Behoud en Versterking Nederlandse Cybersecurity Capaciteit

De noodzaak tot Nederlandse zelfredzaamheid gebaseerd op de nationale behoefte aan eigen hoogwaardige expertise, via kennisontwikkeling en circulatie

Herbert Bos, Michel van Eeten, Bart Jacobs
vanuit dcypher.nl
v1.6, concept 23 november 2017

Braindrain en verlies van soevereiniteit

Terwijl de Nederlandse regering extra geld toewijst aan cybersecurity, dalen de investeringen in cybersecurity-onderzoek al jaren. Ondertussen zijn de regeringen van de ons omringende landen begonnen met een investeringsoffensief in cybersecurity-onderzoek. Deze initiatieven zijn met name ook gericht op het organiseren en versterken van academische capaciteit. Het duidelijkste voorbeeld is Duitsland, waar recent een Helmholtz Center voor cybersecurity wordt neergezet met € 50 miljoen jaarlijkse vaste financiering[1]. Over 2 tot 3 jaar zullen er bij dat ene center meer hoogleraren in cybersecurity werken dan nu in heel Nederland.

Het Helmholtz Center is slechts een van de initiatieven die Duitsland momenteel neemt op het gebied van cybersecurity. Daarnaast is er ook nog het Center for Advanced Security Research Darmstadt CASED en de uitbreiding van het CODE Research Centrum in München[2]. In november wordt een besluit genomen over de locatie van het nieuw op te richten Max Planck Instituut voor cybersecurity. Dit komt of in Darmstadt, of in Bochum (net over de grens). Hier zal jaarlijks zo'n € 10 miljoen naartoe gaan. Het Verenigd Koninkrijk, Frankrijk en Luxemburg volgen de Duitse strategie.

Voor deze buitenlandse academische instituten is veel nieuw hoogopgeleid personeel nodig, dat in de vestigingslanden zelf, net als in Nederland, maar in beperkte mate voorhanden is. De academische wereld is internationaal georiënteerd. Deze instituten zijn nu reeds begonnen met werving, nadrukkelijk ook onder medewerkers van Nederlandse universiteiten. Wanneer toonaangevende Nederlandse hoogleraren cybersecurity een aantrekkelijk aanbod van zo'n instituut accepteren heeft Nederland een serieus probleem. Dit is geen onrealistisch scenario: eerder dit jaar werd bekend dat Nederland's meest geciteerde informaticus Wil van der Aalst een aanbod geaccepteerd heeft om over te stappen naar Aken, om daar met een startkapitaal van € 5 miljoen en (een deel van) zijn huidige Eindhovense groep een nieuwe eigen onderzoekslijn op te zetten.

Het probleem speelt niet op het niveau van hoogleraren, maar over de hele linie. Nog een voorbeeld. De Nijmeegse universitair docent Peter Schwabe is het afgelopen jaar overladen met

[1] De Duitse regering kondigde in het voorjaar de oprichting aan van het Helmholtz Center for Cybersecurity Research (Forschungszentrum für IT-Sicherheit) in Saarbruecken. Zie: https://www.saarland.de/222685.htm en/of https://www.saarland.de/dokumente/thema_innovation/2017-03-14_41_Forschungszentrum_fuer_IT-Sicherheit_EN.pdf. Met de volgende wervende tekst wordt toponderzoekers gewezen op de vacaturelijst in Saarbruecken: "Helmholtz is the largest science organization in Germany. Helmholtz Centers are the largest research investment possible in Germany, fully committed to scientific excellence, and with truly exhaustive, permanent base funding of more than 50 Mio. Euro annually. We will thus grow to at least 500 full-time researchers from base funding, including a huge number (60+) of new permanent faculty. And presumably rather double the size on the long run, if we take any form of third-party funding and increase of the base budget into account. This will turn us into one of, maybe even the, largest cybersecurity research center in the world. A truly unique investment by the German government."

