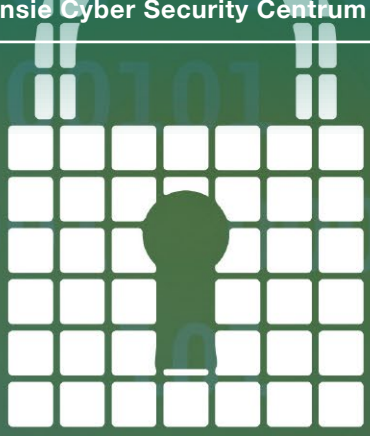
HET DEFENSIE CYBER SECURITY CENTRUM

Kolonel Kees Verdonk, Hoofd Afdeling Defensie Cyber Security Centrum



Kolonel Kees Verdonk is hoofd van het Defensie Cyber Security Centrum (DCSC). Het DCSC is op 1 januari 2019 opgericht als onderdeel van de samenvoeging van het 'oude' JIVC en OPS tot het huidige JIVC. Het DCSC bestaat uit het SIOC[1] (afkomstig uit OPS) en DefCERT[2] (onderdeel van het JIVC). Door deze samenvoeging zijn de cyber securitycapaciteiten binnen het JIVC verder geïntegreerd en versterkt. In dit artikel beschrijft kol Verdonk het belang voor defensie om informatie en de onderliggende ICT-systemen te beschermen (digitale weerbaarheid), de rol van het DCSC in de beveiligingsketen en de toekomstige ontwikkelingen bij het DCSC. ➔

Informatiegestuurd Optreden

Tijdige beschikbaarheid van de juiste informatie is een absolute randvoorwaarde voor de succesvolle inzet van de krijgsmacht. Om die reden heeft de Minister van Defensie in de Defensienota 2018 besloten dat Defensie informatiegestuurd gaat optreden. Het concept Informatiegestuurd Optreden (IGO[3]) is verder uitgewerkt in de onlangs uitgegeven Defensie IT-strategie. IGO vormt daarbij de kern en wordt gedragen door vijf pijlers[4], waarvan Digitale Weerbaarheid er één van is. Immers, bescherming van informatie en de onderliggende ICT-netwerken, systemen en applicaties is essentieel om te voorkomen dat informatie in verkeerde handen valt, wordt gemanipuleerd of niet beschikbaar is. Daarom vormt digitale weerbaarheid ook in de Defensie Cyber Strategie uit november 2018 een belangrijk speerpunt.

Digitale weerbaarheid

Digitale weerbaarheid zorgt ervoor dat informatie:

- tijdig en continu beschikbaar is (beschikbaarheid);
- alleen toegankelijk is voor bevoegde medewerkers (vertrouwelijkheid/exclusiviteit);
- juist, volledig en actueel is en alleen kan worden aangepast door bevoegde medewerkers (integriteit).

Om aan deze eisen te voldoen, moet Defensie een groot aantal maatregelen uitvoeren die onder andere in de HDBV-instructie D/300 (Beveiliging van IT-diensten) is beschreven.
Om deze maatregelen op een logische wijze te groeperen, heeft het JIVC gekozen voor het Cyber Security Framework van het National Institute of Standards and Technology (NIST). Het gebruik van dit framework bevordert het 'eenheid van denken' over informatiebeveiliging en maakt het mogelijk om de volwassenheid ervan beter te beoordelen en te verbeteren. Het framework bestaat uit vijf elementen die samen de schakels van de informatiebeveiligingsketen vormen.
Deze elementen zijn weer verdeeld in 22 categorieën en 108 subcategorieën die goed koppelbaar zijn aan de richtlijnen uit de D/300. De subcategorieën bevatten een normering. Zo stelt het framework de eis dat backups van informatie moeten worden uitgevoerd, onderhouden en getest (als onderdeel van de categorie Protect/Information protection & procedures). De instructie D-300 beschrijft hoe deze norm moet worden ingevuld binnen Defensie.

