwichten.

Hoewel bij de NAVO toen nog geen rekening gehouden werd met dit soort aanvallen, beschouwden sommige Estse leiders de cyberaanval, door zijn organisatie en duur, op-en-top als een oorlogsdaad, aangezien de structuren waarop hij gericht was, volledig waren uitgeschakeld, alsof ze door raketten waren getroffen. De Estse president Toomas Hendrik Ilves beschouwde deze destabiliserende daden als een nieuwe vorm van

[10] *L'Europe face à la criminalité numérique*, *op.cit.*

de déstabilisation comme une nouvelle forme de terrorisme. Mais de telles attaques posent un problème de "traçabilité", à savoir la possibilité de remonter jusqu'à leur auteur, et surtout de le prouver.

Outre la criminalité financière qui s'est développée sur Internet, et qui serait plus rentable que le trafic de drogue, selon Valérie McNiven, conseillère auprès du gouvernement fédéral américain, des opérations de déstabilisation politique ont aussi été menées sur le réseau, ces dernières années.[13]

En effet, malheureusement, le cas estonien n'est pas un cas isolé. Selon le magazine américain "*60 minutes*" du 8 novembre 2007, les grandes pannes du réseau électrique brésilien de janvier 2005 à Rio de Janeiro et de septembre 2007 à Espirito Santo seraient également la conséquence de cyberattaques, dont la source n'est pas identifiée.

Cette hypothèse a également été évoquée pour la coupure géante d'électricité du 10 novembre 2009, toujours au Brésil. En 2008, déjà, lors du conflit russo-géorgien, la Géorgie avait signalé une saturation des serveurs d'une centaine de sites. Des millions de mails offensifs ont ainsi bloqué les sites gouvernementaux, dont celui du président, des sites de médias et de banques.[14]

La Corée du sud, le 6 juillet 2009, a subi des cyberattaques à grande échelle. 25 sites, dont les sites Internet de la présidence sud-coréenne, du ministère de la Défense, du ministère des Affaires étrangères, de la *Shinhan Bank* et *Korea Exchange Bank* ont été touchés, sur fond de tensions avec la Corée du Nord. Selon la presse sud-coréenne, le *National Intelligence Service* aurait sous-entendu la responsabilité de Pyongyang, sans fournir de preuves. La KISA, l'Agence coréenne de la sécurité de l'information, a affirmé qu'il semblait s'agir d'attaques massives et ciblées de type dit de DDoS, ou "déni de service distribué". Depuis le 4 juillet 2009, jour de fête nationale, plusieurs agences gouvernementales américaines avaient été victimes d'une série de cyber-attaques. Elles avaient affecté le Département du Trésor des États-Unis, la *Federal Trade Commission*. Le Danemark a également été la victime de ces attaques pendant plusieurs jours, de nombreux sites Internet du pays ayant été pris pour cible par une horde de pirates protestant contre les caricatures du prophète Mahomet.

terrorisme. Dergelijke aanvallen doen echter een probleem van "traceerbaarheid" rijzen in verband met de mogelijkheid de dader terug te vinden, en vooral met harde bewijzen te komen.

Naast de financiële criminaliteit via het internet, die volgens Valérie McNiven, adviseur bij de Amerikaanse regering, lucratiever zou zijn dan de illegale drugshandel, zijn er de laatste jaren op het net ook politieke destabilisatieoperaties gevoerd.

De aanval op Estland is, helaas, geen alleenstaand feit. Zo zouden volgens het Amerikaanse nieuwsmagazine *60 minutes* van 8 november 2007 de grote stroompannes in Brazilië in januari 2005 in Rio de Janeiro en in september 2007 in Espirito Santo ook te wijten zijn aan cyberaanvallen, waarvan de daders onbekend zijn.

Dezelfde hypothese werd geopperd toen op 10 november 2009 Brazilië andermaal getroffen werd door een gigantische stroomonderbreking. Tijdens het conflict tussen Rusland en Georgië in 2008, liet Georgië weten dat de servers van een honderdtal websites tilt waren geslagen. Zo hebben miljoenen agressieve mails de toegang tot de regeringsites — waaronder die van de president — en tot de sites van media en banken geblokkeerd.

Op 6 juli 2009 was het de beurt aan Zuid-Korea: het land werd overspoeld door een golf van cyberaanvallen waarbij 25 sites, waaronder die van de Zuid-Koreaanse president, de minister van Defensie, de minister van Buitenlandse zaken, de *Shinhan Bank* en de *Korea Exchange Bank* het te verduren kregen, tegen de achtergrond van spanningen met Noord-Korea. Volgens de Zuid-Koreaanse pers, zou de *National Intelligence Service* hebben laten doorschemeren dat Pyongyang daarvoor aansprakelijk was, alhoewel de NIS geen bewijzen aandroeg. Het KISA, het Koreaanse agentschap voor informatiebeveiliging, heeft bevestigd dat het leek te gaan om massale en gerichte aanvallen van het type DDoS (*Distributed denial-of-Service)*. Sinds 4 juli 2009, de dag waarop de Amerikaanse nationale feestdag wordt gevierd, waren een aantal overheidsdiensten in de Verenigde Staten het slachtoffer van een reeks cyberaanvallen, die onder meer het Amerikaanse ministerie van Financiën en de *Federal Trade Commission* op de korrel namen. Ook Denemarken kreeg verscheidene dagen aan een stuk af te rekenen met dat soort aanvallen, toen tal van sites het doelwit werden van een bende cyberpiraten die hun ongenoegen uitten over de Mohammedcartoons.

13 In *Le Monde* 26 mai 2008.
14 http://fr.wikipedia.org/wiki/Cyberattaque.

Depuis que le monde de l'informatique est en constant développement, et encore largement inexploré, de nouveaux pays produisent de jeunes chercheurs en informatique habituellement intéressés à "s'amuser". Des pays comme la Chine, la Grèce, l'Inde, Israël et les deux Corées ont tous été sous les projecteurs des médias américains pour les attaques contre les systèmes d'information liés à la CIA ou la NSA.[15]

Les États-Unis ont pris un grand intérêt dans la protection des systèmes d'information critiques. Des contrats de recherche ont été conclus en matière de sécurité électronique, en faveur de nations comme la Grèce et Israël, pour les aider à se protéger contre les attaques les plus graves et les plus dangereuses. En juillet 2009, plusieurs cyberattaques ont été lancées contre les sites Web du gouvernement, tels que le Pentagone et la Maison blanche, aux États-Unis, et des agences gouvernementales, en Corée du Sud.[16] Le 3 février 2008, plusieurs dizaines de milliers de Qatariens, de Malaisiens et d'Egyptiens en ont fait l'amère découverte, eux qui, face à un écran noir, se sont tout à coup retrouvés privés d'accès à leur compte bancaire, au téléphone ou à la télévision en ligne. Un câble enfoui sous la mer avait tout simplement été sectionné. Après avoir envisagé un accident, les enquêteurs n'excluent pas, aujourd'hui, une piste criminelle.[17]

Les réseaux de transport ou l'alimentation en énergie pourraient être menacés à terme, redoute Guillaume Tissier, un des responsables de la Compagnie européenne d'intelligence stratégique (CEIS), une société privée d'intelligence économique. Le 24 avril 2010, le GovSec, une émanation du département américain de la Défense, a listé les secteurs qui seraient touchés les premiers en cas d'une attaque organisée sur Internet. Les circuits électriques, tout comme les télécoms, seraient déréglés, suivis du système bancaire et de l'approvisionnement en pétrole. Avant de parvenir à une paralysie du pays, avec des pompiers ou des chirurgiens hors d'état de travailler. Le pire devient possible. "*Pourquoi ne pas envisager la perte de la mainmise sur les équipements nucléaires?*" s'interroge-t-on chez l'éditeur israélien *Check Point*.[18]

L'entreprise *Google* a également subi une cyberattaque d'envergure, le 15 janvier 2010, sans doute provenant de Chine.[19] Le groupe Internet a en effet

Aangezien de informaticawereld voortdurend in ontwikkeling is en bij lange na nog niet volledig geëxploiteerd wordt, fabriceren nieuwe landen jonge informaticaonderzoekers, die doorgaans wel geïnteresseerd zijn in een "verzetje". Landen als China, Griekenland, India, Israël en Noord- en Zuid-Korea zijn volop in de Amerikaanse mediabelangstelling gekomen wegens de van daaruit komende aanvallen tegen aan de CIA en de NSA gelinkte informatiesystemen.

