# CYBER EN EOV

Luitenant-kolonel J.P.G. Verhagen EMSD, BS/AL/CDS/D-OBBP/TaskforceCyber

*Een beschouwing van de overeenkomsten en verschillen tussen cyber en EOV naar aanleiding van het 25 jarig bestaan van 102 EOVCie.*

**Op 1 januari 2012 is de Taskforce Cyber opgericht. Deze taskforce vindt zijn oorsprong in de in 2010 uitgegeven visie op cyberoperaties en de in 2011 uitgekomen uitwerking van die visie. De Taskforce Cyber heeft als taak invulling te geven aan de intensivering cyber, zoals aangekondigd in de maatregelennota van 2010, volgend op het regeringsbesluit tot de verregaande bezuinigingen voor Defensie.**

Invulling geven aan de intensivering houdt in het intensiveren van cybercapaciteit op Defensief, Inlichtingen en Offensief gebied, waarbij samenwerking en een kennis/expertise centrum expliciet genoemd werden. In 2011 heeft de toenmalige minister van Defensie, drs. J.S.J. Hillen, de Defensie Cyber Strategie uitgegeven met daarin zes speerpunten: integraliteit, defensief, inlichtingen, offensief, adaptief en innovatief en samenwerking.
Deze zes speerpunten vormen de leidraad voor de verdere ontwikkeling van het Defensie cybervermogen. Belangrijk punt is dat de bestaande verantwoordelijkheden op het defensief, offensief en inlichtingen gebied gehandhaafd moeten blijven. Hierdoor is het Joint Informatievoorzieningscommando (JIVC) verantwoordelijk voor de *Cyberdefense*, de Militaire Inlichtingen en Veiligheidsdienst voor *Cyber intelligence* en de Commandant der Strijdkrachten voor *Cyberoffense*. Binnen deze drie Defensieonderdelen worden de respectievelijke cyberelementen opgericht en gevuld, waarbij het Commando Landstrijdkrachten het op te richten Defensie Cybercommando in Single Service Management zal krijgen. In het Defensie Cybercommando komen de offensieve capaciteit en het Defensie Cyber Expertise Centrum als sub-eenheden.

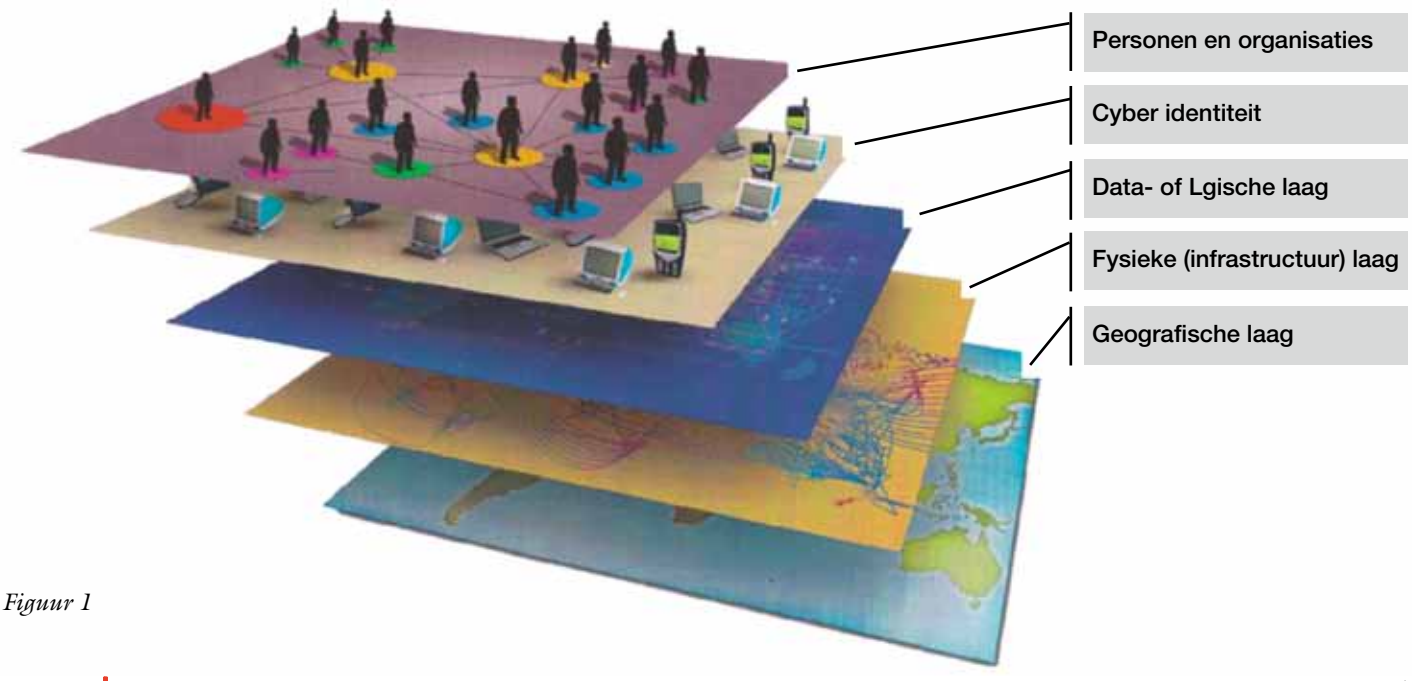
Bovenstaande is in vogelvlucht de cyberintensivering binnen het Ministerie van Defensie. Maar in vogelvlucht zijn er vele details die niet aan de orde komen. Een daarvan is dat 'cyber' wel heel veel lijkt op Elektronische Oorlogvoering en sommigen zelfs de discussie voeren welke van de twee nu ondergeschikt zou moeten zijn aan de ander. Die discussie wil ik in dit stuk beslechten, door in te gaan op de overeenkomsten en verschillen die ik zie tussen cyber en EOV.

