Cybersecurity-onderzoek aan universiteiten, wetenschappelijke kennisinstituten en hogescholen

een kwalitatieve en kwantitatieve sterkte-zwakte analyse

Motto: '*When we play together we are really big*!'

Auteurs: Jan Piet Barthel en Floor Frederiks
Met medewerking van: Melanie Lemmen, Annemarie Venemans, Esther Poort, Frans van Steijn

Inhoudsopgave

1. Inleiding en verantwoording

Het Ministerie van Economische Zaken en Klimaat (EZK) heeft NWO en TNO verzocht het nationale kennisaanbod op het terrein van cybersecurity in kaart te brengen (de opdracht is opgenomen als Bijlage 5 bij deze analyse). Dit verzoek vloeit voort uit een Verkenning "Versterking kennis, onderzoek en innovatie", die in september 2018 van start is gegaan. NWO is gevraagd om zich te richten op het kennisaanbod bij universiteiten, wetenschappelijke kennisinstituten en hogescholen, terwijl TNO zich heeft gericht op het eigen aanbod van cybersecuritykennis. Beide analyses gezamenlijk vormen het antwoord op de vraag van het Ministerie van EZK en een beeld van het cybersecurity onderzoek in Nederland. Het kwantificeren en kwalificeren van het Nederlandse onderzoek op het gebied van cybersecurity moet inzicht geven in het aandeel en de relatieve kwaliteit van het Nederlandse cybersecurityonderzoek ten opzichte van de 'rest van de wereld'.

NWO is de Nederlandse Organisatie voor Wetenschappelijke Onderzoek en heeft als hoofdtaak het financieren van wetenschappelijk onderzoek aan Nederlandse publieke onderzoeksinstellingen. NWO richt zich op alle wetenschappelijke disciplines en onderzoeksvelden. De beschikbare middelen worden ingezet via nationale competitie op basis van kwaliteit en onafhankelijke beoordeling- en selectieprocedures. Daarnaast beheert NWO een aantal instituten, met name in de bètawetenschappen, waar wetenschappelijk onderzoek wordt uitgevoerd. Organisatorisch en beheersmatig zijn de financieringsfunctie en de onderzoeksfunctie van NWO van elkaar gescheiden. Deze analyse is uitgevoerd vanuit het NWO-bureau, zonder betrokkenheid vanuit de NWO-instituten (behalve dan waar onderzoekers uit deze instituten zijn geïnterviewd als relevante spelers in het cybersecurity onderzoekslandschap).

Het doel van deze analyse was niet het beoordelen van de kwaliteit van het onderzoek van de individuele onderzoeksgroepen. Externe *peer review* vindt in het academische en hbo-veld over het algemeen plaats langs disciplinaire lijnen. Voor een zeer multidisciplinair vakgebied als cybersecurity betekent dit dat er geen integrale beoordeling van de kwaliteit van de relevante onderzoeksgroepen beschikbaar was. Daarom is er in deze analyse voor gekozen om alle onderzoeksleiders aan hogescholen en universiteiten te interviewen over hun visie op het Nederlandse cybersecurityonderzoek. De geïnterviewden is gevraagd kritisch te reflecteren op a) het eigen onderzoek in het domein van cybersecurity en b) de positionering van Nederland op dit onderzoeksterrein. Tevens is de onderzoekers gevraagd aan te geven wat nodig is om het cybersecurity onderzoeksveld van Nederland te versterken. Deze rapportage is daarmee een zelfanalyse door het veld, waaruit geen harde conclusies kunnen worden getrokken over de kwaliteit van het onderzoek (zoals bij de gebruikelijke evaluaties volgens het SEP-protocol wel het geval is).

NWO heeft de analyse uitgevoerd in nauwe samenwerking met het onafhankelijke evaluatie- en adviesbureau 'De Onderzoekerij'. Dit bureau heeft ruime ervaring met onderwijs- en onderzoeksbeoordelingen. NWO heeft gezorgd voor de benodigde context en de algehele coördinatie van de analyse. Bij de start van de analyse heeft NWO twintig instellingen (waaronder zes hogescholen) geïdentificeerd waar cybersecurityonderzoek wordt gedaan. Bij het identificeren van onderzoeksgroepen is uitdrukkelijk zowel het relevante alfa-, bèta- als gamma-georiënteerd onderzoek in beschouwing genomen, evenals het onderzoek in internationaal samenwerkingsverband. Voorafgaand aan de interviews is alle onderzoeksleiders verzocht een vragenlijst in te vullen voor het kwantitatieve deel van het onderzoek. Deze vragenlijst en de vragen voor de interviews zijn in nauwe afstemming met De Onderzoekerij opgesteld. De interviews, waarin de nadruk lag op de kwalitatieve aspecten, zijn door De Onderzoekerij afgenomen. De interviewers hebben op hoofdlijnen de criteria van het Standard Evaluation Protocol (SEP) gevolgd, te weten kwaliteit, relevantie en levensvatbaarheid van het onderzoek en de opleiding van promovendi. Van brieven en vragenlijsten zijn zowel Nederlandse als Engelse versies ontwikkeld. Een aantal interviews is in het Engels gedaan.

Over de precieze definitie van cybersecurity zijn talloze discussies gaande. Voor deze analyse hanteren we als kader voor het cybersecurity onderzoek in Nederland de Nationale Cyber Security Research Agenda, of kortweg NCSRA[1]. Cybersecurity, privacy en gegevensbescherming maken daar deel van uit. Van deze agenda zijn inmiddels drie edities verschenen. In de achterliggende jaren vormden opeenvolgende edities van de NCSRA steeds het kader voor thematische cybersecurity onderzoeksprogrammering via NWO en SBIR[2] Calls for Proposals.

[1] zie voor de laatste NCSRA-editie: https://www.dcypher.nl/sites/default/files/uploads/documents/NCSRA-III_0.pdf

[2] SBIR = Small Business Innovation Research

2. Kwantitatieve analyse

Voorafgaand aan de interviews heeft NWO de 26 onderzoeksgroepen (verbonden met 20 instellingen) een vragenlijst toegestuurd (Bijlage 1 van deze analyse). De kwantitatieve analyse in dit hoofdstuk is gebaseerd op de ingevulde vragenlijsten. De geselecteerde onderzoeksgroepen hebben aangegeven hoeveel FTE er aan cybersecurityonderzoek besteed wordt. Het gaat daarbij om personele inzet die wordt besteed aan cybersecurityonderzoek dat, ongeacht de financieringsbron, bijdraagt aan de uitvoering van één van de drie NCSRA-edities. Uren besteed aan ander onderzoek, onderwijs of neventaken worden buiten beschouwing gelaten; dit betekent dus dat de inzet van één staflid over het algemeen lager is dan 1 FTE.
De resultaten zijn verzameld in tabellen 1a (WO) en 1b (HBO).

Peildatum: 1 januari 2019

Tabel 1a Personele inzet WO

Vaste staf in FTE	Tijdelijke staf in FTE (excl. PhD's)	Aantal PhD's (werknemers + contract)[3]	Externe PhD's[4]	Vacatures (vast)
32	38	110	39	15

Tabel 1b Personele inzet HBO

Vaste staf in FTE	Tijdelijke staf in FTE (excl. PhD's)	Aantal PhD's (werknemers + contract)	Externe PhD's	Vacatures (vast)
13	6	1	0	3

Als we de universitaire onderzoeksgroepen die zich met de alfa-gamma (met name juridische) kant van cybersecurity bezighouden afsplitsen van de bèta georiënteerde onderzoeksgroepen, ontstaat het volgende beeld (tabellen 1c, 1d):

Tabel 1c Personele inzet WO alfa-gamma

Vaste staf in FTE	Tijdelijke staf in FTE (excl. PhD's)	Aantal PhD's (werknemers + contract)	Externe PhD's	Vacatures (vast)
9	7	13	20	0

Tabel 1d Personele inzet WO bèta

Vaste staf in FTE	Tijdelijke staf in FTE (excl. PhD's)	Aantal PhD's (werknemers + contract)	Externe PhD's	Vacatures (vast)
23	31	97	19	15

Tabel 2 geeft het aantal promoties weer in de afgelopen 4 jaar op onderzoek dat valt binnen de huidige of vorige edities van de NCSRA:

Tabel 2 Cybersecurity promoties

	Aantal cybersecurity promoties in de afgelopen 4 jaar
WO alfa-gamma	8
WO bèta	57
HBO	0

[3] Volgens de definitie van het SEP: "All PhD candidates conducting research with the primary aim/obligation of graduating, based on a 0.8-1.0 FTE contract. This includes PhD candidates with employee status (AiO/promovendi) and contract PhD candidates without employee status, receiving external funding or a university scholarship, who are conducting research under the authority of the research unit with the primary aim of graduating (beurspromovendus)."

[4] Buitenpromovendi

Hierbij moet aangetekend worden dat promotietrajecten in het HBO niet heel gebruikelijk zijn (zie ook tabel 1b); aan hogescholen wordt het onderzoek veelal uitgevoerd door docent-onderzoekers die niet naar een promotie toewerken (of al eerder gepromoveerd zijn). Een totaal aantal promoties van 65 in vier jaar betekent ruwweg de publicatie van 16 proefschriften per jaar, in alle privacy- en cybersecurity-wetenschapsdisciplines in Nederland. Gezien het aantal promovendi dat momenteel een cybersecurity-gerelateerd promotieonderzoek uitvoert, zal dit aantal naar verwachting in de toekomst licht stijgen.

De bevraagde instellingen hebben in de afgelopen jaren drie octrooien en patenten ontvangen op het terrein van cybersecurity. Dat aantal kan uitgroeien tot vijf, want twee patenten zitten nog in het aanvraagproces. Met name op het gebied van cryptografie worden in de academische wereld patenten vermeden, omdat ze als schadelijk worden gezien voor implementatie in de echte wereld. Ook merkte een aantal onderzoekers op dat het aantal onderzoekresultaten dat in de praktijk gebruikt wordt, veelzeggender is dan het aantal patenten dat uit onderzoek voortkomt.

Nederland kent verschillende cybersecurity-opleidingen of opleidingen met een cybersecurityspecialisatie. In tabel 3 worden de opleidingen die tijdens interviews zijn genoemd, weergegeven.