De Verenigde Staten zijn groot belang gaan stellen in de bescherming van kritische informatiesystemen. Inzake elektronische beveiliging zijn onderzoekscontracten gesloten ten met landen als Griekenland en Israël om hen te helpen zich tegen de zwaarste en de gevaarlijkste aanvallen te beschermen. In juli 2009 waren regeringssites in de Verenigde Staten, zoals die van het Pentagon en het Witte Huis, het doelwit van cyberaanvallen, net zoals dat het geval was met overheidsinstellingen in Zuid-Korea. Op 3 februari 2008 deden enkele tienduizenden Qatarezen, Maleisiërs en Egyptenaren de wrange ontdekking dat ze op een zwart beeld moesten zitten staren omdat hun plotseling de toegang tot hun bankrekening, telefoon of on-line televisie ontnomen werd doordat een in de zeebodem ingegraven kabel simpelweg was doorgesneden. Nadat de speurders aanvankelijk aan een ongeluk hadden gedacht, sluiten zij vandaag niet uit dat dit het werk is van criminelen.

L'Express rapporteert het volgende: *"Les réseaux de transport ou l'alimentation en énergie pourraient être menacés à terme", redoute Guillaume Tissier, un des responsables de la Compagnie européenne d'intelligence stratégique (CEIS), une société privée d'intelligence économique. Le 24 avril 2010, le GovSec, une émanation du département américain de la Défense, a listé les secteurs qui seraient touchés les premiers en cas d'une attaque organisée sur Internet. Les circuits électriques, tout comme les télécoms, seraient déréglés, suivis du système bancaire et de l'approvisionnement en pétrole. Avant de parvenir à une paralysie du pays, avec des pompiers ou des chirurgiens hors d'état de travailler. Le pire devient possible. "Pourquoi ne pas envisager la perte de la mainmise sur les équipements nucléaires?" s'interroge-t-on chez l'éditeur israélien* Check Point*."*[11].

Ook het bedrijf *Google* heeft op 15 januari 2010 een forse cyberaanval te verduren gekregen, wellicht vanuit China[12]. De internetgroep heeft immers gepreciseerd dat

15 http://fr.wikipedia.org/wiki/Cyberterrorisme.
16 http://fr.wikipedia.org/wiki/Cyberterrorisme.
17 In *L'Express* 6 mai 2008, http://www.desinfos.com/IMG/pdf/cyberguerre.pdf.
18 In *L'Express* 6 mai 2008, http://www.desinfos.com/IMG/pdf/cyberguerre.pdf.
19 http://pisani.blog.lemonde.fr/category/pointsdevue/.

11 *L'Express*, 6 mei 2008, zie http://www.desinfos.com/IMG/pdf/cyberguerre.pdf.
12 http://pisani.blog.lemonde.fr/category/pointsdevue/.

précisé que la cyberattaque visait en priorité les accès à des comptes Gmail de militants chinois des droits de l'Homme. Face à ce piratage, *Google* s'est érigé en défenseur de la liberté d'expression, en demandant expressément aux autorités chinoises d'autoriser le fonctionnement, sans filtrage, de son moteur de recherche. En cas de refus, *Google* s'est dit prêt à quitter le pays.[20]

Le 30 janvier 2010, dans un discours clé consacré à la liberté d'Internet, la secrétaire d'État américaine Hillary Clinton, a dénoncé les pays pratiquant le filtrage. Elle a également réclamé à la Chine une enquête "*minutieuse*" et "*transparente*" sur les cyber-attaques menées contre Google. La secrétaire d'État américaine a estimé que *"les pays qui lancent des* cyber*attaques devront en subir les conséquences"*. Le président Barack Obama a récemment nommé un conseiller spécial en matière de cybersécurité. L'armée américaine se dotera, quant à elle, d'un centre de commande afin de lutter contre les menaces grandissantes contre la sécurité informatique des États-Unis.

L'armée chinoise est régulièrement accusée de vouloir attaquer les systèmes informatiques américains. D'ores et déjà, Internet apparaît comme le nouveau champ de bataille planétaire, et ce pour l'ensemble des pays, quelque soit leur pouvoir militaire effectif.[21]

Devenir cyberdélinquant est un jeu d'enfant, s'inquiète l'Otan. Mais cela peut provoquer des dégâts aussi importants que les armes conventionnelles. [22]

De fait, devenir "cybercombattant" est à la portée de tout le monde, ou presque. Avec un peu d'ingéniosité et moins de 500 euros en poche, il est possible de bloquer l'accès à un site gouvernemental durant plusieurs heures! Il suffit d'acheter des listes d'adresses e-mails, disponibles sur des forums Internet grand public, que ces derniers parlent de la mode ou de la dernière tendance gastronomique.

Ces portes d'entrée offrent la possibilité à l'apprenti pirate de repérer les ordinateurs les plus fragiles, de les infecter et d'en prendre le contrôle à distance. Réitérée à l'envi, l'opération permet de disposer d'une petite armée de machines esclaves (un "*botnet*"). L'opération est efficace et quasiment anonyme. [23]

[20] Chambet Patrick, *le* cyber*terrorisme*, Edelweb - Groupe ON-X, http://www.chambet.com/publications/Cyberterrorisme.pdf.

[21] http://www.zdnet.fr/actualites/hillary-clinton-les-pays-qui-lancent-des-cyber-attaques-devront-en-subir-les-consequences-39712410.htm.

[22] In *L'Express* 6 mai 2008, http://www.desinfos.com/IMG/pdf/cyberguerre.pdf.

[23] *Ibidem*.

de cyberaanval vooral de toegang tot de Gmail-accounts van Chinese mensenrechtenactivisten viseerde. Toen *Google* met die piraterij te maken kreeg, is het bedrijf voor de vrije meningsuiting opgekomen, waarbij het de Chinese autoriteiten uitdrukkelijk vroeg toe te staan dat zijn zoekrobot zonder filters zou mogen functioneren.[13]

Op 30 januari 2010 heeft VS-minister van Buitenlandse Zaken Hillary Clinton in een cruciale toespraak over de vrijheid op het internet de landen aangeklaagd die filters toepassen. Voorts heeft zij geëist dat China een nauwgezet en transparant onderzoek zou voeren naar de cyberaanvallen tegen Google. Volgens de Amerikaanse minister van Buitenlandse Zaken zullen de landen die cyberaanvallen lanceren daar de gevolgen van moeten dragen [14]. Onlangs heeft VS-president Barack Obama een bijzondere adviseur inzake cyberveiligheid benoemd. Het VS-leger zal zich toerusten met een commandocentrum om de almaar grotere dreiging voor de computerveiligheid van de Verenigde Staten te bestrijden.

Het Chinese leger wordt er geregeld van beschuldigd dat het de Amerikaanse informaticasystemen wil belagen. Het internet lijkt nu al het nieuwe planetaire slagveld te worden voor alle landen, wat ook de daadwerkelijke militaire macht ervan zij.

L'Express wijst er ook op: "*Devenir* cyber*délinquant est un jeu d'enfant, s'inquiète un expert de l'Otan. Mais peut provoquer des dégâts aussi importants que les armes conventionnelles."* [15].