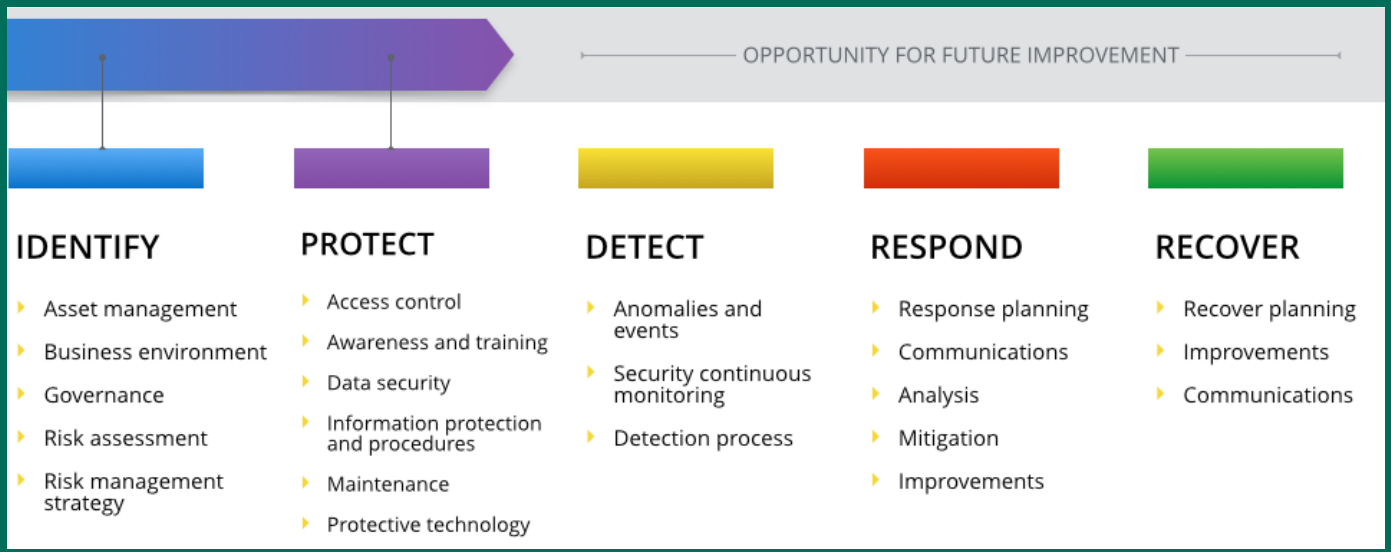
Om de beveiligingsketen te sluiten, zijn meerdere organisaties betrokken zoals de Beveiligingsautoriteit (BA), het JIVC, de systeemeigenaren (bijv. HDP voor PSFT) en de Opco's. Bij de invulling van de schakel Identify hebben met name commandanten, systeemeigenaren en beveiligingsfunctionarissen een belangrijke rol. De elementen Protect en Recover liggen vooral bij de afdelingen Architectuur (inrichting van de IT-infrastructuur) en bij de IT-beheerorganisaties (uitvoering van de beveiligingsmaatregelen).

De rol van het DCSC

Binnen de beveiligingsketen levert het DCSC een unieke bijdrage aan de digitale weerbaarheid van Defensie door:

- leveren van informatie en advies ter ondersteuning van alle schakels uit het framework;
- het detecteren (Detect) van kwetsbaarheden en inbreuken

[1] SIOC: Security Intelligence & Operation Centre.
[2] DefCERT: Defense Computer Emergency Response Team.
[3] "InformatieGestuurd Optreden (IGO) houdt in dat we in staat zijn om alle relevante informatie op ieder gewenst niveau tijdig te verwerven, te verwerken en te verspreiden opdat we zo veel mogelijk met de juiste middelen, op het juiste moment op de juiste plaats zijn. Dit stelt eisen aan (de kwaliteit en mogelijkheden) van materieel waarmee we werken en aan onze manier van werken" (uit de Defensienota 2018).
[4] De overige pijlers zijn: Robuust, Wendbaar, Interoperabel en Data-gedreven.



Het NIST Cyber Security Framework.

op de bescherming van informatie (incidenten);
- het reageren (Respond) op informatiebeveiligingsincidenten samen met de systeemeigenaren en technisch beheerders van de netwerken, systemen en applicaties.

Het DCSC voert deze taken niet alleen uit voor ICT-netwerken en systemen die bij JIVC onder beheer zijn, maar - voor zover mogelijk- ook voor systemen die onder de verantwoordelijkheid van de Opco's vallen.

Informatie en advies

Cyberdreigingen tegen Defensie zijn omvangrijk, divers en variëren van zgn. scriptkiddies met eenvoudige en goedkope hacking tools tot aan staten met geavanceerde cyberwapens. Bovendien ontwikkelen deze wapens zich snel waardoor ook de aard en omvang van de dreiging voortdurend wijzigt. Het is daarom noodzakelijk dat de basisbeveiliging (mn. de schakels Identify en Protect) bij Defensie goed op orde is.
Anderzijds is actuele informatie over nieuwe dreigingen en kwetsbaarheden belangrijk om eventuele zwakke plekken in de eigen basisverdediging tijdig te signaleren en op te lossen. Daarom beschikt het DCSC over een Sectie Situational Awareness die dergelijke informatie verzamelt, analyseert en de betrokken partners (binnen en buiten Defensie) informeert.