Allereest wil ik ingaan op wat cyber is. Daarna op wat het belang van de krijgsmacht is om cyberoperaties te kunnen uitvoeren. Dan geef ik mijn visie op de overeenkomsten en verschillen met de EOV en ik sluit af met een mogelijk toekomstige ontwikkeling.

## CYBER, WAT IS HET?

Onder het digitale domein (cyber domein) moet niets meer of minder worden verstaan dan het geheel van ICT-middelen en -diensten. Hiermee wordt dus niet alleen het internet bedoeld, maar ook alle niet (altijd) met internet verbonden netwerken of andere digitale apparaten.[1] Denk daarbij aan de digitale systemen in auto's, hoog geclassificeerde netwerken, fabrieken, vitale infrastructuren en wapen- en sensorsystemen. Dit geheel noemen we cyberspace.
Als we cyberspace gedetailleerder bekijken zien we vijf lagen zoals weergegeven in figuur 1. Cyberspace kan alleen functioneren als alle lagen in samenhang met elkaar opereren.
Van onder naar boven zien we een geografische laag, een fysieke (infrastructuur) laag, een data- of logische laag, een cyber identiteit laag en een personen en organisatie laag.
De geografische laag geeft de locatie op aarde aan (waar de hardware componenten uit de cyberspace zich bevinden). Hij is van belang omdat cyberspace op zich geen grenzen kent, maar de grenzen wel degelijk van belang zijn, bijvoorbeeld in juridische zin.

1 Zie Adviesraad Internationale Vraagstukken (AIV), 2011, Digitale oorlogvoering.




*Figuur 1*

In de fysieke (infrastructuur) laag vinden we fysieke ICT objecten (de zogenaamde hardware): systemen, computers, servers, controllers (denk hierbij aan SCADA of PCS[2] systemen), bekabeling, routers, switches. Op zich doen deze 'apparaten' niets. Zij moeten gestuurd worden. De sturing vindt plaats in de logische laag.

De data- of logische laag is de laag die de fysieke laag laat functioneren en deze koppelt aan de onderliggende laag (cyber-identiteit). In deze laag bevinden zich 'cyber-objecten' zoals protocollen, software of, generiek gesteld, code en de data die de fysieke laag bewerkt, verwerkt en produceert. Door de code zijn de fysieke ICT objecten (hardware) van de fysieke laag in staat opdrachten uit te voeren, met elkaar te communiceren, en door mensen bestuurd te worden. De mensen vormen de vijfde laag in cyberspace, maar zij bewegen zich in cyberspace door een virtuele weergave: de cyberidentiteit.