Tabel 3 *Cybersecurity opleidingen in Nederland gerelateerd aan onderzoeksgroepen:*

Opleiding	Instelling	# studenten 2018-2019
Specialisatie cybersecurity binnen Computer Science (WO Master Cybersecurity)	TUD/UT	50
Internationale cybersecurity opleiding	EIT Digital master school (UT)	13
Executive masteropleiding cybersecurity	UL/TUD/HHS	25
Specialisatie cybersecurity in Computer Sciences (Ba)	RUN	80
Specialisatie cybersecurity (Ma) (TRU/e master program)	TUe / RUN	50
Masteropleiding Security and network engineering	UvA	30
Master programma Computer Systems Security	VU	50
Bachelor Security Studies (met verschillende CS-vakken)	UL	250
Master Crisis & Security Management (met verschillende CS-vakken)	UL	300
Law and Technology (Ma): drie cybersecurity gerelateerde vakken: Cybercrime; Capita Selecta Privacy and Data Protection; en Privacy and Data Protection)	TILT	110
Master Internet Law, IP in the Information Society, ICT, Master International technology law (met verschillende CS-vakken)	VU	150
Masteropleiding Cyber Security Engineering	HHS	10
Specialisatie Forensische ICT	HL	150

Naast de opleidingen die in deze tabellen genoemd worden bieden verschillende universiteiten en hogescholen cybersecurityvakken binnen bredere bachelor- en masteropleidingen aan. Ook zijn er meer hogescholen die cybersecurity bacheloronderwijs aanbieden dan in de interviews genoemd zijn. Een volledig overzicht van cybersecurity opleidingen aan universiteiten en hogescholen is te vinden op de dcypher website: https://www.dcypher.nl/opleidingen. Dat overzicht is in samenwerking met de genoemde universiteiten en hogescholen tot stand gekomen.

Een aantal instellingen is voornemens om een nieuwe opleiding op het terrein van cybersecurity te starten. Deze staan weergegeven in tabel 4.

Tabel 4 *Nieuwe Cybersecurity opleidingen (nog te starten):*

Opleiding	Instelling
Bachelor Digital Society	UM
Master van het European Centre on Privacy and Cybersecurity (accreditatie aanvraag zojuist ingediend)	UM
Track Cyber Security Governance in masteropleiding Crisis and Security Management	UL
Master Cyber Safety	NHL Stenden
Bachelor Cyber Security (plan fase)	HR, HHS en HL

Uit bovenstaande tabellen valt op te maken dat het grootste aantal studenten zich bevindt binnen de niet-technische cybersecurity-opleidingen (zo'n 800 van de 1.300 studenten). Ook voor de nieuw op te zetten opleidingen geldt dat deze veelal een sociaal-wetenschappelijke signatuur hebben.

Door de verwevenheid van onderwijs en onderzoek, met name aan academische instellingen maar ook aan hogescholen, vinden onderzoeksresultaten snel hun weg naar het onderwijs. De docenten die de opleidingen bemensen, voeren immers voor het overgrote deel zelf ook onderzoek uit op het terrein van cybersecurity. Kennisdisseminatie vindt allereerst plaats in de kennisinstelling waar deze recente kennis is ontwikkeld. Die kennis sijpelt tevens door in het bredere onderwijscurriculum, bijvoorbeeld in de universitaire masterprogramma's. In dit proces zien we een intra-universitaire vermenigvuldigingsfactor. Eén PhD-project leidt geregeld tot kennisverspreiding onder honderden masterstudenten. Omgekeerd vormen de cybersecurity-opleidingen de kweekvijver voor de onderzoeksgroepen: hieruit recruteren zij talentvolle studenten voor onderzoekstages en promovendi voor promotietrajecten. Een breed palet aan kwalitatief goede opleidingen draagt hiermee bij aan de kwaliteit van het cybersecurityonderzoek in Nederland.[5]

[5] Deze passage is afgeleid uit de brief van dcypher aan de Cyber Security Raad over de "oogst" van opeenvolgende NCSRA-edities, november 2018.

3. Kwalitatieve analyse - onderzoeksveld

De nu volgende hoofdstukken 3, 4, 5 en 6 beschrijven de kwalitatieve analyse, gebaseerd op de interviews met onderzoekers door De Onderzoekerij. Voor zover hieronder conclusies en aanbevelingen worden weergegeven, zijn deze afkomstig van de onderzoekers zelf, gedeeld tijdens de interviews. In hoofdstuk 7 (Conclusies en aanbevelingen) wordt beschreven wat de analyse van NWO is, op basis van alle kwalitatieve en kwantitatieve informatie.

3.1 Onderzoeksgebieden van cybersecurity

Onderstaande tabellen 5a en 5b geven een overzicht van de relevante cybersecurity onderzoeksgroepen in Nederland. Per onderzoeksgroep zijn opgenomen:

- het vakgebied;
- het wetenschapsdomein (bèta of alfa-gamma);
- de onderzoekers die voor deze analyse zijn geïnterviewd;
- de pijler(s) van de NCSRA III waaronder hun onderzoek te scharen valt (de NCSRA kent de volgende pijlers: design, defence, attacks, governance en privacy);
- de specifieke onderzoeksonderwerpen waarmee de betreffende onderzoeksgroep zich bezighoudt.

Een aantal opmerkingen bij deze tabellen:

1. Een belangrijke kanttekening is dat het cybersecurity-onderzoek in veel gevallen slechts een onderdeel vormt van het hele onderzoeksgebied waarin de onderzoekers werkzaam zijn.
2. De onderzoeksonderwerpen passen veelal onder meerdere pijlers van de NCSRA. Een aantal onderzoekers geeft aan dat de subgebieden per pijler niet altijd dekkend zijn en passend bij het onderzoek dat zij uitvoeren. Bij multidisciplinair onderzoek is het aangeven van een NCSRA-pijler minder evident.
3. Opvallend is het lage aantal vrouwelijke hoogleraren en lectoren in cybersecurity. Met name de technische kant, voortkomend uit de informatica, is toch vooral een mannenaangelegenheid.
4. In Bijlage 3 en 4 wordt per onderzoeksgroep een meer uitgebreide beschrijving gegeven van de onderwerpen waar de groep zich mee bezig houdt. Ook is hier informatie te vinden over de omvang van de verschillende groepen. Hierbij is ervoor gekozen om de focus te leggen op het aantal onderzoek-FTE (de capaciteit die per groep kan worden ingezet specifiek voor cybersecurityonderzoek) in plaats van het aantal publicaties.[6]

Tabel 5a WO (groepen zijn alfabetisch gerangschikt)

Onderzoeksgroep	Orientatie	Geïnterviewde	Pijler	Onderwerpen
CWI, cryptologie	bèta	Jos Baeten, Ronald Cramer, Karin Blankers	Design Attacks Privacy	- Cryptologie (o.a. cryptografische protocollen, quantum gebaseerde cryptografie, wiskundige cryptografie at large)
EUR Centre for the Law and Economics of Cyber Security	alfa-gamma	Bernold Nieuwesteeg	Governance	- Regulations, risk analysis and insurance of cybersecurity - Cyber warranties
NSCR, Cluster Cybercrime	alfa-gamma	Catrien Bijleveld Rutger Leukfeldt (tevens HHS) Stijn Ruiter (tevens UU)	Privacy Defence Attacks	- The Human Factor in Cybercrime

[6] In de wetenschappelijke wereld is steeds meer discussie over het gebruik van aantallen publicaties als maat voor onderzoekskwaliteit. Deze gewoonte leidt tot prikkels om zo veel mogelijk te publiceren, iets wat de kwaliteit van het onderzoek niet per se ten goede komt.

OU, onderzoeksgroep security and privacy	bèta	Marko van Eekelen, Harald Vranken	Defence Privacy Deels Design	- Software tools voor security onderwijs - Attribute based security - AI voor security - Privacy engineering and measuring privacy
RU Nijmegen, Digital Cyber Security Group	bèta	Bart Jacobs, Peter Schwabe	Privacy Design Defence Governance	- Real world cryptography - Privacy and Identity management - Systems security and vulnerability analysis
RUG, Information Systems Group	bèta	Fatih Turkmen	Design Privacy	- (Formal) analysis of security systems - Privacy enhancing technologies
TiU, Tilburg Institute for Law, Technology, and Society (TILT)	gamma	Ronald Leenes Bert-Jaap Koops Maša Galič	Privacy Governance	- Wetgeving en beleid rond cybercrime en cybersecurity - Privacy en bescherming van persoonsgegevens
TUD, Techniek, Bestuur en Management, onderzoeksleider (TBM) faculteit elektrotechniek, wiskunde en informatica (EWI)	gamma bèta	Michel van Eeten (TBM) en Inald Lagendijk (EWI) beiden lid van de cybersecurity research group	Design Defence Attacks Governance Privacy	- Cryptografie met focus op toegepaste cryptografie (EWI) - Toepassing AI op gebied van cybersecurity vraagstukken (EWI) - Empirische cybersecurity (TBM)
TU/e, security and embedded networked systems groep	bèta	Sandro Etalle	Defence (beetje attacks, design, privacy)	- netwerk monitoring, situational awareness en specificeren en afdwingen van gebruiksrechten - Threat intelligence en economische aspecten van cybersecurity - Security van Embedded Systemen en IoT security
TU/e, coding theory and cryptography groep	bèta	Tanja Lange	Design Attacks Privacy	- cryptografische bouwblokken (ontwerp, praktische analyse en efficiënte implementatie) incl. post-quantum cryptografie - betrouwbare en privacybeschermende verwerking van gevoelige gegevens, onkloonbare authenticatiemethodes en whitebox cryptografie
UT, Design and Analysis of Communication Systems Group (DACS)	bèta	Aiko Pras	Attacks Defence Design	- Datasecurity - Netwerk security (Focus op DDoS aanvallen)
UT, Services and Cybersecurity (SCS)	bèta	Andreas Peter, Willem Jonker	Desing Attack Defence Privacy	- Ontwerp van ICT systemen die aan privacy en veiligheidsdoelstellingen voldoen

UL, Cybersecurity binnen systeemgroep van LIACS	bèta	Erik van der Kouwe	Defence	- Automatic defence against zero-day attacks - Measuring effectiveness of defences
UL, Cybersecurity Governance	alfa-gamma	Bibi van den Berg	Governance	- Cybersecurity in geopolitiek perspectief: internationale normen voor statelijke actoren - Cybersecurity en nationale veiligheid: wat is de impact van niet-intentionele en accidentele cybersecurity incidenten? - Cybersecurity in organisaties: empirische validatie van cybersecurity awareness programma's - Cybercrime, opsporing versus privacy: data protection versus internationale samenwerking op het terrein van opsporing.
UM, European Centre on Privacy and Cybersecurity (ECPC)	alfa-gamma	Paolo Balboni	Governance Privacy	- Multidisciplinair juridisch en technologisch onderzoek toegepast op cybersecurity vraagstukken
UvA, Instituut voor Informatierecht (IViR)	gamma	Nico van Eijk	Governance Privacy	- Privacy/gegevensbescherming, data-governance, informatieveiligheid (binnen overheid, politie en nationale veiligheid). - Normatieve kaders.
UvA, System and Networking Laboratory	bèta	Cees de Laat	Design Attacks Governance	- Ontwerpen van veilige infrastructuren bouwen: self depending systems, veilig houden van data en security by design.
VU, Systems security	bèta	Herbert Bos	Design Defence Attacks	- Low level systems (o.a. hardware en besturingssystemen) op het gebied van defensieve security, offensieve security en reverse engineering
VU, Center for law and internet	gamma	Arno Lodder	Governance Privacy	- Onderzoek van de normering van nieuwe technologieën vanuit perspectief van gegevensbescherming en privacy

Tabel 5b HBO (groepen zijn alfabetisch gerangschikt)

Onderzoeksgroep	Oriëntatie	Geïnterviewde	Pijler	Onderwerpen
Avans, lectoraat digitalisering en veiligheid	bèta	Ben Kokkeler	Design Defence Governance Privacy	- Impact van digitale technologie in het publieke domein, met focus op veiligheid in de openbare ruimte: smart public safety.

