Samen cyberveiligheid verhogen

Op 13 november 2018 kwamen zo'n 130 mensen samen in New Babylon in Den Haag voor de matchmakingsbijeenkomst in het kader van een nieuw NWO-programma op het terrein van cybersecurity. De onlangs gelanceerde derde editie van de National Cybersecurity Research Agenda dient als leidraad bij het formuleren van onderzoeksvoorstellen.

Voor deze editie van de nationale onderzoeksagenda hebben we gekozen voor vijf pijlers die iets toevoegen aan het cybersecurityveld

Na een korte uitleg over doel en opzet van het NWO-programma door de opstellers ervan, kreeg hoogleraar Herbert Bos van de Vrije Universiteit Amsterdam als een van de schrijvers van de derde editie van de National Cyber Security Research Agenda (zie kader) het woord. 'Voor deze editie van de nationale onderzoeksagenda hebben we nadrukkelijk niet gekozen voor bepaalde onderzoeksthema's, maar voor vijf pijlers die iets toevoegen aan het cybersecurityveld. Daarnaast hebben we bewust ook meerdere disciplines betrokken bij het opstellen van deze agenda. Zo biedt deze agenda een kapstok voor alle cybersecurity-onderzoek uitdagingen van de verschillende ministeries en van de Nederlandse onderzoeksgroepen op dit terrein.'
Bos benadrukt dat de vijf pijlers niet op zichzelf staan. 'Neem een vraag als: Kunnen we een systeem ontwikkelen dat automatisch aanvallen detecteert en afwendt? Die valt zowel binnen de pijler Aanvallen als binnen Verdediging. Dat soort verbindingen is precies wat we met deze agenda willen bewerkstelligen.'

Meer dan technologie alleen

In dit programma is expliciet ruimte voor samenwerking tussen exacte wetenschappen en de sociale en geesteswetenschappen, iets wat met name tot uitdrukking komt binnen de pijler Governance. Bibi van den Berg, hoogleraar aan de Universiteit Leiden en lid van de Programmaraad van het NWO-programma Maatschappelijk Verantwoord Innoveren: 'De afgelopen jaren is het besef gegroeid dat cybersecurity meer is dan een technologisch vraagstuk alleen. Ook menselijk gedrag, governance en recht maken onderdeel uit van cybersecurity uitdagingen.' Cyberspace is een wereldwijd, grensoverschrijdend fenomeen, vertelt ze. 'Dat leidt tot allerlei uitdagingen, zoals op het terrein van het reguleren van cybercrime. Wiens wil is wet op internet?

Cybersecurity is ook een complex organisatievraagstuk. Bedrijven zitten niet meer in een kasteel met een slotgracht eromheen. Ze zijn steeds meer onderdeel van een netwerk. En dat netwerk is zo veilig als de zwakste schakel. Bij al deze uitdagingen is een terugkerende vraag welke rol een overheid kan en moet spelen om burgers, bedrijven en zichzelf te beschermen tegen cyberaanvallen en uitval van systemen.'

De Governance pijler van de agenda gaat onder andere over dit soort vragen, zegt ze. 'Hoe moet je je organisatie inrichten? Welke rol speelt de interactie tussen mens en technologie in cybersecurity vraagstukken? Wat is de impact van economische factoren? Hoe kun je beleid maken op het gebied van veiligheid in relatie tot cyberspace? Wie is er verantwoordelijk als er iets misgaat? En hoe zit het met ketenverantwoordelijkheid en wet- en regelgeving?'

