CYBER (SECURITY)

GEEN ROCKET SCIENCE, MAAR HOLLANDSE NUCHTERHEID

Dit artikel is tot stand gekomen met medewerking van de heer Peter van de Himst MBA MSec (Beveiligingsautoriteit) en luitenant-kolonel Edwin Saiboo (Kenniscentrum C2 Ondersteuning Landoptreden).

In onze wereld die wij defensie noemen, kennen wij verschillende vormen van veiligheid. Een toepasselijke oneliner die ook het essentiële verschil aangeeft is dan ook: "we moeten veilig (*safety*) maar ook beveiligd (*security*) werken".

INLEIDING

Vanwege de doorontwikkeling van allerlei (wapen)systemen, zijn wij steeds meer afhankelijk geworden van computers. We noemen dit voor het gemak 'ICT'. Onder ICT wordt verstaan: "het geheel aan digitale informatie, informatie-infrastructuren, computers, systemen, toepassingen en de interactie tussen informatietechnologie en de fysieke wereld waarover communicatie en informatie-uitwisseling plaatsvindt".
Deze ICT moet worden beschermd tegen onbevoegde beïnvloeding van binnenuit of buitenaf door het implementeren van beveiligingsmaatregelen.

BEVEILIGINGSMAATREGELEN

Beveiligingsmaatregelen zijn in te delen in drie categorieën:
- **O**rganisatorische,
- **B**ouwkundige en
- **E**lektronische maatregelen.

De zgn. 'OBE-mix'.
O-maatregelen zijn alle handelingen of het nalaten daarvan die door de mens, de gebruiker, moeten worden uitgevoerd. Op een schaal van 0 tot 100 vragen de O-maatregelen om 10% investering maar hebben een rendement van 80%.
B-maatregelen zijn maatregelen zoals hekken, muren, beglazing. B-maatregelen vergen 20% investering en dragen met een rendement van 17% bij aan de totale beveiliging.
E-maatregelen, alle detectiemiddelen, elektronische toegangssystemen en CCTV-camera's, kennen de hoogste investering (70%) en bieden slechts 3% rendement. Echter de een kan niet zonder de ander, dus moet de optimale mix worden gevonden.

TE BESCHERMEN BELANGEN

Voor de beveiliging van Te Beschermen Belangen (TBB) bij defensie is het Defensie Beveiligingsbeleid (DBB) opgesteld. Het DBB bestaat uit een hoofddocument en diverse Uitvoeringsbepalingen (UB'n) en is tot stand gekomen door een gezamenlijke inspanning van de Beveiligingsautoriteit (BA) en defensieonderdelen.
De UB'n zijn onderverdeeld in vijf categorieën.
Dit zijn:
- Algemeen & Organisatie,
- Personele beveiliging,
- Fysieke beveiliging,
- Informatiebeveiliging en
- Industrieveiligheid.

De UB'n vormen het 'uitvoerbare beleid'. In deze documenten staat in begrijpelijke taal omschreven welke maatregelen getroffen moeten worden ter bescherming van een TBB.
In het kader van cyber security kan echter niet worden volstaan om alleen naar de UB'n op het gebied van de informatiebeveiliging te kijken. Ook de overige UB'n zijn van belang om een optimale mix te kunnen samenstellen.