Detectie van kwetsbaarheden en inbreuken

De detectie-activiteiten van het DCSC zijn er zoveel mogelijk op gericht om inbreuken te voorkomen door kwetsbaarheden in ICT-netwerken en systemen tijdig op te sporen en deze samen met de IT-beheerorganisatie en de systeemeigenaren op te lossen. De Sectie Assessments van het DCSC voert daarom op verzoek van Opco's en systeemeigenaren onderzoeken uit naar de kwetsbaarheden en restrisico's van (operationele) systemen. Zo heeft de Sie Assessments onder andere onderzoeken uitgevoerd op het Battlefield Management System

(BMS), diverse commandovoeringssystemen op schepen en informatiesystemen voor het F-35-project. Daarbij wordt onder meer gekeken op welke wijze deze systemen in operationele omstandigheden worden gebruikt. In overleg met de opdrachtgever wordt de onderzoeksmethode vastgesteld die kan variëren van een 'eenvoudige' desk study tot een volledige penetratietest[5] in een operationele setting.

Naast specifieke onderzoeken monitort het DCSC dagelijks de ICT-netwerken en systemen van Defensie met behulp van sensoren. De Sectie Monitoring 'bekijkt' en 'zoekt' daarbij vooral naar (de afwijkingen in) het netwerkverkeer, de loggingsdata van systemen en applicaties, en het activiteiten door gebruikers op de werkstations (end points). Vanwege de continue aanpassingen in de verouderde ICT-netwerkstructuur[6], de snel evoluerende dreigingen en nieuwe kwetsbaarheden maakt monitoring intensief gebruik van schaars cyberpersoneel.

Bovendien kan DCSC niet alle netwerken/systemen 'zien' die in gebruik zijn bij Defensie. Het gaat dan vooral om (lokale) netwerken die door de Opco's zelf worden beheerd. Daarom maakt DCSC afspraken met de Opco's over de monitoring en incident response-maatregelen voor deze netwerken.

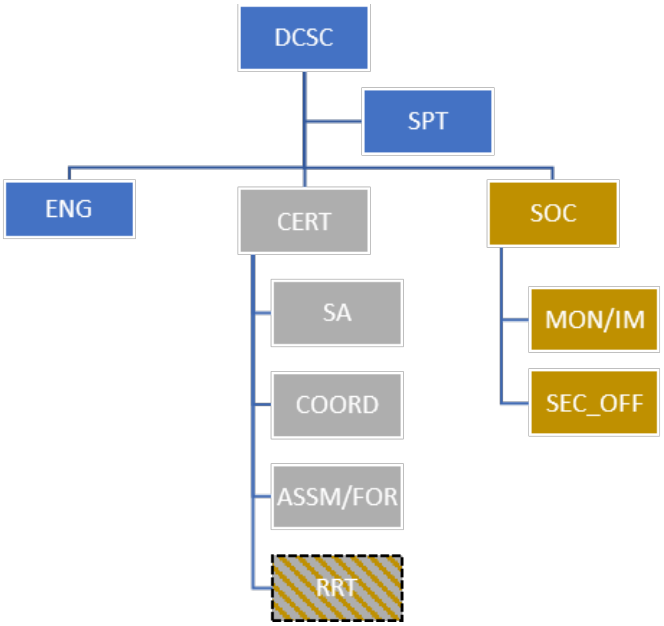
Incident Response

Mocht er zich een incident voordoen, dan is het belangrijk de onveilige situatie snel op te lossen om de schade zoveel mogelijk te beperken. Hiertoe beschikt het DCSC over een Sie Incident Management en drie Security Officers die direct de afhandeling van het incident coördineren samen met de direct betrokken spelers (zoals de technisch beheerder en beveiligingsfunctionaris bij het JIVC of het Opco, de systeemeigenaar, BA, MIVD). Per maand handelt DCSC enige honderden incidentmeldingen af.

