



Ministerie van Defensie



Defensie Cyberstrategie 2025

Digitale slagkracht
voor de bescherming
van het Koninkrijk
en bondgenoten

Samenvatting

Context

De dagelijkse cyberaanvallen die de belangen van Nederland en Europa schaden, zijn onverminderd groot. Statelijke en niet-statelijke actoren zetten hun machtsmiddelen in het cyberdomein agressief in om strategische doelen na te streven in alle conflictfasen van strategische rivaliteit tot crisis en oorlog.

Deze toegenomen cyberdreiging manifesteert zich op een aantal manieren. Ten eerste is de omvang van de cyberdreiging tegen Nederland en Defensie toegenomen. Zo is Defensie dagelijks doelwit van cyberaanvallen. Ten tweede is in Oekraïne cyber in een oorlogscontext zichtbaar, met cyberactiviteit op het gevechtsveld en cyberaanvallen gericht op de maatschappij. Tot slot worden cyberdreigingen dynamischer met steeds geavanceerdere aanvalstechnieken binnen een technologische wapenwedloop.

Bovendien digitaliseert de wereld in een hoog tempo, en Defensie is hierop geen uitzondering. Zowel thuis als op het (digitale) slagveld ondergaat Defensie een continue digitale transformatie. In een dergelijke gedigitaliseerde samenleving is het een maatschappijbrede opgave om ons blijvend tegen cyberdreigingen teweer te stellen, adaptief in te spelen op de veranderlijkheid van de dreiging en voorbereid te zijn op escalatie. Onderdeel daarvan is een goed functionerende Defensieorganisatie en een slagvaardige krijgsmacht met gevechtskracht in het cyberdomein. Daarnaast is Defensie zelf ook in hoge mate afhankelijk van digitale systemen¹.

Taken van Defensie in het cyberdomein

In deze context heeft Defensie drie taken in het cyberdomein:

- 1. Eigen cyberveiligheid in alle omstandigheden**
Defensie moet de eigen systemen veilig houden als dagelijks doelwit van een verscheidenheid aan aanvallen. Deze omstandigheden vergen zicht en grip op de dreiging, en constante inspanning om Defensie digitaal veilig te houden. Defensie moet bovendien rekening houden met actoren die er niet voor terugdeinzen om Defensiemedewerkers digitaal in hun thuisomgeving te raken. Defensie is bovendien digitaal verbonden met de bredere maatschappij, waarbij afhankelijkheden bestaan die kunnen zorgen voor wederzijdse keteneffecten met impact op de inzetbaarheid van de krijgsmacht.
- 2. Uitvoeren van militaire cyberoperaties**
Het cyberdomein is een operationeel domein waarin militaire operaties worden uitgevoerd. Militaire cyberoperaties kunnen op zichzelf staan, maar ook onderdeel zijn van grotere operaties. Ze kunnen bijvoorbeeld ondersteunend zijn aan informatieoperaties die weer integraal onderdeel uitmaken van een militaire campagne op het land. Een cyberoperatie kan tevens een alternatief zijn voor kinetisch optreden.
- 3. Cyberweerbaarheid van het Koninkrijk en bondgenoten**
Defensie speelt een specifieke rol bij de cyberweerbaarheid van het Koninkrijk en bondgenoten. Deze moeten zich continu verdedigen tegen hybride dreigingen. Cyberaanvallen door statelijke of daaraan verbonden actoren bedreigen voortdurend vitale processen waar Defensie en onze bondgenoten afhankelijk van zijn. Cyberweerbaarheid vraagt dan ook een internationale en maatschappijbrede aanpak, waarbij Defensie nauw samenwerkt met andere departementen, bedrijven en bondgenoten.

¹ Digitale systemen omvatten zowel Communicatie- en Informatiesystemen (CIS), ook wel aangeduid met Informatietechnologie (IT), als Sensor-, Wapen- en Commandovoeringssystemen (SEWACO), ook wel operationele technologie (OT) genoemd. Naast de militaire systemen van de krijgsmacht, beschikt Defensie ook over civiele systemen die cybervelig moeten zijn, zoals civiele dienstauto's, mobiele telefoons, liften, brandmeldsystemen, etc.

Digitale slagkracht
voor de bescherming
van het Koninkrijk
en bondgenoten

Randvoorwaarden

Defensie kan bovenstaande taken alleen succesvol uitvoeren door continu te investeren in innovatieve militaire cybertoeepassingen, voor zowel de eigen cyberveiligheid als de cyberslagkracht van de krijgsmacht.

Hiervoor moet Defensie samenwerken met private partijen om hun kennis en expertise te benutten. Daarnaast is het van belang dat Defensie een aantrekkelijke werkgever is voor cyberspecialisten. In tijden van oplopende spanning zal de krijgsmacht bovendien moeten kunnen opschalen met de inzet van reservisten en ondersteuning door civiele overheden en bedrijven, om zo de benodigde cybercapaciteiten te kunnen leveren.

Speerpunten

In antwoord op de hedendaagse uitdagingen, zet Defensie een proactieve koers in met drie strategische speerpunten:

- 1. Permanente proactieve inzet tegen agressieve cyberactoren.**
Defensie wil haar cyberslagkracht op een doorslaggevende wijze in kunnen zetten, zowel in de huidige 'grijze zone' tussen oorlog en vrede als in het scenario van gewapend conflict. Hiervoor introduceert Defensie een nieuwe koers: een permanente proactieve cyberinzet om meer offensief tegendruk te geven. Zo gaat Defensie de aanhoudende cyberaanvallen actief tegen. De krijgsmacht wordt ingezet om militaire cyberoperaties uit te voeren om Nederland te beschermen en bondgenoten te steunen. Deze inzet wordt afgestemd met andere betrokken actoren en in samenhang met (contra)inlichtingen, rechtshandhaving en diplomatieke instrumenten. Door al deze instrumenten in samenhang in te zetten, kunnen we agressieve cyberactoren tijdig onderkennen en hun handelingsvrijheid inperken door hun activiteiten te verstoren of hun aanvalsmiddelen onbruikbaar te maken. Het uitgangspunt daarbij blijft dat Nederland escalatie wil voorkomen.
- 2. Versterking en integratie op alle niveaus.**
Defensie investeert in cyberslagkracht op alle niveaus van militair optreden. Naast het versterken van de cybercapaciteiten, worden deze capaciteiten dichter bij elkaar georganiseerd, en, rekening houdend met functionele sturing, onder eenduidige militaire leiding aangestuurd om ze effectief en geïntegreerd in te kunnen zetten. Niet alleen krijgen individuele commandanten op alle niveaus inzicht in en grip op de cyberspecten bij de uitvoering van hun taak, maar de krijgsmacht positioneert zich om in geval van gewapend conflict cybercapaciteiten gericht en effectief in te kunnen zetten.

- 3. Synergie met publieke en private partijen, en bondgenoten.**
Defensie draagt bij aan de cyberveiligheid van civiele dienstverleners en digitale infrastructuur waar Defensie en onze bondgenoten afhankelijk van zijn. Dit wordt ondersteund door calamiteitenoefeningen met kritieke publieke en private partners, het mobiliseren van private partijen voor cyberondersteuning en actieve participatie in innovatieve publiek-private ecosystemen. Bovendien blijft Defensie de samenwerking met de NAVO, de EU en andere bondgenoten versterken door samen te trainen en oefenen, en multilaterale samenwerkingsverbanden te benutten voor internationale coördinatie en informatiedeling.

Uitvoering

De Defensienota's 2022 en 2024 bieden een basis voor de financiering van deze strategie. De technologische ontwikkelingen en verdere digitalisering van de wereld zullen niettemin in de toekomst steeds om nieuwe investeringen blijven vragen om ons te wapenen tegen digitale dreigingen. Deze zullen via het reguliere plannings- en investeringsproces verlopen.

Tot slot is het van belang dat Defensie ruimte krijgt voor effectieve uitvoering van cybersecuritytaken en gevechtskracht in het cyberdomein. Hiervoor moet Defensie de ruimte binnen de bestaande kaders van taken en bevoegdheden benutten en, waar nodig, bestaande wetgeving aanpassen en nieuwe ontwerpen. Op deze manier kan Defensie zich ook in het cyberdomein voorbereiden op inzet in het grijze gebied en tijdens grootschalig gewapend conflict, om zo een effectieve bijdrage te leveren aan de veiligheid en weerbaarheid van het Koninkrijk en bondgenoten

Overzicht Defensie Cyberstrategie

Defensie Cyberstrategie

Digitale slagkracht voor de bescherming van het Koninkrijk en bondgenoten

Staten zetten hun machtsmiddelen in het cyberdomein agressief in om strategische doelen na te streven. Nederland is dagelijks doelwit van cyberaanvallen. In een gedigitaliseerde samenleving is het een maatschappijbrede opgave om ons blijvend tegen cyberdreigingen te weer te stellen, adaptief in te spelen op de veranderlijkheid van de dreiging en voorbereid te zijn op escalatie van geopolitieke spanningen. De aanhoudende en steeds geavanceerdere cyberdreiging vraagt om een permanente proactieve inzet van Defensie om meer offensief tegendruk te geven in het cyberdomein.

De Defensie Cyberstrategie stelt de taken van Defensie centraal en geeft richting aan de wijze waarop Defensie haar cybercapaciteiten gaat inzetten in de huidige omstandigheden.

Speerpunten

Permanente proactieve inzet tegen agressieve cyberactoren

Versterking en integratie op alle niveaus

Synergie met publieke en private partijen, en bondgenoten

Taken

Eigen cyberveiligheid in alle omstandigheden

Uitvoeren van militaire cyberoperaties

Cyberweerbaarheid van het Koninkrijk en bondgenoten

Randvoorwaarden

Innovatief vermogen in publiek-private ecosystemen

Voldoende gekwalificeerd cyberpersoneel



Inhoudsopgave

Samenvatting	3
Inleiding	8
Strategische Context	10
Taken en Speerpunten	12
Doelen, Aanpak en Middelen	14
Taak 1: Eigen cyberveiligheid in alle omstandigheden	15
Taak 2: Uitvoeren van militaire cyberoperaties	17
Taak 3: Cyberweerbaarheid van het Koninkrijk en bondgenoten	19
Randvoorwaarde 1: Innovatief vermogen in Publiek-Private Ecosystemen	21
Randvoorwaarde 2: Voldoende gekwalificeerd cyberpersoneel	22
Slotwoord	23
Bijlage 1: Begrippenlijst	24
Bijlage 2: Doctrinaire en bestuurlijke uitgangspunten	26



Inleiding

Context

Cyberdreigingen tegen Nederland nemen toe en vormen een steeds groter risico voor het Koninkrijk. Zowel staten als andere actoren proberen via het digitale domein hun invloed uit te oefenen, waardoor onze nationale veiligheid en economie ernstig worden bedreigd. Daarnaast neemt de kans toe dat Nederland betrokken raakt bij een gewapend conflict, waarbij cyberaanvallen een belangrijke rol zullen spelen. In deze context is het essentieel dat Defensie zich blijft aanpassen aan een snel veranderende digitale omgeving.