MAATREGELEN IN HET KADER VAN CYBER SECURITY

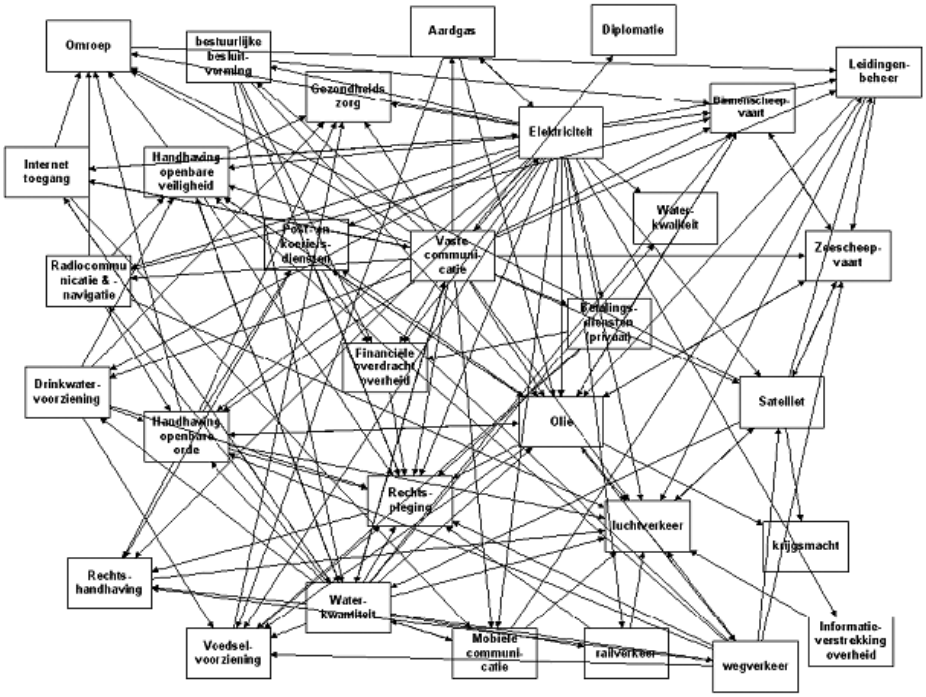
Om maatregelen in het kader van cyber security te kunnen uitvoeren, moet er allereerst (cyber) beveiligingsbewustzijn bestaan. Beveiligingsbewustzijn wordt bereikt door defensiepersoneel bewust te maken van de uitvoering van diverse handelingen ten behoeve van de beveiliging van de Te Beschermen Belangen. De beveiligingscoördinatoren (BC'n) en de BA leveren hiertoe een inspanning om diverse bewustwordingsprogramma's aan te bieden. Ideeën op het gebied van cyber security awareness die op stapel staan, zijn: cyber security demonstrator en het digitaal rijbewijs. Ook wordt er gedacht aan de mogelijkheid om zogenaamde "tips van de dag" met een afsluitende vraag op MULAN basis te presenteren.

CYBER SECURITY

Cyber security is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

[Bron: Nationale Cyber Security Strategie of NCSS]

In enge zin is cyber security niets meer of minder dan het uitvoeren van alle noodzakelijke beveiligingsmaatregelen. Met andere woorden, u draagt bij aan de cyber security door het uitvoeren van de voorgeschreven set van beveiligingsmaatregelen. Cyber se-



Figuur 1: Schematische weergave van de vitale infrastructuur. Bron: Instituut Clingendael.

curity spitst zich echter primair toe op ICT. De Rijksoverheid heeft een Nationale Cyber Security Strategie (NCSS) uitgebracht omdat de toenemende afhankelijkheid van ICT de samenleving steeds kwetsbaarder maakt voor misbruik en (grootschalige) verstoring. In het verlengde daarvan kan worden gesteld dat veilige en betrouwbare ICT van fundamenteel belang is voor het functioneren van de samenleving. ICT biedt kansen, maar verhoogt ook de kwetsbaarheid omdat in die omgeving steeds meer vitale producten en diensten (vitale infrastructuur) met elkaar verweven zijn. Zie figuur 1.

Een moedwillige of een onopzettelijke verstoring als gevolg van technisch of menselijk falen of door natuurlijke oorzaken kan leiden tot (maatschappelijke) ontwrichting. De complexiteit van ICT-voorzieningen en onze toenemende afhankelijkheid van deze voorzieningen leiden tot nieuwe kwetsbaarheden die misbruik en verstoring in de hand werken (denk aan het Stuxnet of het {vermeende} virus bij de Amerikaanse UAV's). Als een "aanval" op de proces besturende ICT van de elektriciteitsvoorziening succesvol zou zijn, zijn de gevolgen aanzienlijk. Zie hiervoor figuur 2.

Binnen uw eigen (operationele) werkomgeving zou u met de ICT-systemen die bij uw eenheid in gebruik zijn, ook een dergelijk overzicht kunnen samenstellen. U noteert hiervoor de gebruikte ICT-systemen en trekt pijlen naar de ontvangers van de informatie uit die systemen. Vanzelfsprekend tekent u ook de pijlen terug naar het bewuste ICT-systeem als dat door andere systemen wordt "gevoed". Vervolgens "schakelt" u één ICT-systeem uit. De uitschakeling is in dit geval het resultaat van een succesvolle onbevoegde beïnvloeding (dit zou dus ook een cyber attack kunnen zijn). Na de uitschakeling volgt u de pijlen en zet u de afhankelijke ontvangers op zwart. Op vrij eenvoudige wijze kunt u hiermee aantonen wat de afhankelijkheid van anderen is van uw ICT-systemen.

