CSR MAGAZINE

Cyber Security Council
Cyber Security Raad

Het belang van een integrale aanpak voor cyberweerbaarheid • Top aan het woord over het belang van een integrale cyberweerbaarheidsstrategie en het versterken van onze digitale autonomie met behoud van een open economie.

The importance of a comprehensive approach to digital resilience • High-level governnent-officials and businessleaders speaking about the importance of a comprehensive cyber strategy and strengthen our digital autonomy while maintaining our open economy.

Jaargang 6, nummer 1, februari 2022
Volume 6, Issue 1, February 2022

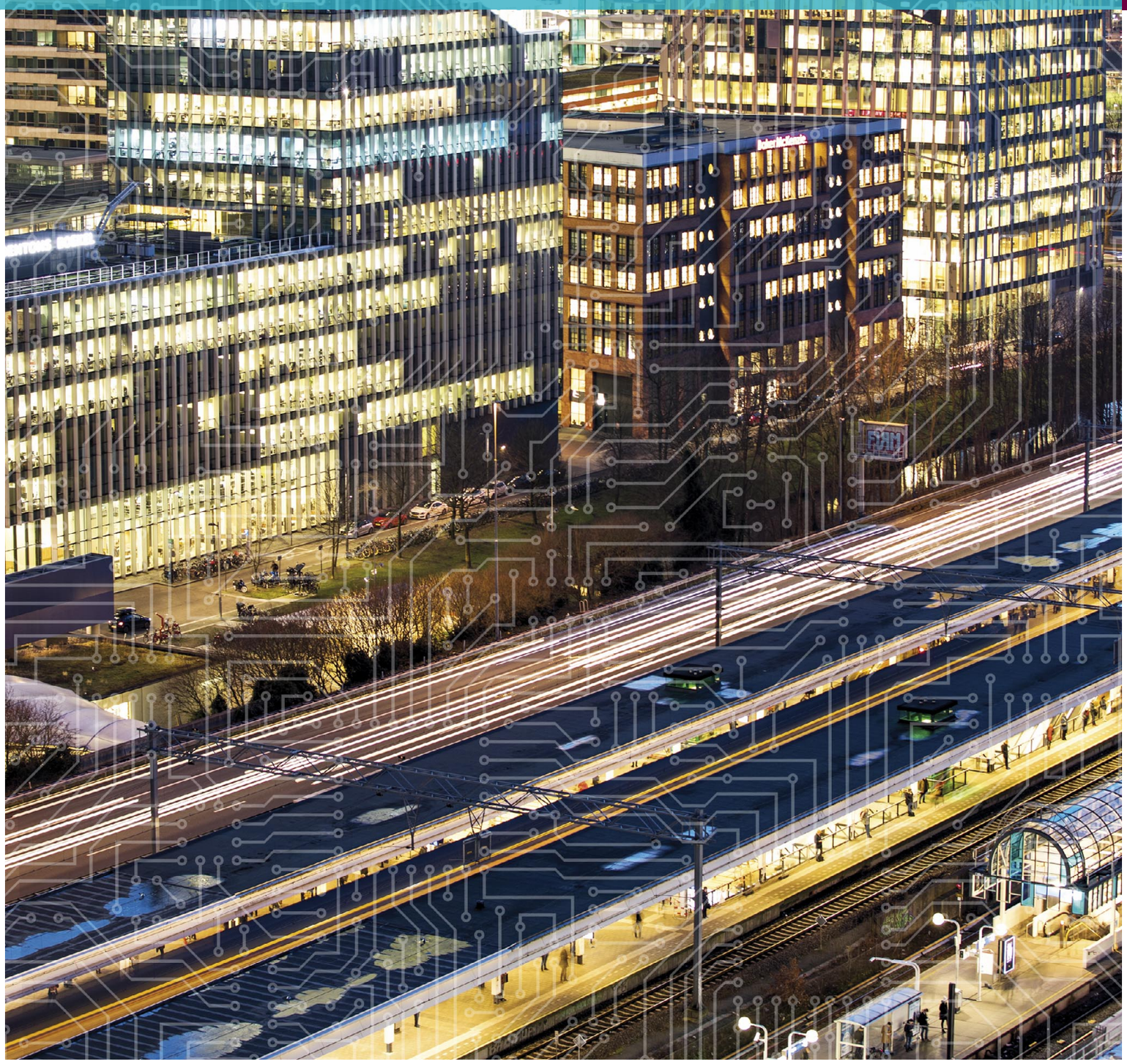


Photo: Jeroen de Bakker

INHOUDSOPGAVE CONTENTS

Mr P.J. (Pieter-Jaap) Aalbersberg EMPM
National Coordinator for Counterterrorism and Security and co-chair of the CSR.

Mrs S.C. (Sylvia) van Es LLM
President of Philips Netherlands and co-chair of the CSR.

Mr prof. dr. M.J.G.(Michel) van Eeten
Professor of Governance & Cybersecurity at TU Delft and has been a member of the CSR since its inception.

A DIALOGUE BETWEEN THE PUBLIC, PRIVATE AND SCIENTIFIC COMMUNITIES:

‘DIGITALISATION CANNOT BE CONSIDERED SUCCESSFUL UNTIL WE ARE ABLE TO GUARANTEE SECURITY’

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.

