Cybersecurity

A State-of-the-art Review: Phase 2

Samenvatting

Erik Silfversten, Victoria Jordan, Kevin Martin, Diana Dascalu, Erik Frinking

This publication presents the final report of a RAND Europe study commissioned by the WODC on behalf of the Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Samenvatting

De Nationale Coördinator voor Terrorismebestrijding en Veiligheid (NCTV) is een overheidsorganisatie die deel uitmaakt van het Nederlandse Ministerie van Justitie en Veiligheid. De NCTV beschermt Nederland tegen tegen bedreigingen die de maatschappij zouden kunnen ontwrichten en draagt zorg voor de veiligheid van vitale infrastructuur. Om die opdracht te vervullen bereidt de NCTV momenteel een onderzoeksagenda voor die beoogt de samenwerking met de wetenschappelijke gemeenschap te versterken, de wetenschappelijke discussie te bevorderen, en de NCTV en de wetenschappelijke gemeenschap op bepaalde blinde vlekken opmerkzaam te maken. Met het oog op de afbakening en het opstellen van deze onderzoeksagenda zijn drie zogenoemde *state-of-the-art* studies op gebied van terrorismebestrijding, crisisbeheer en cybersecurity uitgevoerd.

Dit rapport draagt bij aan het samenstellen van een algemeen overzicht van de *state-of-the-art* kennis op gebied van cybersecurity. In Fase 1 van deze studie was de opdracht om een *quick-scan* uit voeren van onderzoek op het gebied van cybersecurity en om te aan te stippen welke onderwerpen meer aandacht verdienden. In Fase 1 was het hoofddoel uit te maken welke huidige cybersecurity-onderwerpen verder moesten worden uitgediept in Fase 2.

We hebben vier thema's geïdentificeerd als de meest urgente en relevante onderwerpen voor de NCTV:

- Cybersecurity-governance vanuit het perspectief van de nationale veiligheid;
- Vertrouwen in informatie en data;
- De beveiliging van vitale infrastructuur; en
- Veiligheid van de supply chain.

Doelstellingen en methodologie

De NCTV heeft twee van deze vier thema's geselecteerd voor verder onderzoek in Fase 2, te weten:

- Cybersecurity-governance vanuit het perspectief van de nationale veiligheid; en
- De beveiliging van vitale infrastructuur.

De onderzoeksvragen voor de twee thema's zijn gebaseerd op een combinatie van het onderzoek in Fase 1 en de input van de NCTV. Beide thema's en de bijhorende onderzoeksvragen voor Fase 2 zijn opgesomd in de onderstaande tabel.

Tabel 0.1 Overzicht van onderzoeksvragen voor Fase 2

Onderwerp	Onderzoeksvragen
1. Cybersecurity-governance vanuit een nationale veiligheidsperspectief;	1.1 Hoe kunnen het huidige governance-model en de huidige initiatieven op het vlak van cybersecurity in Nederland op elkaar worden afgestemd en verbeterd?
	1.2 Hoe kan een systeem-verantwoordelijkheid voor cybersecurity gecreëerd worden?
	1.3 Welke lessen kunnen getrokken worden uit vergelijkingen met de nationale cybersecurityinitiatieven van andere landen?
	1.4 Hoe kan worden nagegaan welke kennis en vaardigheden nodig zijn voor nationale cybersecurity-governance?
	1.5 Hoe moeten efficiëntie en effectiviteit gemeten worden met betrekking tot de beleidsvorming op het gebied van cybersecurity?
2. Beveiliging van vitale infrastructuur	2.1 Welke risico's en uitdagingen zijn gebonden aan het samenspel tussen de oude vitale infrastructuur en nieuwe technologie?
	2.2 Hoe kan het huidige ontwikkelingsniveau van cybersecurity in de vitale infrastructuur sector gemeten en begrepen worden?
	2.3 Wat kan gedaan worden om de veiligheid van operationele technologie in vitale sectoren te verbeteren?
	2.4 Wat kan gedaan worden om te vermijden dat bepaalde individuen en georganiseerde groepen schade berokkenen aan de vitale infrastructuur?

