CSR Cyber Security Raad

CSR Magazine

CSR Magazine 01 2022

Deze printvriendelijke versie bevat niet de volledige inhoud van het online magazine, maar alleen de teksten en een beperkte selectie foto´s. Het hele online magazine met alle foto´s, video´s en multimedia kan worden bekeken op: https://magazines.cybersecurityraad.nl/csrmagazine/2022/01/index

Nog een tip voor het geval u het magazine wil printen: Heeft u een Windows-computer en bekijkt u het magazine met het programma Chrome? Dan adviseren we u voor het afdrukken alleen gebruik te maken van het zogenoemde dialoogvenster (Ctrl+P).

‘Digitalisering is alleen succesvol als we de veiligheid kunnen garanderen’

Foto Jeroen de Bakker

De Cyber Security Raad (CSR) vierde afgelopen jaar zijn tienjarig-jubileum. De raad brengt vanuit het publieke, private en wetenschappelijke perspectief advies uit over de maatschappelijke vraagstukken die de digitalisering met zich meebrengt, waaronder het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid', een belangrijk advies voor het nieuwe kabinet voor een open, (digitaal) veilige en welvarende samenleving. In dit gesprek blikken covoorzitters Pieter-Jaap Aalbersberg en Sylvia van Es samen met wetenschapper Michel van Eeten terug op het afgelopen decennium en kijken ze samen vooruit naar welke rol de raad in de toekomst moet spelen.

Kracht en toegevoegde waarde CSR

In de afgelopen tien jaar heeft de raad verschillende adviezen en producten uitgebracht. Wat is het belang van de raad en de adviezen die jullie hebben uitgebracht volgens u?

Pieter-Jaap: "Over het geheel genomen is tien jaar kort, maar de digitalisering van de samenleving zit midden in een enorme versnelling. Als raad zijn we hier onderdeel van. En terwijl in het umfeld van alles verandert en in beweging is, zie ik binnen de raad een constante: we kijken al tien jaar lang vanuit een meervoudig perspectief en vanuit een bepaalde gelijkwaardigheid naar digitalisering. Privaat, wetenschap en publiek zit met elkaar aan tafel en vanuit ieders eigen verantwoordelijkheid proberen de leden tot een gezamenlijke duiding en tot goede adviezen te komen. Die samenwerking werkt, omdat partijen zien dat ze vanuit hun expertise iets toevoegen aan het geheel. Die werkwijze is internationaal uniek en van grote waarde."

Michel: "De CSR is inderdaad uniek. Dat komt inderdaad door de samenstelling publiek, privaat en wetenschap. De overheid zit zelf ook in de raad en adviseert daarmee in feite zichzelf. Dat is ongebruikelijk, maar het is tegelijkertijd onze kracht. We moeten samen tot een advies komen en kunnen bepaalde zaken niet doorschuiven naar een andere partij. Dan kom je tot een ander resultaat dan wanneer de overheid bijvoorbeeld zelf een advies schrijft op basis van extern opgehaalde kennis en expertise. De leden schrijven de adviezen echt samen en zelf, wat uniek is voor mensen in deze posities. Ook de openheid van de gesprekken in de raad is bijzonder. De kracht daarvan zie je terug in de adviezen."

Sylvia: "Absoluut, de kracht van de raad zit in de verschillende perspectieven, visies en invalshoeken. Onderlinge discussies leiden tot nieuwe inzichten en verrijken onze adviezen. Waarbij iedereen hetzelfde doel voor ogen heeft: verbetering van de digitale veiligheid."

Pieter-Jaap: "Alle leden zitten in de raad om Nederland digitaal veilig te maken. We dienen dus ons algemene belang. Door de unieke samenstelling van de raad (publiek-privaat-wetenschap) is het mogelijk om prioriteiten, knelpunten en incidenten vanuit diverse invalshoeken strategisch te benaderen en een integrale visie op kansen en bedreigingen te ontwikkelen en advies uit te brengen."

Speerpunten advies & plannen kabinet

Een van de meest recente adviezen die de raad heeft uitgebracht is het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid'. Wat is de belangrijkste kernboodschap uit dit adviesrapport voor het huidige kabinet?

Pieter-Jaap: "De titel van het adviesrapport zegt het al: we moeten toe naar een integrale aanpak. Ons advies is fundamenteel, want met de toevoeging en doorontwikkeling van het digitale element staan we voor een totale nieuwe infrastructuur van onze samenleving. Die infrastructuur moet goed en veilig zijn en de zwakkeren beschermen. We leren steeds meer over de combinatie online en offline. Het belang ervan is de afgelopen jaren door de coronacrisis alleen maar toegenomen. Dat maakt dat je vanuit een breder perspectief naar digitalisering moet kijken. Het gaat niet alleen over cybersecurity, maar over de vraag hoe we

onze samenleving met deze digitale infrastructuur op een veilige manier gaan inrichten. Het digitale landschap is nu nog te erg versnipperd."

Michel: "Dat klopt, al is versnipperd misschien niet helemaal het juiste woord: het suggereert dat er ooit een geheel was. Als je de digitale wereld zou vergelijken met individuele bomen in een jong bos, is het nu zaak de bomen er bewust van te maken dat ze samen een bos vormen. Opleiden van experts is onderdeel van de integrale aanpak waar we voor staan. Ook daar is een flinke investering nodig: er is een schreeuwend tekort aan gekwalificeerde mensen. Ze worden door andere landen zo'n beetje bij ons uit de schoolbanken weggerukt. Er is extra inspanning nodig om de tekorten niet verder op te laten lopen en onze kennispositie en digitale autonomie te behouden. Want als we zelf niet over de nodige kennis beschikken, zijn we overgeleverd aan het buitenland. De afgelopen jaren is er het een en ander aan middelen vrijgekomen. Dat heeft geleid tot relevant en goed onderzoek, maar de organisatie is nog erg ad hoc. Hoe gaat het verder als straks al die PhD's zijn afgerond?"

Sylvia: "Cybersecurity moet topprioriteit zijn. Digitalisering is pas een succes als we niet alleen de veiligheid kunnen garanderen voor bedrijven en organisaties, maar ook voor individuen. Een integrale benadering en eenduidig beleid is inderdaad noodzakelijk, echter is daarvoor wel een forse investering nodig: minimaal 833 miljoen euro, zoals terug te lezen is in ons adviesrapport 'Integrale aanpak cyberweerbaarheid'. Ik zie in het coalitieakkoord hoopvol stemmende zinnen over een centraal gecoördineerde en structurele samenwerking tussen overheid, bedrijfsleven en wetenschap. Tegelijkertijd zie ik nog een groot gat tussen de investeringen die wij adviseren en de investeringen die worden voorgesteld. Om Nederland ook in de toekomst een open, vrije en welvarende samenleving te laten zijn moet het nieuwe kabinet hiermee aan de slag."

Pieter-Jaap: "Digitalisering komt inderdaad veel naar voren in het akkoord. De aanstelling van een staatssecretaris Digitalisering en de instelling van een vaste Kamercommissie voor Digitale Zaken zijn een stap in de goede richting. Op financiën is er helaas geen apart blokje voor digitalisering. Daar kunnen we nog een stap in zetten."

Blik in de toekomst

Wat zijn, naast de hiervoor genoemde aandachtspunten, de belangrijkste toekomstige uitdagingen op gebied van digitalisering en digitale veiligheid? En welke rol zien jullie daarbij voor de CSR weggelegd?

Michel: "Ik denk dat onze agenda de eerste paar jaar te veel werd bepaald door wie er naar ons toekwam. We kregen pas in een laat stadium de beleidsplannen te zien en werden dan als een soort stempelpost gevraagd om goedkeuring. Inmiddels worden we eerder in het proces betrokken. De raad is nu meer sturend en autonomer geworden en er is meer ruimte om vooruit te denken over de grote vragen waar het beleid nog niet op voorgesorteerd is. Nu is dat bijvoorbeeld: encryptie. Een heet hangijzer waar publiek en privaat uiteenlopende meningen over hebben. Terwijl buiten de raad het debat daardoor totaal vastligt, gaan we binnen de raad het gesprek aan. Juist omdat de raad een van de weinige plekken is waar je zulke gevoelige gesprekken kan voeren. Iedereen voelt de urgentie van het gesprek en we moeten kijken hoever we samen komen."

Sylvia: "Het feit dat we in Nederland koploper op het gebied van digitalisering zijn, is een mooie basis. Maar ik zie nog wel uitdagingen, bijvoorbeeld in het ontsluiten van data op een verantwoorde manier. Voor technologieën als kunstmatige intelligentie zijn nu eenmaal grote hoeveelheden ontsloten data nodig. De wetgeving zou op Europees niveau geharmoniseerd moeten zijn, maar is in de praktijk op uitvoeringsniveau nog versnipperd. Ook is een verdere verheldering van een aantal dataprotectie- concepten, zoals anonimisering, noodzakelijk. Ik maak me in dat kader zorgen over een *level-playing field*, zowel binnen Europa als ten opzichte van de rest van de wereld. We moeten voorkomen dat we op achterstand komen te staan. Onderaan de streep geldt dat digitale veiligheid van het grootste belang is, alle kansen en mogelijkheden om innovaties te bereiken hangen daarvan af."

Pieter-Jaap: "De ontwikkelingen gaan zo snel, dat we als raad pro-actiever moeten zijn. We moeten meer vooruitkijken naar wat er op ons afkomt en nagaan of we daar goed op zijn voorbereid. Nieuwe technologieën brengen ook nieuwe dilemma's met zich mee. De CSR kan die in kaart brengen en oplossingsrichtingen meegeven, zonder direct een oplossing te benoemen. Cybersecurity gaat niet meer puur over hardware en software. Het gaat ook over anders kijken naar data en wat het grootschalig gebruik daarvan voor de samenleving betekent. Hoe bescherm je als overheid je burgers? Dit moet samen met de wetenschap en private sector worden opgepakt. Al die samengestelde issues, daar moet de CSR de komende jaren uit zichzelf stappen in gaan zetten."

Vaste Kamercommissie Digitale Zaken: eerste stap in goede richting

Foto Jeroen de Bakker

Sinds maart 2021 bestaat de vaste Kamercommissie voor Digitale Zaken. Hard nodig volgens velen, waaronder fungerend voorzitter Renske Leijten. In 2021 heeft ze de commissie vormgegeven: welke thema's horen bij Digitale Zaken en welke taken heeft deze? Nu het nieuwe kabinet er is, is het voor haar tijd om de voorzittershamer door te geven.

De vaste Kamercommissie voor Digitale Zaken is opgericht na een aanbeveling van de tijdelijke commissie Digitale Toekomst, bedoeld om de Kamer meer greep te laten krijgen op de ontwikkelingen in de digitale wereld. ''We hebben een specialistische en een horizontale functie. Dit betekent dat we ons echt bekwamen in het thema en namens de Kamer dit thema behandelen. Maar tegelijkertijd spelen we ook een verbindende rol, omdat digitalisering zo'n breed onderwerp is wat op alle beleidsterreinen een rol speelt, waarbij we Kamerbreed informatie over de digitale wereld delen. Dit kun je vergelijken met de functie van de commissie Rijksuitgaven, die de Kamer informeert over hoe je begrotingen afleest bijvoorbeeld.''