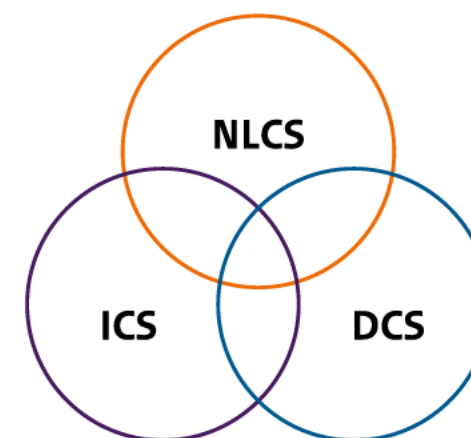
De wereld digitaliseert in een rap tempo, en Defensie is hierop geen uitzondering. Defensie ondergaat momenteel een digitale transformatie om de gevechtskracht van de krijgsmacht te vergroten, geïntegreerde effecten te realiseren en een informatie- en beslisdominantie te bereiken. Deze transformatie is een voortdurend proces. De snelheid waarmee digitalisering en innovatie plaatsvinden, vraagt om een Defensieorganisatie die in staat is om digitale ontwikkelingen effectief te benutten. Door hierop in te zetten, kan Defensie optimaal gebruikmaken van de mogelijkheden die digitalisering biedt en haar positie in een snel veranderende wereld behouden en versterken.

In een dergelijke gedigitaliseerde samenleving is het een maatschappijbrede opgave om ons blijvend teweer te stellen tegen cyberdreigingen, adaptief in te spelen op de veranderlijkheid van de dreiging en voorbereid te zijn op escalatie. Onderdeel daarvan is een sterke Defensieorganisatie en een krijgsmacht met gevechtskracht in het cyberdomein, een domein dat zich kenmerkt door een permanente strategische rivaliteit tussen staten en waar een strikt onderscheid tussen gereedstelling en inzet niet langer goed hanteerbaar is. Het is onvermijdelijk geworden dat we militaire cybercapaciteiten inzetten om ons digitaal veilig te houden.

Herziening

Uit de evaluatie van de vorige strategie uit 2018 bleek een behoefte aan een strategische koers met een concrete aanpak en een samenhangende aansturing van cybercapaciteiten. Daarnaast vraagt de huidige geopolitieke situatie om een proactieve benadering van de cyberweerbaarheid van het Koninkrijk en bondgenoten.

Deze nieuwe Defensie Cyberstrategie stelt de cybertaken van Defensie centraal en geeft richting aan de wijze waarop Defensie haar cybercapaciteiten wil inzetten. De strategie laat zien hoe Defensie in het cyberdomein zal handelen ten aanzien van de eigen cyberveiligheid, bij militaire inzet en om bij te dragen aan nationale cyberweerbaarheid.



Interdepartementale strategieën

Synergie tussen Defensie, andere overheden, private partijen en bondgenoten in het cyberdomein is daarbij essentieel. Naast de eigen taken van Defensie in het cyberdomein, geeft deze strategie ook nadere invulling aan de rol van Defensie binnen interdepartementale strategieën, zoals de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, de Nationale Technologiestrategie (NTS), de Nederlandse Cybersecuritystrategie (NLCS) en de Internationale Cyberstrategie (ICS). Belangrijke aspecten uit deze beleidsstukken waar deze strategie nadere invulling aan geeft, zijn zicht op de dreiging, digitale slagkracht, publiek-private en internationale samenwerking en een proactieve benadering.

Tot slot hangt deze strategie nauw samen met de Digitale Transformatiestrategie van Defensie (DTS)² en de Defensie Strategie voor Industrie en Innovatie (D-SII)³. De synergie tussen deze strategieën stelt Defensie in staat digitale ontwikkelingen ten volle te benutten bij de uitvoering van haar taken.

Leeswijzer

Deze Defensie Cyberstrategie bestaat uit vijf hoofdstukken. Hoofdstuk 1 beschrijft de context van de strategie en het belang van de herziening. Hoofdstuk 2 duidt de uitdagingen waar Defensie voor staat.

Hoofdstuk 3 beschrijft de taken van Defensie in het cyberdomein en de speerpunten van deze strategie.

Deze taken zijn:

1. **Eigen cyberveiligheid in alle omstandigheden**
2. **Het uitvoeren van militaire cyberoperaties**
3. **Cyberweerbaarheid van het Koninkrijk en bondgenoten**

De speerpunten van de strategie betreffen:

1. **Permanente proactieve cyberinzet**
2. **Versterking en integratie op alle niveaus in de organisatie**
3. **Synergie met publiek en private partijen, en bondgenoten**

In hoofdstuk 4 zijn de bijhorende strategische doelen, de beoogde aanpak en middelen, van de cybertaken uitgewerkt. Daarnaast beschrijft dit hoofdstuk de randvoorwaarden die nodig zijn om deze taken te kunnen uitvoeren:

1. **Innovatief vermogen in Publiek-Private Ecosystemen**
2. **Voldoende gekwalificeerd cyberpersoneel**

De bijlagen bevatten essentiële achtergrondinformatie bij de strategie. Bijlage 1 geeft een uitleg van gebruikte begrippen. Bijlage 2 bevat de doctrinaire en bestuurlijke uitgangspunten voor het optreden van de krijgsmacht in het cyberdomein, en vormt de conceptuele basis voor de strategie. Tevens beschrijft deze bijlage de bestuurlijke taakuitvoering van Defensie in het cyberdomein.

² Digitale Transformatie Strategie Defensie, Kamerstuk 36592, nr. 23.

³ Defensie Strategie voor Industrie en Innovatie, Kamerstuk 31125, nr. 134



Strategische Context

Op basis van onder meer rapportages en dreigingsanalyses van de inlichtingen- en veiligheidsdiensten, en open bronnen zoals wetenschappelijke artikelen, ziet Defensie de volgende vier trends in het cyberdomein.

Globale context: polarisatie en proliferatie

Het cyberdomein is een speelveld voor regionale en mondiale dominantie geworden waar een strikt onderscheid tussen gereedstelling en inzet niet langer goed hanteerbaar is.⁴ Het cybermiddel wordt ingezet in een permanente strategische rivaliteit tussen staten in het grijze gebied tussen oorlog en vrede. De voorbereidingen voor cybersabotage spelen zich tegelijkertijd af onder de grens van een gewapend conflict.

In hybride conflictvoering ligt een militaire reactie volgens de huidige kaders niet direct voor de hand. De aanhoudende cyberaanvallen laten bovendien zien dat er momenteel te beperkt sprake is van afschrikking in het cyberdomein. Nederland staat voor een dilemma: de krijgsmacht kan binnen deze kaders slechts beperkt optreden in de 'grijze zone', terwijl tegenstanders zich hier juist op toeleggen omdat het effectief is en de consequenties minimaal zijn.

Omvang: veelheid en verscheidenheid aan assertieve actoren

Het aantal en de omvang van cyberaanvallen gericht tegen Nederlandse belangen en Defensie nemen onverminderd toe door een verscheidenheid aan actoren. Zo richt het offensieve cyberprogramma van Rusland zich onder meer op Nederlandse kritieke infrastructuur en zet China cyberoperaties in om waardevolle (militaire) kennis buit te maken in Nederland. Diverse voorbeelden van succesvolle aanvallen in de afgelopen jaren, zoals de Chinese spionagemalware op een computer-netwerk van Defensie en de Russische hack bij de Nationale Politie, laten zien hoe reëel een onzichtbare dreiging kan zijn. Defensie en andere sectoren zijn bovendien ook doelwit van niet-statelijke cyberactoren, zoals hacktivisten of criminelen. De verschillende actoren zijn niet altijd te onderscheiden en werken in sommige gevallen ook samen.

Oorlogscontext: cyberactiviteit op het gevechtssveld en gericht op civiele doelen

De oorlog in Oekraïne laat zien dat cyber- en hybride oorlogvoering krachtige *force multipliers* zijn, maar (nog) niet doorslaggevend zijn voor militair succes. Een continue digitale verdediging weet de impact van voortdurende Russische aanvalspogingen te beperken. Veel cyberaanvallen zijn gericht op dezelfde doelwitten als bij kinetische aanvallen: de overheid, militaire en civiele infrastructuur voor communicatie, energie en transport. Rusland voert ook beïnvloedingsoperaties uit door cyberoperaties en psychologische oorlogsvoering te combineren. Samen met nieuwe technologieën maakt dit de hoeveelheid en gerichtheid van informatieoperaties efficiënter en meer schaalbaar. Ook China en Iran integreren digitale spionage, sabotage én beïnvloeding in hun operaties.

Dynamiek: Geavanceerde aanvalstechnieken en een technologische wapenwedloop

In het cyberdomein vindt een voortdurende wedloop tussen aanvallers en verdedigers plaats: cyberactoren passen zich snel aan en aanvalstechnieken wijzigen voortdurend. Daarnaast zorgen digitale ontwikkelingen als kunstmatige intelligentie en kwantumtechnologie voor een complexer dreigingslandschap. Voor zulke sleuteltechnologieën geldt dat deze bepalend zijn op het (digitale) speelveld. Dat betekent dat een succesvolle implementatie van deze technologieën een strategisch militair voordeel kan opleveren.

Daarnaast worden informatie en cybermiddelen steeds vaker als wapen gebruikt. In hybride conflictvoering speelt informatie een cruciale rol. Landen met offensieve cyberprogramma's richten zich onder meer op het stelen van data. Door toepassing van kunstmatige intelligentie op buitgemaakte gegevens kunnen bijvoorbeeld sluwe beïnvloedingscampagnes worden ontwikkeld.