Deze onderzoeksvragen vormen de basis voor de doelstellingen in Fase 2:

- Verder uitbouwen van de kennisontwikkeling met betrekking tot de onderzoeksvragen;
- De aandacht vestigen op onderwerpen die een diepgaander onderzoek vergen; en
- Gebieden identificeren waar de NCTV zou kunnen tussenkomen en aanbevelingen doen voor toekomstige verbetering.

De studie maakt gebruik van *mixed-methods*: een combinatie van literatuuronderzoek, casestudies, interviews en workshops met deskundigen.

Overzicht van de belangrijkste bevindingen vanuit het perspectief van nationale veiligheid

'Governance' is de combinatie van de benaderingswijzen van verschillende belanghebbenden om hun respons op een gezamenlijk probleem te identificeren, formuleren en coördineren. Dus een cybersecurity-governance-structuur vanuit het perspectief van nationale veiligheid is een combinatie van benaderingswijzen van verschillende belanghebbenden om hun proactieve en reactieve respons op cyber-risico's te identificeren, formuleren en coördineren.

Deze studie heeft onderzocht hoe de huidige cybersecurity-governance-structuur en initiatieven ter verbetering van deze structuur in Nederland afgestemd en verbeterd kunnen worden, en hoe een

verantwoordelijk systeem voor cybersecurity kan worden gecreëerd. De studie heeft aan het licht gebracht dat de huidige cybersecurity-governance-structuur een belangrijk discussieonderwerp is, en dat er verschillende initiatieven aan de gang zijn die de huidige situatie van cybersecurity-governance-structuur in Nederland onderzoeken en hoe die in de toekomst kan verbeterd worden.

Het huidige model cybersecurity-governance in Nederland kenmerkt zich door een op consensus gebaseerd 'poldermodel'. In de praktijk betekent dit dat de Nederlandse governance-structuur een netwerk-model volgt, waarbij meerdere organisaties samenwerken, en waar elke organisatie verantwoordelijk is voor cybersecurity binnen het eigen domein. Deze studie heeft een aantal uitdagingen geïdentificeerd vanuit het perspectief van nationale cybersecurity in Nederland:

- **Onduidelijke functies en verantwoordelijkheden binnen de structuur van cybersecurity-governance en gebrek aan soepelheid en proactiviteit in cybersecurity beleidsvorming.** De studie toont aan dat het gedecentraliseerd governance-model het moeilijk maakt om duidelijke algemeen geldende functies en verantwoordelijkheden vast te leggen. De studie toont ook aan dat middelen en inspanningen meer gericht zijn op crisisbeheer en reactieve respons, dan op een proactieve aanpak die de weerstand van de Nederlandse digitale maatschappij bevordert.
- **Uitdagingen in verband met informatie-uitwisseling.** Afdoende en productieve informatie-uitwisseling is essentieel voor de preventie- en reactie-fases in de respons op cybersecurity bedreigingen. Deze studie heeft twee domeinen van informatie-uitwisseling geïdentificeerd die voor verbetering vatbaar zijn: informatie-uitwisseling en kennis van de cybersecuritysituatie binnen de nationale regering, en informatie-uitwisseling tussen organisaties met verantwoordelijkheid op gebied van cybersecurity.
- **Uitdagingen die voortvloeien uit een gebrek aan of dubbel gebruik van regelgeving kunnen leiden tot een complexer governance-systeem.** De huidige governance-structuur kan leiden tot een gebrek aan samenhang in de regelgeving met soms tegenstrijdige vereisten die de inspanningen om de cybersecurity te bevorderen, kunnen ondermijnen. In deze context kan een meer proactief en afdwingbaar minimumniveau van cybersecuritynormen bijdragen tot de afstemming van de cybersecuritymethodes en de verschillende niveaus van cybersecurity in de diverse departementen en ministeries aanpakken.
- **Onderscheid tussen vitale en niet-vitale infrastructuur.** Dit onderscheid speelt een cruciale rol in de Nederlandse huidige cybersecurity-governance-structuur, waarbij de vitale infrastructuurdiensten onderworpen zijn bijkomende wetten en regels, verplicht zijn incidenten te melden en deel uitmaken van het Nationaal Cyber Security Centrum (NCSC) informatie-uitwisselingsstructuur. Het resultaat is dat niet-vitale diensten minder strenge veiligheidseisen hebben en daardoor mogelijk belangrijk veiligheidsadvies mislopen; zelfs als dit essentieel is voor de weerstand van de maatschappij of de nationale veiligheid.
- **Uitdagingen op het vlak van toezicht en evaluatie.** Deze studie toont aan dat er geen afdwingbare, overheidsbrede cybersecuritystandaard is en dat elke overheidsorganisatie haar eigen aanpak voor cybersecurity heeft. Bovendien is de rol van het NCSC voornamelijk adviserend. Dit maakt het moeilijk om cybersecurityregels af te dwingen, te evalueren, en te waarborgen voor alle deelnemers aan het Nederlands ecosysteem.