HHS, lectoraat Network and Systems Engineering Cyber Security	bèta	Thomas Quillinan	Design (beetje attacks)	- Identiteit en toegangsmanagement - De beveiliging van systemen en the Internet of Things - Bruikbare beveiliging
HHS, lectoraat Cybersecurity in het MKB	alfa-gamma	Rutger Leukfeldt	Defence Privacy	- Cybersecurity in het MKB
HHS, lectoraat Cybersecurity & Safety	alfa-gamma	Marcel Spruit	Governance	- Governance van cybersecurity - Awareness m.b.t. veiligheid van de cyberwereld - Kwalificatie van professionals in cybersecurity - In kaart brengen van hacktivisme en de geëigende aanpak ervan.
HL, lectoraat Digital Forensics	bèta	Hans Henseler	Attacks	- Open source intelligence - Digital Forensics - E-Discovery
HR, lectoraat Privacy & Cybersecurity	bèta	Mortaza S. Bargh	Design Privacy	- Privacy by design - Security by design
HvA, lectoraat Forensisch onderzoek	alfa-gamma	Christianne de Poot	Attacks Privacy	- Rechercheprocessen - Opsporingsmethoden en bewijsvoering - Vormen van criminaliteit
NHL Stenden, lectoraat Cybersafety	alfa-gamma	Wouter Stol	Defence Attacks Governance	- Digitale weerbaarheid van mens en organisatie - Politie en digitalisering - Bestuurlijke handhaving in een digitale omgeving

3.2 Sterke punten van het onderzoek

Het is lastig gebleken om uit de interviews af te leiden op welke onderzoeksterreinen Nederland bij uitstek vooraanstaand is. De onderzoekers hebben over het algemeen geen concreet antwoord gegeven op deze vraag; men heeft zich beperkt tot een positief beeld van het eigen onderzoek. Het valt op dat (bijna) alle onderzoekers vinden dat ze onderscheidend zijn ten opzichte van andere Nederlandse groepen. Wel wordt een aantal sterktes door meerdere respondenten genoemd, namelijk:

- De toepassingsgerichtheid ofwel toepasbaarheid van het onderzoek, bewustzijn van hoge relevantie voor de maatschappij;
- De multidisciplinaire aanpak/benadering, met de kanttekening dat de niet-technische disciplines hier juist ruimte voor verbetering zien.
- Privacy onderzoek (reden voor de NSF uit de VS destijds om hierin samen met NWO een joint research programma uit te rollen)

Uit de interviews komt naar voren dat Nederlands onderzoek kapitaliseert op de aanwezigheid van een grote internet exchange, een *open access* ambitie en een *non discriminatory* cultuur.

Een andere manier om een beeld te krijgen van de sterktes van het Nederlandse cybersecurityonderzoek, is door te kijken naar verworven subsidies van de *European Research Council* (ERC). Dit zijn zeer prestigieuze, persoonsgebonden Europese beurzen voor wetenschappelijk onderzoek, met een honoreringspercentage van slechts 10-15%. Er bestaan ERC Starting Grants, Consolidator Grants en Advanced Grants, elk gericht op onderzoekers in een andere fase van hun loopbaan. De volgende Nederlandse wetenschappers hebben in de periode 2010-2019 een ERC-beurs verworven met onderzoek dat valt binnen de scope van de NCSRA:

Universiteit, onderzoeksgroep	Onderzoeker	Titel onderzoeksproject	Type subsidie	Jaar
Radboud Universiteit, Digital Security Group	Peter Schwabe	Engineering post-quantum cryptography	Starting	2018
Radboud Universiteit, Digital Security Group	Joan Daemen	Foundations of security in symmetric cryptography	Advanced	2018
Radboud Universiteit, Digital Security Group en Vrije Universiteit Brussel, Law Science and Technology	Mireille Hildebrandt	Counting as a Human Being in Computational Law	Advanced	2018
Radboud Universiteit, Applied Ethics	Tamar Sharon	The Digital Disruption of Health Research and the Common Good. An Empirical-Philosophical Study	Starting	2018
Centrum Wiskunde & Informatica, Cryptology	Ronald Cramer	Algebraic Methods for Stronger Crypto’	Advanced	2017
Radboud Universiteit, Digital Security Group	Bart Jacobs	Quantum computation, logic, and security	Advanced	2012
Centrum Wiskunde & Informatica, Cryptology	Krzysztof Pietrzak (sinds 2011: Institute of Science and Technology Austria)	Provable Security for Physical Cryptography	Starting	2010
Vrije Universiteit Amsterdam, VUSec	Herbert Bos	Rosetta's Way back to the Source - Towards Reverse Engineering of Complex Software	Starting	2010
Universiteit Twente, Formal Methods and Tools Group	Marieke Huisman	Verification of concurrent data structures	Starting	2010

3.3 Knelpunten van het onderzoek

Hoewel onderzoekers enthousiast zijn over hun eigen onderzoek, zijn er ook belemmerende factoren die succesvol onderzoek in de weg staan. De volgende knelpunten worden door onderzoekers genoemd:

- de beschikbaarheid van financiering;
- aantrekken van capabele onderzoekers;
- aandacht voor multidisciplinariteit en niet-technische wetenschappen.

Hieronder worden deze knelpunten nader uitgewerkt.

3.3.1 Financiering

De beschikbaarheid van financiering verschilt erg tussen groepen. Onderzoeksgroepen op hogescholen geven allemaal aan weinig financiering te hebben. Dit heeft te maken met het feit dat er geen menskracht beschikbaar is om subsidieaanvragen in te dienen. Bijkomend probleem is dat hogescholen over het algemeen moeite hebben met het aantrekken van onderzoekers. Blijkbaar geven de schaars beschikbare onderzoekers de voorkeur aan een academische onderzoek omgeving. Ook kleine universitaire onderzoeksgroepen geven aan dat het verwerven van financiering moeilijk is.

Grotere (universitaire) onderzoeksgroepen hebben minder moeite met het verwerven van financiering. Vooral de grotere groepen binnen het universitaire bètadomein lijken gemakkelijker subsidies te verwerven uit de tweede geldstroom. Daarnaast hebben zij ook meer financiering via de derde geldstroom, bijvoorbeeld afkomstig van bedrijven, dan kleinere groepen en hogescholen.

Een onderzoeker geeft aan dat je inventief moet zijn in het zoeken naar financiering omdat het via het huidige onderzoeksfinancieringsmodel in Nederland heel erg moeilijk is om voor subsidies in aanmerking te komen. Uit de interviews komen de volgende oorzaken naar voren:

- Het systeem van onderzoeksfinanciering is zeer competitief en het beschikbare budget is beperkt.
- Het Nederlandse onderzoeksfinancieringsysteem wordt als zeer kwetsbaar ervaren doordat alleen tijdelijk personeel wordt gefinancierd (zie ook onder de paragraaf 'menskracht').
- De verplichting aan consortia om bij onderzoeksvoorstellen private cofinanciering in te brengen is een hindernis, met name voor onderzoekers in het niet bèta-domein. Het is voor hen heel moeilijk om private partners te vinden.
- De criteria bij het beoordelen van aanvragen worden ervaren als conservatief, eerder disciplinair dan multidisciplinair, eerder op het onderzoeksaanbod dan op de maatschappelijke vraag gericht.

3.3.2 Menskracht

Het is voor de onderzoeksgroepen, zowel aan hogescholen als aan academische instellingen, extreem lastig om de juiste mensen te vinden en te houden. Hierboven is al opgemerkt dat hogescholen moeite hebben met het aantrekken van personeel, doordat onderzoekers de voorkeur lijken te geven aan een academische omgeving. De onderzoeksomgeving aan een hogeschool is anders: hogescholen zijn, anders dan universiteiten, in de eerste plaats gericht op onderwijs. Dit heeft logischerwijs consequenties voor ondersteuning en faciliteiten voor onderzoek. Ook zijn onderzoekers over het algemeen zelf opgeleid binnen een academische setting (tijdens hun promotie) en zijn ze mogelijk niet optimaal bekend met het praktijkgerichte onderzoek aan een hogeschool.

Doordat academisch onderzoek binnen Nederland vrijwel uitsluitend op projectbasis wordt gefinancierd, is het Nederlandse onderzoeksysteem kwetsbaar. Instellingen worden geacht hun vaste staf te financieren uit de eerste geldstroom (de rechtstreekse bijdrage van de overheid) en onderzoeksubsidies zijn bedoeld voor het financieren van tijdelijk personeel, zoals promovendi, en materiële kosten. De consequentie hiervan is dat het aantal vaste stafleden bij veel onderzoeksgroepen relatief beperkt is. Daarnaast moeten deze vaste stafleden hun eigen financiering organiseren (en dus veel subsidieaanvragen indienen) om promovendi aan te stellen die de onderzoeksprojecten kunnen uitvoeren. Mede hierdoor wordt het Nederlandse beloningssysteem voor onderzoek door vele academische onderzoekers als slecht ervaren.

De mogelijkheid om betere arbeidsvoorwaarden te bieden, zou kunnen bijdragen aan het aantrekken van academische (top)onderzoekers. Dit betreft niet alleen het eigen salaris maar ook beschikbaarheid van voldoende vaste wetenschappelijke staf/promovendi, basisfinanciering voor onderzoek en/of vrijstelling van allerlei neventaken. In dit verband hebben geïnterviewden herhaaldelijk verwezen naar de Duitse situatie. In de Nederlandse situatie kan een instellingen aan potentiële nieuwe onderzoekers geen aanbiedingen doen van het kaliber als in Duitsland: een eigen instituut met budget en onderzoekers voor een langere termijn. Overigens blijkt uit de interviews dat het ook lastig is om junior en medior onderzoekers aan te trekken. Vanwege de goede arbeidsmarkt voor deze onderzoekers, zijn zij geneigd om naar het bedrijfsleven of naar het buitenland te vertrekken. Voor deze groep speelt ook nog de onzekerheid van tijdelijke aanstellingen voor academici mee.

