HCSS Security

Naar een Cybercapaciteitenportfolio voor de Koninklijke Landmacht

Louk Faesen, Tim Sweijs, Frank Bekkers & Timon Domela Nieuwenhuis Nyegaard

Inhoudsopgave

1 Inleiding

1.1 Context

Moderne conflictvoering heeft een hybride karakter waarbij het onderscheid tussen oorlog en politiek, conflict en vrede, soldaat en burger en gevechtsveld en veilige gebieden is vervaagd. Militaire organisaties zijn permanent actief, in een bredere omgeving dan een min of meer afgebakend 'gevechtsveld', en vanuit een breder palet aan te bereiken effecten. Militaire cyberoperaties vormen een integraal onderdeel van het takenpakket van een moderne krijgsmacht. Er is sprake van wisselwerking en synergie tussen activiteiten in de fysieke wereld enerzijds, en in cyberspace, het elektromagnetische spectrum en de informatieomgeving anderzijds. De capaciteiten die essentieel zijn voor militaire dominantie op het tactische niveau – daar waar tegenstanders elkaar direct treffen – worden door de synchronisatie tussen cyberoperaties, elektronische oorlogsvoering (EOV) en informatieoperaties ook strategisch ingezet, met effecten buiten het directe slagveld.[1]

De Nederlandse defensieorganisatie heeft het afgelopen decennium forse stappen gezet in het ontwikkelen van strategieën, structuren, capaciteiten en een doctrine voor het cyberdomein.[2] Tegelijkertijd liggen er nog belangrijke uitdagingen in dit snel ontwikkelende domein. Diverse bondgenoten en tegenstanders hebben een voorsprong in zowel de omvang als in de strategische en operationele inbedding van militaire cybercapaciteiten.[3] Defensie werkt aan de ontwikkeling van defensieve en offensieve cybercapaciteiten op verschillende niveaus. Het Defensie Cybercommando DCC is hierbij het leidend orgaan. DCC is tevens het aangewezen organisatieonderdeel om, bij gegeven mandaat, offensieve operaties uit te voeren. Sinds juli 2018 valt het DCC direct onder de Commandant der Strijdkrachten, waar het voorheen was ondergebracht bij de Landmacht (als single-service manager). Sinds 2019 positioneert het DCC zich meer als strategische effectenbrenger en richt zich minder op tactische effecten. Hierdoor ontstaat er een vacuüm dat door de Operationele Commando's moet worden opgevuld. De Landmacht bezint zich daarom op haar eigen rol in het cyberdomein, het elektromagnetische spectrum en de bredere informatieomgeving. De leidende gedacht is dat verkrijgen, aanwenden en inzetten van cyber en elektromagnetische capaciteiten steeds meer een randvoorwaarde is voor succes in het (land)optreden.

---

[1] Zo worden bijvoorbeeld Russische EOV-capaciteiten niet alleen ingezet voor tactische counter-A2/AD of Supression of Enemy Air Defences (SEAD) toepassingen, maar ook voor psychologische en cyberoperaties. In het conflict in Oost-Oekraïne heeft de Russische krijgsmacht toegang weten te krijgen tot communicatiemiddelen van de Oekraïense troepen en dit gebruikt om de moraal van deze troepen te ondermijnen. Het Russische vermogen om het elektromagnetisch spectrum en cyberspace uit te buiten, in combinatie met holistisch militair denken, resulteert in een sterke focus op psychologische oorlogsvoering. In deze context zijn EOV-capaciteiten door Rusland vaak ingezet om effecten te realiseren die verder gaan dan de conventionele NAVO-toepassing van EOV. Zie Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025* (ICDS: September 2017), p.V.

[2] De Nederlandse Defensie Doctrine voor Militaire Cyberspace Operaties (NDD-MCO) is de meest recente aanvulling op de eerste Defensie Cyberstrategie uit 2012 en de actualiseringen daarvan in 2015 en 2018. De actualisering uit 2015 voorzag in de oprichting van het Defensie Cyber Commando (DCC), de gezamenlijke Joint Sigint Cyber Unit (JSCU) van de AIVD en de MIVD en de versterking van het Defensie Computer Emergency Response Team (DefCERT) binnen DCSC.

[3] Dit blijkt uit openbronnen analyses van de inzet van militaire cyber-capaciteiten door andere landen als ook uit de publicatie van cyberdoctrines en field manuals.

Cyber-Elektromagnetische Activiteiten (CEMA)

Net als cyberspace doorkruist het elektromagnetisch spectrum (EMS) de fysieke domeinen. EMS betreft de vrije ruimte waarin signalen worden uitgewisseld op verschillende frequenties ter ondersteuning van onder meer communicatie-, radar- en satellietsystemen. Door het beperkte bereik van de meeste signalen is nabijheid vereist. De Operationele Commando's voorzien in die nabijheid. Binnen het landoptreden is de EOV-compagnie de gespecialiseerde eenheid om het EMS te benutten. Vaak vormen radioverbindingen, 4G, 5G en WiFi in het EMS de draadloze toegang tot civiele ICT-systemen (IP-based of mobiele netwerken en systemen) en militaire ICT-systemen (tactische radio's en datalinks).

Deze draadloze verbindingen vormen de basis voor Cyber-Elektromagnetische Activiteiten (CEMA). CEMA omvat onder meer "het inzetten van EOV-capaciteiten voor het opzetten en uitvoeren van cyberoperaties."[4] Dit geeft bijvoorbeeld toegang tot vijandelijke (wapen-) systemen. EOV- en cybercapaciteiten hebben dus veel raakvlakken en kunnen elkaar versterken, mits ze gesynchroniseerd en gecoördineerd worden ingezet. Er is, kortom, noodzaak tot afstemming om ervoor te zorgen dat de verschillende operaties elkaar complementeren in termen van doel- en effectbereiking binnen het landoptreden; en om potentiële interferentie en conflicten in het gebruik van de bijbehorende capaciteiten te voorkomen.[5] Het EMS en cyberspace vormen de basis voor een groot aantal joint functies en door de overlap van de domeinen en middelen, al dan niet voor verschillende doeleinden, is het verstandig om een effectgerichte multidomeinbenadering te hanteren waarbij deconflictering en afstemming van deze verwante activiteiten gecoördineerd worden en ondersteund worden door inlichtingenactiviteiten.[6]

1.2 Deze notitie

Tegen deze achtergrond heeft het Commando Landstrijdkrachten (CLAS) het *Den Haag* Centrum voor Strategische Studies (HCSS) gevraagd te onderzoeken wat de (mogelijke) rol van de Landmacht in het cyberdomein kan c.q. moet zijn en welke capaciteiten de Landmacht dient te ontwikkelen om de bij deze rol passende effecten te kunnen bereiken. Deze notitie vormt het resultaat van de analyse en heeft tot doel bij te dragen aan de gedachtenvorming over een effectgerichte benadering die de schaarse cyberexpertise en -middelen efficiënt inzet. De notitie richt zich op cyberoperaties die relevant zijn voor het landoptreden en hoe deze ondersteund worden door inzet van, deels al bestaande, capaciteiten in het elektromagnetische spectrum.

---

[4] Ministerie van Defensie, *Visiedocument Joint Elektronische Oorlogsvoering (EOV) Concept 1.6*. (mei 2019), p7.
[5] P.A.L. Ducheine, J van Haaster en R. van Harskamp, *Manoeuvring And Generating Effects In The Information Environment*.
[6] Deconflictering behelst het delen van informatie om vast te stellen of meerdere actoren zich richten op hetzelfde individu of dezelfde organisatie voor verschillende doeleinden. Als er bijvoorbeeld heimelijke inlichtingen worden verzameld bij een bepaald doelwit, kan deze inlichtingenoperatie abrupt gestopt worden door een cyberaanval van een bondgenootschappelijke partij. Door deconflictering kunnen actoren bewust worden van hun gedeelde belangen om zo inbreuk op elkaars activiteiten te minimaliseren en de effectiviteit van een operatie te maximaliseren. Zoals beschreven in Hoofdstuk 0, hoort de geïntegreerde CEMA-aanpak onderlinge concurrentie voor dezelfde middelen en wederzijds interferentie te voorkomen of in ieder geval in goede banen te leiden.

De notitie is opgesteld op basis van een analyse van de militaire en academische literatuur en van interviews met betrokkenen binnen Defensie. Daarbij waren de volgende deelvragen leidend:

1. **Effecten**: welke (militaire) effecten dienen te worden bereikt in cyberspace? In hoofdstuk 2 worden de benoemde effecten van de NAVO *Allied Joint Doctrine for Cyberspace Operations* benoemd en als uitgangspunt gebruikt om de rol van de Landmacht nader te duiden.
2. **Rol Landmacht:** wanneer is de Landmacht aan zet in cyberspace? Dit wordt behandeld in hoofdstuk 3.
3. **Activiteiten:** Welke activiteiten moet de Landmacht ontplooien om de door haar beoogde effecten te realiseren voor de land-cyber integratie? Hoofdstuk 4 gaat hier op in.
4. **Ontwikkeling:** Hoe kunnen de relevante capaciteiten worden ontwikkeld binnen de Landmacht? Hiertoe worden in het slothoofdstuk 5 aanbevelingen gedaan voor de DCTOMPFI-aspecten Doctrine, Commandovoering, Training, Organisatie, Materieel, Personeel, Faciliteiten en Interoperabiliteit.

De grijze zone en het Nederlandse mandaat

Landen als Rusland en China maken volop gebruik van de 'grijze zone' van conflict, het schemergebied tussen vrede en oorlog. Ze benutten offensieve cyber- en informatiemiddelen om onder de juridische drempel van oorlogsvoering ambiguïteit te creëren.[7] Het mandaat, en daarmee de handelingsruimte, van vele westerse landen om in vredestijd offensieve militaire tegenmaatregelen te treffen is beperkt.

De VS heeft tot dusver gereageerd met *cross-domain deterrence*, waarin afstraffing vooral publieke attributie, het vervolgen van hackers en het opleggen van sancties betrof. Het Amerikaanse CYBERCOM beargumenteert dat deze vorm van afschrikking niet effectief is gebleken, mede door het gebrek van geloofwaardigheid van Amerikaanse tegenmaatregelen in cyberspace.[8] De nieuwe Amerikaanse *defend forward* en *persistent engagement* doctrine zou hier een einde aan moeten maken.[9] Onder deze doctrine opereert CYBERCOM niet langer alleen reactief, wachtend tot de juridische drempel van conflict is overschreden, maar "ten alle tijde en overal" met als taak de vijand te weren.[10] Het heeft daartoe een breed mandaat om buiten de

[7] De Russische militaire doctrine van 2010 stelt bijvoorbeeld dat: "The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness [...] The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures [...] All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict."
[8] Lauren Williams, "Nakasone Talks Cyber Deterrence at Confirmation Hearing", *Defense Systems*, 2 maart 2019, https://defensesystems.com/articles/2018/03/02/nakasonecybercom-confirmation.aspx.
[9] US Department of Defense, *Department of Defense Cyber Strategy: Summary*, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[10] Paul M. Nakasone, 'A Cyber Force for Persistent Operations', *Joint Force Quarterly* 92, no. 1, (2019), http://cs.brown.edu/courses/csci1800/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf.

Amerikaanse netwerken en grenzen effecten te bewerkstelligen.[11] Door niet alleen de ontwikkeling maar ook de *openlijke* inzet van offensieve cybercapaciteiten te stimuleren, beweegt de VS van continue cyberspionage naar continue cyberaanvallen[12] en normaliseert zo cyberagressie als een legitiem machtsinstrument in vredestijd. Deze mogelijkheid tot meer proactieve en offensieve (re-)acties in het kader van hybride oorlogsvoering brengt echter een hoog risico van misinterpretatie en escalatie met zich mee.[13] Het grijze gebied tussen vrede en oorlog wordt daarbij vergroot en de strategische compressie – het ineenvloeien van de tactische, operationele en strategische niveaus – in het cyberdomein versterkt.

Als gevolg van deze ontwikkeling in de Amerikaanse cyberdoctrine komt het beperkte offensieve Nederlandse mandaat onder (nog) meer druk te staan.[14] De Nederlandse krijgsmacht kan niet op dezelfde offensieve manier optreden in vredestijd. De Wet op de Inlichtingen- en veiligheidsdiensten (WIV) laat geen offensieve cyberoperaties toe, met uitzondering van tegenmaatregelen.[15] Zelfs als mandaat zou worden verleend voor offensieve operaties buiten oorlogstijd, is er nog geen gedetailleerde uitwerking van de *rules of engagement* voor militaire operaties in of via cyberspace.[16] Het is ook niet geheel duidelijk op welk niveau binnen de hiërarchie de autoriteit en toestemming voor verschillende capaciteiten is belegd, en hoe deze besluitvorming plaatsvindt. Nieuwe missies zoals de Nederlandse bijdrage aan de NAVO *enhanced Forward Presence* (eFP) – feitelijk geen missie in de klassieke zin maar een permanente activiteit – hebben eveneens geen offensief mandaat.

Deze notitie pleit zeker niet voor een Nederlands equivalent van het vergaande Amerikaanse mandaat dat openlijke kinetisch-equivalente cyberoperaties in vredestijd toestaat. Hierdoor brokkelt het onderscheid tussen oorlog en vrede verder af en draagt zo eerder bij aan de versterking van de eindeloze 'conflict in de grijze zone'-doctrine van Rusland. Maar de notitie signaleert wél de noodzaak om na te denken over de rol van en de taakverdeling binnen de krijgsmacht in het cyberdomein en de bredere informatieomgeving.