Deze studie heeft ook onderzocht welke lessen Nederland kan trekken uit de verschillende nationale cybersecurity-governance-structuren. Om deze vraag te beantwoorden heeft het onderzoeksteam casestudies uitgevoerd naar nationale governance-modellen in een vijftal landen: Estland, Duitsland, Zweden, het Verenigd Koninkrijk en de Verenigde Staten. Echter, deze internationale casestudies kunnen slechts in beperkte mate lessen opleveren voor het Nederlandse governance-systeem. Een casestudie-analyse kan illustreren hoe andere landen hun huidige cybersecurity-governance benaderen, maar kan geen volledig antwoord bieden op de vraag of en in welke mate ze succesrijk zijn binnen hun nationale structuren of in vergelijking met elkaar.

De governance van cybersecurityvaardigheden die nodig is voor nationale veiligheid

Deze studie heeft ook onderzocht hoe vaardigheden die nodig zijn voor de handhaving van de nationale cybersecurity kunnen worden geïdentificeerd en beheerd. De Nederlandse overheid legt veel nadruk op het belang van voldoende cybervaardigheden om de digitale veiligheid van het land te waarborgen, vooral op gebied van nationale veiligheid; in dit verband zijn reeds verschillende initiatieven in gang gezet. Deze studie identificeert drie algemene uitdagingen op het gebied van cybersecurityvaardigheden in het kader van nationale veiligheid:

- **De gedecentraliseerde verantwoordelijkheid voor personeelskwesties** die het moeilijker maakt om het cybersecuritypersoneel in de diverse overheidsorganisaties en –agentschappen te coördineren;
- **Het gebrek aan een algemeen aanvaarde taxonomie.** Er bestaat in Nederland geen algemene en gezamenlijke taxonomie van cybersecurityvaardigheden of beroepen. Dit bemoeilijkt het inschatten van de huidige vaardigheidssituatie en de mogelijke verbeteringen die daaraan zouden kunnen worden gemaakt.
- **Problemen in verband met werving en retentie**. Werving en retentie zijn bekende uitdagingen die vaak voorkomen in de cybersecurity-sector. Als gevolg van de competitieve arbeidsmarkt hebben overheidsorganisaties het moeilijk om cybersecurity-personeel te werven en toegang te hebben tot voldoende krachten met de vereiste vaardigheden op vlak van nationale veiligheid, voornamelijk binnen de organisatie zelf, maar ook via outsourcing en partnerschapscontracten met de commerciële cybersecurity-sector.

De studie identificeert verschillende benaderingswijzen en interventies om deze drie uitdagingen aan te pakken, onder andere:

- Een gemakkelijk toegankelijke kennisbank om een gemeenschappelijk begrip van cybersecurity te bevorderen;
- Personeelsstrategieën om de overheidsinspanningen op het gebied van cybersecurityvaardigheden af te stemmen;
- Competentiekaders en loopbaantrajecten om personeelsbeheer en ontwikkeling en instandhouding van vaardigheden te stroomlijnen;
- Analyse van opleidingsbehoeften om te bepalen welke vaardigheden op gebied van nationale veiligheid vereist zijn voor alle functies en belanghebbenden.

Evaluatie in het kader van de cybersecurity- beleidsvorming

Deze studie onderzoekt ook hoe effectiviteit en efficiëntie van nationale cybersecuritybeleid kan worden gemeten of geëvalueerd met het oog op betere informatiebeslissingen en beleidsvorming:

- Kaders om na te denken over welk bewijsmateriaal nodig is voor cybersecurity beleidsvorming.
- Benaderingswijzen die eerder werden gebruikt voor evaluatie in het cyberdomein.
- Benaderingswijzen van andere sectoren die kunnen gebruikt worden voor evaluatie in het cyberdomein.

