



Cybersecurity

A State-of-the-art Review

Samenvatting

Erik Silfversten, Erik Frinking, Nathan Ryan, Marina Favaro

© 2019 Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC),
Ministerie van Justitie en Veiligheid. Auteursrechten voorbehouden.



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).

WODC publications do not represent the opinions of the Minister of Justice and Security.

All WODC reports can be downloaded free of charge at www.wodc.nl

Preface

The NCTV (*Nationaal Coördinator Terrorismedebestrijding en Veiligheid* – ‘National Coordinator for Security and Counterterrorism’) partners with government, science and business in order to both protect the Netherlands against threats that can disrupt society, and ensure that Dutch vital infrastructure is – and remains – safe. This document presents the executive summary of a RAND Europe study commissioned by the WODC (*Wetenschappelijk Onderzoek- en Documentatiecentrum* – ‘Research and Documentation Centre’), on behalf of the NCTV. The study examines the current state-of-the-art in the field of cybersecurity as part of a broader programme of work that aims to develop a broad research agenda for the NCTV. This programme of work also includes two other state-of-the-art studies in the fields of crisis management and counterterrorism, which are published separately by the WODC.

This document and its accompanying report cover the methods and analysis undertaken to assess the state-of-the-art in the field of cybersecurity, and provides research questions for the NCTV to consider in the preparatory work for the research agenda. The report should be of interest to individuals and organisations involved in cybersecurity policymaking in the Netherlands and beyond.

RAND Europe is a not-for-profit, independent policy-research organisation that aims – through objective research and analysis – to improve policy-and decision making in the public interest. RAND Europe’s clients include national governments, multilateral institutions and other organisations with a need for rigorous, independent interdisciplinary analysis. Part of the globally operating RAND Corporation, RAND Europe has offices in Cambridge, UK, and Brussels, Belgium.

For more information about RAND Europe or this document, please contact Erik Silfversten (erik_silfversten@rand.org).

RAND Europe
Rue de la Loi 82, Bte 3
1040 Brussels
Belgium
Tel: +32 (2) 669 2400

RAND Europe
Westbrook Centre, Milton Road
Cambridge CB4 1YG
United Kingdom
Tel: +44 1223 353 329

Achtergrond en context

De digitale transformatie heeft het hedendaagse leven ingrijpend veranderd en zal dit waarschijnlijk in de komende jaren blijven doen. Technologie is een belangrijke motor voor het realiseren van maatschappelijke en economische welvaart, maar het heeft ook een donkere kant. Overheden, bedrijven, maatschappelijke organisaties en burgers worden geconfronteerd met een scala aan bestaande en nieuwe cybersecurity dreigingen. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) stelde in het Cybersecuritybeeld Nederland (CSBN) vast dat de digitale weerbaarheid van Nederland achterblijft bij de groeiende digitale dreiging.

De missie van de NCTV is het beschermen van Nederland tegen bedreigingen die de samenleving kunnen ontwrichten. In het kader van dit streven naar een digitaal veilig Nederland werkt de NCTV samen met de wetenschap, het bedrijfsleven en binnen de overheid. Om haar missie te volbrengen, is de NCTV momenteel een brede onderzoeksagenda aan het ontwikkelen. Hiermee worden drie doelstellingen beoogd: de samenwerking met wetenschappelijk onderzoek te intensiveren; wetenschappelijke discussies op gebieden die van belang zijn voor de NCTV te stimuleren; en de blinde vlekken binnen de kennis van de NCTV en de wetenschappelijke gemeenschap te identificeren. Drie ‘*state-of-the-art*’ studies op het gebied van terrorismebestrijding, crisisbeheersing en cybersecurity zijn onderdeel van dit programma.

Doelstellingen

Namens de NCTV heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) RAND Europe de opdracht gegeven om de *state-of-the-art* in cybersecurity te onderzoeken. *State-of-the-art* verwijst in deze context naar een overzicht van prominente risico's, bedreigingen en beleidskwesties op het gebied van cybersecurity en, daarnaast, probleemgebieden die niet genoeg aandacht krijgen van de NCTV of de wetenschap.

