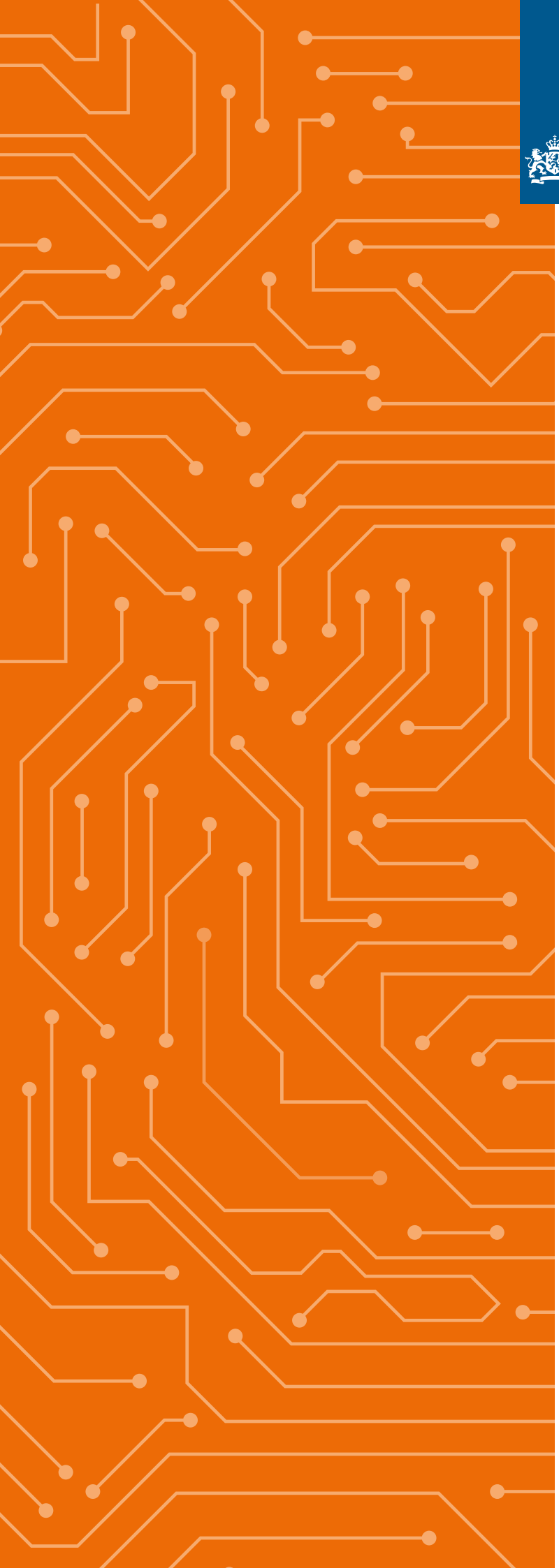
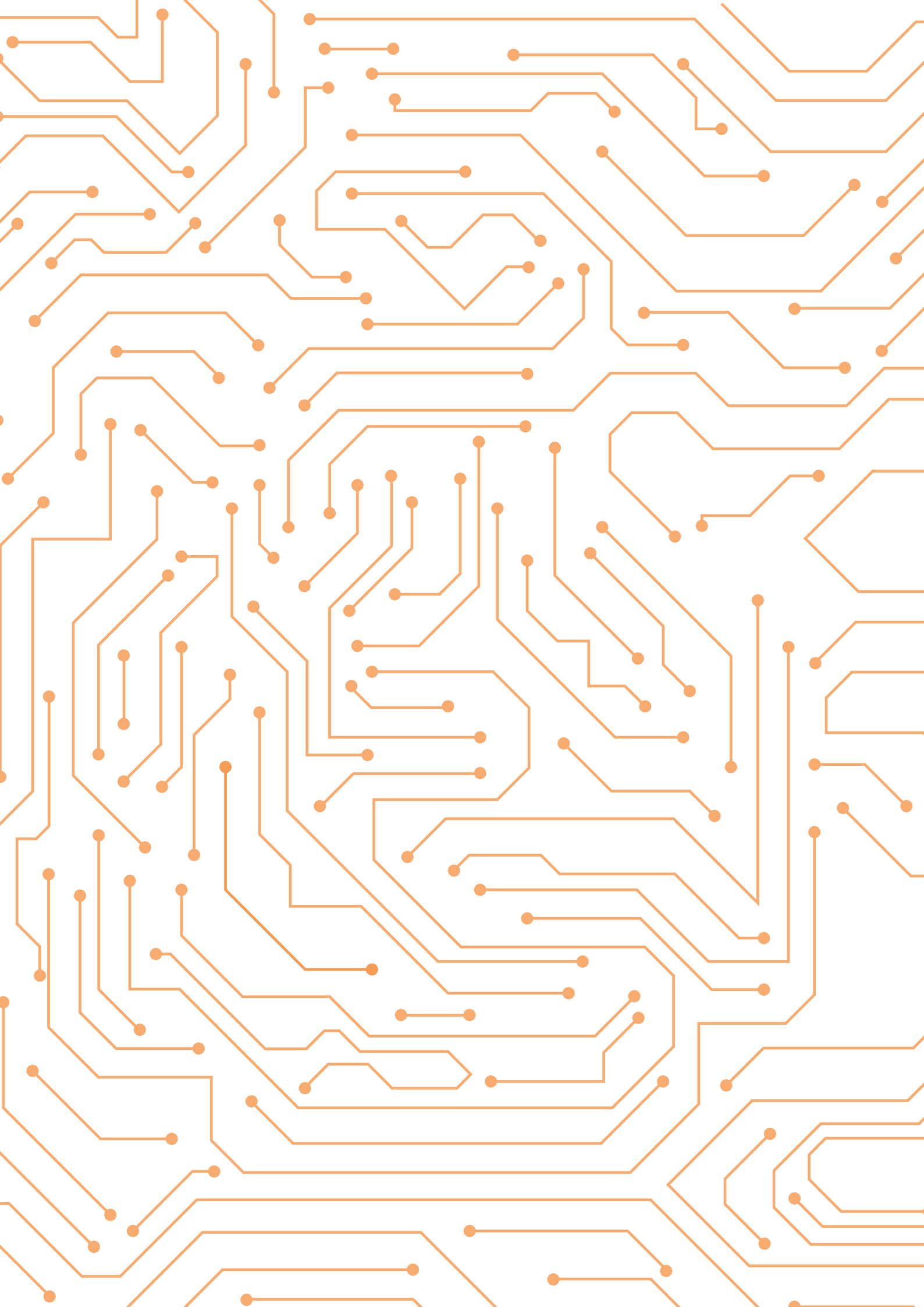