De precieze invulling van de commissie was bij de oprichting nog niet gedefinieerd, dat was de eerste opdracht. ''Ik heb toen gezegd dat we rustig moeten bezinnen: wat willen we als commissie betekenen? Het risico bij een breed onderwerp als de digitale wereld is dat je het putje wordt van álle digitale zaken. Maar als het gaat over digitale toepassingen in de klas, moet dit vooral een zaak zijn voor onderwijsspecialisten. Terwijl een discussie over algoritmen wel van een niveau is wat de commissie naar zich toe mag trekken.''

Bij de oprichting van de Kamercommissie zochten de leden naar consensus onder de partijen. In een vertrouwelijke omgeving voerden ze gesprekken met experts en brainstormden ze over de basis van de commissie. Hieruit volgden zes fundamentele thema's voor de commissie, zie kader voor meer uitleg over deze thema's. ''Met deze zes aandachtsvelden laten we zien waar wij als commissie prioriteit aan geven, maar ze zeggen niks over de onze standpunten. We zeggen dat de Kamer hier een visie over moet vormen, dat gebeurt via een debat tussen de partijen. Wij als commissie zorgen ervoor dat het debat überhaupt gevoerd wordt.''

Staatssecretaris Digitalisering

Het nieuwe kabinet heeft voor het thema digitalisering zelfs een staatssecretaris benoemd. Sinds januari is Alexandra van Huffelen staatssecretaris Koninkrijksrelaties en Digitalisering. Renske Leijten benadrukt dat de commissie hierover geen standpunt heeft, maar dat zij persoonlijk positief aankijkt tegen een bewindspersoon op dit onderwerp. ''Mits ze ook echt een mandaat vanuit het kabinet heeft, waarmee ze ook daadwerkelijk met de benodigde slagkracht aan de gang kan.''

Volgens het SP-Kamerlid is de benoeming van een staatssecretaris rondom het onderwerp digitale zaken niet het belangrijkste. ''Het gaat er om dat binnen de hele overheid moet worden gekeken naar de structuur van digitale toepassingen, hoe gaan we hier als departementen, overheidsorganisaties en lokale overheden mee om? Er zijn al *information officers* en functionarissen gegevensbescherming binnen de overheid, maar deze hebben nog niet de prioriteit die wel nodig is. De staatssecretaris is hopelijk degene die ervoor kan zorgen dat mensen met deze functies op een belangrijke plek in de organisatie terechtkomen.''

Wat in de commissie wel breder leeft, is het risico wat het benoemen van zowel een Kamercommissie als Staatssecretaris voor Digitale Zaken met zich meebrengt. ''Partijen en andere departementen moeten niet gaan achteroverleunen met het idee dat alle problemen rond digitalisering nu worden opgelost. De problemen zitten overal en zijn te urgent om af te schuiven.''

De Nederlandse maatschappij is op allerlei vlakken afhankelijk van de digitale communicatie. De veiligheid van deze infrastructuur is onder andere van belang voor ons welzijn, de economie en de democratie. Wat opvalt in deze markt is de

dominantie van enkele buitenlandse techbedrijven, die ook nog eens niet-Europees zijn. ''Dit is inderdaad een ontwikkeling die we als commissie signaleren en die verweven zit in de aandachtspunten die we op hebben gesteld. Maar nogmaals: de commissie heeft geen standpunt op de manier hóe we hier mee om moeten gaan. We faciliteren het debat door thema's te agenderen, maar het inhoudelijke debat moet in de Tweede Kamer gevoerd worden.''

Vanuit de commissie Digitale Zaken worden rapporteurs naar het buitenland gestuurd om daar te onderzoeken hoe andere overheden omgaan met deze vraagstukken. Door corona is dit niet helemaal volgens plan gelopen. Maar volgens Leijten gaat dit in 2022 weer veel gebeuren en wordt de Europese samenwerking steeds beter.

Digitalisering gaat iedereen aan

Voor veel jonge mensen is de digitale wereld heel normaal. Maar het gros van de bevolking is niet opgegroeid met internet, smartphones en DigiD. Leijten herkent dit en pleit dan ook voor helderder taalgebruik als we het hierover hebben. "Het begrip cybersecurity alleen is al voor veel mensen onbegrijpelijk. Terwijl het simpelweg gaat over een veilige digitale wereld, iets wat impact heeft op het dagelijkse leven van elke Nederlander. Veel mensen hebben door te moeilijk taalgebruik niet door dat het ook over hún leven gaat, als we praten over cybersecurity, algoritmes en ransomware.''

Het gesprek over cybersecurity (of digitale veiligheid) moet toegankelijker worden gemaakt volgens Leijten. De oplossing ligt daarbij volgens haar niet bij het optuigen van een heel nieuw instituut rondom de Nationale Coördinator Digitalisering, wat volgens haar te veel tijd en geld kost. Terwijl het juist nu belangrijk is om snel stappen te zitten, want alle sectoren gaan steeds meer te maken krijgen met digitalisering en alle uitdagingen die daarbij komen kijken. Het Landelijk Dekkend Stelsel van informatieknooppunten (LDS) kan al een belangrijke rol vervullen. ''Ontwikkel zo'n stelsel vanuit wat er al bestaat, breng al het goede samen en maak daar binnen informatiedeling zo makkelijk mogelijk. Tegelijkertijd moeten we ervoor zorgen dat digitale veiligheid op alle departementen prioriteit heeft. Als die twee punten goed geregeld zijn, kun je een digitale infrastructuur bouwen waar kennis, ervaringen maar ook waarschuwingen met op een veilige en efficiënte manier met elkaar gedeeld worden.''

Verantwoordelijkheid

Er moeten grote politieke keuzes worden genomen, die duidelijke maatschappelijke impact gaan hebben. De discussie hierover moet gevoerd worden, maar volgens Leijten moet de focus daarvan niet op het individu liggen. ''Op die manier zou je de verantwoordelijkheid bij de consument leggen en niet bij de politiek en grote bedrijven. Terwijl ik vind dat burgers uit moeten gaan van het voorzorgsprincipe van de overheid. Wij moeten, samen met de private sector, ervoor zorgen dat het digitale systeem veilig te gebruiken is. Als jij je aan de regels houdt en niks geks doet, moet het niet zo zijn dat het alsnog heel fout gaat. Denk dan aan het lekken van privégegevens of scams waar teveel mensen nog steeds intrappen.''

De oplossing ligt volgens haar bij het weghalen van het verdienmodel voor criminelen. Dit kan alleen met genoeg capaciteit om te monitoren én te handhaven. En hiervoor zijn dan weer duidelijke wettelijke kaders nodig. ''Dit zijn vraagstukken die in Den Haag nog lang niet goed genoeg zijn besproken, er ligt dus nog een hele taak op ons te wachten. En ja, dit is ook een Europese discussie, want de digitale wereld kent geen landsgrenzen. De capaciteitstekorten binnen onze veiligheidsorganisaties zijn groot. Dit moet topprioriteit zijn voor het nieuwe kabinet. Hier ben ik niet heel optimistisch over.''

Toch is de eerste stap die de Kamer gezet heeft een goed begin. De commissie zorgt ervoor dat digitalisering als overkoepelend vraagstuk wordt behandeld. Tegelijkertijd zorgde deze stap ook voor een ander inzicht: ''We zijn als commissie enorm geschrokken van het kennisniveau binnen de overheid dat enorm laag is. Als overheid moeten we ervoor zorgen dat de kennis in huis komt en blijft. Dit hoeft niet alleen met financiële middelen worden gerealiseerd. We moeten zorgen dat de overheid een aantrekkelijke werkomgeving is waar mensen beseffen dat ze echt maatschappelijke impact maken met hun werk.''

Europa neemt voortouw versterking digitale soevereiniteit

Foto De Beeldunie

Met 92% van de Europese data in Amerikaanse clouds, is het herstel van de digitale soevereiniteit van de Europese Unie (EU) inmiddels een kernambitie van de Europese Commissie voor de komende vijf jaar. "We zijn in Europa te afhankelijk van technologie van China en de Verenigde Staten en moeten in onze eigen behoeften kunnen voorzien" aldus Ursula von der Leyen in haar State of the Union dit jaar. De Europese digitale innovatiestrategie en agenda is inmiddels vol onderweg.

Lokke Moerel, lid van de Cyber Security Raad (CSR) namens de wetenschap: "In Europa is de urgentie echt doorgedrongen en dat zien we ook in de landen om ons heen. Zo is digitale soevereiniteit in Duitsland inmiddels *Chefsache*. Als we in Europa een gesprekspartner willen zijn, zullen we op nationaal niveau een aantal stappen moeten zetten. Uitgangspunt daarbij dient te zijn: sterk in eigen huis, sterk in Europa, sterk in de rest van de wereld." Gerrit van der Burg, lid van de CSR namens de publieke sector: "In Nederland staat dit onderwerp nog onvoldoende op de politieke agenda en wordt cybersecurity tot nog toe vooral reactief aangepakt. We reageren in crisismode en vrijwel niet vanuit het bredere perspectief van strategische autonomie. Dat moet echt anders."

Volgens Moerel en Van der Burg is Nederland een van de meest gedigitaliseerde landen. De coronacrisis heeft dit proces verder versneld. "Er ontstaan daardoor steeds meer nieuwe afhankelijkheden en kwetsbaarheden", stelt Van der Burg. "De cyberdreigingen nemen toe en we worden steeds afhankelijker van de digitale infrastructuur die in handen is van een beperkt aantal grote buitenlandse marktspelers. Dit kan grote gevolgen hebben voor onze nationale en economische veiligheid en daarmee het verdienvermogen van Nederland." Moerel: "De hamvraag is hoe behouden we als Nederland ook in de digitale wereld controle over onze *essentiële economische ecosystemen* en *democratische processen*. "

Nieuwe technologieën zetten onze digitale soevereiniteit onder druk

Gebrek aan controle over kritische technologieën resulteert in nieuwe afhankelijkheden. Zo is de huidige encryptie niet bestand tegen de rekenkracht van de toekomstige kwantumcomputers. Moerel en Van der Burg vinden dat we nu moeten innoveren om onze kritische informatie ook in de toekomst te kunnen beschermen. Dat is niet alleen relevant voor toekomstige informatie, maar ook voor onze huidige informatie. Moerel: "Vergeet niet dat sommige vreemde staten stelselmatig onze versleutelde communicatie onderscheppen in de verwachting die later met kwantumcomputers te kunnen ontsleutelen en te analyseren met behulp van kunstmatige intelligentie, ofwel AI." Van der Burg: "We zien criminelen op grote schaal automatisch kwetsbaarheden in software opsporen en exploiteren. We zullen echt moeten innoveren om de cybercriminelen een stap voor te blijven."