Het cybersecurity *state-of-the-art* onderzoek bestaat uit twee fasen:

- 1) **Fase 1** is gericht op het uitvoeren van een eerste scan van prominente of onderbelichte kwesties in het cybersecuritydomein die meer aandacht verdienen van de NCTV.
- 2) **Fase 2** is gericht op het onderzoeken van de onderzoeksvragen geïdentificeerd in Fase 1 en zal in een afzonderlijke studie worden uitgevoerd.

Dit onderzoek omvat alleen Fase 1 van dit proces. Het overkoepelende doel is om de relevante thema's te verkennen op het gebied van cybersecurity die in Fase 2 verder dienen te worden onderzocht. Drie onderzoeksvragen, zoals weergegeven in Tabel 0.1, geven invulling aan het bereiken van de doelstelling.

Tabel 0.1 Overzicht van Fase 1 vragen

V1. Over actuele en opkomende cybersecurity onderwerpen	V2. Over het NCTV-domein	V3. Over de te volgen aanpak in Fase 2
<p>V1.1 Wat zijn de meest prominente, actuele en opkomende cybersecurity onderwerpen die worden bestudeerd?</p> <p>V1.2 Hoe grondig zijn deze onderwerpen onderzocht?</p> <p>V1.3 Zijn de onderwerpen onderzocht met behulp van gegevens van hoge kwaliteit en geschikte methoden?</p>	<p>V2.1 Welke van deze prominente cybersecurity onderwerpen vallen binnen het domein van de NCTV?</p> <p>V2.2 Welke cybersecurity onderwerpen zijn inbegrepen en welke zijn uitgesloten van het domein van de NCTV en waarom?</p>	<p>V3.1 Hoe kunnen de hierboven besproken cybersecurity onderwerpen worden vertaald naar toekomstige onderzoeksactiviteiten, wat mogelijk het ontwikkelen van onderzoeksvragen en vaststellen van geschikte methodologieën vereist?</p> <p>V3.2 Is systematisch literatuuronderzoek een geschikte methode? Zo ja, welk soort systematisch literatuuronderzoek is het meest geschikt voor de geïdentificeerde onderzoeksvragen?</p> <p>V3.3 Wat zou een mogelijke afbakening kunnen zijn voor een literatuuronderzoek (bijvoorbeeld naar publicatieperiode, groepen waarvan dreiging uitgaat enz.)?</p>