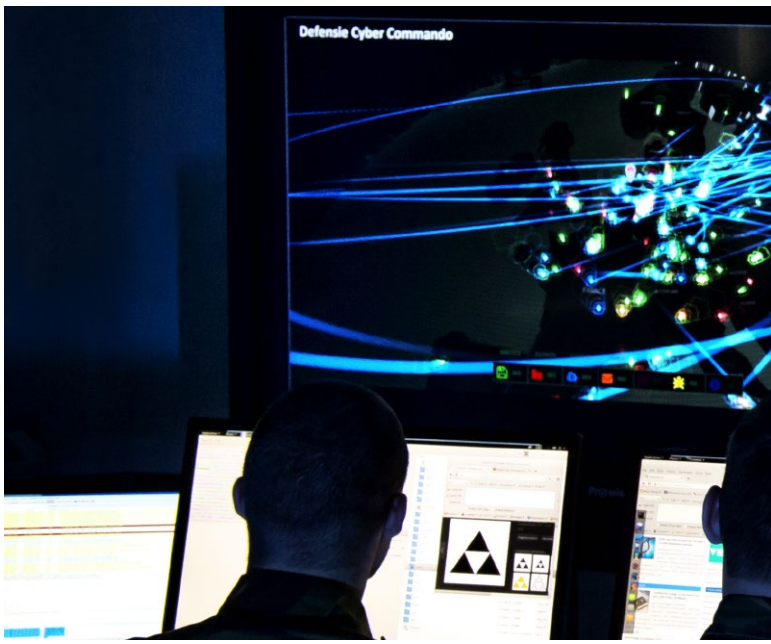
Daarnaast onderzoekt de Sectie Forensisch Onderzoek de toedracht, oorzaken en – indien mogelijk – de daders van het incident. De onderzoeksresultaten wordt vervolgens gebruikt om het incident op een juiste wijze op te lossen, als bewijsmateriaal voor een eventueel strafrechtelijk onderzoek (KMar) en als

[5] Bij een penetratietest of pentest (binnendringingstest) wordt getracht onder gecontroleerde omstandigheden informatie uit een beveiligd systeem te verkrijgen of te manipuleren zonder de vereiste toegangsgegevens door gebruik te maken van kwetsbaarheden.

[6] bijv. door upgrades/herconfiguratie van systemen en de ontplooiing van tijdelijke netwerken tijdens oefeningen/missies.



Organisatiestructuur DCSC per 1 januari 2019.



inlichtingenbron voor de MIVD. Daarnaast kunnen met deze informatie eventueel bestaande kwetsbaarheden in de ICT-netwerken worden opgespoord en opgelost. Verder beschikt het DCSC over drie Rapid Reaction Teams (RRTs) die binnen 72 uur kunnen worden ingezet om incidenten in binnen- en buitenland op te lossen. Deze capaciteit is ook aan de EU aangeboden. De teams bestaan 'in rust' alleen uit materieel. Bij inzet worden de teams gevuld met medewerkers uit de andere DCSC-afdelingen tot een maximaal van zeven personen. De deelnemers worden per incident uitgekozen op basis van de benodigde expertise om het incident op te lossen.

Interne DCSC-ondersteuning

Om haar taken goed uit te voeren, heeft het DCSC de beschikking over twee eigen ICT-netwerken die worden beheerd door de Sectie Engineering.

Deze sectie voert ook het technisch beheer uit van al het IT-materieel (hard- en software) dat bij het DCSC aanwezig is en zorgt er bijvoorbeeld voor dat het RRT-materieel inzetgereed is. Daarnaast levert de Sectie Support alle noodzakelijke non-IT ondersteuning, bijvoorbeeld bij de inzet van de RRT, bij bezoeken aan missies en bij oefeningen (vervoer, overnachtingen, diplomatieke zaken, clearances, etc.).