DEFENSIEVISIE CYBER OPERATIONS

In de Militair Strategische Visie van de CDS wordt het Cyberdomein genoemd als de vijfde dimensie naast Lucht, Land, Zee en de Ruimte. Het Eindrapport Verkenningen noemt Cyber als prioriteit. Het is een intensivering in alle beleidsopties. Dit heeft erin geresulteerd dat Cyber één van de weinige domeinen is waar Defensie intensiveert in plaats van daarop te bezuinigen.
Om invulling te geven aan deze ontwikkeling is een Visie van Defensie op cyber operations geschreven. Deze visie is goedgekeurd door het Departementaal Beraad waarin alle key spelers van Defensie zijn vertegenwoordigd. Naast de inspanningen van Defensie op dit terrein is er ook een Nationale Cyber Security Strategie (NCSS) geschreven. Deze is op internet te vinden.
De visie van Defensie is uitgewerkt naar personele, materiële en financiële consequenties. Deze uitwerking is eveneens in het Departementaal Beraad goedgekeurd. De verdere implementatie zal in 2012 ter hand worden genomen door een Taskforce Cyber die voor 2015 moet resulteren in de oprichting van een Defensie cyber Commando en een Defensie Cyber Expertise Centrum.

SAMENSPEL VAN DIVERSE VERMOGENS

Het cyber domein is een dynamische, innovatieve en technologische omgeving. Binnen cyber operations vallen strategische, operationele en tactische elementen samen. Om hier effectief uitvoering aan te kunnen geven, zijn een aantal vermogens benodigd:
- een Inlichtingenvermogen om een *situational awareness* te creëren,
- een Defensief vermogen om onszelf te beschermen tegen aanvallers en
- een Offensief vermogen om een tik uit te kunnen delen.

Ter ondersteuning van het kennis- en vaardighedenpeil wordt een separaat Cyber Expertise Center (CEC) opgezet. Deze zal samenwerkingsverbanden moeten aangaan

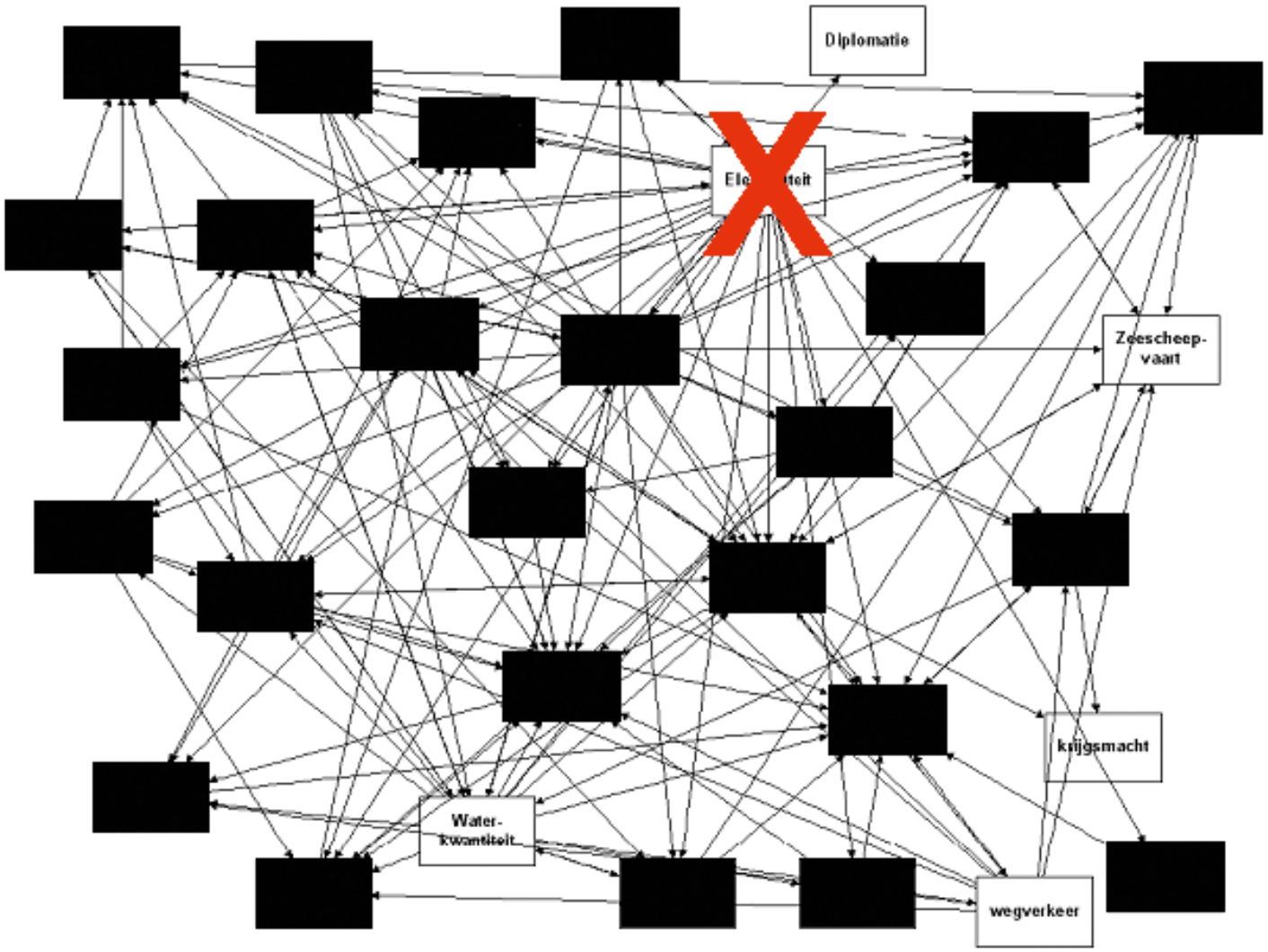
VOORBEELD VAN BEVEILIGING VAN EEN ICT-SYSTEEM