Last year, the Cyber Security Council (CSR) celebrated its tenth anniversary. Based on public, private and scientific perspectives, the CSR publishes recommendations on the social issues associated with digitalisation. These recommendations include the CSR Advisory Report ‘A comprehensive approach to digital resilience’, which sets out important advice for the new government regarding a digitally secure, open and prosperous society. In this interview, co-chairs Pieter-Jaap Aalbersberg and Sylvia van Es join scientist Michel van Eeten in reflecting on the past decade and looking ahead together to the role the CSR must assume in the future.

Pieter-Jaap Aalbersberg

Photo: Arenda Oomen

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.”

Strength and added value of the CSR
Over the past ten years, the CSR has released a variety of advisory documents and products. What is your view of the significance of the Council and the recommendations you have issued?

Pieter-Jaap: ‘Although ten years is quite a brief period in the larger scheme of things, the digitalisation of society is currently undergoing enormous acceleration. We in the CSR are part of that acceleration. And while the global context is in a general state of flux, with all kinds of changes occurring, I see a constant factor in the CSR: for ten years now, we have been considering digitalisation from a plurality of perspectives and based on a certain sense of equality. In the Council, private, scientific and public parties all come to the table as members and – based on their respective areas of responsibility – attempt to reach consensus of opinion and solid recommendations. This cooperation succeeds because the parties recognise that they are using their expertise to contribute to the greater whole. That working method is unique at the international level and is extremely valuable.’

Michel: ‘The CSR is indeed unique. And that is indeed down to the nature of its composition – public, private and scientific. The Dutch government has a seat on the Council as well, meaning that it effectually advises itself. While this is unusual, it is also an asset for us. Our job is to arrive at a joint recommendation; there are certain matters we cannot hand off to other parties. As a result, we arrive at a different result than you would get if the government were to formulate its own recommendation based on externally collected knowledge and experience. CSR members actually write the recommendations themselves, and as a group, which is quite unique for people in this kind of position. The openness of the dialogue within the CSR is remarkable as well, and the value of this is reflected in its recommendations.’


Sylvia van Es

Photo: Arenda Oomen


Michel van Eeten

Photo: Arenda Oomen

“De openheid van de gesprekken in de raad is bijzonder. De waarde daarvan zie je terug in de adviezen.”

‘The openness of the dialogue within the CSR is remarkable, and the value of this is reflected in its recommendations.’

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

Sylvia: ‘Absolutely – the CSR's strength lies in the variety of perspectives, visions and approaches it contains. Discussion among its members yields new insights and enriches our recommendations. And everyone is working toward the same goal: improving digital security.’

Pieter-Jaap: ‘Each and every member is on the Council to improve the digital security of the Netherlands. In other words, we serve our public interest. The CSR's unique composition (public, private and scientific) makes it possible to strategically approach priorities, obstacles and incidents from a variety of perspectives; to develop an integral vision on opportunities and threats; and to issue recommendations in this area.’

Key points of advice & the government's plans

Among the most recent recommendations published by the Council is the CSR Advisory Report ‘A comprehensive approach to digital resilience’. What key message from this report is most important for the current Dutch government?

Pieter-Jaap: ‘The message is right there in the title: we must work toward a comprehensive approach. Our advice is fundamental, as the integration and further development of the digital element is presenting us with a completely new infrastructure for our society. That infrastructure must be effective and safe and serve to protect the weaker among us. We are learning more and more about the combination of online and offline, the significance of which has only increased in recent years due to the COVID crisis. This calls for examining digitalisation from a broader perspective. It's not only a question of cybersecurity, but of how we will use this digital infrastructure to build a safe structure for our society. As it stands now, the digital landscape is still too fragmented.’

Michel: ‘I agree, although “fragmented” might not be quite the right word: it suggests there was once a unified whole. If you were to think of the digital domain as the individual trees in a newly planted forest, what we must do now is make the trees aware that, together, they make up a forest. Training experts is one aspect of the comprehensive approach we favour. This, too, will require heavy investments, as there is an acute shortage of qualified people. Other countries are eagerly snatching up Dutch students before they even graduate. Extra effort is needed to prevent this shortage from growing and to preserve the knowledge position and digital autonomy of the Netherlands. Because if we don’t possess the necessary knowledge ourselves, we will be at the mercy of other countries. While various resources have been allocated for this purpose in recent years, leading to relevant and high-quality research, the organisation of these efforts is still extremely ad hoc. What happens next, when all those PhD tracks have been completed?’

Sylvia: ‘Cybersecurity must be a top priority. Digitalisation cannot be considered successful until we are able to guarantee security – not only for businesses and organisations, but for individuals as well. While a comprehensive approach and unambiguous policy are indeed necessary, they will require a hefty investment: at least 833 million euros, as stated in our advisory report ‘A comprehensive approach to digital resilience’. I see cause for optimism in certain passages in the coalition agreement of the new government, which refer to centrally coordinated and structural cooperation between the government and the business and scientific communities. At the same time, I see a large gap between the proposed investments and the investments we have recommended. To ensure the Netherlands remains an open, free and prosperous society in the future, the new government must take action in this area.’