Ministerie van Defensie

Defensie Cyber Strategie 2018

Investeren in digitale slagkracht voor Nederland



Inhoudsopgave

Inleiding

Ons land moet op Defensie kunnen rekenen als het erop aankomt. Optreden tegen ernstige digitale bedreigingen van onze veiligheid, in nationaal en in internationaal verband, hoort daarbij.

Met de verslechtering van de internationale veiligheidssituatie en de verscherping van geopolitieke belangentegenstellingen is de bijdrage die Defensie aan onze digitale veiligheid levert des te belangrijker geworden. Het Cyber Security Beeld Nederland 2018 maakt duidelijk dat de grootste digitale bedreiging van onze nationale veiligheid uitgaat van staten. Dit heeft onmiskenbaar gevolgen voor de bijdrage die van Defensie wordt verwacht bij het tegengaan van die dreiging. Bovendien moet ons steeds meer gedigitaliseerde land zijn voorbereid op geavanceerde digitale dreigingen in het geval van een onverhoopt militair conflict. Defensie heeft hierin een verantwoordelijkheid te nemen, zowel in nationaal verband als in de NAVO.

Deze Defensie Cyber Strategie is opgesteld binnen de kaders van de Defensienota, de Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS) en de Nederlandse Cyber Security Agenda (NCSA) en draagt bij aan de uitvoering van deze strategieën. Zij bouwt voort op de basis die na het verschijnen van de eerste Defensie Cyber Strategie in 2012 is gelegd met de oprichting van het Defensie Cyber Commando (DCC) en de Joint Sigint Cyber Unit (JSCU) van de AIVD en de MIVD en de versterking van het Defensie Computer Emergency Response Team (DefCERT) en de Koninklijke Marechaussee. Er zijn sinds 2012 veel stappen gezet. Het is nu tijd om te versnellen en te verbinden.
De cyberintensivering uit het regeerakkoord, oplopend tot 20 miljoen euro structureel vanaf 2021, maakt dit mogelijk.

Aan de hand van deze strategie investeert Defensie in cybercapaciteiten om:

- Te allen tijde de baas te zijn van haar eigen IT en wapensystemen en haar digitale weerbaarheid te verzekeren. Dit blijft de komende jaren een belangrijk aandachtspunt;
- Nog beter te weten wie onze nationale veiligheid in het digitale domein bedreigen. De MIVD vervult hierin samen met de AIVD een onmisbare rol;
- Over meer mogelijkheden te beschikken om digitale aanvallen te verstoren of af te schrikken;
- Samen met civiele partners de veiligheid van Nederland en van onze vitale infrastructuur en processen te waarborgen in het geval van een onverhoopt militair conflict waarbij digitale aanvalsmiddelen worden ingezet;
- Digitale middelen doelgericht in te zetten om in het kader van militaire operaties het overwicht te verkrijgen en te behouden

Digitale slagkracht voor Nederland is een ambitieus doel. Maar het is een noodzakelijke ambitie, gelet op de hoofdtaken van Defensie op het gebied van de bescherming van het eigen en NAVO-grondgebied, het bevorderen van de internationale rechtsorde en het ondersteunen van de civiele autoriteiten.

