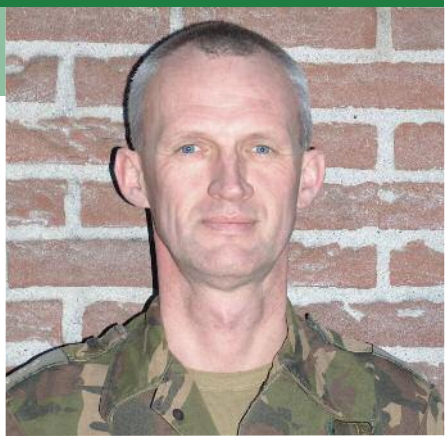
KWESTIE VAN BALANS

Luitenant-kolonel Ron Bertelink, dagvoorzitter Symposium Cyber Operations



Lkol Ron Bertelink is als informatiebeveiligingsarchitect werkzaam bij het Command & Control Support Centre van de Defensie Materieel Organisatie. Naast een groot aantal operationele functies, waaronder bataljonscommandant en een tweetal uitzendingen, heeft hij meer dan 12 jaar ervaring in verschillende functies als specialist in de militair operationele informatiebeveiliging. Lkol Bertelink gaat in dit artikel nader in op de wereld van cyberspace, een wereld waar we deel van uit maken - of we willen of niet. Een wereld met andere mores dan de fysieke wereld. Wat betekent 'balans' in cyberspace? Ga mee op patrouille in cyberspace.

DEFINITIE CYBER

Cyber is afgeleid van het Griekse woord *κ υ β ε ρ ν η τ η σ (kybernetes)*, dat stuurman betekent. De bekendste moderne afleiding van dit woord is cybernetica: meet- en regeltechniek. Deze wetenschap stond model voor moderne complexe technologie. Dit is de reden dat 'cyber' vaak als voorvoegsel wordt gebruikt waar het om moderne technologie gaat.

Cyberspace is de virtuele dimensie die is ontstaan door het grootschalig gebruik en de verbondenheid van computers. Cyberspace ontleent in de praktijk zijn enorme mogelijkheden vooral aan wereldwijd verbonden en vertakte op IP (Internet Protocol) gebaseerde netwerken en software. Nagenoeg alle elektrische apparaten, van telefoon tot koelkast, functioneren dankzij software en zijn vaak verbonden. Zelfs componenten die pure hardware lijken bevatten meer software (firmware) dan we denken.

Probleem is dat het IP is ontworpen en geïmplementeerd met functionaliteit als oogmerk. Er is nauwelijks rekening gehouden met kwaadwillend gebruik.
De balans tussen functionaliteit en beveiliging ligt volledig scheef. Commerciële software heeft doorgaans ook functionaliteit en financieel gewin als oogmerk. Beveiliging is daaraan ondergeschikt. De balans hangt ook hier helemaal scheef. De laatste jaren zien we dat beveiliging meer aandacht krijgt, maar het achteraf proberen te beveiligen van producten zal slechts een kleine verbetering opleveren.

Cyberspace is daarmee een dimensie geworden die enorme functionaliteit koppelt aan een grote kwetsbaarheid. Gevoelige en kritische toepassingen gebruiken echter steeds meer de krachtige functionaliteit in cyberspace.
Een ideale basis voor criminele en andere ongewenste activiteiten.

Cybercrime is de criminaliteit die gebruik maakt van de omstandigheden in cyberspace. Een vergelijkbare definitie is te maken voor cyberterrorisme.

Cyberdefense is het nemen van beveiligingsmaatregelen om dreigingen en kwetsbaarheden in cyberspace tegen te gaan om zo op een veilige manier de gewenste functionaliteit te kunnen benutten.

Cyberwarfare is oorlogvoering in cyberspace. Het is grootschalig en gaat tussen landen en/of internationale (militaire) organisaties. Cyberwarfare kan worden verdeeld in een defensieve en een offensieve uitvoering.

CYBERWARFARE

Defensieve cyberwarfare

Verdediging tegen cyberwarfare kan grofweg worden onderscheiden in drie soorten.

1. De dreiging buitenhouden (defensief).
2. Bewaken of de dreiging zich voordoet en dan optreden (reactief).
3. De dreiging uitschakelen (zowel proactief, als reactief).