Er is een nieuw ICT-systeem ontworpen. Voordat het in gebruik genomen kan gaan worden, moet de categorie-indeling worden vastgesteld. Laten we in dit voorbeeld aannemen dat de VIR E&E analyse uitwijst het een TBB-2 (Stg. Geheim) wordt. Om dit systeem geaccrediteerd te krijgen, moeten er dus OBE-beveiligingsmaatregelen worden getroffen. Deze maatregelen worden abstract voorgeschreven in de rapportage naar aanleiding van de VIR E&E. Wanneer aan de voorgeschreven beveiligingsmaatregelen is voldaan, wordt door de eigenaar of de gebruiker Statement of Compliance (SoC) ingediend. Aan de hand van de ingediende SoC wordt door de BA gecontroleerd of het eventuele restrisico acceptabel is.

De te treffen beveiligingsmaatregelen omvatten alle deelgebieden van de Integrale beveiliging. Zo zal er in het kader van Algemeen en Organisatie moeten worden beschreven welke maatregelen er zijn getroffen voor bijvoorbeeld de toegangscontrole tot het object of het compartiment waar het TBB staat opgesteld. Hoe luidt de bezoekersregeling en op welke wijze wordt de interventie in geval van een alarm geborgd. Is er een beveiligingsfunctionaris aangesteld met een handelingsmandaat namens de verantwoordelijke commandant?

Op het gebied van de Personele beveiliging moet er worden aangegeven dat de gebruikers van dit systeem zijn voorzien van een geldige Verklaring van Geen Bezwaar op het juiste niveau (in dit geval minimaal B-niveau).