Personen en organisaties nemen in cyberspace een virtuele plaats in. Een account bij een internetprovider of bij een (bedrijfs-) intranet creëert een virtueel persoon in cyberspace. Een persoon of organisatie kan vele cyberidentiteiten hebben. Het omgekeerde is echter ook waar: een groep personen kan gebruik maken van hetzelfde account en vormt daarmee maar een cyberidentiteit.[3]

In de laatste laag zijn de personen en organisaties die gebruik maken van de cyberspace. Het zijn de fysieke personen en de organisaties die alle lagen van cyberspace tot de geografische laag hebben gemaakt, besturen, en gebruiken. De cyber-identiteit laag en de personen en organisaties samen wordt ook wel de sociale laag genoemd.

## BELANG

Defensie heeft een belang in het gebruik van cyberspace. Ten eerste is er een belang omdat Defensie, net zoals de gehele Nederlandse samenleving afhankelijk is geworden van het gebruik van ICT. Het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie concludeert in het Cybersecurity beeld Nederland dat deze afhankelijkheid alleen maar zal toenemen. In datzelfde Cybersecurity beeld Nederland wordt geconcludeerd dat de grootste dreiging op overheid en bedrijfsleven digitale spionage is en blijft, mogelijk vanuit staten. De grootste kwetsbaarheid ligt bij de eindgebruiker, die een beperkte kennis en mogelijkheden lijkt te hebben om de beveiliging goed te doen. Die eindgebruikers zijn ook onze militairen, zowel privé als binnen de militaire organisatie.
Het tweede belang komt voort uit de Nationale Cyber Security Strategie. Hierin wordt gesteld dat elke eigenaar van een netwerk zelf verantwoordelijk is voor de cybersecurity van dat netwerk.[4] Defensie is daarin een van de spelers. Defensie heeft daarbij wel een onderliggend, of beter gezegd een bovenliggend belang. Naast onze netwerken zijn onze wapen- en sensorsystemen doorspekt met ICT. Wanneer die niet goed beveiligd worden en daardoor niet (optimaal) gebruikt kunnen worden komt onze rol en daarmee onze taak in gevaar. Onze rol is die van zwaardmacht – een geweldsinstrument van de regering – met een drieledige taak: de bescherming van de integriteit van het eigen en bondgenootschappelijke grondgebied, met inbegrip van het Koninkrijk in het Caribisch gebied; bescherming en bevordering van de internationale rechtsorde en stabiliteit; ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal (art 97 GW). Dit geeft gelijk aan waarom Defensie zowel defensieve, inlichtingen als offensieve capaciteit nodig heeft: defensief, bescherming van de netwerken (inbegrepen de wapen- en sensorsystemen); inlichtingen: zorgdragen voor voldoende kennis over een mogelijke bedreigingen op Defensie zodat defensief maatregelen genomen kunnen worden en offensief binnen bestaande juridische kaders kan worden voorbereid; offensief: het kunnen 'slaan' van een actor binnen de daarvoor geldende juridische kaders. In feite niets anders dan we binnen het zee-, land-, lucht- en ruimtedomein ook zien.