⁴ Rapport "Tanden voor de Leeuw", Kamerstuk 33763, nr. 158



Taken en Speerpunten

Taken

Defensie heeft drie taken in het cyberdomein:

Taak 1: Eigen cyberveiligheid in alle omstandigheden

Defensie moet de eigen systemen veilig houden in alle omstandigheden. Dat geldt zowel dagelijks in Nederland als tijdens inzet elders in de wereld. Onder 'eigen systemen' verstaat deze strategie alle systemen van Defensie met een digitale component, dus zowel Communicatie- en Informatiesystemen (CIS), ook wel aangeduid met informatietechnologie (IT), als Sensor-, Wapen- en Commandovoeringssystemen (SEWACO), ook wel operationele technologie (OT) genoemd. Naast de militaire systemen van de krijgsmacht, beschikt Defensie ook over civiele systemen die cyberveilig moeten zijn, zoals mobiele telefoons, kantoorautomatisering, liften, inbraakdetectie, brandmeldsystemen, dienstauto's etc.

Taak 2: Uitvoeren van militaire cyberoperaties

De NAVO beschouwt cyberspace naast land, zee, lucht en ruimte als een operationeel domein. De krijgsmacht moet in staat zijn om vanuit cyberspace fysieke, virtuele en cognitieve effecten te bereiken die tactische, operationele en strategische militaire doelen kunnen dienen.

Militaire activiteiten in het cyberdomein hangen samen met militaire activiteiten in een ander domein of met andere machtsmiddelen die een staat kan inzetten, zoals diplomatie of rechtshandhaving. Militaire cyberoperaties kunnen bijvoorbeeld ondersteunend zijn aan informatie-operaties die weer integraal onderdeel uitmaken van een militaire campagne op het land. Een cyberoperatie kan ook een alternatief zijn voor kinetisch optreden. Defensie wil cybereffecten in NAVO-missies en -operaties kunnen inbrengen om zo gezamenlijk slagkracht te genereren.

Taak 3: Cyberweerbaarheid van het Koninkrijk en bondgenoten

Defensie draagt bij aan een veilige samenleving en heeft een ook een rol bij de cyberweerbaarheid van het Koninkrijk en bondgenoten. Defensie voert, al dan niet onder gezag van andere ministeries, specifieke cybertaken uit, onder meer vanuit de eigen inlichtingen- en veiligheidstaak, politietaken en bijstandstaak, en ondersteunt anderen met unieke kennis en capaciteiten. Cyberweerbaarheid vraagt een internationale en maatschappijbrede aanpak, waarbij Defensie nauw samenwerkt met andere departementen, bedrijven en bondgenoten, waaronder de NAVO en de EU.

Speerpunten

Defensie slaat een proactieve koers in om deze cybertaken slagvaardig uit te voeren. De nieuwe cyberkoers van Defensie kenmerkt zich door de volgende drie speerpunten:

Speerpunt 1: Permanente proactieve cyberinzet tegen agressieve cyberactoren

Defensie wil haar cyberslagkracht op een doorslaggevende wijze in kunnen zetten, zowel in de huidige grijze zone tussen oorlog en vrede als in het scenario van gewapend conflict. Hiervoor introduceert Defensie een nieuwe koers: een permanente proactieve inzet om meer offensief tegendruk te geven in het cyberdomein. Zo gaat Defensie de aanhoudende cyberaanvallen actief tegen.

Reactieve maatregelen zijn niet meer voldoende om Nederland tegen kwaadwillende cyberactoren te beschermen. De aanhoudende en steeds geavanceerdere cyberaanvallen vragen om een permanente inzet van Defensie om de continue dreiging actief tegen te gaan, zowel om zichzelf cyberveilig te houden als om het Koninkrijk en bondgenoten te beschermen. Bovendien is het noodzakelijk continu te werken aan een goede uitgangspositie ten opzichte van kwaadwillende actoren om hun vrijheid van handelen tot een aanvaardbaar niveau te beperken.

De krijgsmacht wordt ingezet om militaire cyberoperaties uit te voeren om Nederland te beschermen en bondgenoten te steunen. Deze inzet wordt afgestemd met andere betrokken actoren en in samenhang met (contra)inlichtingen, rechtshandhaving en diplomatieke instrumenten. Door al deze instrumenten in samenhang in te zetten, kunnen we agressieve cyberactoren tijdig onderkennen en hun handelingsvrijheid inperken door hun activiteiten te verstoren of hun aanvalsmiddelen onbruikbaar te maken. Het uitgangspunt daarbij blijft dat Nederland escalatie wil voorkomen

Speerpunt 2: Versterking en integratie op alle niveaus

Defensie investeert in zowel de cyberslagkracht om militaire cyberoperaties uit te voeren, als in de integratie daarvan in de nationale en internationale structuren. Daarnaast investeert Defensie verder in tactische CEMA-capaciteiten (*Cyber- and Electromagnetic Activities*) om militaire eenheden competent te maken in cyber en het elektromagnetisch spectrum op het gevechtssveld. De krijgsmacht werkt de militaire strategie voor cyberinzet uit om in geval van gewapend conflict cybercapaciteiten gericht en effectief in te kunnen zetten.

Naast het versterken van de cybercapaciteiten, worden deze capaciteiten dichter bij elkaar georganiseerd, en, rekening houdend met functionele sturing, onder eenduidige militaire leiding aangestuurd. Dat omvat ook de cybersecurity van de eigen systemen, inclusief risicobeheersing bij uitval of compromittatie.

Speerpunt 3: Synergie met publieke en private partijen, en bondgenoten

Defensie draagt bij aan de cyberveiligheid van civiele dienstverleners en digitale infrastructuur waar Defensie en onze bondgenoten afhankelijk van zijn. De krijgsmacht houdt bijvoorbeeld calamiteitenoefeningen met kritieke publieke en private partners en kan worden ingezet bij cyberincidenten, zowel in binnen- als buitenland.

Omgekeerd is Defensie voor de eigen cyberveiligheid afhankelijk van toeleveranciers en moet Defensie private partijen weten te mobiliseren voor cyberondersteuning aan de krijgsmacht in geval van een (dreigend) gewapend conflict. Defensie gaat actief participeren in innovatieve publiek-private ecosystemen om technologisch voor te blijven op tegenstanders.

In samenspraak met andere departementen zal Defensie bezien hoe haar groeiende rol in de cyberverdediging van Nederland past in het Nederlandse cybersecuritystelsel. Tot slot versterkt Defensie de samenwerking met bondgenoten. Defensie zet in op het versterken van multilaterale samenwerkingsverbanden, zoals de NAVO en de EU. Daarbij benut Defensie internationale coördinatie en informatie-delingsmechanismen voor schaalvoordelen, versnelde respons, en effectieve inzet. Militaire cyberoperaties worden zoveel mogelijk uitgevoerd met gelijkgezinde bondgenoten.

Doelen, Aanpak en Middelen

De doelen, aanpak en middelen van deze strategie zijn uitgewerkt op basis van de drie cybertaken van Defensie: de cyberveiligheid van de eigen systemen, het uitvoeren van militaire cyberoperaties, en de cyberweerbaarheid van het Koninkrijk en bondgenoten. In aanvulling daarop heeft Defensie de doelen, aanpak en middelen vastgesteld voor de twee essentiële randvoorwaarden: innovatief vermogen en voldoende gekwalificeerd cyberpersoneel.

Taak 1: Eigen cyberveiligheid in alle omstandigheden

Visie

Defensie moet de eigen systemen veilig houden, aangezien deze dagelijks doelwit zijn van cyberaanvallen. Zulke cyberaanvallen stoppen niet bij het hek van een kazerne.

Het niet adequaat beschermen van de eigen systemen kan een grote impact hebben op de inzetbaarheid van de krijgsmacht. Daarnaast kan een cyberincident bij Defensie verstrekken gevolgen hebben voor zowel nationale als internationale partners, waaronder publieke en private organisaties, en de maatschappij als geheel. Daarom treft Defensie proactief maatregelen om cyberrisico's in kaart te brengen en te beheersen, en om tijdig te kunnen acteren op eventuele cyberincidenten.

De cyberveiligheid kan echter alleen op peil worden gehouden als ook het digitale fundament op orde is en Defensie beschikt over een moderne, robuuste digitale infrastructuur. Militaire eenheden moeten bovendien in staat zijn om hun zelfbeschermingsfunctie uit te voeren binnen het cyberdomein. Defensie moet daarbij rekening houden met actoren die er niet voor terugdeinzen om Defensiemedewerkers digitaal in hun thuisomgeving te raken. Daarnaast stelt Defensie hoge eisen aan de beschikbaarheid, betrouwbaarheid en integriteit van zowel bestaande als nieuwe hardware en software, inclusief die uit de toeleveringsketen.

In een militaire organisatie is de commandant integraal verantwoordelijk voor de uitvoering van de opgedragen taak. Dat betekent dat commandanten op alle niveaus de eigen cyberrisico's moeten beheersen en inzicht hebben in de cybergereedheid van de eenheid. Ook de interne en externe coördinatie van cyberincidenten en –calamiteiten zal gaan plaatsvinden in de reguliere commandostructuur, om effectiever te kunnen handelen en samenwerken met andere overheden, private partijen en bondgenoten.

Doelen en Aanpak

Defensie heeft voor de eigen cyberveiligheid vijf strategische doelen met bijbehorende aanpak vastgesteld:

1. **Defensie heeft zicht en grip op het groeiende digitale aanvalsoppervlak en dreigingen tegen eigen systemen**
Commandanten krijgen inzicht in de status van hun digitale systemen en het bijhorende dreigingslandschap.

Ook worden commandanten in staat gesteld om adequaat te kunnen reageren in het geval van een cyberincident. Bovendien wordt de taak van Defensie om eigen systemen en netwerken cyberveilig te houden, wettelijk vastgelegd.