De diverse benaderingswijzen hebben verschillende toepassingen, potentiële voordelen, en het is daarom nuttig om enkele fundamentele evaluatievragen te overwegen bij de beschouwing ervan (namelijk: *waarom* moeten we prestaties meten, *wat* moeten we meten, en *hoe* moeten we ze meten?). De tabel hieronder (Tabel 0.2) biedt een overzicht van de verschillende benaderingswijzen en waar ze de meeste waarde aanvoegen.

Tabel 0.2 Overzicht van verschillende evaluatiemethoden

Benaderingswijze of kader	**Nut en toegevoegde waarde**
Model voor beleidsvorming inzake cybersecurity	Het bewijsmateriaal gebruikt voor de bepaling van het cybersecuritybeleid beoordelen en verbeteren.
Post-incident analyse en analyse van getrokken lessen	De responsmechanismen inzake incidenten of aanvallen analyseren, beoordelen en verbeteren, ook op gebied van cybersecurity-governance, zowel binnen het algehele systeem als binnen de structuur van crisisbeheer of incidentrespons.
Zelfevaluatie van het niveau van cybersecurity	Het cybersecurityniveau van organisaties beoordelen en helpen verbeteren.
Programma-evaluatie	De impact van specifieke programma's of interventies binnen de nationale cybersecurity evalueren.
Prestatie-audits en "Value for Money"	De bredere prestatie-specifieke programma's of de algemene nationale aanpak van cybersecurity evalueren (met name de besparing, efficiëntie en effectiviteit.
Oefeningen en games	Minder gekende gebieden van cybersecurity onderzoeken en beter bewijsmateriaal ontwikkelen voor de beleidsvorming. Uitoefenen, testen en beoordelen van governance-structuren en -plannen, vooral met betrekking tot incidentrespons en crisisbeheer.
Met van de waarde van nationale cybersecurity	De algehele bijdrage en waarde van het nationale cybersecuritysysteem definiëren en meten.
Methoden voor besluitvorming onder "deep uncertainty"	Het toekomstig beleid en verbeteringen inzake nationale cybersecurity beoordelen en bijschaven.

Samenvatting van de belangrijkste bevindingen met betrekking tot vitale infrastructuur en beveiliging

Vitale infrastructuur omvat de elementen die noodzakelijk worden geacht voor het functioneren van de samenleving (bv. energiecentrales, watervoorzieningssystemen, vervoersinfrastructuur, democratische instellingen en overheidsprocessen, enz.). Recente ontwikkelingen zoals het aansluiten van bepaalde componenten van de vitale infrastructuur op het internet en de verrijking van de vitale infrastructuur met nieuwe en opkomende technologieën vormen nieuwe cybersecurity uitdagingen. Het heeft ook geleid tot veel recent onderzoek door regeringen die hun vitale infrastructuur willen beveiligen.

Vitale infrastructuur en technologie

Op het gebied van vitale infrastructuur en technologie hebben wij vooral de risico's en uitdagingen onderzocht die zijn gelieerd aan de wisselwerking tussen de traditionele vitale infrastructuur en nieuwe technologieën. Het onderzoeksteam concludeert dat Nederlandse deskundigen een goed inzicht hebben in de wisselwerking tussen traditionele en nieuwe technologieën, maar dat risico's en uitdagingen niet altijd op de correcte manier worden benaderd en beheerd. Deze risico's zijn verbonden aan:

- **Slijtage en veroudering** van een deel van de vitale activa, waardoor een risico bestaat op systeemfalen of misbruik. Deze uitdagingen moeten worden aangepakt door een beter begrip van de betrokken activa en van de wisselwerking tussen leveranciers en afnemers, bijvoorbeeld door asset management en duidelijk omschreven beveiligingsafspraken tussen leveranciers en afnemers.
- . De richtlijn betreffende de veiligheid van netwerken en informatie-systemen (NIS-richtlijn) ondervangt dit risico gedeeltelijk door het aanwijzen van essentiële aanbieders die afhankelijk zijn van ICT. Maar het is van belang om de risico's gebonden aan het cascade-effect beter in kaart te brengen.
- **De kloof tussen Operational Technology (OT) en Information Techology (IT)** blijft een obstakel voor het aanpakken van reeds geïdentificeerde risico's. Naarmate dit samenspel toeneemt, neemt ook de urgentie toe om deze kloof te overbruggen via onderwijs, bewustmaking, opleidingen en samenwerking tussen IT-experts en operationele technologieën.

