De Minister van Justitie

TOESPRAAK
(2 december 2014 - NL/FR)

Belgian Intelligence Studies Centre – Building Belgium's Cyber intelligence Knowledge Capacity

---

Geachte heren en dames diensthoofden,

Leden van de veiligheids-, inlichtingen- en politiediensten, en van de toezichtsorganen,

Professoren en academische onderzoekers,

Heren en dames journalisten,

Alsook elk andere aanwezige geïnteresseerd in de boeiende materie van de cyberveiligheid,

Malware, botnets, phishing. De terminologie en de wegen van de cyberspace zijn, zeker voor iemand van mijn generatie, complex en

vaak onbegrijpelijk. Gelukkig zijn ze voor jullie en jullie respectievelijke diensten en organisaties, niet ondoorgrondelijk.

De kansen die cyberspace biedt, niet alleen voor legale, maar in toenemende mate ook voor illegale activiteiten, zijn niet onopgemerkt gebleven. België en zijn burgers zijn de voorbije jaren en maanden meermaals slachtoffer geweest van cyberincidenten. Criminelen wenden in toenemende mate het internet aan om hun actieterrein uit te breiden. Ook de enorme datacaptatie van sommige buitenlandse mogendheden, niet enkel om hun veiligheidsomgeving maar ook om hun economische positie te verhogen en te verstevigen, is mij en de gehele regering niet ontgaan.

Geen enkele democratische rechtsstaat kan dit toelaten. Hoewel België op vlak van het bestrijden van cyberincidenten nog veel werk voor de boeg heeft, zie ik wel redenen voor optimisme en vooruitgang.

Eén : de bewustwording van burgers en overheid voor de gevaren van cyberspace neemt stap per stap toe. Dit is belangrijk want het zorgt ervoor dat de weerbaarheid van de maatschappij tegen dergelijk type van bedreigingen toenemen.

Twee : ik heb het voornemen om het wettelijk instrumentarium ter bestrijding van cyberincidenten aan te passen en uit te breiden. Het strafrechtelijk en politioneel kader moet worden uitgebreid aan de noden terzake. Ook de wetgeving van toepassing op de inlichtingen- en veiligheidsdiensten laat ruimte voor verbetering en modernisering.

Drie : het feit dat de publieke, private en academische sector elkaar vinden in een gemeenschappelijk belang.

1. Prise de conscience

Le sentiment que les incidents-cyber portent atteinte à la société belge est *fortement* ancré chez le citoyen et le pouvoir public. Le seul point positif aux nombreux et souvent graves incidents-cyber qui ont eu lieu en Belgique ces dernières années, est la prise de conscience chez les politiciens et les citoyens que ce type de danger a augmenté de façon de façon exponentielle.

Le pouvoir public a réagi sur ce point. Comme vous le savez, l'accord gouvernemental contient un volet séparé sur la cyber-sécurité avec la ferme intention d'opérationnaliser le Centre pour la "Cybersecurité belge" (CCSB). Cela a d'ailleurs été récemment reconfirmé par notre Premier Ministre à la Chambre des Représentants. Ce centre jouera un rôle central de coordination dans la façon de relever les défis liés à la cybersécurité en Belgique.

Nous devons également profiter de la vigilance accrue de nos citoyens. Toutes vos instances constatent continuellement le nombre croissant de communications sur des cyberincidents, mais chacun a conscience que le nombre effectif de ces incidents est beaucoup plus élevé.

"Mesurer" est encore toujours la base du savoir et le crime ne peut être combattu que lorsqu'il est effectivement dénoncé. C'est pour cette raison que tout le monde doit être sensibilisé afin de signaler réellement les incidents aux instances compétentes.

Fedict, CERT, ADIV, VSSE, FCCU, ADCC, het BIPT, BelNIS…. L'embarras du choix. Beaucoup d'instances, chacune avec ses propres spécialités et qualités. Les entreprises, les citoyens individuels et souvent aussi les instances publiques ne savent pas qui contacter en cas d'incidents « cyber », ni a fortiori connaître la législation sur la cyber-sécurité.

L'information et la sensibilisation de nos citoyens, afin de les orienter vers les instances adéquates pour obtenir une aide, une enquête et d'éventuelles poursuites judiciaires, sont une responsabilité commune.

La déclaration et l'enregistrement correct de cyberinfractions devra, en effet, devenir un automatisme pour les citoyens et le pouvoir public.