Pieter-Jaap: ‘Digitalisation does indeed feature prominently in the coalition agreement. The appointment of a State Secretary for Digitalisation and a Standing

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."

BACK TO TOP

Photo: Jeroen de Bakker

"De kracht van de raad zit in de verschillende perspectieven, visies en invalshoeken"

'The CSR's strength lies in the variety of perspectives, visions and approaches it contains.'

Parliamentary Committee on Digital Affairs are steps in the right direction. The financial side, unfortunately, does not include a separate heading for digitalisation. This is something we can work on going forward.'

Looking toward the future

Besides the aforementioned points for attention, what are the major future challenges in connection with digitalisation and digital security? And what role do you feel the CSR will have in meeting those challenges?

Michel: 'I think that in the first few years, our agenda depended much too strongly on whoever approached us. We were unable to review the policy plans until quite late in the game, at which point we were more or less expected to rubber-stamp them. Now, we are being involved at an earlier stage of the process. The Council has taken on a more supervisory role, with greater autonomy, and has greater freedom to think ahead to the major questions that have yet to be addressed by policymakers. Right now, one such question concerns encryption. It's a hot-button issue on which public and private opinion varies widely. This dissent has led to complete deadlock in the public discourse outside the CSR – whereas within the CSR, we are now opening a dialogue. We're doing so specifically because the Council is one of the few places where such sensitive conversations can take place. Everyone recognises the urgency of conducting this dialogue; we must try and see how far we get together.'

Sylvia: 'The fact that the Netherlands is leading the way in terms of digitalisation offers a great foundation for our efforts. Yet I still see certain challenges ahead, for instance with regard to managing access to data responsibly. Technologies like artificial intelligence require tremendous quantities of accessible data. And although legislation should ideally be harmonised at the European level, the reality is that it remains fragmented at the level of implementation. There is also a need for further clarification regarding a number of data-protection concepts, such as anonymisation. In that light, I have concerns about the levelness of the playing field, both within Europe and in comparison to the rest of the world. We must avoid a situation in which we are at a disadvantage. The bottom line is that cybersecurity is of the utmost importance: all our opportunities and possibilities for innovation depend on it.'

Pieter-Jaap: 'The rapid pace of developments means that we on the Council must be more proactive. We must make more of an effort to look ahead, to what is coming our way, and evaluate whether we are effectively prepared to meet it. New technologies also present new dilemmas. The CSR is in a position to identify such dilemmas and put forth potential solutions, without immediately settling on a remedy. Cybersecurity is no longer solely a matter of hardware and software. Today, it is also about adopting a new perspective on data and considering the societal implications of its widespread use. It's about what a government can do to protect its citizens. These are matters that must be addressed in cooperation with the scientific community and private sector. Those complex issues are areas in which the CSR will need to show initiative in the coming years.'

Renske Leijten
Member of the Dutch Parliament, acting chairman Standing Parliamentary Committee on Digital Affairs

Photo: Arenda Oomen

A STANDING PARLIAMENTARY COMMITTEE ON DIGITAL AFFAIRS:

A FIRST STEP IN THE RIGHT DIRECTION

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.

The Standing Parliamentary Committee on Digital Affairs was installed in March 2021. This was urgently needed according to many, including acting chairman Renske Leijten. In 2021 she helped design the committee by identifying suitable themes and tasks for a digital affairs committee. Now that the new government is in office, the moment has come for her to pass the gavel to her successor.

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.''

The Standing Parliamentary Committee for Digital Affairs was established in response to a recommendation by the Digital Future Temporary Committee to give the House of Representatives a better handle on developments in the digital world. 'We have both a specialist function and a horizontal function. This means that while we develop in-depth expertise on this subject and deal with it on behalf of the House, we also serve to connect parties. After all, digitalisation is a very broad subject with relevance for all policy areas. So we share information about the digital world with all sections of the House. Our task is rather like that of the Central Government Expenditure Committee, which informs all sections of the House on how to read budgets, for example.'

The exact description of the committee's work had not yet been formulated by the time of its establishment; in fact this was its first task. 'I said that we should take our time and reflect: what do we want to contribute as a committee? When dealing with a broad subject like the digital world, there is a risk that you'll end up with *all* digitalisation issues on your plate. But topics concerning digital applications in the classroom, for example, should really be covered by education specialists. A discussion about algorithms, on the other hand, is of a level that the committee should be allowed to handle.'

When the parliamentary committee was being created, its members looked for consensus between the parties. In a confidential setting they had talks with experts and held brainstorming sessions on what the committee's foundations should be. This resulted in six fundamental themes for the committee; see the box for further details. 'These six areas of attention reflect our priorities as a committee, but they say nothing at all about our viewpoints. We insist that the House itself should form a vision about these issues, which calls for a debate among the

“De politiek moet aan de slag, want de impact van digitalisering op mensenlevens is enorm”

‘Politicians must get to work, as the impact of digitalisation on human lives is enormous’

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 informatie-knooppunten (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.’’