"De fait, devenir cyber*combattant est à la portée de tout le monde, ou presque. Avec un peu d'ingéniosité et moins de 500 euros en poche, il est possible de bloquer l'accès à un site gouvernemental durant plusieurs heures! Il suffit d'acheter des listes d'adresses e-mails, disponibles sur des forums Internet grand public, que ces derniers parlent de la mode ou de la dernière tendance gastronomique...*

*Ces portes d'entrée offrent la possibilité à l'apprenti pirate de repérer les ordinateurs les plus fragiles, de les infecter et d'en prendre le contrôle à distance. Réitérée à l'envi, l'opération permet de disposer d'une petite armée de machines esclaves (un "*botnet*"). L'opération est efficace et quasiment anonyme."*[16].

[13] Patrick Chambet, *Le* cyber-*terrorisme*, Edelweb – ON-X-Groep, zie http://www.chambet.com/publications/Cyberterrorisme.pdf.

[14] http://www.zdnet.fr/actualites/hillary-clinton-les-pays-qui-lancent-des-cyber-attaques-devront-en-subir-les-consequences-39712410.htm.

[15] *L'Express*, 6 mei 2008, zie http://www.desinfos.com/IMG/pdf/cyberguerre.pdf.

[16] *Ibidem.*

Les experts de l'OTAN ciblent trois types de menaces. Celles, très réelles, des criminels qui en veulent à votre carte de crédit (un numéro de carte bancaire s'achète 15 dollars sur Internet); celle, encore théorique, d'une attaque par des groupes terroristes qui s'en prennent à des installations électroniques, en minant, par exemple, la confiance des utilisateurs. Enfin, la menace, très actuelle, où un pays exerce sa volonté par des pressions à travers Internet. [24]

Depuis le 11 septembre 2001, les pays largement informatisés ont commencé à prendre sérieusement en compte les risques de cyberterrorisme contre leurs entreprises et leurs sociétés en général. Mais il ne faut pas oublier que le cyberterrorisme, même s'il semble actuellement entrer dans une nouvelle phase d'expansion, n'est pas un phénomène nouveau.[25] Avec une culture de la connectivité ancrée de plus en plus profondément dans les sociétés dites "modernes", il est promis à un bel avenir.

Aujourd'hui, on ne saurait plus vivre sans certains services, dont l'épine dorsale est constituée par des réseaux informatiques qui pourraient être réduits à néant par quelques attaques bien réelles, judicieusement menées dans le monde virtuel. Les principaux médias évoquent souvent la possibilité d'une attaque de grande envergure faisant appel aux réseaux informatiques pour saboter des infrastructures critiques, dans le but de mettre des vies humaines en danger ou de causer des perturbations sur une échelle nationale, soit directement, soit par le dérèglement de l'économie nationale.[26]

Le 24 avril 2007, le GovSec, une émanation du département américain de la Défense, a listé les secteurs qui seraient touchés les premiers en cas d'une attaque organisée sur Internet. Les circuits électriques, tout comme les télécoms, seraient déréglés, suivis du système bancaire et de l'approvisionnement en pétrole. Avant de parvenir à une paralysie du pays, avec des pompiers ou des chirurgiens hors d'état de travailler. Les réseaux de transport ou l'alimentation en énergie pourraient être menacés à terme. Le pire devient possible. Et qui sait, les installations nucléaires présentes dans de nombreux pays?

Le cyberterrorisme est la convergence entre le terrorisme traditionnel et les réseaux, à commencer par Internet. On peut donc définir le cyber-terrorisme comme

Le Monde schrijft: *"Les experts de l'OTAN ciblent trois types de menaces. Celles, très réelles des criminels qui en veulent à votre carte de crédit (un numéro de carte bancaire s'achète 15 dollars sur Internet); celle, encore théorique, d'une attaque par des groupes terroristes qui s'en prennent à des installations électroniques, en minant, par exemple, la confiance des utilisateurs. Enfin, la menace, très actuelle, où un pays exerce sa volonté par des pressions à travers Internet."*[17].

Patrick Chambet van zijn kant wijst erop: *"Depuis le 11 septembre 2001, les pays largement informatisés ont commencé à prendre sérieusement en compte les risques de cyberterrorisme contre leurs entreprises et leur société en général. Mais il ne faut pas oublier que le cyberterrorisme, même s'il semble actuellement entrer dans une nouvelle phase d'expansion, n'est pas un phénomène nouveau. Avec une culture de la connectivité ancrée de plus en plus profondément dans les sociétés dites "modernes", il est promis à un bel avenir.*

Aujourd'hui, on ne saurait plus vivre sans certains services dont l'épine dorsale est constituée par des réseaux informatiques qui pourraient être réduits à néant par quelques attaques bien réelles, judicieusement menées dans le monde virtuel."[18]. De belangrijkste media hebben het vaak over de mogelijkheid om met gebruikmaking van de informaticanetwerken een grootschalige aanval op te zetten om de systeemrelevante infrastructuurvoorzieningen te saboteren, teneinde mensenlevens in gevaar te brengen of wereldwijde verstoringen te veroorzaken, hetzij rechtstreeks, hetzij door 's lands economie te ontregelen.

Op 24 april 2007 heeft, volgens *L'Express, "le GovSec, une émanation du département américain de la Défense, a listé les secteurs qui seraient touchés les premiers en cas d'une attaque organisée sur Internet. Les circuits électriques, tout comme les télécoms, seraient déréglés, suivis du système bancaire et de l'approvisionnement en pétrole. Avant de parvenir à une paralysie du pays, avec des pompiers ou des chirurgiens hors d'état de travailler. Le pire devient possible."*[19]. En, wie weet geldt dat voor de kerninstallaties in veel landen?

Patrick Chambet geeft voorts het volgende aan: "*Le cyberterrorisme est la convergence entre le terrorisme traditionnel et les réseaux, à commencer par Internet.*

[24] In *Le Monde* 26 mai 2008, http://www.spyworld-actu.com/spip.php?article7841.

[25] Chambet Patrick, *le* cyber*terrorisme*, Edelweb - Groupe ON-X, http://www.chambet.com/publications/Cyberterrorisme.pdf.

[26] Voir *supra*.

[17] *Le Monde,* 26 mei 2008, zie http://www.spyworld-actu.com/spip.php?article7841

[18] Patrick Chambet, *Le* cyber-*terrorisme*, Edelweb – ON-X-Groep, zie http://www.chambet.com/publications/Cyberterrorisme.pdf

[19] L'Express, 6 mei 2008, zie http://www.desinfos.com/IMG/pdf/cyberguerre.pdf

l'action délibérée de destruction, de dégradation ou de modification de données, de flux d'informations ou de systèmes informatiques vitaux d'États ou d'entreprises cruciales au bon fonctionnement d'un pays, dans un but de dommages et/ou de retentissement maximum, pour des raisons politiques, religieuses ou idéologiques. Ces dommages peuvent être économiques, sociaux, environnementaux, et même vitaux pour les individus dans certains cas.[27] Il faut absolument distinguer le cyberterrorisme du simple cybercrime, qui consiste à détourner l'usage d'un système dans un but simplement crapuleux. De même, le cyberterrorisme ne doit pas être amalgamé avec le "*hacktivism*", qui est certes motivé, lui aussi, par des éléments idéologiques, mais qui cherche surtout à réveiller la société et à l'éduquer sur certains sujets, pas forcément à la détruire. Enfin, le cyber-terrorisme se distingue du cybercombat par le caractère généralement civil de ses cibles.[28] Le cyberterrorisme est en pleine expansion, grâce notamment à son coût d'accès très faible. Ensuite, nos sociétés devenant de plus en plus dépendantes des réseaux d'information, la disparition de ceux-ci peut provoquer des effets économiques, logistiques et émotionnels considérables.[29]