Optie 1 is momenteel voor defensie IV de meest gebruikte. Feitelijk zijn nagenoeg alle informatiebeveiligingsmaatregelen gebaseerd op het buitenhouden van aanvallen. Vaak wordt de metafoor van de ondoordringbare kasteelmuur gebruikt die onze informatiesystemen isoleert van de onbetrouwbare buitenwereld. We zien echter dat er steeds meer behoefte komt om wel met die buitenwereld te communiceren. Dit betekent dat de poort in de kasteelmuur wordt geopend met toegangscontrole of dat zelfs de hele muur wordt weggehaald. Daarbij zal er binnen het systeem moeten worden opgelet of er geen ongewenste indringers schade aanbrengen. Dit is de situatie van optie 2. De laatste optie is dat er actief wordt opgetreden buiten het systeem om dreigingen voortijdig te elimineren of nadat ze zich openbaren. De grens tussen de drie soorten van verdediging is niet heel scherp en er is een sterke onderlinge afhankelijkheid.

KENMERKEN VAN CYBERSPACE

Cyberspace onderscheidt zich op een aantal punten van de traditionele dimensies en operationele theaters. De meest opvallende punten zijn:

1. **Anonimiteit**. Het is mogelijk om anoniem op te treden in cyberspace. Bij een aanval kunnen de effecten goed merkbaar zijn maar is het onmogelijk zeker te stellen waar de aanval vandaan kwam en wie hem heeft geïnitieerd. Ook kan men zich in cyberspace eenvoudig een andere geloofwaardige identiteit toe-eigenen. In cyberspace weet je nooit zeker met wie of wat je van doen hebt.
2. **Geen vaste relatie tussen input en impact**. In cyberspace kan een groot gevolg soms een heel kleine oorzaak hebben. Een scriptkiddie kan meer schade aanbrengen dan een cyberleger. Een bug in de software kan de hele elektriciteitsvoorziening in een land stil leggen. Het is moeilijk tot onmogelijk zeker te stellen of er sprake is van een cyberaanval of een technisch incident.
3. **Tijd en ruimte factoren**. In cyberspace spelen afstanden geen rol van betekenis. Grenzen tussen landen bestaan nauwelijks. Aanvallen kunnen vanaf iedere plaats naar elk doel op de wereld worden ingezet. Het theater is daarmee bijna oneindig groot. De omvang groeit met de dag, met een groeiende dreiging tot gevolg.
4. **Onzichtbare schade**. In cyberspace kan worden gestolen zonder dat er iets wordt gemist. Systemen kunnen worden overgenomen zonder dat het opvalt. Vooral de moderne aanvallen zijn helemaal gebaseerd op deze onzichtbaarheid.

Als we naast deze punten in ogenschouw nemen dat de afhankelijkheid van cyberspace groter is dan van welke andere dimensie, dan is duidelijk dat hier sprake is van een gevaarlijke situatie.

Offensieve cyberwarfare

Het mag duidelijk zijn dat aanvallen ook door de eigen partij kunnen worden uitgevoerd. Offensieve cyberwarfare kan bijdragen aan het succes van militaire operaties. De belangrijkste doelen zouden dan zijn:

1. Het achterhalen van inlichtingen door in te breken op vijandige systemen.
2. Het manipuleren van informatie ter misleiding van een tegenstander.
3. Het ontzeggen van de informatievoorziening van een tegenstander door zijn netwerk aan te vallen.

Om offensieve cyberwarfare uit te voeren is steeds minder nodig. Veel software *tooling* is vrij verkrijgbaar en zo gebruiksvriendelijk dat het ook door niet-specialisten kan worden gebruikt. Alleen om zwaar beveiligde systemen aan te vallen, waar de openbare hack tools nog geen opening in kunnen vinden, zal het lonen om eigen software te ontwikkelen en de aanval door specialisten te laten uitvoeren. Groot voordeel van het gebruik van eigen ontwikkelde malware is dat een virusscanner de aanval niet zal opmerken (*zero day attack*).

De belangrijkste voorwaarde om offensieve cyberwarfare uit te voeren is verbinding (*connectivity*) met het aan te vallen systeem. Dit betekent dat de aanval vanuit een gekoppeld netwerk of vanuit het netwerk zelf plaats moet vinden. Ook is het mogelijk om de aanval indirect uit te voeren via een besmetting vanaf externe media (USB-stick, cd, dvd, portable harddisk).