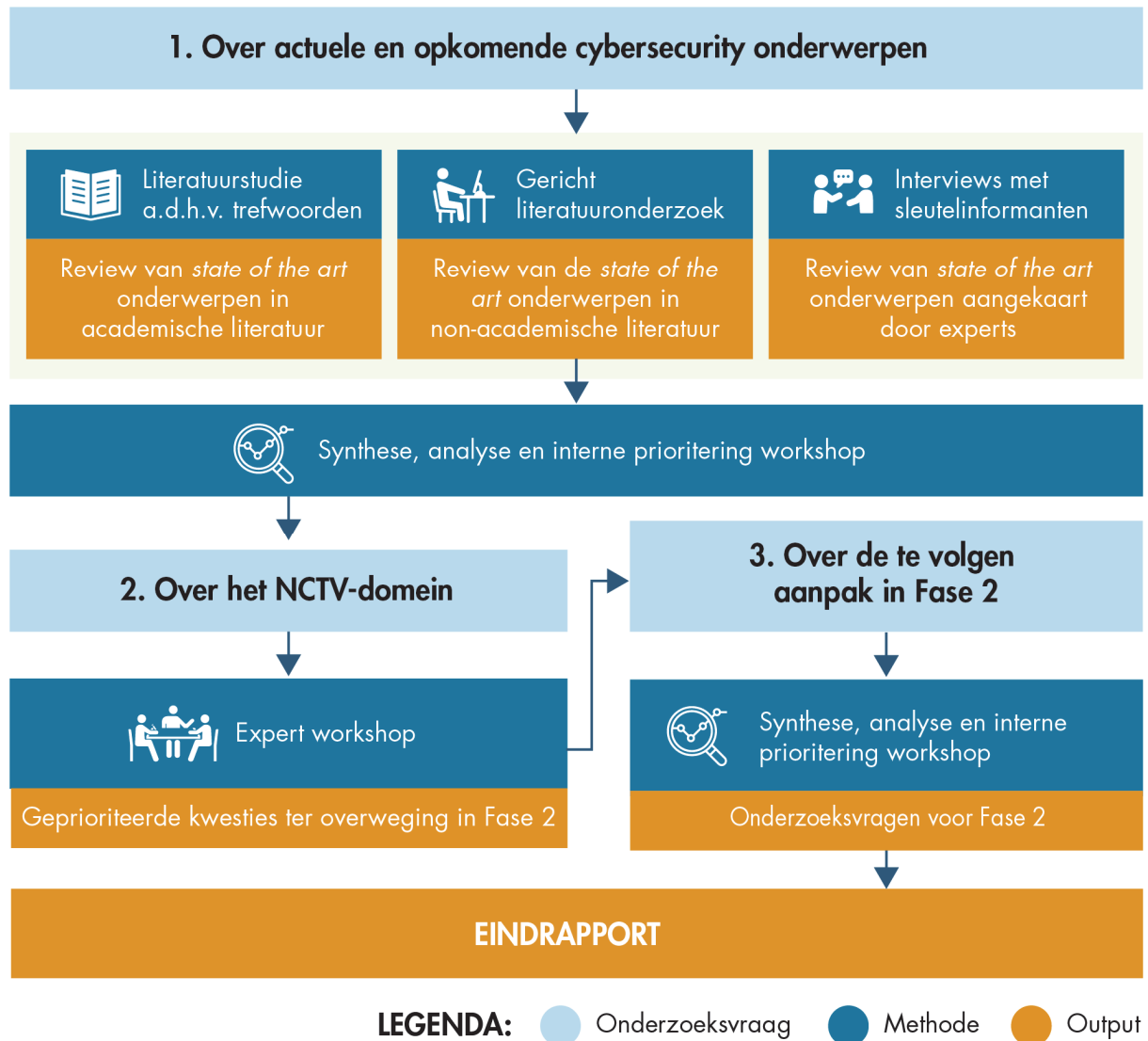
De NCTV gebruikt momenteel een conceptueel "driehoeksmodel" met belangen, dreigingen, weerbaarheid om haar agenda te bepalen. Om bij te dragen aan de ontwikkeling van de toekomstige onderzoeksagenda, heeft de NCTV een alternatief raamwerk ontwikkeld dat zich vooral richt op de actoren binnen het veld van cybersecurity. Deze raamwerken zijn niet gebruikt bij het formuleren van de onderzoeksvragen binnen dit onderzoek en worden daarom afzonderlijk van het hoofdrapport besproken. Bijlage 1 van dit rapport bevat een verdere toelichting van de conceptuele raamwerken en worden hun sterke en zwakke punten besproken, gezien in het licht van de bevindingen van dit onderzoek.

Methodologie

In dit onderzoek is een combinatie van verschillende methoden toegepast, zoals weergegeven in Figuur 0.1. In Bijlage A is een volledig overzicht te vinden van de in dit onderzoek toegepaste methodologie. We hebben gekozen voor deze benadering om een momentopname mogelijk te maken van de *state-of-the-art* in cybersecurity. Uit deze momentopname komen de prominente, actuele en opkomende cybersecurity onderwerpen duidelijk naar voren, evenals gesignaleerde hiaten in de kennis.

Binnen deze *mixed-methods* benadering is een breed scala aan bronnen geraadpleegd en zijn diverse experts en belanghebbenden geraadpleegd, waardoor een zo volledig mogelijke *state-of-the-art* kon worden opgesteld. Tot slot heeft de betrokkenheid van experts bij het prioriteren van cybersecurity onderwerpen voor de NCTV tot relevante resultaten geleid.

Figuur 0.1 Overzicht van *state-of-the-art* ontwikkeling



Voornaamste bevindingen van de state-of-the-art

V1 Over de huidige en opkomende cybersecurity onderwerpen

Dit *state-of-the-art* onderzoek heeft drie algemene bevindingen:

- Onderzoek op het gebied van cybersecurity wordt bemoeilijkt door de complexiteit en het gebrek aan definities.** In het algemeen bouwen wetenschappers voort op het werk van hun voorgangers. Maar de grenzen van het werkveld van cybersecurity verschuiven voortdurend en in

hoog tempo. Het is moeilijk vast te stellen op welke gebieden onderzoek reeds is uitgevoerd, welke gebieden nog steeds over het hoofd worden gezien, of waar kennis nog steeds tekortschiet.