"Inmiddels staat nagenoeg alle data van Nederlandse overheden, bedrijven en personen in de cloud van een handjevol buitenlandse aanbieders", vervolgt Moerel. "Als we onszelf tien jaar geleden hadden gevraagd of *dit in principe* een goed idee zou zijn, zou je geen voorstanders vinden. Als een van deze bedrijven uitvalt, is het net alsof de elektriciteit uitvalt, dan liggen hele sectoren van onze economie stil. We zouden nooit de switch van ons elektriciteitsnetwerk in handen van een buitenlandse partij geven. Van der Burg: "De situatie op het gebied van opsporing van digitale criminaliteit is net zo fragiel. We zijn voor strafrechtelijk onderzoek deels afhankelijk van de medewerking van enkele buitenlandse spelers. Als deze geen medewerking geven of dit te lang duurt, omdat het hoofdkantoor eerst goedkeuring moet geven, leidt dat ertoe dat wij ons werk niet goed kunnen doen. We zien in de praktijk dat dit ons te afhankelijk kan maken, hetgeen gevolgen heeft voor onze rechtsstaat en de positie van slachtoffers."

Data als wapen: Ook TikTok is een kwestie van nationale veiligheid

Moerel stelt dat het niet alleen gaat over de afhankelijkheden voor de bedrijfsvoering en publieke taken. "Het gaat ook over wat andere staten met de informatie over onze burgers en bedrijven kunnen. Inmiddels beschouwen China en de Verenigde Staten toegang tot elkaars data als een kwestie van nationale

veiligheid. Er werd lacherig over gedaan toen voormalig president Trump de TikTok-app had verbannen uit de Amerikaanse app stores, maar inmiddels heeft ook President Biden een Executive Order uitgevaardigd die het mogelijk maakt om doorgifte van gevoelige gegevens van Amerikaanse burgers naar China te voorkomen. China heeft inmiddels ook een export verbod op important data, waaronder ook data valt die het leven, wonen en werken van Chinese burgers in kaart kan brengen. Ook verbood China onlangs de DiDi-app (de Chinese Uber) uit de Chinese app stores toen dit bedrijf een beursnotering in de Verenigde Staten kreeg. We moeten hier echt naar kijken. Onze privacy-wetten beschermen wel de individuele privacy van burgers maar niet onze collectieve data. Ik durf inmiddels de stelling wel aan dat de TikTok-app inderdaad een kwestie van nationale veiligheid is."

De CSR heeft onlangs adviezen uitgebracht over een *'Integrale aanpak cyberweerbaarheid'* en *'Nederlandse Digitale Autonomie en Cybersecurity'*. Belangrijkste constatering van de raad is dat cybersecurity tot nog toe vooral technisch en reactief wordt aangepakt en vrijwel niet vanuit het bredere perspectief van strategische autonomie. Moerel: "Doordat de soevereiniteitsvraag steeds meer gebieden van economie, maatschappij en democratie raakt, dient aansturing centraal plaats te vinden, maar als raad zien we dat de benodigde integratie van beleid ontbreekt. In een eerder advies constateerden we al dat we als Nederland op dit moment onvoldoende inzicht hebben in onze nieuwe afhankelijkheden en daardoor niet in staat zijn om voldoende proactief gecoördineerd technologiebeleid te kunnen voeren op het gebied van onderzoek, valoratie en industriële capaciteiten. Kortom, het huidige reactief handelen dient te worden gecombineerd met proactief monitoren en anticiperen. Dit vergt sturing vanaf het hoogste niveau."

Digitale autonomie chefsache

Volgens Van der Burg en Moerel moet de verantwoordelijkheid voor digitale autonomie dus op het hoogste politieke- en ambtelijke niveau worden belegd. Van der Burg: "Het moet in feite permanent onderwerp van gesprek zijn op het hoogste niveau: in de politiek, bijvoorbeeld de ministerraad, en ook in het bedrijfsleven. We moeten dagelijks bezig zijn om voor Nederland grenzen te trekken en onze onafhankelijkheid te bewaken." Moerel: "Op dit moment heeft digitale autonomie wel de aandacht van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Klimaat en Justitie en Veiligheid, maar er wordt te veel in silo's gewerkt. We moeten een eenduidig beleid hebben, alleen dan kunnen we ook als Nederland een bijdrage leveren in Europa. Als je niks meebrengt aan tafel ben je ook geen volwaardige gesprekspartner." Op de vraag wat digitale autonomie kost en welk land vooroploopt, antwoordt Van der Burg: "Het is lastig om de situatie in verschillende landen met elkaar te vergelijken. Daarvoor lopen onder meer uitgangsposities te ver uiteen. We zouden wel een voorbeeld kunnen nemen aan het Verenigd Koninkrijk, waar structureel budget wordt gereserveerd voor het bewaken van de digitale autonomie. Een vast percentage van het bruto binnenlands product (bbp) zou ook in Nederland verstandig zijn."

Europese tech

Hoewel de afhankelijkheden van buitenlandse aanbieders op dit moment groot zijn, ziet de CSR geen reden tot fatalisme. Moerel: "Techinnovaties gaan altijd in golven en er is altijd weer een nieuwe golf. Er is veel mogelijk als we goed investeren. Het besef groeit dat we alternatieven nodig hebben. Laten we vooral gericht innoveren en samenwerken on dit te bereiken, waardoor tevens een gericht beroep kan worden gedaan op Europese cofinanciering." Van der Burg: "Daarmee samenhangend moeten we ook zorgen dat we voldoende zicht hebben op wat er allemaal in onze eigen *techscene* gebeurt. Het mag eigenlijk niet gebeuren dat we min of meer verrast worden door de verkoop van bijvoorbeeld een kritisch internetbeveiligingsbedrijf. Kroonjuwelen moet je zien te behouden voor Nederland. Ook moeten we de ontwikkeling van startups goed monitoren en ervoor waken dat nieuwe technologieën worden misbruikt door criminelen."

GAIA-X

In het CSR-advies *'Nederlandse Digitale Autonomie en Cybersecurity'* wordt onder andere gesproken over het GAIA-X-project, dat is geïnitieerd door Duitsland en Frankrijk. Moerel: ik zie dat vaak wordt gedacht dat de bedoeling van GAIA-X is om onze eigen Europese cloudspeler op te zetten. Dit is echter niet het doel van GAIA-X. Het doel is tot *schaalbaarheid* van de cloudinfrastructuur in Europa te komen door interoperabiliteit tussen de verschillende clouddiensten te realiseren. Dit wordt bereikt door het stellen van gemeenschappelijke technische standaarden en juridische kaders voor de digitale infrastructuur. Deze vorm van interoperabiliteit gaat dus verder dan portabiliteit van data en applicaties van de ene naar de andere leverancier ter voorkoming van vendor lock-in; het betreft echt het creëren van open API's, interoperabiliteit van sleutel beheer bij encryptie, eenduidig identity & access management, etc. Na aanvankelijke aarzeling, zien we dat inmiddels een Nederlandse coalitie actief aan dit project bijdraagt. Ik ben zelf betrokken bij een interessante Europese *use case* op het gebied van energie. Het begint echt te komen in Europa." Van der Burg: "Ik zie GAIA-X ook wel als voorbeeld voor betere interoperabiliteit van andere producten en processen. Ook op het gebied van

opsporingsmogelijkheden en technieken. Nederland is al behoorlijk goed op het gebied van hightech opsporing, maar het helpt natuurlijk als we heel Europa meekrijgen. We moeten meer Europese slagkracht ontwikkelen en komen tot uniforme aanpakken."

Digitale autonomie blijft op agenda CSR

Van der Burg: "Digitale autonomie blijft nog wel even op de agenda van de CSR. De technische en geopolitieke ontwikkelingen gaan zo snel dat we hier de vinger aan de pols houden. Digitale autonomie dient ook – evenals cybercrimebestrijding - een aparte plek te krijgen in het jaarlijks gepubliceerde Cybersecuritybeeld Nederland." Moerel vult aan: "De raad verdiept zich de komende tijd in het vraagstuk hoe onze collectieve data door vreemde mogendheden kan worden ingezet als wapen en hoe we ons daar beter tegen kunnen beschermen. Ander onderwerp op de agenda is hoe we burgers meer controle over hun data kunnen geven door een betrouwbare universele Nederlandse digitale identiteit. Op een aantal onderdelen van ons advies inzake digitale autonomie zijn inmiddels de eerste stappen gezet, zoals het verhogen van de bewustwording van strategische autonomie in cybersecurity en het verbeteren van het Nederlandse valorisatie en innovatieklimaat. Onderdeel van het advies van de CSR was een handreiking *'Toetsingskader digitale autonomie* en cybersecurity', dat inmiddels door het ministerie van Economische Zaken en Klimaat wordt geoperationaliseerd."

NIS2, een ambitieuze update van de Europese cybersecurity-richtlijn

Foto Hollandse Hoogte - ANP Foto

De cyberweerbaarheid van 27 Europese lidstaten verbeteren is geen eenvoudige klus. Om de uitdagingen van de toekomst aan te gaan, moet je ambitieus zijn. "Er is genoeg strategie, maar de komende jaren draait het om executie, executie, executie", zegt Bart Groothuis, Europarlementariër voor de VVD vanuit Brussel.

Snijvlak van geopolitiek en technologie

Groothuis werkt al bijna twee jaar in Brussel. "Ik houd mij bezig op het snijvlak van geopolitiek en technologie en dan specifiek over nieuwe dreigingen. Daarvoor was ik zeven jaar werkzaam bij Defensie als hoofd cybersecurity. In het parlement heb je iemand nodig die een wetgevingsdossier trekt en dat noem je een rapporteur. Op basis van de inhoud probeer ik dan een meerderheid te vinden. Die rol bevalt mij ook goed. Daar kan ik al mijn ideeën en expertise over cybersecurity in kwijt."

Forse uitbreiding

Hij las de adviezen vanuit de Cyber Security Raad en negen van de tien zag hij ook terugkomen in de NIS2, de richtlijn voor cybersecurity vanuit Brussel. "De NIS2 is dus de richtlijn die straks wetgeving wordt in Nederland, maar ook in de andere 27 lidstaten. We hebben al wetgeving uit 2016, de NIS, maar die mankeert. Deze verschilt namelijk per land, waardoor je moet voldoen aan andere richtlijnen. De NIS2 is dus een update en deze is een stuk ambitieuzer. De vorige keer was er nog discussie of Europa hier überhaupt iets te zeggen had over cyberweerbaarheid. Dat is echt *water under the bridge*."

De richtlijn moet dus vooral ambitieuzer, maar op welke vlakken gaat dit gebeuren? Groothuis ziet veranderingen op drie terreinen: "Allereerst is er een forse uitbreiding van de *scope*. Het aantal bedrijven en entiteiten dat we eerst vitaal noemden, gaan we nu betitelen als 'important and essential'. Het is afhankelijk van de dienstverlening die jij aanbiedt aan de samenleving. Als je meer dan 50 medewerkers hebt en meer dan 10 miljoen euro omzet, ben je onderdeel van deze *scope*. Ben je kleiner, maar lever je essentiële dienstverlening, zoals een clouddienst, dan behoor je er ook toe. Je moet dan bepaalde cybersecurity-

maatregelen treffen, bijvoorbeeld een meldplicht bij incidenten of dreigingen. Door deze wijziging gaan we naar zo'n 160.000 entiteiten in Europa.