*Figuur 2: De hoofdtaken van defensie.*

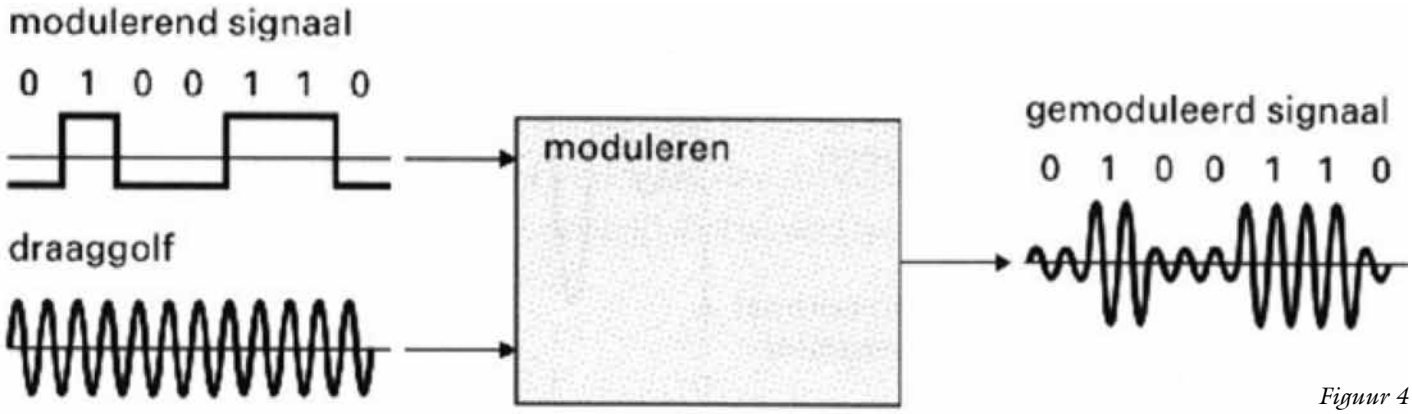
## CYBER EN EOV

Zonder verder in te gaan op het zee-, land, lucht- en ruimtedomein, nu de stap naar EOV. EOV capaciteit zien we namelijk ook terug in alle domeinen en met een zelfde driedeling. Elektronische oorlogvoering bestaat uit electronic surveillance, *electronic attack en electronic protection*. Dit is de eerste overeenkomst met cyber, grafisch weergegeven in figuur 3.


*Figuur 3*

Het verschil daarin is dat cyber het vijfde domein wordt genoemd en EOV binnen de domeinen als capaciteit wordt geduid. De domeindiscussie hoeft echter in de context van dit stuk niet gevoerd te worden.
Een tweede overeenkomst is te zien in de offensieve kant van beide capaciteiten. Offensieve cyberactiviteiten richten zich qua locatie op andermans cyber middelen, waar zij, zonder toestemming van de eigenaar, als deel van een militaire operatie 'schade' toebrengen aan c.q. beïnvloeden van het gedrag van een andere actor. Als deel van een militaire operatie 'schade' toebrengen aan c.q. beïnvloeden van het gedrag van een andere actor is een doelstelling die ook met EA wordt nagestreefd.
Een derde overeenkomst is dat zowel EOV als cyber gebruik maken van het elektromagnetisch spectrum. Daar ligt echter ook het tweede verschil.

2 SCADA = Supervisory Control And Data Acquisition, PCS = Process Control System
3 Zie P. Ducheine & J. van Haaster, 'Cyber-operaties en militair vermogen', in: Militaire Spectator 2013-9, pp. 268-387.
4 Dit is niet de exacte bewoording, maar wel de strekking van het gestelde.




*Figuur 4*

EOV richt zich op het elektromagnetisch spectrum 'in de vrije ruimte'. Alle vormen van emissie kunnen door EOV middelen worden opgevangen en daarna geanalyseerd, en wellicht ook nog worden gemanipuleerd en hergebruikt. Cyber daarentegen gebruikt het elektromagnetisch spectrum vooral in de 'beperkte ruimte': computers, gegevensdragers, bekabeling en alle andere typen van hardware die we terugvinden in de fysieke (infrastructuur) laag. Er is een duidelijk koppelvlak aan te wijzen: wifi. Door gebruik te maken van wifi wordt de 'beperkte ruimte' gekoppeld aan de 'vrije ruimte' en omgekeerd. Wifi moet echter niet te beperkt worden gezien, maar dient als herkenbaar voorbeeld. Wat opvalt, is dat in dit koppelvlak een verschil kan leiden tot synergie.

Wanneer we traditioneel kijken richt de EOV zich op emissie (golven) en cyber op datastromen ('enen en nullen'). Wat we bij een koppelvlak als wifi zien gebeuren is dat de een gebruik gaat maken van de ander: datastromen worden gemoduleerd op draaggolven. Opeens zijn cyber en EOV gecombineerd zoals in figuur 4 weergegeven.