Vitale infrastructuur en maturity van cybersecurity

In de studie identificeren wij verder hoe de huidige maturity niveaus van cybersecurity binnen de vitale infrastructuursector kunnen worden gemeten en begrepen. De studie identificeert verschillende benaderingswijzen en modellen die worden gebruikt om de cybersecurity maturity van vitale infrastructuur te beoordelen. We identificeren verder ook verschillende uitdagingen die verband houden met het bepalen van cybersecurity maturity:

- **De bestaande modellen voor de maturity-bepaling in de vitale infrastructuurbrengen verschillende uitdagingen met zich mee**, zoals bijvoorbeeld de moeilijkheid om bruikbare en meetbare indicatoren te definiëren en de constante evolutie op het gebied van cybersecurity, die een constante bijwerking van normen en modellen vereist.

- **De spanning tussen de maturity-bepaling op algemeen niveau en de meting op sectorniveau** wordt beschreven als een afweging tussen algemene toepasbaarheid en verdere toespitsing. Deskundigen suggereerden dat de overheid in dit verband sectorale aanbevelingen en richtlijnen zou moeten bieden.
- **Het debat over de voordelen van een juridische aanpak van het cybersecurity-niveau en de nadruk op een coöperatieve benadering suggereert** dat er een risico bestaat dat de maturity-bepaling van cybersecurity een 'checklist-oefening' wordt. Er is verder onderzoek nodig naar de motivering achter beoordelingen en de voordelen van regelgeving.
- **Het vermelden van de risico's verbonden aan de supply chain en onderlinge afhankelijkheden in maturity-beoordelingen** blijkt essentieel voor een nauwkeurige niveaubepaling van de cybersecurity en voor een beter en uitgebreider begrip van de risico's.

Vitale infrastructuur en het verbeteren van cybersecurity

In de studie identificeren wij tenslotte wat er kan worden gedaan om de beveiliging van operationele technologie in vitale sectoren te verbeteren en om te beschermen tegen mogelijke bedreigingen van actoren en georganiseerde groepen of netwerken van actoren. De studie identificeert de volgende actiepunten die essentieel zijn voor het verbeteren van de beveiliging van operationele technologie:

- **De beveiliging van vitale infrastructuur moet steunen op een geïntegreerde en veelzijdige aanpak,** die rekening houdt met zowel activa als hun omgeving. Een dergelijke aanpak kan voordeel halen uit toekomstige technologische ontwikkelingen zoals het beheer van de supply chain dat afhangt van hash-chain of cryptografische auditlogs, zero trust-architectuur, voorraadbeheer op basis van geautomatiseerde processen en kunstmatige intelligentie (AI), en zelfherstel.
- **Sectoroverschrijdende informatie-uitwisseling blijkt cruciaal voor het verbeteren van de veiligheid van de vitale infrastructuur in Nederland.** Dit werd geïdentificeerd als een gebied waar de overheid de rol van coördinator zou kunnen spelen om uitdagingen op het gebied van vertrouwen en vertrouwelijkheid te helpen overbruggen.
- **Veranderingen in organisatiestructuren,** vooral in de richting van multidisciplinaire teams, en een betere coördinatie tussen operatie-, beveiligings-, management en juridische teams kunnen bijdragen tot een verbetering van de beveiliging en leiden tot een beter begrip van bestaande risico's.

