# Markt en overheid samen ten strijde in cyberspace

**Overheid en bedrijfsleven hebben elkaar nodig, nu er een oorlog gevoerd wordt in cyberspace. Cybersecurity leent zich uitstekend voor strategische samenwerking, omdat voor een krachtig antwoord gebundelde expertise en informatie nodig zijn. Markt en overheid hebben immers met dezelfde cyberdreigingen te maken.**

President Obama ondertekende onlangs een 'executive order' die ervoor moet zorgen dat de publieke en de private sector meer samenwerken in cybersecurity. Hij deed dit op de Summit on Cybersecurity and Consumer Protection, die mede tot doel had om publiek en privaat te verenigen. Ongeveer rond dezelfde tijd kondigde Facebook een netwerk voor security experts aan om informatie te delen, ThreatExchange, waar inmiddels ook onder meer Yahoo en Pinterest aan meedoen. Samenwerken en kennis delen lijken sleutelwoorden voor het voeren van deze strijd in cyberspace, zoals ook wordt onderkend in de Nederlandse Nationale Cyber Security Strategie 2 (NCSS2).

**Dreiging vanuit cyberspace raakt ons allemaal**

De dreiging vanuit cyberspace is groeiende, zodanig zelfs dat specialisten spreken van een cyberwar. Omdat die zich afspeelt in de 'onzichtbare' wereld van netwerken en computers, is de maatschappij zich echter niet altijd van deze oorlog bewust. "We hebben het hier niet over een DDoS-aanval waardoor de dienstverlening even uitvalt. Het vraagstuk neemt in omvang en kwaadaardigheid toe, zodanig dat je inmiddels kunt spreken van een 'cyberbattlefield' met grootschalige aanvallen op kritische infrastructuur", zegt Jaap Schekkerman, Director Global Cyber Security en Thought Leader Cyber Security bij CGI. Hij noemt een aantal incidenten. Zo werd in december vorig jaar ternauwernood een ontploffing van een ijzersmelterij in Duitsland voorkomen. Cyberaanvallers hadden de software van de hoogoven overgenomen, waardoor deze niet meer was af te sluiten. In 2008 werd er een oliepijpleiding in Turkije opgeblazen, onlangs werd pas openbaar dat dit het gevolg was van een cyberaanval. Het conflict in Oekraïne kent een virtuele evenknie onder de naam EPIC-TURLA, malware die vooral overheden in Europa en het Midden-Oosten heeft geïnfecteerd en die volgens Schekkerman "een spionagetoolkit is, die informatie steelt en beschikt over capaciteiten om netwerken te vernietigen". Net als bij Stuxnet, de malware die het Iraanse kernprogramma verstoorde, gaat het hier om heel geavanceerde software. "Hackers hebben hier de middelen niet voor, dit moet afkomstig zijn van door overheden gesponsorde groepen."

**Cyberlegers**

Wat er na Stuxnet gebeurde, illustreert dat een cyberwar al gaande is. Schekkerman vertelt dat Iran als antwoord zijn eigen cyberleger samenstelde en een tegenaanval lanceerde, die 'Operation Cleaver' wordt genoemd. Daarmee nestelde het zich de afgelopen jaren in de vitale infrastructuur van allerlei landen, van Zuid-Korea tot de Verenigde Staten. "Er zijn diverse incidenten geweest. Zo werden de beveiligingspoortjes op een luchthaven in Zuid-Korea overgenomen. We weten niet precies wat geïnfecteerd is, wat ze zullen gebruiken voor welk type aanval en op welke manier." Operation Cleaver maakt gebruik van bekende kwetsbaarheden in software, waarvoor oplossingen beschikbaar zijn.


Foto: AP/Hollandse Hoogte

## CGI en cybersecurity

**Cybercrime is een wereldwijd fenomeen dat vraagt om een krachtig en gebundeld tegengeluid. Daarom werkt CGI nauw samen met internationale veiligheids- en standaardisatieorganisaties. CGI is een van de weinige aanbieders die beschikt over tien Security Operations Centers die continu de beste oplossingen voor infrastructuren identificeren en implementeren, en maandelijks meer dan 550.000.000 cyberevents onderscheppen en afhandelen. Bij CGI werken meer dan 1400 beveiligingsexperts wereldwijd.**

*cginederland.nl/cybersecurity*

Tijdens de sessie over cybersecurity op het iBestuur Congres 2014 werd gesteld dat ook in de Nederlandse vitale infrastructuur veel van dit soort 'achterdeuren' openstaan. "En die zijn nog steeds niet allemaal gesloten", zegt Schekkerman. Daarmee beginnen is de allereerste stap naar veiliger systemen.

**Samen in innovatie en expertise**

Zoals Nederland het Defensie Cyber Commando (DCC) heeft opgezet, zo hebben landen als de VS, Israël, India, China, Rusland en Iran ook hun eigen divisies voor cyberwar. Partijen als IS en Anonymous gebruiken het cyberdomein om hun politieke en ideologische doelen te bereiken. Om je hier als land tegen te wapenen zul je moeten samenwerken met andere landen én met de private sector. Dat Nederland gericht investeert in cybersecurity en de markt uitnodigt om hierin mee te denken in de NCSS2 is daarom een belangrijke stap. Een ander goed voorbeeld van samenwerking op dit vlak is The Hague Security Delta. In dit grootste samenwerkingsverband van Europa werken overheden, kennisinstellingen en marktpartijen samen in innovatie en expertise voor veiligheid in onder meer cybersecurity en de vitale infrastructuur.

"Een pasklare oplossing voor dit vraagstuk is er niet", concludeert Schekkerman. "Ik geloof dat samenwerkingsverbanden als ThreatExchange een goede optie zijn, want daarin wordt informatie gedeeld tussen partijen die elkaar vertrouwen. Hetzelfde doet CGI in haar wereldwijde netwerk van partners en klanten. Het gevaar mag voor het grote publiek onzichtbaar zijn, een cyberwar lijkt in veel opzichten op een traditionele oorlog: je moet antwoorden blijven ontwikkelen, want het is een continue wapenwedloop."