Het tweede gaat over de informatie-uitwisseling. Sinds de introductie van de General Data Protection Regulation (GDPR) (AVG in Nederland) is er veel twijfel over aansprakelijkheid. Mag je persoonsgegevens wel delen? Kun je achterhalen waar domeinen geregistreerd staan? Daar willen we met de NIS2 een juridische basis voor bieden. Zodat ook internationale bedrijven en overheden onderling weer gegevens kunnen uitwisselen. Dat is heel erg belangrijk voor de cybersecurity-community en dat is waar ik het uiteindelijk voor doe, zodat zij zich vertegenwoordigd voelen in Brussel."

Cybersecurity in de boardroom

"Ten derde gaan we cybersecurity *chefsache* maken, zoals ook de Cyber Security Raad adviseert. Een mooi Duits woord, wat betekent dat het een onderwerp is wat besproken moet worden op tafel bij de chef, in de boardroom op CEO-niveau. We hebben nu bedacht om het senior management persoonlijk aansprakelijk te stellen. Er zit een boete in: 2% van je jaaromzet als je echt aantoonbaar niet je maatregelen hebt getroffen. Waarom 2%? Bij een ransomware-aanval wordt vaak 2% van je jaaromzet geëist. Daarom komt straks de keuze: geef ik het aan die ransomware-aanvallers uit Rusland, geef ik het als boete aan de overheid of investeer ik dat bedrag in veiligheid en cybersecurity?"

Europa moet proactief handelen

Cyberweerbaarheid staat dus steeds hoger op de agenda in Europa. Groothuis ziet de NIS als de basis, maar er zijn nog meer initiatieven om cyberweerbaarheid te verhogen. "Het tweede is de introductie van de Cyber Resilience Act. Dat is een puzzelstukje wat nog mist en dat gaat over *connected devices*, oftewel apparaten die kunnen verbinden met het internet. Je kunt straks software- en hardware-ontwikkelaars persoonlijk aansprakelijk stellen voor slechte producten. Bij het derde – en dat vind ik het mooiste – kom je uiteindelijk op het operationele vlak. Dit is onderdeel van de cybersecurity-strategie en gaat over DNS-capability. Bij een grootschalige aanval, zoals bij Petya in de Rotterdamse Haven, wordt het mogelijk om een domein te blokkeren. Heel simpel en erg doeltreffend.

Binnen Europa moeten we dit meer gaan doen: niet meer reactief reageren, maar proactief handelen. We weten heel goed waar de aanvallen vandaan komen, dus we moeten die kennis gebruiken om juist de problemen voor te zijn. Ook in Nederland. Daarvoor moet je ook je handen vuil maken en soms juridisch scherp aan de wind varen, maar dat is wel nodig.

Als jij echt een ambitieuze strategie wilt, betekent dat operationaliseren van je wensen. Er is genoeg strategie, maar we missen de executie. Daar moeten we de komende jaren op inzetten. *Make it happen.* De juridische basis wordt gelegd in Brussel, maar nu is het tijd voor politieke wil en doorzettingskracht in Nederland. Passief informatie delen, die tijd is belangrijk, maar er komt iets bij."

Groothuis erkent dat Nederland lang voorop heeft gelopen. "Er was veel energie. De afgelopen jaren lopen we echter steeds meer achterop en is er zelfs sprake van achteruitgang. Binnen het Verenigd Koninkrijk is er één duidelijke organisatie waar je mee dealt, maar in Nederland is dit niet zo duidelijk: soms het Nationaal Cyber Security Centrum (NCSC), soms de Politie of de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). In Europa maken we nu een *framework* en daarin zie je ook dat in 17 landen deze diensten zijn geconvergeerd, maar in Nederland blijft het versnipperd."

Op zoek naar gelijkgestemden

Voor de EU liggen er genoeg uitdagingen in de toekomst. Groothuis ziet vooral een noodzaak om te investeren. "Het gaat de komende jaren om *deep security*. Dat is het allerbelangrijkste, als je het hebt over digitale autonomie. Je kunt heel veel afnemen van andere landen en partners, maar je moet je grootste belangen zelf goed beveiligen.

Het gaat bijvoorbeeld over cryptografie. In Nederland moet eigenlijk gezegd worden: we hebben een eigen cryptografische basis nodig, gemaakt door de AIVD, uitgegeven door een Nederlands bedrijf. Zodat je het hele proces controleert. Een aantal jaren geleden werd er door het ministerie van Buitenlandse Zaken nog gewerkt met Kaspersky-antivirussoftware uit Rusland. Elke mail van een diplomaat kon gecontroleerd worden. Dat is natuurlijk niet okay. Als je echt *deep security* wilt, moet je daar ook als Nederland in investeren.

Als het om Europa gaat, moet je op zoek naar gelijkgestemde landen en regio's. Er is geen ruimte meer voor samenwerkingen met geopolitieke tegenstanders die dan producten en diensten verzorgen voor je vitale sector. Waarom moeten we gezichtsherkenningssoftware vanuit China gebruiken? Dit geldt bijvoorbeeld ook voor 5G.

In de NIS2 zorgen we er ook voor dat er een *supply chain review* in de wetgeving komt. Als we Chinese, Iraanse of Russische apparatuur niet vertrouwen, dan kunnen

we deze laten weren. We gaan vanuit onze eigen jurisdictie bepalen wat we wel en niet toelaten op onze markt.

De laatste belangrijke trend is dat we ransomware niet meer alleen gaan zien als een crimineel verdienmodel, maar ook als een vorm van buitenlandse politiek vanuit Rusland. Vrijwel alle ransomware komt uit die hoek. Alle veiligheidsdiensten in Europa bevestigen dit beeld.

En zoals Joe Biden dit nu aanpakt met Vladimir Poetin, dat is hoe we het ook moeten doen vanuit Brussel. In hun laatste gesprek ging het voor het eerst in 60 jaar niet over nucleaire wapens, maar over ransomware en over cyberaanvallen.

In de EU hebben we ook een Cyber Diplomacy Box om sancties aan Rusland op te leggen en de lidstaten mandaat te geven, maar deze wordt nog te weinig ingezet. Dit is niet alleen een cybersecurity-probleem, maar ook een diplomatiek probleem. Zolang we dit niet adresseren, doen we het niet goed. Ik mis de stem van de Cyber Security Raad ook in dit gesprek. We moeten het probleem bij de bron aanpakken."

Haast gaan maken

Joe Biden tekende in mei het voorstel *Improving the Nation's Cybersecurity* naar aanleiding van een reeks cyberincidenten. Groothuis ziet daarin vooral de noodzaak om haast te maken. "Het is een waterbed-effect. Om een voorbeeld te geven: toen er veel fraude en malware was met internetbankieren, hebben de banken in Nederland de handen ineengeslagen. Binnen drie maanden werd de criminaliteit met 90% gereduceerd. Maar in de andere landen om ons heen steeg het juist. Als de Amerikanen beginnen met spoedwetgeving, dan moeten wij dus ook haast gaan maken. De Amerikanen houden zich vooral bezig met het aanpakken van de keten. En daar is ook winst te behalen voor de EU. Daarom hebben we dat ook verwerkt in de NIS2."

Groothuis ziet 2022 als het jaar waarin er spijkers met koppen worden geslagen. "De Fransen hebben in januari het voorzitterschap van de EU overgenomen. We proberen het rond die periode ook af te ronden. Daarna wordt het naar het Nederlands Parlement gestuurd en die moeten er dan chocola van gaan maken. Dan zullen we zien hoe Nederland zich verhoudt tot deze nieuwe richtlijn."

"Digitale veiligheid keiharde voorwaarde voor onze manier van leven en vrijheid"

Foto Arenda Oomen

Als officier van de Koninklijke Marine moet ik allereerst wijzen op de nautische herkomst van het woord cyber. Het oud-Griekse woord kubernetes betekent stuurman of roerganger. In 2021 is die etymologie helemaal in de vergetelheid geraakt en associëren we cyber met alles wat met computers en computernetwerken te maken heeft. En toch kan de oude nautische betekenis ook nu nog van waarde zijn wanneer we kijken naar de cyberweerbaarheid van Nederland, onze digitale autonomie en de rol van Defensie daarin.

De betekenis van het oorspronkelijke Griekse woord beschrijft ten eerste heel goed de rol die de Cyber Security Raad wat mij betreft moet spelen in het nationale cyberlandschap: die van roerganger. De roerganger houdt koers, bewaakt de toestand van het schip en adviseert de kapitein over kansen en bedreigingen die aan de horizon opdoemen. Zo ook adviseert de CSR het kabinet over de ontwikkelingen en bedreigingen in het cyberdomein. Dat kunnen we niet anders doen dan in een goede mix van overheid, publiek-privaat, wetenschap, civiel en militair. We hebben de gezamenlijkheid van al deze perspectieven en expertise keihard nodig want onze tegenstanders maken geen onderscheid wanneer zij onze vitale belangen aanvallen.

Daarmee komen we op de dreigingen aan de horizon. Net als de samenleving digitaliseert ook Defensie meer en meer. Onder het principe van Informatie Gestuurd Optreden stellen wij data en informatie centraal in de manier waarop wij opereren. Onze netwerken en IT-systemen worden daardoor steeds belangrijker voor onze effectiviteit. Daarin liggen kansen maar ook bedreigingen. We zullen allereerst ervoor moeten zorgen dat we onze eigen systemen en netwerken veilig houden zodat we daarmee onze operationele doelstellingen kunnen behalen en de Nederlandse strategische belangen kunnen beschermen.

Net zoals de Nederlandse marine sinds jaar en dag handelsvloten beschermt, zo heeft Defensie als geheel een beschermende rol voor de Nederlandse samenleving en haar belangen. Onze economie draait voor een groot deel op digitale infrastructuur en services, ons land herbergt één van de grootste internetknooppunten van de wereld, en onze samenleving digitaliseert steeds verder. Digitale veiligheid is daardoor een keiharde voorwaarde geworden voor onze manier van leven en onze vrijheid. Defensie staat voor die digitale veiligheid, als betrouwbare partner in onze nationale cybersecurity-structuren. Dit ontslaat private partijen overigens niet van hun verantwoordelijkheid om zelf hun eigen beveiliging op orde te hebben.

Het cyberdomein is, net als internationale wateren, toegankelijk voor iedereen; het is een *global commons*. Nationale soevereiniteit is daarom een lastig begrip. Dreigingen, zeker in het digitale domein, stoppen niet bij landsgrenzen. Daarom zoeken wij ook nadrukkelijk de samenwerking met onze bondgenoten in NAVO en EU verband. Binnen NAVO hebben we onder de noemer Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) afspraken gemaakt over de inzet van militaire cyber capaciteiten en binnen de EU werken we aan gezamenlijke capaciteiten zoals een *Cyber Information Domain Coordination Cell* of *Cyber Rapid Response Teams* onder de vlag van *Permanent Structured Cooperation* (PESCO). Daarnaast neemt Defensie deel aan verschillende cyberoefeningen en -trainingen in Europees of NAVO-verband.