2. Aanpassing wettelijk instrumentarium

De wittebroodsweken van het internet zijn voorbij. Naast de klassieke dreigingen en delicten hebben de cyberdreigingen en -delicten duidelijk hun digitale weg gevonden.

Hierbij mogen we niet vergeten dat achter de binaire codes, de pishing mails of de spyware personen, groeperingen of zelfs landen zitten. Cyberveiligheid is namelijk meer dan zich louter verdedigen tegen nullen en ééntjes. Elke veiligheidsinbreuk is de verantwoordelijkheid van een bepaald individu of entiteit of deze zich nu in Poelkapelle, Shanghai of São Paulo bevindt.

Ons doel moet er dan ook vooreerst in bestaan deze individuen en entiteiten te detecteren en te identificeren. Elk cyberonderzoek – of

dit nu gerechtelijk is of zich bevindt binnen het domein van de intelligence – is in essentie een zoektocht naar informatie. Hierbij kent de digitale wereld vanzelfsprekend haar eigen technische logica, maar berust het evenzeer op vertrouwde technieken als fysieke surveillance, forensisch onderzoek, getuigenissen en het, met gerechtelijke toestemming, afluisteren en opnemen van privécommunicatie. Het goede nieuws is dat de kennis en kunde van de overheid in cyberonderzoek aanwezig is en zich in stijgende lijn bevindt.

Eens de detectie en identificatie is gebeurd moet er een duidelijke strategie zijn die zowel het individuele geval alsook het fenomeen op zich moet beheersen en bestrijden. Wat de individuele gevallen betreft moet de via cyberonderzoek ingewonnen en geanalyseerde informatie de gerechtelijke actoren helpen in hun strijd tegen strafinbreuken. Wat betreft het strategisch niveau moeten fenomeenanalyses terzake de bevoegde beleidsverantwoordelijken ondersteunen in het bepalen van de noodzakelijke prioriteiten en intenties binnen dit domein. Op beide niveaus moet de reactie effectief en efficiënt zijn, logischerwijze met respect voor onze fundamentele waarden en grondrechten.

Zowel bij de fase van de detectie en identificatie als bij de fase van de beheersing en bestrijding hoop ik u te kunnen helpen. U weet dat één van mijn prioriteiten als minister van Justitie bestaat uit de modernisering van ons strafrechtelijk kader. Ook de wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, de zogenaamde BIM-wet, wordt aangepast. Het cybergebeuren zal hierin zeker zijn plaats krijgen.

3. Samenwerking tussen publieke, private en academische actoren

Laat me ten slotte afsluiten met het enorme belang te onderstrepen van een goede samenwerking tussen de overheid, de privésector en de academische wereld.

Naast de vermelde kennis en kunde bij de overheid, is er een belangrijk segment binnen de privésector die bedreven is in het detecteren, identificeren en beheersen van cyberdreigingen als tevens in het preventief beveiligen van informatica-infrastructuren opdat ze

afdoende beschermd zouden zijn tegen mogelijke cyberinbreuken en –aanvallen.

A côté de ces entreprises privées, nos universités et nos écoles d'enseignement supérieur disposent également de ces connaissances et de ce savoir-faire. Les deux développent du matériel et du logiciel qui ont de l'importance pour la cyber-sécurité et le « cyber-intelligence ». Toutes construisent des réseaux et provoquent les développements technologiques.

Il serait donc regrettable que le pouvoir public, le secteur privé et le monde académique n'unissent pas leurs efforts. Le défi est de créer des rapports de collaboration efficaces. Dans cette optique, je ne peux que me réjouir de ce qu'on appelle la "Cyber Security Coalition". Vos recommandations sont plus que bienvenues et j'espère que vous trouverez dans le pouvoir public un partenaire fiable et bienveillant.

Partager l'information doit nous mettre dans une position permettant de prévenir de futures cyberagressions et de réagir de façon adéquate

sur les différentes cybermenaces. La mise en commun de l'information publique et privée est dans l'intérêt de tous et doit nous aider à nous faire une idée de toutes les cybermenaces car nous disposons dans notre pays des compétences nécessaires. L'expertise en matière de cybersécurité existe ainsi que la volonté du pouvoir public et privé de travailler ensemble et de partager les informations.

Ik maak me natuurlijk geen illusies. We staan aan het begin van een lange strijd. Criminelen, of ze nu individuen zijn of ondersteund worden door staten, zullen altijd zoeken naar de zwakke punten in onze informatica-infrastructuur. Ons enige antwoord hierop moet bestaan uit het betrekken van de hele samenleving bij het domein cyberveiligheid.

Thank you