2. **Alle systemen en data zijn op basis van een risico-afweging afdoende berekend op dreigingen**
Dit doet Defensie door commandanten inzicht te geven in hun cybergereedheid en hen in staat te stellen hun cyberrisico's te kunnen beheersen. Om dit te bereiken, worden onder andere rollen en verantwoordelijkheden voor informatiebeveiliging gestroomlijnd en wordt geïnvesteerd in *Security Operations Centers* (SOCs). Daarnaast hanteert Defensie een risico-gebaseerd beleid voor bestaande en nieuwe systemen, maakt Defensie afhankelijkheden en kwetsbaarheden in de toeleveringsketen inzichtelijk en stimuleert het gebruik van innovatieve oplossingen met geavanceerde technologieën.
3. **Defensiepersoneel handelt cyberveilig doordat het daartoe de kennis, inzicht en, middelen voor heeft.**
Defensie houdt het eigen personeel continu bewust van cyberdreigingen en biedt concrete handvatten om met deze dreigingen om te gaan. Hiervoor worden middelen beschikbaar gesteld zodat medewerkers de mogelijkheid hebben cyberveilig te handelen.
4. **Defensie zorgt voor de digitale bescherming van het eigen personeel en het thuisfront**
Defensie helpt eigen personeel en hun thuisfront omtrent digitale dreigingen en het veilig gebruik van sociale media en digitale systemen. Zo worden cyberveilige middelen beschikbaar gesteld voor personeel (zowel uitgezonden als thuis).
5. **Defensie beschikt over een modern en robuust digitaal fundament**
Defensie ondergaat een digitale transformatie om de informatie-infrastructuur te moderniseren en informatie-technologie zo te benutten dat het de gevechtskracht versterkt. Deze transformatie is essentieel om de systemen robuust en weerbaar te maken tegen huidige en toekomstige cyberdreigingen. Bovendien wordt niet-kwantumveilige cryptografie vervangen door quantumveilige varianten, geprioriteerd op basis van risico. Daarnaast neemt Defensie maatregelen om te voorkomen dat gegevens die nu nog zijn beschermd met huidige cryptografie, in de toekomst alsnog kunnen worden ontsleuteld door meer geavanceerde technologieën, het zogenaamde 'store now, decrypt later' principe.

Organisatie en Middelen

De uitvoering van de strategie op het gebied van de eigen cyberveiligheid vindt voor een belangrijk deel plaats binnen de huidige organisatiestructuur, in het bijzonder met de volgende organisatiedelen:

- Het **Directoraat-Generaal Beleid** (DGB) en de **Chief Information Office** (CIO) dragen zorg voor beleid en kaderstelling;
- De **Militaire Inlichtingen- en Veiligheidsdienst** (MIVD) voor (contra-)inlichtingen;
- Het **Netherlands Joint Force Command** (NLD JFC) is belast met de opbouw van het cyberomgevingsbeeld en de domeinoverstijgende beheersing van cyberincidenten- en calamiteiten in alle omstandigheden;
- Het **Defensie Cybercommando** (DCC) heeft als cyberstafelement onder meer tot taak namens CDS de inzet van de cybercapaciteiten integraal aan te sturen;
- Het **Commando Materieel en IT** (COMMIT), met daarin het Joint Informatievoorzieningscommando (JIVC), waaronder ook het Defensie Cyber Security Centrum (DCSC), voor ondersteuning op cyberveiligheidsgebied aan de krijgsmacht gedurende de gehele levenscyclus van CIS en SEWACO;
- De **Security Operating Centers** (SOCs) zijn het middel voor commandanten op lager niveau om in de operatie invulling te geven aan de zelfbeschermingsfunctie in het cyberdomein.

Om deze cybertaak en bijhorende doelen te kunnen uitvoeren, zijn aanvullende middelen, beleid en juridische kaders nodig. Financiering hiervoor zal via het reguliere plannings- en investeringsproces verlopen. De Digitale Transformatiestrategie van Defensie geeft richting aan de algehele modernisering en doorontwikkeling van de digitale infrastructuur van Defensie. De MIVD richt een *Cyber Fusion Cell* in om Defensiebreed cyberdreigingsinformatie te verzamelen, analyseren en te delen. Daarnaast legt de nieuwe Wet op de Defensie gereedheid (Wodg) deze taak wettelijk vast om zo daarmee de vereiste juridische grondslag te creëren om de eigen systemen veilig te kunnen houden. Waar mogelijk zal Defensie werken conform de Cyberbeveiligingswet. Tevens zijn aanvullende kwantumveilige cryptografische middelen nodig om systemen en gegevens te beschermen tegen kwantumcomputers. Tot slot gaat Defensie aan de slag met nieuw beleid ten behoeve van het stimuleren van cyberveilig gedrag van medewerkers en het thuisfront.

Taak 2: Uitvoeren van militaire cyberoperaties

Visie

Defensie beschouwt cyber als een volwaardig operationeel domein, naast land, lucht, maritiem en ruimte. In het cyberdomein worden militaire activiteiten en operaties uitgevoerd die zowel defensief als offensief van aard kunnen zijn.

Cyberactiviteiten zijn nauw verweven met militaire operaties in andere domeinen, wat een geïntegreerde benadering en een robuust digitaal fundament vereist. Daarnaast kunnen cyberactiviteiten in het digitale domein ook samenhangen met andere machtsmiddelen die Nederland kan inzetten, zoals diplomatie en rechtshandhaving. Bovendien biedt het cyberdomein niet alleen een aanvulling op andere domeinen, maar kunnen cyberoperaties ook dienen als een alternatief voor traditionele kinetische operaties. Tot slot zijn activiteiten in het cyberdomein op tactisch niveau verweven met activiteiten in het elektromagnetisch spectrum.

Doelen en Aanpak

Defensie heeft voor de militaire taak in het cyberdomein vier strategische doelen met een bijbehorende aanpak vastgesteld:

1. **De krijgsmacht is continu in staat een adequaat cyberomgevingsbeeld op te bouwen en te integreren in het totale operationele omgevingsbeeld**
Hiertoe wordt de samenwerking tussen bestaande stafelementen en cyberentiteiten geïntensiveerd. Door deze intensievere samenwerking en aanvullende investeringen is Defensie in staat een cyberomgevingsbeeld te creëren dat wordt geïntegreerd in het totale omgevingsbeeld. Dit omgevingsbeeld wordt daarnaast aangevuld met cyberomgevingsbeelden van civiele overheden en private partijen.

2. **De krijgsmacht weet cyberinzet te coördineren, de conflicteren, integreren en synchroniseren met iedere andere vorm van militaire inzet, inclusief operaties van bondgenoten, met NAVO-plannen, en met de inzet van niet-militaire machtsmiddelen**
Defensie stuurt militaire cyberoperaties in de bestaande commandostructuur aan. Dit houdt onder andere in dat deze militaire cyberoperaties tijdig worden voorbereid met ondersteuning van de Militaire Inlichtingen- en Veiligheidsdienst, en gesynchroniseerd zijn met andere machtsmiddelen. Cyberinzet wordt daarnaast geïntegreerd in alle niveaus van de commandovoering, inclusief planning en doelselectie zodat cyberaspecten altijd meegenomen worden in de besluitvorming en uitvoering van militaire operaties. Bovendien neemt Defensie deel aan interdepartementale en internationale scenario-ontwikkelingen en cyberoefeningen, zoals van de NAVO en de EU.

3. **De krijgsmacht weet het cyberdomein te benutten om eigenstandig effecten te bereiken in en vanuit dat domein**
Om dit te bereiken bepaalt Defensie tijdig en adaptief de militaire-strategische richting voor potentiële cyberinzet. Daarnaast worden operationele cybercapaciteiten continu doorontwikkeld en versterkt door onder meer te investeren in zo realistisch mogelijke (multidomein) training. Cybereenheden oefenen met eenheden gespecialiseerd in vormen van informatieoperaties om een geïntegreerde aanpak te garanderen.

Daarnaast kan Defensie oorlogsmisdaden in en via het cyberdomein opsporen, om bij te dragen aan de handhaving van de internationale rechtsorde. Tot slot moet de inzet van cybermiddelen getoetst kunnen worden aan het nationale en internationale recht, om ervoor te zorgen dat Defensie handelt in overeenstemming met de geldende normen en wetgeving.

4. **Militaire eenheden zijn competent in het cyberdomein en het elektromagnetisch spectrum, en beschikken over de juiste capaciteiten en bevoegdheden, afhankelijk van hun taakstelling en gereedheidsstatus**
Tactische cyber en elektromagnetische capaciteiten van de krijgsmacht worden uitgebreid en versterkt. Om deze capaciteiten effectief in te zetten, is het noodzakelijk om een gepast juridisch kader te creëren, bestaande uit wetgeving, regelgeving en militaire orders. Dit zorgt ervoor dat eenheden beschikken over de relevante bevoegdheden om hun taakstellingen en opdrachten uit te voeren. Daarnaast worden eenheden competent gemaakt en voorzien van middelen om het internet operationeel veilig te benutten voor tactische inlichtingen uit open bronnen.

Organisatie en Middelen

Defensie kan deze strategie om militaire cyberoperaties uit te voeren grotendeels met bestaande middelen die Defensie reeds tot haar beschikking heeft uitvoeren, in het bijzonder door de volgende organisatiedelen:

- Het **Directoraat-Generaal Beleid** (DGB) is belast met de politiek-bestuurlijke besluitvorming voor militaire (cyber) operaties;
- Het **Netherlands Joint Force Command** (NLD JFC) is de entiteit voor het plannen, voorbereiden, uitvoeren en ondersteunen van multidomein inzet, waaronder cyberinzet;
- Het **Defensie Cybercommando** (DCC) is de entiteit die militaire cyberoperaties aanstuurt en uitvoert, waarbij de **Militaire Inlichtingen- en Veiligheidsdienst** (MIVD) een onmisbare rol speelt. Multidisciplinaire Cyberteam van het DCC werken hiertoe samen met en binnen de MIVD;
- De **Operationele Commando's** beschikken over de middelen voor tactische cyber en elektromagnetische activiteiten op het gevechtsveld en de **Koninklijke Marechaussee** over forensische middelen voor hun rechtshandavingstaken.

Defensie heeft in de afgelopen jaren geïnvesteerd in de militaire cybercapaciteiten en blijft dat doen. Defensie verbetert zowel de cyberslagkracht om militaire cyberoperaties uit te voeren, als in de integratie daarvan in de nationale en internationale structuren. Daarnaast continueert Defensie de investeringen in tactische cyber en elektromagnetische capaciteiten om militaire eenheden competent te maken in cyber en het elektromagnetisch spectrum op het gevechtsveld.