We keren terug naar het oude Griekenland. Om zich te beschermen tegen aanvallen van vijandelijke schepen, die probeerden met ramtactieken hun formatie te breken, vormden de Griekse triremen een cirkelvormige *kyklos* ter bescherming. Vanuit die positie konden zij anticiperen op de bewegingen van hun tegenstander en hielden zij de kern van hun vloot, hun vitale belangen, veilig. Een zwakke plek in de *kyklos* betekende een kwetsbaarheid voor het vlootverband. Defensie is één van deze schepen in de cirkel, maar we kunnen het nadrukkelijk niet alleen. Samen met publieke en private partners in Nederland en met onze internationale militaire partners binnen NAVO en EU moeten wij de cirkel gesloten houden. Samen vormen wij een *kyklos* rondom de Nederlandse samenleving: wij beschermen wat ons dierbaar is.

“Cyberveiligheid verdient aandacht van burgemeester”

Foto ANP Foto

Sjoerd Potters is burgemeester van gemeente De Bilt en portefeuillehouder cyberveiligheid binnen het College van Burgemeesters en Wethouders. Zelf is hij van huis uit jurist en geen cyberexpert, maar dat ziet hij niet als een reden om zich niet met het thema bezig te houden. Sterker nog, digitalisering en cyberweerbaarheid raken zoveel andere domeinen dat ze de aandacht van de burgemeester verdienen. Dat we langs de digitale weg kwetsbaar zijn voor ontwrichting, is voor Potters evident. Maar dat we dit niet altijd overal scherp genoeg op het netvlies hebben ook. Hoe kunnen we daar iets aan doen? Welke rol ziet hij weggelegd voor zichzelf als burgemeester en voor gemeenten in het algemeen? Daarover gaan we met hem in gesprek.

Cyberweerbaarheid is in De Bilt onderdeel van de portefeuille van de burgemeester en dat is niet voor niets aldus Potters: “Als je technische mensen spreekt, blijkt het effect van een cyberincident veel groter is dan je als leek zou verwachten. En een incident is ook niet zomaar opgelost. Het is niet een kwestie van de server uitzetten en weer verder. Bewustwording daarvan buiten de technische wereld is belangrijk.

Maar de wereld van cyberweerbaarheid heeft de neiging erg geïsoleerd te blijven. Cyberspecialisten richten zich vooral op hun eigen vakgebied en mensen die erbuiten staan doen het al snel af als “ingewikkeld” en “iets voor specialisten”. Terwijl het digitale domein en het fysieke domein afgelopen jaren steeds meer verweven zijn geraakt en de impact van een cyberincident op de maatschappij groot kan zijn. Dan verdient het de aandacht van de burgemeester. Ik zie het als mijn taak om de verbinding tussen die domeinen te versterken.”

“Een cyberincident heeft steeds vaker en steeds grotere gevolgen in de ‘echte’ wereld. Als de digitale wereld afgesloten wordt zijn bewoners, veel meer dan tien jaar geleden, de dupe. Paspoorten kunnen niet worden uitgegeven, stoplichten en bruggen werken niet of uitkeringen worden niet uitbetaald met alle gevolgen van dien. Een ransomware- of een DDoS-aanval klinkt voor veel mensen abstract. Maar als daardoor een server vastloopt die verkeerslichten regelt, heb je een fysiek effect. Het grappige is dat de ernst van situatie dan groter wordt beleefd en mensen in een andere actiemodus gaan.”

Rampenoefeningen

“Als een incident het fysieke domein raakt, hebben we een crisisstructuur die goed werkt. Maar bij cyberdreiging krijgen we met nieuwe scenario’s te maken. Met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties hebben we vorig jaar een simulatie gedaan van een digitaal incident met impact in het fysieke domein. Daaruit bleek dat we het in het fysieke domein inderdaad goed geregeld hebben. Met name in de overgang van het digitale naar het fysieke domein was ruimte voor verbetering.”

“Als het om digitale zaken gaat, zijn we gewend om binnenshuis te opereren met de Chief Information Security Officer (ofwel CISO) en eventueel met een externe expertise partij, terwijl het juist belangrijk is om ook naar buiten te treden. We moeten eerder hulplijnen inschakelen die we binnen het fysieke domein al hebben opgezet. Daarom gaan we toekomstige trainingen op rampen en incidenten beginnen met een digitale component in plaats van bijvoorbeeld een LPG-tank die dreigt te ontploffen. Waarbij we natuurlijk wel een overloop inbouwen naar de fysieke wereld. Hoe gaat die overgang van digitaal naar fysiek? Hebben we op tijd door wat de gevolgen kunnen zijn? En hebben we de crisisrespons dan op orde? Zo proberen we de twee werelden beter te verbinden. Dat gebeurt voor zover ik weet nog niet bij veel gemeenten.”

Borging binnen de organisatie

“De Baseline Informatieveiligheid Overheid wordt bij ons toegepast en uitgevoerd. Alle gemeenten hanteren die als ondergrens. Het is een fijn middel, want je hoeft niet zelf op zoek naar hoe het moet. Als burgemeester sta ik in nauw contact met de Chief Information Security Officer (CISO). We hebben bijna elke week contact. Ik ben dan wel portefeuillehouder cyberweerbaarheid, maar het is niet alleen iets van mij. Het moet binnen het gemeentelijk bestuur breder gedragen worden.”

In het college bespreekt Potters het thema op vaste momenten in de planning-en-control cyclus. "Ik merk dat het soms ook moeilijk is om de leden mee te krijgen. Ook zij hebben al snel het idee het heel technisch is en hebben de risico’s onvoldoende op netvlies. Daarom doen we binnenkort een cybertraining met het hele college. Om de discussies over cyberweerbaarheid en investeringen ook in de raad goed te kunnen voeren, hebben we twee raadsrapporteurs, die we in aparte sessies samen met de CISO bijpraten. Zij hebben deskundigheid op digitalisering en cyberweerbaarheid en vinden het leuk om de raad daarin mee te nemen.”

Openheid zorgt voor bewustwording

Potters heeft gemeenten eerder opgeroepen onderling meer informatie over cyberincidenten te delen: “Wat betreft informatiedeling zijn we binnen gemeenten de schaamte gelukkig wel een beetje voorbij. We delen onderling meer als er iets gebeurt. Het incident bij gemeente Hollandse Kroon heeft daaraan heeft bijgedragen. Zij zijn toen heel open geweest. Ik vind dat van kracht getuigen. Voor ons was het een belangrijk leermoment en we hebben het er in college uitgebreid over gehad: hoe zijn wij voorbereid? Het heeft voor meer bewustwording gezorgd.”

“Gemeente De Bilt is onderdeel van een samenwerkingsverband van zes of zeven gemeenten”, vervolgt Potters. “De gemeentelijke CISO’s zitten in een poule. Ze wisselen daarbinnen veel kennis en informatie uit en vervangen elkaar indien nodig. Om het hek zo stevig mogelijk te houden, doen we samen regelmatig testen om kwetsbaarheden op te sporen. Daar komt vaak zinvolle informatie uit waar me mee aan de slag gaan. Laatst bleek bijvoorbeeld dat wij onze zaken goed op orde hadden, maar dat een buitenstaander via een kwetsbaarheid bij een andere gemeente binnen twee stappen in onze systemen kon komen. Daar schrokken we van en hebben we natuurlijk ook meteen iets aan gedaan. We hebben ook een crisisteam ingericht voor als er een incident is. Het is helder wie waar verantwoordelijk voor is en wie we moeten inschakelen als we meer expertise nodig hebben. Onze technische mensen staan via de Informatiebeveiligingsdienst voor gemeenten in goed contact met het Nationaal Cyber Security Centrum ofwel NCSC. Vrijwel alle gemeenten hebben dat soort afspraken gemaakt. Goed contact tussen

CISO, bestuurders en de NCSC is van groot belang. Je moet weten hoe de lijnen lopen en de lijnen moeten kort zijn."

Volgens Potters ben je voor cyberweerbaarheid sterk afhankelijk van andere partijen in je netwerk. "Niet alleen van andere gemeenten, maar ook van uitvoerende organisaties en dienstverlenende bedrijven. Zo was er een datalek in het snelheidscamerasysteem in een van de dorpen. Het bleek makkelijk kentekengegevens uit te lezen. We hadden het op papier helemaal goed geregeld met die partij in een verwerkersovereenkomst. Maar met het sluiten van overeenkomsten ben je er niet, je moet toezicht houden door de juiste te vragen stellen. Een landelijk keurmerk voor digitale dienstverleners zou ons daar wel bij kunnen helpen. We hebben ook een Voedsel- en Warenautoriteit. Die checkt op zaken die niet iedereen zomaar kan doorgronden maar wel gecontroleerd moeten worden in het algemeen belang. Veilige digitale dienstverlening is ook van groot algemeen belang."

Nationale cyberweerbaarheidsstrategie

Potters ziet dat cyberdreiging van verschillende kanten komt en toeneemt: "Daar moeten we ons als samenleving veel meer samen en integraal op voorbereiden. Welke rol we als gemeente spelen, is afhankelijk van waar dreiging vandaan komt. Als die bijvoorbeeld interstatelijk is, zal de centrale overheid coördinerend moeten optreden om de crisis te bezweren, maar wij moeten als gemeente in staat zijn om de maatschappelijke effecten te beperken. Lokaal moeten gemeenten hun zaken op orde hebben, binnen de veiligheidsregio oefenen en afspraken maken. We moeten een cyberincident aanvliegen als een klassieke ramp. Bij fysieke incidenten zijn gemeenten in de lead, maar een cyberincident is natuurlijk minder afgebakend. Dan is de vraag wat wordt er verwacht van veiligheidsregio's en gemeenten. Daar goede afspraken over maken is essentieel. Voor zover ik weet zijn die er nog niet. Nu is het wachten tot er een keer iets gebeurt en dat is zonde. Wij leren overigens lessen van de COVID-crisis over afspraken tussen het Rijk, de veiligheidsregio's en gemeenten. Daar speelt ook regelmatig de vraag: wie is waar verantwoordelijk voor? Ik hoop en verwacht dat die lessen hun weg vinden naar het cybersecurity-domein. Bij de Vereniging van Nederlandse Gemeenten ziet Potters dat cyberweerbaarheid een belangrijk aandachtspunt is en daar ziet hij zeker een belangrijke rol voor gemeenten weggelegd. "Maar ik denk ook dat digitalisering en cyberweerbaarheid zo belangrijk zijn, dat een ministerie met dat als specifiek taakveld op zijn plaats zou zijn. Daarmee straal je als overheid het belang van het thema uit en geef je het een gezicht in het publieke debat. Dat kan ook helpen bij het bevorderen van de bewustwording."

Veilig internet en veilige samenleving via Nederlandse stijl

Foto Jeroen de Bakker

In Nederland is elke dag een organisatie het slachtoffer van een aanval van cybercriminelen. In oktober 2021 verscheen de digitale aanval op industrieconcern VDL in het nieuws, waarbij wereldwijd 105 bedrijven werden geraakt, ook in Nederland. Zo kwam onder andere een groot deel van de productie van auto's bij Nedcar in Born stil te liggen. Recent nog blijkt ook Log4j, een belangrijke softwaretool voor veel internetapplicaties, een ernstige kwetsbaarheid te bevatten. Het gros van hacks, kwetsbaarheden en ransomware-aanvallen krijgt echter helemaal geen aandacht. De Nederlandse overheid zet veel stappen om te werken aan een cyberweerbare samenleving onder meer met de vorming van het Landelijk Dekkend Stelsel van informatieknooppunten (LDS). Een van de betrokken organisaties in het LDS is Dutch Institute for Vulnerability Disclosure (DIVD), zij zijn kritisch maar hoopvol over de toekomst van het stelsel.