3.3.3 Aandacht voor multidisciplinariteit en niet-technische disciplines

Hoewel sommige respondenten de multidisciplinariteit van hun onderzoek als sterk punt noemen, hebben verschillende respondenten ook aangegeven dat hier nog veel verbetering mogelijk is. Vooral respondenten die niet in het technische domein werken, gaven aan dat de focus van het Nederlandse onderzoek nog primair op de technische kant ligt en dat de sociale/geesteswetenschappelijke kant wordt onderbelicht. Ook gaven zij aan dat bij subsidieprogramma's de focus vooral op technische aspecten ligt en dat er onvoldoende aandacht is voor juridische en privacyaspecten, terwijl dat voor overheid en beleid relevante factoren zijn. Bovenstaande geldt zowel voor universiteiten als hogescholen. Voor een multidisciplinaire benadering is een verandering in mindset nodig. Bij ieder onderzoek zou ook moeten worden gekeken wat de maatschappelijke, ethische en juridische aspecten hierbij zijn (zoals regelgeving, veiligheid, privacy). Dit gebeurt momenteel nauwelijks. Een extra belemmerende factor hierbij is dat er vooral in disciplinaire tijdschriften wordt gepubliceerd, waar multidisciplinaire publicaties moeilijk een plaats vinden.

3.4 Toekomstplannen

Alle onderzoeksgroepen hebben vooral ambities voor de toekomst op hun eigen onderzoeksgebied. Ook zijn er verschillende respondenten die aangeven dat zij hun onderzoeksdomein willen verbreden zodat zij ook binnen

de onderzoeksgroep meer kennis hebben over aanpalende onderzoeksterreinen (en minder afhankelijk zijn van derden).

Verschillende respondenten geven aan dat het essentieel is om meer vaste permanente staf te verkrijgen en dat dit een belangrijk doel is voor de nabije toekomst. De behoefte aan meer vaste staf komt ook voort uit verkregen onderzoekssubsidies die vaak worden verstrekt voor tijdelijke (promotie-)onderzoekstrajecten. Budgetten voor dit soort trajecten zijn toegenomen, zonder dat budgetten voor vaste staf naar evenredigheid toenemen.

4. Kwalitatieve Analyse - Samenwerkingen

Groepen werken allemaal met anderen samen, nationaal en internationaal, met publieke en private organisaties. Dit zijn over het algemeen geen structurele samenwerkingen maar tijdelijk voor de duur van een project.

4.1 Samenwerkingen met andere onderzoeksinstituten

De meeste onderzoeksgroepen hebben voorkeurspartners, enerzijds door overlap in onderwerpen en anderzijds omdat het onderzoek van de groepen complementair is. Daarnaast zijn verschillende samenwerkingsprojecten/-verbanden genoemd, waaronder het NWO Zwaartekracht Programma Quantum Software Consortium en het Cyber Science Center (HBO). Opvallend is dat het INTERSECT consortium, gehonoreerd in de eerste ronde van het NWA-programma, bestaat uit onderzoekers van universiteiten, hogescholen en TNO naast een flink aantal private- en publieke organisaties. Hier is dus echt sprake van een kennisketenbreed consortium.
Een bijzondere vorm van samenwerken is de personele unie: veel onderzoekers hebben parttime aanstellingen aan andere instituten. Door aanstellingen aan meerdere instituten wordt hun perspectief op het cybersecurity-onderzoek inhoudelijk verbreed.
In verschillende regio's beginnen clusters rondom het thema cybersecurity te ontstaan. Denk aan The Hague Security Delta (HSD) rond Den Haag, AMSec rond Amsterdam en een regionaal cluster in oprichting rond Enschede met de Universiteit Twente als kern. De laatste twee clusters beschouwen zichzelf als voorlopers op clustervorming en regie op nationale schaal.

4.2 Samenwerkingen met bedrijven

Op basis van de interviews is er geen complete lijst samen te stellen van alle samenwerkingen met bedrijven. Een aantal onderzoeksgroepen geeft aan met een enorm aantal bedrijven samen te werken, die niet in één lijst te vangen zijn. Andere groepen hebben alleen de belangrijkste samenwerkingspartners genoemd. Over het algemeen kan gezegd worden dat met name in het bètadomein de samenwerking met bedrijven groot is. Een aantal opmerkingen uit de interviews over de samenwerking met bedrijven:

- We hebben in Nederland een zwakke cultuur wanneer het gaat om samenwerking tussen bedrijven en wetenschap. Bedrijven vragen zich vaak direct af: "what is in it for me?". Dit geldt nog meer voor sociale- en geesteswetenschappen dan voor technische wetenschappen;
- Er zou meer aandacht moeten komen voor valorisatie van onderzoek: stimuleren dat universitair onderzoek ook van meerwaarde is voor Nederlandse bedrijven (en daarmee de Nederlandse economie). Het bedrijfsleven klaagt dat bevindingen uit Nederlands onderzoek niet ten gunste komen van Nederlandse bedrijven. Nu profiteren vooral grote spelers als Apple en Google;
- Gezien het grote aantal kleine bedrijven op dit terrein (veel kleine startups) is het van belang om na te denken hoe kleinere bedrijven kunnen worden meegenomen in gezamenlijke onderzoeksprojecten. Flexibiliteit in het subsidiesysteem kan hieraan bijdragen. Nu gaan veel financieringsvormen uit van een vierjarig commitment van een private cofinancier, een looptijd die voor veel kleine bedrijven niet realistisch is.

Naast bedrijven is samenwerking met publieke instanties (lokaal, nationaal), zoals politie en justitie ook belangrijk. Hoewel cybersecuritykennis en -expertise voor hen vaak onontbeerlijk is voor de uitoefening van hun overheidstaken, hebben zij voor deze samenwerking geen extra middelen beschikbaar. Respondenten stellen voor dat hiermee meer rekening gehouden zou moeten worden in projectfinanciering.

4.3 Internationale samenwerking

Voorkeurslanden om mee samen te werken zijn vooral de Europese landen. Specifiek Duitsland wordt veel genoemd. Bij het aantrekken van PhD-kandidaten richten onderzoekers zich ook het eerste op Europese kandidaten. De meeste onderzoeksgroepen zijn huiverig om samen te werken met landen als China en Iran. Aangegeven wordt dat samenwerking met onderzoekers uit deze landen ook bijna onmogelijk is omdat bedrijven waarmee wordt samengewerkt weigeren met mensen uit deze landen samen te werken. De VS wordt door verschillende onderzoekers als aantrekkelijke samenwerkingspartner genoemd, maar sommige onderzoekers zijn terughoudender geworden over de samenwerking met de VS. Overigens wordt in het geval van samenwerking eerst naar de kwaliteit van de onderzoeksgroep gekeken alvorens naar het land te kijken.

4.4 Landelijke afstemming en coördinatie

Alle geïnterviewden zijn voorstander van gecoördineerde samenwerking in Nederland. Hiervoor worden de volgende redenen opgegeven:

- De kansen op succes bij een gezamenlijke onderzoekssubsidieaanvraag worden groter geacht;
- Er is op dit moment veel versnippering en veel onderzoeksgroepen zijn klein, soms slechts bestaand uit enkele personen. Ook daardoor is er weinig samenhang tussen de verschillende onderzoeksinspanningen, terwijl vaak aan dezelfde problematiek wordt gewerkt, maar dan uit verschillende invalshoeken; men is soms onvoldoende van elkaars werk op de hoogte.
- Meer mogelijkheden om samen te werken met het bedrijfsleven;
- Meer kunnen handelen vanuit een langetermijnperspectief in plaats van uit huidige kortcyclische instrumenten;
- Zonder samenwerking is er veel concurrentie om dezelfde schaarse middelen.

De onderzoeksgroepen zijn tevreden over de rol die dcypher als onafhankelijk platform speelt in het cyber domein. Er is ook tevredenheid over de onderzoeksagenda NCSRA, die onder coördinatie van dcypher tot stand is gekomen.

Op de vraag of in Nederland in de toekomst meer samengewerkt moet worden reageert iedereen positief. Over de manier waarop moet worden samengewerkt verschillen de meningen. Een enkele respondent wil geen nationaal instituut voor cybersecurity onderzoek[7], omdat dat politiek te ingewikkeld is. Cybersecurity is een aandachtspunt voor meerdere departementen, maar onderzoekers ervaren dat de onderlinge samenwerking soms stroef loopt. De meeste respondenten staan echter wel positief tegenover een nationaal instituut of regieorgaan voor cybersecurity. Over de vorm hiervan zijn in de interviews verschillende suggesties gedaan:

1. Oprichting van een virtueel instituut met een centrale administratie. Het instituut moet worden ingericht rondom een aantal thema's. Ieder thema heeft een coördinator. Per thema pak je samen dingen op in plaats van te concurreren. Als je werkt met een aantal thema's (die een aantal jaren lopen) zorgt dit voor meer structuur. De zichtbaarheid en herkenbaarheid worden vergroot, zodat bedrijven en instituten weten wie ze op welk thema moeten aanspreken;
2. "Hub and spokes"-model vanuit Ierland: er is een centrale organisatie (hub) en de "spokes" (spaken) worden thematisch ingevuld (kan op diverse locaties);
3. Binnen een instituut werken met meerjarige programmafinanciering (naar NSF-voorbeeld). De gedachte is dat verschillende coalities van onderzoeksgroepen kunnen concurreren in een soort 'call' waarin gevraagd wordt een centrum/onderzoekslijn rondom dat thema op te zetten;
4. Een fysiek nationaal instituut: één plek waar mensen echt daadwerkelijk samenkomen (en niet virtueel). De beste ideeën ontstaan als mensen bij elkaar zitten. De kracht van wetenschap is dat je over de disciplines heen kijkt;
5. De nationale coördinatie moet bewust ruimte maken voor een goede mix van vrij en thema-gestuurd onderzoek. Daarbij moet strategisch gestuurd worden op wat Nederland als land wil bereiken op cybersecurity gebied. Dit moet in een nieuw, flexibel onafhankelijk orgaan worden ondergebracht.

[7] In november 2017 heeft de Tweede Kamer de motie Verhoeven/Rutte aangenomen. In deze motie wordt de regering verzocht de mogelijkheid te onderzoeken om een instituut voor onderzoek op het gebied van cybersecurity op te richten (Kamerstukken II, 2017/18, 34 775 VI, nr. 68)

5. Kwalitatieve Analyse - Onderwijs

De arbeidsmarkt voor cybersecuritystudenten (wo en hbo) is zeer gunstig. Veel studenten vinden een baan al voordat zij hun diploma op zak hebben. Het gros van de studenten zoekt een baan in het bedrijfsleven, met name om financiële redenen. Het grootste knelpunt binnen het cybersecurity-onderwijs is het vinden van geschikte docenten. De werkdruk is hoog.

Onderzoekers zien verschillende mogelijkheden om het onderwijs te versterken:

- Meer samenwerking zowel voor regulier als postacademisch onderwijs;
- Betere naam geven aan het onderwijs (branding);
- Meer internationale educatie;
- Double degree programma's;
- Scholarships;
- Selectie op kwaliteit van studenten (sommige universitaire studenten zouden beter op een hogeschool passen);
- Meer docenten (vaste aanstellingen) en mogelijkheid om mensen uit bedrijfsleven voor de klas te zetten;
- Ontwikkeling van opleidingen op cybersecuritygebieden die nu nog niet afgedekt worden.