[2] https://www.unibw.de/willkommen/startseite-meldungen/groesstes-forschungszentrum-fuer-cyber-entsteht

prijzen[3]. Hij is wereldleider op het strategische gebied van post quantum crypto, waar de Nederlandse overheid (i.h.b. de AIVD) groot belang aan hecht. Aan de VU in Amsterdam sleepte Cristiano Giuffrida de afgelopen jaren de ene prestigieuze prijs na de andere binnen[4] en was over 2016 volgens de *Computer Science Rankings*[5] de nummer twee van de wereld in Computer Systems Security (gemeten naar het aantal toppublicaties). Hij is een toponderzoeker op het gebied van hacken, *zero-days*, en automatische exploit generation — kennisgebieden die van strategisch belang zijn voor Nederland. Er is inmiddels aan hem getrokken door het Helmholtz Center. Laatste voorbeeld: het verschil in investeringen belemmert ook het aantrekken van nieuw talent in Nederland. Stjepan Picek is afkomstig van het MIT en is net begonnen als universitair docent aan de TU Delft. Tot zijn grote verbazing is er geen enkele open call van onderzoeksfinancier NWO in cybersecurity om promovendi te financieren. Zelfs in Kroatië, zijn thuisland, is er meer geld beschikbaar. Wat zullen Schwabe, Giuffrida en Picek doen met een *offer they cannot refuse*, zoals een hoogleraarschap aan een topinstituut met een eigen start-budget?

Het pijnlijke verschil in investering tussen Nederland en de buurlanden, verslechtert het klimaat in alle Nederlandse academische topgroepen in cybersecurity. Er dreigt een braindrain die de kwaliteit van Nederlandse expertise uitholt. Dat heeft niet alleen gevolgen voor de kwaliteit van Nederlandse opleidingen en innovatie, maar ondermijnt ook de soevereiniteit van Nederland om eigen keuzes te maken en zelfredzaam te zijn op het gebied van cybersecurity.

Wat doet Nederland?

Het korte antwoord: nagenoeg niets. Al sinds 2014 (!) is er geen nationale cybersecurity call-for-proposals van NWO meer geweest. De afgelopen jaren is de investering in cybersecurity onderzoek steeds verder teruggelopen, tot onder € 1 miljoen per jaar. Ter vergelijking: dat is minder dan 2% van de investering die Duitsland doet. Zeker, de Nederlandse economie is kleiner dan de Duitse, maar afgemeten aan de verhouding tussen beide economieën zou *het Nederlandse investeringsniveau zeker een factor 10 hoger moeten liggen dan het nu ligt*.

Er komt vermoedelijk in 2018 een nieuwe nationale cybersecurity call, maar die zal hooguit in de orde van € 2-3 miljoen bedragen, verdeeld over enkele jaren. Daarmee blijft het investeringsniveau op het huidige lage peil. Het is *too little, too late*. Voor het goede begrip: het uitdenken en schrijven van onderzoekvoorstellen vergt veel voorbereidingstijd en heeft in Nederland een lage honoreringskans van 5-20%. Dit vormt een pijnlijk contrast met de omvangrijke initiële budgetten die bij aanstellingen in het buitenland zonder moeizame procedures beschikbaar gesteld worden.

In de laatste miljoenennota van het kabinet Rutte II wordt € 26 miljoen uitgetrokken voor cybersecurity. Maar helemaal niets hiervan is bedoeld voor onderzoek en wetenschappelijke expertise. Alles wordt besteed aan versterking van de capaciteit van de overheid, bij de politie, inlichtingendiensten en defensie. Wie leidt die experts op die de overheid gaat werven met dat extra geld? In het regeerakkoord van het nieuwe kabinet Rutte III wordt (vanaf 2019) een extra € 69 miljoen voor dit doel begroot. Hoeveel daarvan daadwerkelijk voor onderzoek bestemd is, is vooralsnog onbekend, maar het gaat hooguit om een klein aandeel.

---

[3] Bijvoorbeeld de Nederlandse prijs voor ICT-onderzoek in 2017 en in 2016 de Internet Defense Prize van Facebook, voor het nieuwe beveiligingsalgorithme New Hope dat bestand is tegen quantum berekeningen, ontwikkeld samen met collega's Alkim, Ducas en Pöppelmann.

[4] Bijvoorbeeld de Roger Needham en Dennis Ritchie prijzen voor het beste proefschrift in computersystemen in Europa, en de hele wereld, respectievelijk. Ook won hij drie van de vier Pwnie Awards (vaak omschreven als "the hacker's community's oscars") die ooit aan onderzoekers in Nederland zijn toegekend.