Hoofdstuk I

De bijdrage van Defensie aan de digitale veiligheid van Nederland en de NAVO

Statelijke actoren en criminele groeperingen opereren steeds minder terughoudend in het digitale domein. Cyberaanvallen en -incidenten zijn aan de orde van de dag. Ze zijn niet langer uitsluitend als op zichzelf staand te beschouwen. Steeds vaker is sprake van met elkaar samenhangende incidenten, die tezamen een campagne vormen van statelijke actoren en hun proxies, bedoeld om het economische verdienmodel, de vitale infrastructuur, de militaire capaciteiten of de democratische orde van landen te ondermijnen. Er moet ook rekening mee worden gehouden dat bepaalde staten doelgericht malware plaatsen in industriële controlesystemen in vitale sectoren ter voorbereiding op een eventueel militair conflict. Het gaat hier om activiteiten of operaties die erop zijn gericht de voorwaarden te creëren voor een militaire operatie (shaping the battlefield). Defensie heeft een verantwoordelijkheid om hiertegen, in nauw overleg met civiele partners, op te treden. Duidelijk is hoe dan ook dat als een (onmiddellijke dreigende) cyberaanval een dusdanige omvang aanneemt dat deze kan worden gezien als een (onmiddellijke dreigende) gewapende aanval, iedere staat op basis van het internationaal gewoonterecht en artikel 51 van het VN Handvest, het recht heeft zich te verdedigen.

Een goede verdediging en beveiliging zijn niet voldoende om kwaadwillenden ervan te weerhouden digitale aanvallen uit te voeren. Steeds meer bondgenoten nemen in het digitale domein daarom een actievere houding aan (active defense). In het kader van zowel de eerste als de derde hoofdtaak is een actievere bijdrage van Defensie binnen de bestaande structuren noodzakelijk. Ter versterking van deze bijdrage investeert Defensie de komende jaren in de volgende capaciteiten en concepten:

1. Inlichtingen: handelingsvermogen en attributie
2. Bijdragen aan afschrikking door militair vermogen in het digitale domein
3. Digitale weerbaarheid en bescherming eigen netwerken en systemen
4. Onderzoek naar nationale terugvalmogelijkheden
5. Militaire bijstand en steunverlening aan civiele autoriteiten
6. Rechtshandhaving (Koninklijke Marechaussee)

1 Inlichtingen

Handelingsvermogen:

Het overgrote deel van de digitale aanvallen kan worden afgeslagen door de IT- of CERT-organisatie van de getroffen partij. Om de heimelijke, persistente digitale aanvallen van statelijke actoren (Advanced Persistent Threats, APT's) tegen te gaan is echter ook (contra-)inlichtingen onderzoek nodig. Dit onderzoek levert unieke inlichtingen op, waarmee effectieve defensieve maatregelen genomen kunnen worden. De MIVD stelt inlichtingen over dreigingen in het cyberdomein ter beschikking aan relevante actoren binnen en buiten Defensie, die op basis daarvan maatregelen kunnen nemen, zoals het DefCERT, het Openbaar Ministerie, het Nationaal Cyber Security Centre (NCSC), en bedrijven. Om digitale spionage of sabotage te detecteren kunnen door de MIVD en AIVD verworven technische kenmerken van cyberaanvallen in het Nationaal Detectie Netwerk (NDN) worden ingezet. Het NDN is een samenwerkingsverband dat als doel heeft digitale dreigingen tegen vitale sectoren en de rijksoverheid beter en sneller waar te nemen, zodat schade kan worden voorkomen of beperkt. De bijdrage van de MIVD aan het NDN zal worden uitgebreid. Er zullen nieuwe verdedigingsinstrumenten worden ingezet waarmee een actieve verdediging tegen digitale aanvallen kan worden ontwikkeld. Daarnaast wordt het aantal sensoren uitgebreid, om digitale aanvallen beter en sneller te kunnen detecteren en onderzoeken en effectief op te kunnen (laten) treden tegen de dreiging. Naast deelname aan het NDN zal de MIVD, zoals aangekondigd in de NCSA, eveneens deelnemen aan het samenwerkingsplatform met NCSC, AIVD en Politie om op een gezamenlijke locatie snel relevante (technische) informatie over cyberdreigingen kunnen delen. Inlichtingen staan daarnaast aan de basis van het militaire vermogen in het cyberdomein. Offensieve cybercapaciteiten bouwen voort op de inlichtingenpositie. Op basis van inlichtingen van de MIVD kan het Defensie Cyber Commando de militaire capaciteiten vormgeven. Tot slot kan de MIVD binnen de kaders van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) op basis van inlichtingen ook zélf in actie komen om acute dreigingen in het digitale domein te verstoren.