Bij het hoofdstuk Fysieke beveiliging wordt aangegeven welke maatregelen zijn getroffen ter bescherming van het TBB. Een belangrijk onderdeel van deze paragraaf is de vermelding dat de toegang tot het TBB is voorzien van dubbele authenticatie. Dit is een randvoorwaarde bij TBB 1 en TBB 2. Ook wordt in dit deel van de SoC aangegeven dat de bouwkundige uitsteltijd langer is dan de interventietijd. Dit wordt positief bewakingsrendement genoemd. Als dit niet behaald kan worden, moet er risicomanagement worden toegepast. In geval van een TBB 2 heeft de beveiligingscoördinator van het betrokken defensieonderdeel de bevoegdheid om gekwantificeerd risicomanagement/-acceptatie toe te passen. De BA wordt over dit besluit geïnformeerd. Indien het een TBB 1 betreft, ligt de bevoegdheid voor risicoacceptatie alleen bij de BA.
Bij de Informatiebeveiliging worden onder meer de getroffen logische maatregelen verwoord (logging, authenticatie, encryptie, (vercijferde) opslag. Een belangrijk gegeven bij de maatregelen op het gebied van de informatiebeveiliging is het updaten van de software (security patches) en niet te vergeten de antivirus software. Bij sommige IT-diensten wordt zelfs de frequentie van antivirus controles voorgeschreven. In het kader van de cyber security is het wel of niet aanwezig zijn van een (externe) koppeling een cruciaal gegeven. Hier zal tijdens een accreditatie nauwgezet naar gekeken worden. Als er externe gegevensdragers (USB-sticks, externe harddisks) op het systeem worden gebruikt, moeten deze zijn toegelaten voor het gebruik en de opslag van de informatie. Bij defensie zijn inmiddels drie USB-sticks geaccrediteerd. Twee van deze sticks zijn geschikt voor de opslag en/of het transport van gerubriceerde gegevens vanaf de rubricering Departementaal Vertrouwelijk. De bovengenoemde maatregelen zijn uiteraard niet uitputtend, maar geven u wel een beeld dat cybersecurity niet alleen uit ICT-maatregelen bestaat.



Figuur 2: "Restant" vitale infrastructuur als de elektriciteitsvoorziening in ongerede is geraakt.

met de overige overheid, wetenschappelijke instituten en de industrie.
De CDS is in de lead gepositioneerd bij de ontwikkeling van de cyber vermogens. De programmamanager Cyber operations moet een en ander op de rails zetten waarna de operatonele aansturing op termijn zal worden vormgegeven in het Defensie Cyber Commando.

DEFENSIEF VERMOGEN: VERGROTEN

Het Defensieve vermogen kent een aantal aspecten die de komende jaren verder verbeterd moeten worden.
Gezien de noodzakelijke externe koppelingen die tegenwoordig nodig zijn voor het beheer op afstand en de ondersteuning door de industrie, moet het beheer en beveiliging van netwerken die onder verantwoordelijkheid van Defensie vallen, verder worden versterkt.
Hetzelfde geldt voor het beheer en beveiliging van meet, regel- en wapensystemen. Bijvoorbeeld een wapensysteem zoals een JSF komt met performance based logistics ondersteuning door de industrie. Dit betekent dat online koppelingen met de industrie noodzakelijk zijn om hier invulling aan te kunnen geven.
Voor het standaardiseren en zekerstellen van het minimale beveiligingsniveau van de verschillende oplossingen moet de accreditatie van deze systemen verder ter hand worden genomen.

DOORONTWIKKELING DEFCERT

Het *Defence Computer Emergency Response Team*, ook wel DefCERT richt zich op het beschermen van de Defensie ICT-infra. Het is operationeel gegaan in oktober 2010. Eind 2012 moet het volledig op sterke zijn en alle initieel noodzakelijke geachte ondersteuning kunnen leveren. Echter gezien de ontwikkeling van het Cyber domein zal deze step-by-step ontwikkeling verder gaan om uiteindelijk alle netwerken en systemen van Defensie te kunnen ondersteunen. Ook zal er in toenemende mate worden samengewerkt met nationale en internationale partners. Hiertoe heeft de Beveiligingsautoriteit zitting in het zogenaamde *Cyber Capability Team* (CyberCaT) van de NAVO.
Een belangrijke capaciteit betreft de doorontwikkeling van DefCERT. Dit moet meer ondersteuning gaan leveren bij het monitoren, het geven van een response, de analyse van eventuele incidenten, etc.

WERK AAN DE WINKEL

Al deze capaciteiten kunnen niet zonder de gebruiker. Het vergroten van het bewustzijn van eindgebruiker ten aanzien van cyber dreigingen is een absolute must.
Het toepassen van risicomanagement in een statische omgeving raakt langzaam maar zeker meer ingesleten. Het dynamiseren van risicomanagement zal de komende jaren verder moeten worden opgepakt zodat beter kan worden ingespeeld op veranderende omstandigheden.
De response op vijandige cyber activiteiten moet uitgewerkt worden voor bijvoorbeeld *Business Continuity Management* en *graceful degradation*.