2. **Er zijn veel kennis- of onderzoekshiaten en ze zijn veelal hardnekkig.** Het veld kent een aantal hiaten in het onderzoek, die vaak niet door Nederlandse studies worden geadresseerd. Er is bijvoorbeeld een gebrek aan onderzoek naar: nationale veiligheidsvraagstukken; aansturing vanuit de overheid; ethische kwesties; en juridische zorgen. Risico's die kleven aan afhankelijkheden van buitenlandse technologie of van toeleveringsketens buiten Nederland zijn op basis van de huidige literatuur en expertkennis nog niet goed te doorgronden. Opkomende onderwerpen zijn vaak nog onvoldoende onderzocht (bijvoorbeeld *Internet of Things*, kunstmatige intelligentie, cryptomunten, het *dark web* en kwantumtechnologie). Daarnaast blijft hun impact op de Nederlandse nationale veiligheid onbekend.
3. **Binnen cybersecurity onderzoek is er vaak sprake van ontoereikende of ontbrekende gegevens en methoden, zowel op technisch als op beleidsvlak.** Op veel deelterreinen lijkt er een gebrek aan betrouwbare, verifieerbare gegevens, en grootschalige longitudinale datasets in het bijzonder. Dit maakt het lastig om de aard van de uitdaging of het probleem te definiëren, te verwoorden en uiteindelijk te begrijpen. Het is daarom ook moeilijk om mogelijke oplossingsrichtingen te onderzoeken. Het gebrek aan gegevens of passende methoden kan het voor beleidsmakers ook moeilijk maken om te begrijpen op welke basis beslissingen moeten worden genomen, hoe beslissingen in de loop van de tijd hebben uitgepakt en wat de impact ervan was.

Dit *state-of-the-art* onderzoek heeft een breed scala van cybersecurity onderwerpen geïdentificeerd die door deskundigen als prominente kwesties worden beschouwd of significante hiaten in de literatuur zijn. We hebben belangrijke thema's, prominente kwesties en vastgestelde onderzoekshiaten of blinde vlekken die in eerste instantie naar voren komen geconsolideerd. Dit leidde tot de identificatie van 60 prominente cybersecurity onderwerpen of vermeende hiaten.

Via een gestructureerde en iteratieve aanpak hebben we vervolgens vergelijkbare onderwerpen gegroepeerd om een shortlist met onderwerpen op te stellen voor de workshop met deskundigen. Het consolideren leidde tot een shortlist van 11 onderwerpen. Figuur 0.2 geeft weer hoe we van de lange lijst van 60 onderwerpen tot de 11 clusters zijn gekomen.

Figure 0.2 Trechter van *long-list* tot *short-list*



We hebben een short-list opgesteld van onderwerpen die vervolgens tijdens een workshop met deskundigen is gescoord en bediscussieerd . Het doel van deze workshop was het identificeren en bepalen van de voor de NCTV meest relevante onderwerpen die in een toekomstige onderzoeksagenda moeten worden opgenomen. Dit leidde tot het identificeren van 11 brede algemene cybersecurity onderwerpen, zoals toegelicht in Tabel 0.2.

Tabel 0.2 Shortlist van prominente cybersecurity onderwerpen die in de *state-of-the-art* review zijn geïdentificeerd

