CYBER: THE GOOD, THE BAD AND THE UGLY

De heren Jo Godderij, Raymond Bierens en Roy Jansen, ATOS

Het cyberdomein lijkt tegenwoordig het wilde westen wel: (elektronische) geldtransporten worden overvallen, maar ook individuen, (digitale) forten en zelfs landen worden niet gespaard bij dergelijke aanvallen. In dit artikel geven de auteurs hun visie op cyber met de daarbij horende uitdagingen voor Defensie, officieren verbindingsdienst in het bijzonder.

OVER DE AUTEURS

De volgende drie auteurs hebben, vanuit hun internationale rol een bijdrage geleverd aan dit artikel:

- Jo Godderij lgen b.d., VP Government Affairs Europe & Middle East
- Raymond Bierens, Head of Global Portfolio Management Defence and Security
- Roy Jansen, Cyber Competence Lead Atos Consulting

Samen met sales & client manager Mark Ostendorf vervult dit team binnen Atos een centrale rol in de uitwisseling van opgedane kennis en ervaring op gebied van cyber bij Defensie.

In zowel operaties als bedrijfsvoering is IT voor iedere defensieorganisatie onmisbaar. Enerzijds als middel om op kosten-efficiënte wijze haar werk uit te voeren, anderszijds om samenwerking tussen defensieorganisaties en –andere actoren te faciliteren. Concepten als network enabledoperations, joint & combined optreden en comprehensive approach zijn onuitvoerbaar als daarbij de juiste IT-ondersteuning ontbreekt.
Door deze toenemende samenwerking en afhankelijkheid, wordt het netwerk waarover deze samenwerking plaatsvindt een belangrijke succes- of faalfactor. De negative impact van eventuele cyberaanvallen of cyber indringers, wordt met deze samenwerkingsvormen daardoor groter. Zeker indien uiteindelijk mogelijk een 'cyber weapon of mass destruction' wordt gepositioneerd.
Niet voor niets beschouwen Defensieorganisaties om die reden het cyberdomein als een vijfde domein van oorlogsvoering. De cyberstrategieën van de Verenigde Staten en Groot-Brittannië zijn daar het beste voorbeeld van. Daaruit komt eveneens naar voren dat in het cyberdomein zowel ruimte is voor defensieve als offensieve acties (kader 1).
Maar tegen wiens acties moet verdedigd worden of wie dient aangevallen te worden? Wie zijn "the good, the bad and the ugly" in het cyberdomein?

HET ATOS CYBER MODEL

Om "the good, the bad and the ugly" te beschrijven, heeft Atos voor haar klanten op het terrein van Defensie, Veiligheid en Nationale Kritische Infrastructuur een cybermodel ontwikkeld (zie figuur 1).

Figuur 1: Atos Cyber Security Model

> ***'These cyber-capabilities are still like the Ferrari you keep in the garage and only take out for the big race and not just for a run around town, unless nothing else can get you there,' said one Obama administration official briefed on the discussions.***
>
> *Bron: 'US Debated cyberwarfare in Attack Plan on Libia' (NY Times on 17/10/2011)*

Bovenin het model zijn de 'ugly' terug te vinden, terwijl onderin de 'good' zijn gepositioneerd. Hoe de 'bad' te vinden zijn, wordt later uitgelegd. Ook zijn in het model de door Atos gedefinieerde 'cyber capabilities' te zien: verdedigen & aanvallen versus samenwerken & identificeren.

THE GOOD

Cyber moet worden bezien vanuit de optiek van nationale veiligheid. De Nederlandse krijgsmacht heeft drie hoofdtaken. Als eerste de bescherming van het eigen en het bondgenootschappelijk grondgebied (inclusief het Koninkrijk der Nederlanden in het Caraïbisch Gebied). Ten tweede de bevordering van de internationale rechtsorde en stabiliteit. En tenslotte ook de ondersteuning van civiele autoriteiten bij rechtshandhaving, rampen bestrijding en humanitaire hulp, zowel nationaal als internationaal.
In onze visie zijn alle partijen met wie Defensie vanuit deze kerntaak moet samenwerken als 'the good' te kwalificeren. In het kader van de eerste kerntaak betreft dit andere Defensieorganisaties, bij de tweede kerntaak kritische nationale infrastructuren en bij de derde kerntaak betreft het de gehele veiligheidsketen.