Om deze cybertaak en bijhorende doelen te kunnen uitvoeren zijn aanvullende middelen nodig bovenop de reeds geplande investeringen. Financiële dekking zal binnen budgetten van belanghebbende Defensieonderdelen worden gezocht, via het reguliere plannings- en investeringsproces. De eerder genoemde digitale transformatie komt ook de gevechtskracht in het cyberdomein ten goede. Verdere versterking zit met name in de verbetering van de militaire commandovoering zodat die in staat is permanent te sturen op militair-strategische doelstellingen en doelstellingen binnen een eenduidig kader van wet- en regelgeving, inzetmandaat, plannen en militaire orders. Ook voor deze taak is de voorziene *Cyber Fusion Cell* een essentiële toevoeging om te kunnen opereren met een gedeeld cyberomgevingsbeeld. Voor relatieopbouw en samenwerking met bondgenoten bouwt de krijgsmacht een Militair Cyberliaison Netwerk op. Tot slot werkt Defensie aan operationele internetvoorzieningen zodat militaire eenheden het internet overal en veilig kunnen gebruiken als bron voor tactische inlichtingen.

Taak 3: Cyberweerbaarheid van het Koninkrijk en bondgenoten

Visie

Defensie speelt een specifieke rol bij de cyberweerbaarheid van het Koninkrijk en haar bondgenoten. Er is momenteel een te beperkt afschrikkingseffect in het cyberdomein waarneembaar; cyberaanvallen door statelijke of daaraan verbonden actoren blijven voortdurend vitale processen bedreigen, ondanks de tot nu geleverde inspanningen.

Cyberweerbaarheid vraagt dan ook een internationale en maatschappijbrede aanpak, waarbij Defensie nauw samenwerkt met andere departementen, private bedrijven en bondgenoten. Ook al is de algehele cyberweerbaarheid primair een civiele aangelegenheid, Defensie speelt hierin wel een significante rol vanuit de inlichtingen- en veiligheidstaak, de rechtshandhaving, de landsverdediging en eventuele militaire steunverlening.

In aanvulling op contra-inlichtingenactiviteiten van de inlichtingen- en veiligheidsdiensten zet Defensie de krijgsmacht in om militaire cyberoperaties uit te voeren om Nederland te beschermen en bondgenoten te steunen. Daarnaast levert Defensie waar mogelijk op verzoek ondersteuning aan civiele overheden, private partners en bondgenoten gericht op het verhogen van cyberweerbaarheid, zoals capaciteitsopbouw, handhaving, detectie en respons om een effectieve inzet te bewerkstelligen. Defensie zal met andere betrokken departementen bezien hoe deze groeiende rol in de cyberverdediging van Nederland past in het toekomstige Nederlandse cybersecuritystelsel.

Doelen en Aanpak

Voor de bijdrage aan de maatschappijbrede cyberweerbaarheid heeft Defensie zes strategische doelen met een bijbehorende aanpak vastgesteld:

1. **Defensie werkt aan een nationaal en bondgenootschappelijk cyberomgevingsbeeld en verstrekt gericht cyberinformatie en -inlichtingen**
Dit doet Defensie door in interdepartementaal verband het aanvalsoppervlak van te beschermen belangen in beeld te brengen en te houden. Ten behoeve van dit cyberomgevingsbeeld draagt Defensie bij aan onderzoek, actieve monitoring, detectie, preventie en respons.

Om informatie-uitwisseling te optimaliseren, wordt continu bepaald welke informatie (geautomatiseerd) kan worden gedeeld. Daarnaast stimuleert Defensie informatie-uitwisseling door de informatiebehoefte van partners en bondgenoten beter te begrijpen en de eigen informatiebehoefte kenbaar te maken. Om het bewustzijn en de weerbaarheid van het Koninkrijk en bondgenoten op het gebied van cyberveiligheid te vergroten, maakt Defensie – waar mogelijk – cyberaanvallen en bijbehorende technische werkwijzen openbaar via de geëigende interdepartementale kanalen. Tot slot steunt Defensie multilaterale initiatieven op het gebied van informatie-uitwisseling waar schaalvoordelen kunnen worden behaald.
2. **Defensie draagt in interdepartementaal verband bij aan de cyberveiligheid van civiele dienstverleners, toeleveranciers en digitale infrastructuur waar de krijgsmacht en bondgenoten afhankelijk van zijn voor inzet**
Defensie identificeert kritieke dienstverleners die essentieel zijn voor de operaties van de krijgsmacht op basis van een (cyber)risicoanalyse. Daarnaast draagt Defensie bij aan cyberweerbaarheid van deze kritieke dienstverleners en toeleveranciers om te voorkomen dat zwakke plekken in de keten kunnen worden misbruikt door cyberactoren. Verder werkt Defensie in interdepartementaal verband samen met civiele partners aan kennisoverdracht, waarbij praktijkervaringen en personeel worden uitgewisseld en gezamenlijk wordt geoefend.

Tot slot stelt Defensie in interdepartementaal verband passende eisen aan toeleveranciers en civiele dienstverleners, waaronder het ter beschikking stellen van telemetrie en logging om geavanceerde cyberdreigingen te kunnen detecteren.

3. **Defensie staat klaar om bij ernstige cybercalamiteiten ondersteuning en militaire steun te verlenen, afhankelijk van andere militaire prioriteiten, onder meer via de nationale crisisbeheersingsstructuur of afgestemd via internationale coördinatiemechanismen**
De krijgsmacht kan worden ingezet bij ernstige cyberincidenten en neemt hiertoe deel aan calamiteitenoefeningen die gehouden worden met kritieke publieke en private partners. Defensie dient daarbij snel en adequaat te reageren op tijdskritische verzoeken voor ondersteuning.
4. **Defensie weet civiele overheden en private partijen te mobiliseren voor cyberondersteuning aan de krijgsmacht in geval van (dreigend) gewapend conflict**
In het geval van een (dreigend) gewapend conflict draagt Defensie de maatschappijbrede aanpak voor cyberweerbaarheid actief uit. Deze aanpak wordt tevens opgenomen in landelijke crisisplannen. Daarnaast kunnen cyberreservisten worden opgeroepen en cyberspecialisten uit een netwerk van bedrijven worden ingehuurd om waar nodig ondersteuning te bieden.
5. **Defensie draagt in interdepartementaal verband bij aan de bestrijding van (gedigitaliseerde) criminaliteit**
Defensie benut het cyberdomein voor de militaire politietaak en grenspolitietaak, evenals voor het taakveld bewaken en beveiligen. Het cyberdomein is onderdeel van handhaving, opsporing en inlichtingen, waardoor criminele digitale activiteiten kunnen worden opgespoord. Ten slotte wordt gewerkt aan een effectieve toepassing van digitale technieken en geautomatiseerd onderzoek om de opsporingstaak te versterken.
6. **Defensie draagt bij aan een proactieve benadering tegen aanhoudende statelijke cybercampagnes**
Defensie beschermt het Koninkrijk en ondersteunt bondgenoten door militaire cyberoperaties uit te voeren, waar nodig met offensieve middelen, in aanvulling op contra-inlichtingenactiviteiten. Zulke cyberoperaties worden interdepartementaal afgestemd met andere instrumenten, zoals cyberdiplomatie en rechtshandhaving.

Organisatie en Middelen

De uitvoering van de strategie op het gebied van de maatschappelijke cyberweerbaarheid vindt voor een belangrijk deel plaats met bestaande middelen die Defensie reeds tot haar beschikking heeft:

- De **Militaire Inlichtingen- en Veiligheidsdienst** (MIVD) speelt hierin vanuit haar organieke taak een centrale rol bij de maatschappijbrede cyberweerbaarheid.
- Het **Netherlands Joint Force Command** (NLD JFC) is de entiteit om nationale en internationale cybersteunverzoeken te beoordelen en het Defensie Cybercommando (DCC) om de daaruit voortvloeiende inzet aan te sturen.
- De **Koninklijke Marechaussee** (KMAR) maakt gebruik van cybercapaciteiten in de uitvoering van de rechtshandhavingstaken.
- Defensie sluit aan bij het interdepartementale cyberweerbaarheidsnetwerk onder leiding van het **Nationaal Coördinator Terrorismebestrijding en Veiligheid** (NCTV).

Defensie stemt de inzet van deze middelen af met andere instrumenten die Nederland kan inzetten via de bestaande interdepartementale overleg- en crisisstructuren. Dit is in lijn met de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, dat de interdepartementale en civiel-militaire samenwerking op het gebied van (digitale) veiligheid voorziet. In aanvulling daarop draagt ook de uitvoering van de Nationale Digitaliseringsstrategie (NDS) bij aan een weerbare overheid.

Ook voor deze cybertaak van Defensie is de eerder genoemde *Cyber Fusion Cell* van belang ten behoeve van het tijdig analyseren en delen van relevantie cyberdreigingsinformatie. Verder werkt Defensie aan aanvullend beleid voor het bevorderen van de cyberweerbaarheid van dienstverleners en toeleveranciers van Defensie. Aanvullende financiering zal via het reguliere plannings- en investeringsproces moeten worden opgelopen.

Randvoorwaarde 1: Innovatief vermogen in Publiek-Private Ecosystemen

Visie

Om doorslaggevende voordelen ten opzichte van tegenstanders in het cyberdomein te verkrijgen en behouden, werkt Defensie continu aan een technologische voorsprong.

Een robuust digitaal fundament en investeringen in innovatieve (militaire) cybertoeepassingen zijn essentieel voor zowel de cyberslagkracht als de cyberveiligheid van Defensie. Aangezien Defensie niet in dezelfde mate kan investeren in nieuwe kennis en technologieën als de private sector, is het belangrijk om samen te werken met private partijen om hun kennis en expertise aan te boren. Partnerschappen met de private sector zijn dan ook cruciaal: ze stellen Defensie in staat om te profiteren van de laatste ontwikkelingen en trends in de cybersector.