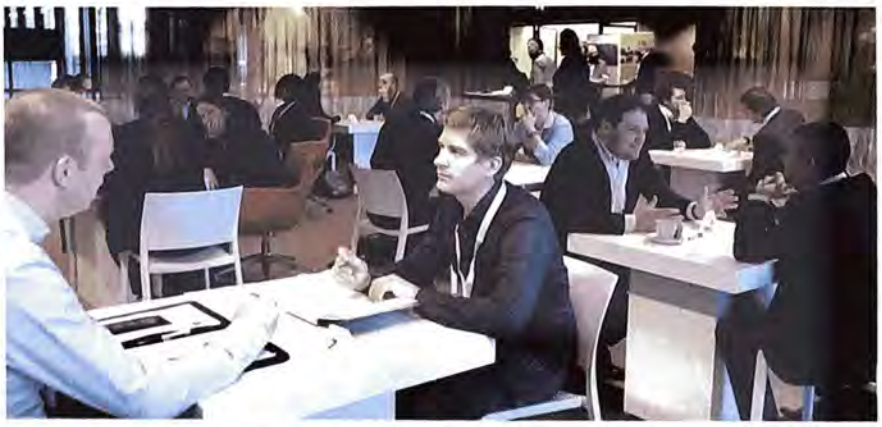
Daarnaast komen er nieuwe problemen op. 'Veel denken is nu nog gericht op de bescherming en veerkracht van data en systemen, maar sinds twee jaar hebben we ook te maken met fake news en desinformatie. Dat is een uitdaging die wij ook zien als cybersecurity vraagstuk. Hoe bescherm je de democratische rechtstaat in tijden van nepnieuws?'

Omdat cybersecurity nog een jong onderzoeksveld is, kunnen onderzoekers er nog veel eigen ideeën in kwijt, denkt Van den Berg. Ze hoopt dan ook dat wetenschappers met verschillende achtergronden samen aan onderwerpen gaan werken die voor alle betrokken disciplines uitdagende vraagstukken bevatten. 'Maar houdt het behapbaar,' waarschuwt ze. 'Probeer in je voorstel duidelijk te maken wat de uitkomst van het onderzoek zal zijn. Welke bijdrage levert het onderzoek? En waarom zou iemand buiten jouw eigen bubbel daarin geïnteresseerd moeten zijn?

Maatwerk in publiek-private samenwerking

Zeker op het gebied van cybersecurity is het van belang in een vroeg stadium bedrijven bij het onderzoek te betrekken. Dat is niet altijd makkelijk, weet ook Petra Oldengarm, directeur van Cyberveilig Nederland. Deze nieuwe brancheorganisatie voor cybersecuritydienstverleners is in mei 2018 opgericht en vertegenwoordigt inmiddels al bijna veertig bedrijven.

'Door onderzoeksfinanciers wordt nogal makkelijk gedacht in one size fits all-oplossingen voor publiek-private samenwerkingen. Maar de meest gekozen oplossing, waarbij bedrijven verplicht niet alleen *in kind* maar ook *in cash* moeten bijdragen, en projecten vaak vier jaar of nog langer duren, past niet bij mijn achterban. De meeste Nederlandse cybersecuritybedrijven zijn beperkt in omvang, hebben geen researchafdeling, zijn vaak nog jong, en volop aan het groeien. Daardoor is het voor hen vele malen makkelijker om *in kind* bij te dragen dan *in cash*.'



De matchmakingsbijeenkomst in november bood onderzoekers en bedrijven een kans om elkaar te leren kennen.

National Cyber Security Research Agenda

Op 5 juni 2018 lanceerde dcypher de derde editie van de National Cyber Security Research Agenda (NCSRA-III). Mark Bressers nam namens Mona Keijzer, staatssecretaris van het Ministerie van Economische Zaken en Klimaat, het eerste exemplaar van de agenda in ontvangst uit handen van een vertegenwoordiging van het schrijfteam, bestaande uit Herbert Bos, Michel van Eeten, Sandro Etalle, Frank Fransen, Jaap Henk Hoepman, Erik Poll en Jan Piet Barthel.
De agenda is tot stand gekomen na vele consultaties met vertegenwoordigers van het onderzoeksveld, de topsectoren en de routes uit de Nationale Wetenschapsagenda. De agenda is opgebouwd uit vijf pijlers, te weten: Ontwerp, Verdediging, Aanvallen, Governance en Privacy.