Is hiermee alles gezegd over 'the good'? Niet helemaal, want iedere 'good guy' die (een deel van zijn) bedrijfsprocessen in handen geeft van een private partij, maakt daarmee de connectie/samenwerking met deze ketenpartner onderdeel van het cyberdomein. Bij outsourcing, in welke vorm van ook, dient ook te worden gekeken hoe de cyber security van deze samenwerking wordt ingevuld.

THE BAD

The 'bad' is misschien wel de meest lastige om te omschrijven. De 'bad guys' zijn zichzelf namelijk niet eens altijd bewust dat ze 'bad' zijn. Want de gebruiker wiens pc tot een botnet behoort of de gebruiker die een USB-stick van een conferentie in een pc stopt, kan zonder het zichzelf te beseffen ineens een 'bad guy' zijn geworden. Daarom spreken wij om die reden over een "thin line" tussen goed en kwaad' in het cybermodel.
De rode draad bij deze 'bad guys' is wel dat, ongeacht of zij organisaties of individuen zijn, zij zich afdoende dienen te beschermen tegen pogingen om hun IT over te nemen en het ontvangende netwerk ook voldoende in staat moet zijn om vast te stellen of de persoon (of organisatie) die het netwerk betreedt, ook daadwerkelijk degene is die hij/zij claimt te zijn. Om die reden is voor Atos **identificeren onlosmakelijk aan cyber verbonden.**

Het netwerk betreden kan daarbij op twee manieren. De eerste mogelijkheid is de medewerker of burger die gebruik maakt als klant van een netwerk (bijvoorbeeld bij het inloggen op een overheidssite). De tweede mogelijkheid is op het moment dat de persoon ook daadwerkelijk inlogt op het systeem om daarmee als medewerker aan het werk te gaan.

THE UGLY

Het aanwijzen van de 'ugly' lijkt op het eerste gezicht niet zo moeilijk. Het is hierbij echter wel van belang een onderscheid te maken tussen verschillende typen. Want de complexiteit, de financiële middelen en doelstelling van diegenen die cyberdreigingen willen hanteren, kunnen sterk variëren.
De (georganiseerde) misdaad heeft in het bijzonder als doel om op pc's op zoek te gaan naar financiële informatie of de computer (onwetend) onderdeel te maken van een botnet. Een terroristische groepering zou zich echter eerder richten op het verspreiden van een ideologische boodschap en het zaaien van angst door mogelijkerwijs een of meerdere systemen te infiltreren. Een vijandige natie kan zich tenslotte heel specifiek richten op kritieke infrastructuren of communicatienetwerken.
Maar als geschiedenis ons één ding leert, is dat de grootste dreiging altijd van binnenuit komt. Daarom dient met de 'insider threat' terdege rekening worden gehouden.

CYBER CHANGE

De kritische lezer zal na het lezen van de vorige drie paragrafen terecht concluderen: zo veel nieuws is er dus eigenlijk niet. Waar de Grieken al gebruik maakten van het Paard van Troje, zo kapen criminelen nu pc's via een Trojan-virus.
En is er nu een groot verschil tussen de anarchisten die in 1920 een bom lieten afgaan in Wall Street en de huidige oorlog tegen terrorisme? Je zou zelfs de volgende vraag kunnen stellen: is Anonymous niet de moderne cyberversie van Robin Hood?
Hoewel de mogelijke tegenstanders in het cyberdomein t.o.v. vroegere tijden niet echt zijn veranderd, kan de impact van hun acties wel groter zijn dan ooit in de geschiedenis. En een aantal factoren maken het alleen nog maar complexer:

- Hoe kun je jezelf verdedigen tegen een vijand die je niet ziet?
- Hoe stel je met zekerheid de identiteit vast als je een tegenstander denkt te zien?
- Hoe verdedig je je tegen de lage instapkosten van het ontwikkelen van een dreiging?
- Is een 'balance of power' denkbaar zoals een non-proliferatie verdrag?

De cyberaanval op Estland in 2007 is een sprekend voorbeeld hoe groot de impact van een cyberaanval kan zijn, maar tegelijkertijd ook hoe lastig het is om de identiteit van de tegenstander vast te stellen.