[5] http://csrankings.org/

Strategisch belang van eigen cybersecurity kennis

In het algemeen geldt: de eigen beveiliging moet je vooral zelf doen. Natuurlijk zijn coalities belangrijk, maar juist op het gebied van beveiliging is soevereiniteit en autonome belangenafweging, gebaseerd op kennis van zaken, van groot belang. Moderne gedigitaliseerde samenlevingen zijn kwetsbaar door hun grootschalige gebruik van ICT, voor de meest essentiële processen (waaronder communicatie, vervoer, aansturing en bestuur), zoals de afgelopen jaren herhaaldelijk gebleken is. Het is daarom van strategisch belang dat Nederland een eigen kennispositie heeft en behoudt op het hoogste niveau, en zelf in staat is, en ook de capaciteit heeft, om nieuwe generaties van cybersecurity experts op te leiden.

Hoe ziet het veld eruit?

Nederland heeft een aantal cybersecurity centra voor academisch onderwijs en onderzoek, geconcentreerd in Amsterdam, Delft, Eindhoven, Nijmegen en Twente. In de bijlage worden hun specialisaties kort beschreven. Deze centra zijn de grote leveranciers van hoog gekwalificeerd personeel aan de Nederlandse overheid en ook aan cybersecurity industrie. Er bestaan veel, vooral bilaterale contacten, tussen universiteiten en het bedrijfsleven en de overheid. Het onderwerp cybersecurity wordt intrinsiek gekenmerkt door scherpe onderlinge verhoudingen, waarbij men elkaar kritisch de maat neemt en fouten of zwakheden hardop benoemt, omwille van het hogere doel van betere beveiliging. Er is in dit veld dus geen sprake van een topsector-achtige warme deken waaronder iedereen gezellig samen ligt. Er is juist sprake van verschillende inzichten en opvattingen – bijvoorbeeld over het belang van privacy of over de rol van Snowden – die tot voortdurende discussies en verbeteringen leiden. Het cybersecurity veld is er juist bij gebaat dat de neuzen verschillende kanten op staan, zodat tegendraadse denkers de ruimte krijgen en kunnen wijzen op gevaren en aanvalsmogelijkheden waar anderen niet aan denken.

Wat kan Nederland doen? Kennis en circulatie!

Omwille van het behoud en versterking van de Nederlandse kennispositie m.b.t. cybersecurity worden in deze tekst twee voorstellen geschetst die elkaar onderling versterken. Deze voorstellen worden aangeduid met *kennis* en *circulatie.* Het eerste ‘kennis’ voorstel is vooral academisch georiënteerd, en richt zich op versterking van het cybersecurity onderwijs en onderzoek aan de universiteiten. Het tweede ‘circulatie’ voorstel richt zich op de operationele cybersecurity wereld bij de overheid en het bedrijfsleven, via het oprichten van een *pool* van experts die de mogelijkheid krijgen om makkelijk heen en weer te bewegen tussen overheid, bedrijfsleven en universiteiten (in wat wel de triple helix genoemd wordt).

De cybersecurity industrie groeit met circa 2.500 fte per jaar (VKA analyse[6]). Dat is in lijn met het rapport Verhagen[9]: 10% van de ICT banengroei, die geschat is op 25.000 fte. Van deze instroom zijn jaarlijks zeker 25 (1%) PhD’s met topkennis in cybersecurity nodig. Niet alleen worden er te weinig PhD’s geleverd voor de arbeidsmarkt, de braindrain trekt ook nog eens de senior onderzoekers weg die de nieuwe PhD’s moeten opleiden, alsook de andere vormen van hoger onderwijs verzorgen. Het tekort aan experts voor onderzoek, onderwijs en publieke en private ondernemingen zal dus in hoog tempo gaan oplopen.

De slotsom is duidelijk: als de Nederlandse overheid investeert in de cybersecuritycapaciteit van Nederland, dan dienen de investeringen in cybersecurity-onderzoek gelijke tred te houden. De neerwaartse spiraal moet doorbroken worden en er moet een antwoord komen op de braindrain. De huidige voornemens voldoen daartoe niet.