6. Kwalitatieve Analyse – Internationale positionering van het Nederlandse onderzoek

Op de vraag op welke punten (onderzoeksonderwerpen) Nederland sterk is, noemen de meeste respondenten hun eigen vakgebied. Het blijkt moeilijk om daaroverheen te kijken. Verschillende respondenten geven ook aan dat het lastig is om deze vraag vanuit een breder perspectief te beantwoorden, vooral omdat zij andere onderzoeksgebieden onvoldoende kennen. Wel geven verschillende respondenten aan dat Nederland op verschillende deelterreinen sterk is, waarbij zij soms ook specifieke andere onderzoeksgroepen noemen. De onderzoekers geven echter aan Nederland slechts een kleine speler in het veld te vinden: het land is te klein om gewicht in de schaal te leggen maar te groot om te centraliseren. Dat maakt het volgens een onderzoeker op dit moment moeilijk om impact te hebben.

Op de vraag waar Nederland volledige soevereiniteit zou moeten nastreven, geeft slechts een enkeling een specifiek onderwerp. Zo is *identity management* genoemd, waarbij het van belang is aan te sluiten bij nationale cultuur en wetgeving en dus niet zomaar buitenlandse oplossingen kunnen worden geïmporteerd. Ook genoemd werden automatische cyberaanvallen en verdedigingscapaciteit. Verschillende respondenten geven aan dat het vooral van belang is om voldoende kennis en kunde in huis te hebben om de wetenschappelijke kennis op verschillende terreinen toe te passen. Bijvoorbeeld: bij cryptografie worden de wetenschappelijke ontwikkelingen wereldwijd gedeeld (open oplossingen/wereldstandaarden). Zorg ervoor dat je voldoende mensen hebt met kennis en kunde om de Nederlandse overheid te adviseren/ondersteunen.

De NCSRA III is een brede agenda. Bij elke pijler uit de NCSRA III zijn voor digitale soevereiniteit belangwekkende onderwerpen te noemen. De bepaling van een Nederlandse “top 5” vraagt nader overleg tussen het kennisveld, overheid en kennistoepassers en -gebruikers. Uit nadere gesprekken met het kennisveld komt een eerste voorlopig lijstje onderwerpen naar boven als inhoudelijke speerpunten voor Nederland, waar ook industriële belangstelling voor is:

1. Monitoring, detectie en reporting;
2. Identity management en privacy;
3. Security & privacy by design;
4. Vulnerability finding, analysis, and mitigation;
5. IoT security (het onderwerp van het INTERSECT NWA programma)

7. Conclusies en aanbevelingen

Dit is een synthese van het resultaat van de kwantitatieve en kwalitatieve analyses, de context waarin het cybersecurityonderzoek in Nederland plaatsvindt en de reflectie van NWO daarop.

Financiering (hoe het beter kan)

Volgens onderzoekers dient er in Nederland meer aandacht te zijn voor onderzoek naar cybersecurity. Indien de overheid cybersecurity-onderzoek daadwerkelijk als prioriteit beschouwt, is het volgens de onderzoekers van belang om na te denken over de instrumenten voor financiering hiervan. Het bestaande onderzoeks-financieringssysteem op basis van projectfinanciering is dan volgens de onderzoekers niet toereikend. Dit betekent dat het uitbreiden van de permanente staf voor onderzoek én onderwijs noodzakelijk is om de toenemende vraag naar kennis en kunde op het gebied van cybersecurity het hoofd te kunnen bieden. Middelen zijn nodig om vaste staf aan te trekken en toekomstperspectief te bieden. Daar ligt ook een verantwoordelijkheid binnen de onderzoeksinstellingen zelf: zij zijn verantwoordelijk voor het aanstellen van vaste staf vanuit de eerste geldstroom. In dat opzicht is het opvallend dat het monodisciplinaire cybersecurity-onderzoek ontbreekt in de sectorplannen voor de Social Sciences en Humanities (SSH).

Op veel onderwerpen binnen de cybersecurity is samenwerking met publieke partijen van wezenlijk belang. Cybersecurity is immers een thema waar de overheid in het kader van de staatsveiligheid een bijzondere verantwoordelijkheid voor heeft. In toenemende mate worden er publiek-private consortia gevormd die een groot deel van de kennisketen afdekken. In subsidieprogramma's wordt vaak de verplichting opgenomen dat het indienende consortium private cofinanciering inbrengt. Met name voorstellen uit SSH-disciplines kunnen heel moeilijk voldoen aan deze eis. Het is van belang om in de voorwaarden van subsidieprogramma's oog te hebben voor de bijdrage die publieke organisaties kunnen leveren en niet puur te focussen op private cofinanciering.

Als er meer budget beschikbaar zou komen voor cybersecurity, is het essentieel om te bepalen wat de onderzoeksgebieden zijn waar meer kennis en expertise noodzakelijk of gewenst is. Het is belangrijk om fundamentele vragen te stellen in plaats van de waan van de dag van nieuwe technologische ontwikkelingen te volgen. Belangrijk is evenzeer om in het keuze- en prioriteringsproces de juiste partijen te betrekken waarmee in een dialoog die fundamentele vragen geadresseerd kunnen worden. Dit betekent onder meer een vertaling van de beleidsagenda van het Rijk in een kennisontwikkelingsprogramma: denk aan het stellen van onderzoeksprioriteiten afgeleid van digitale soevereiniteitsdoelstellingen.

Samenwerking (in de totale keten van kennisvraag en -aanbod)

Goede samenwerkingsrelaties over de volle breedte van de kennisketen zijn een voorwaarde voor maatschappelijke verankering van nieuwe cybersecuritykennis in Nederland en zijn noodzakelijk voor het op peil houden van onze cybersecurity. Bevorderen van die ketenbrede samenwerking vraagt een flexibel subsidiesysteem: een mix van financieringsinstrumenten voor de korte, middellange en lange termijn. In dit verband moet het SBIR[8]-instrument niet worden vergeten, dat voorziet in aanbestedingen voor middellange termijn onderzoek. Dat geldt ook voor pilots als Scientist on the Job, een instrument voor een kortetermijn-injectie van wetenschappelijke kennis in een onderneming. Dit is in Nederland nog niet aangeslagen, maar wordt in Australië wel succesvol toegepast.

Een zo gewenste optimale aansluiting tussen schakels in de kennisketen vraagt om verbinding tussen kennisaanbod en kennisvraag, zowel met de publieke sector (het Rijk) als met de private sector. Dat laatste betekent de verbinding leggen met brancheverenigingen Cyber Veilig Nederland (CVNL), waarmee vele cybersecuritybedrijven zijn geassocieerd. Ook verbinding met VNO-NCW is van belang, waarbij vele gebruikers van cybersecurity-oplossingen (behoeftestellers) zijn aangesloten, zoals banken, telecombedrijven en energiemaatschappijen. In de separaat door CVNL opgeleverde analyse van de kennisvraag vanuit de cybersecurity sector, staan opties genoemd voor het bijeenbrengen van vraag en aanbod.

De onderzoekers die voor deze analyse zijn gevraagd, zien het grote belang van samenwerking tussen onderzoeksgroepen en zijn van mening dat deze geïntensiveerd zou kunnen worden. Het veld lijkt positief te staan tegenover meer landelijke coördinatie, maar de meningen verschillen over de precieze invulling hiervan.

[8] SBIR = Small Business Innovation Research

Wel staat voor onderzoekers voorop dat de coördinatie op een onafhankelijke manier vormgegeven moet worden.

Ecosysteem (internationaal meer gewicht in de schaal en soevereiniteitskeuzes 'voor Nederland in Europa')
Deze analyse heeft, wellicht door de vorm waarvoor is gekozen, geen specifieke sterktes van het Nederlandse cybersecurity onderzoek aan het licht gebracht. De tabellen 1a en 1b beschouwend, kan geconcludeerd worden dat de nationale cybersecurity onderzoeksgroepen tezamen een omvang hebben van een middelgroot onderzoeksinstituut en het complete spectrum aan cybersecuritydisciplines afdekken. Neem bijvoorbeeld het in 2017 opgerichte Code Research Institute on Cyber Defence uit München, met alleen al 13 cybersecurity hoogleraren en 200 stafleden. Als het gehele Nederlandse cybersecurityveld zich als eenheid positioneert ten opzichte van een dergelijk groot Duits instituut, is sprake van een (enigszins) gelijkwaardige samenwerkingspartner. Overigens zijn er in Duitsland ten minste nog twee van dergelijke cybersecurity-instuten: het Helmholtz Center for Information Security - CISPA in Saarbrücken en het Max Planck Institute for Cyber Security and Privacy Protection in Bochum. Deze overwegingen moeten een rol spelen in de discussie over een cybersecurity-ecosysteem.

Het antwoord op de vraag: '*How to manage distributed knowledge in the Netherlands*?' ligt eigenlijk voor de hand: '*When we play together we are really big*!' Dat betekent grensoverschrijdend denken. Grenzen tussen disciplines en kennisinstellingen, tussen landen binnen en buiten Europa. Dat is waar het ecosysteem over gaat. Een centraal loket is ook vaak genoemd: waar bedrijven de weg gewezen wordt naar kennisinstellingen en via welke onderzoeksgroepen contact leggen met het bedrijfsleven.

Capacity building
Er is een schaarste aan goed opgeleide cybersecurity-experts in alle disciplines, maar aan technisch opgeleide cyber experts in het bijzonder. Uit tabel 3 valt op te maken dat van de ruim 1.300 studenten die momenteel wetenschappelijk onderwijs volgen met ten minste een forse cybersecurity component, de meerderheid (ruim 800 studenten) dit doet vanuit juridisch of sociaal-wetenschappelijk perspectief. Hier lijkt een mismatch te zijn met de behoefte van het onderzoeksveld, dat getuige tabel 1c en 1d met name gericht is op de bèta-technische kant. Het is de vraag of deze discrepantie makkelijk op te lossen is, hoewel de toenemende belangstelling van Nederlandse studenten voor bèta-technische opleidingen kansen lijkt te bieden.

BIJLAGEN

1. Schriftelijke vragenlijst
2. Lijst van geïnterviewde personen
3. Beschrijving van de cybersecurity onderzoeksgroepen WO in NL met hun aandachts-/focusgebieden
4. Beschrijving van de cybersecurity onderzoek lectoraten HBO in NL met hun aandachts-/focusgebieden
5. Opdrachtomschrijving EZK

BIJLAGE 1: Schriftelijke vragenlijst

1a) Naam instituut/onderzoeksgroep waarbinnen het onderzoek wordt uitgevoerd.

1b) Op welke onderzoeksgebieden van cybersecurity bent u actief? Kunt u de bijgevoegde lijst met speerpunten per kennisinstelling waar nodig actualiseren, of als uw instelling ontbreekt, deze toevoegen?
(Zie steekwoordenlijst 19-CSRE-115 en hbo-, wo-overzichten 19-CSRE-093a, b)

2a) Kunt u in onderstaande tabel aangeven hoeveel onderzoeks FTE er binnen uw instituut/onderzoeksgroep aan onderzoek op het gebied van cybersecurity wordt besteed?