CYBER STRATEGIES

Het is nog maar zeer de vraag of het cyberdomein echt nieuwe strategieën vereist. Niet voor niets publiceerde het NATO Cyber Center of Excellence recentelijk een abstract van Sun Tzu en Cyber War. Alle militaire strategieën zoals vermomming, gelaagde verdediging, training en simulatie zijn toepasbaar op het cyber domein.
De grootste uitdaging bij uitvoering van deze strategiën ligt in het asymmetrische karakter van cyber. Om je hiertegen te wapenen is een holistische benadering nodig. Indien een Defensieorganisatie bestand is tegen een cyberaanval, maar het blijkt eenvoudig om bijvoorbeeld de financiële transacties of energievoorziening of de communicatie infrastructuur plat te leggen, dan is dezelfde Defensieorganisatie nog steeds machteloos. De recente incidenten rondom Diginotar tonen aan dat ook de cyber ketting net zo sterk is als de zwakste schakel.

CYBER DEFENCE

Bescherming tegen externe cyber dreigingen vereist een reeks van high performance beveiligingsdiensten. Deze beveiliging hangt nauw samen met de bescherming tegen de dreiging van binnenuit. Verschillende vormen van beveiliging spelen een cruciale rol, zoals o.a. beveiliging van de werkplek tegen malware, gebruik data-encryptie en beveiliging van de fysieke en IT-infrastructuur. Ook toegang tot Defensienetwerken op afstand verdient daarbij de aandacht.

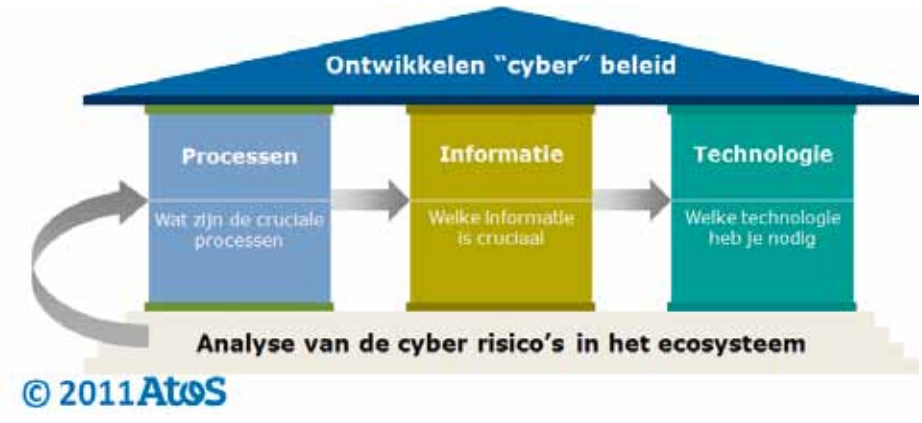
> ***'The U.S. might be able to blow up a nuclear plant somewhere, but a number of countries could strike back with a cyber attack and I can't assure you that as you go to war with a cyber security-conscious, cyber security-capable enemy that any of our stuff is going to work.'***
>
> *Bron: Richard A. Clarke, former US presidential adviser on cybersecurity (MSNBC on 02/11/2011)*

> ***In april 2007 werden diverse systemen en netwerken in Estland platgelegd met behulp van een reeks van gecoördineerde botnet aanvallen uit het buitenland. Dit heeft geresulteerd in dagen van onbereikbaarheid voor de belangrijkste diensten. Pas veel later bleek dit het werk te zijn van een etnisch Russische Estse burger die het oneens was met de verhuizing van een Russisch oorlogsmonument in Tallinn.***

Hoevelen van u mailen dagelijks bestanden naar uw Hotmail of Gmail-adres om thuis verder te werken? Dat is werken in de Cloud, maar wel een public Cloud die volgende de Patriot Act toegankelijk is voor de Amerikaanse overheid.
Governance, Risk en Compliance (GRC) spelen een belangrijke rol bij bescherming van de organisatie en de kritieke processen, informatie en infrastructuur. Cyber bewustzijn bij werknemers is eveneens van cruciaal belang voor het welslagen van opereren in het 5e domein. Het zou daarom een overweging kunnen zijn om alle Security Operation Centers (SOC) van Defensie en Binnenlandse Veiligheid te koppelen aan de SOC's van diverse kritieke infrastructuur organisaties. Informatie uitwisseling over verdachte activiteiten in het cyberdomein en gezamenlijk dreigingen te analyseren en vijanden te identificeren is geen wens maar noodzaak.

