Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96843
2509 JE Den Haag

www.tno.nl

Ministerie van Economische Zaken en Klimaat
T.a.v. DG Bedrijfsleven en Innovatie
Postbus 20401
2500 EK DEN HAAG

Datum
18 oktober 2019

Onze referentie
2019 SR 53

Retouradres: postbus 96843, 2509 JE Den Haag

Onderwerp
Zelfevaluatie cybersecurity onderzoek TNO-NWO

Geachte heer

Op verzoek van het ministerie van EZK hebben TNO en NWO gezamenlijk een sterkte-zwakte analyse uitgevoerd van het kennisaanbod op het terrein van cybersecurity in Nederland.

Hierbij bieden wij u het resultaat van deze analyse aan. In deze brief lichten wij onze werkwijze en de belangrijkste conclusies en aanbevelingen toe.

Gevolgde werkwijze bij deze analyse
De analyse bestaat uit twee onderdelen: het deel (door NWO uitgevoerd) dat zich richt op het wetenschappelijk en praktijkgericht onderzoek aan universiteiten en hogescholen, en het deel (door TNO uitgevoerd) dat zich richt op het toegepaste onderzoek. Deze twee onderdelen kenden ieder hun eigen aanpak en de uitkomsten zijn als resultaat hiervan verschillend van aard.

- TNO heeft een zelfevaluatie uitgevoerd op haar eigen cybersecurity-onderzoeksactiviteiten en zich hierbij gebaseerd op de *Kennis Positie Audits* (KPA's) die expertisegroepen binnen TNO op reguliere basis uitvoeren. Bij deze KPA's beoordelen externe commissies de zelfevaluaties van de expertisegroepen, hetgeen leidt tot een extern gereviewde score. In het TNO-gedeelte van deze analyse worden kwaliteit, impact en vitaliteit van het cyber-onderzoek afgeleid uit de extern gereviewde KPA scores van betrokken expertisegroepen.
- Voor het NWO-gedeelte van de rapportage, gericht op het onderzoek aan universiteiten en hogescholen, ligt dit anders.[1] Allereerst is NWO een onderzoeksfinancier, en betreft de evaluatie dus niet het eigen onderzoek. Daarnaast is er voor gekozen om alle onderzoeksleiders aan hogescholen en universiteiten te interviewen over hun visie op het Nederlandse cybersecurity-

[1] Externe *peer review* in het academische en hbo-veld vindt 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 is.

onderzoek. Het NWO-gedeelte van de rapportage is daarmee een zelfanalyse door het veld en geen externe beoordeling van de kwaliteit van het onderzoek.

Parallel aan deze sterkte-zwakte analyse heeft TNO op verzoek van EZK tevens een onderzoek uitgevoerd naar het versterken van de cybersecurity-innovatieketen; het betreft het beschrijven en analyseren van de gehele innovatieketen. Onderdeel van dit traject is een patenten- en citatieanalyse van Nederlandse publicaties op het terrein van cybersecurity door het CWTS. Waar relevant, zijn de uitkomsten van deze citatieanalyse betrokken in de conclusies en aanbevelingen hieronder t.a.v. het onderzoek van TNO. De citatieanalyse is minder bruikbaar gebleken voor een beoordeling van het universitaire onderzoek, omdat een groot aantal relevante tijdschriften niet opgenomen was in de database die voor de analyse is gebruikt.

Omvang, kwaliteit en aard van het onderzoek
Onderdeel van deze sterkte-zwakte analyse is een kwantificering van de omvang van het cybersecurity-onderzoeksveld.

Dit levert het volgende beeld op:

- TNO heeft 110 cybersecurity-experts die actief zijn op cybersecurity onderzoek.
- De onderzoekscapaciteit aan de universiteiten bedraagt in totaal 32 FTE aan vaste staf, 38 FTE aan tijdelijke staf en 110 promovendi.
- De onderzoekscapaciteit aan de hogescholen bedraagt in totaal 13 FTE aan vaste staf, 6 FTE aan tijdelijke staf en 1 promovendus.

Hiermee is de totale onderzoekscapaciteit in Nederland bescheiden te noemen, zeker in vergelijking met een land als Duitsland. Als de onderzoekscapaciteit wordt uitgesplitst naar aandachtsgebieden, blijkt het beeld voor de academische instellingen en TNO vergelijkbaar te zijn. Van de vaste stafleden aan de academische instellingen richt 75% zich op de bèta-technische kant van cybersecurity en 25% houdt zich bezig met de sociaal-wetenschappelijke en juridische aspecten (bij de promovendi is de verhouding zelfs 88% vs. 12%). Bij TNO is de personele bezetting ongeveer 70% bèta-technisch van aard en 30% sociaal-wetenschappelijk/ juridisch.