Attributie

De toenemende cyberdreiging vraagt om een krachtige, internationale respons, gebaseerd op internationale afspraken. Dat gebeurt nog onvoldoende. Het kabinet wil vaker daders van cyberaanvallen (publiekelijk) aanspreken op hun gedrag. Dit vereist allereerst detectie en vervolgens, politieke en eventueel juridische, attributie. Het vaststellen wie de actor achter een cyberoperatie is (technische attributie) is daarvoor een onmisbare en complexe schakel die intensief onderzoek vergt. Door middel van hoogwaardig en kennisintensief inlichtingenonderzoek tracht de MIVD, in samenwerking met partners als AIVD en politie, de actor achter de cyberaanval en diens intenties te achterhalen, zodat het kabinet over kan gaan tot politieke attributie en gerichte tegenmaatregelen kan nemen. Een actief politiek attributiebeleid draagt bij aan het afschrikkend vermogen en het minder aantrekkelijk maken van Nederland als doelwit van cyberaanvallen. Een statelijke actor die (publiekelijk) wordt aangesproken op zijn daden, zal een andere afweging maken dan een aanvaller die in volledige anonimiteit kan opereren. Zo draagt Nederland bij aan het tegengaan van straffeloosheid in het digitale domein.

2. Bijdragen aan afschrikking door militair vermogen in het digitale domein

Afschrikking betekent dat een tegenstander afziet van (herhaling van) een aanval omdat hij ervan overtuigd is dat de kosten daarvan niet opwegen tegen de opbrengsten. Afschrikking is niet domeingebonden, met andere woorden: aanvallen vanuit een ander domein kunnen worden afgeschrikt met cybermiddelen, en omgekeerd kan afschrikking tegen cyberaanvallen ook uit de andere domeinen komen. De operationele capaciteiten van het Defensie Cyber Commando dragen bij aan het totale arsenaal van afschrikkingsmiddelen waarover de regering beschikt. Afschrikking maakt Nederland een minder aantrekkelijk doelwit voor (cyber-)aanvallen en is dus vóór alles een middel voor conflictpreventie. Naast het vermogen aanvallen te attribueren, vergt afschrikking geloofwaardige offensieve capaciteiten. Door integratie in (lopende) missies en operaties zal Defensie werken aan de zichtbaarheid en geloofwaardigheid van haar digitale militaire capaciteiten.

De NAVO is voor het kabinet de hoeksteen van het Nederlandse veiligheidsbeleid. Nederland heeft zich met andere bondgenoten sterk gemaakt voor bondgenootschappelijke erkenning van cyberspace als militair domein. Het bondgenootschap heeft deze erkenning gegeven tijdens de top van Warschau in 2016. Sindsdien is er hard gewerkt aan het operationaliseren van het digitale domein, bijvoorbeeld door het vormgeven van een mechanisme waarmee cybercapaciteiten in NAVO-missies en –operaties geïntegreerd kunnen worden. Dit zal een bijdrage leveren aan de collectieve verdedigings- en afschrikkingstaak. Nederland heeft zich tijdens de NAVO-top in Brussel in juli 2018 dan ook bereid verklaard met cybercapaciteiten bij te dragen aan bondgenootschappelijke missies en operaties.

3. Digitale weerbaarheid en bescherming eigen netwerken en systemen

Om een bijdrage te kunnen leveren aan de digitale veiligheid van Nederland en de veilige en effectieve inzet van de krijgsmacht te waarborgen, is het noodzakelijk dat de eigen digitale weerbaarheid van Defensie meegroeit met de dreiging. Inzet van Defensie is dan ook aangemerkt als vitaal proces binnen het stelsel van vitale infrastructuur. De IT-systemen van Defensie zijn volledig verweven met de bedrijfs- en commandovoering en met sensor- en wapensystemen. Defensie is voor haar functioneren afhankelijk van deze IT-systemen en de informatie die daarop beschikbaar is. Cyberaanvallen op IT-, sensor- wapen- en commandosystemen kunnen de inzetbaarheid en de doeltreffendheid van de krijgsmacht ondermijnen. Een hoog niveau van beveiligingsbewustzijn en een doeltreffende bescherming van systemen en netwerken vereisen daarom een blijvende inspanning. Preventieve maatregelen vormen de noodzakelijke basis van digitale weerbaarheid, het samenspel van bewustzijn, preventie, detectie en handelingsvermogen. Om de systemen van Defensie te beschermen, moeten deze maatregelen over de gehele breedte van de IT-keten worden geïmplementeerd, van software-ontwikkeling tot afscherming van netwerken. Dit stelt ook hoge eisen aan het personeel dat werkt aan het ontwerp, de beveiliging, het gebruik en de instandhouding van IT-systemen. De kennis van het personeel moet actueel zijn, en het personeel moet de beschikking hebben over de laatste technieken.

Alle betrokken defensieonderdelen dienen zich in te spannen om Defensie te vrijwaren van cyberdreigingen. De defensieve cyberketen bestaat uit meerdere lagen, verdeeld over de gehele defensieorganisatie. Cyber governance en –beleid geven richting, focus en kaders aan de inspanningen in het cyberdomein. Security by design betekent dat reeds bij het ontwerpen van IT-systemen wordt gezorgd voor het implementeren van veiligheidsmaatregelen. Security assessments analyseren en beoordelen systemen op restrisico's en compliancy en toezicht vinden plaats op naleving van beleid en regelgeving. Beveiliging en bewaking richt zich met name op de koppelingen tussen de netwerken van Defensie en de buitenwereld. Incident response zorgt voor mitigatie van cyberincidenten.