CYBER IDENTIFICATIE

Het beschermen van gebruikers tegen risico's door middel van identificatie moet worden beschouwd als een integraal onderdeel van de cyberstrategie. Naarmate processen meer cruciaal zijn voor het cyber ecosysteem, des te groter de ingezette middelen dienen te zijn. Hierbij kan gedacht worden aan geavanceerde biometrische identificatie oplossingen voor toegang tot high security omgevingen.



Figuur 2: Bouw je eigen cyber beveiliging

CYBER SAMENWERKING

Samenwerking in het cyber ecosysteem is van cruciaal belang. Dit betekent dat er een zware druk komt te liggen op de cyberveilige communicatie binnen Defensie en met alle samenwerkingspartners buiten de grenzen van de 'klassieke' organisatie.

Communicatie is het domein van de verbindelaren. Toch is het beveiligen van communicatie binnen, maar ook tussen organisaties nog vaak een blinde vlek in de cyberstrategie van organisaties.

Te vaak kiezen organisaties ervoor een 'digitaal fort' te bouwen, ontoegankelijk voor iedereen, maar daarmee worden ze ook ontoegankelijk voor klanten en samenwerkingspartners. Tegelijkertijd leiden alle technologische trends zoals ´Cloud Computing´ en ´bring-your-own-device´ ertoe dat 'digitale forten' verleden tijd zijn en informatiebeveiliging en informatie-uitwisseling belangrijke elementen zijn in ieders manier van werken en dus in iedere cyberstrategie. Atos hanteert hierbij vier pragmatische stappen.

CYBER STEP-BY-STEP

Ontwikkel eerst het integrale beleid en doctrine op het gebied van cyber. Dit betreft een aantal lastige vraagstukken, zoals het onderscheid tussen cyberverdediging en -aanval en het vaststellen wanneer sprake is van een cyberaanval en wat daarop volgende acties zouden kunnen/mogen zijn.
Gebruik het beleid en de doctrine om voor ieder proces binnen het ecosysteem te identificeren welke het meest cruciaal zijn en nooit mogen worden aangetast. Identificeer vervolgens de informatie en data in deze cruciale processen en welk niveau van beveiliging die nodig hebben. Pas dan begint de zoektocht naar juiste technologische oplossingen om die kritieke processen en informatie te beschermen.
Gebruik het beleid en de doctrine om voor ieder proces binnen het ecosysteem te identificeren welke het meest cruciaal zijn en nooit mogen worden aangetast. Identificeer vervolgens de informatie en data in deze cruciale processen en welk niveau van beveiliging die nodig hebben. Pas dan begint de zoektocht naar juiste technologische oplossingen om die kritieke processen en informatie te beschermen.
Een goed voorbeeld hiervan is de samenwerking Transglobal Secure Collaboration Program (TSCP) voor veilige communicatie voor de complete supply chain bij verschillende defensie toeleverende industrie. Nederland neemt deel in het internationale TSCP programma via het Ministerie van Defensie. Defensie wordt hierin ondersteund door het Nationaal Lucht- en Ruimtevaartlaboratorium.