Les cyber-attentats ont pour but de causer un maximum de dommages et/ou un maximum de retentissement médiatique, culturel ou social. La simple défiguration ("*defacement*") de sites *Web* peu importants constitue donc à peine le premier niveau des cyberattentats. Ceux-ci consisteront plutôt à faire tomber des sites critiques ou de grande visibilité, ou à rendre inopérantes les infrastructures critiques d'un pays ou d'une organisation. On peut aussi considérer la corruption de données vitales comme un cyberattentat, puisque la confusion et la chute de confiance créées seront de nature à porter préjudice à la société. [30] Les cibles des cyberattentats seront donc constituées prioritairement par: les installations de gestion des télécommunications, les sites de génération et de distribution d'énergie, les installations de régulation des transports, les installations de distribution de produits pétroliers, les centres de gestion du courrier postal, les sites de distribution d'eau, les institutions financières et bancaires, les services d'urgence, de santé et de sécurité publique, les services gouvernementaux, les médias et les éléments symboliques d'une société et d'un mode de vie comme les enseignes de grande distribution et les industries représentatives. Une attaque sur plusieurs de ces cibles,

On peut donc définir le cyber*-terrorisme comme l'action délibérée de destruction, dégradation ou modification de données, de flux d'informations ou de systèmes informatiques vitaux d'États ou d'entreprises cruciales au bon fonctionnement d'un pays, dans un but de dommages et/ou de retentissement maximum, pour des raisons politiques, religieuses ou idéologiques. Ces dommages peuvent être économiques, sociaux, environnementaux, et même vitaux pour les individus dans certains cas. Il faut absolument distinguer le cyberterrorisme du simple cybercrime, qui consiste à détourner l'usage d'un système dans un but simplement crapuleux. De même, le cyberterrorisme ne doit pas être amalgamé avec le "*hacktivism*", qui est certes motivé lui aussi par des éléments idéologiques, mais qui cherche surtout à réveiller la société et à l'éduquer sur certains sujets, pas forcément à la détruire. Enfin, le cyberterrorisme se distingue du cybercombat par le caractère généralement civil de ses cibles*.[20]" Het cyberterrorisme is in volle opgang, onder meer dankzij de zeer lage toegangskosten. Bovendien zijn onze samenlevingen almaar meer afhankelijk van de informatienetwerken en kan het verdwijnen ervan aanzienlijke economische, logistieke en emotionele gevolgen hebben[21].

Chambet preciseert ook nog dat "*les cyberattentats [ont] pour but de causer un maximum de dommages et/ou un maximum de retentissement médiatique, culturel ou social. La simple défiguration ("*defacement*") de sites* Web *peu importants constitue donc à peine le premier niveau des cyberattentats. Ceux-ci consisteront plutôt à faire tomber des sites critiques ou de grande visibilité, ou à rendre inopérantes les infrastructures critiques d'un pays ou d'une organisation. On peut aussi considérer la corruption de données vitales comme un cyberattentat, puisque la confusion et la chute de confiance créées seront de nature à porter préjudice à la société. Les cibles des cyberattentats seront donc constituées prioritairement par: les installations de gestion des télécommunications (…), les sites de génération et de distribution d'énergie (…), les installations de régulation des transports (…), les installations de distribution de produits pétroliers (…), les centres de gestion du courrier postal (…),les sites de distribution d'eau (…), les institutions financières et bancaires (…), les services d'urgence, de santé et de sécurité publique (…), les services gouvernementaux (…), les médias (…) [et] les éléments symboliques d'une société et d'un mode de vie (grande distribution, industries*

27 Voir *supra*.
28 Voir *supra*.
29 Voir *supra*.
30 Voir *supra*.

20 Chambet Patrick, le cyberterrorisme, Edelweb – Groupe ON-X. Zie: http://www.chambet.com/publications/Cyberterrorisme.pdf, blz. 2.
21 Zie Chambet Patrick, le cyberterrorisme, Edelweb – Groupe ON-X.

simultanément, pourrait avoir un effet dévastateur pour un pays non préparé.[31]

Depuis le début des années 1990, la Chine développe ses capacités en cyberguerre. La doctrine militaire chinoise intègre la cyberattaque comme une composante de sa stratégie visant à défaire un ennemi mieux équipé ou supérieur en nombre.

Lors d'une allocution devant le congrès, le directeur de la CIA, George J. Tenet, a affirmé que la Chine cherchait à contourner l'avance technologique de l'armée américaine en utilisant la cyberguerre comme arme asymétrique. La volonté de la Chine étant de faire fi de l'obsolescence de ses chars, bateaux et avions et de se concentrer sur les failles technologiques adverses. L'armée de libération populaire a bien compris la dépendance sans cesse croissante des armées modernes vis à vis de l'informatique et de leur besoin permanent de communiquer.[32]

L'Inde a également réagi en lançant *e2Labs*, la première école indienne de lutte contre la piraterie informatique, nichée à Hyderabad, dans le centre du pays. Des experts forment, depuis 2003, au rythme de 250 par an, ceux qui devront répondre aux attaques en ligne.[33] En 1999, l'Inde se dotait d'un Institut des Technologies de l'Information et les premiers cours étaient donnés sur le campus temporaire de Hyderabad dans le but de former les étudiants aux rudiments de la cyberguerre. Dans le même temps, étaient crées trois instituts militaires délivrant un enseignement axé sur les technologies de l'information.[34] En 2002, est née l'Université de Défense Nationale (*National Defense University*) dont l'objet est la guerre de l'information et la révolution numérique. Récemment, les premier diplômés d'une licence en informatique sont sortis de cette école. Parallèlement, l'Inde a également mis au point une stratégie de cyber-guerre incluant l'assistance du secteur privé du logiciel, si cela s'avérait nécessaire. Le développement de moyens par le gouvernement indien s'expliquerait notamment par les activités offensives du Pakistan dans le domaine numérique. L'Inde s'est donné les moyens d'une réelle politique de développement informatique et a fait en sorte d'intégrer la cyber-guerre dans sa doctrine militaire. Aujourd'hui, l'Inde possède

représentatives,...). Une attaque sur plusieurs de ces cibles simultanément pourrait avoir un effet dévastateur pour un pays non préparé."[22].

In *Cyberterrorisme, mythe ou réalité*, stipt Cédric Thevenet het volgende aan:, "*Depuis le début des années 1990, la RPC développe ses capacités en cyberguerre. La doctrine militaire chinoise intègre la cyberattaque comme une composante de sa stratégie visant à défaire un ennemi mieux équipé ou supérieur en nombre.*

Lors d'une allocution devant le congrès, le directeur de la CIA, George J. Tenet, a affirmé que la Chine cherchait à contourner l'avance technologique de l'armée américaine en utilisant la cyberguerre comme arme asymétrique. La volonté de la RPC étant de faire fi de l'obsolescence de ses chars, bateaux et avions et de se concentrer sur les failles technologiques adverses. L'Armée de Libération Populaire a bien compris la dépendance sans cesse croissante des armées modernes vis à vis de l'informatique et de leur besoin permanent de communiquer."