4. Onderzoek naar nationale terugvalmogelijkheden

Onderzocht zal worden welke Defensievoorzieningen in samenwerking met welke partijen kunnen worden ingezet om kritieke processen draaiende te houden wanneer er sprake is van maatschappij-ontwrichtende ICT-uitval als gevolg van een digitale aanval. Voorzieningen als het fysiek gescheiden en beveiligd glasvezelnetwerk van Defensie (het Netherlands Armed Forces Integrated Network, NAFIN) kunnen hierbij een rol spelen.

5. Militaire bijstand en steunverlening aan de civiele autoriteiten

Om bij te dragen aan de nationale veiligheid gaat Defensie de uitvoering van de derde hoofdtaak in het digitale domein versterken door een grotere bijdrage te leveren aan bestaande civiele structuren. Gezien de aard van de dreigingen richt Defensie zich daarbij met name op de vitale infrastructuur door intensievere samenwerking met de verantwoordelijke veiligheidspartners, met name het NCSC. Vraag en aanbod van cybercapaciteiten van Defensie worden in overleg met de civiele autoriteiten en betrokken publieke en private partners in kaart gebracht. Door in een vroeg stadium betrokken te zijn bij sectorspecifieke ontwikkelingen en dreigingen, zal Defensie in voorkomend geval effectiever over kunnen gaan tot het verlenen van bijstand en steun. Om dit te bereiken wil Defensie een grotere en concrete bijdrage leveren aan de bestaande civiele structuren op het gebied van informatiedeling en respons.

Informatiedeling

Information Sharing and Analysis Centres (ISAC's) zijn opgericht om een vertrouwde omgeving te creëren waarbinnen organisaties uit dezelfde sector op tactisch niveau informatie kunnen delen over (sectorspecifieke) cyberdreigingen, incidenten, ervaringen en mitigerende maatregelen, met als doel de digitale weerbaarheid te versterken. Deelnemers aan een ISAC hebben een spilfunctie binnen hun eigen organisatie op het gebied van informatiebeveiliging, ICT-security en –beleid. In de meeste ISAC's zijn het NCSC, de AIVD en de politie aangesloten. In de Airport ISAC is de Koninklijke Marechaussee een vaste partner. Het permanente netwerk dat een ISAC met zich meebrengt en de informatie die uitgewisseld wordt, vormen een belangrijke meerwaarde voor alle deelnemers. Door hun aard en samenstelling bieden ISAC's een ideaal platform om meer kennis op

te doen over sectorspecifieke cyberdreigingen en mogelijkheden van Defensie om zo nodig bij te dragen aan mitigerende maatregelen. Defensie zal in samenspraak met het NCSC en de leden van de ISAC's verkennen of betrokkenheid van Defensie bij de ISAC's kan worden geïntensiveerd.

Respons

Het Nationaal Response Netwerk (NRN) is een netwerk van CERT-organisaties, gecoördineerd door het NCSC, met als doel de technische respons op cybersecurityincidenten te versterken. Dit gebeurt door kennis, ervaring en personeel uit te wisselen. Zo wordt samenhang georganiseerd en worden bestaande capaciteiten versterkt. Naast het NCSC zijn de huidige NRN-partners ook DefCERT, Belastingdienst, Rijkswaterstaat, Surf, en de Informatie Beveiligingsdienst van de gemeenten. Defensie zal actief bijdragen aan het NRN en streven naar uitbreiding van het netwerk. Ook zal Defensie zich inzetten om het NRN te gebruiken als platform voor oefeningen met vitale sectoren en het NCSC. Gezamenlijke oefeningen zorgen ervoor dat organisaties bekend raken met elkaars procedures, belangen en werkwijzen en daardoor effectiever kunnen samenwerken indien zich daadwerkelijk een calamiteit voordoet.

6. Rechtshandhaving (Koninklijke Marechaussee)

Defensie heeft een beheersmatige verantwoordelijkheid bij de uitvoering van de politietaken van de Koninklijke Marechaussee. Ook de Koninklijke Marechaussee moet toegerust zijn op de toenemende cyberdreiging. Met name de digitalisering van grensprocessen en de toenemende digitale identiteitsfraude leveren risico's op. Risico's die zowel door een betere verdediging als door opsporing dienen te worden beheerst. Voor de uitvoering hiervan worden door de Koninklijke Marechaussee samenwerkingsverbanden met onder andere de politie en FIOD aangegaan.