N.B. het gaat alleen om personele inzet die daadwerkelijk aan onderzoek op dit gebied wordt besteed. Dat wil zeggen: onderzoek dat ongeacht de financieringsbron bijdraagt aan de uitvoering van één van de drie NCSRA edities. FTE dat aan onderwijs of aan ander onderzoek wordt besteed, dient buiten beschouwing te worden gelaten.

Voorbeeld: een staflid met een voltijdse aanstelling geeft onderwijs (80%) en doet onderzoek (20%). Daarvan is de helft gerelateerd aan cybersecurity onderzoek. Dit staflid wordt voor 0,1 FTE CS onderzoek meegeteld.

Peildatum: 1 januari 2019

Vaste staf in FTE	Tijdelijke staf in FTE (excl. PhD's)	Aantal PhD's (werknemers + contract)[1]	Externe PhD's[2]	Vacatures (vast/tijdelijk)

[1] Volgens de definitie van het SEP: All PhD candidates conducting research with the primary aim/obligation of graduating, based on a 0.8-1.0 FTE contract. This includes PhD candidates with employee status (AiO/promovendi) and contract PhD candidates without employee status, receiving external funding or a university scholarship, who are conducting research under the authority of the research unit with the primary aim of graduating (beurspromovendus).
[2] Buiten promovendi

2b) Hoeveel promoties met als hoofdthema 'cybersecurity', waarbij de hoofdverantwoordelijkheid voor het PhD-traject binnen uw kennisinstelling lag, zijn er in de afgelopen vier jaar geweest?

2c) Verzorgt uw instelling een opleiding op het gebied van cybersecurity (wo masteropleiding of hbo bacheloropleiding)?

- Instelling heeft geen opleiding op dit gebied
- Instelling heeft wel een opleiding op dit gebied:
  - Naam van de opleiding
  - Aantal studenten in 2018-2019

2d) Hoeveel cybersecurity octrooien, patenten zijn er in de afgelopen 4 jaar aan uw instelling verleend?

3) Met welke onderzoeksgroepen werkt u samen op het gebied van cybersecurity onderzoek
a) in Nederland?
b) in internationaal verband?

4) Internationale positionering
a) Op welke onderwerpen heeft Nederland internationaal gezien een sterke positie/ waarin onderscheidt Nederlands cybersecurity onderzoek zich?
b) Op welke onderwerpen heeft Nederland internationaal gezien een zwakke positie?

5) Wat is er nationaal gezien nodig om cybersecurity onderzoek aan de universiteiten en hbo-instellingen in Nederland te versterken?

6) Hoe kijkt u aan tegen de bestaande initiatieven die er zijn om verbindingen te leggen en regie te voeren op het gebied van cybersecurity onderzoek en hoger onderwijs in Nederland? (o.a. dcypher, NCSRA, activiteiten van NWO, betrokken departementen)?

7) Welke wensen en behoeften wilt u ons laten overbrengen aan ‘Den Haag’ (Departementen, NWO, dcypher, etc.)?

BIJLAGE 2: Lijst van geïnterviewden (mondeling/schriftelijk)

WO-instelling	Geïnterviewde
CWI	Jos Baeten, Ronald Cramer
EUR	Bernold Nieuwesteeg
NSCR	Catrien Bijleveld, Stijn Ruiter
OU	Marko van Eekelen, Harald Vranken
RUN	Bart Jacobs, Peter Schwabe
RUG	Fatih Turkmen
TiU	Ronald Leenes, Bert-Jaap Koops, Maša Galič
TUD	Inald Lagendijk, Michel van Eeten
TU/e	Sandro Etalle, Tanja Lange
UT	Aiko Pras, Andreas Peter, Willem Jonker
UvA	Cees de Laat, Nico van Eijk
UL	Bibi van den Berg, Erik van der Kouwe
Univ Maastricht	Paolo Balboni
VU	Herbert Bos, Arno Lodder

HBO-instelling	Geinterviewde
Avans	Ben Kokkeler
HHS	Marcel Spruit, Rutger Leukfeldt, Thomas Quillinan
HL	Hans Henseler
HR	Sunil Choenni, Mortaza S. Bargh
HvA	Christianne de Poot
NHL Stenden	Wouter Stol

BIJLAGE 3: Overzicht van academische onderzoeksgroepen in cybersecurity

Onderzoeksgroepen zijn alfabetisch gerangschikt. Achter de naam van elke groep staan tussen haakjes twee getallen die een maat vormen voor hun relatieve "impact", achtereenvolgens: "onderzoek-FTE in vaste dienst" en "aantal (externe) promovendi".

a. Centrum Wiskunde & Informatica (CWI) Amsterdam (3,8 FTE – 6 promovendi)
De CWI Cryptology groep is wereldwijd één van de leidende onderzoeksgroepen op gebied van cryptologie. De groep richt zich op onderzoek op het gebied van de fundamentele en wiskundige aspecten van de cryptologie. Het onderzoek leidt met regelmaat tot praktische toepassingen of maatschappelijke impact. Het onderzoek van de groep richt zich onder andere op de volgende onderwerpen:

- Quantum-safe cryptografische systemen en standaarden (ontwerp en analyse):
  public-key cryptografie (incl. encryption, signatures, fully homomorphic encryption),
  symmetric-key cryptografie (incl. hash functies, streamciphers)
- Cryptoanalyse van huidige en toekomstige cryptografische systemen en standaarden,
  incl. computational number theory
- Theorie en praktijk van cryptografische protocollen
- In het bijzonder: theorie (CWI) en praktijk (TNO) van secure multiparty computation (MPC):
  Privacy-Protection (o.a. Health, Finance)
- Quantum-gebaseerde cryptografie
- Wiskundige cryptografie at-large

b. Erasmus Universiteit Rotterdam (EUR) (0,6 FTE – 0 promovendi)
Het Centre for the Law and Economics of Cyber Security is het cybersecuritycentrum van de Erasmus Universiteit. De missie is het vergroten van het publieke debat omtrent efficiënte en effectieve cybersecurity investeringen. Het centrum bestudeert in samenwerking met publieke en private actoren de impact van rechtsinstrumenten op de markt voor cybersecurity.
Het centrum is leidend op de volgende onderwerpen:

- Cyberverzekeringen en cyber risk pooling
- Meldplicht datalekken en de AVG
- Systemen voor kennisdeling in cybersecurity
- Rechtseconomische analyse van wetgeving en contracten met betrekking tot cybersecurity

Het centrum **verbindt** de cybersecurityonderzoekers binnen de Erasmus Universiteit, **adviseert** overheden en bedrijven bij strategievorming voor het verbeteren van wetgeving en contracten en **inspireert** door aanwezigheid in diverse publieke fora en media.

c. Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) Amsterdam (0,9 FTE – 1 promovendus)
Het cybersecurity onderzoek binnen het NSCR wordt uitgevoerd binnen het cluster Cybercrime, waarbinnen twee senioren werken, een postdoc, twee PhDs en een junior, een VENI onderzoek wordt uitgevoerd, en waaraan ook een aantal (inter)nationale fellows is verbonden.
Onderwerpen die bestudeerd worden zijn:

- Levenslopen en risicofactoren van daders van cyberdelicten
- Online en offline netwerken van plegers van cybercrime
- Aanpak van cybercriminaliteit

Het NSCR draagt bij aan een cursus Cybercriminaliteit aan de Vrije Universiteit (vakgroep Strafrecht en Criminologie) en verzorgt de summer school cursus Cybercrime & the Human Factor. Binnen Europa is het NSCR trekker van de European Society of Criminology Working Group on Cybercrime.

d. Open Universiteit Nederland (2 FTE – 2 promovendi)
De security & privacy onderzoeksgroep van de Open Universiteit bestaat uit 12 onderzoekers. Haar onderzoek richt zich voornamelijk op:

- Software tools voor ondersteuning van security onderwijs, zoals een distributed virtual computer lab
- Attribute-based security & privacy, zoals privacy-preserving authenticatie en authorisatie

- AI voor security, zoals automatische detectie van botnets en machine-learning voor detectie van software vulnerabilities
- Digital fingerprinting, zoals browser fingerprinting defenses en fingerprinting door smartphone apps

De onderzoeksgroep verzorgt de security vakken in de bachelor Informatica, de master Software Engineering en de master Computer Science. Daarnaast verzorgt de groep ook post-initiëel onderwijs, waaronder de post-initiële opleiding *certified IT security engineer*, zowel on-premise als online, de security componenten in de opleiding *smart services*, en de MOOC *introduction to cryptography*.

e. Radboud Universiteit Nijmegen (RUN) (4 FTE – 21 promovendi)

De volgende gegevens betreffen de Digital Security groep binnen het Institute for Computing and Information Sciences. De groep is internationaal leidend op de volgende onderwerpen:

- Privacybescherming en identity management, inclusief (medische) toepassingen
- Security van kleine apparaten, i.h.b. smart cards en smart phones
- Post quantum cryptografie
- Toegepaste cryptografie en standaarden (met name SHA-3 en AES), en efficiënte en beveiligde implementatie.

De Nijmeegse Digital Security groep van meer dan 50 leden verzorgt sinds 2013 een cybersecurity bachelor opleiding met een jaarlijkse instroom van bijna 100 studenten. Samen met de Technische Universiteit Eindhoven wordt het "TRU/e" cybersecurity master programma verzorgd, waaruit (aan Nijmeegse kant) jaarlijks zo'n 25 afgestudeerden voortkomen. Dit aantal zal de komende jaren toenemen wanneer de sinds 2013 gegroeide bachelor instroom gaat afstuderen.

f. Rijksuniversiteit Groningen (RUG) (0 FTE – 2 promovendi)

Within the Bernoulli Institute of the RUG the Information Systems Group is the principal one conducting research related to cybersecurity. The group has been recently established (2017) and includes expertise in Security/Privacy, Business Process Management and Applied Machine Learning (pattern recognition). The group looks for ways of applying security/privacy technologies to problems in machine learning (and vice versa) and medicine where RUG has a strong presence.

The group performs research on:

- Security infrastructures (authentication, authorization)
- (Formal) analysis of security systems
- Privacy enhancing technologies (applied to machine learning)
- Trust management

g. Tilburg University (TiU) (1,4 FTE – 10 promovendi)

Het Tilburg Institute for Law, Technology, and Society (TILT) is een vooraanstaand internationaal instituut op het snijvlak van recht, regulering en technologie, waarbij cybersecurity een van de speerpunten is. Onderwerpen waar TILT leidend in is:

- Wetgeving en beleid rond cybercrime en cybersecurity
- Privacy en bescherming van persoonsgegevens
- Het snijvlak tussen veiligheid, grondrechten en technologie in concrete sectoren, zoals e-health, energie en robotica

Daarnaast participeert TiU in de Jheronimus Academy of Data Science (JADS), met aandacht voor veiligheid en privacy van data science in zowel onderzoek als onderwijs op Bachelor- en Masterniveau.

h. TU Delft (TUD) - TBM, EWI (3,3 FTE – 23 promovendi)

Faculteiten Techniek, Bestuur en Management en Elektrotechniek, Wiskunde en Informatica.