India is niet achterwege gebleven. In *L'Express* van 6 mei 2008 heeft Guillaume Grallet daarover het volgende bericht: "*Bienvenue à e2Labs, la première école indienne de lutte contre la piraterie informatique, nichée à Hyderabad, dans le centre du pays. Sur deux étages d'un immeuble érigé dans les années 1950, des experts forment, depuis 2003, au rythme de 250 par an, (…) ceux qui devront répondre du tac au tac aux attaques en ligne*."[23] Cédric Thévenet bevestigt dat en preciseert voorts: "*En 1999, l'Inde se dotait d'un Institut des Technologies de l'Information20 et les premiers cours étaient donnés sur le campus temporaire de Hyderabad dans le but de former les étudiants aux rudiments de la cyberguerre. Dans le même temps, étaient crées trois instituts militaires délivrant un enseignement axé sur les technologies de l'information. En 2002, est née l'Université de Défense Nationale (*National Defense University*) dont l'objet est la guerre de l'information et la révolution numérique. Récemment, les premier diplômés d'une licence en informatique sont sortis de cette école. Parallèlement, l'Inde a également mis au point une stratégie de cyberguerre incluant l'assistance du secteur privé du logiciel, si cela s'avérait nécessaire. Le développement de moyens par le gouvernement indien s'expliquerait notamment par les activités offensives*

31 Voir *supra*.
32 Thevenet Cédric, Cyber*terrorisme, mythe ou réalité* in Terrorisme.net, 2005.
33 In L'Express 6 mai 2008.
34 Thevenet Cédric, Cyber*terrorisme, mythe ou réalité* in Terrorisme.net, 2005.

22 Chambet Patrick, le cyberterrorisme, Edelweb – Groupe ON-X. Zie: http://www.chambet.com/publications/Cyberterrorisme.pdf, blz. 4.
23 *L'Express*, 6 mei 2008.

un puissant réseau de programmeurs et des centres de formation, qui en font un acteur incontournable dans le monde informatique.[35]

À la différence de la guerre froide, cette nouvelle bataille n'est pas bipolaire, ni même multipolaire au sens classique. Elle offre au contraire un porte-voix inespéré aux revendications les plus minoritaires et les plus isolées. Ainsi, en Iran, plusieurs universités auraient développé un cursus afin de former des hackers de haut vol. La Corée du Nord, elle aussi, possède sa propre école de pirates: le *Mirim College*, dans la région de Hyungsan, d'où sortent une centaine de soldats chaque année. D'autres pays comme la Russie, le Pakistan ou l'Iran sont de plus en plus intéressés par ce nouveau concept et cette nouvelle manière de "faire la guerre".

Dans ce nouveau désordre du monde, les États-Unis, peut-être les plus conscients de leur retard, ont été les premiers à dégainer en créant le *Cyber Command*, une unité spécialisée dans les attaques sur Internet. Ils sont particulièrement dynamiques sur la question et se préparent même à mener des guerres sur Internet, comme en témoignent les projets de l'*US Air Force*. Ces opérations seront coordonnées grâce à la création d'un cybercommandement qui, à terme, pourrait regrouper 10 000 personnes.[36] Le cinquième terrain de bataille, après l'air, la terre, la mer et l'espace...

Pendant l'été 2002, le président Bush signait la directive présidentielle sur la sécurité nationale n° 16, ordonnant au gouvernement américain de préparer des plans nationaux de lutte électronique offensive contre des ennemis potentiels. En mars 2005, au cours d'une audience au Sénat américain, l'*US Strategic Command* (Stratcom) révélait l'existence du *Joint Functional Component Command for Network Warfare* (JFCCNW). Il s'agit d'une unité composée de hackers, au service de l'armée américaine, dont la mission prioritaire est la protection des réseaux du ministère américain de la

[35] Thevenet Cédric, Cyber*terrorisme, mythe ou réalité* in Terrorisme.net, 2005.

[36] *Un partenariat international se noue face au* cyber-*terrorisme* in le Journal du Net, 26 mai 2008.

du Pakistan dans le domaine numérique. (…) L'Inde s'est donné les moyens d'une réelle politique de développement informatique et a fait en sorte d'intégrer la cyberguerre dans sa doctrine militaire. Aujourd'hui, l'Inde possède un puissant réseau de programmeurs et des centres de formation qui en font un acteur incontournable dans le monde informatique."[24].

In tegenstelling tot de Koude Oorlog is die nieuwe veldslag niet bipolair en zelfs niet multipolair in de traditionele zin. Hij biedt daarentegen een onverhoopt forum voor de meest minoritaire en geïsoleerde eisen. In *L'Express* van 6 mei 2008 stond, van de hand van Guillaume Graillet, het volgende bericht te lezen: "*En Iran, plusieurs universités auraient développé un cursus afin de former des hackers de haut vol. La Corée du Nord, elle aussi, possède sa propre école de pirates: le Mirim College, dans la région de Hyungsan, d'où sortent une centaine de soldats chaque année*."[25] Andere landen, zoals Rusland, Pakistan of Iran, hebben almaar meer belangstelling voor dat nieuwe concept en voor die nieuwe manier van "oorlogvoering".

In die "nieuwe wereldwanorde" waren de Verenigde Staten, die zich wellicht meer van hun achterstand bewust waren, de eerste om zich defensief op te stellen, door de oprichting van *Cyber Command*, een in cyberaanvallen gespecialiseerde eenheid. De Verenigde Staten zijn aangaande dit vraagstuk bijzonder dynamisch en bereiden zich zelfs voor op oorlogvoering via het internet, zoals blijkt uit *US Air Force*-projecten. Die operaties zullen worden gecoördineerd dankzij de oprichting van een cybercommando, dat uiteindelijk meer dan 10 000 mensen zou kunnen groeperen[26]: het vijfde strijdtoneel, na de lucht, het land, de zee en de ruimte.

Tijdens de zomer van 2002 tekende president Bush presidentiële richtlijn nr. 16 over de nationale veiligheid, waarbij de Amerikaanse regering gelast werd nationale plannen voor te bereiden in verband met de offensieve elektronische bestrijding van potentiële vijanden. In maart 2005 onthulde het *US Strategic Command* (STRATCOM) tijdens een hoorzitting in de Amerikaanse Senaat het bestaan van de *Joint Functional Component Command for Network Warfare* (JFCCNW). Het gaat om een eenheid bestaande uit hackers, die werkt in dienst van het Amerikaanse leger, met als prioritaire taak de

[24] Thevenet Cédric, Cyber*terrorisme, mythe ou réalité* in Terrorisme.net, 2005. Zie: http://www.terrorisme.net/pdf/2006_Thevenet.pdf, blz. 16-17.

[25] *L'Express*, 6 mei 2008.

[26] "*Un partenariat international se noue face au* cyber-*terrorisme*" in "Journal du Net", 26 mei 2008.

défense, mais également une participation active au CNA.[37]

Le 30 janvier 2010, le chef de l'agence des télécommunications de l'ONU, Hamadoun Touré a insisté, au Forum de Davos, sur le fait que le monde avait besoin d'un traité pour se défendre des "cyberattaques" avant qu'elles ne se transforment en "cyberguerre" ou "guerre sur internet".

Il a proposé un accord international, dont la structure "*ressemblerait à un traité de paix avant une guerre*". Les pays doivent protéger leurs citoyens et leur droit d'accès à l'information, promettre de ne pas abriter les cyberterroristes et devraient "*s'engager à ne pas en attaquer un autre*", a dit John Negroponte, directeur des services de renseignement américains dans l'administration de George W. Bush. Il a cependant estimé que les agences de renseignement dans les principaux pays seraient les premières à "*exprimer des réserves*" sur un tel projet. Susan Collins, une sénatrice républicaine qui siège dans les commissions de la Défense et de l'Intérieur au Sénat américain, a estimé que la perspective qu'une attaque sur internet déclenche une guerre est désormais prise en considération par les États-Unis.[38]

La Belgique est également consciente de ce risque. En effet, dans notre pays, c'est le SGRS (Service de renseignement militaire) qui a pour mission principale de rechercher, d'analyser et de traiter le renseignement relatif à toute menace pour l'intégrité du territoire national, les plans de défense militaire, l'accomplissement des missions des forces armées ou la sécurité des ressortissants belges à l'étranger. Le SGRS veille également à la sécurité du personnel relevant de la Défense, des installations et des secrets militaires et du potentiel scientifique et économique. Il doit par ailleurs neutraliser d'éventuelles cyberattaques et en identifier les auteurs. L'un des auteurs de la présente proposition de résolution a d'ailleurs interpellé, lors de la législature 52, le ministre de la Défense sur le rôle du SGRS et le

bescherming van de netwerken van het Amerikaanse ministerie van defensie, maar ook een actieve deelname aan *Computer Network Attack*[27].