Uit de externe peer review van TNO blijkt dat TNO over de hele linie tenminste nationaal leidend is en ook internationaal erkend in het toegepast onderzoek dat zij uitvoert. Zoals hierboven opgemerkt is het niet mogelijk om directe uitspraken te doen over de kwaliteit van het onderzoek aan hogescholen en universiteiten. Wel komt uit de interviews vanuit het NWO deel een aantal sterke punten van het Nederlandse onderzoek naar voren:

- de toepassingsgerichte insteek van het onderzoek, resulterend in hoge relevantie van de resultaten voor de maatschappij;
- de multidisciplinaire aanpak van het onderzoek, waar mogelijk en van meerwaarde;
- het onderzoek op het terrein van privacy.

Cybersecurity is een vakgebied dat vele (wetenschaps)disciplines doorsnijdt. Een multidisciplinaire benadering heeft vaak meerwaarde, maar ook het monodisciplinaire onderzoek (bijvoorbeeld de juridische aspecten van cybersecurity) is uiterst waardevol. Het zijn juist ook de niet-technische disciplines die in het academische cybersecurityonderzoek nog onderbelicht lijken te zijn. Hoewel de multidisciplinaire insteek van het onderzoek in de NWO-analyse door onderzoekers als sterk punt wordt genoemd, valt tegelijkertijd op dat met name onderzoekers uit de alfa/gamma-hoek van mening zijn dat deze samenwerking nog versterkt zou kunnen worden. Dit lijkt erop te wijzen dat bèta-technische universitaire onderzoekers vooral samenwerken met onderzoekers met een vergelijkbare achtergrond. Binnen TNO werken de verschillende disciplines nagenoeg standaard samen op cybersecurity-onderzoek. Daarbij wordt gewerkt vanuit sterktes op onderwerpen als ‘Monitoring & Detectie, Automated Security, Cyber and Electromagnetic Activities (CEMA), Cyber Workforce Development en Ketenweerbaarheid’. Overall is het beeld dat er in Nederland goed en relevant onderzoek wordt gedaan op het terrein van cybersecurity: de kennisbasis is sterk, hoewel relatief beperkt van omvang.

Samenwerking en impact van het onderzoek
Uit beide analyses blijkt duidelijk dat deze sterke kennisbasis nog niet zo breed ingezet c.q. toegepast wordt als wenselijk zou zijn. Vraag naar en aanbod van cybersecurity-kennis ontmoeten elkaar nog onvoldoende. Voorts blijkt ook het absorptievermogen bij met name overheidsorganisaties niet toereikend te zijn om het onderzoek c.q. de innovaties te implementeren dan wel opvolging te geven. Een nadere analyse wordt gegeven in het onderzoek naar het versterken van de innovatieketen. Ook kan de samenwerking *binnen* het onderzoeksveld nog verder worden versterkt.

Met name uit de NWO-rapportage komt heel sterk de behoefte van het Nederlands cybersecurity onderzoeksveld naar voren om meer als een geheel op te trekken. De beschikbare onderzoekscapaciteit in Nederland is beperkt en zonder goede nationale samenwerking en coördinatie wordt het heel lastig om echt impact te hebben. Het versterken van de nationale samenwerking en regie over de kennisketen zou een van de doelen moeten zijn binnen een nieuw ‘cyber-ecosysteem’. Ook zou betere onderlinge samenwerking moeten leiden tot een betere herkenbaarheid en zichtbaarheid richting het bedrijfsleven en andere betrokken partijen.

Voor veel kennisinstellingen blijkt het lastig om samenwerking met in Nederland gevestigde cybersecurity-technologie bedrijven op een structurele, meerjarige wijze vorm te geven. Samenwerkingen komen overigens wel regelmatig tot stand, maar zijn veelal op ad hoc projectbasis. Deze sector bestaat voor een flink deel uit mkb en startups die weinig middelen beschikbaar hebben om direct en langdurig te investeren in R&D. Dit bemoeilijkt de overdracht van nieuw ontwikkelde kennis naar de Nederlandse markt. Ook hier verwijzen wij voor een nadere analyse naar het onderzoek rond het versterken van de innovatieketen.

Onderzoekers in de sociale en geesteswetenschappelijke hoek ondervinden dat het extreem lastig is om private cofinanciering te vinden voor hun onderzoek.

Op veel cybersecurity-gerelateerde onderwerpen is gelijktijdige samenwerking met zowel publieke als private partijen zeer relevant. In toenemende mate zullen dientengevolge publiek-private consortia worden gevormd die een groot deel van de kennisketen afdekken. Een goed voorbeeld hiervan is het INTERSECT-consortium, dat recent 8,2 M€ financiering heeft verworven in de eerste subsidieronde van het NWA-programma. In dit consortium werken onderzoekers van universiteiten, hogescholen en TNO samen met een groot aantal publieke en private partijen. Het is van belang om in de voorwaarden van subsidieprogramma's oog te hebben voor de bijdrage die publieke organisaties kunnen leveren. NWO werkt op dit moment uit op welke manier zowel private als publieke cofinanciering een plaats kan krijgen in de calls die NWO zal gaan uitvoeren in het kader van het Kennis- en Innovatieconvenant 2020-23.