Zes thema’s als basis voor de commissie Digitale Zaken

1. **Opkomende en toekomstige technologieën.** Denk hierbij aan kunstmatige intelligentie en blockchain.
2. **Digitaal burgerschap en democratie.** Gericht op de digitale vaardigheden van burgers, bedrijven en overheden voor deelname in de digitale samenleving. Belangrijk onderwerp is de invloed van digitalisering op onze democratie.
3. **Digitale grondrechten en data-ethiek.** Het bewaken en stellen van juridische kaders vanuit publieke waarden en grondrechten voor digitalisering. In het bijzonder rondom de verzameling en toepassing van data over burgers en bedrijven.
4. **Digitale infrastructuur en economie.** Gericht op de vaste en mobiele communicatienetwerken waarmee digitalisering mogelijk is. Maar ook aandacht voor de onderlinge verhoudingen en machtsposities op de onlinemarkten, zoals telecommunicatie als 5G en 6G.
5. **Online veiligheid en cybersecurity.** Gericht op de veiligheid van digitale technologieën en de beveiliging van informatie. Onderwerpen zoals cybersecurity en encryptie vallen onder dit thema.
6. **Digitaliserende overheid.** Analyseren en richting geven aan de toepassing van digitale technologieën door de overheid. Hoe is de digitale dienstverlening door de overheid geregeld? En hoe past de overheid open source software en open data toe?

Six themes as a basis for the Committee on Digital Affairs

1. ***Emerging and future technologies.*** *Examples include artificial intelligence and blockchain.*
2. ***Digital citizenship and democracy.*** *With a focus on the digital skills that citizens, companies and public authorities need to be able to participate in digital society. One key topic in this regard is the impact of digitalisation on our democracy.*
3. ***Fundamental digital rights and data ethics.*** *Monitoring and creating legal frameworks for digitalisation from a public values and fundamental rights perspective. More specifically in connection with the collection and application of data on citizens and companies.*
4. ***Digital infrastructure and economy.*** *With a focus on the fixed and mobile communication networks that enable digitalisation. This theme also covers the mutual relations and balance of power in online marketplaces, such as those for telecommunication (5G and 6G).*
5. ***Online safety and cybersecurity.*** *With a focus on the safety of digital technologies and information security. This theme covers topics such as cybersecurity and encryption.*
6. ***The digitalising government.*** *Analysing and giving direction to the application of digital technologies by the government. How are the government's digital services organised? And how does the government apply open source software and open data?*

political parties. It is the Committee's task to make sure that a debate like that is taking place at all.’

Minister for Digitalisation

The new government has even appointed a minister specifically for the subject of digitalisation. Alexandra van Huffelen was appointed Minister for Digitalisation - and Minister for Kingdom Relations - last January. Renske Leijten emphasises that while the Committee has no opinion on the matter, she herself is happy that digitalisation has now been given its own minister. 'Provided of course that she has a real mandate from the government that will enable her to get to work with the impact required.’

According to Leijten, who herself is a member of the SP party, the appointment of a minister on this subject as such is not the most important thing. ‘What we really need to do is to review the structure of digital applications in all government domains: how do we deal with this as a ministry, as a public-sector organisation or as a local authority? Information officers and data protection officers already exist within the government, but they do not yet have the priority that they deserve. Hopefully, the minister will be able to ensure that these officers are appointed in prominent positions in their respective organisations.’

One concern among the committee members however is the risk posed by the appointment of both a parliamentary committee and a Minister for Digitalisation. ‘Parties and other ministries shouldn't lean back and think that all problems in connection with digitalisation will now be solved. Those problems are everywhere and they're simply too urgent to ignore.’

Dutch society depends on digital communications in a variety of fields. The safety of this digital infrastructure is important for all sorts of things - our well-being, our economy, our democracy. One striking fact about this market is the dominance of several tech companies based abroad; in fact they are not even European. ‘This is indeed a development that we have observed within the Committee, one that is integrated in the points for attention that we have formulated. But again, the Committee has no opinion as to how we should deal with this. We facilitate the debate by placing themes on the agenda, but the debate itself must be held in the House of Representatives.’

Rapporteurs from the Committee on Digital Affairs are sent abroad to study how other governments are tackling these issues. Due to the COVID-crisis, this did not go entirely according to plan, but Leijten says that these missions will resume 2022 and European collaboration will continue to improve.

Digitalisation concerns us all

For many young people the digital world is something they take for granted. However, the majority of Dutch citizens did not grow up with the Internet, smartphones and DigiD. Recognising this, Leijten argues that it is important to use plain language when we communicate on the subject. ‘The very concept of cybersecurity is hard to understand for many people. But it's simply about a safe digital world, a matter that has an impact on the daily lives of every person in this country. Due to the use of complicated language, many people do not realise that these things - cybersecurity, algorithms and ransomware - also affect their own lives.’

The debate on cybersecurity (or digital security) should be made more accessible, says Leijten. In her view, establishing an entirely new institute with a National Coordinator for Digitalisation is not the best solution, as this would be a lengthy and expensive process while it is important to act fast. Digitalisation and all the challenges it brings is becoming an ever more urgent issue for all sectors. The Nationwide Network of Information Hubs (LDS) is an important step in that direction. ‘We should develop such a

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.’’