Onderwerp	Titel	Omschrijving
1	Cybersecurity vanuit het perspectief van de nationale veiligheid	Vanuit de invalshoek van nationale veiligheid is cybersecurity een breed begrip. Hedendaagse benaderingen gebruiken veelal een holistische benadering gericht op de samenleving als geheel. Onze analyse duidt aan dat de kennis van deskundigen over verschillende aspecten van cybersecurity vanuit de invalshoek van nationale veiligheid laag wordt geacht. Dit geldt ook voor kennis van de wijze waarop verschillende landen het cyber domein benaderen en daarbinnen opereren.
2	Aansturing van cybersecurity op nationaal niveau	De toegenomen afhankelijkheid van ICT in de samenleving vormt een uitdaging voor overheden om cybersecurity optimaal te reguleren op het nationale niveau. Het wordt steeds belangrijker dat landen een breed spectrum aan cybersecurity incidenten en aanvallen anticiperen, detecteren, voorkomen en beperken. Een gecoördineerde samenwerking tussen de publieke en private sector is hier ook van belang, zowel in eigen land als internationaal.
3	Onderwijs en vaardigheden	Cybersecurity kan niet worden verbeterd zonder te beschikken over voldoende gekwalificeerde en ervaren cybersecurity professionals. Door het vastgestelde tekort aan cyberprofessionals en de grote vraag naar deze professionals op de arbeidsmarkt spannen organisaties zich in toenemende mate in om bekwame professionals te werven en te behouden. In een krappe arbeidsmarkt wordt de publieke sector doorgaans geconfronteerd met aanzienlijke concurrentie vanuit de private sector.
4	Opgaven voortkomend uit de implementatie van basale cybersecurity regelingen	Organisaties blijven worstelen met het implementeren van basale en effectieve cybersecurity controles om zichzelf te beschermen tegen incidenten en aanvallen. In zowel de publieke als private sector blijven cyberincidenten op grote schaal plaatsvinden door de afwezigheid van adequate cybersecurity maatregelen, zoals bijvoorbeeld procedures op het gebied van risicobeheersing, technische controles en het organiseren van taken en verantwoordelijkheden binnen organisaties.
5	Veiligheidskwesties in de productieketen	Veiligheidskwesties in de productieketen zijn van belang voor technologie-intensieve organisaties en sectoren. In globaliserende markten met wederzijds afhankelijke productieketens is het noodzakelijk om te begrijpen welke technologie wordt gebruikt, waar deze vandaan komt, hoe deze werkt, hoe deze kan worden getest en geverifieerd, en hoe kan worden gegarandeerd dat deze veilig en zoals beoogd functioneert.
6	Menselijke aspecten van cybersecurity	Er zijn talloze menselijke gedragingen in <i>cyberspace</i> die systemen in gevaar brengen en de effectiviteit van beveiligingsprotocollen bedreigen. Menselijk gedrag is een achilleshiel voor ieder informatiesysteem aangezien individueel handelen kwetsbaarheden kan blootleggen (zoals het hergebruik van wachtwoorden). Daarnaast zijn mensen kwetsbaar voor gerichte aanvallen die gebruik maken van ' <i>social engineering</i> ' (bijv. <i>phishing</i> , imitatie en <i>shoulder-surfing</i>). Individueel gedrag kan als zodanig ook andere veiligheidsinterventies in gevaar brengen.