Vitaliteit en knelpunten
Zowel TNO als de universiteiten en hogescholen geven aan dat het een uitdaging is om (voldoende) gekwalificeerde personeelsleden te werven. Het verloop bij de universiteiten en hogescholen is relatief groot. In mindere mate geldt dit ook voor TNO. Hierbij dient te worden opgemerkt dat de personeelsleden die TNO verlaten over het algemeen beschikbaar blijven voor de Nederlandse arbeidsmarkt.
De universitaire onderzoeksgroepen ervaren dat het lastig is om goede masterstudenten te verleiden tot een promotieonderzoek vanwege de grote vraag naar cybersecurity-geschoolden in het bedrijfsleven, gecombineerd met betere arbeidsvoorwaarden. Ook promovendi die hun universitaire promotie hebben afgerond kiezen veelal voor een loopbaan in het bedrijfsleven; daarnaast zet een deel de academische loopbaan voort in het buitenland. Dit leidt tot zorgen bij de vaste staf over het behouden van wetenschappelijk talent voor de Nederlandse onderzoekswereld.

Een specifiek probleem bij de academische instellingen is dat de projectfinanciering om promovendi aan te stellen in de afgelopen jaren gestegen is, terwijl de vaste formatie niet navenant meegegroeid is. Hierdoor drukt de begeleiding van de promovendi steeds zwaarder op het beperkte aantal stafleden. Dit probleem is overigens niet specifiek voor het cybersecurity-veld, maar manifesteert zich op vele (met name exacte) universitaire onderzoeksterreinen. De universiteiten zijn hier aan zet: om de toenemende vraag naar kennis en kunde op het gebied van cybersecurity het hoofd te kunnen bieden, is versterking van de permanente staf voor onderzoek én onderwijs noodzakelijk. In deze context is het relevant om te noemen dat NWO momenteel, op verzoek van de minister van OCW, samen met de VSNU en de KNAW werkt aan een integraal advies over hoe de druk op het universitaire systeem (waaronder ook de matchingsdruk veroorzaakt door projectfinanciering) kan worden verlicht.

In het studiejaar 2018-19 volgden ruim 1300 studenten een cybersecurity-gerelateerde opleiding aan een wo- of hbo-instelling. Opvallend is dat het grootste deel hiervan (zo'n 800 studenten) zich richtte op de niet-technische kant van cybersecurity. Hoewel deze studenten uiteraard ook zullen doorstromen naar het bedrijfsleven en de publieke sector, lijkt hier een mismatch te zijn qua disciplinaire achtergrond met de maatschappelijke vraagstukken. Dit vormt in potentie een bedreiging voor de toekomstige kwaliteit van het Nederlandse onderzoek. Overigens is er ook buiten onderzoeksinstellingen een grote behoefte aan hoog opgeleide cybersecurity-experts in alle disciplines.

Uitdagingen
De sterkte-zwakte analyse heeft een aantal specifieke onderwerpen geïdentificeerd waar extra inzet geboden is, zoals hierboven uiteen gezet is. Samenvattend zien wij twee grote uitdagingen.

1. De onderzoeks- en opleidingscapaciteit op cybersecurity in Nederland is beperkt, terwijl de vraag naar cybersecuritykennis in de komende jaren zal toenemen. Het is zaak om deze capaciteit te versterken en de samenwerking tussen alle spelers te optimaliseren om zo tot focus en massa in het onderzoek te komen.
2. Er is nog te weinig structureel en meerjarig onderzoek in samenwerking met de bedrijven in Nederland die cybersecurity-technologie ontwikkelen. Het aandeel private financiering voor onderzoek uit deze groep bedrijven is beperkt en overdracht van onderzoeksresultaten naar deze marktgroep daardoor ook niet optimaal. Anderzijds zouden een betere coördinatie en afstemming van het onderzoek tot meer private investeringen kunnen leiden, omdat de behoefte vanuit de markt naar specifieke expertise wel aanwezig is.

Het aanpakken van deze twee uitdagingen moet in onze ogen centraal staan in een toekomstig cybersecurity-ecosysteem. Welke beleidsrichting daarvoor het meest geschikt is, is geen onderdeel geweest van deze inventarisatie. Dit vloeit voort uit het onderzoek naar het versterken van de cybersecurity-innovatieketen dat TNO op verzoek van EZK aan het uitvoeren is.

Tot slot willen wij u nog twee overwegingen meegeven. Ten eerste vormt deze sterkte-zwakte analyse een momentopname, een 'foto'. Als er nieuw beleid wordt ingezet om het Nederlandse ecosysteem te versterken, is het essentieel om een goede integrale monitoring in te richten om te volgen of het beleid de gewenste effecten heeft. Daarnaast achten wij het essentieel dat de overheid en het kennisveld met elkaar in gesprek gaan om te bepalen wat de belangrijke onderzoeksonderwerpen zijn in de komende jaren.

Hoe vertalen de beleidsprioriteiten van de overheid zich in een kennisontwikkelingsprogramma? Op welke terreinen moet Nederland absoluut zelf onderzoek doen en waar werken we samen, en met wie? Wij vragen u om het voortouw te nemen in een dergelijk proces.

Hoogachtend,

Voorzitter NWO Raad van Bestuur

Voorzitter TNO Raad van Bestuur/CEO