[6] Economische Kansen Nederlandse Cybersecurity-Sector, een verkenning door VKA in opdracht van het ministerie van EZ.

Als Nederland structureel gemiddeld 25 PhD's wil opleiden per jaar, dan dient er een kennisprogramma te komen waarvoor aan de overheid en NWO een **structurele financiering van € 6 miljoen per jaar** gevraagd wordt, en dus van € 60 miljoen voor een periode van 10 jaar. De middelen hiervoor zijn er. Naast de investering in cybersecurity capaciteit van de overheid zelf, heeft het ministerie van EZK een programma van € 200 miljoen voor kennis en innovatie, heeft het ministerie van OCW € 50 miljoen beschikbaar voor de Nationale Wetenschap Agenda, waarin tenminste voor drie 'routes' cybersecurity uitdagingen worden geagendeerd[7], heeft de Directie Cybersecurity van het ministerie van J&V geld voor onderzoek beschikbaar, net als het Cyber Commando van het ministerie van Defensie, en heeft NWO cybersecurity al jaren als speerpunt aangewezen. Deze partijen zijn gezamenlijk in staat om de braindrain en het verlies aan soevereiniteit te stuiten met een structurele investering.

Het tweede onderdeel, circulatie, vereist een fonds dat gevuld wordt door de operationele partijen die hier aan deelnemen.

Voorstel I: kennis

Het onderwijs en onderzoek aan de Nederlandse universiteiten wordt gedaan door een combinatie van vast en tijdelijk personeel. Sommige posities zijn per definitie tijdelijk, zoals een 4-jarige promotie plaats voor een 'AiO' (assistent in opleiding, PhD in het engels) of een 'postdoc' plaats voor een pas gepromoveerde onderzoeker (typisch tussen 1 en 5 jaar). Deze tijdelijke posities zijn bijna altijd extern gefinancierd, op basis van een onderzoekvoorstel dat, na een open competitie, betaald wordt door een onderzoeksfinancier (tweede geldstroom), zoals bijvoorbeeld NWO (domein ENW, TTW en/of SGW), of ERC of Horizon2020[8], of soms ook rechtstreeks door een bedrijf (derde geldstroom). Het is aan de vaste staf om dit soort onderzoeksvoorstellen te schrijven en in te dienen. Zoals reeds genoemd, de succespercentages zijn laag en liggen, enigszins afhankelijk van de financieringsbron, typisch tussen de 5 en 20%. Het onderwijs wordt grotendeels door de vaste staf gegeven, waarbij de tijdelijke medewerkers een beperkte ondersteunende rol hebben, bijvoorbeeld bij het geven van werkcolleges. Door de zware belasting van de vaste staf wordt veel van het onderzoek de facto door tijdelijke medewerkers gedaan.

De onderstaande punten zijn erop gericht om het onderzoek en onderwijs in de cybersecurity uit te breiden en het perspectief voor succesvolle vaste stafleden te verbeteren. Dat laatste moet het academische werk in Nederland aantrekkelijker maken en de kans op vertrek verkleinen. Het perspectief dat gekozen wordt is 10 jaar. De hier voorgestelde versterking van onderzoek en onderwijs leidt tevens tot de noodzakelijke toename van het aantal aan de Nederlandse samenleving af te leveren topspecialisten in cybersecurity. De behoefte aan meer cybersecurity professionals wordt onder andere tot uitdrukking gebracht in het rapport Verhagen[9]. Ook volgens dat rapport kunnen we zonder verhoging van de (academische) cybersecurity capaciteit in Nederland de voeten niet digitaal droog houden.