Hoofdstuk II
Digitaal winnen in militaire operaties

In artikel 97 van de Grondwet staat dat er een krijgsmacht is, onder meer “ten behoeve van de handhaving en de bevordering van de internationale rechtsorde.” De verwijzing in dit artikel naar de internationale rechtsorde hangt nauw samen met artikel 90, dat bepaalt dat de regering de ontwikkeling van de internationale rechtsorde bevordert. Mede vanwege de toegenomen instabiliteit in landen aan de randen van Europa zal deze tweede hoofdtaak ook de komende periode veel van Defensie vragen. Door de ondermijning van de internationale rechtsorde komen ook de open en vrije internationale (handels)stromen in het geding. Het veilig houden van aanvoerroutes te land, ter zee, in de lucht en in het digitale domein is een belang van de internationale gemeenschap waarvoor het kabinet zich inzet. Nederland spant zich in ter bevordering van de internationale rechtsorde, conflictpreventie en stabilisatie. Dit doet Nederland mede door vanuit een geïntegreerde benadering deel te nemen aan militaire missies en operaties in bondgenootschappelijk verband.

Het digitale domein zal in elk toekomstig conflict een belangrijke rol spelen en het kabinet stelt vast dat voor een effectieve uitvoering van de tweede hoofdtaak van de krijgsmacht in het digitale domein, verdere ontwikkeling van cybercapaciteiten noodzakelijk is. Om meer overwicht te creëren in het digitale domein bij inzet van de krijgsmacht ten behoeve van de bevordering van de internationale rechtsorde, investeert Defensie de komende jaren verder in de volgende capaciteiten en concepten.

1. Oprichting samengestelde cyber mission teams

Als onderdeel van het militair vermogen kunnen cybercapaciteiten een bijdrage leveren aan militaire missies en operaties. Om militair optreden in het digitale domein mogelijk te maken, moet vroegtijdig diepgaande kennis beschikbaar zijn over kwetsbaarheden binnen systemen van potentiële tegenstanders. Vanuit haar wettelijke taken ondersteunt de MIVD het DCC met inlichtingen die noodzakelijk zijn voor een effectieve militaire inzet in het digitale domein. Omdat voor inlichtingenoperaties en militaire operaties in het digitale domein soortgelijke kennis en vaardigheden nodig zijn, worden naar internationaal voorbeeld cyber mission teams gevormd bestaande uit zowel MIVD-personeel als personeel van de krijgsmacht. De hiervoor aangewezen medewerkers opereren binnen de kaders van de Wiv en worden bij inzet van de krijgsmacht onder commando geplaatst van de Commandant der Strijdkrachten binnen het betreffende mandaat. Ook zullen indien nodig componenten vanuit het DefCERT en de operationele commando's aan deze teams worden toegevoegd. Om militaire inzet in het cyberdomein te kunnen toetsen op rechtmatigheid gaat de Koninklijke Marechaussee investeren in kennisopbouw op dit gebied.

2. Cybercapaciteiten als vast onderdeel in militaire planning

Het digitale aspect wordt in een vroeg stadium van de planningsfase van elke (potentiële) missie in beschouwing genomen. Dit komt tot uiting in (militaire) adviezen en analyses van de Directie Operaties en in daarop volgende (operatie)plannen. Wanneer de krijgsmacht daadwerkelijk wordt ingezet ter handhaving en bevordering van de internationale rechtsorde, is vervolgens artikel 100 van de Grondwet van toepassing op de informatieverstrekking aan de Staten-Generaal. Artikel 100 stelt dat de regering verplicht is de Staten-Generaal vooraf in te lichten over "de inzet of het ter beschikking stellen van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde." In de artikel-100 brieven zal voortaan een cyber-paragraaf worden opgenomen wanneer dat een relevant aspect is van de missie. Hierin wordt omschreven, binnen de grenzen van wat publiekelijk kan worden gedeeld, welke bijdrage militaire cybercapaciteiten leveren aan de missie of operatie in kwestie. Op deze wijze bevordert Defensie de bewustwording, binnen en buiten haar eigen organisatie, van het toenemend belang van het digitale domein als volwaardig domein van militair optreden.

Hoofdstuk III

Voorwaarden: personeel, kennisontwikkeling en innovatie en cryptografie

Deze strategie heeft de ontwikkelingen en prioriteiten geschetst die ertoe moeten leiden dat Defensie op termijn ook in het digitale domein haar drie hoofdtaken effectief kan uitvoeren. Dit zal niet mogelijk zijn zonder invulling te geven aan de voorwaarden die op al die maatregelen betrekking hebben: personeel, kennisontwikkeling en innovatie en cryptografie.