Net als bij andere vormen van militair optreden zal moeten worden gewerkt vanuit een heldere doctrine om alle voorwaarden voor succesvol optreden in te kunnen vullen.

CYBER EN DEFENSIE ALS SPELER

De dreigingen in cyberspace worden doorgaans opgedeeld in de eerdergenoemde drie categorieën: cybercrime, cyberdefense en cyberwarfare. Elke categorie kent een ministerie als belangrijkste probleemeigenaar. Omdat het echter vaak niet mogelijk is om vast te stellen tot welke categorie een aanval hoort is het onmogelijk om een aanval direct onder verantwoordelijkheid van een ministerie te plaatsen. Er zit dus niets anders op dan alle aanvallen centraal te melden en na een analyse toe te wijzen aan een acterend ministerie. Dit vereist de oprichting van een centraal meldpunt waar alle partijen inclusief banken en nutsbedrijven hun cyberincidenten moeten melden. Een relatie met Government Computer Emergency Response Team (GOVCERT) ligt voor de hand. Op het gebied van organisatie en taakstelling is een duidelijke parallel met de Nationale Coördinator Terrorismebestrijding (NCTb) zichtbaar. Daarnaast zal het Nationale centrale Coördinatie- en meldpunt Cyber Defense (NCCD) een directe lijn met het NCTb moeten hebben waar het gaat om cyberterrorisme.

Om de aanvallen te kunnen melden zullen ze eerst moeten worden gedetecteerd. Aanvallen kunnen echter heimelijk plaatsvinden. Er zal dus moeten worden geïnvesteerd in speciale tooling die onzichtbare aanvallen kan detecteren. Deze tooling vereist specialistische kennis en opleiding. Het centraal en nationaal regelen van tooling en uitrol, kan en zal winst opleveren. Ook kan deze tooling voor detectie automatisch de centrale meldingen verzorgen. Er moet dan wel worden beseft dat ook de detectiesystemen deel uit gaat maken van cyberspace. Het detectiesysteem zal actief moeten zijn op netwerken en systemen van verschillende beveiligingsniveaus. Dit zal speciale maatregelen vereisen. On-line koppelingen zullen niet altijd mogen.

Zodra de aanval is gedetecteerd en centraal gemeld, zal het onderzoek naar de herkomst vastlopen op het probleem van herleidbaarheid naar de plaats en identiteit van de initiator. Normaliter is dat een vruchteloze operatie. Aanvallers nemen in de regel maatregelen om onvindbaar te zijn. Het moet echter mogelijk zijn om met speciale tooling en hoogopgeleide cyberonderzoekers verder in de cybermist te kijken en met grotere nauwkeurigheid de initiator aan te wijzen. Aan de hand van de aard van de aanval en de herkomst moet centraal worden besloten om de actoren van de ministeries aan te wijzen. In die gevallen waarin de aanval duidelijk in een categorie hoort kan de actor zelf al besluiten te reageren. Denk hierbij vooral aan cybercrime. De melding zal wel moeten worden gedaan.

Mocht het gaan om cyberwarfare, dan zal de taak om te reageren primair bij defensie moe-

CYBERWARFARE EN DEFENSIE NU

De huidige informatiesystemen van defensie die bijzondere en gerubriceerde informatie verwerken zijn beveiligd op een risicomijdende manier. Op basis van strikte regelgeving zijn de systemen fysiek en cryptografisch geïsoleerd van onvertrouwde omgevingen. Deze risicoarme manier van inrichten van de informatievoorziening is gezien de aard van de informatie absoluut vereist. De systemen zijn alleen kwetsbaar voor:

- **Fysiek geweld**

Deze dreiging valt feitelijk buiten cyberwarfare, maar zodra onbevoegd personeel toegang heeft tot de informatie-infrastructuur is het degraderen van een systeem met een bijl heel eenvoudig. Bewaking, fysieke afscherming, redundantie, back-up voorzieningen en toegangscontroles zijn voorwaardelijk om een systeem en zijn informatie te laten overleven.