1. **Open competities voor tijdelijke AiO en postdoc projecten** (€ 40 miljoen). In de periode van 10 jaar wordt vier keer een open competitie uitgeschreven voor het indienen van cyber security voorstellen in brede zin, ook voor aanverwante wetenschapsgebieden. Dat laatste wil zeggen dat niet alleen harde (bèta) technische voorstellen ingediend kunnen worden, maar ook multidisciplinaire voorstellen met onderwerpen uit bijvoorbeeld de juridische, medische, bestuurlijke, of sociaal wetenschappelijke hoek. Richtinggevend hiervoor zal een

[7] Denk aan routes als 'Tussen conflict en coöperatie', 'Waarde creatie door verantwoorde toegang tot en gebruik van big data' en 'Op weg naar veerkrachtige samenlevingen'.
[8] In Europese competities scoren Nederlandse cybersecurity onderzoekers zeer goed, hetgeen hun internationale concurrentiekracht toont.
[9] Adviesrapport "Nederland Digitaal Droge Voeten" door Herna Verhagen.

herziene versie van de Nationale Cyber Security Research Agenda (NCSRA) zijn. Deze competitie zal op de gebruikelijke transparante wijze georganiseerd worden, met onafhankelijke beoordeling van de ingediende onderzoeksvoorstellen door experts.

2. **Open competitie voor gerichte ondersteuning van senior onderzoekers** (€ 20 miljoen). Via dit middel kunnen universiteiten in Nederland jaarlijks een bedrag aanvragen van € 2 miljoen voor een van de volgende initiatieven.
   - Een startup-budget voor een nieuw aangestelde hoogleraar op (een onderdeel van) het vakgebied cybersecurity, om de snelle opbouw van een eigen groep mogelijk te maken.
   - Een retentie-budget voor een zittende actieve hoogleraar, minstens 5 jaar na benoeming, om ruimte te scheppen voor nieuw onderzoek waarin de hoogleraar zelf een leidende rol kan spelen.

   Gegeven het totale budget kan in totaal 10 keer zo'n startup/retentie voorstel gehonoreerd worden. Dit leidt tot een aanzienlijke versterking van de beschikbare capaciteit. Toekenning vindt in beide gevallen plaats op basis van een onderwijs- en onderzoeksvoorstel waaruit het strategische cybersecurity belang voor Nederland blijkt[10].

De gevraagde middelen zullen ondergebracht worden bij een ervaren onderzoeksfinancier, zoals NWO, die op onafhankelijke en transparante wijze uitvoering dient te geven aan bovenstaande plannen. Leidende beoordelingscriteria zijn: wetenschappelijke kwaliteit en maatschappelijk belang. Nadere uitwerking van deze plannen kan aan dcypher[11] gevraagd worden.

Voorstel II: circulatie

In het Nederlandse bedrijfsleven en bij de overheid bestaat een groot tekort aan hoog opgeleide cybersecurity experts. Regelmatig worden specialisten op dit gebied door de ene werkgever bij de ander 'weggekocht'. Er zijn geen grote verschillen tussen de aanvangssalarissen in de publieke en de private sector. Wel is het zo dat salarissen in het bedrijfsleven harder kunnen groeien dan bij de overheid. Dit maakt de private sector aantrekkelijker. Daartegenover zijn cybersecurity functies bij de overheid soms 'spannender', vanwege de grotere bevoegdheden die ermee gepaard gaan. Ook werken sommigen gewoon liever voor de 'publieke zaak'.

Grote incidenten zoals 'Diginotar' in 2011 hebben aangetoond dat nauwe publiek-privaat-nonprofit samenwerking van groot belang is in tijden van crisis. Juist dan komt het er op aan dat professionals elkaar weten te vinden en elkaars werkzaamheden, verantwoordelijkheden en rollen begrijpen. Concreet gaat het over cybersecurity experts bij overheidsorganisaties als politie, inlichtingen-diensten, defensie, nationaal cyber security centrum, bij bedrijven als KPN, Fox-IT, Compumatica, Deloitte, KPMG, etc., en bij universiteiten, kennisinstellingen en operationeel verantwoordelijken zoals TNO, SIDN en SURFnet.

Het circulatie voorstel (Voorstel II) is er op gericht om een 'pool' te vormen waarin cybersecurity experts bij de overheid, het bedrijfsleven en de non-profit sector opgenomen kunnen worden. Organisaties kunnen lid worden van deze 'circulatie club', op basis van nader uit te werken voorwaarden en (financiële) verplichtingen. Medewerkers van aangesloten organisaties kunnen vervolgens lid worden van de pool. Dit biedt de volgende mogelijkheden om academische en operationele kennis te laten circuleren. Concreet gaat het daarbij om de volgende drie punten.