Samenwerking

Uit bovenstaande blijkt dat samenwerking een absolute must is om de informatie en de ICT-netwerken goed te beschermen en de beveiligingsketen te sluiten. Daarom heeft het DCSC voor elke Opco een aparte coördinator aangesteld die het Opco adviseert over digitale weerbaarheid en gezamenlijke activiteiten coördineert, zoals de afstemming van monitoring en Incident Response activiteiten. Daarnaast heeft het DCSC regelmatig overleg met de beveiligingsorganisaties van HDBV (BA), het JIVC en de Opco's, de Directie Operaties van de CDS, MIVD, het Defensie Cyber Commando en de Hoofddirectie Beleid over cyber security gerelateerde onderwerpen. In lijn met de Defensie Cyber Strategie neemt ook de samenwerking tussen de ministeries toe die overheidsbreed wordt gecoördineerd door het Nationaal Cyber Security Centrum (Min-V&J). Zo neemt het DCSC onder meer deel aan het Nationaal DetectieNetwerk (NDN) en het Nationaal Response Netwerk (NRN). Het NDN richt zich onder andere op de verzameling en verspreiding van informatie over dreigingen en kwetsbaarheden. In het NRN worden de incident response procedures van de ministeries op elkaar afgestemd zodat zij elkaar kunnen ondersteunen bij een cyberaanval. Daarnaast is het DCSC diverse malen verzocht om ondersteuning te leveren aan grote evenementen. Zo heeft het DSCS op verzoek van het Ministerie van Binnenlandse Zaken het ICT-netwerk van de Global Entrepreneurship Summit 2019 op kwetsbaarheden onderzocht. Tot slot werkt DCSC ook in internationaal verband samen met EU/NAVO-partners[7] zoals bij inzet (bijv. de eFP-missie) en tijdens de jaarlijkse NAVO-oefening CYBER COALITION.

Way Ahead

Dit jaar heeft vooral in het teken gestaan van de oprichting van het DCSC en het opzetten van de interne bedrijfsvoering. Voor de komende periode richt het DCSC zich op de verdere verbetering van haar huidige taken, zoals de verdere versterking van de monitoringcapaciteit om meer ICT-netwerken op meerdere wijzen te monitoren en te onderzoeken.

Daarnaast vinden er experimenten plaats om de detectie- en response-activiteiten zoveel mogelijk te automatiseren. Hierdoor kunnen kwetsbaarheden snel worden gedetecteerd en

[7] Dit jaar is het DCSC de voorzitter van de EU PESCO-werkgroep over Cyber Rapid Reaction Teams (CRRT).

opgelost. Daarnaast neemt door de automatisering het aantal menselijke fouten af en kan het schaarse cyberpersoneel voor andere noodzakelijke taken binnen het DCSC worden ingezet.
Ook de informatiepositie van het DCSC en de mogelijkheid om informatie sneller te verspreiden, zal de komende periode verder worden verbeterd door onder andere de aanschaf van nieuwe Threat Intelligence-systemen en het gebruik van moderne datascience-technieken.

Daarnaast investeert het DCSC samen met de HDBV/Beveiligingsautoriteit en de Opco's in het opzetten van een defensiebreed monitoring- en Incident Response-framework dat door de Opco's wordt gebruikt bij het opzetten van lokale monitoring- en incident response-functionaliteiten voor de eigen netwerken. Daarbij wordt ook rekening gehouden met de toekomstige vervanging van de huidige IT-infrastructuur.

Tot slot gaat het DCSC de behoeftes aan cyberonderzoeken (assessments) op ICT-systemen defensiebreed coördineren zodat het schaars cyberpersoneel effectief en efficiënt wordt ingezet. Bovendien kunnen op deze wijze de onderzoeksresultaten sneller en beter met alle partijen worden gedeeld.
Afsluitend kan worden gesteld dat door de actuele cyberdreigingen en de snelle technologische ontwikkelingen het DCSC functioneert in een uitdagende en dynamische omgeving. In deze omgeving levert het DCSC samen met haar partners een waardevolle bijdrage aan de bescherming van belangrijke informatie(netwerken) tegen cyberaanvallen en ondersteunt daarmee direct de succesvolle inzet van de krijgsmacht.

Nieuw!

De doctrine voor cyberoperaties

Er is een Nederlandse Defensie Doctrine voor Militaire Cyberspace Operaties die hierover een gemeenschappelijk beeld schetst. Het Defensie Cyber Commando ontwikkelde het document samen met de NLDA. De doctrine is inmiddels vastgesteld en voorzien van de handtekening van Commandant der Strijdkrachten luitenant-admiraal Rob Bauer.

Commandant DCC commodore Elanor Boekholt-O'Sullivan legt uit: "Na een aantal jaren van nadenken en experimenteren, is nu vastgelegd hoe de krijgsmacht momenteel aankijkt tegen militaire operaties in, of via cyberspace. Deze doctrine vormt de basis voor hoe we de planning, uitvoering en beoordeling van militaire cyberspace operaties aanpakken. Ik hoop dat veel collega's even tijd nemen om er kennis van te nemen. De activiteiten in cyberdomein zullen alleen maar groeien, het is dus goed om op de hoogte zijn van wat Defensie ook in dit domein op de mat legt."