Doelen en Aanpak

Defensie heeft voor cyberinnovatie een viertal strategische doelen met een bijbehorende aanpak vastgesteld:

1. **Defensie is onderdeel van innovatieve partnerschappen ten behoeve van het verhogen van de cybergereedheid van Defensie en het uitvoeren van militaire cyberoperaties door de krijgsmacht**
Defensie draagt bij aan wetenschappelijk onderzoek en kennisopbouw over militaire concepten en technologieën. Defensie benut bovendien multilaterale samenwerkingsverbanden binnen de NAVO en EU om schaalvoordelen te behalen en werkt samen met het bedrijfsleven om innovatie te stimuleren. Samen met het bedrijfsleven worden innovatieve (deel)producten geverifieerd en gevalideerd. Tot slot positioneert Defensie zich als een herkenbare en betrouwbare partner, zowel nationaal als internationaal.
2. **Defensie is in staat snel nieuwe cybertechnologieën te valideren en implementeren**
Defensie ontwikkelt, test en valideert nieuwe technologieën en oplossingen dichtbij de operationele uitvoering. Daarnaast verbetert Defensie de randvoorwaarden voor kort-cyclische innovatie en implementatie. Hierbij is aandacht voor onder andere cultuur, faciliteiten en juridische kaders. Als betrouwbare samenwerkingspartner creëert Defensie duidelijke voorwaarden voor samenwerking en worden cyberrends en marktontwikkelingen nauw in de gaten gehouden om oplossingen te vinden voor militaire toepassingen.

3. **Defensie weet het vertrouwen van de maatschappij te behouden ten aanzien van de (militaire) toepassing van nieuwe technologieën in het cyberdomein en draagt bij aan de ontwikkeling van (internationale) normen hierover**
Defensie zal zich blijven inspannen om uit te leggen hoe nieuwe technologieën essentieel zijn om militaire dreigingen het hoofd te blijven bieden. Daarnaast draagt Defensie actief bij aan internationale discussies over de ethische en juridische aspecten van het gebruik van nieuwe technologieën in het cyberdomein.
4. **Defensie is binnen Nederland voortrekker van autonomie op het gebied van (post-kwantum) cryptografie en offensieve cybercapaciteiten**
Defensie bouwt strategische samenwerkingsverbanden op met vertrouwde bedrijven en onderzoeksinstituten. Daarnaast faciliteert Defensie langdurige investeringen om ervoor te zorgen dat het innovatief vermogen rondom deze sleutelgebieden ook in de toekomst gewaarborgd is.

Organisatie en Middelen

Bij het realiseren van deze randvoorwaarde spelen de **Nederlandse Defensie Academie** (NLDA) en het **Cyber Warfare & Training Centre** (CWTC) een sleutelrol: deze partijen ontwikkelen en dragen academische en praktische cyberkennis over binnen Defensie. Daarnaast spelen de **Cyber Innovation Hub** (CIH) en de afdeling **Kennis, Innovatie, eXperimenten en Simulatie** (KIXS) een rol in het stimuleren van cyberinnovatie binnen Defensie in samenwerking met derde partijen, waaronder de betrokken departementen, wetenschappelijke instellingen en bedrijven.

Randvoorwaarde 2: Voldoende gekwalificeerd cyberpersoneel

De cybercapaciteiten van Defensie zijn afhankelijk van kundig en gespecialiseerd cyberpersoneel. Aangezien dergelijk personeel schaars is, moet Defensie een aantrekkelijke werkgever zijn om hen aan te trekken en te behouden.

Dit vereist het bieden van perspectief en een stimulerende werkomgeving. Bovendien zal de krijgsmacht in tijden van oplopende spanning moeten kunnen opschalen met de inzet van reservisten en ondersteuning door civiele overheden en bedrijven, om zo de benodigde cybercapaciteiten te kunnen leveren.

Doelen en Aanpak

Om over voldoende cyberpersoneel te kunnen beschikken, heeft Defensie vier strategische doelen met een bijbehorende aanpak vastgesteld:

1. Defensie voert een innovatief personeelsbeleid om schaars en specialistisch cyberpersoneel te vinden, binden, boeien en inspireren

Defensie voert centrale regie op de prioritering en vulling van cyberfuncties en werkt aan een passende beloning voor cyberpersoneel. Defensie levert maatwerk bij de werving en selectie van schaars personeel en investeert daarnaast in leiderschap aan cyberpersoneel. Defensie leidt zelf hoogwaardig cyberpersoneel op en gaat strategische partnerschappen aan met bedrijven, scholen en andere kennisinstellingen. Daarnaast worden uitdagende oefenen en trainingsprogramma's voor zowel eigen personeel als externe experts en talenten opgezet. Bovendien wordt de mogelijkheid onderzocht om een aparte aanstellingsvorm te creëren voor militair cyberpersoneel, waarbij er differentiatie kan plaatsvinden in de eisen die worden gesteld tijdens de keuring.

2. Defensie verhoogt bij niet-cyberspecialisten het basisniveau aan kennis over het cyberdomein

Dit doet Defensie door cyber(kennis) te integreren in alle niveaus van trainen en opleiden. Er worden gerichte cyberopleidingen voor operationele functies (zoals commandanten, planners en scenariobouwers) geboden en cyberaspecten worden geïntegreerd in technische opleidingen.

3. Defensie beschikt over een flexibele schil van cyberreservisten, die over unieke cyberkennis en -ervaring uit private en publieke organisaties beschikken, en afhankelijk van hun huidige functie en als de omstandigheden daarom vragen, volledig beschikbaar zijn voor militaire inzet

Defensie draagt zorg dat cyberreservisten in vredesomstandigheden de mogelijkheid hebben om hun civiele baan af te wisselen met militaire inzet. Voor iedere reservist wordt zorgvuldig afgewogen of de militaire beschikbaarheid niet ten koste gaat van een civiele baan in een vitaal proces. Cyberreservisten worden gericht getraind om snel op te schalen en onze militaire cybercapaciteit te versterken in tijden wanneer dat nodig is. Bovendien werkt Defensie aan strategische partnerschappen met bedrijven om snel maatschappijbreed op te kunnen schalen ten tijde van crisis.

4. Defensie werkt aan oplossingen om cyberwerkzaamheden te extensiveren door automatisering en toepassing van kunstmatige intelligentie

Defensie identificeert welke arbeidsintensieve en automatiseerbare taken prioriteit moeten krijgen. Ook wordt bij cyberinnovatie gericht geïnvesteerd in arbeidsextensieve oplossingen en toepassing van kunstmatige intelligentie.

Organisatie en Middelen

Om deze randvoorwaarden te realiseren, is het **Directoraat-Generaal Beleid** (DGB) verantwoordelijk voor het ontwikkelen van personeelsbeleid, met daarinbinnen differentiatie voor cyberpersoneel. Het **Cyber Warfare & Training Centre** (CWTC) en de **Cyber Academie** zijn met de **Nederlandse Defensie Academie** (NLDA) en **Operationele Commando's** verantwoordelijk voor het trainen van cyberpersoneel ten behoeve van de krijgsmacht. Verder gaat de Defensiestaf een centrale rol spelen bij het stellen van Defensiebrede prioriteiten voor de vulling van cyberfuncties. Tot slot hebben de **Cyber Innovation Hub** (CIH) en de afdeling **Kennis, Innovatie, eXperimenten en Simulatie** (KIXS) een rol bij het implementeren van cyberinnovatie ten behoeve van arbeidsextensieve oplossingen.



Slotwoord

Het huidige cyberdreigingslandschap en de geopolitieke situatie brengen uitdagingen met zich mee. In een steeds verder digitaliserende wereld, waarin statelijke en niet-statelijke actoren hun machtsmiddelen in het cyberdomein agressief inzetten om strategische doelen na te streven, moet Defensie zichzelf cyberveilig kunnen houden. Daarnaast moet Defensie, ter bescherming van het Koninkrijk en bondgenoten, haar cyberslagkracht op een doorslaggevende wijze in kunnen zetten wanneer de regering daarom vraagt, zowel in het grijze gebied tussen oorlog en vrede, als in een gewapend conflict.

Het is daarom essentieel dat Defensie een voorsprong houdt op potentiële tegenstanders. De afgelopen jaren heeft Defensie geïnvesteerd in haar cybercapaciteiten en dat blijft Defensie de komende jaren doen. Deze herziene cyberstrategie scherpt de cybertaken van Defensie aan en geeft op basis daarvan richting aan de wijze waarop Defensie haar cybercapaciteiten moet, wil en kan inzetten in de huidige omstandigheden.

Ten eerste betekent dat een permanente proactieve cyberinzet om samen met andere departementen weerstand te bieden aan de aanhoudende cyberaanvallen onder de grens van gewapend conflict. Ten tweede worden de cybercapaciteiten dichter bij elkaar georganiseerd en eenduidiger aangestuurd, zodat de krijgsmacht slagvaardig in het cyberdomein kan optreden. Tot slot streeft Defensie naar zo veel mogelijk synergie op cybergebied door samen te werken met overheden, private partijen en bondgenoten.

Om dat te realiseren blijft Defensie investeren in haar cyberpersoneel en de samenwerking zoeken met andere departementen, private partijen, kennisinstellingen en bondgenoten. Alleen zo kan Defensie innovatief blijven, de cyberweerbaarheid van Nederland en haar bondgenoten vergroten en cyber als het nieuwe front het hoofd bieden. De technologische ontwikkelingen en steeds verdere digitalisering van de wereld zullen ook in de toekomst steeds om nieuwe investeringen blijven vragen om ons te wapenen tegen digitale dreigingen.



Bijlagen

Bijlage 1: Begrippenlijst

Deze bijlage beschrijft wat de belangrijkste begrippen in deze strategie betekenen. De definities zijn ontleend aan gangbare standaarden, maar zo geformuleerd dat de betekenis in de context van deze strategie en hun onderlinge relatie duidelijk is. Wanneer een definitie verwijst naar een ander begrip in de lijst, dan is dit aangegeven met →.