Op 30 januari 2010 benadrukte dr. Hamadoun Touré, secretaris-generaal van de Internationale Telecommunicatie Unie (VN), in Davos dat de wereld een verdrag nodig heeft om zich te kunnen verdedigen tegen cyberaanvallen alvorens die evolueren tot een "cyberoorlog" of "oorlog op het internet."

Hij stelde een internationale overeenkomst voor, waarvan de structuur "*would look like a peace treaty before a war*". De landen moeten hun burgers beschermen, alsook hun recht op toegang tot informatie, moeten beloven geen cyberterroristen onderdak te bieden en "*should commit themselves not to attack another*". John Negroponte, directeur van de Amerikaanse inlichtingendiensten onder George W. Bush, vond echter dat de inlichtingendiensten in de grote landen de eersten zouden zijn "*to express reservations*" over een dergelijk akkoord. Susan Collins, een Republikeinse senator die zitting heeft in de commissies defensie en binnenlandse zaken van de Amerikaanse Senaat, merkte op dat de Verenigde Staten voortaan rekening houden met het vooruitzicht dat een cyberaanval een oorlog kan ontketenen[28].

België is zich ook van dat risico bewust. Bij ons heeft de (militaire) Algemene Dienst Inlichting en Veiligheid (ADIV) als eerste taak "het inwinnen en analyseren van inlichtingen die betrekking hebben op elke activiteit die de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen, de vervulling van de opdrachten van de strijdkrachten, of de veiligheid van de Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen. Daarnaast moet deze dienst zorgen voor de militaire veiligheid van personeel dat afhangt van Defensie, van militaire installaties en geheimen en van het wetenschappelijk en economisch potentieel. De dienst moet daarenboven eventuele cyberaanvallen neutraliseren en de daders identificeren". Een van de indieners van dit voorstel van resolutie heeft overigens

[37] Thevenet Cédric, Cyberterrorisme, mythe ou réalité "Terrorisme.net, Série Mémoires et Thèses", 2005 (http://www.terrorisme.net/pdf/2006_Thevenet.pdf).

[38] François Raffenne, Le débat stratégique américain, 2007, I.F.R.I, (http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWT-bqYSg1Ws4l4yAA).

[27] Thevenet Cédric, "Cyber*terrorisme, mythe ou réalité*" in "Terrorisme.net, Série Mémoires et Thèses", 2005 (http://www.terrorisme.net/pdf/2006_Thevenet.pdf).

[28] François Raffenne, *Le débat stratégique américain*, 2007, I.F.R.I.,en AFP, persbericht van 30 januari 2010 (http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWT-bqYSg1Ws4l4yAA).

risque de diminution de ses budgets de fonctionnement, au vu des missions dont il avait la charge.[39]

Le 2 juin 2010, une conférence s'est tenue à Bucarest afin d'examiner le rôle que doit jouer l'OTAN dans la défense contre les cyberattaques. Cet événement s'inscrivait dans le cadre de l'élaboration du nouveau concept stratégique de l'Alliance. Plus de 100 participants représentant des sociétés informatiques de premier plan, le secteur bancaire, le secteur du renseignement, l'OTAN, l'Union européenne et d'autres institutions, ont pris part à cette conférence, intitulée "*La* cyber*défense dans le contexte du nouveau concept stratégique de l'OTAN*". Ils ont débattu du caractère impérieux de la cybersécurité et des défis que celle-ci pose pour la communauté internationale au sens large, y compris pour les pays de l'OTAN. Selon le rapport du Groupe d'experts sur le nouveau concept stratégique de l'OTAN, les cyberattaques dirigées contre les systèmes modernes de communication constitueront l'une des menaces les plus probables pour les alliés dans les dix ans à venir.

Ce rapport formule la recommandation suivante: *"L'OTAN doit accélérer ses efforts face au danger de* cyber*attaques, en protégeant ses propres systèmes de communication et de commandement, en aidant les Alliés à mieux pouvoir prévenir et se relever de telles attaques, et en mettant au point toute une gamme de moyens de* cyber*défense pour une détection et une dissuasion efficaces."* [40]

Le 4 août 2010, une nouvelle division a été créée au sein du Secrétariat international de l'OTAN pour faire face à un éventail grandissant de risques et de défis non traditionnels. La nouvelle Division Défis de sécurité émergents a commencé ses travaux début août: elle mettra en particulier l'accent sur le terrorisme, la prolifération des armes de destruction massive, la cyberdéfense et la sécurité énergétique. Avec cette nouvelle division, l'OTAN se dote en outre d'une capacité d'analyse stratégique qui lui permettra de suivre et d'anticiper les développements internationaux qui pourraient avoir des incidences sur la sécurité de l'Alliance. La création de la Division Défis de sécurité émergents souligne la volonté de placer les défis de sécurité nouveaux et non traditionnels au cœur des préoccupations de l'Alliance.

tijdens de 52e zittingsperiode de minister van Landsverdediging geïnterpelleerd over de rol van de ADIV en het risico van een vermindering van de werkingsbegroting, in het licht van de taken waarvoor hij verantwoordelijk is [29].

Op 2 juni 2010 werd in Boekarest met de steun van de NAVO een conferentie gehouden om te onderzoeken welke haar rol in de verdediging tegen cyberaanvallen is. Die conferentie maakte deel uit van de ontwikkeling van het nieuwe strategische concept van de Alliantie. Meer dan 100 deelnemers uit toonaangevende informaticaondernemingen, de banksector, de inlichtingensector, de NAVO zelf, de Europese Unie en andere instellingen namen deel aan die conferentie, met als thema "Cyber *Defence in the Context of the New NATO Strategic Concept*". Zij bespraken er de dringende aard van de cyberveiligheid en de uitdagingen ervan voor de internationale gemeenschap in het algemeen, inclusief voor de NAVO-landen. Volgens het rapport van de groep van experts over het nieuwe strategische concept van de NAVO zullen de cyberaanvallen tegen de moderne communicatiesystemen in het komende decennium voor de geallieerden een van de meest waarschijnlijke bedreigingen vormen.

Dat rapport doet de volgende aanbeveling: "*NATO must accelerate efforts to respond to the danger of* cyber *attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of* cyber *defence capabilities aimed at effective detection and deterrence*".

Op 4 augustus 2010 wordt in de NAVO-"*International Staff*" een nieuwe afdeling opgericht om aan een groeiend aantal risico's en niet-traditionele uitdagingen het hoofd te bieden. De nieuwe "*Emerging Security Challenges division"* (ESCD) begon haar werkzaamheden begin augustus: zij zal vooral focussen op terrorisme, de proliferatie van massavernietigingswapens, cyberverdediging en energiezekerheid. Met deze nieuwe afdeling beschikt de NAVO nu over "*Strategic Analysis Capability*"die haar in staat zal stellen zicht te krijgen op de internationale ontwikkelingen die op de veiligheid van de Alliantie een weeslag zouden kunnen hebben. De oprichting van de ESCD onderstreept de vastberadenheid om nieuwe, niet-traditionele veiligheidsuitdagingen bij de Alliantie centrale aandacht te geven.

[39] Question orale de Denis Ducarme au ministre de la Défense, 14 mai 2008, question 5231(CRIV 52 COM 209).

[40] http://www.nato.int/cps/fr/SID-BC09BDE7-7157D286/natolive/news_64088.htm?mode=news

[29] http://www.comiteri.be/index.php?option=com_content&task=view&id=53&Itemid=0&phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb&lang=NL en mondelinge vraag van de heer Denis Ducarme van 14 mei 2008 aan de minister van Landsverdediging over "de ADIV" (nr. 5231) (CRIV 52 COM 209).