DIVD draagt bij aan meer veiligheid op digitaal gebied, door het preventief waarschuwen van organisaties voor kwetsbaarheden in hun digitale systemen voordat kwaadwillende hackers hier gebruik van maken. Chris van 't Hof, een van de oprichters van de stichting, en Frank Breedijk, een ethisch hacker die al vanaf

het begin bij DIVD is betrokken, vertellen over hun drijfveren, missie en de rol die zij voor het DIVD en de overheid zien in de toekomst.

Van kwetsbaarheid tot hack

De urgentie van het werk ligt volgens Chris bij het volgende: 'Wij scannen het hele internet, waarbij er kwetsbaarheden naar voren komen. We zien daardoor de hoeveelheid potentiele slachtoffers, verbazen ons hoe weinig slachtoffers bekend worden en beseffen dat het gros van de wel gehackte organisaties niet in het nieuws komt.''

Wat wel in het nieuws komt zijn de grote zaken, zoals de kwetsbaarheid van de softwaretool Log4J en die rondom softwareleverancier Kaseya. Hun software werd door Revil, een waarschijnlijk Russische groepering, gehackt. De hackers van DIVD hadden twee maanden daarvoor al acht kwetsbaarheden in de software geconstateerd en gemeld bij Kaseya. Het ontwikkelen van een patch (een update van het systemen waardoor het weer veilig is) was echter net niet op tijd klaar. Dat lek in het systeem betekende miljoenen potentiële slachtoffers, wat uiteindelijk leidde tot duizenden echte slachtoffers. Kaseya werkte samen met onder andere DIVD aan oplossingen voor de hack.

De Kaseya-zaak maakt voor Van 't Hof het belang van een LDS en het bestaansrecht van DIVD weer duidelijk: ''Er ligt hier een taak, namelijk het scannen van het internet en het melden van de kwetsbaarheden, die nog niet goed kan worden opgepakt binnen het stelsel.''

Het LDS is een structuur waarbinnen publieke en private partijen samenwerken om informatie en kennis over cybersecurity uit te wisselen met als doel digitale ontwrichting te voorkomen én Nederland cyberweerbaarder te maken. Dit zijn partijen zoals CERTs (computercrisisteams), sectorale en regionale samenwerkingsverbanden, het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center (DTC). Volgens Van 't Hof kan een groot deel van de organisaties in Nederland niet worden bediend door dit LDS: ''dat zijn bijvoorbeeld de midden- en kleinbedrijven, websites van sportclubs of volkstuinen en de kleine webshops. Deze gaten in het LDS vullen wij op met ons onderzoek, want wij scannen iedereen.''

Informatiedelen is key

Van 't Hof en Breedijk zijn blij met de nieuwe ontwikkelingen die er nu omtrent het LDS gaande zijn, waarbij er een vernieuwende publiek-private samenwerking wordt opgezet. Want, de overheid is nu eenmaal gebonden aan wet- en regelgeving die zorgt voor beperkingen in de mogelijkheden. Beiden zijn optimistisch dat er nu een wetswijziging voor de Wet beveiliging netwerk- en informatiesystemen (Wbni) in de maak is om het LDS verder vorm te geven. Ook over de aanpak vanuit de overheid rondom de kwetsbaarheid in de softwaretool Log4J zijn zij positief. Het NCSC heeft hier wel de nationaal coördinerende rol op zich genomen. Zij zijn echter wel van mening dat het drie voor twaalf is en dat er meer snelheid nodig is, het particuliere initiatief is daarom nu broodnodig volgens hen.

Van 't Hof: ''Ons initiatief is een samenwerking met de overheid, maar we kunnen het niet vanuit de overheid laten organiseren. Een overheidsorgaan kent beperkingen in het ongevraagd scannen en melden van kwetsbaarheden in systemen. Deze komen voort uit bijvoorbeeld de Algemene verordening gegevensbescherming (AVG) en de Wbni. Maar wij opereren vanuit een jurisprudentie, waarin de rechter heeft gezegd dat scannen en melden mag wanneer je handelt in maatschappelijk belang, je het proportioneel doet en het op geen andere manier kan.''

Op de vraag of de overheid hun taken niet moet overnemen, zijn Van 't Hof en Breedijk duidelijk: ''We opereren in een niche waarin de overheid en het bedrijfsleven (nog) niet in kunnen acteren, waarmee we een zeer directe bijdrage aan de nationale veiligheid leveren. Het veilig houden van internet is een taak in het algemeen belang en moet dus bij de overheid liggen, zoals zij dit nu ook doen bij de kwetsbaarheid in de softwaretool Log4j. Maar zolang het DIVD dit op een manier kan en doet die de overheid nog niet kan, hebben we bestaansrecht.'' Neemt de overheid hun taak over? Breedijk: ''Dan is er wel een ander probleem waar wij als vrijhaven voor creatieve en ethische hackers mee aan de slag kunnen.''

Samenwerking overheid en DIVD

''Vergelijk ons met het Rode Kruis. Dat zij bestaan, betekent niet dat er geen ambulances en ziekenhuizen meer nodig zijn. Zij komen alleen op plekken waar de overheid niet kan of wil komen'', vervolgt Breedijk.

Dat een onafhankelijke organisatie dit werk oppakt, is volgens Van 't Hof ook nog om een andere reden belangrijk. "Het gaat om een ongelofelijke hoeveelheid data, waarmee je ook macht in handen hebt. Wanneer een overheid of bedrijf dit in handen heeft, ontstaat al snel een situatie waarin ze het ook zouden kúnnen gebruiken voor andere zaken dan cybersecurity. Alleen die schijn moet en kun je al voorkomen, door het bij een onafhankelijke organisatie als het DIVD neer te leggen."

Het DIVD wijst dan alle organisaties op hun kwetsbaarheden en potentiële lekken. Breedijk vergelijkt een waarschuwing van het DIVD met het luchtalarm. ‘’Wil je het luchtalarm niet horen? Dan heb je pech. Zo ook onze meldingen: je kunt ze wel negeren, maar we zullen ze altijd blijven versturen zodra we een kwetsbaarheid ontdekken.’’

Nederland voorloper

‘’Toen Nederland in 2016 voorzitter was van de EU, kwam iedereen hier kijken hoe wij bezig waren op het gebied van de Coordinated Vulnerability Disclosure”, vervolgt Van 't Hof. “We waren en zijn op dat gebied echt voorloper, de Nederlandse digitale poldercultuur is uniek. Dit is in het buitenland wel anders, waar vaak twee smaken mogelijk zijn: het scannen en melden mag echt niet en dit betekent dat er snel tegen je geprocedeerd wordt of de overheid zegt dat er zoveel gehackt wordt, dat beleid daartegen helemaal geen zin heeft.’’

Het feit dat de Nederlandse overheid de activiteiten van DIVD toestaat en zelfs met de organisatie samenwerkt, zien beide DIVD’ers als een duidelijk signaal van welwillendheid vanuit de overheid. Het coördineren en samenwerken is uniek en is een goede en essentiële stap op weg naar meer veiligheid op het internet.

Idealistische hackers

Het werken aan het grotere maatschappelijke goed benoemt Van 't Hof als belangrijke drijfveer voor alle DIVD’ers: ‘’het rechtvaardigheidsgevoel is bij iedereen aanwezig, waardoor je samenwerkt met gelijkgestemden aan een gemeenschappelijk doel: het veiliger maken van het internet en daarmee onze samenleving.’’ Breedijk vult aan: ‘’Zodra mensen het internet niet meer vertrouwen, betekent dat het einde van het internet. Terwijl het internet zo mooi en belangrijk is, ook voor onze samenleving. Veiligheid is een basis voor vertrouwen.’’

Van 't Hof: ‘’Wat ook niet onderschat moet worden is de lol, creativiteit en inspiratie die voortkomt uit het werken bij DIVD, met al die bijzondere mensen waarmee je samenwerkt. De DIVD’ers werken meestal zelf ook in de ICT, maar binnen DIVD hebben ze echt alle vrijheid om te doen wat ze leuk vinden en goed kunnen voor een mooi maatschappelijk doel.’’ Breedijk vult aan: "Het is heel fijn om samen met anderen deze passie te delen en daar je ziel en zaligheid in te leggen.’’

Race om innovatie in cyberdomein

Foto Hollandse Hoogte - ANP Foto

Om ervoor te zorgen dat Nederland nu en in de toekomst cyberweerbaar en voldoende digitaal autonoom is, vormt versterking van onderzoek, onderwijs en innovatie een van de belangrijkste speerpunten. Dat concludeerde de Cyber Security Raad (CSR) vorig jaar in het adviesrapport ‘Integrale aanpak cyberweerbaarheid’. Eddy Boot, in juni 2021 aangetreden als directeur van dcypher, hoopt hier met zijn samenwerkingsplatform een belangrijke rol in te spelen. “Effectief samenwerken vereist een verandering van aanpak en gedrag van alle betrokken partijen.”

Boot, die ruim twee decennia bij onderzoeksinstituut TNO werkzaam was en daar veel ervaring opdeed met publiek-private samenwerkingen, vergelijkt de totstandkoming van innovatie en de uitdagingen die daarmee gepaard gaan graag met een estafetterace. “Een hoogleraar en diens promovendi gaan van start met fundamenteel onderzoek. Op enig moment geven zij het estafettestokje over aan de toegepaste onderzoekers, bijvoorbeeld aan een partij als TNO. Die helpen op hun deel van het traject de innovatie verder naar volwassenheid door samen te werken met onderzoeksconsortia, *spin outs* of startups. Vervolgens geven zij het stokje weer over aan de cyberindustrie die er nieuwe producten en diensten van kan maken. En zo komt het estafettestokje, en daarmee de innovatie, uiteindelijk bij de eindgebruiker terecht. Tot zover klinkt dat goed, maar iedereen die weleens een echte estafetterace heeft gezien, weet ook wat het grootste risico is. Namelijk dat

een van de lopers het stokje uit handen laat vallen. Dat gevaar ligt ook bij innovatie op de loer, wat wel blijkt uit de wat zwaar aangezette beeldspraak van *the valley of death*. Veel potentieel vernieuwende producten en diensten sneuvelen gedurende het innovatieproces in deze gedoemde vallei. Bijvoorbeeld omdat aanbieders en eindgebruikers onvoldoende of slechts lokaal worden bereikt. Of omdat de bestaande financieringsmogelijkheden niet worden gevonden."

Zo ligt de vallei des doods bezaaid met gemiste kansen, en daar wil Boot verandering in brengen. Zijn oplossing? De samenwerking rond innovatie in het cybersecuritydomein moet niet pas vanaf de finishlijn plaatsvinden, maar al bij het startschot. “Als alle partijen vanaf de start aan boord zijn, levert dat niet alleen een groter commitment van de betrokkenen op. Je speelt ook in op het feit dat innovatie zelden lineair verloopt. Dit maakt het lastig om bepaalde fasen van onderzoek, innovatie en valorisatie vooraf aan te wijzen en te bepalen wanneer partijen het beste kunnen instappen”, zo redeneert de dcypher-directeur.