7	Begrijpen van cyber-criminelen en slachtoffers	Het aanpakken van cybercrime staat al geruime tijd hoog op de agenda van de Nederlandse autoriteiten. Maar cybercriminaliteit ontwikkelt zich voortdurend. Actuele en opkomende problemen zijn bijvoorbeeld de vercommercialisering van de <i>tools</i> van cybercriminelen, het toepassen van nieuwe technologieën en de toegenomen mogelijkheden voor uitbuiting (bijvoorbeeld het groeiend aantal apparaten dat is aangesloten op het internet).
8	Vertrouwen in informatie en gegevens	De samenleving produceert, gebruikt en is steeds meer afhankelijk van data. Besluitvorming laat zich geleidelijk aan steeds meer sturen door autonome technologische hulpmiddelen zoals kunstmatige intelligentie. Het zal daarom steeds belangrijker worden om gegevens en opkomende besluitvormingsmethoden te controleren en te verbeteren. Op deze manier dient ervoor gezorgd te worden dat ze betrouwbaar en vrij van vooringenomenheid zijn.
9	Vertrouwen in <i>computing</i>	Technologische ontwikkelingen hebben de manieren waarop de samenleving functioneert fundamenteel veranderd. Technologie is tegenwoordig niet meer weg te denken uit iedere sector. Door automatisering zijn we steeds afhankelijker geworden van computergerelateerde hardware en software. Om die reden is het van groot belang ervoor te zorgen dat er geschikte mechanismen bestaan om systemen die in alle aspecten van de samenleving worden gebruikt te testen, certificeren, controleren en beveiligen. Deze systemen dienen te functioneren zoals bedoeld en moeten veilig gebruikt kunnen worden gedurende hun hele levenscyclus.
10	Beveiliging vitale infrastructuur	Vitale infrastructuur omvat alle fysieke faciliteiten die noodzakelijk worden geacht voor het goed functioneren van de economie en de samenleving (bijv. energiecentrales, dammen, overheidsdataservers) en wordt doorgaans gezien als een van de pijlers van cybersecurity van een land. Recente ontwikkelingen zoals het aansluiten van bepaalde delen van de vitale infrastructuur op het internet en het verrijken van de vitale infrastructuur met nieuwe of opkomende technologieën of oplossingen (bijv. automatisering, virtualisatie, clouddiensten, kunstmatige intelligentie, enz.), vormen nieuwe en wezenlijke uitdagingen voor cybersecurity.
11	Het economische model van cybersecurity	Gebrek aan cybersecurity kan worden veroorzaakt door ontwerpfouten, door het nalaten van het nemen van voorzorgsmaatregelen of door menselijke fouten. In werkelijkheid storingen vaak veroorzaakt door de aanwezigheid van verkeerde prikkels. Kwetsbaarheden in hardware, software en services kunnen verscheidene oorzaken hebben. Het economische model van cybersecurity is onderhevig aan een reeks negatieve economische factoren (bijv. de tragedie van de meent, netwerkeffecten, externaliteiten, asymmetrische informatie en adverse selectie, ' <i>liability dumping</i> ', moreel risico enz.).

V2 Over het NCTV domein

De 11 themagebieden zijn in een workshop door Nederlandse cybersecurity deskundigen beoordeeld, besproken en geprioriteerd. Op basis hiervan zijn de meest prominente kwesties in kaart gebracht waarop de NCTV verdere actie zou moeten ondernemen. In de workshop werden blinde vlekken in ieder onderwerp uitgelicht. Daarnaast werd er gesproken over de manier waarop cybersecurity momenteel in organisaties – van universiteiten tot bedrijven en de overheid – in heel Nederland wordt uitgevoerd en toegepast. De 11 onderwerpen werden beoordeeld op hun:

- **Belang** in het veld (d.w.z. of een onderwerp gezien wordt door deskundigen als een ondergeschikt, opkomend, of significant risico of bedreiging).
- **Begrip over** het onderwerp vanuit het perspectief van deskundigen en uitvoerders (d.w.z. gering, groeiend of goed begrip).
- **Relevantie voor de NCTV** (laag/gemiddeld/hoog)
- **Urgentie om actie te ondernemen** (laag/gemiddeld/hoog).

Vier onderwerpen kwamen naar voren als het meest prominent, urgent en relevant voor de NCTV. Deze zouden door de NCTV overwogen moeten worden om verder te verkennen in Fase 2 van het *state-of-the-art* project. Begrip over deze onderwerpen wordt als beperkt gezien, ondanks de zichtbare aandacht die ervoor bestaat en het eerdere werk dat is uitgevoerd.