BACK TO TOP

Photo: Jeroen de Bakker

“De urgentie wordt binnen Den Haag gevoeld, nu is het tijd om stappen te zetten”

‘There is clear sense of urgency in The Hague: it is now time to make real steps’

network based on existing resources, combine the best aspects and make it as easy as possible to share data within that network. At the same time, we need to make sure that all ministries recognise digital security as a priority. Once you get those two things right, you can start building a digital infrastructure where all parties can share knowledge, experiences - and warnings too - in a safe and efficient manner.’

Responsibility
Major political choices will have to be made, and they are going to have a considerable impact on society. While it is important to have this debate, its focus should not be on the individual citizen, according to Leijten. ‘That would be tantamount to placing responsibility on consumers rather than on politics and big companies. In my view, citizens should be able to rely on the government observing the precautionary principle. Together with the private sector, we need to make sure that it is safe to use the digital system. If you stick to the rules and don't do anything strange, it should be impossible for really serious problems to occur, such as private data leaks or scams that are still victimising so many people.’

According to Leijten, the solution is to deprive the criminals involved from their earnings model. This is only possible if enough monitoring and enforcement capacity is available, which, in turn, requires clear statutory frameworks. ‘All these issues need to be discussed in far more detail in The Hague, so clearly we still have a lot to do. And we shouldn't forget that this debate is also held at the European level. After all, the digital world knows no national boundaries. Our security departments are struggling with huge capacity shortages. This should be a top priority for the new government. I'm not awfully optimistic about this.’

Still, this first step by the House of Representatives is a good start. The Committee ensures that digitalisation will now be dealt with as an umbrella issue. At the same time, this step has also produced a new insight: ‘The Committee was really shocked by the extremely low level of knowledge within the government. It is important for us as the government to obtain the relevant knowledge and to retain it. It is not just financial means that can help to achieve this. We need to make sure that the government is an attractive place to work where people see that their efforts really have an impact on society.’

Mrs prof. E.M.L. (Lokke) Moerel LL.M.
Senior of Counsel Morrison & Foerster & Professor Global ICT Law, Tilburg University

Mr G.W. (Gerrit) van der Burg LLM
Chairman of the Board of Prosecutors-General

EUROPE IS TAKING THE LEAD IN STRENGTHENING DIGITAL SOVEREIGNTY

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.

With 92% of all European data stored in American clouds, it is one of the European Commission's key priorities for the next five years to restore the EU's digital sovereignty. 'We've become too dependent here in Europe on Chinese and US technologies and we should to take steps to meet our own needs,' said Ursula von der Leyen in her State of the Union *this year. The European digital innovation strategy and agenda are now well under way.*

Lokke Moerel, member of the Dutch Cyber Security Council on behalf of the scientific community: 'The sense of urgency is now really felt in Europe, as can be clearly seen in the countries around us. In Germany, for example, digital sovereignty is now recognised as a boardroom priority – *Chefsache*. If we want to take part in the debate at the European level, we'll also need to make several steps at the national level. Strong at home, strong in the EU, strong in the world: that should be our motto in this context.' Gerrit van der Burg, member of the Dutch Cyber Security Council on behalf of the public sector: 'In the Netherlands, this topic doesn't yet feature on the political agenda as prominently as it should. Our approach to tackling cybersecurity issues has remained largely reactive. We tend to respond in crisis mode, and hardly ever adopt the broader perspective of strategic autonomy. This must change.'

According to Moerel and Van der Burg, the Netherlands is one of the most digitalised countries. The coronavirus crisis has only accelerated this process. 'The crisis is generating an ever growing number of new dependencies and vulnerabilities,' says Van der Burg. 'Cyber threats are increasing, and we are becoming more and more dependent on a digital infrastructure controlled by a small number of big foreign market players. This can have major consequences for our national and economic security and, as a result, for the country's earning capacity.' Moerel: 'The key question is this: How are we going to retain control, as a country, over our *vital economic ecosystems* and *democratic processes* in a digital world? '

New technologies are eroding our digital sovereignty

A lack of control over critical technologies will result in new dependencies. For example, current encryption strategies are no match for the computing power of future quantum computers. According to Moerel and Van der Burg, if we want to be able to protect our critical information in the future, we will need to innovate now. This concerns existing information as well as future information. Moerel: 'Remember that some foreign states are systematically intercepting our encrypted information, anticipating that quantum computers and AI will enable them to decrypt and analyse it at some later stage.' Van der Burg: 'We're seeing criminals using automated tools to detect and exploit software vulnerabilities on a large scale. If we want to stay ahead of cybercriminals, innovation is of the essence.'

'Practically all data from Dutch government bodies, businesses and individuals is now stored in the clouds of a handful of foreign providers,' Moerel continues. 'If we'd asked ourselves ten years ago whether we thought this would, in principle, be a good idea, we'd all have said: no. If one of those companies fails, it's like a power failure: entire sectors of our economy will come to a standstill. After all, we'd never place our central power switch in the hands of a foreign party.' Van der Burg: 'The situation as regards detecting and investigating digital crime is just as fragile. In criminal investigations, we partly depend on the cooperation of several foreign players. If they refuse to cooperate or take a long time doing so because it requires prior head office approval, this will affect our ability to do our job. Practice has already shown that this over-dependence has consequences for our democratic rule of law and the position of victims.'