---

[11] Op 15 augustus 2018 heeft President Trump het National Security Presidential Memorandum 13 (NSPM-13) ondertekend. Dit document is niet publiek waardoor het nog onduidelijk is hoe het nieuwe autorisatieproces voor offensieve cyberoperaties eruit ziet. Het lijkt er echter op dat beslissingen tot het uitvoeren van *deny* (*waaronder disrupt, degrade* en *destroy* valt) en *manipulate* door het hoofd van CYBERCOM kan worden gepleegd zonder formele interdepartementale goedkeuring van het State Department. Die laatste keek met name naar de toepassing van internationaal recht en normen. Stefan Soesanto (2019): Trend Analysis: The Evolution of US deterrence strategy in Cyberspace (1988-2019), August 2019, Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf

[12] Nakasone, 'A Cyber Force for Persistent Operations.'

[13] Alexander Klimburg, 'Mixed Signals: A Flawed Approach to Cyber Deterrence' *Survival* (2020): 107-130,

[14] Louk Faesen en Deborah Lassche, 'Persistent Engagement in het Cyberdomein: Stabilisatie of Escalatie', *Militaire Spectator* (aankomend).

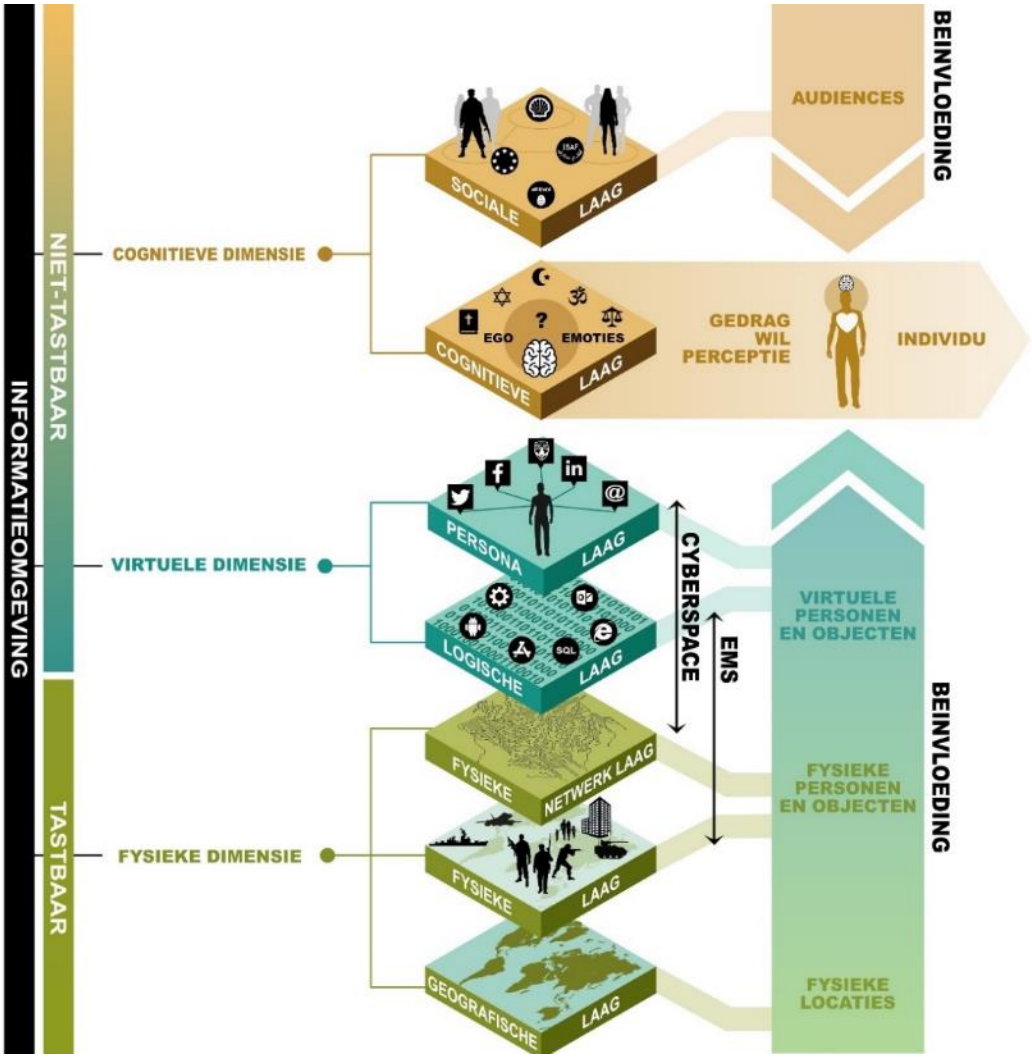
[15] Offensieve operaties worden uitgevoerd door de krijgsmacht onder een internationaal mandaat (bijvoorbeeld een UNSC Resolutie of zelfverdediging ex art. 51 UN Handvest). De doelomschrijving van art. 97 Grondwet is hierbij leidend, procedureel speelt art. 100 van de Nederlandse Grondwet een rol. Voor meer informatie zie: Arnold, K., & Ducheine, P. A. (2015, 20 februari). Besluitvorming bij cyberoperaties. Militaire Spectator, pp. 56-70.

[16] In een door de CDS geleide operatie worden deze bepaald door de SG aanwijzing A974 en de uitwerking hiervan in de 'Operatie Aanwijzing'. "De toestemming om cyberspaceneffecten te plannen en daadwerkelijk te creëren moet zijn verwoord in het regeringsbesluit en, hieruit voortvloeiend, het afgeleide mandaat en de rules of engagement (ROE) vóór het starten van een militaire cyberspace operatie" (Ministerie van Defensie, z.j., p. 36).

2 Effecten in cyberspace

2.1 Wat is cyberspace?

Het vijfde domein van oorlogsvoering, cyberspace[17], doorkruist de vier andere domeinen land, zee, lucht en ruimte, en is nauw verwant met het elektromagnetische spectrum, de informatieomgeving en *signal intelligence* (SIGINT). Dit soort operaties zijn vaak afhankelijk van dezelfde middelen en kunnen vergelijkbare effecten bewerkstelligen in de fysieke, virtuele en cognitieve dimensie. Tegelijk vergen ze verschillende expertise: een hacker heeft een ander specialisme dan een EOV-specialist of een beïnvloedingspecialist. Door de overlap in middelen en effecten is het van belang om deze operaties te coördineren in een geïntegreerde, effectgerichte benadering.



Figuur 1: De dimensies en lagen van de informatieomgeving (Bron: CLAS Visie Informatiegestuurd Optreden)

[17] Cyberspace wordt in de NDD-MCO gedefinieerd als "het geheel van alle met elkaar verbonden (of autonome) fysieke en/of virtuele netwerken, software-gestuurde systemen en/of apparaten, software en data".

Cyberspace kan worden uitgelegd aan de hand van het 'lagen'-model in Figuur 1. Van belang zijn de fysieke, logische, en cyber-persona laag. De fysieke netwerklaag omvat de apparatuur en infrastructuur benodigd om data te kunnen produceren, opslaan, verwerken en versturen. De logische laag omvat alle niet-tastbare elementen die data of code bevatten, zoals software en *operating systems*. In de cyber-persona-laag representeren personen of organisaties zich in cyberspace, bijvoorbeeld door middel van een emailadres of een sociale media-account. De informatieomgeving vult deze drie lagen van cyberspace aan met lagen uit de cognitieve en fysieke dimensie. Dit accentueert het gegeven dat cyberoperaties vooral worden ingezet om (indirecte) effecten teweeg te brengen binnen de cognitieve en fysieke dimensie die verder gaan dan het aantasten van de vertrouwelijkheid, integriteit of beschikbaarheid van een netwerk of data.[18] Het doel van het Stuxnet-virus was niet om enkel de integriteit van industriële controlesystemen in Natanz aan te tasten, maar die inbreuk te gebruiken om de Iraanse nucleaire ambities te vertragen door de koelsystemen te beschadigen. Daarnaast kunnen Cyber-Elektromagnetische Activiteiten (CEMA) als vector dienen voor informatieoperaties of psychologische operaties (PSYOPS) met als doel "het beïnvloeden, verstoren, aantasten of misbruiken van het besluitvormingsproces van tegenstanders."[19]

2.2 Militaire effecten in cyberspace

Binnen cyberspace zijn verschillende effecten te onderscheiden die, mede door een vergelijkbare terminologie, in het algemeen goed kunnen worden verbonden met de effectgerichte aanpak in de andere domeinen. We nemen de effecten beschreven in de NAVO AJP-3.20 als startpunt om de interoperabiliteit met bondgenoten te waarborgen[20]. Een effectgerichte aanpak stelt het te bereiken effect centraal, en maakt daarvoor middelen vrij ongeacht het domein waarin ze werkzaam zijn.

Vanuit een **defensieve benadering** zijn de volgende effecten gericht op het beschermen binnen de netwerken, systemen, individuen en platformen van de Landmacht:

- **Secure**: "prevent compromise of the confidentiality, integrity and availability (CIA) of designated parts of cyberspace and the data stored or processed therein by adversarial cyberspace operations (COs)".[21]
- **Isolate**: "block the line(s) of communication between adversary and their malicious code/activity within affected systems."
- **Contain**: "stop malicious code/activity from further spreading."
- **Neutralise**: "render malicious code/activity permanently incapable of further affecting the CIA of parts of systems."
- **Recover**: "remove and mitigate the effects of malicious code/activity in affected systems in order to restore functionality."

---

[18] Ministerie van Defensie, *Informatie als wapen, middel en doel* (20 december 2016); P.A.L. Ducheine, J van Haaster en R. van Harskamp, *Manoeuvring And Generating Effects In The Information Environment*; J. van Haaster, *On Cyber: The Utility of military cyber operations during armed conflict* (University of Amsterdam,2019).
[19] Ibid, 14.
[20] NATO AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations* (Edition A, Version 1, January 2020).
[21] NATO AJP-6, Allied Joint Doctrine for Communication and Information Systems, for NATO network and systems secure functions (Edition A, Version 1, February 2017).

Vanuit een **offensieve benadering** worden vijandelijke systemen geëxploiteerd of aangevallen om de volgende effecten te behalen:[22]

- **Manipulate**: "to control, change, or compromise the integrity of adversary's information, systems and/or networks in a manner that supports the commander's objectives."
- **Exfiltrate**: "to gather, download, disclose or gain possession of information through unauthorised access." Dit effect draagt, in samenwerking met andere inlichtingenbronnen (HUMINT, SIGINT, OSINT, etc.) bij aan de situational understanding en awareness, wat vervolgens weer een ondersteunende functie heeft voor defensieve of offensieve effecten."
- **Degrade**: "to deny access to, or operation of, an asset to a reduced level of its capacity and/or performance. A desired reduction level is normally specified."
- **Disrupt**: "to completely deny access to, or operation of, an asset for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent for a period of time."
- **Destroy**: "to completely and irreparably deny access to, or operation of, an asset. The asset is affected to the maximum extent, both in terms of outage time and damage caused."

[22] In vergelijking met conventionele wapens kunnen cybermiddelen in het algemeen gerichter en minder gewelddadig het doelwit aangrijpen en nevenschade minimaliseren. Anderzijds kan het risico op nevenschade bij cyberoperaties ook relatief groot zijn. In tegenstelling tot bijvoorbeeld een artillerieaanval, kunnen cyberoperaties gevolgen hebben buiten het missieverband of operatiegebied en in andere domeinen dan cyberspace die de veiligheid van andere – neutrale, bondgenootschappelijke of civiele – actoren kunnen ondermijnen. De effecten van tactische of operationele cyberoperaties kunnen in potentie wereldwijd optreden. Dit risico verkleint de afstand tussen tactische en strategische niveaus en moet meegenomen worden in de planning van cyberoperaties.

3 Rol Landmacht in Cyberspace

3.1 Tactische cyberoperaties

Door de positionering van het DCC als strategische effectbrenger ontstaat er een vacuüm op het niveau van de tactische cybereffecten. De Operationele Commando's moeten dit vacuüm vullen. Dit is lastig omdat de precieze positionering van het DCC nog onvoldoende is uitgekristalliseerd; en omdat de drie traditionele niveaus van oorlogsvoering – strategisch, operationeel, tactisch – in het cyberdomein moeilijk zijn te ontrafelen. In deze notitie proberen wij meer duidelijkheid te scheppen over de tactische effecten die de landmacht zou moeten bewerkstelligen. Tactische cyberoperaties zijn gericht op de volgende effecten:

1. **Beschermen Landmacht netwerk, individuen en platform.** Het waarborgen van de vertrouwelijkheid, de integriteit en de beschikbaarheid van de eigen netwerken, binnen en buiten missieverband, is een randvoorwaarde voor het hedendaags militair optreden. Dit vergt inbedding van de CERT-verantwoordelijkheid[23] binnen de Landmacht, alsmede van dreigingsanalyses en oefeningen waarin rekening wordt gehouden met niet (meer) volledig functionerende systemen. Het Landmacht netwerk bevat ook de digitale SeWaCo+ systemen van de ingezette eenheden en eventueel die van bondgenoten.
2. **Bewerkstelligen *situational awareness* & *understanding.*** Het in kaart brengen van het cyber *key terrain* is, tezamen met de informatie uit andere (cyberspace en elektromagnetische) ISR-middelen en elektromagnetische middelen, essentieel voor offensief en defensief informatiegestuurd landoptreden. Het omvat verschillende vormen van inlichtingen (CEMA, OSINT, HUMINT, etc.) die niet alleen door de inlichtingendiensten maar ook door de Landmacht worden verzameld in missieverband.

Door de positionering van het DCC komt daar nu bij:

3. **Exploiteren en aanvallen van vijandelijke systemen op het tactische niveau**. Militaire cyberoperaties kunnen worden ingezet om de slagkracht te vergroten en offensieve effecten te realiseren in het gevechtsveld.

In alle gevallen, en zeker voor dit laatste, is het nodig om vast te stellen wat precies het tactische niveau betekent waarnaar verwezen wordt.