Lors d'une conférence sur les cyberconflits, qui s'est tenue au Centre d'excellence pour la cyberdéfense en coopération (CCD-COE) à Tallinn (Estonie) le 15 juin 2010, le président estonien Toomas Hendrik Ilves a de nouveau déclaré que si les cyberattaques dont certains pays ont été victimes avaient été menées avec des armes cinétiques, *"nous aurions été à l'OTAN confrontés à une situation relevant au minimum de l'article 4 et, plus vraisemblablement, de l'article 5."*.

Évoquant la vulnérabilité aux cyberattaques des sociétés ouvertes, il a insisté sur la nécessité d'une approche multinationale, car la plupart des infrastructures critiques sont elles-mêmes multinationales. Il a ajouté que nous devons assurer *"la résilience de nos infrastructures critiques qui dépendent des réseaux informatiques"*, afin de les protéger le plus possible d'une attaque éventuelle.[41] Le lien devient de fait plus étroit que jamais entre la sécurité informatique et la sécurité nationale. Le CCD COE a été créé en 2008 en vue de renforcer la capacité de cyberdéfense de l'OTAN. Il est actuellement parrainé par l'Estonie, la Lettonie, la Lituanie, l'Allemagne, l'Italie, la République slovaque et l'Espagne. Si la coopération au niveau de l'OTAN est indispensable, il conviendrait que chaque pays de l'OTAN définisse une approche nationale de la cybersécurité englobant la totalité des acteurs importants.

La société de sécurité internet *McAfee* a fait savoir, au cours d'un débat lors du forum de Davos, le 29 janvier 2010, que la Chine, les États-Unis, la Russie, Israël et la France figurent parmi les vingt pays engagés dans une course aux "cyberarmes" et qu'ils se préparent à de possibles hostilités sur Internet.[42] Les conflits actuels étant de plus en plus accompagnés par des attaques informatiques, la menace du cyberterrorisme doit maintenant être intégrée à toute politique de sécurité. Les principes de défense à appliquer sont ceux de la sécurité des systèmes d'information en général: vous avez entre les mains une excellente source de référence pour cela.[43] Il faut donc travailler sur les concepts de défense en profondeur, coupler la sécurité organisationnelle et la sécurité logique, sans oublier la sécurité physique. Attaques, contre-attaques, blocages, opérations de sabotage, espionnage qui ne dit pas son nom... Sur

Op een conferentie over cyberconflicten, gehouden in het "*Cooperative* Cyber *Defence Centre of Excellence*" (CCD COE) in Tallinn (Estland), heeft de Estse president Toomas Hendrik Ilves op 15 juni 2010 verklaard dat mochten de cyberaanvallen waarvan sommige landen het slachtoffer waren geweest, met kinetische wapens hebben plaatsgehad, "*we in NATO would [have been] faced minimally with an Article 4 and most likely with an Article 5 scenario*"[30].

Erop wijzend dat de open samenleving kwetsbaar is voor cyberaanvallen, beklemtoont hij de nood aan een multinationale aanpak, omdat de meeste belangrijke infrastructuren zelf multinationaal zijn. Hij voegde eraan toe dat "*we need to make our computer-dependent critical infrastructure resilient"*, om die infrastructuur in de mate van het mogelijke tegen een eventuele aanval te beschermen[31]. De relatie tussen de *e-security* en de nationale veiligheid wordt in de praktijk nauwer dan ooit. De *Cooperative* Cyber *Defence Centre of Excellence (CCD COE)* werd in 2008 opgericht om de NAVO-slagkracht inzake cyberverdediging te verhogen. Momenteel wordt het centrum mede ondersteund door Estland, Letland, Litouwen, Duitsland, Italië, de Republiek Slovakije en Spanje. Hoewel de NAVO-lidstaten in NAVO-verband moeten samenwerken, moet elke lidstaat een nationaal cyberveiligheidsbeleid ontwikkelen, dat rekening houdt met alle belangrijke actoren.

De internetbeveiligingsfirma McAfee deelde tijdens een debat op een forum in Davos op 29 januari 2010 mee dat China, de Verenigde Staten, Rusland, Israël en Frankrijk tot de twintig landen behoren die verwikkeld zijn in een cyberwapenwedloop, en dat zij zich voorbereiden op mogelijke vijandelijkheden op het internet[32]. Patrick Chambet noteert in dat verband het volgende: *"Les conflits actuels étant de plus en plus accompagnés par des attaques informatiques, la menace du cyberterrorisme doit maintenant être intégrée à toute politique de sécurité. Les principes de défense à appliquer sont ceux de la sécurité des systèmes d'information en général: vous avez entre les mains une excellente source de référence pour cela. Il faut donc travailler sur les concepts de défense en profondeur, coupler la sécurité organisationnelle et la sécurité logique, sans oublier la sécurité physique."*[33]

41 http://www.nato.int/cps/fr/SID-AA04B2D5-E730CDD2/natolive/news_64615.htm?mode=news..

42 In Actualités de la Fondation, Prometheus 1er février 2010

43 Chambet Patrick, *le* cyber*terrorisme*, Edelweb – Groupe ON-X.

30 NAVO, persberichten van 2 juni 2010 (http://www.nato.int/cps/en/SID-BC09BDE7-7157D286/natolive/news_64088.htm?mode=news), 4 augustus 2010 (http://www.nato.int/cps/en/natolive/news_65107.htm) en 15 juni 2010 (http://www.nato.int/cps/en/SID-E8EDFEB7-EE5C1752/natolive/news_64615.htm).

31 http://www.nato.int/cps/fr/SID-AA04B2D5-E730CDD2/natolive/news_64615.htm?mode=news.

32 In *Actualités de la Fondation*, *Prometheus* , 1 februari 2010.

33 Chambet Patrick, *Le* cyber*terrorisme*, Edelweb – Groupe ON-X.

Internet, de nouvelles formes de conflits se développent à profusion, avec le risque de paralyser l'ensemble des services d'un pays. Une extension des champs de bataille dans le monde virtuel, que les États ne peuvent plus ignorer.[44] Le cyberterrorisme a parfois été qualifié de terrorisme sans mort. Cela pourrait changer à l'avenir car, d'ores et déjà, Internet apparaît comme le nouveau champ de bataille planétaire.[45]

Denis DUCARME (MR)
David CLARINVAL (MR)

"Attaques, contre-attaques, blocages, opérations de sabotage, espionnage qui ne dit pas son nom... Sur Internet, de nouvelles formes de conflits se développent à profusion, avec le risque de paralyser l'ensemble des services d'un pays. Une extension des champs de bataille dans le monde virtuel, que les États ne peuvent plus ignorer."[34]*. "Le cyberterrorisme a parfois été qualifié de terrorisme sans mort. Cela pourrait changer à l'avenir"* [35]*,* want "*d'ores et déjà, Internet apparaît comme le nouveau champ de bataille planétaire."*[36]*.*

44 In *L'Express* 6 mai 2008.
45 In *L'Express* 6 mai 2008.

34 In *L'Express*, 6 mei 2008.
35 Chambet Patrick, *Le* cyber*terrorisme*, Edelweb – Groupe ON-X.
36 In *L'Express*, 6 mei 2008.