Personeel

Om in het digitale domein succesvol te zijn, is diepgaande kennis van het domein onontbeerlijk. Cyber- en IT-professionals beschikken over de benodigde kennis en ervaring. Vanwege de schaarste aan specialisten op de arbeidsmarkt is het niet vanzelfsprekend dat Defensie altijd over die kennis zal kunnen beschikken. Defensie onderzoekt de komende tijd mogelijke oplossingen voor het beter vinden, boeien en binden van cyberprofessionals, zowel militairen als burgers. Daarbij wordt aandacht besteed 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. Ook het benutten van uitwisselingsmogelijkheden binnen en buiten (inclusief marktpartijen) Defensie zorgt ervoor dat de kennis van cyberprofessionals actueel blijft, medewerkers meer tevreden zijn en het netwerk van cyberprofessionals wordt versterkt.
Om cyber- en IT-professionals mogelijkheden te bieden voor ontwikkeling binnen het domein zullen functies worden gecategoriseerd. Om binnen de overheid concurrentie te voorkomen en interoperabiliteit te bevorderen zet Defensie zich in voor uniforme functiebeschrijvingen en gelijkwaardige waarderingen voor cyber- en IT-professionals.

Kennisontwikkeling en innovatie

Kennisontwikkeling en innovatie op het gebied van cybersecurity is nodig om voor te blijven op tegenstanders en nieuwe digitale dreigingen het hoofd te kunnen bieden. Bovendien maakt een hoogwaardige, autonome kennispositie Defensie minder afhankelijk van cybersecurity-expertise en -oplossingen van anderen. In de NCSA is kennisontwikkeling dan ook genoemd als een van de zeven hoofdambities op het terrein van cybersecurity voor de komende jaren. Het gaat daarbij zowel om fundamenteel als toegepast cybersecurity-onderzoek. Dat betekent multidisciplinair onderzoek in de gehele kennisketen dat zowel naar oplossingen voor de langere als kortere termijn kijkt. Daarom is Defensie in 2018 ook lid geworden van het Dutch Cybersecurity Platform for Higher Education and Research (Dcypher). Dit platform zorgt onder andere voor agendering en coördinatie van cybersecurity-onderzoek en hoger onderwijs.

De recent verschenen derde editie van de Nationale Cybersecurity Research Agenda (NCSRA) is een belangrijk kader voor cybersecurity kennisontwikkeling in Nederland. Defensie heeft actief bijgedragen aan de totstandkoming van deze agenda. Defensie intensiveert vanaf 2019 de middelen voor onderzoek op het terrein van cyber. Van bijna 4 miljoen euro de afgelopen jaren zal Defensie met ingang van 2019 bijna 6,5 miljoen euro per jaar in cyberonderzoek investeren. Daar waar mogelijk wordt dat samen met andere departementen gedaan, zoals ook is aangekondigd in de Nederlandse Digitaliseringsstrategie.

Defensie voert samen met een aantal andere partijen een studie uit naar de opzet, vorm en organisatie van een in 2019 op te richten Cyber Innovation Hub, waarin departementen, onderzoeksinstellingen en bedrijven samen werken aan gezamenlijke en geprioriteerde veiligheidsvraagstukken op het gebied van cyber(security). Het doel van de Cyber Innovation Hub is cyberkennis en -kunde in Nederland te versterken, innovaties en experimenten te faciliteren en een ecosysteem van partners te bouwen, om zo bij te dragen aan het reduceren van cyberdreigingen.
In 2018 heeft het Digital Trust Center (DTC), onderdeel van het ministerie van Economische Zaken en Klimaat, een subsidie verstrekt aan de Stichting Nederlandse Industrie voor Defensie en Veiligheid (NIDV) voor de realisatie van een Nationaal Cyber Register voor ABDO-bedrijven en technologie- leveranciers. Het Register richt zich op het verbeteren van cyberweerbaarheid bij (toekomstige) ABDO-bedrijven waar met vertrouwelijke of staatsgeheimen informatie wordt gewerkt. Hierbij wordt nauw samengewerkt met de MIVD als steller en autorisatieverlener van de ABDO, maar ook met de AIVD, het NCSC en het DTC.