3.2 Het tactische niveau in cyberspace

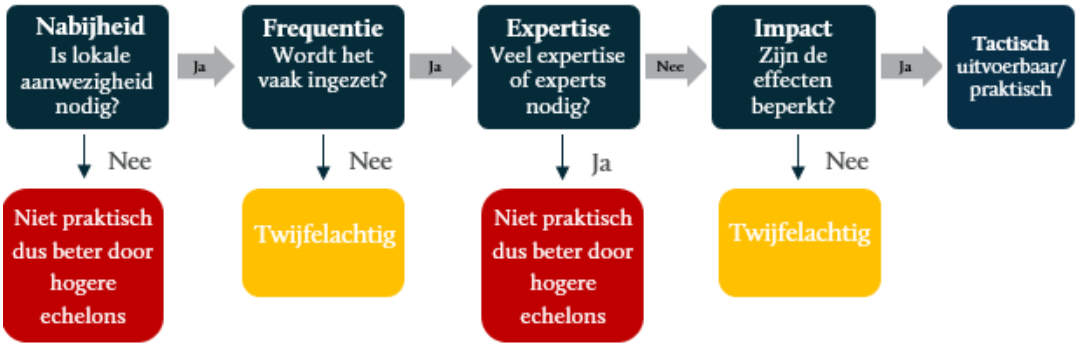
De scheiding tussen het tactische, operationele en strategische niveau van oorlogsvoering stamt uit de negentiende eeuw. In de afgelopen decennia is de discussie opgekomen over de afbakening en het onderscheid tussen deze niveaus. Is het onderscheid nog zinvol als het handelen op het tactische niveau directe strategische implicaties kan hebben en andersom? Als gevolg van deze strategische compressie moeten commandanten acterend op tactisch niveau ook nadenken over effecten op 'hogere' niveaus en op langere termijn, en andersom.[24] De *Joint Doctrine Publicatie 5*

[23] CERT staat voor Computer Emergency Response Team
[24] Binnen de Landmacht reikt het tactische niveau tot en met het legerkorpsniveau.

Commandovoering vermeldt dat ondanks dat "het niet altijd praktisch is om een strikte scheiding tussen de niveaus aan te brengen, [...] ze naar aard en functie wel te onderscheiden [zijn]. Bovendien is de organisatie van de Strijdkrachten veelal gebaseerd op de onderscheiden niveaus."[25] We nemen daarom het bestaan van de onderscheidende niveaus als een gegeven. Om het tactische niveau voor CEMA nader te duiden, hanteren we vier factoren geïntroduceerd door het Amerikaanse onderzoeksinstituut RAND:[26]

- **Nabijheid**. 'Ruimte' heeft een andere invloed in cyberspace dan in fysieke operaties. Actoren en objecten die deel uitmaken van de informatieomgeving kunnen zich overal ter wereld bevinden. De ruimte waarin operaties plaatsvinden – het digitale slagveld – is erg breed. Tegelijk zijn de digitale afstanden snel te overbruggen en dus erg 'kort'. Een groot deel van de offensieve cyberoperaties kan derhalve op afstand worden uitgevoerd. De toegevoegde waarde van de Landmacht bestaat uit het voorzien van lokale toegang tot netwerken, uit het veiligstellen van de communicatie en coördinatie die nodig zijn om operaties voor commandanten op afstand beschikbaar te maken, en uit de integratie in het tactische landoptreden.
- **Frequentie**. Ook 'tijd' heeft een wat andere annotatie in cyberspace dan in fysieke operaties. Hoewel cyberoperaties in enkele seconden een doelwit aan de andere kant van de wereld kunnen aanpakken, vergen ze vaak een enorme lange voorbereidingstijd. Als een capaciteit vaak en snel kan worden ingezet in het operatiegebied zonder veel voorbereidingstijd, ligt de activiteit op het tactische niveau. Zodra een operatie verder gaat dan het uitbuiten van bekende zwakbaarheden; en weken, maanden of zelfs jaren aan voorbereiding, expertise en inlichtingenwerk vergt, dan is voorbereiding op het strategische niveau vereist.
- **Expertise**. Als er een hoge mate van specialistische kennis & kunde vereist is, dan is het meestal effectiever en efficiënter deze centraal te organiseren en op een hoger niveau te beleggen. Dit gebeurt ook voor andere hoog-specialistische functies binnen de krijgsmacht. De inzet gebeurt dan op aanvraag en ter beoordeling van het hogere echelon.
- **Impact**. Blijven de effecten en impact beperkt dan kan het op een lager niveau uitgevoerd worden. Effecten in cyberspace zijn meestal moeilijker te voorspellen dan in de traditionele operationele domeinen. Het cyberdomein is meer vatbaar voor misinterpretatie en miscalculatie. Hoe complexer de operatie, hoe moeilijker het is om een overzicht te hebben van de mogelijke neveneffecten. Een offensieve cyberoperatie kan bijvoorbeeld de veiligheid van andere vijandige, neutrale of vriendelijke systemen binnen de missie en erbuiten aantasten of inlichtingenoperaties met hetzelfde doelwit belemmeren.

[25] Ministerie van Defensie, *Joint Doctrine Publicatie 5: Commandovoering* (maart 2012), p17.
[26] Isaac Porche III et al. , *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Beyond* (Santa Monica: RAND, 2017).



Figuur 2: Flowchart praktische uitvoerbaarheid van offensieve cyberoperaties in de landomgeving

Als lokale aanwezigheid nodig is, de activiteit frequent plaatsvindt, er relatief beperkte expertise vereist is en de effecten en impact beperkt blijven, dan is de activiteit een aangelegenheid van de Landmacht en dient zij zelf over de benodigde capaciteiten te bezitten. Naarmate de tactische effecten niet meer in een gecontroleerde omgeving kunnen worden voorbereid en het ambitieniveau stijgt (met inzet van specifieke middelen die niet *Commercial Off the Shelf* verkrijgbaar zijn), zal de frequentie afnemen terwijl de benodigde expertise, de impact en de voorbereiding toenemen en in de strategische context voorbereid moeten worden. Deze beoordeling wordt idealiter in coördinatie en samenwerking met DCC gemaakt. De componenten van deze beslisboom kunnen door de Landmacht verwerkt worden in de besluitvormingsprocedures (zie Figuur 2).[27]

Om cyber en elektromagnetische activiteiten (CEMA) succesvol binnen de Landmacht in te bedden kunnen belangrijke lessen worden getrokken uit de Amerikaanse context. Binnen de Amerikaanse landmacht heeft zowel de integratie van cyberspace in de manoeuvrefunctie van het landoptreden als het *CEMA support to Corps and Below (CSCB)*-initiatief bijgedragen aan het definiëren en integreren van tactische cyberoperaties met een sterke EOV en informatieoperaties (IO) component. De noodzaak van integratie werd urgenter toen de omvang van de Russische EOV in Oekraïne duidelijk werd.[28]

De integratie van cyberspace in de manoeuvrefunctie wordt anders benaderd dan van het ruimtedomein. Beide zijn van belang voor het landoptreden, maar er wordt niet verwacht dat de landcommandant beschikt over uitgebreide kennis van de ruimte; inzet van ruimtemiddelen is in belangrijke mate een 'commodity'. Cyberspace daarentegen is wel 'commander's business' – succes hangt niet alleen af van de specialisten, maar ook hoe succesvol de specialistische kennis wordt vertaald naar en begrepen door de commandant. Het gevolg is dat cybertraining niet alleen aan specialisten wordt gegeven, maar onderdeel is geworden van bredere trainingsprocedures binnen alle niveaus van de Amerikaanse landmacht.

Het CSCB-initiatief heeft bijgedragen aan de inbedding van tactische cyberoperaties binnen de Amerikaanse landmacht. Het initiatief werd in 2015 opgezet om cyber-, EOV-

[27] Isaac Porche III et al., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Beyond* (Santa Monica: RAND, 2017), 56.
[28] Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Talinn: RKK ICDS, september 2017).

en informatieoperaties te koppelen aan de *brigade combat teams* (BCTs). Het betrof een experiment gericht op drie vragen: zijn cyberoperaties nuttig voor BCTs?; welke capaciteiten en expertise zijn op dit niveau nodig voor een succesvolle cyberintegratie?; en hoe moet de landmacht veranderen om zich aan te passen aan oorlogsvoering in het digitale tijdperk?[29]

Naast het leveren van apparatuur, capaciteiten en autoriteit aan de BCTs zijn, onder toezicht van het *US Army Cyber Command,* CEMA-teams ingezet om training te geven aan de BCTs.[30] In het begin van het initiatief was er geen landmacht cyberdoctrine, waren er geen expeditionaire cybercapaciteiten die relevant waren voor de BCTs, en beschikten de BCTs niet over de benodigde kennis om cyberspace te integreren in hun planning. Bovendien waren de *Combat Training Centers* die als experimenteeromgeving moesten fungeren huiverig om een nieuwe, nog onvoldoende begrepen capaciteit toe te laten in hun trainingsomgeving. De kleine CEMA-teams die werden toegevoegd aan de BCTs moesten een Concept for Operations (CONOPs) opstellen voor cyber op het tactische niveau, dit raamwerk aan de 'manoeuvre'-gemeenschap overdragen en steun van het leiderschap verkrijgen voor het uitbreiden van de trainingsomgeving met een realistische cybercomponent. Tegelijkertijd ontwikkelden ze een reeks expeditionaire CEMA capaciteiten zonder de steun van de gebruikelijke acquisitiekanalen of R&D.[31]

De bijdrage van dit initiatief aan de inbedding binnen de Amerikaanse landmacht is drieledig en is ook relevant voor de Landmacht. Er zijn al verschillende specialistische *information manoeuvre*-experimenten opgezet binnen de Landmacht, maar de Nederlandse Landmacht is ook gebaat bij een initiatief als het CSCB waar de relevantie en inbedding van CEMA voor de bredere manoeuvre eenheden wordt gestimuleerd.

1. **Opwaardering van (verwaarloosde) EOV- en IO-capaciteiten op het tactische niveau.** Onder de noemer *information dominance* werd de combinatie van cyber, EOV en IO verankerd in tactische landoperaties. Ondanks de verschillen in de vereiste expertise moet het oude model waarin deze activiteiten verzuild werden ingezet en aangestuurd worden vervangen door een gesynchroniseerde benadering. Binnen de Nederlandse Landmacht wordt er reeds fors geïnvesteerd in de modernisering van EOV-capaciteiten en de ontwikkeling van IO, en krijgt CEMA een centrale plek binnen *information manoeuvre*.
2. **Opzet van expeditionaire CEMA eenheden**. Het Amerikaanse CSCB initiatief leidde tot de opzet van twee expeditionaire CEMA-eenheden met substantiële financiering voor het ontwikkelen van capaciteiten. Indien ons land, binnen de Nederlandse maat, een soortgelijke expeditionaire eenheid zou willen formeren, moet er kritisch worden gekeken wat mogelijk is in termen van bemanning, training en materieel – zo is binnen het Amerikaanse 915th Cyber Warfare Support Battalion een dringend tekort aan staf (met slechts 18% van de posities bemand en 55% binnen de Intelligence, Electronic Warfare and Space Unit).

---

[29] Sarah White, *Subcultural Influence on Military Innovation*: The Development of U.S. Military Cyber Doctrine, (PhD diss., Harvard University, 2019), https://dash.harvard.edu/bitstream/handle/1/42013038/WHITE-DISSERTATION-2019.pdf?sequence=1.
[30] Kimberly Underwood, *Army CEMA Teams Advance Information, Electronic and Cyber Warfare*, *AFCEA*, augustus 2018, https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare.
[31] Ibid.

3. **Opleiden van de landmachteenheden.** De Amerikaanse BCT-staf werd al doende opgeleid voor CEMA. Dit leidde tot acceptatie en draagvlak voor dergelijke operaties. De mate van cybertraining werd een belangrijke maatstaf voor een succesvolle training. Ook binnen de Nederlandse context moet er niet alleen aandacht worden besteed aan het opleiden van specialisten, maar ook aan de vertaalslag voor de bredere staf. Dit vereist niet alleen een grondige technologische basiskennis; de toegevoegde waarde van officieren binnen het CSCB-initiatief uitte zich vooral in het vermogen om CEMA-mogelijkheden begrijpelijk uit te leggen voor de 'manoeuvre'-gemeenschap.

CSCB kwam voort uit het groeiende besef dat cyber zou falen binnen de Amerikaanse landmacht als het niet relevant werd gemaakt voor de bredere organisatie. De uiteindelijke invloed van het CSCB blijkt uit de oprichting van nieuwe tactische cybereenheden en van de beslissing om cyberofficieren en capaciteiten in te bedden in de staf van de manoeuvre-eenheden en om cyber en EOV te verankeren in tactische landoperaties.[32]

[32] White, *Subcultural Influence on Military Innovation*.

4 Cyberoperaties ter ondersteuning van landoptreden

Bij de effecten uit §2.2 en de vier doelen uit §3.1 horen activiteiten en operaties die relevant zijn voor effectgericht landoptreden (Zie onderstaande tabel voor een overzicht).[33] Een lijst met definities en uitgebreidere beschrijvingen van de activiteiten onder deze vier hoofddoelen is opgenomen in de Annex. Deze lijst is opgesteld aan de hand van de strategieën, doctrines en andere militaire publicaties van Nederland, NAVO en bondgenoten (met name de VS).

Effect	**Defensieve benadering** *Secure; Isolate; Contain; Neutralise; Recover*	*Exfiltrate*	**Offensieve benadering** *Deny; Destroy; Disrupt; Degrade; Manipulate, Deceive*
Doel	Beschermen netwerk, SeWaCo+ systemen en individuen	Bewerkstelligen *situational awareness* & *understanding*	Aanvallen en exploiteren vijandelijke systemen
Methode	Identificeren en beschermen *cyber key terrain* en SEWACO-systemen; CEMA voor bescherming eigen eenheden	Inlichtingenverzameling (CNE) of informatie-exploitatie van de operationele en tactische omgeving (*cyber key terrain*)	Computer Network Exploitation (CNE) Computer Network Attack (CNA) of offensive cyberspace operation (OCO); EOV; Information manoeuvre
Operatie	Cybersecurity Baseline; Defensive Syberspace Operation (DCO); Electronic Protection & Hardening; Emissiecontrole; EMS management; SATCOM bescherming; Defensieve Information manoeuvre	Cyberspace ISR; SIGINT; HUMINT ; Electronic Reconnaissance; Electronic Intelligence; Inlichtingen *reachback;* Spectrum Management Operaties	Cyberspace ISR; Intelligence preparation of the battlefield; Operational preparation of the environment; Spectrum Management Operations; Offensive Cyberspace Operation; Electronic Attack; Electronic Warfare Support; operationele *reachback*; Informatieoperaties

[33] Met name omdat de situatie in het nationale domein in termen van zelfstandige taken en verantwoordelijkheden voor de krijgsmacht in formele zin nog erg beperkt zijn, en in termen van de zich langzamerhand vormende concepten voor een meer omvattende nationale rol van de krijgsmacht nog erg ondoorzichtig, concentreren we ons hier vooralsnog op de inzet in missies.