Photo: Arenda Oomen

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 kwantum-computers. Moerel en Van der Burg vinden dat we nu moeten innoveren om onze kritische

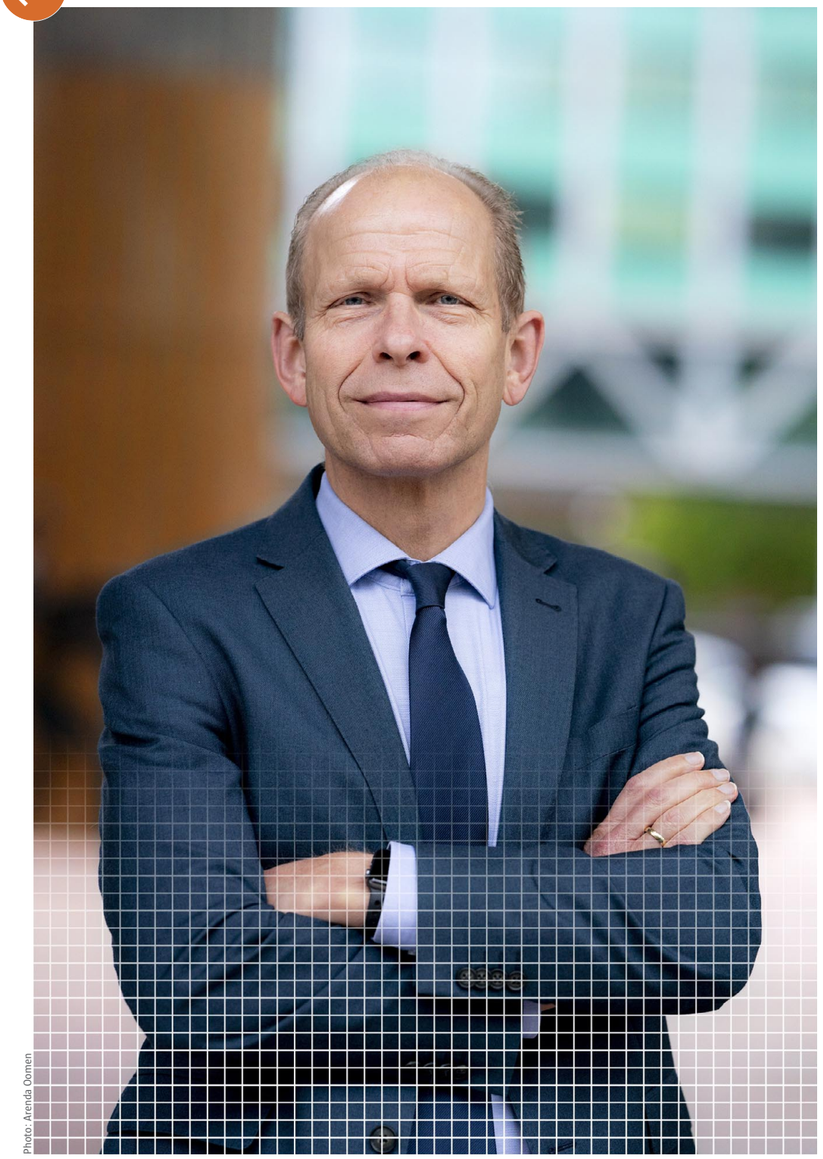


Photo: Arenda Oomen

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 elektriciteitnetwerk 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 prompt 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.”

“Uitgangspunt voor digitale autonomie dient te zijn: sterk in eigen huis, sterk in Europa, sterk in de rest van de wereld.”

‘Strong at home, strong in the EU, strong in the world: that should be our motto for digital autonomy.’

Data as a weapon: Even TikTok is a matter of national security
According to Moerel, this is not just a matter of dependency in the context of business operations and public tasks. ‘We should also think of what other states can do with information about our citizens and companies. China and the United States, for example, already consider access to each other's data as a matter of national security. When former US President Trump banned the TikTok app from US app stores, many people ridiculed this decision, but President Biden has also issued an Executive Order that enables the government to prevent transfer of sensitive data of US citizens to China. China itself has also banned the export of important data, including data that could be used to map the private lives and working lives of Chinese citizens. In addition, China recently banned the DiDi app (the Chinese equivalent of Uber) from Chinese app stores as soon as the company was listed on a US stock exchange. We really need to look into this. While our privacy laws do protect citizens’ individual privacy, they do not protect our collective data. I think I can now assert that the TikTok app is indeed a matter of national security.’

The Dutch Cyber Security Council has published advisory reports on an ‘*Integral Approach to Cyber Resilience*’ and ‘*Digital Autonomy and Cybersecurity in the Netherlands*’. The Council's most important observation is that to date, the approach to cybersecurity has been largely technical and reactive, with very little attention for the broader perspective of strategic autonomy. Moerel: ‘Now that the issue of sovereignty is becoming relevant for more and more aspects of our economy, society and democracy, there is a need for central control. However, as a Council we note that the policy integration required for that is lacking. In an earlier advisory report, we already noted the lack of insight in the Netherlands into our new dependencies, resulting in an inability to pursue a sufficiently proactive and coordinated technology policy in the fields of research, valorisation and industrial capacities. In short, we should combine our current reactive approach with proactive monitoring and anticipation. This calls for control from the most senior level.’