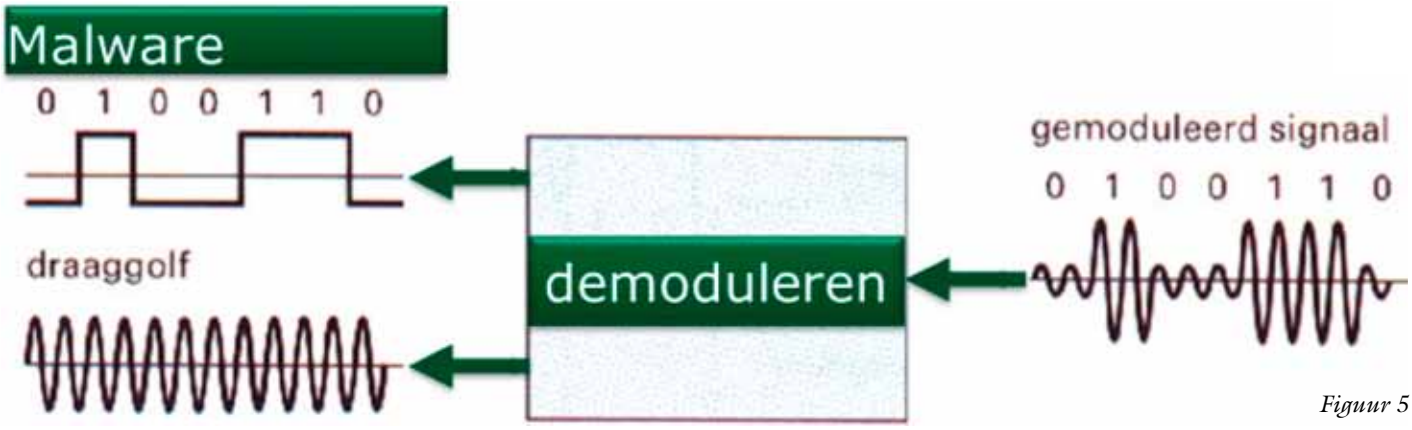
Op die manier wordt het mogelijk om via opgevangen signalen de gemoduleerde data te analyseren waardoor (in het gunstigste geval) mogelijkheden tot inbraak in genetwerkte systemen aan het licht komen. Concreet bijvoorbeeld account gegevens waaronder passwords, protocollen, samenstellingen van netwerken, softwareversies etc.

Dit alles staat in het kader van het opvangen van golven en het analyseren van de gegevens die verwerkt worden tot informatie en inlichtingen. In het kader van offensief of het verbeteren van de informatie vergaring biedt modulatie ook kansen zoals weergegeven in figuur 5.

Wanneer de mogelijkheid bestaat om uitzendingen te doen op de systemen (bijvoorbeeld radio of straalzendersystemen) van een andere actor (of opponent) met een gemoduleerd signaal, kan na demodulatie *malware* het systeem binnen dringen. Deze *malware* kan andere poorten openzetten zodat het makkelijker wordt op een andere manier het systeem binnen te dringen, of juist het wegsluizen van informatie te vergemakkelijken. Ook kan deze *malware* schade aanrichten in het systeem om daarmee de in een militaire operatie gewenste effecten te bereiken. Het koppelvlak tussen cyber en EOV zorgt zo voor synergie. Het nader uitwerken van deze gedachte zou in de toekomst van de EOV en cyber kunnen zorgen voor een nauwe samenwerking tussen deze twee capaciteiten.

## TOEKOMST

In de visie op EOV zijn vier wijzen van inzet geconstateerd: statisch, verplaatsbaar, mobiel en uitgestegen. Binnen de EOV is dit niet geheel nieuw, maar een voortzetting op al bestaande concepten. Met nieuwe moderne middelen is een en ander beter en wellicht gemakkelijker uitvoerbaar.
Voor cyber is de statische wijze van inzet nu in ontwikkeling. De defensieve capaciteit binnen het JIVC die vanuit een locatie in Nederland zijn werkzaamheden uitvoert; MIVD die vanuit haar locatie inlichtingen verzorgt en offensief waar nog niet een definitieve locatie voor is gekozen.
Over een verplaatsbare capaciteit zijn wel ideeën. Bijvoorbeeld voor het defensief, waarbij het inrichten van een vooruitgeschoven CERT in een inzetgebied met een reachback naar het DefCERT een optie kan zijn, analoog aan TITAAN met een MCCC in het inzetgebied en een centrale capaciteit in Nederland.
De mobiele en de uitgestegen variant zijn nog niet zo ver. Hierover moet nog nagedacht worden. Wellicht is het mogelijk de synergie zoals hierboven beschreven met EOV te beschouwen in de gedachtevorming van mobiele en uitgestegen cybercapaciteit.
In de nabije toekomst is een nauwere samenwerking tussen cybercapaciteiten en EOV zichtbaar. Hoewel niet de term EOV gebruikt wordt maar SIGINT, wat toch nauw verwant is met EOV. De Joint SIGINT Cyber Unit is wat hier bedoeld wordt. Een samenwerking tussen AIVD en MIVD waarbij SIGINT en cyber bij elkaar worden gebracht om voordelen te behalen uit deze combinatie. Wellicht is dit voor EOV en cyber op een lager niveau ook mogelijk. Waar twee capaciteiten een overeenkomst vertonen in de onderverdeling van de inzetwijzen (figuur 3) en de vermenging zoals in figuur 5 weergegeven, ligt een nauwe samenwerking in de toekomst voor het oprapen.




*Figuur 5*