TUD is gespecialiseerd in empirische cybersecurity: het meten en verbeteren van security in real-world omgevingen. Deze socio-technische benadering is gebaseerd op een intensieve integratie van *hardcore* computer science met economie, econometrie, risicoanalyse, psychologie en recht. Onderwerpen waar TUD leidend in is:

- Economische incentives voor security in online markten, zoals hosting en betaalnetwerken
- Analyse van criminele markten en verdienmodellen en van effectiviteit van interventies tegen cybercrime
- Machine learning op grote datasets van incidenten, vulnerabilities en netwerkverkeer o.a. voor betere detectie en security metrics voor bedrijven.
- Security en Privacy by design.

TUD verzorgt met andere groepen de 4TU masteropleiding cybersecurity. In Delft stromen jaarlijks zo'n 25-30 studenten in dit programma.

i. TU Eindhoven (TU/e) - Ei/Psi (4,2 FTE – 16 promovendi)

Aan de TU/e werken meer dan 30 onderzoekers aan beveiliging in het 'Eindhoven Institute for the Protection of Systems and Information' (Ei/PSI) dat Security (o.l.v. prof. Etalle) en Cryptography (o.l.v. Prof. Lange) groepen samen brengt. De TU/e speelt een internationaal leidende rol in:

- netwerk monitoring, situational awareness en economische aspecten van cybersecurity, specificeren en afdwingen van gebruiksrechten
- cryptografische bouwblokken (ontwerp, praktische analyse en efficiënte implementatie) incl. post-quantum cryptografie
- betrouwbare en privacybeschermende verwerking van gevoelige gegevens, onkloonbare authenticatiemethodes en whitebox cryptografie.

In de bachelor biedt de TU/e twee populaire security specialisatie pakketten aan met elk meer dan 60 studenten. Samen met RUN verzorgt de TU/e het "TRU/e" cybersecurity master programma.

j. TU Twente (UT) - DACS, SCS (2,7 FTE – 21 promovendi)

Design and Analysis of Communication Systems (DACS) en Services and Cyber Security groepen:
Het cybersecurity onderzoek binnen de UT wordt gecoördineerd binnen het Digital Systems Institute (DSI). Onderwerpen waaraan gewerkt worden:

- internet en netwerk security, waarop de UT internationaal leidend is, met een focus op detectie en bescherming tegen Distributed Denial of Service (DDoS) of Domain Name System (DNS) aanvallen.
- security en Privacy by design, inclusief security & privacy engineering, systems security en secure data management
- verificatie en validatie van distributed software, cyber risk management en model checking of cyber physical systems.

De UT participeert in het cybersecurity onderwijs van de 4TUs en het European Institute of Technologies (EIT) en biedt een MOOC aan op het gebied van internet security. De UT coördineert het onderzoek binnen het EU Concordia netwerk.

k. Universiteit van Amsterdam (UvA) - SNE, IViR (1,4 FTE – 9 promovendi)

De System and Network Engineering (SNE) groep onderzoekt internet architecturen en systemen voor gedistribueerde data verwerking, met als kern toegang tot- en veiligheid van netwerk infrastructuren. In combinatie met security gerelateerde onderwerpen voert SNE thans baanbrekend onderzoek uit naar:

- programmeerbare netwerken op globale schaal om cyberaanvallen te detecteren en af te slaan
- multi-domein data infrastructuur methoden gericht op waarborgen van data eigendomsrechten en overeengekomen gebruik
- computationele vertrouwen (trust) modellen, stabiliteit van data marktplaatsen op basis van afspraken en individueel gedrag.

De UvA verzorgt een master Security and Network engineering met hoge rankings en jaarlijks ongeveer 35 studenten aflevert. Voorts verzorgt de groep samen met de VU collega's meerdere vakken in de joint masters programma's.

Het Instituut voor informatierecht (IViR) houdt zich bezig met juridische vragen op het gebied van governance en privacy waarbij cybersecurity een onderwerp kan zijn. Het IViR doet onderzoek naar domeinen zoals vrijheid van meningsuiting, privacy/gegevensbescherming, data-governance, informatieveiligheid (binnen overheid, politie en nationale veiligheid), ofwel de informatie-rechtelijke benadering van cybersecurity. Belangrijk zijn normatieve kaders: hoe ga je als overheid om met dit soort vraagstukken, wat voor toezicht wil je hebben, wil je Europese regels, wat doe je met nationale veiligheid en law enforcement, hoe kijk je aan tegen lokale overheden die zich bezighouden met data en de risico's daarvan?

l. Universiteit Leiden (UL) – LIACS, ISGA (2 FTE- 6 promovendi)

In de cybersecurity groep van het Leiden Institute of Advanced Computer Science (LIACS) wordt onderzoek gedaan naar defenses, in bijzonder automatische bescherming tegen zero-day aanvallen en naar het meten van de effectiviteit van dergelijke defenses.

Binnen het Institute of Security and Global Affairs (ISGA) doet onderzoeksgroep Cyber Security Governance sociaal- en geesteswetenschappelijk onderzoek op het cyberdomein, waar moderne technologie overlapt met traditionele concepten zoals governance, soevereiniteit, handhaving, internationale relaties en conflicten. De groep onderzoekt de impact van cyber op de samenleving, bestudeert hoe complexe cyberonderwerpen gereguleerd (kunnen) worden door verschillende actoren in de publieke, non-gouvernementele en private sector. Sleutelthema's zijn:

- Cybersecurity in geopolitiek perspectief: internationale normen voor statelijke actoren
- Cybersecurity en nationale veiligheid: wat is de impact van niet-intentionele en accidentele cybersecurity incidenten?
- Cybersecurity in organisaties: empirische validatie van cybersecurity awareness programma's
- Cybercrime, opsporing versus privacy: data protection versus internationale samenwerking bij opsporing.

ISGA verzorgt onderwijs in de Bachelor Security Studies, in de Master Crisis & Security Management (vanaf september 2020 met een geheel eigen cybersecurity governance track), en in de eigen Executive Master Cyber Security (samen met de TU Delft en de Haagse Hogeschool).

Het centrum voor recht en digitale technologie van de faculteit rechtsgeleerdheid, eLaw, is een multidisciplinair onderzoeksinstituut gericht op de juridische, ethische, maatschappelijke en technologische aspecten van de regulering van het internet en andere digitale technologieën. Focusgebieden zijn:

- Cybersecurity en cybercrime, gericht op fysieke veiligheid en informatiebeveiliging, maar ook op waarborgen voor fundamentele rechten en vrijheden. Daarbij spelen internet governance en de verantwoordelijkheden van betrokken stakeholders een belangrijke rol.
- Bijdragen van technologie aan preventie, opsporing en vervolging van misdrijven.

eLaw verzorgt een Advanced Master opleiding Law & Digital Technologies en keuzevakken op het terrein van onder meer internetrecht, privacy recht en cybercrime.

m. Universiteit Maastricht – ECPC (1,9 FTE – 0 promovendi)

Focus areas of the European Centre on Privacy and Cybersecurity (ECPC) at Maastricht are legal and organisational aspects of cybersecurity. This makes the ECPC a unique player in the research domain/market on cybersecurity not just in the Netherland but at the European level.

Examples of relevant research activities are:

- Global Dimension of Data Management and Protection, Privacy and Cybersecurity, and Data-Driven Contracts;
- Cybersecurity, Personal Data, and Judicial Independence – the Impact of Data Leaks on Judicial Independence and the Traditionally Conceived of Rights of Victims and the Accused;
- Personal Data Protection and Cybersecurity: How to Effectively Address these Issues in Large Organisations Building on the Concept of "Data Protection by Design as Positive Sum", i.e., Privacy + Security

Examples of relevant teaching activities:

- Advanced Master in Privacy, Cybersecurity, Data Management and Leadership (LLM) - a two-year programme starting in September 2020;
- The courses on "Data Security Management" and "Data Breach Management" in the *Data Protection Officer (DPO) Certification;*
- The course on "Security Risk Assessment and Data Protection by Design in the *Professional Diploma.*

To develop its educational activities (research and teaching) the ECPC can count on a multi-disciplinary team composed by cybersecurity researchers, lawyers and practitioners (consultants and in-house specialists, e.g., CISOs CTOs, CIOs of large organisations).

n. Vrije Universiteit (VU) Amsterdam - CLI, VUSec (3,6 FTE – 32 promovendi)

In 1984 the Center of Law and IT (CLI) started as one of the first centers of this kind in the world. Over the last ten years the focus has been on internet law broadly, and particularly on data protection/privacy, cybersecurity, robot law, AI and e-commerce law. This is reflected in research as well as teaching, with a Dutch master Internet/IP (since 2011), English master International technology law (since 2018), and bachelor minor Law, Ethics & Technology (2017), and courses on cybercrime, emerging technologies, AI, block chain and privacy. Recent Ph.D theses were on Cyberwar (2017) and Privacy and the internet of things (2019). The research output also has societal impact, e.g. being quoted by the EU Court of Justice and the Dutch Supreme Court.

De computer security groep VUSec richt zich als enige in Nederland op computersystemen security, dicht op de bits en bytes, de hardware, compilers, en besturingssystemen. De onderwerpen waarop VUSec internationaal leidend is:

- Geavanceerde exploitatietechnieken in software en hardware en verdediging daartegen (zoals "software hardening")
- Reverse engineering (van malware en goedaardige software), vulnerability finding/fuzzing en automatische exploit generatie
- Operating System Security

De VUSec groep verzorgt samen met de UvA een joint master programma *Computer System Security* die door de studenten als de zwaarste master track binnen computer science wordt beoordeeld. Momenteel schrijven zich rond de 30 studenten in voor deze specialisatie en krijgen daar vakken over de allerlaatste aanvals- en verdedigingstechnieken.

VUSec maakt deel uit van AMSec, het Amsterdam Cyber Security Center, waarin VU, UvA, CWI en NSCR krachten hebben gebundeld.