Als ‘platform der platformen’ wil Boot er met dcypher voor zorgen dat de partijen die het verschil kunnen maken gezamenlijk aan de startlijn verschijnen. “Iedereen houdt het stokje vast en draagt daarmee verantwoordelijkheid. En alle partijen gaan zo samen richting de finish. Het gevolg: de hoogleraar krijgt op het juiste moment de relevante onderzoeksvragen, de toegepaste onderzoekers zijn beter in staat om de innovatie in het veld te testen, cyberaanbieders kunnen sneller ontwikkelen en eindgebruikers starten vroegtijdig aan het implementeren van de nieuwe producten en diensten”, schetst Boot.

Door die betere samenwerking binnen het cybersecuritydomein moet een aantal problemen worden getackeld. Boot ziet onder meer een gebrek aan cybersecurity-expertise en het ontbreekt bovendien aan het valoriseren van innovaties. “De doelstellingen van dcypher zijn daarom duidelijk: meer mensen, meer kennis en toepassing en meer valorisatie”, vertelt hij. Daarbij is er volgens Boot een cruciale rol voor innovatie weggelegd. “Alleen met echt nieuwe soorten oplossingen kunnen we de huidige problemen het hoofd bieden.”

Winnende equipe

In de estafetterace om Nederland veiliger, slimmer en digitaal autonomer te maken, wil Boot met dcypher de sportcoach zijn die ervoor zorgt dat er een winnende equipe aan de start verschijnt. Een rol waarin hij zelf dus ook pas kortgeleden van start is gegaan. Tijdens zijn eerste maanden als dcypher-directeur trok Boot vooral het veld in om scherp te krijgen waar de kansen en uitdagingen liggen. Daarbij vielen hem verschillende zaken op. “Ik zie veel betrokkenheid, nieuwe ideeën, grote ambities en de bereidheid van partijen om samen te werken. Ook is de omvang en het aantal partijen op het gebied van cybersecurity vrij beperkt, waardoor dit veld redelijk goed te overzien is. Veel van deze partijen in onderwijs, onderzoek, bedrijfsleven en overheid kennen elkaar al lang en kennen de uitdagingen waar de sector voor staat. Wat mij ook opvalt is de behoefte aan meer middelen en betere samenwerking in het veld”, zo geeft hij aan.

De problematiek op het gebied van cybersecurity is volgens Boot complex, omdat elke individuele partij, organisatie en autoriteit zijn eigen mogelijkheden, maar ook zijn eigen beperkingen heeft. “Geen van deze partijen is in staat de problemen volledig onafhankelijk van de andere partijen op te lossen. Daarom is er meer multidisciplinaire samenwerking nodig, over de hele cybersecurity-innovatieketen. Ik geloof er daarbij in dat echt effectief samenwerken een verandering van aanpak en gedrag van alle betrokken partijen vereist. We zullen allemaal rekening moeten houden met elkaars vaak verschillende positie, perspectieven en belangen. En je moet elkaar soms ook wat willen gunnen, voor het grotere geheel. Het gaat erom een scherpe, gezamenlijke ambitie te formuleren en die vervolgens waar te maken.”

Spin in het web

Als samenwerkingsplatform kan dcypher een belangrijke rol spelen om de sector dichter bij elkaar te brengen, hoopt Boot. “Wij zijn een onafhankelijke spin in het web. Vanuit die makelaarsrol stimuleren we partijen in het cybersecuritydomein om beter samen te werken op het gebied van innovatie. De innovaties die hieruit voortkomen, zullen de slagkracht en effectiviteit van cybersecurity in Nederland verbeteren, zowel strategisch en tactisch als operationeel. Tegelijkertijd hebben wij natuurlijk ook geen magisch elixer om vraag, aanbod en financiering beter bij elkaar te brengen”, zo geeft hij toe. “Wat we wél kunnen doen, is een voorbeeld stellen voor anderen, het veld activeren om samen te focussen op de problemen die eerst moeten worden opgelost en het oplossen van deze problemen vervolgens te faciliteren. Daarnaast kunnen we helpen om financiering onder de juiste voorwaarden te krijgen en er ten slotte voor te zorgen dat de gehele cybersecurity-innovatieketen - van onderwijs en onderzoek tot bedrijfsleven en overheid - optimaal is ingericht. Veel mensen hebben elkaar al gevonden en zijn deels al goed georganiseerd. Voor dcypher ligt er de mooie taak om dat te stroomlijnen en naar een volgende fase te brengen door vraag en aanbod beter op elkaar aan te laten sluiten.” Boot bouwt als directeur van dcypher door op het werk dat de voorganger van het platform de afgelopen jaren heeft verzet. Voor de komende vier jaar ziet hij een aantal duidelijke prioriteiten. “De afgelopen periode heeft het platform veel

bereikt op het gebied van onderwijs en onderzoek. Dat wil ik verder versterken en uitbouwen."

Verdienvermogen

Als belangrijk nieuw aspect noemt hij valorisatie: het verdienvermogen van cybersecurity door innovatie. Boot: "We willen producten en diensten sneller op de markt hebben door kennisontwikkeling te versnellen, de cyberindustrie te versterken en het absorptievermogen van eindgebruikers te verhogen. Daarvoor werken we momenteel onder meer aan een digitaal portal om financieringsinstrumenten beter toegankelijk en toepasbaar voor het cybersecurityveld te maken (zie kader). Ook zijn we bezig met het organiseren van een matchmaking event met bedrijven en onderzoeksinstellingen in de EU en starten we meerjarige *roadmaps* waarin partijen over de hele keten langjarig samenwerken aan onderzoek, toepassing en economische bedrijvigheid. Het is echt tijd om door te pakken. Of, zoals Europarlementariër Bart Groothuis dcypher onlangs toevertrouwde: strategie is executie, en executie is strategie."

"Nederland moet bepalen waar we van zijn"

Foto Nationale Beeldbank

In februari 2021 werd de ACademic Cyber Security Society (ACCSS – spreek uit access) opgericht. Een vereniging voor wetenschappers in Nederland die actief zijn op het gebied van cybersecurity. Inmiddels hebben ruim 90 wetenschappers en 8 onderwijsinstituten zich bij ACCSS aangesloten en de organisatie verwacht de komende jaren nog flink te groeien. Dat is niet alleen belangrijk voor de wetenschap, maar ook voor de Nederlandse strategie op het gebied van cyberveiligheid. We spreken hierover met Bibi van den Berg, als Hoogleraar Cybersecurity Governance verbonden aan de Universiteit Leiden en voorzitter van ACCSS (en tevens lid van de Cyber Security Raad namens de wetenschap) en Aiko Pras, professor cyberveiligheid aan de Universiteit Twente en vicevoorzitter van ACCSS.

In oktober 2020 stopte het oude dcypher, een netwerkorganisatie voor cybersecurity. Daarmee verdween onder andere een belangrijke verbindingsplek voor cybersecuritywetenschappers. ACCSS heeft dit gat opgevuld. Daarom ziet Bibi van den Berg verbinding ook als een belangrijke taak van de vereniging: "ACCSS is geboren vanuit het idee dat cybersecuritywetenschappers in Nederland behoefte hebben aan een vaste plek van waaruit we aan een eigen netwerk kunnen bouwen." Dat is volgens Van den Berg ook de reden waarom ACCSS zowel bèta, alfa en gamma-wetenschappers verbindt. "Cybersecurity is een multidisciplinair vakgebied wat grenzen binnen de academische wereld overschrijdt. Helaas is er tussen veel wetenschappers soms nog geen goed contact, terwijl ze wel met dezelfde thematiek te maken hebben. Wij wilden een plek creëren waar wetenschappers elkaar makkelijk kunnen vinden voor project- of subsidieaanvragen."

Ook Aiko Pras ziet een belang voor ACCSS om wetenschappers te verenigen: "Als je naar de cybersecuritydreigingen kijkt die op ons afkomen, dan groeien die veel sneller dan mensen lang voor mogelijk hielden. Het besef begint nu te komen dat het onze samenleving bedreigt. Tegelijkertijd hebben we een groot tekort aan experts die hierover kunnen adviseren. Daarom is het belangrijk om ons als wetenschappers te verenigen, zodat we meer onderzoek kunnen doen en het onderwijs kunnen verbeteren."

Met één stem spreken

Een derde pijler is zichtbaarheid. Via ACCSS is het mogelijk om beter en vaker de stem van de wetenschap te laten horen. "Het is belangrijk dat we vanuit de wetenschap een bijdrage leveren aan alle plannen en agenda's die momenteel worden ontwikkeld", stelt Van den Berg. "Natuurlijk kunnen standpunten van wetenschappers van elkaar verschillen, er moet ruimte blijven voor verschil van

inzicht, maar op bepaalde belangrijke onderwerpen wil je wel met één mond spreken. Doordat ACCSS bestaat is dat echt een vertegenwoordigde stem."

Die stem laat de organisatie dan ook geregeld horen. Deze zomer deed ACCSS een oproep om het betalen van losgeld voor ransomware door publieke partijen te stoppen en in september publiceerde het een oproep om gegevens over datalekken openbaar te maken voor verder onderzoek. Momenteel werkt de organisatie aan een voorstel voor een Groeifonds om onderzoek en onderwijs in cybersecurity verder te bevorderen. Daarin moet budget beschikbaar komen voor onderzoek en scholing.

ACCSS werkt ook samen met het in de herfst van 2021 opnieuw opgerichte dcypher, wat nu onder het ministerie van EZK valt. Van den Berg legt uit: "Dcypher is bezig met het opstellen van een onderzoeks- en onderwijsagenda, daar dragen wij aan bij. We zien onszelf daarom ook als een van de belangrijke onderaannemers van dcypher." Volgens Pras gaat die rol zelfs veel verder dan onderaannemerschap. "Het voordeel van ACCSS is dat we naast de bestaande hiërarchie staan die je bijvoorbeeld ziet bij de overheid. Daardoor sta je sterker en kan je beter invloed uitoefenen. Dcypher heeft ons dus ook heel hard nodig."

Verbeteren vindbaarheid

Naast verbinding is vindbaarheid een tweede taak van het ACCSS. Van den Berg: "Sommige cybersecuritywetenschappers zijn heel zichtbaar voor media, in het publieke debat en voor financiers van onderzoek. Dat geldt alleen lang niet voor iedereen. Het is daarom waardevol dat er een plek is met één brievenbus, waar iedereen die in contact wil komen met cybersecuritywetenschappers terecht kan." Dat daar behoefte aan is, werd direct na de oprichting duidelijk: "Er waren direct partijen die ACCSS benaderden met hulpvragen, bijvoorbeeld voor het uitzetten van projecten. Ze hadden de middelen, maar waar moesten ze zijn? ACCSS vervult dan een soort makelaarsfunctie: we koppelen de juiste wetenschapper aan het juiste project. Dat doen we niet alleen voor Hoogleraren, maar we hebben bijvoorbeeld ook een groep PhD-studenten die nu werk en onderzoek combineren voor de overheid."