1. **De aansturing van cybersecurity vanuit het perspectief van de nationale veiligheid** is gericht op het toenemende gebruik, de afhankelijkheid van ICT en de ontwrichtingen die ermee gepaard gaan. Dit stelt overheden voor de vraag hoe de aansturing van gebieden die met nationale veiligheid te maken hebben, moet plaatsvinden. Deelnemers aan de workshop suggereerden dat een nieuwe aansturingsstructuur Nederland weerbaarder kan maken tegen cybersecurity problemen. Onduidelijke verdeling van rollen en verantwoordelijkheden, inconsistenties in het taalgebruik, ineffectieve organisatiestructuren en tekortschietende wettelijke mandaten kunnen volgens de deskundigen in potentie de nationale veiligheid in gevaar brengen.
2. **Vertrouwen in informatie en gegevens** is gericht op het almaar toenemende volume aan gegevens die bedrijven, de overheid, de samenleving en individuen produceren en consumeren. Het vertrouwen in informatie en gegevens wordt uitgehold door de toenemende maatschappelijke afhankelijkheid van gedigitaliseerde informatie en nieuwsbronnen. Publieke en private organisaties gebruiken nieuwe methoden om steeds grotere datasets te analyseren. Deze methoden maken steeds meer gebruik van toenemende autonome analyse en besluitvormingsmiddelen, zoals kunstmatige intelligentie en *machine learning*. Het wordt steeds belangrijker om gegevens en opkomende besluitvormingsmethoden te controleren en te valideren op hun betrouwbaarheid en om te zien of ze vrij van vooringenomenheid zijn.
3. **De beveiliging van de vitale infrastructuur** wordt in westerse landen doorgaans gezien als een van de pijlers van cybersecurity van een land. **De vitale infrastructuur** omvat die diensten die noodzakelijk worden geacht voor het goed functioneren van de samenleving (bijv. elektriciteitscentrales, watervoorzieningssystemen en vervoersinfrastructuur). Recente ontwikkelingen zoals het aansluiten van bepaalde componenten van de vitale infrastructuur op het internet en het verrijken van de vitale infrastructuur met nieuwe of opkomende technologieën of oplossingen (bijv. automatisering, virtualisatie, clouddiensten en kunstmatige intelligentie), vormen nieuwe en essentiële cybersecurity uitdagingen. Hoewel er sprake is van nieuwe trends, zijn er ook aanhoudende tekortkomingen in het aanpakken van bestaande problemen, in het beschermen tegen bekende kwetsbaarheden en in het moderniseren van cyber-fysiek systemen.
4. **Veiligheid van de toeleveringsketen** is van belang voor de publieke én private sector. Door toenemende onderlinge verbanden en afhankelijkheden zijn beide sectoren in vergelijkbare mate aan risico's in hun toeleveringsketen blootgesteld. Door het alomtegenwoordige gebruik van ICT moeten organisaties de risico's bij aanleverende partijen identificeren en maatregelen hiervoor

treffen (bijv. gebruikersbeheer, lees- en schrijfrechten en overeenkomsten sluiten voor het delen van gegevens) om mogelijk beveiligingsinbreuken of cyberincidenten te beperken. Toenemende complexiteit (bijv. in de vorm van meer geïntegreerde systemen/CPU's) en opkomende technologieën (bijv. het gebruik van door derden ontwikkelde algoritmen) maken het lastiger om de veiligheid van alle componenten en systemen die in de gehele toeleveringsketen worden gebruikt te testen, controleren en beveiligen.

V3 Over de toe te passen benadering in Fase 2

Beleidsmakers, onderzoekers en uitvoerders zullen zich allemaal moeten aanpassen aan het dynamische cyberecosysteem. De volgende onderzoeksvragen en voorgestelde richtingen voor toekomstig onderzoek kunnen bijdragen aan meer doelmatig en doeltreffend cybersecuritybeleid en interventies.

Voor ieder thematisch gebied hebben we drie of vier onderzoeksvragen voor Fase 2 van het project geformuleerd. Deze worden weergegeven in Tabel 0.3. Deze indicatieve onderzoeksvragen zijn het resultaat van het samenbrengen van al het binnen deze studie verzamelde materiaal. Het zijn echter niet de enige onderzoeksvragen die binnen dit gebied mogelijk en uitvoerbaar zijn.

Tabel 0.3 Overzicht van prominente cybersecurity onderwerpen en onderzoeksvragen

Thematisch gebied	Onderzoeksvragen
1. Aansturing van cybersecurity vanuit een nationale veiligheidsperspectief	<p>1.1 Hoe kan de doelmatigheid en doeltreffendheid van nationale aansturingssystemen voor cybersecuritybeleid worden gemeten?</p> <p>1.2 Welke capaciteiten, vaardigheden en functies (zoals inlichtingen, bedrijfsactiviteiten, coördinatie, bevelvoering en controle, training, enz.) moeten belanghebbenden hebben om cybersecurity bedrijfsactiviteiten te waarborgen?</p> <p>1.3 Welke lessen kunnen worden getrokken uit internationale vergelijkingen van nationale aansturingssystemen in cybersecurity?</p> <p>1.4 Hoe kunnen het huidige aansturingmodel en cybersecurity initiatieven (zoals strategieën, onderzoeksagenda's, roadmaps enz.) op elkaar worden afgestemd en verbeterd?</p>
2. Vertrouwen in informatie en gegevens	<p>2.1 Hoe kunnen opkomende besluitvormingsmethoden (zoals algoritmen, <i>machine learning</i> en toepassingen van kunstmatige intelligentie) worden gecontroleerd en beveiligd om ervoor te zorgen dat ze accuraat zijn en zonder vooringenomenheid?</p> <p>2.2 Hoe kan maatschappelijk vertrouwen in informatie en gegevens worden begrepen en versterkt?</p> <p>2.3 Hoe kan het vertrouwen in informatie en gegevens in de informatievoorzieningsketen worden behouden?</p>