Actor Actor	Een persoon of partij die activiteiten ontplooit om een politiek, militair of crimineel doel te bereiken.
Commandovoering Command & Control (C2)	Hoofdfunctie van militair optreden om de krijgsmacht te leiden en te besturen teneinde de opgedragen doelen te bereiken door de effectieve en efficiënte inzet van →militaire capaciteiten.
Communicatie- en Informatiesysteem (CIS) Communication & Information System	Concrete toepassing van informatie- en communicatietechnologie (ICT) voor het verzenden, opslaan en verwerken van gegevens ten behoeve van de →informatievoorziening.
Contra-inlichtingen (CI) Counterintelligence	Het onderkennen en tegengaan van veiligheidsdreigingen op het gebied van spionage, sabotage en ondermijning.
Cyberaanval Cyber Attack	1. Een →cyberactiviteit om een systeem digitaal binnen te dringen of van buitenaf te manipuleren. 2. Een type militaire →cyberoperatie om een →systeem te degraderen, verstoren of vernietigen dan wel de daarin aanwezige gegevens te manipuleren of exfiltreren.
Cyberactiviteit Cyber Activity	Handeling van een →actor in →cyberspace met als doel op, of door middel van, een of meer systemen een effect te bereiken.
Cyberactor Cyber Actor	Een persona of partij die activiteiten in →cyberspace ontplooit met een politiek, militair of crimineel doel.
Cybercapaciteit Cyber Capability	Het vermogen om in →cyberspace een effect te bereiken.
Cyberdomein Cyber Domain	→Cyberspace als een van de vijf →operationele domeinen waarin de krijgsmacht opereert, naast land, zee, lucht en ruimte.
Cyberdreiging Cyber Threat	Het risico dat →cyberactiviteiten van een →cyberactor vanwege een kwetsbaarheid in een systeem negatieve effecten kunnen hebben.
Cyberdreigingsinformatie Cyber Threat Intelligence (CTI)	Gegevens die nodig zijn om specifieke →cyberdreigingen te onderkennen.
Cybergereedheid Cyber Readiness (Index)	De mate van →cyberweerbaarheid van een militaire eenheid of ander organisatiedeel van Defensie.
Cyberincident Cyber Incident	Een →cyberaanval of een andere inbreuk op de →cyberveiligheid.
Cybermiddel Cyber Means	Een systeem om →cyberactiviteiten mee uit te voeren.
Cyberoperatie Cyber Operation	Gecoördineerd geheel van activiteiten om een of meer effecten te bereiken in of vanuit het →cyberdomein, in de vorm van een →militaire operatie, →inlichtingenoperatie of rechtshandhaving.
Cyberomgevingsbeeld Recognized Cyber Picture	Continu omgevingsbeeld van het →cyberdomein, inclusief de detectie, identificatie en monitoring van →cyberactoren en →cyberactiviteiten ten behoeve van de planning en uitvoering van operaties en deconflicte van →cyberactiviteiten.
Cyberspace Cyberspace	1. het totaal van het elektromagnetisch spectrum wordt gebruikt voor de digitale verwerking, opslag en verzending van gegevens; 2. het totaal van alle losstaande en verbonden communicatie- en informatie-technologie en andere elektronische systemen met de daarin aanwezige gegevens.
Cyberveiligheid Cyber Security	De mate waarin een systeem effectief is beschermd tegen interne en externe →cyberdreigingen.
Cyberweerbaarheid Cyber Resilience	De →cyberveiligheid van systemen en het vermogen om →cyberincidenten en de effecten daarvan te mitigeren.
Cyber- and Electromagnetic Activities (CEMA)	Samenhangende →cyberactiviteiten en →elektromagnetische activiteiten.
Defensie Ministry of Defence	Het ministerie dat de krijgsmacht beheert en inzet, alsmede daaraan ondersteunende activiteiten uitvoert.
Elektromagnetische Activiteiten Electromagnetic Activities	Handeling van een →actor in het elektromagnetisch spectrum met als doel een effect op een of meer systemen te bereiken.
Informatieoperatie Information Operation	Een operatie gericht op het beïnvloeden van de informatiepositie van een →actor dan wel het verbeteren en beschermen van de eigen informatiepositie.
Informatievoorziening Information Services	De functie om relevante en accurate informatie op ieder gewenst niveau tijdig beschikbaar te maken voor besluitvorming en taakuitvoering.
Inlichtingenoperatie Intelligence Operation	Een (cyber)operatie uitgevoerd door een inlichtingen- of veiligheidsdienst om inlichtingen te vergaren of →contra-inlichtingenactiviteiten uit te voeren.
Militaire (cyber)operatie Military (Cyber) Operation	Een operatie uitgevoerd door de krijgsmacht (in het →cyberdomein).
Operationeel domein Operational Domain	Manoeuvrerruimte waarin of van waaruit militaire effecten kunnen worden gerealiseerd, te weten land, zee, lucht, ruimte en →cyberspace.
Operationele omgeving Operational Environment	Het geheel van fysieke, informationele en sociaal-culturele factoren die van invloed zijn op een (cyber) operatie.
Post-kwantum cryptografie Post-quantum Cryptography	Cryptografie die is ontworpen om niet gebroken te kunnen worden met een kwantumcomputer.
Sensor-, wapen- en commandosystemen Sensor, Weapon and C2 Systems	De concrete toepassing van operationele technologie (OT) voor detectie, geweldsuitoefening en commandovoering.

Bijlage 2: Doctrinaire en bestuurlijke uitgangspunten

Deze bijlage met doctrinaire uitgangspunten schetst het conceptuele kader voor militair optreden in het cyberdomein in de Nederlandse bestuurlijke context. Het vormt de conceptuele uitgangspunten voor de Defensie Cyberstrategie.

Kenmerken van het Cyberdomein

Het cyberdomein (ook wel cyberspace) is het wereldwijde totaal van alle losstaande en verbonden communicatie- en informatie-technologie en andere elektronische systemen en netwerken met de daarin aanwezige gegevens, die gegevens verwerken, opslaan of versturen.⁵ Het omvat dus alle digitale systemen en verbindingen ertussen, inclusief alle hardware, software en data.

Het cyberdomein onderscheidt zich van de andere domeinen doordat het volledig door de mens is gecreëerd en de eigenschappen steeds veranderen. Cyberspace bestaat uit fysieke en niet-fysieke elementen. Het is afhankelijk van fysieke infrastructuur op land (zendmasten, routers, datacentra, radars), de zee (onderzeese kabels, sensoren op schepen), in de lucht (sensoren in vliegtuigen en drones) of in de ruimte (observatie-, navigatie- en communicatiesatellieten). Software maakt logische communicatie en gegevensverwerking op de fysieke infrastructuur mogelijk (netwerkprotocollen, firmware, besturingssystemen, databases, toepassingen, mobiele apps). Dat stelt mensen in staat virtuele identiteiten te creëren (gebruikersnamen, profielen, telefoonnummers, mailadressen), informatie te verzamelen, te bewerken en uit te wisselen (bestanden, e-mail, webpagina's, sociale media) en zo sociale netwerken op te bouwen. Ook systemen beïnvloeden de sociale netwerken (geautomatiseerde transacties, advertenties, contentsselectie, chatbots); virtuele entiteiten sorteren dus effecten in de reële wereld.

Cyberspace heeft geen gedefinieerde geografische grenzen en strekt zich virtueel uit over de fysieke grenzen van de andere domeinen. Cyberspace kan worden benaderd vanuit alle andere domeinen en kan omgekeerd zelf alle andere domeinen benaderen. Naast tijd-ruimte-factoren, wijkt het cyberdomein af van de overige domeinen doordat het volledig door de mens is gecreëerd en het in stand wordt gehouden door fysieke, kunstmatige componenten. Hierdoor is het mogelijk om, meer dan in de andere domeinen, het domein zelf te manipuleren. Daarnaast beïnvloedt cyber de mens en zijn sociale omgeving.

De voortdurende technologische ontwikkeling, in het bijzonder de opkomst van kunstmatige intelligentie en de koppeling van mens met machine, zal de interactie van de mens door en met cyber intensiever maken.

Cyberspace wordt naast land, zee, lucht en ruimte beschouwd als een operationeel domein, omdat er in en vanuit cyberspace fysieke, virtuele en cognitieve effecten kunnen worden bereikt die tactische, operationele en strategische militaire doelen kunnen dienen. Tegelijk kunnen militaire activiteiten in een domein ook samenhangen met militaire activiteiten in een ander domein en met andere machtsmiddelen die een staat inzet, zoals diplomatie of rechtshandhaving. Cyberoperaties kunnen bijvoorbeeld ondersteunend zijn aan (digitale) informatieoperaties die weer integraal onderdeel uitmaken van een militaire campagne op het land, of kunnen bijdragen aan het vastleggen van oorlogsmisdaden. Activiteiten in het cyberdomein zijn op tactisch niveau vaak niet los te zien van activiteiten in het elektromagnetisch spectrum.

De informatieomgeving en het cyberdomein kennen een andere snelheid en dynamiek dan de fysieke domeinen. Cyberoperaties zijn altijd contextspecifiek en hebben daardoor vaak lange aanlooptijden. Dit maakt tijdige inlichtingen en manoeuvre in cyberspace noodzakelijk. Potentiële tegenstanders met een hybride doctrine maken bovendien geen hard onderscheid tussen vreedstijd en conflict; zij gebruiken de informatie-omgeving op dit moment al voor beïnvloeding. Daarom is het militair-strategisch van essentieel belang om reeds voordat sprake is van een feitelijk conflict, onszelf in de informatie-omgeving en het cyberdomein in een goede uitgangspositie te manoeuvreren en handelingsopties voor te bereiden

Cyberorganisatie

Kerndepartement

Het ministerie van Defensie is, zoals alle ministeries, ingesteld op basis van artikel 44 van de grondwet. Het kerndepartement is een van de zeven Defensieonderdelen, te weten de Bestuursstaf. Hierin zijn de politieke leiding, de ambtelijke leiding en de militaire leiding georganiseerd. **Voor de cybertaken zijn de volgende organisatie-elementen van de Bestuursstaf van belang:**

- Het **Directoraat-Generaal Beleid** (DGB) is verantwoordelijk voor integraal en uitvoerbaar beleid. Daaronder valt het strategisch cyberbeleid en de interdepartementale en internationale beleidsafstemming (Directie Strategie en Kennis, DSK), de integrale planning en begroting van cybercapaciteiten in het kader van krijgsmachtontwikkeling (Directie Operationeel Beleid en Plannen, DOBP), de politieke besluitvorming voor cyberinzet (Directie Internationale Aangelegenheden, DIA), en de beveiligingsautoriteit voor integrale beveiliging, waaronder informatiebeveiliging (Directie Bedrijfsvoering en Evaluatie, DBE).
- De **Chief Information Office** (CIO) is verantwoordelijk voor het ontwikkelen en bijhouden van beleid en kaders voor de cyberveiligheid van defensiesystemen en -netwerken. Ook het zorgdragen voor voldoende aandacht binnen de organisatie voor digitale weerbaarheid, beheer en verbetering van de IT-, data-infrastructuur inclusief de benodigde technologische vernieuwing, is de verantwoordelijkheid van de CIO. Ter invulling van deze verantwoordelijkheden werkt de CIO nauw samen met partners in interdepartementaal en internationaal verband.
- De **Defensiestaf** (DS) is de staf van de Commandant de Strijdkrachten (CDS) en gaat over de opbouw van cybercapaciteiten en integratie met andere capaciteiten (Directie Plannen, DPLAN), aansturing van de operationele gereedheid van cybercapaciteiten (Directie Aansturen Operationele Gereedheid, DAOG).
- De **Militaire Inlichtingen- en Veiligheidsdienst** (MIVD) maakt als bijzondere organisatie-eenheid administratief onderdeel uit van de Bestuursstaf. Vanuit hun organieke taak gebruiken zij het cyberdomein om inlichtingenoperaties uit te voeren; tegelijk leveren zij inlichtingen over het handelen van actoren in het cyberdomein en kunnen ze maatregelen nemen om malafide activiteiten tegen te gaan.