- **Gebruikersfouten**

Veel gehoord is de uitspraak dat de grootste dreiging tegen informatiesystemen vanuit het eigen personeel komt. Bij defensiesystemen ligt dit genuanceerder. Zonder vertrouwen in het eigen personeel zou defensie als gewapende macht niet kunnen functioneren. Wel is er de dreiging dat personeel fouten maakt in het volgen van de regelgeving en procedures. Naast technische maatregelen zoals hardening, zijn opleiding en training van personeel in het veilig omgaan met de systemen en een betrouwbaar controleproces noodzakelijk. Hoewel deze aspecten zeker aandacht krijgen is de situatie nog niet ideaal. Er raken nog steeds gegevensdragers kwijt en er worden andere fouten gemaakt waarbij onbewust te grote risico's worden gelopen. Daarbij komt dat veel commandanten nog steeds de kennis ontberen over de kwetsbaarheid van, en de dreiging tegen hun informatievoorziening en ze zien informatiebeveiliging als nodeloos belastend. Risicomanagement wordt dan al snel risico-ontkenning. Externe controles vinden incidenteel plaats, maar het zou beter zijn om dit structureel en permanent op te pakken.

- **Slecht beheer**

Systemen voldoen in de eerste periode na hun operationeel stellen en bijbehorende accreditatie volledig aan de beveiligingsnormen. Het systeem is goed ingericht en alle instellingen en versies zijn juist en getest. Als het systeem langere tijd in gebruik is ontstaat het gevaar van vervuilen en achterlopen met software updates, virus definities, etc. Ook ontstaan er dilemma's zoals bij het updaten van software. Een update kan zeer noodzakelijk zijn maar kan ook onbedoelde schade veroorzaken. Omdat de systemen niet met het internet zijn gekoppeld moeten de updates manueel – met de daarbij horende vertraging – via externe media plaatsvinden. Voordat een update operationeel gaat zal hij in een labomgeving getest moeten worden op goede werking. Een ander risico is het ondeskundig aanpassen van het systeem om functionele en operationele redenen. Toevoegen van verkeerde software en hardware, het maken van gevaarlijke koppelingen en het vervangen van componenten leveren enorme risico's op. Het is dus noodzakelijk dat er een strak en deskundig beheer plaatsvindt volgens afgedwongen procedures. Dit is de enige manier om het systeem op niveau te houden. Dit vereist een duidelijke beheersdoctrine en deskundig (en schaars) personeel.

ten worden neergelegd. Deze reactie moet bestaan uit het nemen van maatregelen om de aanval te beëindigen en besluitvorming over een reactie naar de agressor. Hiervoor staat een heel spectrum aan acties ter beschikking variërend van protest, internationaal overleg en zelfs tegenaanvallen. Belangrijk hierbij is de bewijslast.

Defensie zal een rol hebben in de verkenningen van cyberspace en het vergaren van inlichtingen om zo verrassing te voorkomen en voorbereid te zijn indien moet worden gereageerd.

CYBER EN DEFENSIE ALS GEBRUIKER

De Defensie Informatie Voorziening (IV) leunt zwaar op het Internet Protocol en commerciële software. Alle voorwaarden zijn daarmee ingevuld voor een kwetsbare IV. Om op een veilige wijze de geboden en gewenste functionaliteit te benutten is de oplossing gekozen om de Defensie cyberspace te scheiden van de grote wereldwijde cyberspace (internet). Deze scheiding blijkt echter steeds meer onder spanning te staan. Om allerlei redenen ontkomt men er niet aan om informatie en data uit te wisselen tussen defensiesystemen en de onbekende buitenwereld. Denk hierbij aan bestanden van open bronnen, informatie van partners die voor hun IV gebruik maken van het internet, maar ook aan virusdefinities. De hiervoor gebruikte draaistoelinterfaces kunnen niet garanderen dat aanvallen buiten worden gehouden. Het duurt hooguit wat langer voordat je er last van krijgt. Tel hierbij op de behoefte om sneller informatie te kunnen delen door de defensienetwerken fysiek te koppelen aan de buitenwereld en de situatie dreigt te ontstaan dat de defensie IV naadloos deel uit gaat maken van de wereldwijde cyberspace.