BIJLAGE 4: Overzicht van cybersecurity onderzoeksgroepen in het HBO

Onderzoeksgroepen zijn alfabetisch gerangschikt. Achter de naam van elke groep staan tussen haakjes twee getallen die een maat vormen voor hun relatieve "impact", achtereenvolgens: "onderzoek-FTE in vaste dienst" en "aantal (externe) promovendi".

a. **Avans Hogeschool** (1,8 FTE – 0 promovendi)

- Lectoraat Digitalisering en Veiligheid Avans Hogeschool
  Ben Kokkeler
  https://www.avans.nl/onderzoek/expertisecentra/veiligheid/lectoraten/digitalisering-en-veiligheid
  Het lectoraat Digitalisering en Veiligheid onderzoekt de impact van digitale technologie in het publieke domein, met focus op veiligheid in de openbare ruimte: smart public safety. Snelle technologische veranderingen bieden kansen voor verbetering van het werk van professionals in het sociale veiligheidsdomein, daagt hen ook uit om hun handelingsrepertoire te verrijken. Met het onderzoek worden praktische toepassingen in 3 clusters uitgewerkt: smart organizations, smart local governance en smart citizens.
- Lectoraat Ondermijning Avans Hogeschool
  Emile Kolthoff
  https://www.avans.nl/onderzoek/expertisecentra/veiligheid/lectoraten/ondermijning
  Het onderzoek is gericht op de mogelijkheden en beperkingen van het recht in relatie tot veiligheidsvraagstukken. Hierbij wordt maatschappelijke veiligheid benaderd vanuit de criminologische invalshoek, maar wordt ook uitdrukkelijk over de grenzen van die discipline heen gekeken. Het lectoraat maakt inzichtelijk hoe **processen en mechanismen van ondermijning** werken.

Andere groepen/onderzoekers binnen Avans die aan cybersecurity werken:

- Colette Cuijpers: lector Recht en digitale technologie aan de Juridische Hogeschool Avans-Fontys. complementair zijn aan elkaar.
- Twee nieuwe lectoren:
  a. Daniel Telgen: Professor Robotization & Sensoring at Avans University of Applied Sciences
  b. Ander de Keijzer: Lector (Professor) Data Science & ICT at Avans University of Applied Sciences

b. **Haagse Hogeschool (HHS)** (2,3 FTE – 0 promovendi)
https://www.dehaagsehogeschool.nl/onderzoek/kenniscentra/coecs

- Lectoraat Cyber Security & Safety Haagse Hogeschool
  Marcel Spruit
  Het onderzoek richt zich op de volgende (multidisciplinaire) thema's:
  1. Governance van cybersecurity in organisaties
  2. Awareness met betrekking tot de veiligheid van de cyberwereld
  3. Kwalificatie van professionals in cybersecurity
  4. Het in kaart brengen van hacktivisme en de geëigende aanpak ervan.
- Lectoraat Cybersecurity in het MKB Haagse Hogeschool
  Rutger Leukfeldt
  Het onderzoek betreft het helpen van het mkb in Nederland om meer digitaal veilig en bewust te worden.
  Het onderzoek richt zich op drie onderzoekslijnen:
  1. weerbaarheid van mkb'ers,
  2. inzicht in cybercriminaliteit en
  3. aanpak van cybercriminaliteit gericht op mkb'ers
- Lectoraat Network and Systems Engineering Cyber Security Haagse Hogeschool
  Thomas Quillinan
  Het onderzoek richt zich op drie hoofdonderwerpen:
  1. Identiteit en toegangsmanagement;
  2. De beveiliging van systemen en the Internet of Things;
  3. Bruikbare beveiliging.

c. **Hogeschool Leiden (HL)** (0,5 FTE – 0 promovendi)

- Lectoraat Digital Forensics Hogeschool Leiden
  Hans Henseler
  https://www.hsleiden.nl/digital-forensics
  Het lectoraat houdt zich bezig met toegepast onderzoek gericht op het werkveld van digitale experts bij politie, opsporingsdiensten en bedrijfsleven (e-discovery). Daarnaast richt het onderzoek zich ook op de toepassing van digital forensics. Bij het zoeken naar sporen in open internetbronnen en in slimme apparaten die onderdeel zijn van het 'Internet of things', waarbij alledaagse voorwerpen zijn verbonden met het netwerk en gegevens kunnen uitwisselen. De resultaten van het toegepast onderzoek vertaalt het lectoraat direct door naar het onderwijs en naar toepassingen voor samenwerkingspartners in het werkveld.

d. **Hogeschool Rotterdam (HR)** (0,5 FTE – 0 promovendi)

- Lectoraat Privacy & Cybersecurity Hogeschool Rotterdam
  Mortaza S. Bargh
  https://www.hogeschoolrotterdam.nl/onderzoek/lectoren/creating-010/lectoren/dr.-ir.-Shoae-Bargh-Mortaza/
  Het onderzoek betreft privacy en security engineering (privacy by design en security by design; het ontwerpen en realiseren van privacybescherming en veilige informatiesystemen), waarbij vanuit een technologische oriëntatie gezocht wordt naar de samenhang tussen privacy en cybersecurity. Daarnaast wordt de verbinding gezocht tussen de benadering van privacy en cybersecurity vanuit zowel het design- als het engineeringsperspectief bij de realisatie van informatiesystemen.
- Lectoraat Future Information & Communication Technology, Hogeschool Rotterdam
  Sunil Choenni
  https://www.hogeschoolrotterdam.nl/onderzoek/lectoren/creating-010/lectoren/dr.-ir.-sunil-choenni/
  Het lectoraat betreft de onderzoekslijn Big Data/Open Data. Hierin hebben blockchaintechnologie (bitcoin), Open Data en analyse van overheidsbestanden de aandacht. Onderzocht wordt hoe het mogelijk is een nieuwe blockchain te laten functioneren vanuit technologisch perspectief.

  Beide lectoren zijn betrokken bij Privacylab010 en houden zich o.a. bezig met **privacy by design**.

e. **Hogeschool van Amsterdam (HvA)** (0 FTE – 0 promovendi)

- Lectoraat Forensisch Onderzoek Hogeschool van Amsterdam
  Christianne de Poot
  http://www.hva.nl/kc-techniek/gedeelde-content/onderzoeksprogrammas/forensisch-onderzoek/over-forensisch-onderzoek.html?origin=w5mvPUssRyKnmJZMLJGAfg
  Het doel van het lectoraat is kennis te ontwikkelen voor de politiepraktijk en het (politie)onderwijs. Het lectoraat Forensisch Onderzoek richt zich niet alleen op de ontwikkeling en het gebruik van nieuwe technologische mogelijkheden in de opsporing, maar ook bijvoorbeeld op de verbinding en informatieoverdrachttussen de tactische en de forensische recherche, de overdracht van informatie uit forensisch onderzoek naar het Openbaar Ministerie en de Zittende Magistratuur en op het theoretisch kader en de wetenschappelijke basis van het forensische onderzoek.

f. **NHL Stenden** (7,8 FTE- 3 promovendi)

- Lectoraat Cybersafety NHL Stenden
  Wouter Stol
  https://www.nhlstenden.com/onderzoek/cybersafety
  De problemen met veiligheid op internet nemen de komende jaren toe, zo is de verwachting. Hoe maken we onze digitale samenleving zo veilig mogelijk? De onderzoeksgroep Cybersafety beantwoordt deze vraag met het doen van hoogwaardig, onafhankelijk en praktijkgericht veiligheidskundig onderzoek en het geven van onderwijs op hbo- en wo-niveau.

- https://cybersciencecenter.nl/
  Het Cyber Science Center is een samenwerkingsverband van NHL Stenden Hogeschool, Politieacademie en Open Universiteit. Het Cyber Science Center is een landelijk initiatief waarbij veiligheidsvraagstukken

rondom digitalisering vanuit verschillende vakgebieden zoals criminologie, computerwetenschap, rechten, psychologie, filosofie en communicatie worden benaderd.
- Lopende onderzoeken: https://cybersciencecenter.nl/onderzoek/

BIJLAGE 5: Opdrachtformulering Sterkte-zwakte analyse kennisveld cybersecurity in Nederland

Inleiding

Afgelopen twee jaar is er door de relevante ministeries op het gebied van cybersecurity, NWO en TNO intensief samengewerkt rond de Maatschappelijke Uitdaging Veilige Samenleving (MU VS) en intussen zijn ook externe verkenners aan de slag geweest teneinde mogelijkheden te verkennen voor versterking van de kennis en innovatieketen voor cybersecurity, de opzet van een Kennis- en Innovatie Agenda daartoe en hoe een langjarige samenwerking, tussen publieke en private partijen, over de hele kennis- en innovatieketen heen kan worden georganiseerd.
Daarnaast is in het kader van de vernieuwing topsectorenbeleid gestart met een missie gedreven aanpak onder andere op veiligheid waar cybersecurity deel van uitmaakt. Onderdeel hiervan is dat de schakels van de innovatieketen op het terrein van cybersecurity goed op elkaar zijn afgestemd. Uitgangspunt is dat, gegeven de beperkte schaal van Nederland, er op nationaal niveau beleidskeuzes binnen het cybersecurity-domein moeten worden gemaakt.
Ter verdere onderbouwing van te maken keuzes is het van belang een kwalitatieve en kwantitatieve analyse te maken van het kennisveld op het gebied van cybersecurity in Nederland (cybersecurity kennis aanbod).

Doel analyse

Het doel is het uitvoeren van een analyse om de Nederlandse excellentie van dit kennisveld te kwantificeren en te kwalificeren. Deze analyse geeft inzicht in het aandeel en de relatieve kwaliteit van de Nederlandse wetenschappelijke kennisontwikkeling in dit domein (relatief ten opzichte van de kennisontwikkeling in de 'rest van de wereld').
Concrete vraagstelling;

- Breng in kaart waar in Nederland (instelling niveau ?) fundamenteel en toegepast onderzoek plaatsvindt. Neem indien mogelijk HBO hierin mee.
    - Betrek hierbij mogelijke regionale verbondenheid met het bedrijfsleven en eventuele economische activiteiten die daaruit voortvloeien.
- Kwantificeer dit onderzoek, in termen van onderzoekscapaciteit en publicaties.
    - Breng daarbij in kaart op welke deelterreinen dit onderzoek plaatsvindt, zo mogelijk naar economisch of maatschappelijk toepassingsgebied.
- Evalueer de opbrengst van deze onderzoeksactiviteiten in kwalitatieve zin. TNO en NWO worden hierbij gevraagd een afgestemde vorm (zelf)evaluatie te hanteren.
    - Geef een kwalitatief (en indien mogelijk gereviewed door een extern panel) beeld over bijvoorbeeld internationale waardering van onderzoeksresultaten, ingeschatte noodzaak tot versterking van de (inter)nationale positie van het vakgebied en relevantie van het onderzoek.
- Betrek in de analyse zowel, alpha, bèta als gamma georiënteerd onderzoek als wel het onderzoek in internationaal samenwerkingsverband.

Opdracht en looptijd

Doelstelling is dat de analyse een belangrijke inhoudelijke bijdrage gaat leveren aan de onderbouwing van beleidskeuzes op het terrein van kennis en innovatie en eventuele financiering door publieke en private partijen daarvan. Afgezien van tussentijdse deliverables dient de geconsolideerde analyse op 1 juni 2019 gereed te zijn.
De opdracht wordt verleend aan de hand van een plan van aanpak voor beide onderdelen van de analyse (NWO en TNO) en de daarbij behorende planning en begroting. In het plan van aanpak wordt onderscheid gemaakt tussen de minimale omvang van de analyse en de ideale, maar niet dwingend noodzakelijke omvang van de analyse ("need to have" en "nice to have").