In de studie vinden wij niet veel bewijsmateriaal over de bescherming van vitale infrastructuur op gebied van bestaande dreigingen van actoren en georganiseerde groepen. Overleg met deskundigen leverde echter waardevolle inzichten op:

- **De huidige prioriteit moet liggen bij het aanpakken van acute dreigingen,** die misschien minder storend zijn dan Advanced Persistent Threats (APT's), maar vaker voorkomen vanwege de huidige lage maturity niveaus van verscheidene leveranciers van vitale infrastructuur.
- **Functies en verantwoordelijkheden tussen de overheid en de privé-sector** moeten duidelijk worden gedefinieerd om zo APT's te vermijden en een betere respons op en onderzoek naar dergelijke aanvallen te verzekeren.

- **Deze vraag wordt gezien als een geopolitieke kwestie, die daarom een geopolitieke benadering van de overheid vereist,** onder andere door beroep te doen op internationale samenwerking om externe dreigingen te identificeren en aan te pakken.

Aanbevelingen

Om deze uitdagingen het hoofd te bieden, maken we een reeks aanbevelingen voor de NCTV zoals hieronder samengevat.

1. De NCTV dient de rol van het onderscheid tussen vitale en niet-vitale infrastructuur binnen het Nederlandse beheersmodel nader te onderzoeken

Zoals hierboven vermeld, kan het nodig zijn om het onderscheid tussen vitale en niet-vitale infrastructuurdiensten of -processen opnieuw te bekijken. Voor de NCTV kan het daarom zinvol zijn om verder te onderzoeken hoe vitale infrastructuur wordt geïdentificeerd en gecategoriseerd, hoe afhankelijkheden en risico's op het gebied van cybersecurity in kaart worden gebracht, begrepen en gedeeld, en welke eisen in Nederland worden gesteld aan organisaties met verschillende vitale niveaus. Daarom moet de NCTV naar het volgende streven:

- **Alternatieve benaderingswijzen inzake de identificatie en classificatie van vitale infrastructuur onderzoeken en beoordelen,** inclusief meer horizontale en sector-agnostische benaderingen;
- **Onderzoeken hoe afhankelijkheden tussen vitale sectoren en organisaties in kaart kunnen worden gebracht** (zie ook de onderstaande aanbevelingen met betrekking tot de beveiliging van vitale infrastructuur); en
- **Onderzoeken hoe het delen van informatie tussen vitale en niet-vitale sectoren verbeterd kan worden** zodat organisaties de juiste informatie op het juiste moment ontvangen.

2. De NCTV moet verder onderzoek doen naar en investeren in proactieve en preventieve benaderingswijzen van nationale cybersecurity, die verder gaan dan het huidige, meer reactieve paradigma

Binnen het gedecentraliseerde beleidsmodel van het Nederlandse systeem zijn de verantwoordelijkheden voor cybersecurity verspreid over meerdere ministeries en organisaties. Het cybersecurity domein is ook continu in ontwikkeling en vereist constante aanpassing, dus is het belangrijk dat de Nederlandse overheid flexibel en proactief blijft in haar aanpak van nationale cybersecurity. Daarom moet de NCTV meer onderzoek doen naar en investeren in proactieve benaderingswijzen van cybersecurity, waaronder:

- **Ervoor zorgen dat er regelmatig uitgebreide oefeningen plaatsvinden** om de beleidsstructuren en incident-responsplannen te testen zodat alle belanghebbenden een duidelijk begrip hebben van hun rollen en verantwoordelijkheden en goede werkrelaties met hun collega's ontwikkelen.
- **Onderzoeken hoe de NCTV en het NCSC proactievere cybersbeveiligingsdiensten zouden kunnen opzetten**, inclusief bijvoorbeeld proactieve kwetsbaarheidsscans van Nederlandse netwerken.

- **Investeren in verder onderzoek naar hoe cybersecurity afhankelijkheden en systeemrisico's beter kunnen worden geïdentificeerd en verminderd** (zie ook de onderstaande aanbevelingen inzake de beveiliging van vitale infrastructuur).

3. De NCTV zou verder onderzoek moeten doen naar de rol van minimale beveiligingsstandaarden en de mogelijke behoefte aan verdere nalevingsmechanismen

In de studie beschrijven wij ook mogelijke problemen door het gebrek aan geharmoniseerde standaarden voor cybersecurity binnen de overheidsorganisaties en een gebrek aan minimale eisen voor en -standaarden voor cybersecurity. Dit kan het eventueel moeilijk maken om voor alle organisaties in Nederland een toereikende cybersecurity-basisniveau te waarborgen. Het is ook gebleken dat het niet altijd eenvoudig zal zijn organisaties ertoe te bewegen cybersecurity-adviezen of -richtlijnen na te leven, zelfs wanneer specifieke kwetsbaarheden of bedreigingen zijn geïdentificeerd.