Digital autonomy – a boardroom priority
According to Van der Burg and Moerel, responsibility for digital autonomy should be assigned to the highest political and administrative level. Van der Burg: ‘It should really be a permanent item on the agenda at the most senior level: in politics, such as in the Council of Ministers, but also in business. We need to make a continuous effort to set limits for the Netherlands and protect our independence.’ Moerel: ‘Digital autonomy is currently on the radar of the Dutch Ministry of the Interior and Kingdom Relations, the Dutch Ministry of Economic Affairs and Climate Policy and the Dutch Ministry of Justice and Security. However, we need to break out of the policy silos and develop a coherent policy if we, as a country, want to be able to contribute in a European context. If you can't offer a clear contribution, you won't be regarded as a full partner in the conversation.’ When asked about the cost of digital autonomy and which country is taking the lead, Van der Burg says that ‘it’s difficult to compare the situation in different countries, if only because they started from very different positions. However, we might try to follow the example of the United Kingdom, which is systematically setting aside funds to protect its digital autonomy. Reserving a fixed percentage of the gross domestic product would also be a sensible choice for the Netherlands.’

European tech
Despite the current dependence on foreign providers, which is considerable, the Council believes there is no reason to despair. Moerel: ‘Technological innovation always comes in waves, so a new wave will come. There will be plenty of opportunities if we invest wisely. There’s a growing awareness that we need alternatives. To that end, let’s now

Controle over democratische processen

- Hier gaat het vooral over het functioneren van en vertrouwen in de rechtsstaat. Wanneer de staat geen controle heeft over het verkiezingsproces, omdat dit is geïnfiltreerd en wordt gemanipuleerd door vreemde mogendheden (*fake news*), staat onze digitale soevereiniteit onder druk. Tijdens de coronacrisis hebben we gezien dat Rusland en China stelselmatig de *COVID-response* van de EU en de lidstaten probeerden te ondermijnen met gerichte misinformatie campagnes.

Controle over essentiële economische ecosystemen

- **Economische spionage**: Door systematische diefstal van onze kennis uit de topsectoren en universiteiten komt ons toekomstig verdienvermogen onder druk te staan
- **Soevereiniteit-respecterende cloud**: Voor innovatie met artificiële intelligentie (AI) is enorme rekenkracht vereist (hetgeen cloud computing vergt) en verder grote hoeveelheden geharmoniseerde data. Hiervoor is het nodig dat de data in een bepaalde industriesector wordt gecombineerd. Dat is op dit moment lastig, omdat de data van onze bedrijven in silo's in de clouds van de grote techbedrijven staat, waardoor deze data niet beschikbaar is voor Nederlandse en Europese innovatie. Toegang tot geharmoniseerde data en de cloud-infrastructuur wordt het fundament voor de Nederlandse en Europese innovatie- en kennisinfrastructuur. Daarover, zeggenschap houden, is een wezenlijk onderdeel van de Nederlandse strategische autonomie.
- **Veilige digitale communicatienetwerken**: We zijn in toenemende mate afhankelijk van digitale communicatie voor het welzijn van burgers en voor een sterke economie. Denk aan video-vergaderen, en *smart homes*, maar ook aan nieuwe veiligheids-kritische diensten zoals smart *energy grids*, intelligente mobiliteitssystemen en op afstand bedienbare zorgrobots. Doordat de ontwikkeling en het beheer van de onderliggende technische systemen en -netwerken (zoals routers, switches, DNS-servers) steeds vaker worden gedomineerd door buitenlandse partijen, hebben organisaties en individuen slechts een beperkt inzicht in hun afhankelijkheden van deze partijen en hun systemen, laat staan dat ze daar controle over hebben. Dit beperkt onze mogelijkheden om autonoom te beslissen en te handelen over hoe we onze digitale infrastructuur inrichten en aan welke van die partijen we het transport van onze data toe willen vertrouwen.

Control over democratic processes

- This particularly concerns the functioning of and trust in our democratic rule of law. Once the state loses control over the election process because it is infiltrated and manipulated by foreign powers (*fake news*), our digital sovereignty will come under pressure. During the coronavirus crisis, we saw Russia and China systematically attempting to undermine the *COVID response* of the EU and its Member States using targeted misinformation campaigns.