4.1 Beschermen van het netwerk, SeWaCo-systemen en individuen

Onder het opereren en beschermen van het netwerk vallen ook de sensor-, wapen- en commandovoerings (SeWaCo) systemen die gebruik maken van cyberspace of het EMS. Dit bevat de *Secure*, *Isolate*, *Contain*, *Neutralise* en *Recover* effecten van de defensieve benadering zoals omschreven in §2.2, alsmede de maatregelen die nodig zijn om een *cybersecurity baseline* vast te stellen. De digitale kwetsbaarheden van de bedrijfssystemen en de SeWaCo-systemen kunnen de inzetbaarheid, de doeltreffendheid, het vertrouwen en de reputatie van de krijgsmacht ondermijnen.[34] Om deze systemen en het netwerk waarin ze zijn opgenomen te beschermen, moeten de vertrouwelijkheid, de integriteit en de beschikbaarheid (c*onfidentiality, integrity, availability* – CIA) van de netwerken en data gewaarborgd zijn. Op deze manier wordt ervoor gezorgd dat de SeWaCo-systemen operationeel en toegankelijk zijn (beschikbaarheid), volledig en onveranderd zijn (integriteit), en dat de inhoud van deze systemen niet door derden kan worden onderschept (betrouwbaarheid).

Het cyberdomein en elektromagnetische spectrum bieden zowel voordelen als kwetsbaarheden voor de individuen en de SeWaCo-systemen van de Landmacht. Zo zijn de cyber-persona van individuen zowel binnen als buiten missieverband kwetsbaar voor bijvoorbeeld *phishing* of beïnvloedingsoperaties die het vertrouwen in een missie of de organisatie kunnen ondermijnen. De bescherming van SeWaCo-systemen wordt onder meer gesteund door het identificeren en beschermen van het *cyber key terrain*, cyber *defence*, *electronic hardening*, emissiecontrole en spectrummanagementoperaties. Veel systemen komen echter uit een tijd dat er onvoldoende aandacht was voor cybersecurity en zijn (nog) onvoldoende beschermd.[35] De cybersecurity van deze systemen is een blijvende inspanning die door de hele ICT-keten moet worden geïmplementeerd. Van de ontwikkeling en aankoop tot aan de operationele afscherming en instandhouding moet er meer cyberbewustzijn en kennis gecreëerd worden.

De instandhouding van CIA kan onmogelijk te allen tijde gegarandeerd worden. In de dreigingsanalyse (en in trainingen) moet er daarom rekening worden gehouden met storingen in CIA van het netwerk en de SeWaCo systemen. Het gaat dus allereerst om bewustzijn van relevante dreigingen en vervolgens om de effectieve bescherming van systemen en netwerken. Beide vereisen een blijvende inspanning. De effectgerichte aanpak en de capaciteiten die hiervoor nodig zijn dienen gericht te zijn op beveiliging van het netwerk (*securing the network*) en verdediging van het netwerk (*defending the network*).

---

[34] Een *cybersecurity baseline* bepaalt de mate van veiligheid die nodig is om zelf effectief en met vrijheid van handelen te kunnen optreden in cyberspace. Het is een fundamentele randvoorwaarde voor verscheidene militaire cyberoperaties (Ministerie van Defensie, *Nederlandse Defensie Doctrine voor Militaire Cyberspace Operaties,* p26). De *baseline* vormt hiermee de eerste stap in het bepalen van de praktische uitvoerbaarheid van een tactische offensieve cyberoperatie. Vervolgens moet er gekeken worden naar de risico's die gepaard gaan met het uitvoeren van een cyberoperatie om zo de *situational awareness & understanding* te vergroten. Deze risico's worden in hoofdstuk 0 beschreven.
[35] Djenna Perreijn, "Digitaal weerbaar op de grond," *Materieelgezien*, juni 2018, https://magazines.defensie.nl/materieelgezien/2018/06/09_digitaal_weerbaar.

De beveiliging van het netwerk gebeurt onafhankelijk van specifieke dreigingen (*threat agnostic*) maar wel netwerkspecifiek en stelt commandanten in staat effectief en veilig te communiceren, informatie te delen en te beheren. Het is met name belegd bij de netwerkbeheerders, het Joint Informatievoorziening Commando (JIVC) en het Defensie Cybersecurity Centrum (DCSC). DCSC voorziet in het monitoren (SOC) en incident response (DefCERT).

De verdediging van het netwerk reageert op dreigingen en is voornamelijk belegd bij de DefCERT-functie van het DCSC, die een adviesrol vervult voor de systeemmanagers binnen Defensie en de eindverantwoordelijkheid draagt voor de implementatie van dit advies. DCSC heeft enkel bevoegdheden om binnen het eigen netwerk te opereren. Hiervoor gebruikt DCSC verschillende sensoren voor het monitoren van het Defensienetwerk om zo onregelmatigheden te signaleren. Van commandanten op brigadeniveau en hoger wordt verwacht dat ze zélf (en dus niet DCSC) verantwoordelijk zijn voor de verdediging van hun deel van het netwerk; ze kunnen zo nodig wel steun bij DCSC aanvragen. De CERT-verantwoordelijkheid is vooralsnog nog niet of onvoldoende ingebed binnen de Landmacht. Tevens moet de vertrouwelijkheid, integriteit en de beschikbaarheid van de Landmacht-netwerken niet alleen gewaarborgd worden tijdens oefeningen en missies, maar ook in vredestijd met zijn 'grijze zone'-dreigingen.

Het valt in dit verband op te merken dat de verantwoordelijkheden – en daarmee de rol van de Landmacht – met betrekking tot de cybersecurity van de Landmacht SeWaCo-systemen die gebruikt worden in de aansturing van (land)operaties momenteel nog niet duidelijk genoeg zijn gedefinieerd. Wel duidelijk is dat op alle niveaus (dus ook bij de Landmacht) adequate capaciteiten benodigd zijn om hier invulling aan te geven.

4.2 Bewerkstelligen *situational awareness & understanding*

Het bewerkstelligen van *situational awareness & situational understanding* (SA/SU) omvat het verzamelen, verwerken, duiden, integreren, beschikbaar stellen en evalueren van verzamelde data en informatie over de eigen situatie, omgeving en (f)actoren uit alle zeven lagen van de informatieomgeving (incl. cyberspace en het EMS).[36] SA/SU binnen cyberspace wordt verkregen door eerst het *cyber key terrain* (CKT) in kaart te brengen, gedefinieerd in de *Defensie Cyber Doctrine* als "Onderdelen van cyberspace die essentiële missie activiteiten, operaties of functies mogelijk maken [...] CKT omvat dan ook iedere area (zoals hardware, software, netwerken, personeel, infrastructuur) waarvoor geldt dat inbeslagname, behoud of verstoring een duidelijk voordeel oplevert voor een van de strijdende partijen."[37] De Amerikaanse FM 3-12 heeft een bredere definitie van *key terrain in cyberspace.* Het bevat niet alleen de onderdelen (knooppunten, links, activiteiten) maar ook de *processen* die zich in de fysieke, logische of cyber-persona laag bevinden en een voordeel opleveren of van groot belang zijn voor het succes van een missie.[38] Een volgende stap is de praktische toepassing van bestaande

[36] Koninklijke Landmacht, *Visie Informatiegestuurd Optreden voor de Landmacht* (oktober 2020). .
[37] Ministerie van Defensie, *Nederlandse Defensie Doctrine voor Militaire Cyberspace Operaties* (juni 2019) p.39.
[38] *FM 3-12 Cyberspace and Electronic Warfare Operations* (2017). De onderliggende factoren die bepalend zijn voor een *cyber key terrain* zijn nog niet doorontwikkeld en variëren afhankelijk van de gebruiker,

militaire concepten binnen CKT en andersom. Dit betekent dat 'manoeuvre'-commandanten op alle niveaus de notie van CKT moeten omarmen. Een verdieping naar de implicaties en toepassing van wat, bijvoorbeeld, *trailing the flag* of de *high ground* binnen CKT betekent zou daarbij een meerwaarde opleveren voor de integratie van cyberoperaties in het militaire denken.

Figuur 3 combineert informatie uit het operationele gebied met die uit het netwerk om zo bij te dragen aan het in kaart brengen van CKT. Getracht wordt relevante vijandige, neutrale en bondgenootschappelijke activiteiten in cyberspace en het EMS te identificeren, te categoriseren en te monitoren. Dit draagt, samen met de informatie uit andere (cyberspace) ISR-middelen[39] en elektromagnetische middelen[40], bij aan het lokaliseren en benoemen van vijandelijke systemen, maar ook aan het beter kunnen beschermen van het eigen netwerk, individuen en systemen. Een goede SA/SU is bijvoorbeeld van belang voor offensieve operaties als bepaalde – vooral commerciële – knooppunten in cyberspace gebruikt worden door meerdere entiteiten die zowel vriendelijk, neutraal of vijandig van aard kunnen zijn.

Inlichtingen worden binnen Defensie in eerste instantie verzameld door de MIVD, soms in nauwe samenwerking met de AIVD. In tweede instantie kan deze rol vervuld worden door andere onderdelen van de krijgsmacht, zeker op het gebied van *human intelligence* (HUMINT) tijdens een landoperatie. Zoals beschreven in de volgende paragraaf, kunnen deze inlichtingen op hun beurt cyber- en EOV-operaties ondersteunen. In de Joint EOV-visie wordt beschreven hoe Defensie de informatie die ze heeft verkregen uit de domeinen land, zee, lucht, ruimte, cyber en EMS onderling kan delen door middel van gekoppelde processen en systemen én door gebruik te maken van een geïntegreerde nationale EOV-database.[41] Op deze manier kan er (*near*) *real time* SA/SU in het EMS worden verkregen. Dit draagt weer bij aan snellere besluitvorming en het verkrijgen van informatiedominantie.

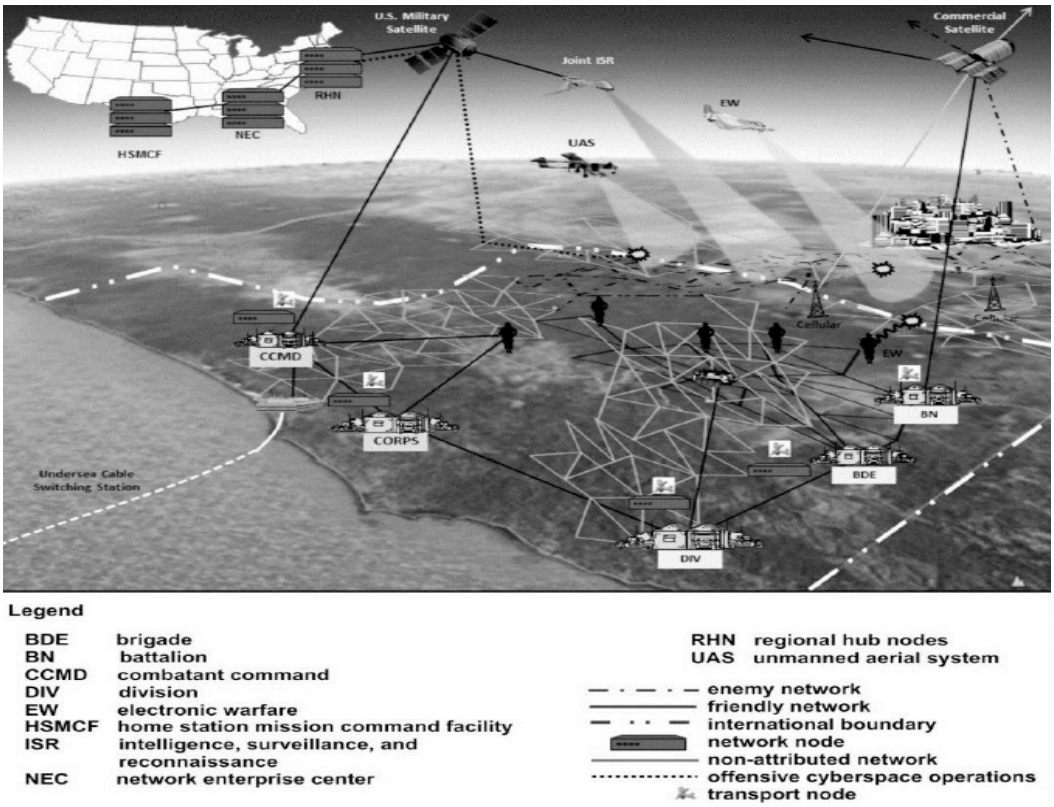
---

missie, beschikbare data en technologie. De moeilijkheid zit in het bepalen welke informatie relevant is, hoe deze wordt weergegeven en gekoppeld aan de fysieke en kinetische laag waarin landoperaties plaatsvinden. Het verkrijgen van zo een efficiënt overzicht blijft een moeilijke opgave, ondanks de verschillende methoden en raamwerken die als voorbeeld kunnen dienen – zie bijvoorbeeld de "cyberspace and the operational variables" in *FM 3-12 Cyberspace and Electronic Warfare Operations* (2017) p. 1-18; of het Cyber Common Operating Picture design in Conti, et al., *Towards a Cyber Common Operating Picture* (Talinn: NATO CCD COE Publications, 2013).