KRACHTEN BUNDELEN

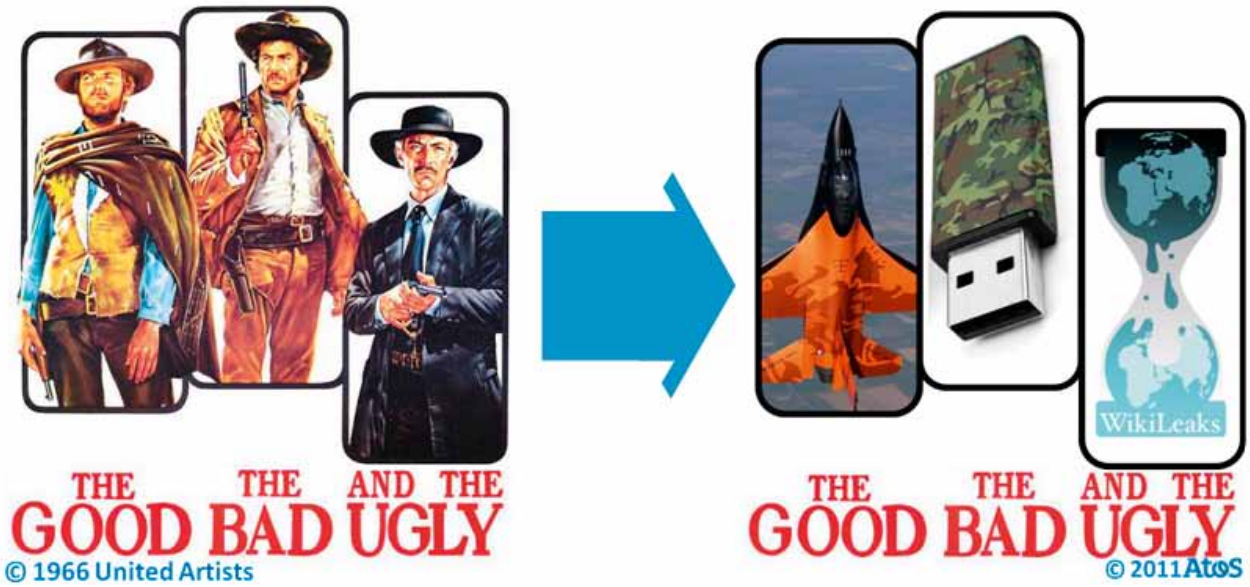
De western-wereld eind 19e eeuw en de cyberwereld begin 21e eeuw verschillen niet zo veel van elkaar. 'The good, the bad and the ugly' zijn er nog steeds maar heten nu anders. Dezelfde militaire strategieën, zelfs terug naar Tsun Zu, zijn nog toepasbaar. Alleen is de impact en het bereik van het cyber wapen wellicht groter dan welk wapen ooit ontwikkeld in de geschiedenis van de mensheid. Het kan met enorme complexiteit vanuit iedere lokatie tegen relatief lage kosten worden ingezet en het vinden van de dader zal een gigantische uitdaging zijn.
Om deze dreiging het hoofd te bieden is samenwerking een must en geen 'nice-to-have' meer. Het cyber ecosysteem is te kwetsbaar geworden en technologie heeft een te bepalende rol gekregen in alles wat we doen. Het tot nu toe ondenkbare wordt inmiddels denkbaar. Een paar recente voorbeelden:

- De meerderheid van alle printers ter wereld is verbonden met internet voor updates, maar zijn daarmee kwetsbaar.
- Een cyber aanval op een waterleidingbedrijf in Amerika zorgde voor een defect in de watervoorziening.
- Meer dan 80% van het Stuxnet virus blijkt in haar werking generiek te zijn en kan ook gericht worden op andere doelen. Het recent verschenen Duqu virus, een 'afstammeling' van Stuxnet is daar een voorbeeld van.
- Atos High Performance Security SOC voor de Olympische Spelen verwerkt dagelijks 12.000.000 security events.
- NATO verwerkt dagelijks 30.000.000 security events waarvan er 6.000 door analisten worden beoordeeld. Dit leidt uiteindelijk tot 12 incidenten. 15% van de aanvallen op NATO systemen zijn afkomstig van botnets (bron: 'NATO Perspective on Cyber Defence and Botnets', Virginia Aguilar (ESCD) & Ömer Hasret, NCSA/NCIRC op 09/03/2011)

TOT SLOT

Met dit artikel beogen auteurs aan te geven dat Defensie, als onderdeel van haar kerntaak tot bescherming van het grondgebied en met haar ervaring in militaire doctrine, een vooraanstaande rol zou moeten hebben in het beveiligen van het cyber ecosysteem. Maar ook dat dit systeem veel breder is dan Defensie alleen en ook veel breder dan alleen de IT afdeling. Cyber is een aandachtspunt voor de ambtelijke top, niet alleen voor de "CIO".

Maar boven alles is het een oproep tot samenwerking tussen alle partijen die een mogelijk doelwit kunnen vormen voor een cyberaanval. Communicatie staat centraal in het weerstaan van elke cyberaanval en ook hier zou Defensie kennis, aangevuld met kennis van de industrie, een cruciale rol vervullen. Want net als in de film, willen we toch ook dat de 'good guys' winnen?



Figuur 3: Western vs Cyber