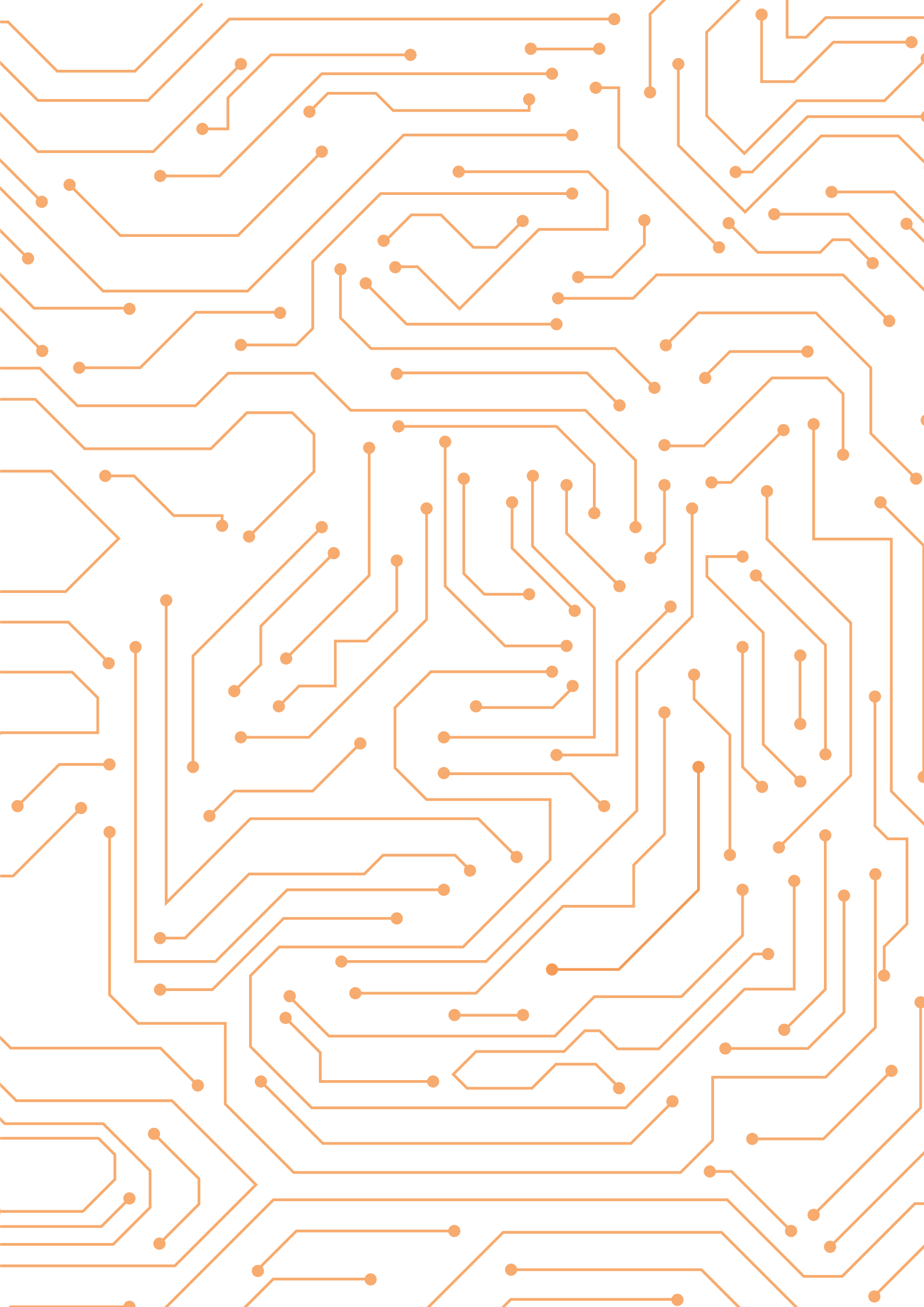
Cryptografie

Defensie maakt zowel in operationele als niet-operationele omstandigheden en zowel bij de reguliere kantoorautomatisering als bij sensor-, wapen- en commandovoeringssystemen, dagelijks gebruik van Hoog Gerubriceerde Informatie (HGI). Deze goed beveiligde HGI heeft niet alleen grote operationele belangen, het valt ook onder de Wet op de staatsgeheimen en moet voldoen aan onder andere het Voorschrift Informatiebeveiliging Rijk. Veilige opslag en verspreiding van deze informatie vereist hoogwaardige cryptografische producten. De ontwikkeling van nieuwe cryptografie staat niet stil, maar hetzelfde geldt voor de mogelijkheden voor het breken van codes. Dit betekent dat ook cryptografische producten gedurende hun levenscyclus moeten worden aangepast aan deze ontwikkelingen.

Het gebruik van cryptografische toepassingen om veilig met HGI te kunnen omgaan, vindt met name plaats binnen de Rijksoverheid, in een kleine markt waarin Defensie de grootste afnemer is. Defensie gaat een strategisch partnerschap aan met Fox-IT om ook op de lange termijn zekerheid te krijgen over de ontwikkeling en blijvende beschikbaarheid van cryptografische producten.

Tot slot

Defensie kan en zal niet over één nacht ijs gaan bij het investeren in digitale slagkracht voor Nederland. Stilstand is gezien het huidige cyber-dreigingsbeeld echter geen optie. Offensieve cybercapaciteiten ontwikkelen, digitale weerbaarheid vergroten en een solide inlichtingenpositie opbouwen, is boven alles mensenwerk, dat om blijvende inspanningen en investeringen vraagt. De deuren van de defensieorganisatie zullen hierbij waar mogelijk open moeten staan of gaan: we kunnen de dreigingen en uitdagingen die vanuit het digitale domein op ons af komen niet alleen aan. Met andere departementen, kennisinstellingen, bedrijven, de defensie- en veiligheidsindustrie en internationale partners kunnen we echter zorgen voor een digitaal veiliger Nederland. Ieder vanuit zijn eigen rol en expertise, maar met vereende krachten en een duidelijk gedeeld belang.



UITGAVE
Ministerie van Defensie
Herziene druk, november 2018
LAYOUT
MediaCentrum Defensie | Den Haag

TEKST
Ministerie van Defensie

FOTO'S
MediaCentrum Defensie | Den Haag

INTERNET
www.defensie.nl/materieelprojecten