[39] *Cyberspace intelligence, surveillance* en *reconnaissance* (ISR) betreft inlichtingenoperaties, vaak uitgevoerd door SIGINT-units, gericht op het verzamelen van tactische en operationele inlichtingen om het vijandelijk gebruik in cyberspace in kaart te brengen. Het doel is ondersteuning van de militaire planning, specifiek voor (toekomstige) offensieve of defensieve cyberoperaties, maar ook in algemene zin. Headquarters, Department of the Army, *FM 3-12: Cyberspace and Electronic Warfare Operations* (april 2017), 1-9

[40] Electronic Reconnaissance en Electronic Intelligence door middel van GPS en sensoren - inclusief optische, elektro-optische, thermische, millimetergolf- of multispectrale sensoren.

[41] Ministerie van Defensie, *Visiedocument Joint Elektronische Oorlogsvoering (EOV) Concept 1.6.* (mei 2019), 7.



Figuur 3: Het operationeel gebied in combinatie met netwerkinformatie.[42]

4.3 Aanvallen en exploiteren van vijandige systemen

Militaire cyberoperaties kunnen worden ingezet om de slagkracht te vergroten en de offensieve effecten *disrupt, degrade, destroy,* en *manipulate* te realiseren. Cyberinlichtingenoperaties die bijdragen aan SA/SU spelen ook een cruciale rol in het exploiteren van vijandige systemen om inlichtingen te verzamelen (*exfiltrate*) ter voorbereiding van offensieve operaties.[43] Een succesvolle aanval wordt namelijk vrijwel altijd voorafgegaan door inlichtingenoperaties.[44]

Een CEMA-benadering zorgt ervoor dat schaarse offensieve cyber- en EOV-middelen gecoördineerd, efficiënt en wederzijds ondersteunend worden ingezet om de slagkracht op het gevechtsveld te vergroten. Offensieve militaire cybercapaciteiten zoals jamming, het uitschakelen van een radarsysteem om een luchtaanval mogelijk te maken, worden

[42] Headquarters, Department of the Army, *FM 3-12: Cyberspace and Electronic Warfare Operations* (april 2017), 1-17.
[43] Netwerkaanvallen worden vaak voorafgegaan door netwerkexploitaties. Voormalig NSA en USCYBERCOM Director Michael Hayden beschrijft dit in zijn boek *Playing to the Edge* (2017) als: "Reconnaissance should come first in the cyber-domain. […] How else would you know what to hit, how, when – without collateral damage?"
[44] *Intelligence Preparation of the Battlefield* is nauw verwant aan ISR en analyseert het vijandige gebruik van cyberspace en het EMS. In deze analyse wordt gekeken naar de afhankelijkheid van genetwerkte capaciteiten; defensieve cybercapaciteiten en zwakheden in het netwerk; EOV-capaciteiten; motivatie en bereidheid om cyberoperaties uit te voeren tegen bondgenootschappelijke eenheden; de mogelijkheid om cyberoperaties te combineren met andere operaties; en sociale media.

als slagkracht (of *fires*) beschouwd.[45] In deze tactische context speelt CEMA voor de Landmacht een belangrijke rol. Steeds vaker worden EOV geïntegreerd met cyber- en informatieoperaties, bijvoorbeeld wanneer EOV vijandelijke communicatie omleidt via een netwerk dat onder surveillance staat. Tactische CEMA vinden meestal plaats binnen de context van conventionele militaire operaties, bijvoorbeeld *jamming* van vijandelijke communicatie of hoogwaardige tactische effecten die een lange voorbereidingstijd nodig hebben in de strategische context zoals *counter-A2/AD* of *Supression of Enemy Air Defences* (SEAD). Bovendien kan CEMA de effectiviteit van traditionele wapensystemen verhogen met doelgeleiding gebaseerd op datalinks en netwerken.[46]

Tactische CEMA-toepassingen variëren met het ambitieniveau en de beschikbare middelen. Relatief bescheiden zijn *close access operations* door een klein *special forces* teams. Bij een hoger ambitieniveau gaat het om cyber- en EW-*fires* waarbij vijandelijke SEWACO-systemen misleid worden. Dit is een hoogtechnologische – en kostbare – categorie waarbij CEMA als SEAD wordt ingezet, met als voorbeeld het *Senior Suter* programma.[47] CEMA kan ook functioneren als vector voor beïnvloedingsoperaties, waarbij de aandacht gericht is op het beïnvloeden van het gedrag van een doelwit, inclusief de manier waarop deze informatie verzamelt, verwerkt, waarneemt, verspreidt en ernaar handelt. Informatieoperaties en psychologische operaties zijn dus gericht op de boodschap zelf die via een transmissiemedium (steeds vaker digitaal) terecht komt bij de doelgroep die gepresenteerd wordt door cyber-persona.[48]

---

[45] Deze *fires* kunnen op hun beurt weer cyberoperaties ondersteunen als het slagen van deze operatie afhangt van fysieke aanwezigheid. Aangezien cyberoperaties gedeeltelijk gebruikmaken van het EMS, moeten ze worden afgestemd met SIGINT- en EMS-operaties, waarin een EOV-capaciteit ook als afleverplatform voor nauwkeurige cybereffecten kan dienen. *Electronic Warfare* wordt in de Amerikaanse context beschreven in *JP 3-13.1* en bevat capaciteiten zoals *Electronic Attacks, Electromagnetic Deception, Electromagnetic Intrusion, Electromagnetic Jamming,* en *Electromagnetic Pulse.* Met name binnen de operationele en de tactische context waarin de Landmacht opereert kan slagkracht niet alleen door en via cyberspace, maar ook door en via het elektromagnetische spectrum verworven worden. Dit kan resulteren in zowel psychologische, logische en fysieke effecten.

[46] Department of the Army, *FM 3-38: Cyber Electromagnetic Activities*, 1-9

[47] Het Senior Sutter programma is onderdeel van het geclassificeerd Amerikaanse *Big Safari* initiatief en ontwikkeld door *BAE Systems*. Het is een prijzige en gesofisticeerde vorm van CEMA gericht op het binnendringen van communicatie- en computernetwerken, voornamelijk van luchtverdedigingssystemen, waarna de aanvaller de systeemadministrator functie overneemt. Het programma kent twee onderdelen: één voor het implementeren van gegevens-invoer en één voor het bewaken van gegevens-uitvoer. Het eerste blok stelt de operatoren in staat om te controleren wat vijandige radars kunnen zien. Het belangrijkste platform voor de gegevensverzameling is het *RC-135 Rivet Joint elektronische bewakingsvliegtuig*. Het tweede blok dient voor de malware injectie in vijandige netwerken door middel van het *EC-130 Compass Call elektronische aanvalsvliegtuig*. Een derde blok is toegevoegd dat specifiek gericht is op het penetreren van netwerken die meer tijd-kritische en tactisch ongrijpbare doelen aansturen, zoals mobiele raketwerpers. Zie Lt Col Prashant Mishra (Retired), *Operation Orchard - The Attack on Syrian Nuclear Reactor* (juli 2019), https://www.linkedin.com/pulse/operation-orchard-modern-electronic-warfare-prashant-mishra-7k-; Air Force Technology, *The Israeli ' E-tack' on Syria – Part I*, (maart 2008) https://www.airforce-technology.com/features/feature1625/.

[48] Wanneer CO werkzaam zijn ter ondersteuning van een IO richten ze zich in het algemeen op de integratie van offensieve en defensieve capaciteiten uitgeoefend in en door cyberspace, in samenwerking met andere informatie-gerelateerde capaciteiten (IRC) en in coördinatie met meerdere "lines of operation" (operatielijnen) en "lines of effort" (inspanningslijnen), *JP 3-13*, p. II-9

5 Aanbevelingen

Militaire cyberoperaties zijn niet alleen essentieel voor moderne oorlogsvoering (als *enabler*) maar ook een wezenlijk onderdeel ervan. Dit betekent dat cyberspace functioneel geïntegreerd dient te worden in het landoptreden (anders dan capaciteiten in de ruimte die ook een essentiële *enabler* vormen voor het landoptreden, maar die de landcommandant niet volledig hoeft te kennen en te snappen om er nuttig gebruik van te kunnen maken). Dit geldt zowel tijdens militaire inzet als op momenten en onder omstandigheden waarin er (nog) helemaal geen sprake is van militaire inzet (althans in de gebruikelijke zin). De effectiviteit van de Landmacht wordt mede bepaald door activiteiten in cyberspace die voorafgaand aan of onder de drempel van gewapend conflict plaatsvinden.

Met de gekozen focus op strategische cybereffecten van het DCC dient de Landmacht eigen CEMA-capaciteiten te ontwikkelen. Dit ter bescherming van de eigen netwerken, SeWaCo+ systemen en individuen; om situational awareness and understanding te verkrijgen; en om het kunnen aanvallen, exploiteren en beïnvloeden van vijandelijke systemen en actoren op het slagveld. Om de benodigde capaciteiten te ontwikkelen en in te bedden binnen de Landmacht, moet aandacht worden geschonken aan alle DCTOMPFI-elementen: Doctrine, Commandovoering, Training, Organisatie, Materieel, Personeel, Faciliteiten, beleid en interoperabiliteit.[49] Op basis van deze indeling geven we de volgende overwegingen en aanbevelingen.

5.1 Doctrine

Cyberspace en elektromagnetische capaciteiten (tezamen CEMA) moet geïntegreerd worden in de doctrine voor landoptreden als wezenlijk element van het gecoördineerde en op effecten gerichte optreden, waarbij er niet alleen oog is voor de fysieke impact, maar ook voor de informatiedominantie van de Landmacht (zie bijvoorbeeld US Field Manual 3-12 CEMA). De strategische richtlijnen voor militaire cyberoperaties zijn tot op zekere hoogte uitgewerkt in de Defensie Cyber Strategie en de NDD-MCO. Deze richtlijnen laten echter nog te veel ruimte en ambiguïteit met betrekking tot de integratie van cyber in het landoptreden en de operationalisering van de benodigde capaciteiten. Hoe wordt de inzet van cybercapaciteiten begrijpelijk gemaakt in traditionele 'manoeuvre'-begrippen zoals 'het kiezen van zwaartepunten' – en (waarom) zijn deze begrippen überhaupt van toepassing? Hoe kan het denken over *cyber key terrain* geïntegreerd wordt in de gebruikelijke *key terrain*-analyse van commandanten en staven? Momenteel zijn enkel EOV-operaties gedefinieerd en ingebed in het landoptreden, zij het met achterstand op de gecoördineerde en gesynchroniseerde benadering beschreven in de NAVO-doctrine. Voor volwaardige integratie van CEMA in het manoeuvreoptreden dienen de Operationele Commando's, in samenwerking met DCC, een CEMA-doctrine te ontwikkelen. Zowel tactische cyberoperaties als EOV-activiteiten kunnen ook individueel uitgevoerd worden, maar nooit zonder beschouwing van eventuele wederzijds interferentie.

[49] Dit raamwerk is afgeleid van het Amerikaanse *DOTMLPF-P* raamwerk. Het Amerikaanse *Department of Defense Joint Capabilities Integration System* heeft DOTMLPF-P ontwikkeld als methodologie voor de ontwikkeling en implementatie van nieuwe of uitgebreide operationele capaciteiten. De NAVO heeft deze methodologie aangevuld met I (voor interoperabiliteit).

Het synchroniseren van de verschillende functies van militair optreden om de gewenste effecten te bereiken in de fysieke, virtuele en cognitieve dimensies,[50] vereist dat CEMA-operaties integraal in het besluitvormingsproces worden meegenomen. Een commandant en zijn staf moeten in staat zijn om operatielijnen in cyberspace te ontwikkelen en deze kunnen coördineren met EOV-activiteiten om de slagkracht te vergroten. Ook moeten zij de risico's van cyberactiviteiten goed kunnen inschatten en weten hoe deze te mitigeren (*Collateral Damage Estimates*).

5.2 Organisatie en commandovoering

Expeditionaire Cyber/CEMA Mission Teams die operationele en tactische effecten teweegbrengen moeten voldoende defensieve en offensieve handelingsvrijheid hebben, ook in wettelijke en politieke zin (mandaat); over de juiste eigen expertise beschikken en tegelijk over *reachback*-capaciteit. Deze teams moeten onderdeel zijn van een bredere *Concept of Operations* die moet worden opgezet door DCC en Operationele Commando's. De focus bij het inrichten van dergelijke teams binnen de Landmacht moet liggen op operationele inzetbaarheid in de tactische omgeving.[51] Hier kan gekeken worden naar initiatieven elders – zoals het Amerikaanse *CEMA support to Corps or Below*-initiatief[52] – die waardevolle lessen bieden voor de benodigde expertises voor dergelijke teams.

Cyberoperaties zijn informatiegestuurd. Het verzamelen van inlichtingen is een essentieel onderdeel van elke cyberoperatie. Dit vereist vanwege het soort en de herkomst van de doelinformatie een informatie-exploitatiecapaciteit en een nauwe relatie met de inlichtingendienst, ook op tactisch niveau. Dit vereist weer een vertrouwensband waarbij er sprake is van wederzijdse transparantie en begrip over de respectievelijke interesses en intenties van de MIVD en de tactische eenheden. Dit kan bevorderd worden door het implementeren van de relevante *information security*-richtlijnen, toezichtmechanismen en liaisonposities. Naast naar de MIVD is ook *reachback*-capaciteit naar het DCC en DCSC nodig, al was het maar omdat tactische offensieve cyberoperaties mogelijk strategische gevolgen hebben of om defensieve ondersteuning te krijgen.[53] Om strategische compressie te managen, is organische

---

[50] Headquarters, Department of the Army, *FM 3-38: Cyber Electromagnetic Activities*, 3-2; P.A.L. Ducheine, J van Haaster en R. van Harskamp, *Manoeuvring And Generating Effects In The Information Environment*; Paul A.L. Ducheine en Frans Osinga, (Eds.) '*Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*'. Springer Verlag/TMC Asser (Berlin/The Hague); Amsterdam Law School Research Paper No. 2017-30; Amsterdam Center for International Law No. 2017-25.