Cyberveilig Nederland is in zeker zin ook te vergelijken met zo'n klein, startend bedrijf. 'Waar andere brancheorganisaties actief zijn in delen van de cybersecuritysector, vertegenwoordigen wij de hele sector. We waren dus vanzelfsprekend betrokken bij de formulering van de NCSRA-III. Want hoewel lang niet elk bedrijf tijd of geld heeft om daadwerkelijk bij te dragen aan onderzoeksprojecten, heeft de sector als geheel absoluut baat bij de resultaten van wetenschappelijk onderzoek. Daarnaast zitten we te springen om goed opgeleid personeel. In dat verband zijn initiatieven als de summerschool die dcypher jaarlijks organiseert voor onze leden heel interessant.'

Oldengarm ziet voldoende mogelijkheden voor nuttige samenwerkingen. 'Voor bedrijven is er een duidelijke toegevoegde waarde zodra wetenschappers een >

Laat bedrijven deel uitmaken van bredere consortia, zodat ze ook van elkaar kunnen leren

Petra Oldengarm

aanpak ontwikkelen waar een bedrijf nog even geen prioriteit aan kan geven. Zo hoorde ik tijdens de bijeenkomst over een nieuwe manier om aan de hand van karakteristieken van een aanval de handtekening van een aanvaller te detecteren. Daarmee kun je niet alleen die ene aanval afweren, maar de aanvaller ook voor de toekomst uitschakelen. Dat is nuttig, en iets wat individuele bedrijven over het algemeen niet meteen zelf kunnen ontwikkelen.'

Oldengarm pleit voor vernieuwende vormen van publiek- private samenwerking. 'Laat bedrijven een werkplek aanbieden aan promovendi, zodat zij beter begrijpen wat er in de alledaagse praktijk speelt, en kunnen bijdragen aan werkbare oplossingen. En laat bedrijven deel uitmaken van bredere consortia, zodat ze ook van elkaar kunnen leren.'

De matchmakingsbijeenkomst in november bood onderzoekers en bedrijven een kans om elkaar te leren kennen. Van den Berg: 'dcypher is er de afgelopen jaren op verschillende manieren in geslaagd om heel diverse gemeenschappen met elkaar in contact te brengen. Dat begint nu langzaam zijn vruchten af te werpen." •

Onderzoeksrondes

Cybersecurity - Digitale Veiligheid & Privacy

De Call for Proposals Digitale Veiligheid & Privacy, gebaseerd op de NCSRA-III, is een gezamenlijk initiatief van de NWO domeinen Exacte en Natuurwetenschappen (ENW) en Sociale en Geesteswetenschappen (SGW), alsmede het Nationaal Regieorgaan voor Praktijkgericht Onderzoek SIA (Regieorgaan SIA). De betrokken inhoudelijke partners zijn dcypher, Commit2Data, Sociale Infrastructuur Agenda, en de TKI CLICKNL.
Er is ruim vijf miljoen euro beschikbaar voor onderzoeksprojecten die gericht zijn op resultaten die zowel bijdragen aan de kennisbasis binnen cybersecurity, als op relatief korte termijn toepasbaar zijn bij de maatschappelijke en private partners binnen de projecten. Honoreringen kunnen naar verwachting op 3 december 2019 bekend gemaakt worden.

Nationale Wetenschapsagenda

De Nationale Wetenschapsagenda (NWA) komt voort uit de Wetenschapsvisie 2025. Door vragen van Nederlandse burgers aan de wetenschap zijn 25 routes getrokken. Deze routes identificeren de terreinen waarop de Nederlandse wetenschap bij uitstek het verschil kan maken. Het NWA-programma voorziet in jaarlijkse subsidierondes ter financiering van onderzoek langs twee actielijnen:
1. Ketenbrede consortia binnen alle routes;
2. Thematische samenwerking door vakdepartementen.
Voor de ronde 2018-2019 is binnen actielijn 1 een breed gedragen cybersecurity onderzoeksvoorstel ingediend. Binnen actielijn 2 werken acht ministeries samen aan de inrichting van een cybersecurity programma. NWO ontwikkelt de daarbij behorende call for proposals in afstemming met het veld en dcypher. Ook voor de ronde 2019-2020 hebben de op het thema cybersecurity samenwerkende ministeries een programma-voorstel ingediend.