CYBERSPACE IN VREDESTIJD

Een belangrijk uitgangspunt is dat de gebruikers van cyberspace hun systemen zelf moeten verdedigen en beveiligen tegen de dreigingen vanuit cyberspace. Dit geldt voor Defensie, andere overheden, banken en nutsbedrijven. De beveiliging moet adequaat worden geregeld waarbij nationale regelgeving moet worden gevolgd. Deze beveiliging moet in balans zijn met de noodzakelijke functionaliteit. Ontwikkelingen in de techniek en dreigingen moeten continu worden gevolgd en zo nodig leiden tot aanpassingen van het systeem en zijn beveiliging. Daarnaast zullen de systemen continu moeten worden bewaakt op aanvallen. Dit vereist zoals eerder gemeld speciale tooling en personeel.
Gelijktijdig zullen centraal gecoördineerde cyberverkenningen moeten plaatsvinden om verrassingen te voorkomen.

PUNTEN TER OVERWEGING

Het NCCD zal moeten worden belegd. Mogelijkheid is het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (GOVCERT en AIVD). Met enige fantasie zou ook het Ministerie van Defensie (DEFCERT *Defence Computer Emergency Response Team* en MIVD) deze rol kunnen krijgen. Belangrijk is dat dit meldpunt voor alle partijen betrouwbaar, integer en onbesproken is. Alleen dan zullen alle partijen (banken!) gevoelige incidenten willen melden.
In het schema staan de informatiestromen bij melding van incidenten.
De informatiestroom zal andersom lopen waar het gaat om informatie uit verkenningen en aanwijzingen naar de gebruikers van de systemen.
Het NCCD staat direct in contact met een groot aantal spelers. Ook de AIVD hoort in dit schema op een plaats waar de relatie met het NCTb en BZK tot uitdrukking komt.

TOEKOMST

De huidige cyberspace is onveilig en mistig. Het zal niet lukken om dit op korte termijn te veranderen. Voorlopig zullen we ons dus in die situatie staande moeten houden. Wel kan worden gekeken of dit op langere termijn kan veranderen. Echt veilig zal moeilijk worden maar door een andere visie op software, veiligere en betere routeringprotocollen, betere authenticatie is winst te boeken. Het is echter de vraag of dit cyberbreed gaat gebeuren.

Er zullen altijd redenen blijven waarom cyberspace onveilig blijft. Grote internationale spelers hebben invloed in cyberspace die ze niet kwijt willen. Een land met veel computers kan ze inzetten als botnet. Software die wereldwijd op bijna alle computers staat geeft de bouwer van de software feitelijk de macht over al die computers. Hetzelfde kan worden gezegd over hardware. Er zijn dus partijen die de huidige onveilige cyberspace prima vinden. Ze benutten het functioneel en offensief en zorgen dat hun eigen systemen voldoende weerstand kunnen bieden tegen de dreigingen.

STELLINGEN

1. Het onderscheid tussen *cybercrime*, *terrorism* en *warfare* is alleen te maken als bekend is wie het heeft gedaan met welk doel en met welk effect. Doorgaans is dat niet het geval. Zelfs het effect is vaak verborgen.

2. *Cyberdefense* is een gedistribueerde taak onder centrale (nationale) regie. Iedere gebruiker is zelf verantwoordelijk voor de uitvoering van zijn verdediging maar is gedwongen zich te houden aan centrale aanwijzingen.

3. De nationale organisatie van *cyber operations* (defensief en offensief) moet hiërarchisch worden opgebouwd met heldere informatielijnen en bevelstructuur. Het mag nooit onduidelijk zijn wie de leiding heeft, wie wanneer geïnformeerd moet zijn en wie verantwoordelijk is voor de uitvoering. Alleen dan is slagkracht te garanderen.

4. Vanwege de te verwachten problematiek bij de vulling van een cyber organisatie (Defensie en nationaal) is het te overwegen maximaal organisatiedelen samen te voegen om zo de schaarse capaciteit efficiënt in te zetten. Ook zal dit de communicatie verbeteren en versnellen. Het gevolg zal zijn dat er een verschil ontstaat tussen administratieve organisatie en de daadwerkelijk operationele organisatie. Denk hierbij aan het samenvoegen van GOVCERT met NCCD en DEFCERT met het Commando Cyber Strijdkrachten.

Schema informatiestromen bij melding van incidenten