[51] Binnen de Nederlandse context zijn er reeds cyber mission teams opgezet, bestaande uit personeel van de MIVD, Krijgsmacht en DefCERT, "omdat voor inlichtingenoperaties en militaire operaties in het digitale domein soortgelijke kennis en vaardigheden nodig zijn." Deze opereren echter binnen het kader van de WIV met als hoofddoel inlichtingenverzameling, waardoor ze niet bevoegd zijn om offensieve cyberoperaties uit te voeren. Ministerie van Defensie, *Defensie Cyber Strategie 2018*, p13; *Kamerstuk Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2020,* p88.

[52] Stephen P Stover, Army developing expeditionary cyber-electromagnetic teams to support tactical commanders, US Army, 8 februari 2018, https://www.army.mil/article/200262/army_developing_expeditionary_cyber_electromagnetic_teams_to_support_tactical_commanders.

[53] Gebruik maken van reachback betekent een verkleining van de voetafdruk in het inzetgebied en een efficiënter gebruik van schaarse cyberexpertise. Reachback is echter wel afhankelijk van een robuust CIS-infrastructuur, inclusief bandbreedte. Reachback kan verder een vertragend effect hebben op het commandoproces in tijdkritische situaties.

capaciteit nodig op het tactische niveau, bijvoorbeeld in de vorm van een 'cyber-planner'. Het betekent ook dat commandanten op hogere niveaus moeten kunnen denken in termen van doelen en effecten op lagere niveaus en vice versa.

Het samenhangende karakter van cyberoperaties en de schaarse expertise die hiermee gepaard gaat vergt idealiter een defensiebrede kennisautoriteit met cyberspace-, SIGINT-, EOV- en communicatiesecties – met de aantekening dat deze secties integraal en niet als *stovepipes* werken. Kennis van inlichtingenoperaties, CEMA en communicatie- en spectrummanagement kan gedeeld en gebruikt worden in een hybride centraal-decentraal model waarin DCC ondersteuning kan geven aan de Operationele Commando's.

De rol en de uit te voeren missies van zowel DCC als van de Operationele Commando's van het tactische tot strategische niveau strategische-tactische spectrum zouden in de reguliere Concept of Operations (CONOPs) moeten wordt verhelderd.[54] De CONOPs biedt de visie en intentie hoe operaties in de informatieomgeving doorwerken in de bredere operationele omgeving. Het opstellen van een werkbare CONOPs vergt nauwe samenwerking met alle belanghebbenden, een goed begrip van de operationele uitdagingen van de informatieomgeving en kennis van hoe zowel bondgenoten als tegenstanders dit hebben aangepakt.

5.3 Opleiding en training

Cybersecurity en cyberoperaties moeten worden benaderd als specialisme, maar tegelijkertijd als onderdeel van de bredere trainingsopzet binnen de Landmacht. Zo wordt draagvlak gecreëerd en voorkomen dat cyber als een geïsoleerde of niche-functie behandeld wordt. Een dergelijke duale inbedding kan voorzien in de grote vraag naar cyberexpertise maar draagt ook bij aan het creëren van het besef van het leiderschap op alle niveaus, maar zeker bij het topmanagement, dat nodig is om cyber-operaties integraal onderdeel te laten uitmaken van de bevels- en besluitvormingsketens binnen de organisatie. De aanzienlijke risico's die cyberincidenten kunnen vormen voor de operationele efficiëntie en veiligheid maakt cybersecurity zelfs tot een algemene trainingsprioriteit. Dat begint bij de basisopleiding en moet continu worden onderhouden door de snelle technologische en doctrinaire innovaties. Cyberspecialisten gaan zo dezelfde taal spreken als 'manoeuvre'-militairen. Dit faciliteert een cultuurverandering over het belang en de inzet van cyber als integraal onderdeel van het landoptreden.

De oprichting van een CEMA bureau binnen de Landmacht is een belangrijke stap in de kennisontwikkeling en het identificeren van kennisgaten binnen de organisatie. Gerichte trainingen (bijvoorbeeld door middel van simulaties) verbeteren dan weer de specialistische vaardigheden maar om de operationele ondersteuning te kunnen geven aan het landoptreden moeten cyberoperaties ook een geïntegreerd onderdeel vormen

[54] Onze NAVO bondgenoten hanteren meerdere definities voor de afkorting CONOPs. In de context van deze aanbeveling gaat het dan vooral over: (a) "CONOPs which provides the vision and intent for how the system should work within an operational environment" en (b) ConOps which "allocates what to the how and so completes the chain all the way to an instantiation". Terwijl (a) een traditionele strategische visie mogelijk maakt die ook de operationele omgeving beschrijft, beschrijft (b) een duidelijke commandolijn en toewijzing van missies binnen het DCC, OPCOs, MinDef, Nederland in het algemeen en binnen de alliantie. (a) informeert (b); en vervolgens test en verfijnd (a) waar nodig (b).

van bredere trainingen. Om voorbereid te zijn op intercepties en storingen die de vertrouwelijkheid, integriteit en de beschikbaarheid van haar netwerken aantasten, moet de Landmacht ook met gedegradeerde systemen oefenen.

5.4 Personeel

Cyberexpertise is schaars, binnen Defensie en daarbuiten. De benodigde expertise moet helder worden geformuleerd om ervoor te zorgen dat deze behoefte wordt gedekt door werving, opleiding en training en loopbaanperspectief (behoud), naast eventuele verwerving van relevante diensten buiten de Landmacht. Personeel met cyberexpertise is essentieel om op alle niveaus draagvlak te creëren om cyberoperaties volledig te integreren in het landoptreden. Het verkrijgen van de juiste professionals is geen makkelijke taak; het is een competitief gebied dat vele specialisaties kent. Een cyberteam zal dus bestaan uit meerdere functies en rollen. Voor de Amerikaanse krijgsmacht heeft RAND een inschatting gedaan van de vereiste vaardigheden in de keten, zie onderstaande tabel.[55]

Role	Location	Skill Level (Health Care Analogy)	Quantity	Examples
Cyber technician/ operator/ employer	Forward	Medic	Many: possible one per platoon	A fully functional infantryman, perhaps with an additional skill identifier and toolkit that allows remotely supported cyber services when needed
Planner	Forward	Hospital manager	Moderate: one per unit / brigade	Officer on a brigade staff with knowledge of cyber capabilities; manages the relationship between *reachback* personnel and cyber technicians; knows about and manages authorities and approvals
Forward cyber expert	Forward	Nurse (floating)	Limited	Teams/personnel detached to the brigade level that can be fragmented and organized to lower echelons as needed to carry out full-time cyber-related missions
Reachback cyber expert	Forward	Physician	Few	Tool developers, programmers etc.

[55] Isaac Porche III et al. , *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Beyond* (Santa Monica: RAND, 2017).

De Defensie Cyber Strategie beschrijft hoe Defensie de komende jaren meer aandacht wil besteden aan het verbinden van cyber- en IT-professionals: "Door het uitzetten van loopbaanpaden kan meer inzicht in het geheel aan menselijk cyber-potentieel worden gecreëerd en gerichter worden gestuurd op werving, behoud en loopbaan."[56] Om ervoor te zorgen dat de kennis van cyberprofessionals actueel blijft en medewerkers tevreden blijven moet de Landmacht rekening houden met een aantal factoren. Functies die hoogwaardige cyberkennis en vaardigheden vereisen vergen een bottom-up aanpak met eigen (nieuwe) administratieve processen, training en functies. Cyber en EOV moet defensiebreed een aantrekkelijk carrièrepad worden. Dit betekent een volwaardig en gebalanceerd functiehuis om doorgroeimogelijkheden te faciliteren. Om recht te doen aan het operationele belang en aard van cybereffecten en -capaciteiten, kan het optreden in cyberspace worden gepositioneerd als een eigen wapen (in de betekenis van wapens en dienstvakken). Dit maakt gerichte doorgroeimogelijkheden beter mogelijk, met een positief effect op de wervingskracht en het kennisbehoud binnen de organisatie.

5.5 Materieel en faciliteiten

Door de snelle technologische vooruitgang moet de Landmacht continu innoveren en investeren in cyber- en EOV-middelen om bij te blijven met bondgenoten en tegenstanders. De digitale weerbaarheid van haar eigen ICT- en SEWACO-systemen moet daarbij verzekerd worden. Menselijke expertise en kennisopbouw vormen de basis van cybercapaciteiten, maar wordt ondersteund door technische middelen die in de regel zowel (veel) goedkoper als (veel) vergankelijker zijn dan conventionele militaire middelen.[57] Een gezonde balans tussen ingekochte en in-house onderzoek en innovatie kan ervoor zorgen dat de Landmacht innovatief blijft. Na een jarenlange achterstand, zullen de EOV capaciteiten van de Landmacht significant gemoderniseerd en doorontwikkeld worden.

Binnen de Amerikaanse Landmacht draagt de *Army Rapid Capabilities Office* en het *System of Sytems Engineering and Integration (SoSE&I) Cyber Focal* bij aan het (versneld) ontwerpen, produceren en integreren van cybercapaciteiten. Ze zorgen ervoor dat capaciteiten en acquisitieprogramma's relevant zijn voor de behoeften van de commandant en voldoen aan de ICT infrastructuur door middel van geïntegreerde tests.[58] Zo werden prototypes van 'defensieve cyberspace operatie kits' ontwikkelt als mobiele 'fly away kits' waarmee de *cyber protection teams* expeditionaire bescherming kunnen bieden voor vriendelijke netwerken en systemen die snel opgezet moeten worden ter ondersteuning van landoperaties. De feedback van soldaten informeert het

[56] Ministerie van Defensie, *Defensie Cyber Strategie 2018*, 14.
[57] Met de aantekening dat hele hoogwaardige tactische CEMA capaciteiten, zoals het *Senior Suter*-programma van BAE systems, naar inschatting nog steeds erg duur zijn om aan te schaffen en te operationaliseren.
[58] US Army, *Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Army* (maart 2019), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/A/0604798A_129.pdf; US Army, *Prototypes rapidly deliver cyber capabilities* (juni 2019), https://www.army.mil/article/189601/prototypes_rapidly_deliver_cyber_capabilities.

leiderschap om de juiste expeditionaire cybercapaciteiten te benoemen en operationeel te integreren.[59]

De Landmacht dient cybersecurity een centrale plek te geven bij de ontwikkeling en aanschaf van met name (maar zeker niet alleen) SEWACO-systemen. De Landmacht hoort, samen met DCSC, voor en na het aanschaffen van alle nieuwe (wapen-)systemen de cyberveiligheid ervan, en als regel ook van de desbetreffende toeleveringsketens, te waarborgen. Veilige hardware en software hoort ook bij te dragen aan technische interoperabiliteit met nationale en internationale agentschappen (zie ook §5.7). De modernisering van de netwerkarchitectuur van de Landmacht is een essentiële randvoorwaarde voor de bescherming van het netwerk, individuen en systemen. Verstoringen in de Defensie ICT-infrastructuur in 2014 leidden tot een aantal rapporten waarin de knelpunten in de technische staat van de toenmalige (en grotendeels huidige) infrastructuur zijn beschreven. Naar aanleiding van deze rapporten werd een algehele vernieuwing van de infrastructuur nodig geacht. Het programma 'Grensverleggende IT' (GrIT) beoogt, samen met de markt, te voorzien in deze nieuwe infrastructuur.[60] Recentelijk is in een onderzoek van het BIT echter geconcludeerd dat de risico's van het GrIT nog steeds te groot zijn. Momenteel onderzoekt Defensie de mogelijkheid om de huidige aanpak aan te passen of te concluderen dat een geheel andere aanpak nodig is. De eisen aan de nieuwe infrastructuur van Defensie zijn beschreven in het *Defensie High-Level IT-ontwerp*[61] maar refereren weinig naar cybersecuritymaatregelen.

5.6 Beleid

Er moet meer duidelijkheid verschaft worden over de taken en verantwoordelijkheden voor netwerkbeveiliging, cybersecurity, defensieve en offensieve cyberoperaties. Het mandaat bepaalt tot op grote hoogte de grenzen van inzet van cybercapaciteiten. Om dit mandaat toereikend te laten zijn moet het digitale aspect in een vroeg stadium van de planningsfase van elke (potentiële) missie in beschouwing worden genomen. Een vroege inbedding van cybercapaciteiten in dit besluitvormingsproces komt tot uiting in de adviezen en analyses van de Directie Operaties en in daaropvolgende (operatie)plannen.[62] Een betere afbakening van de verantwoordelijkheden voor inzetbeslissingen tussen het tactische, operationele en strategische niveau is belangrijk. De in deze studie beschreven elementen van de beslisboom (zie Figuur 2) dienen nader gepreciseerd te worden.

Een internationale vergelijking laat zien dat offensieve cybercapaciteiten meestal belegd worden op het strategische niveau. In de Britse *Cyber Primer* wordt beschreven hoe effecten op het tactische niveau vaak veel tijd nodig hebben om toegang te verkrijgen of capaciteiten te ontwikkelen, waardoor het realiseren van *high-end*

[59] *Network Integration Evaluations* (NIE) zijn door soldaten geleide evaluaties die zijn ontworpen om het tactische communicatienetwerk van het leger verder te integreren en verbeteren. Deze evaluaties beoordelen concepten en capaciteiten om een flexibel en adaptief platform voor het Amerikaanse leger te bouwen. *Joint Warfighting Assessments* (JWA) zijn jaarlijkse beoordelingen van concepten en capaciteiten in een joint en coalitie omgeving. Zowel NIE en JWA voorzien waardevolle feedback van de soldaat aan het leiderschap. https://www.army.mil/standto/archive_2017-07-06/

[60] Bureau ICT-toetsing, *Definitief BIT-advies over het programma "Grensverleggende IT"* (31 mei 2016).