---

[10] Het concept van startup- en retentie-budgetten is ook in andere wetenschapsgebieden bekend, zie bijv. Hoofdstuk 5.1 getiteld "Herstel internationale concurrentiepositie bij aanstellen van toptalent" van het rapport "Koersvast" uit 2015 voor het ministerie van OCW, geschreven door de commissie Breimer over de versterking van de disciplines natuurkunde en scheikunde.

[11] Zie de website van het Dutch cybersecurity platform for higher education and research https://www.dcypher.nl.

1. **Kennis en ervaring verbreden**. Experts in de pool hebben een eigen werkgever, maar kunnen tijdelijk geheel of gedeeltelijk bij een andere organisatie gaan werken die ook lid is van de circulatie club. Hiermee kunnen deze experts hun kennis en blikveld verbreden, hetgeen uiteindelijk ook de eigen werkgever weer ten goede komt. De ontvangende werkgever krijgt (tijdelijk) nieuwe expertise in huis, met hopelijk een fris en ander perspectief. Dit vormt een win-win-win situatie.

2. **Kennis en ervaring verdiepen**. Experts in de pool kunnen ook een deeltijd promotie (PhD) traject afspreken met een cybersecurity groep aan een Nederlandse universiteit, als 'buitenpromovendus' ofwel '*industrial doctorate*'. Vanuit de pool wordt een bepaalde minimum inzet hiervoor gegarandeerd, van zeg twee dagen in de week. Een dergelijke bescherming is noodzakelijk omdat externe promovendi nu vaak voortijdig stoppen omdat de operationele druk vanuit de werkgever te groot blijkt te zijn.

3. **Operationele bijstand verlenen in crisissituaties**. Wanneer de hier geschetste pool enige tijd succesvol functioneert ontstaat een groep van cybersecurity experts met brede operationele ervaring die elkaars werkzaamheden begrijpen en elkaar onderling weten te vinden. De pool kan daarom een cruciale rol vervullen in een eventuele cybersecurity crisis, waarbij snelle ad hoc concentratie van werkzaamheden bij de crisishaard makkelijk gerealiseerd kan worden.

De bovenstaande 'circulatie' ideeën bevinden zich nog in een pril stadium en dienen nader uitgewerkt te worden. Daarbij kan dcypher een verbindende rol met de academische wereld spelen, maar is organisatie, aansturing en uitwerking vanuit de sector zelf essentieel. De kosten zijn voorlopig geschat op € 4 miljoen per jaar, ofwel € 40 miljoen voor een periode van 10 jaar. De organisatie van deze pool vereist nadere afspraken over o.a. onderlinge verrekeningen, geheimhouding, veiligheidsonderzoeken, intellectuele eigendomsrechten.

In tabelvorm samengevat:

	instrument	**bedrag per jaar**
kennis	open competities voor tijdelijke AiO en postdoc projecten	€ 4 miljoen
	gerichte ondersteuning van vaste medewerkers	€ 2 miljoen
circulatie	te vormen 'pool' van cybersecurity experts	€ 4 miljoen

Voor het 'kennis' deel van € 4 + € 2 = € 6 miljoen per jaar wordt publieke financiering gezocht. Voor het 'circulatie' deel van € 4 miljoen per jaar zijn investeringen vanuit de deelnemende partijen nodig.

Bijlagen

In bijlage 1 zijn steunverklaringen opgenomen, ontvangen na publicatie van dit plan en op basis van een hiervan afgeleide oproep de noodzaak tot meer structurele investeringen in cybersecurity onderzoek en hoger onderwijs te onderschrijven. Te bereiken door een publiek-privaat-nonprofit bundeling van krachten in onderzoek en kenniscirculatie. Dit is cruciaal voor het overeind houden van de kennisbasis met voldoende kritische massa, het oplossen van het tekort aan docenten en het afleveren van meer experts, zodat de innovatiekracht en soevereiniteit van Nederland behouden blijft.

In bijlage 2 is een (actueel) overzicht van universitaire groepen in cybersecurity met hun onderzoeksonderwerpen opgenomen.

Het volledige plan alsmede de bovengenoemde bijlagen zijn ook te vinden op de dcypher website.