Verbinden van werelden

Waar liggen nog kansen voor de samenwerking tussen wetenschappers? Volgens Pras is dat duidelijk: "Als je naar het verleden kijkt, zie je dat de technische aspecten van cybersecurity altijd goed gecoördineerd waren. We zagen elkaar en we werkten samen. Maar de huidige problemen zijn veel minder technisch van aard, denk bijvoorbeeld aan nepnieuws. Op die gebieden is cybersecurity pas net aan het opkomen. Er verschijnen allemaal clubjes met eigen specialisaties. Cybersecurity is voor hen allemaal nieuw en ze kennen elkaar nog niet. Hoe krijgen we de niet-technische wereld bij elkaar?"

"En het gaat ook om verbinding maken tussen technische mensen en niet-technische mensen", vult Van den Berg aan. "Ik heb een sterk netwerk in niet-technische onderwerpen, maar de connectie met de bèta's, daar gaat het vaak mis. Terwijl het zo belangrijk is om iedereen aan tafel te hebben. Veel onderzoeksprojecten hebben daarnaast als eis dat er multidisciplinair gewerkt moet worden. Dan moet je de juiste mensen wel kunnen vinden."

Juiste vragen boven tafel krijgen

Wetenschappelijke kennis en inzichten zijn belangrijk in het huidige cybersecuritylandschap. De wetenschap heeft namelijk een aantal waardevolle kenmerken. Van den Berg legt uit: "Wetenschappers zijn van de laatste ontwikkelingen en kennis op de hoogte. Ook juist over zaken die nog niet breed bekend zijn. Daarnaast brengen we onafhankelijke expertise in. Wanneer bedrijven adviseren zitten daar soms ook belangen achter. Dat is bij wetenschappers minder het geval."

Volgens Pras zijn wetenschappers ook belangrijk om de juiste vragen boven tafel te krijgen. "In gesprekken tussen de overheid en sectoren wordt vaak de vraag gesteld wat er in die sector moet gebeuren op het gebied cybersecurity. Het is alleen heel lastig om dat te benoemen als cybersecurity niet je kerntaak is. Tegelijkertijd liggen veel sectoren wel wakker van het onderwerp. Juist in dit soort gesprekken is het belangrijk dat de wetenschap aanschuift." Ook Van den Berg benadrukt het belang van wetenschap in publiek-private samenwerking: "Ik word als hoogleraar vaak gevraagd om organisaties en bedrijven mee te helpen met vraag-articulatie. Het is allemaal zo beginnend en nieuw dat het voor veel organisaties niet duidelijk is welke vragen je beantwoord moet hebben om het op orde te hebben."

Doorgeslagen poldermodel

Over de staat van cybersecurity in Nederland zijn beide hoogleraren twijfelend. Volgens Pras zijn er zeker lichtpuntjes: "Wetenschappelijk zie je een aantal initiatieven en onderzoeken in Nederland die heel hoog zijn aangeschreven en ontzettend goed werk doen." Maar als je naar het grotere geheel kijkt, is Pras minder positief: "Kijk naar het buitenland en hoe daar wetenschap en onderwijs

wordt gebruikt en gefinancierd voor innovatie op het gebied van cybersecurity, dan hebben wij nog mijlen te gaan." Ook Van den Berg constateert dat de Nederlandse kenniseconomie op het gebied van cybersecurity langzaam wordt uitgehold, waarbij lage investeringen volgens haar leiden tot een *braindrain*. Daarom is het volgens haar ook belangrijk dat het onderwijs meer aandacht en financiering krijgt: "Dat gaat niet alleen om jonge mensen op de universiteiten of post-masters, maar ook om Leven Lang Leren. Er komen steeds meer mensen die vanuit een andere rol of functie een baan krijgen in cybersecurity en *on the job* moeten leren hoe alles werkt. We moeten met kennisinstellingen en trainingsinstituten veel meer opleidingen voor professionals realiseren. Sommige universiteiten zijn daar al mee bezig, maar het moet verder worden uitgebouwd." Pras valt bij: "Onderwijs wordt als vanzelfsprekend gezien. Maar we moeten onze focus verbreden. Niet alleen kijken naar de universiteiten en hogescholen, maar ook iets bieden aan zij-instromers en doorstromers. Misschien moeten we wel al op de basisschool beginnen."

Ook op het gebied van onderzoek zijn beide hoogleraren kritisch. Van den Berg ziet dat er vaak te weinig met wetenschappers wordt gesproken voordat er onderzoeken worden uitgezet: "Er wordt te veel in de markt opgehaald waar behoefte aan is. Maar niemand heeft dan gevalideerd of er mensen in de wetenschap zijn die daar al mee bezig zijn of iets mee kunnen." Van den Berg pleit dan ook voor meer ruimte voor onderzoeksagendering: Dat betekent niet dat we onze eigen voorstellen gaan maken, maar nu is het wel heel erg de andere kant op. Daardoor valt ook veel onderzoek buiten de boot, zoals fundamenteel onderzoek en onderzoek naar *cutting edge* technologie."

Ook Pras ziet de mismatch op het gebied van onderzoeksvraag en -aanbod. "Waar kan je geld voor krijgen? Vooral voor onderzoek ingegeven door de actualiteit: ransomware, passwordmanagers en back-up-strategieën. Zeker belangrijk, maar aan de grote dingen die we ook nodig hebben, komen we daardoor niet toe."

Waar wordt Nederland van?

Politiek gezien kunnen er volgens beide Hoogleraren nog flinke stappen worden gezet. Dat ligt vooral aan de manier van besluitvorming in Den Haag volgens Pras: "Ik zie dat ons mooie Poldermodel doorgeslagen is. Niemand durft een keuze te maken. Als je dan naar de Europese Unie kijkt, kan je veel zeggen, maar daar gebeurt wel wat, bijvoorbeeld de bouw van een *competence centre* in Roemenië." Het gebrek aan daadkracht brengt volgens Pras een aantal risico's met zich mee: "Nederland draait op een oude economie. De nieuwe economie is een IT-economie, met platformen als Booking.com en Thuisbezorgd. Je moet zorgen dat er op cybersecurity een infrastructuur is die dat kan ondersteunen en de juiste mensen om eraan te werken. Anders kom je er over 10-15 jaar achter dat alles in andere landen zit. Als je maar blijft praten en niet investeert, dan komt er niks."

Ook Van den Berg vindt het tijd dat Nederland de afwachtende houding van zich afschudt: "De grote vraag die Nederland moet beantwoorden is: 'waar worden wij van?'. Dan kan je vervolgens stappen zetten. Cybersecurity is nu ondergebracht bij verschillende ministeries, dan valt er ook veel tussen de kieren door." ACCSS pleit daarom, net als de CSR in het laatste adviesrapport, voor meer regie op het onderwerp. Van den Berg: "Kijk naar een thema als water. Daar hebben we een deltacommissaris aangesteld, los van alle ministeries. Die maakt een plan voor de komende 25 jaar. We zijn kennisleider op dat onderwerp, omdat we hebben gezegd: hier zijn we van."

Tijd om aan de slag te gaan

Van den Berg verbaast zich dan ook waarom Nederland dat niet doet op het gebied van cybersecurity: "Nederland heeft goede randvoorwaarden. We zijn een klein land met hoge internetdichtheid en veel knappe koppen. We kunnen een perfect ecosysteem creëren, maar dan moet je er wel aan beginnen." Pras vult aan: "We kunnen een sterke positie innemen, niet door belastingvoordelen, maar juist door ons ecosysteem." Beide Hoogleraren pleiten dan ook vooral om aan de slag te gaan: "Er liggen genoeg plannen en strategieën, het is tijd dat we dingen gaan uitvoeren. Daar is alleen wel een overkoepelende visie voor nodig."

Elk bedrijf is vitaal

Foto KPN

Sinds de tweede week van december 2021 heeft een kwetsbaarheid in software, die in de media bekend staat als log4j of log4shell, een zeer groot beveiligingsrisico opgeleverd voor iedereen die gebruikmaakt van digitale diensten, in Nederland en wereldwijd. In Nederland adviseert het Nationaal Cyber Security Centrum (NCSC) dan ook aan overheden en bedrijven om zo snel mogelijk te patchen of workarounds in te voeren, en nog belangrijker, om zich voor te bereiden op (grootschalig) misbruik van deze kwetsbaarheid door kwaadwillende partijen. Het toont opnieuw aan hoe kwetsbaar onze digitale samenleving is.

Om een veilige en weerbare digitale infrastructuur te bereiken, is nog veel werk te verrichten. Werk dat nooit 'af' is. Cybersecurity vraagt om permanente aandacht. Zeker voor de vitale sectoren waarvan het functioneren voor de Nederlandse samenleving van fundamenteel belang is. Potentiële cyberaanvallen op energiecentrales, de Rotterdamse haven, bruggen en sluizen, om maar een paar voorbeelden te noemen, kunnen een ongekende economische en sociale impact hebben. Cybersecurity is dus *chefsache* en de weerbaarheid van vitale sectoren is van nationaal belang. Samenwerking en informatiedeling tussen het bedrijfsleven, de wetenschap en de overheid zijn belangrijk. Ook het verbeteren van risico- en dreigingsanalyses en gezamenlijk oefenen horen daarbij. Ik ondersteun dan ook de voorgestelde wetswijziging voor ruimere ontsluiting van dreigings- en incidentinformatie over systemen. Een beter begrip van de risico's leidt tot betere bescherming, en maakt Nederland weerbaarder.

Het verbeteren van cyberweerbaarheid is een kat-en-muisspel. Kwaadwillenden hebben doelen, tactieken en technieken die steeds veranderen. Digitale aanvallen zijn reëel. De overheid en het bedrijfsleven doen daar veel tegen, maar nog niet genoeg. Bedrijven hebben hulp nodig van de overheid om criminelen buiten de deur te houden en op te sporen. De Nederlandse overheid investeert volgens onderzoek van de Cyber Security Raad (CSR) minder in cyberweerbaarheid dan de ons omringende landen. Zo is de Belgische investeringsambitie 14 keer hoger dan de Nederlandse. Nederland dreigt zo de regie te verliezen en achterop te raken in een digitale wereld die per definitie internationaal is en waar aanvallers altijd naar het zwakste punt zoeken. De CSR heeft ervoor gepleit om de investeringen in cyberweerbaarheid op te voeren en meer in lijn te brengen met de ons omringende landen. In het coalitieakkoord wordt aangegeven dat er zal worden geïnvesteerd in een 'brede meerjarige cybersecurity aanpak'. Dat is een goede eerste stap en het is belangrijk dat we hier nu op doorpakken. Daarbij is het van belang dat we het midden- en kleinbedrijf (mkb) niet uit het oog verliezen. Deze ruggengraat van de Nederlandse economie is immers ook vitaal. Het mkb heeft nu vaak niet de middelen om zichzelf goed te beschermen; schaalbare oplossingen op het gebied van cyberweerbaarheid kunnen hierbij helpen.

Uiteindelijk valt en staat digitale veiligheid met een hoog bewustzijn van de kansen en risico's. Onze digitale weerbaarheid vraagt de komende jaren om verhoogde alertheid en actie. Dat moeten we samen doen: een betrokken overheid, kennisinstituten en het bedrijfsleven, waar het mkb essentieel onderdeel van uitmaakt.

"Snel digitaliserende samenleving maakt cybersecurity tot topprioriteit"