[61] Ministerie van Defensie, *Defensie High-level IT-ontwerp* (24 april 2015).

[62] Ibid, 13.

cybereffecten vaak beperkt wordt tot situaties waarin de strategische beloning groot is. Dit komt ook door de vrees voor escalatie en *blowbacks*, deconflicterings- en attributieproblemen, alsmede de noodzaak tot nauwe coördinatie met de inlichtingengemeenschap. Steeds vaker echter zullen tactische CEMA-effecten – zoals het lokaal verstoren van het netwerk van een individueel gebouw –nuttig gebruikt kunnen worden tijdens militaire operaties. Met name in de VS is er een trend tot het *mainstreamen* van cyberoperaties door de besluitvorming en bijbehorende capaciteiten lager in de organisatie tot en met het brigadeniveau) in te bedden. Het *mainstreamen* van cyber wordt in de Britse *Cyber Primer* beschreven als het ontwikkelen van C2- en organisatiestructuren die het mogelijk maken om cybercapaciteiten te leveren en te onderhouden als onderdeel van haar toekomstige slagkracht.[63] Een flexibele structuur benadrukt de complexe aard van cyberoperaties en het belang van gecoördineerd handelen (dus structuur), terwijl tegelijkertijd de wendbaarheid wordt behouden om op snel wisselende en veranderende dreigingen en mogelijkheden in te spelen (dus flexibel). Snelle besluitvorming gevolgd door snel handelen is essentieel.[64]

In de Nederlandse context past een dergelijk benadering bij de principes van opdrachtgerichte commandovoering zoals beschreven in de Doctrine Landoperaties. Opdrachtgerichte commandovoering kent vijf uitgangspunten, waarvan twee sterke nadruk leggen op de handelingsvrijheid van ondercommandanten. De specifieke aard van militaire operaties in het cyberdomein heeft tot dusver geresulteerd in een beperking van deze handelingsvrijheid. Door te voorzien in de Cyber Mission Teams en *reachback* kan hierin veel worden verbeterd.

Verder verdient het feit dat het optreden van de krijgsmacht zich al lang niet meer beperkt tot missies in de traditionele zin aandacht. Denk bijvoorbeeld aan de aanwezigheid van de Landmacht in Litouwen als onderdeel van de *enhanced Forward Presence* (eFP) van de NAVO in de Baltische Staten en Polen, maar ook aan activiteiten in het nationale domein in het kader van hybride dreigingen. Dergelijke permanente activiteiten worden steeds belangrijker maar passen niet in het traditionele missiekader met zijn (politieke) besluitvormingsprocedures over mandaat, *Rules of Engagement* enzovoort. Bij dergelijke activiteiten vormt (juist) de cyberdimensie een wezenlijk element. Bij bepaling van de rol van de Landmacht in het cyberdomein en de bredere informatieomgeving gaat het daarom niet alleen over de taakverdeling en afstemming met het DCC, maar ook om de afstemming tussen wat Defensie doet en wat de diverse publieke en private civiele partijen (zie §5.7).

5.7 Interoperabiliteit

Cyberoperaties zijn bij uitstek joint operaties die een *whole-of-society* (nationaal multi-agency en in samenwerking met niet-statelijke actoren) of *whole-of-alliance* (internationale coalitieoperaties) aanpak behoeft. Interoperabiliteit is hierbij randvoorwaardelijk. Interoperabiliteit, de "*ability to be informed, to support, and to execute*", is een cruciale randvoorwaarde én uitdaging voor cyberoperaties die onderdeel

[63] UK Ministry of Defence, *Cyber Primer, Second Edition* (The Development, Concepts and Doctrine Centre, juli 2016), p67.
[64] Mark Pomerleau, *How the Army will Infuse Cyber Operations on the Battlefield*, Fifth Domain, 5 juli 2018, https://www.fifthdomain.com/dod/army/2018/07/05/how-the-army-will-infuse-cyber-operations-on-the-battlefield/.; Underwood, *Army CEMA Teams Advance Information, Electronic and Cyber Warfare*.

zijn van een *multi-agency*- of coalitieoperatie. Deze drie bekwaamheden volgen elkaar stapsgewijs op van een lager tot een hoger ambitieniveau en vergen inzicht in de middelen, mogelijkheden, doelen, strategieën, doctrines en ideologische context van een ander.

Een belangrijk element van interoperabiliteit is standaardisatie: "Standaardisatie zorgt er vooraf al voor dat de internationale eenheden met elkaar kunnen samenwerken door te werken met op elkaar afgestemde procedures, begrippen, materieel en informatietechnologie."[65] In de NAVO-context verwijst interoperabiliteit vaak naar de mogelijkheid om gezamenlijk op te treden op een coherente, effectieve en efficiënte manier om zo tactische, operationele en strategische doelstellingen te behalen. Op het strategische niveau wordt dit gefaciliteerd door terminologie, strategieën en doctrines, en op het operationele en tactische niveau door TTPs op elkaar af te stemmen. Waar mogelijk dienen de geaccepteerde termen en definities van de NAVO of bondgenoten overgenomen te worden. De NDD-MCO introduceert echter een aantal nieuwe termen, zoals cyber support of cyber attack operations die niet in lijn zijn met die van onze bondgenoten.[66]

Technologische interoperabiliteit voorziet in de compatibiliteit tussen de informatietechnologie van actoren op het gebied van informatievoorziening (CIS), commandovoering, sensoren en vuurkracht. Vaak is echter niet alleen de achterliggende technologie een obstakel voor interoperabiliteit, maar ook kunnen verschillende *information security policies* ervoor zorgen dat informatie niet of beperkt kan worden uitgewisseld. In de nationale context moet er vertrouwen zijn in de veiligheid van de ICT-systemen van de Landmacht voordat een *reachback* kan worden opgezet. Binnen de NAVO wordt er verwijst naar de voorwaardelijke toestand die bij *Communication and Information Systems* (CIS) of de daarop verbonden apparatuur wordt bereikt wanneer informatie of diensten rechtstreeks en probleemloos kunnen worden uitgewisseld.[67] Hiervoor wordt een *Federation of Systems*, een systeem van systemen dat zonder centrale autoriteit beheerd wordt, gebruikt waarin er een constante coördinatie moet zijn tussen de netwerkbeheerders van individuele systemen.[68] Het verbinden van de sensoren binnen Defensie in een federatief netwerk

---

[65] Koninklijke Landmacht, *Landoperaties: Doctrine Publicatie 3.2*, pp3-20.
[66] *Cyber support operaties* (CSO) zijn operaties ter ondersteuning van andere activiteiten en zijn daarbij geschikt om informatie-operaties te ondersteunen. *Cyber-attack* (CA) operaties kunnen volgens de doctrine "worden gebruikt voor 'harde' effecten (gericht tegen infrastructuur, objecten of informatie) of 'softe' effecten (bedoeld om actoren en/of doelgroepen te beïnvloeden)." De ondersteunende functie die cyber heeft voor informatieoperaties is begrijpelijk. Daarentegen is de definitie van cyber aanvallen, waar informatie zowel onder *harde* en *softe* wordt geplaatst, niet conform westerse of juridische begrippen van een aanval waarin informatie niet als wapen of aanval wordt beschouwd. Het Tallinn Manual definieert een 'cyberattack' op basis van het bestaand internationaal recht als "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.'" Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013), 106. De U.S. Director of National Intelligence (DNI) gebruikt een bredere definitie van een cyberattack: "a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data." U.S. Director of National Intelligence (DNI), *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community Senate Select Committee on Intelligence* (maart 2013), https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.
[67] NATO, *AJP-6: Allied Joint Doctrine for Communication and Information Systems* (februari 2017), 1-4.
[68] Ibid.

kan ervoor zorgen dat data efficiënter wordt gedeeld voor evaluatie, verrijking en analyse.

Technologische interoperabiliteit wordt ook bewerkstelligd door een *standards-based approach* die standaarden opstelt conform *best practices* vanuit de overheid, de industrie en academica. [69] Om de eenheid in de cybersecurity-architecturen te bewaken en interoperabiliteit en effectief securitymanagement mogelijk te maken, gebruikt het Amerikaanse *Department of Defense* dezelfde architecturen en cybersecurity *knowledge repositories*[70] waardoor *best practices*, *benchmarks*, standaarden, templates, checklists, tools, richtlijnen, regels en principes integraal gedeeld kunnen worden.[71] De lage instapkosten en de snelle toepassing van geavanceerde technologie kunnen ervoor zorgen dat sommige, vooral niet-statelijke tegenstanders, even goed of beter in staat zijn om cyberspace als *force multiplier* te gebruiken. De uitdaging voor Defensie is om binnen de beperkingen van het nationale en bondgenootschappelijke beleid, doctrine en wetgeving te werken terwijl tegenstanders vrijer en sneller kunnen opereren.

5.8 Tot slot

De Landmacht staat aan het begin van een tegelijk urgent én langjarig ontwikkeltraject van slagkracht in cyberspace en het EMS. Een geïntegreerde CEMA-benadering is daarbij essentieel. Op deze manier worden overlap, deconflictering en afstemming verankerd binnen een effectgerichte benadering die schaarse cyberexpertise en -capaciteiten efficiënt inzet. Het is de hoogste tijd daartoe een visie, CONOPs en roadmaps op te stellen, waarvoor de hier verwoorde overwegingen en aanbevelingen als input kunnen dienen.

[69] National Institute of Standards and Technology Computer Security Resource Center.
[70] Zie bijvoorbeeld: National Vulnerability Database, the Open Vulnerability and Assessment Language Repository, of Risk Management Framework Knowledge Service.
[71] Department of the Army, *ATP 6-02.71: Techniques for Department of Defense Information Network Operations,* A12.

Bibliografie

Atlantic Council Digital Forensic Research Lab. "Electronic Warfare by Drone and SMS: How Russia-backed separatists use "pinpoint propaganda" in the Donbas." Laatste gewijzigd 18mei 2017. https://medium.com/dfrlab/electronic-warfare-by-drone-and-sms-7fec6aa7d696.

Bureau ICT-toetsing. *Definitief BIT-advies over het programma "Grensverleggende IT.* 31 mei 2016.

Chianello, Allessandro (Lkol). *Military Activities in Cyber Space: Classification, Analysis, Organization, Conducting.* [PPT] (NATO Science & Technology Organization: April 2018).

Gregory Conti, John Nelson en David Raymond. *Towards a Cyber Common Operating Picture.* Tallinn: NATO CCD COE Publications 2013.

Dekkers (Lkol) en Grijpstra (Lkol), *Informatie als wapen, middel en doel* (Ministerie van Defensie: December 2016).

Ducheine, P.A.L en Arnold, Kraesten. 'Besluitvorming bij cyberoperaties', *Militaire Spectator* 184, no. 2 (Februari 2015).

Ducheine, P.A.L., van Haaster J. en van Harskamp R. "Manoeuvring And Generating Effects In The Information Environment." *Netherlands Annual Review of Military Studies 2017* (2017): 155-179. https://doi.org/10.1007/978-94-6265-189-0_9.

Ducheine, P.A.L. en Osinga, Frans (Eds.). '*Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises'*. den Haag: TMC Asser, 2017.

Faesen, Louk en Lassche, Deborah. "Persistent Engagement in het Cyberdomein: Stabilisatie of Escalatie", *Militaire Spectator* (aankomend).

Hayden, Michael. *Playing to the Edge: American Intelligence in the Age of Terror.* New York: Penguin Books, februari 2016.

Kjellén Jonas. *Russian Electronic Warfare: – The Role of Electronic Warfare in the Russian Armed Forces* Swedish Defense Research Agency, september 2018

Klimburg, Alexander. "Mixed Signals: A Flawed Approach to Cyber Deterrence." *Survival* 62, no. 1 (2020): 107-130. https://doi.org/10.1080/00396338.2020.1715071.

Koninklijke Landmacht. *Landoperaties: Doctrine Publicatie 3.2*. Doctrine Commissie Koninklijke Landmacht, Februari 2014.

Long en Hunter. *Doctrine Development.* [PPT] US Army Cyber Center of Excellence Directorate of Training, augustus 2015.

McDermott, Roger N. *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum.* Tallinn: RKKICDS, september 2017.

Menn, Joseph. "Special Report: U.S. cyberwar strategy stokes fear of blowback." Reuters. Laatste gewijzigd 10 mei 2013. https://www.reuters.com/article/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510.

Ministerie van Defensie. *Besluit van 19 juli 1997, houdende vaststelling regels inzake geweldgebruik krijgsmacht in de uitoefening van de bewakings- en beveiligingstaak (Besluit geweldgebruik krijgsmacht in de uitoefening van de bewakings- en beveiligingstaak).* 's-Gravenhage: Staatsblad van het Koninkrijk der Nederlanden, 7 augustus 1997.

Ministerie van Defensie. *Defensie Cyber Strategie 2018 – Investeren in Digitale Slagkracht Nederland.* november 2018.

Ministerie van Defensie. *Defensie High-level IT-ontwerp* (24 april 2015).Ministerie van Defensie. *Joint Doctrine Publicatie 5: Commandovoering*. maart 2012.

Ministerie van Defensie. *NDD-MCO.* juni 2019.

Ministerie van Defensie, *Visiedocument Joint Elektronische Oorlogsvoering (EOV) Concept 1.6.* (Mei 2019).

Ministerie van Defensie. *Aanpak Nieuwe IT Defensie Wordt Aangepast.* 28 juni 2019. Beschikbaar via: https://www.defensie.nl/actueel/nieuws/2019/06/28/aanpak-nieuwe-it-defensie-wordt-aangepast.

Ministerie van Defensie. Antwoorden op feitelijke vragen over de *Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2020 (35300-XL)*. oktober 2019.

Nakasone, Paul. "A Cyber Force for Persistent Operations", *Joint Force Quarterly* 92 no.1: 10-14 2019.http://cs.brown.edu/courses/csci1800/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). *Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig.* augustus 2019.