Krijgsmacht

De krijgsmacht is het militaire apparaat van het Koninkrijk dat zijn bestaan en taken ontleent aan artikel 97 van de Grondwet. De krijgsmacht bestaat de jure uit het geheel van alle militairen, waarbij een militair is ingedeeld bij één van de vier krijgsmachtdelen (niet te verwarren met de operationele commando's, zie onder), te weten de Koninklijke Landmacht, Koninklijke Marine, Koninklijke Luchtmacht of de Koninklijke Marechaussee. De krijgsmacht wordt aangestuurd door de CDS, ondersteund door de Defensiestaf.

Het **Netherlands Joint Force Command** (NLD JFC) is namens de CDS belast met de integrale planning en aansturing van alle militaire inzet. Het **Defensie Cybercommando** (DCC) staat, net als het **Netherlands Special Operations Command** (NLD SOCOM), als joint militaire eenheid ook onderdeel van de krijgsmacht, direct onder bevel van de CDS. Het DCC heeft tot taak militaire cybercapaciteiten gereed te stellen, militaire cyberoperaties aan te sturen en uit te voeren. Het dient enerzijds als cyberstafelement voor de CDS maar stelt anderzijds ook militaire cybercapaciteiten gereed en beschikbaar voor inzet.

De Defensieonderdelen waarin de krijgsmachtdelen op dit moment de facto zijn georganiseerd worden gezamenlijk aangeduid als de Operationele Commando's. De Commando's **Landstrijdkrachten**, **Zee­strijdkrachten** en **Luchtstrijdkrachten** beschikken voor hun taakuitvoering over cyberelementen, waaronder:

- Militaire eenheden met middelen om cyber- en elektromagnetische effecten te creëren of effecten door tegenstanders te mitigeren;
- *Security Operation Centres* (SOCs) voor de cybersecuritymonitoring van de eigen Communicatie- en Informatiesystemen (CIS) en Sensor- Wapen- en Commandovoeringssystemen (SEWACO).

Het commando **Koninklijke Marechaussee** beschikt over cybercapaciteiten voor hun rechtshandavingstaken. Ze hebben de capaciteiten om forensisch onderzoek te doen aan digitale apparatuur, maar ook om cyberoperaties uit te voeren ter bestrijding van criminaliteit. Daarnaast beschikken ze over een data science afdeling die bijdraagt aan effectieve en efficiënte criminaliteitsbestrijding.

5 AJP 3.20 Allied Joint Doctrine for Cyberspace Operations

Ondersteunende diensten

Veel logistieke functies die voorheen geïntegreerd onderdeel van de krijgsmacht(delen) waren, zijn in de afgelopen decennia gecentraliseerd en bedrijfsmatig ingericht als ondersteunende diensten. Deze ondersteunende diensten zijn ondergebracht in twee Defensieonderdelen: het Defensie Ondersteuningscommando (DOSCO) en het Commando Materieel en IT (COMMIT).

Onderdeel van COMMIT is het **Joint Informatie-voorzieningscommando** (JIVC), het “IT-bedrijf” van Defensie. Het levert, beheert en opereert communicatie- en informatiesystemen voor heel Defensie. Daarmee is JIVC verantwoordelijk voor een groot deel van de cybersecurity van Defensie. Het **Defensie Cybersecurity Centrum** (DCSC) is zowel het SOC van JIVC als de ondersteuner van andere Defensieonderdelen voor detectie van en respons op malafide cyberactiviteiten, en voert penetratietesten en digitale forensische onderzoeken uit.

Cyberactiviteiten

Naast militaire cyberoperaties door de krijgsmacht, voert Defensie ook andere cyberactiviteiten uit, zoals cybersecurity, tactische cyber- en elektromagnetische activiteiten, en inlichtingenoperaties. Al die verschillende cyberactiviteiten omvatten deels dezelfde technische handelingen, maar dienen een ander doel, de context en interacties verschillen, en er gelden doorgaans andere juridische kaders.

Militaire Cyberoperaties

De regering kan de krijgsmacht als militair machtsmiddel inzetten om anderen te dwingen iets te doen of te laten, zowel door de dreiging met of met de toepassing van dwang of geweld. Het militaire machtsmiddel wordt altijd gebruikt in combinatie met diplomatieke, informationele en economische machtsmiddelen. Militaire inzet vindt plaats in een of meer van de vijf domeinen zee, land, lucht, ruimte en cyber om fysieke, virtuele en cognitieve effecten te bereiken, die een tegenstander dwingen om zijn handelen aan te passen.

Militaire cyberoperaties zijn een unieke krijgsmachtaak, gebonden aan inzetmandaat, die alle defensieve, offensieve of voorwaardenscheppende militaire inzet in het cyberdomein omvatten, inclusief de inlichtingen-functie, als onderdeel van joint, multidomein optreden op alle niveaus (strategisch, operationeel, tactisch).

Hieronder zijn de zes soorten cyberoperaties die de Nederlandse cyberdoctrine onderscheidt schematisch weergegeven, met daarbij de twee soorten die de NAVO-doctrine onderkent. Daarboven zijn de hoofdfuncties van militair optreden weergegeven, en onderaan de cybersecurity die altijd moet zijn gewaarborgd.

Defensieve cyberoperaties zijn gericht op het behouden van eigen vrijheid van handelen in het cyberdomein, bijvoorbeeld door aanvallen te isoleren, neutraliseren en mitigeren.

Offensieve cyberoperaties zijn bedoeld om militaire effecten te bereiken. Dat kan zijn om iets fysiek uit te schakelen, maar ook om een tegenstander de beschikbaarheid van een systeem te ontzeggen. Daarnaast kunnen cyberoperaties systemen en data (onopgemerkt) manipuleren, of informatie uit systemen van een tegenstander onttrekken.

Cybersecurity

Iedere organisatie, dus ook Defensie, moet zijn eigen digitale systemen veilig houden. Dat omvat onder meer het continue bijwerken van software, inrichten en beheren van firewalls, maken van back-ups, afhandelen van beveiligingsincidenten, audits van toegangscontrole, detecteren van ongebruikelijk netwerkverkeer, etc. Dergelijke werkzaamheden zijn op zich geen militaire activiteiten, en zijn voor een belangrijk deel binnen Defensie ook civiel gereorganiseerd en belegd bij ondersteunende diensten. Tegelijk moet de krijgsmacht deze activiteiten als onderdeel van de zelfbeschermingsfunctie wel geïntegreerd met andere militaire functies kunnen uitvoeren.

Tactische Cyber en Elektromagnetische Activiteiten

Cyberactiviteiten en elektromagnetische oorlogsvoering zijn niet hetzelfde, maar zeker op het tactisch niveau wel nauw verweven. Het verstoren van een radar of verbindingsmiddel is een vorm van elektronische oorlogsvoering, maar heeft effect in het cyberdomein omdat het de betrouwbaarheid en beschikbaarheid van informatie in digitale systemen beïnvloedt. Het uitpeilen van zenders op het gevechtsveld kan deels elektromagnetisch zijn, zoals het lokaliseren van een signaal, en deels cyber, zoals het identificeren van entiteiten op basis van digitale informatie in het signaal.

Inlichtingenoperaties

Waar militaire cyberoperaties zijn bedoeld om effecten te creëren die tegenstanders tot ander gedrag dwingen, richten inlichtingenoperaties zich op het achterhalen van het potentieel en de intenties van actoren, al dan niet op het gebied van cyber. In een defensiecontext zijn die actoren doorgaans andere staten en krijgsmachten. Landen met een offensief cyberprogramma maken echter gebruik van proxy’s, wat het onderscheid met criminelen en hacktivisten moeilijk maakt.

Inlichtingenoperaties kunnen gebruik maken van cyberspace om informatie over uiteenlopende, ook niet-cyber gerelateerde, aspecten te achterhalen. Inlichtingenoperaties kunnen een algemeen inlichtingendoel dienen, maar worden ook uitgevoerd ter ondersteuning van militaire operaties. Met name militaire cyberoperaties bestaan voor een wezenlijk deel uit een inlichtingencomponent.

Rechtshandhaving

Rechtshandhaving omvat alle overheidsactiviteiten die zijn gericht op controle op naleving van de wet en, indien nodig, ingrijpen bij overtreding of strafbare activiteiten, inclusief de toetsing van de rechtmatigheid van de inzet van een cybermiddel. Cyber kan in verschillende mate een rol spelen. Bij misdaad kan het cyberdomein ter ondersteuning worden gebruikt, bijvoorbeeld voor communicatie tussen criminelen. Maar cyber kan ook een prominentere rol spelen, bijvoorbeeld als oplichting of afpersing via het internet plaatsvindt. Tot slot kan de misdaad volledig digitaal plaatsvinden, zoals computervredebreuk of ransomware. In een militaire context kan cyber ook worden gebruikt voor de vaststelling van oorlogsmisdaden, zowel door onderzoek op internet als door forensisch onderzoek aan geconfisqueerde apparatuur.

Schematische weergave Militaire Cyberoperaties

Inlichtingen, Commandovoering, Manoeuvre, Vuurkracht, Logistiek, Informatievoorziening, Zelfbescherming, Civiel-Militaire Coördinatie					
Defensive Cyber Operations		Offensive Cyber Operations			
Cyber Defence	Defensive Counter Cyber	Offensive Counter Cyber	Cyber Surveillance & Reconnaissance	Cyber Support	Cyber Attack
Cyber Security					

Notities

Colofon

Dit is een uitgave van
Ministerie van Defensie

Documentnummer
MINDEF20250018099



Digitale slagkracht
voor de bescherming
van het Koninkrijk
en bondgenoten