De NCTV dient de mogelijkheid te onderzoeken om:

- **Minimale cybersecuritystandaarden voor nationale veiligheid te ontwikkelen en implementeren** om zo een cybersecurity-basisniveau tussen de verschillende overheidsafdelingen en -organisaties te versterken en om de IT-infrastructuur van de overheid te harmoniseren ;
- **Minimale cybersecuritystandaarden te ontwikkelen en implementeren voor private bedrijven die IT-diensten leveren aan de overheid** om zo zwakten in de supply chain en cybersecurityafhankelijkheden tussen sectoren te verminderen ; en
- **De behoefte te onderzoeken naar meer bevoegdheid voor het NCSC of een andere overheidsinstantie om cybersecurity-advies of -normen te evalueren, overzicht te bieden en cybersecurity-advies of -normen** af te dwingen buiten het huidige 'pas-toe-of-leg-uit'-kader dat momenteel van kracht is.

4. De NCTV moet van de ontwikkeling van vaardigheden op het gebied van cybersecurity en engineering een hoge prioriteit maken voor de bescherming van de vitale sectoren in Nederland

De huidige vaardigheids- en kenniskloof op het gebied van vitale infrastructuur leidt tot aanzienlijke uitdagingen. Zo bestaat er het risico dat (cyber)veiligheid van vitale infrastructuur ondermijnd wordt en zijn inspecteurs mogelijk beperkt in hun vermogen om om waardevolle inzichten te bieden in het cybersecurity niveau van een organisatie. Deze studie toont aan dat maatregelen op korte termijn nodig zijn om de vaardigheidskloof te dichten en de huidige OT-IT-kloof te overbruggen. De NCTV dient daarom samen met de betrokken ministeries te werken aan:

- **Het investeren in operationeel technologisch onderzoek en bewustwording binnen de overheid** om ervoor te zorgen dat gespecialiseerde instanties zoals het NCSC passende aanbevelingen en richtlijnen kunnen bieden, vooral in geval van kwaadwillige aanvallen. Dit zou ook bijdragen aan de vertrouwensontwikkeling en de samenwerking tussen de overheid en de industrie ten goede komen.
- **Het creëren van synergieën tussen de academische wereld, de industrie, toezichthouders en de overheid** door maatregelen te implementeren zoals baanrotatie in vitale sectoren, detacheringen

voor ambtenaren, verplichte stages voor studenten en gastcolleges van belanghebbenden in de supply chain van de industrie en bij toezichthouders;

- **Het integreren van elementen van operationele technologie en academische IT-curricula** om zo te leiden tot een gedeeld begrip tussen beide disciplines en verdere samenwerking op zowel academisch als industrieel niveau; en
- **Aan het verhogen van het cybersecurity-bewustzijn bij operationele technologiespecialisten** door elementen van cybersecurity aan technische studenten aan te leren en cybersecurity training te geven aan operationele technologiespecialisten die in vitale sectoren werken.

5. De NCTV moet de instrumenten ondersteunen om de risico's in verband met de supply chain van vitale infrastructuur aan te pakken

Cybersecurity maturity in complexe geglobaliseerde supply chains zal naar verwachting een van de belangrijkste kwesties zijn die het komende decennium op het gebied van cybersecurity domineren. Inzicht in de kwetsbaarheden en risico's verbonden aan de supply chains van vitale infrastructuur is daarom essentieel voor de bescherming van de Nederlandse vitale sectoren. Onderwerpen voor nader onderzoek en interventie zijn:

- **De uitbreiding van bestaande modellen voor het in kaart brengen van risico's naar de volledige supply chain van vitale infrastructuur,** inclusief de overweging van relevante externe effecten. Mogelijke elementen zijn het beheer van de supply chain, het gebruik van nieuwe technologieën en het beoordelen van risico's op basis van dienstverlening en de voortzetting ervan in plaats van op operatoren om onderlinge afhankelijkheden beter te identificeren.
- **Onderzoek naar mogelijkheden voor internationale samenwerking in de aanpak van kwetsbaarheden in de supply chain van vitale infrastructuur** om zo geopolitieke allianties en Europese of alliantie-gebaseerde benaderingswijzen te ontwikkelen, dit om onzekerheden gebonden aan internationale supply chains aan te pakken, bijvoorbeeld om modellen voor het in kaart brengen van risico's aan te geven, inclusief externe effecten, en om dreigingen van buitenaf aan te pakken.
- **Informatie en kennis die specifiek is voor operationele technologie beschikbaar maken om een beter begrip van en zicht op de supply chain van operationele technologieproducten en de bijbehorende risico' te krijgen.** Dit zou bijvoorbeeld kunnen gebeuren via initiatieven zoals de ontwikkeling van een operationeel technologie-specifiek platform voor het delen van informatie, of een centrum voor de uitwisseling en analyse van operationele technologie-informatie - een project dat momenteel wordt besproken tussen het NCSC de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO).

Bijkomende punten die de aandacht van de NCTV verdienen

In de tweede fase van deze studie werden bijkomende aandachtsgebieden voor de NCTV geïdentificeerd. Bepaalde aspecten maken al deel uit van de huidige inspanningen om nieuwe capaciteiten te ontwikkelen. In deze gevallen bevelen wij aan dat de NCTV zich richt op:

- Samenwerking met het Ministerie van Onderwijs en andere verantwoordelijke ministeries op gebied van de lopende inspanningen om een vervanger voor dcypher te ontwikkelen, en onderzoek naar de mogelijkheid en waarde van de ontwikkeling van een cybersecurity personeelsbeleid voor de nationale overheid, met een gedeelde kennis van het cybersecurityveld en een gemeenschappelijk competentie-raamwerk en beter afgestemde opleidingseisen en loopbaantrajecten;
- Blijvende samenwerking met CIO Rijk en CISO Rijk om een alomvattend overzicht en begrip te ontwikkelen van de cybersecuritytoestand binnen de rijksoverheid; en
- Blijvende samenwerking met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en andere relevante belanghebbenden om te helpen bij de voortdurende inspanningen om de cybersecurity-wet- en regelgeving op één lijn te krijgen

Andere aanbevelingen zijn gericht op gebieden waar tot nu toe weinig inspanningen werden geleverd. De NCTV zou een leidende rol kunnen spelen in:

- Het ontwikkelen van een wetenschappelijke basis voor maturity modellen inzake cybersecurity via het uitvoeren van degelijke en onafhankelijke evaluaties van de effectiviteit van maturity modellen en het vergelijken van bestaande modellen.
- De ontwikkeling van een wetenschappelijke basis voor de huidige benaderingswijzen op gebied van de cybersecurity regelgeving voor vitale infrastructuur door de verschillen tussen algemene en sectorgeboden normen en hun impact op de cybersecurity van vitale infrastructuur te onderzoeken.
- De ontwikkeling van overheidscapaciteit voor de aanpak van Advanced Persistent Threats (APT's) via de ontwikkeling van een forensische functie binnen de Nederlandse overheid.

Naast deze *state-of-the-art* studie lopen er tegelijkertijd verschillende initiatieven om het benodigde bewijsmateriaal voor de cybersecurity in Nederland verder te ontwikkelen en deze risico's aan te pakken. De uitdagingen en aanbevelingen die in deze studie worden beschreven, moeten daarom ook worden bekeken, naast de resultaten van andere eerdere en lopende onderzoeksinspanningen. Mogelijk zouden dit soort kwesties aangepakt moeten worden door aanvullend onderzoek, terwijl andere misschien aangepakt moeten worden buiten de context van een onderzoeksagenda. Het kan bijvoorbeeld zo zijn dat er goed begrepen wordt wat er dient te gebeuren, maar dat er gebrek is aan politieke wil, budget of operationeel vermogen om deze maatregelen adequaat te implementeren. Deze kwesties verdienen toch de aandacht van de NCTV. En gebieden waar reeds initiatieven lopen kunnen toch nog behoefte hebben aan of baat bij de steun van de NCTV.