NATO. *AAP-06*, *NATO Glossary of Terms and Definitions*. NATO Standardization Office (NSO), 2018.

NATO. *AJP-320, Allied Joint Doctrine for Cyberspace Operations*. NATO Standardization Office (NSO), januari 2020.

NATO. *AJP-3.6A, Allied Joint Electronic Warfare Doctrine.* NATO Standardization Office (NCO), december 2013.

NATO. *AJP-3.9, Allied Joint Doctrine for Joint Targeting*. NATO Standardization Office (NSO), april 2016.

NATO. *AJP-5, Allied Joint Doctrine for Operational-level Planning*. NATO Standardization Office, februari 2019.

NATO. *AJP-6: Allied Joint Doctrine for Communication and Information Systems*. NATO Standardization Office (NCO), februari 2017.

NCTV. *Nederlandse Cybersecurity Agenda.* NCSC, april 2018.

Office of the Director of National Intelligence. "*A Guide to Cyber Attribution. NIC,* september 2018.

Orye, Erwin en Maennel, Olaf. "Recommendations for Enhancing the Results of Cyber Effects*."* In *2019 11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky. Tallinn: NATO CCD COE, mei 2019.

Perreijn, Djenna. "Digitaal weerbaar op de grond." *Materieelgezien, juni 2008.*https://magazines.defensie.nl/materieelgezien/2018/06/09_digitaal_weerbaar.

Pomerleau, Mark. "How the Army will Infuse Cyber Operations on the Battlefield." *Fifth Domain*, 5 juli 2018. https://www.fifthdomain.com/dod/army/2018/07/05/how-the-army-will-infuse-cyber-operations-on-the-battlefield/.

Porche III, Isaac; Paul, Christopher; Serena, Chad C.; Clarke, Colin P.; Johnson, Elizabeth-Erin; en Herrick, Drew. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Beyond* Santa Monica:RAND, 2017.

Roubos, Mark (Maj.), *Elektronische Oorlogsvoering: De dreiging in het elektromagnetische spectrum (EMS) en de effectieve beheersing hiervan* [PPT] (Joint ISTAR Command: 25 oktober 2019).

Sellmeijer (Lkol), *Nederlandse Defensie Doctrine* (Den Haag, Defensiestaf: Februari 2019).

Schmitt, Michael (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press: 2013).

Schmitt, Michael (Ed.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press: 2017).

Soesanto, Stefan, Trend Analysis: The Evolution of US deterrence strategy in Cyberspace (1988-2019), (Augustus 2019), https://css.ethz.ch/content/dam/ethz/special-

interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf.

Stover, Stephen P., "Army developing expeditionary cyber-electromagnetic teams to support tactical commanders." *US Army*, 8 februari 2018. https://www.army.mil/article/200262/army_developing_expeditionary_cyber_electromagnetic_teams_to_support_tactical_commanders.

Tweede Kamer der Staten-Generaal. *Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2020.* 7 november 2019.

U.K. Ministry of Defence. *Cyber Primer, Second Edition.* Swindon: The Development, Concepts and Doctrine Centre, juli 2016.

U.K. Ministry of Defence. *Joint Doctrine Note 1/17 Future Force Concept.* Swindon: The Development, Concepts and Doctrine Centre, juli 2017.

U.K. Ministry of Defence. *Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities.* Swindon: The Development, Concepts and Doctrine Centre, februari 2018.

Underwood, Kimberly. "Army CEMA Teams Advance Information, Electronic and Cyber Warfare." *AFCEA*, 6 augustus 2018. https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare.

U.S. Department of Defense. *Department of Defense Cyber Strategy: Summary.* DoD, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

U.S. Army, *Exhibit R-2, RDT&E Budget Item Justification: PB 2020 Army*. maart 2019. https://www.dacis.com/budget/budget_pdf/FY20/RDTE/A/0604798A_129.pdf.

U.S. Army. *Prototypes rapidly deliver cyber capabilities.* juni 2019. https://www.army.mil/article/189601/prototypes_rapidly_deliver_cyber_capabilities.

U.S. Director of National Intelligence (DNI). *Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community Senate Select Committee on Intelligence.* maart 2013. https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.

White, Sarah. "*Subcultural Influence on Military Innovation:* The Development of U.S. Military Cyber Doctrine." (PhD diss., Harvard University, 2019). https://dash.harvard.edu/bitstream/handle/1/42013038/WHITE-DISSERTATION-2019.pdf?sequence=1.

Williams, Lauren. "Nakasone Talks Cyber Deterrence at Confirmation Hearing', Defense Systems." *Defense Systems*, 2 maart 2019, https://defensesystems.com/articles/2018/03/02/nakasone-cybercom-confirmation.aspx.

Zeleny, Milan. *Human Systems Management: Integrating Knowledge, Management and Systems.* N.J.: World Scientific, januari 2005.

US Army Field Manuals/ATP's/JP's:

Headquarters, Department of the Army, *ATP 2-01.3: Intelligence Preparation of the Battlefield* (Washington DC: Maart 2019).

Headquarters, Department of the Army, *ATP 3-36 (FM 3-36): Electronic Warfare Techniques* (Washington DC: December 2014).

Headquarters, Department of the Army, *ATP 3-60 (FM 3-60): Targeting* (Washington DC: Mei 2015).

Headquarters, Department of the Army, *ATP 6-02.40: Techniques for Visual Information Operations* (Washington DC: Januari 2019).

Headquarters, Department of the Army, *ATP 6-02.53: Techniques for Tactical Radio Operations* (Washington DC: Januari 2016).

Headquarters, Department of the Army, *ATP 6-02.54: Techniques for Satellite Communications* (Washington DC: Juni 2017).

Headquarters, Department of the Army, *ATP 6-02.60: Tactical Networking Techniques for Corps and Below* (Washington DC: Augustus 2019).

Headquarters, Department of the Army, *ATP 6-02.70: Techniques for Spectrum Management Operations* (Washington DC: December 2015).

Headquarters, Department of the Army, *ATP 6-02.71: Techniques for Department of Defense Information Network Operations* (Washington DC: April 2019).

Headquarters, Department of the Army, *ATP 6-02.75: Techniques for COMSEC Operations* (Washington DC: Augustus 2015).

Headquarters, Department of the Army, *FM 3-12: Cyberspace and Electronic Warfare Operations* (Washington DC: April 2017).

Headquarters, Department of the Army, *FM 3-18: Special Forces Operations* (Washington DC: Mei 2014).

Headquarters, Department of the Army, *FM 3-38: Cyber Electromagnetic Activities* (Washington DC: Februari 2014).

Headquarters, Department of the Army, *FM 3-90.1: Offense and Defense*, Vol. 1 (Washington DC: Juli 2001).

Headquarters, Department of the Army, *FM 6-02: Signal Support to Operations* (Washington DC: September 2019).

Joint Chiefs of Staff, *JP 3-12: Cyberspace Operations* (Juni 2018).

Joint Chiefs of Staff, JP 3-13: Information Operations (November 2014).

Joint Chiefs of Staff, JP 3-13.1: Electronic Warfare (Februari 2012).

Joint Chiefs of Staff, JP 3-30: Joint Air Operations (Juli 2019).

Joint Chiefs of Staff, JP 6-01: Joint Electromagnetic Spectrum Management Operations (Maart 2012).

Termen en definities

Cyber key terrain: "Onderdelen van cyberspace die essentiële missie activiteiten, operaties of functies mogelijk maken, worden aangemerkt als cyber key terrain (CKT). CKT omvat dan ook iedere area (zoals hardware, software, netwerken, personeel, infrastructuur) waarvoor geldt dat inbeslagname, behoud of verstoring een duidelijk voordeel oplevert voor een van de strijdende partijen." (NDD-MCO p39) De Amerikaanse FM 3-12 heeft een bredere definitie van *Key Terrain in Cyberspace*: "alle knooppunten (*nodes*), links, processen, of middelen die zich in de fysieke, logische of cyber-persona laag bevinden en een voordeel opleveren of van groot belang zijn voor het succes van een missie."[72]

Cybersecurity baseline bepaalt de mate van veiligheid die nodig is om zelf effectief en met vrijheid van handelen te kunnen optreden in cyberspace. Het is een fundamentele randvoorwaarde voor verscheidene militaire cyberoperaties. Ministerie van Defensie, *Nederlandse Defensie Doctrine voor Militaire Cyberspace Operaties,* p26.

Cyber Support-operaties ondersteunen andere activiteiten door bijvoorbeeld het kapen van de cybermiddelen van een tegenstander of door het gebruiken van de eigen cybermiddelen als platform (vector) om een *payload* (lading of boodschap) over te brengen (NDD-MCO).

Cyberspace Intelligence, Surveillance, Reconnaissance-operaties (ISR) omvatten activiteiten die gericht zijn op het verzamelen en in kaart brengen van informatie over netwerken en systemen van een tegenstander of een specifiek doelwit. Dit gebeurt onder meer door het volgen van nieuwe ontwikkelingen, het zoeken naar bedreigingen en het identificeren van potentieel gevaarlijke situaties of juist kansen (NDD-MCO).

Electromagnetic Hardening: een handeling die voorziet in de bescherming van personeel, voorzieningen of apparatuur door middel van het onderdrukken, filteren, verzwakken, aarden, binden en/of afschermen tegen bepaalde ongewenste effecten van elektromagnetische energie. Joint Chiefs of Staff, *JP 3-13.1: Electronic Warfare* (Februari 2012), p1-8.

Elektromagnetisch spectrum-management: het EMS-gebruik plannen, coördineren en beheren door operationele, *engineering* en administratieve procedures. Doel is het coördineren, prioriteren en de-conflicteren van EMS-afhankelijke systemen. Joint Chiefs of Staff, *JP 6-01: Joint Electromagnetic Spectrum Management Operations* (Maart 2012), pp1-6 / 1-7.

Electronic Attack-operaties gebruiken elektromagnetische energie, gerichte energie of anti-radiatie wapens om personeel, faciliteiten of middelen aan te vallen om zo de slagkracht van de vijand af te breken, te neutraliseren, of te vernietigen. Dergelijke operaties worden ook vaak *fires* genoemd (JP 3-13.1).

Electronic Intelligence is een subcomponent van SIGINT en wordt verkregen via externe non-communicatie radiatie afkomstig van bijvoorbeeld radars, 'surface-to-air' raketsystemen of luchtvaartuigen. *Electronic reconnaissance* bestaat in het detecteren, localiseren, identificeren en evalueren van externe elektromagnetische radiatie en wordt gebruikt om risicoanalyses up to date te houden (FM 3-12).

---

[72] US FM 3-12 (p.1-18): "Identified key terrain in cyberspace is subject to actions the controlling combatant (whether friendly, enemy, or adversary) deems advantageous such as defending, exploiting, and attacking. References to key terrain correspond to nodes, links, processes, or assets in cyberspace, whether part of the physical, logical, or cyber-persona layer. The marked advantage of key terrain in cyberspace may be for intelligence, to support network connectivity, a priority for defense, or to enable a key function or capability."

Electronic Protection betreft operaties die personeel, faciliteiten en middelen beschermen tegen effecten van bondgenootschappelijk of vijandelijk gebruik van het EMS die de slagkracht afbreken, neutraliseren of vernietigen (JP 3-13.1).

Electronic Warfare Support betreft operaties waarbij bronnen van elektromagnetische energie worden onderschept, geïdentificeerd of gelocaliseerd om zo dreigingen te herkennen, doelwitten vaststellen, vooruit te plannen en toekomstige operaties uit te voeren (FM 3-12).

Emissiecontrole: het selectieve en gecontroleerde gebruik van elektromagnetische, akoestische of andere zender-apparatuur om de operationele veiligheid van C2-capaciteiten te optimaliseren. Dit gebeurt door de detectie van vijandelijke sensoren, en door de wederzijdse storing tussen eigen en bondgenootschappelijke systemen en vijandige militaire deceptie te minimaliseren (FM 3-12).

Intelligence Preparation of the Battlefield is nauw verwant aan ISR en analyseert het vijandige gebruik van cyberspace en het EMS. In deze analyse wordt gekeken naar de afhankelijkheid van genetwerkte capaciteiten; defensieve cybercapaciteiten en zwakheden in het netwerk; EOV-capaciteiten; motivatie en bereidheid om cyberoperaties uit te voeren tegen bondgenootschappelijke eenheden; de mogelijkheid om cyberoperaties te combineren met andere operaties; en sociale media. In de NDD-MCO wordt *Intelligence Preparation of the Battlefield* enkel benoemd als *Intelligence Preparation of the Environment* (IPE), maar niet gedefinieerd. De term *Intelligence Preparation of the Battlefield* wordt in detail beschreven in *US Army ATP 2-01.3*.

Operational Preparation of the Environment (OPE): het ondersteunen van activiteiten ten behoeve van het plannen en voorbereiden van een militaire operatie. In tegenstelling tot ISR is OPE niet hoofdzakelijk gericht op het verzamelen van inlichtingen. Headquarters, Department of the Army, *FM 3-12: Cyberspace and Electronic Warfare Operations* (Washington DC: April 2017), p1-10.

Preparation of the Battlefield: "the systematic process of analysing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations"; Headquarters, Department of the Army, *ATP 2-01.3: Intelligence Preparation of the Battlefield* (Maart 2019) p1-1.

Reachback: "het terugvallen op de volledige ondersteuning in het achterblijvende hoofdkwartier via over-the-horizon C2 en CIS39" (Joint Doctrine Publicatie 5 Commandovoering, p89). Het betreft het proces van het verkrijgen van alle producten en diensten van organisaties die niet rechtstreeks zijn ingezet tijdens landoperaties. Voor meer informatie over *Reachback* zie *JP 3-30*. Dit document beschrijft de benodigde systeembeschrijving en apparatuur, zoals regionale knooppunten.

Spectrum Management-operaties bestaan uit de operationele en administratieve procedures met betrekking tot het plannen, coördineren en het management van het gebruik van het EMS om zo cyberspace-, signal- en EOV-operaties te faciliteren (FM 3-12).