3. Beveiliging vitale infrastructuur	<p>3.1 Wat is de wisselwerking tussen verouderde en nieuwe technologieën (bijvoorbeeld IoT-apparaten en 5G-connectiviteit) die meer stelselmatige complexiteit en dynamische bedreigingen voor vitale infrastructuur creëren?</p> <p>3.2 Hoe kan het huidige stadium van cybersecurity binnen de vitale infrastructuur worden gemeten en begrepen?</p> <p>3.3 Wat kan worden gedaan om de veiligheid te verbeteren van de technologie die wordt toegepast in vitale sectoren?</p>
4. Veiligheid van de toeleveringsketen; waaronder zowel de technische als informatie toeleveringsketens	<p>4.1 Wat zijn de belangrijkste problemen, risico's en uitdagingen met betrekking tot de toeleveringsketen in Nederland?</p> <p>4.2 Wat is de omvang en aard van de huidige staat van afhankelijkheden van buitenlandse ICT-voorziening in Nederland?</p> <p>4.3 Hoe kan cyber-weerbaarheid in de toeleveringsketen worden ingebouwd?</p>

Voor elk van de vragen zijn mogelijke methoden en onderzoekbenaderingen aangegeven. De onderzoeksvragen zijn tijdgebonden en zijn mogelijk niet toepasbaar op middellange tot lange termijn (bijv. 24 maanden en nog later), gezien het dynamische cyberecosysteem. De bruikbaarheid van de onderzoeksvragen is contextgebonden met een korte termijn tijdlijn (van circa 0-24 maanden), doordat in deze studie met name urgente onderwerpen zijn geïdentificeerd.

Op basis van de bevindingen in dit rapport worden een aantal onderzoeksvragen voorgesteld die kunnen worden opgenomen in een toekomstige onderzoeksagenda voor de NCTV. Bij elke vraag wordt ook relevante methode en voorlopige onderzoeksopzet aangedragen. Daarnaast bieden we de NCTV een drietal reflecties:

1. Ten eerste zou de NCTV kunnen overwegen een '*bottom-up*'-mechanisme te gebruiken voor de formulering van een toekomstige onderzoeksagenda. Wanneer individuen en organisaties hun onderzoeksideeën kunnen presenteren, kan de NCTV mogelijk flexibeler reageren op nieuwe cybersecurity uitdagingen en kan het zich beter toerusten om hun kennis van het veld te behouden.
2. Ten tweede zou de NCTV ernaar kunnen streven om snel en flexibel te kunnen reageren op uitdagingen en de verantwoordelijkheid op zich te nemen om overheidsoptreden te coördineren voor cybersecurity kwesties waar zich mogelijk risico's voor de nationale veiligheid zouden kunnen ontwikkelen, maar waarbij het niet direct duidelijk is wie er voor de aanpak verantwoordelijk is. Dit is met name van belang voor onderwerpen die mogelijk genegeerd zouden worden als de NCTV geen actie zou ondernemen.

Ten derde zou de NCTV zich ook bewust moeten zijn van cybersecurity kwesties waar aanvullend onderzoek mogelijk niet het antwoord is. Het kan bijvoorbeeld zo zijn dat er goed begrepen wordt wat er dient te gebeuren, maar dat er een gebrek is aan politieke wil, budget of operationeel vermogen om deze maatregelen adequaat te implementeren. Mogelijk zouden dit soort kwesties, die de aandacht van de NCTV verdienen, aangepakt moeten worden buiten de context van een onderzoeksagenda.