PROPOSITION DE RÉSOLUTION

La Chambre des representants,

A. considérant l'importance de mener une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

B. considérant les profondes mutations engendrées par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

C. considérant les risques accrus que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et l'importance que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

D. considérant l'importance de prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en prévoyant l'incrimination de ces comportements, et l'attribution de pouvoirs suffisants aux organes de lutte contre la cybercriminalité, pour permettre une lutte efficace contre ces infractions, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

E. considérant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

F. vu le Pacte international relatif aux droits civils et politiques des Nations Unies, adopté en 1966;

G. vu la Convention sur la cybercriminalité du Conseil de l'Europe, adoptée à Budapest le 23 novembre 2001;

H. vu la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe, adoptée en 1950;

I. vu la Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op het belang een gemeenschappelijk strafbeleid te voeren om de samenleving te beschermen tegen cybercriminaliteit, meer bepaald door een passende wetgeving aan te nemen en de internationale samenwerking te verbeteren;

B. gelet op de diepgaande wijzigingen die worden veroorzaakt door de digitalisering, de convergentie en de permanente mondialisering van de computernetwerken;

C. gelet op het toegenomen risico dat de computernetwerken en de elektronische gegevens tevens worden aangewend om strafbare feiten te plegen, alsook op het belang dat de bewijzen van die strafbare feiten worden opgeslagen en overgezonden via die netwerken;

D. gelet op het belang te voorkomen dat handelingen worden gesteld die afbreuk doen aan de vertrouwelijkheid, de integriteit en de beschikbaarheid van de computersystemen, de netwerken en de gegevens, alsook dat soortgelijke systemen, netwerken en gegevens frauduleus worden gebruikt, door die handelingen strafbaar te stellen en de organen ter bestrijding van de cybercriminaliteit voldoende bevoegdheden te verlenen, opdat zij die misdrijven efficiënt kunnen bestrijden, en door de opsporing, het onderzoek en de vervolging, zowel nationaal als internationaal, te vergemakkelijken, alsook door te voorzien in materiële bepalingen met het oog op een snelle en betrouwbare internationale samenwerking;

E. stipt aan dat voor een doeltreffende bestrijding van cybercriminaliteit een versterkte, snelle en goed functionerende internationale samenwerking in strafzaken vereist is;

F. onder verwijzing naar het Internationaal VN-Verdrag inzake burgerrechten en politieke rechten, aangenomen in 1966;

G. onder verwijzing naar het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, aangenomen in Boedapest op 23 november 2001;

H. gelet op het Verdrag van de Raad van Europa tot bescherming van de rechten van de mens en de fundamentele vrijheden, aangenomen in 1950;

I. onder verwijzing naar het Verdrag van de Raad van Europa tot bescherming van personen met betrekking

du traitement automatisé des données à caractère personnel;

J. considérant le traité de Lisbonne, en particulier ses dispositions relatives à l'espace de liberté, de sécurité et de justice (ci-après "l'ELSJ") et son nouveau cadre juridique relatif à la protection des droits fondamentaux et au renforcement de la citoyenneté européenne, les articles 2, 6 et 7 du traité sur l'Union européenne modifié par le traité de Lisbonne, le protocole n° 8 annexé au traité sur le fonctionnement de l'Union européenne (TFUE), introduit par le traité de Lisbonne, sur l'adhésion de l'Union à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après "CEDH"), ainsi que la Charte des droits fondamentaux de l'Union européenne, qui a la même valeur juridique que les traités;

K. considérant la communication publiée le 10 juin 2009 sous le titre "Un espace de liberté, de sécurité et de justice au service des citoyens" (COM(2009)0262), dans laquelle la Commission expose ses priorités à l'égard de l'ELSJ pour la période 2010-2014, de même que son évaluation du programme et du plan d'action de La Haye (COM(2009)0263) et le tableau de mise en œuvre afférent (SEC(2009)0765), ainsi que les contributions des parlements nationaux, de la société civile et des organes et agences de l'Union européenne;

L. considérant le projet de document de la Présidence du Conseil du 16 octobre 2009 intitulé "Le programme de Stockholm — une Europe ouverte et sûre au service des citoyens", publiée au JOC n°115 du 4 mai 2010,

M. considérant que, dans de nombreux domaines de la justice et des affaires intérieures, les solutions nationales ne suffisent plus, raison pour laquelle il est nécessaire d'élaborer des réponses européennes aux défis internationaux en matière d'immigration, de sécurité et de technologies, y compris les technologies de l'information et de la communication;

N. vu la résolution du Parlement européen sur la communication de la Commission au Parlement européen et au Conseil — un espace de liberté, de sécurité et de justice au service des citoyens — programme de Stockholm (RSP/2009/2534);

O. vu la loi du 13 juin 2005 relative aux communications électroniques;

tot de geautomatiseerde verwerking van persoonsgegevens, aangenomen op 28 januari 1981;

J. gelet op het Verdrag van Lissabon, met name de bepalingen aangaande de ruimte van vrijheid, veiligheid en rechtvaardigheid ("de RVVR") en het nieuwe juridische kader dat dit Verdrag biedt voor de bescherming van de fundamentele rechten en de versterking van het burgerschap van de Unie, de artikelen 2, 6 en 7 van het Verdrag betreffende de Europese Unie, gewijzigd bij het Verdrag van Lissabon, Protocol nr. 8 bij het Verdrag betreffende de werking van de Europese Unie (VWEU), ingevoegd bij het Verdrag van Lissabon, betreffende de toetreding van de Unie tot het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden ("het EVRM"), en het Handvest van de grondrechten van de Europese Unie, dat dezelfde juridische waarde heeft als de Verdragen;

K. onder verwijzing naar de mededeling van de Commissie van 10 juni 2009 "Een ruimte van vrijheid, veiligheid en recht ten dienste van de burger" (COM(2009)0262), waarin zij haar prioriteiten in de RVVR voor de periode 2010-2014 uiteenzet en ook een evaluatie geeft van het Haags programma en het actieplan (COM(2009)0263) en het daarmee samenhangende implementatiescorebord (SEC(2009)0765), alsook gezien de bijdragen van de nationale parlementen, de maatschappelijke organisaties en de EU-agentschappen en -organen;

L. gelet op "Het programma van Stockholm — een open en veilig Europa ten dienste van de burger", het ontwerpdocument van het voorzitterschap van de Raad van 16 oktober 2009, bekendgemaakt in het Europees Publicatieblad nr. 115 van 4 mei 2010;

M. overwegende dat op veel beleidsterreinen van justitie en binnenlandse zaken nationale oplossingen niet langer toereikend zijn en dat het daarom noodzakelijk is te komen tot Europese antwoorden op de internationale uitdagingen van migratie, veiligheid en technologie, met inbegrip van informatie- en communicatietechnologie;

N. onder verwijzing naar de Resolutie van het Europees Parlement van 25 november 2009 over de mededeling van de Commissie aan het Europees Parlement en de Raad — Een ruimte van vrijheid, veiligheid en recht ten dienste van de burger — programma van Stockholm (RSP/2009/2534);

O. gelet op de wet van 13 juni 2005 betreffende de elektronische communicatie;

P. considérant le développement du nouveau concept stratégique de l'OTAN;

Q. vu le sommet de l'OTAN tenu à Lisbonne en 2010, ayant placé la cybersécurité au premier rang des nouveaux défis de sécurité;

DEMANDE AU GOUVERNEMENT:

d'appuyer l'idée que l'OTAN définisse les cyberattaques comme un acte de guerre à part entière;

6 juillet 2010

Denis DUCARME (MR)
David CLARINVAL (MR)

P. in het licht van de ontwikkeling van het nieuw strategisch concept van de NAVO;

Q. gelet op de in 2010 georganiseerde NAVO-Top van Lissabon, waarbij cyberveiligheid bovenaan de lijst van de nieuwe uitdagingen op het stuk van veiligheid werd gezet;

VERZOEKT DE REGERING:

het idee te steunen dat de NAVO cybercriminaliteit zou definiëren als een volwaardige oorlogsdaad;

6 juli 2010

Imprimerie centrale – Cette publication est imprimée exclusivement sur du papier certifié FSC
Centrale drukkerij – Deze publicatie wordt uitsluitend gedrukt op FSC gecertificeerd papier