Control over vital economic ecosystems

- **Economic espionage**: Our future earning model has come under pressure as a result of the systematic theft of knowledge from top sectors and universities.
- **Cloud services that respect sovereignty**: Innovation based on artificial intelligence (AI) requires immense computing power (to be provided by cloud computing) and large amounts of harmonised data. For this purpose, data from a particular sector of industry will have to be combined. However, this is difficult under the present conditions, as the data of our businesses is gathered in silos in the big tech companies' clouds, which means it is not available for Dutch and European innovation. Access to harmonised data and the cloud infrastructure will become the foundation of the Dutch and European innovation and knowledge infrastructure. It is an essential aspect of the Netherlands' strategic autonomy to stay in control of that data and cloud infrastructure.
- **Secure communication networks**: We increasingly depend on digital communications to ensure the well-being of our citizens and a strong economy. Examples abound: video conferences and smart homes, new security-critical services such as smart energy grids, intelligent mobility systems and remote-controlled care robots. With foreign parties playing an increasingly dominant role in the development and management of the underlying technical systems and networks (such as routers, switches and DNS servers), organisations and individuals have little insight into their dependence on – and even less control over – those parties and systems. This is restricting our ability to autonomously act and decide how to design our digital infrastructure, and select the parties to be entrusted with transporting our data.

focus on targeted innovation and collaboration. This will also enable us apply for European co-financing in a targeted manner.' Van der Burg: 'In this context, we should also make sure to keep abreast of what's happening in our own tech scene. For instance, we shouldn't allow ourselves to be caught unawares, more or less, by the sale of a vital Internet security company. We should make an effort in the Netherlands to stay in control of our crown jewels. And we should also carefully monitor the development of start-ups and prevent criminals taking advantage of new technologies.'

Gaia-X

In its advisory report, the Council also refers to the Gaia-X project, which was initiated by Germany and France. Moerel: 'Many people think that Gaia-X is intended as a move to establish our own European cloud player. But that's incorrect. The purpose of Gaia-X is to ensure *scalability* for the cloud infrastructure in Europe by realising interoperability between the various cloud services. This is achieved by setting joint technical standards and legal frameworks for the digital infrastructure. So this form of interoperability goes beyond data and application portability from one vendor to the other to prevent vendor lock-in; it is about actually creating open APIs, interoperability of encryption key management, uniform identity & access management etc. Following some initial hesitation, we are now seeing active contributions to this project by a Dutch coalition. I'm involved in an interesting European user case myself, in the field of energy. Things are now really beginning to move in Europe.' Van der Burg: 'I'm also inclined to regard Gaia-X as an example of improved interoperability for other products and processes, including in the field of investigation tools and techniques. The Netherlands is already pretty advanced when it comes to high-tech investigation, but it will evidently help if we get the whole of Europe on board. We should give Europe more clout and develop uniform approaches.'

Photo: De Beeldunie

Europese tech

Hoewel de afhankelijkheden van buitenlandse aanbieders op dit moment groot zijn, ziet de CSR geen reden tot fatalisme. Moerel: "Tech-innovaties 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 om 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 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

"Digitale autonomie vergt sturing vanaf het hoogste niveau."

'Digital autonomy calls for control from the most senior level"

Digital autonomy remains on the Council's agenda

Van der Burg: 'Digital autonomy is likely to remain on the Council's agenda for some time to come. Given the speed of technical and geopolitical developments, we are keeping our finger on the pulse in the Council. In addition, like the fight against cybercrime, digital autonomy should be an area of special focus in the annual Cyber Security Assessment Netherlands.' Moerel adds: 'In the period ahead, the Council will study the ways in which foreign powers could use our collective data as a weapon and how we could improve our defences against such actions. Another topic on the agenda is giving citizens more control over their data by means of a reliable, universal Dutch digital identity. Several initial steps have already been taken in response to a number of elements in our advice on digital autonomy. For example, there have been efforts to raise awareness of strategic autonomy in cybersecurity and to improve the Dutch valorisation and innovation climate. The Councils's advice included an 'Assessment Framework for Digital Autonomy', which is now being put into practice by the Ministry of Economic Affairs and Climate Policy.'

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.

Moerel: "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 *Toetsingskader digitale autonomie",* dat inmiddels door het ministerie van Economische Zaken en Klimaat wordt geoperationaliseerd."

Wat moet er gebeuren?

Vooruitlopend op nationale strategie- en beleidsvorming dient volgens de CSR een vijftal concrete zaken in gang te worden gezet:

1. Borgen van drie basisvoorzieningen (soevereiniteit-respecterende cloud voor veilige opslag van data en data-analyse, veilige digitale communicatienetwerken en post-kwantumcryptografie);
2. Implementatie van een toetsingskader digitale autonomie cybersecurity;
3. Verhogen van bewustwording van het belang van strategische autonomie in cybersecurity;
4. Verbeteren van het Nederlandse valorisatie- en innovatieklimaat;
5. Een actieve inzet op aansluiting bij EU-beleid dat een relatie met digitale autonomie heeft en waarbij Nederland ook gebruikmaakt van de beschikbare EU-financiering hiervoor.

Deze acties zijn noodzakelijk om op korte termijn onze positie te versterken zodat de digitale autonomie voor cyberweerbaarheid ook in de toekomst kan worden gegarandeerd, cybercrime kan worden bestreden en de Nederlandse samenleving kan blijven vertrouwen op de veiligheid en continuïteit van onze digitale maatschappij.

What needs to be done?

The Dutch Cyber Security Council is of the opinion that, in anticipation of a national strategy and policy, five concrete actions are required:

1. Safeguard the continuity of three basic services (sovereignty-respecting cloud services for the secure storage of data and data analysis, secure digital communication networks, and post-quantum cryptography);
2. Implement an assessment framework for digital autonomy and cybersecurity;
3. Raise further awareness of the importance of strategic autonomy in cybersecurity;
4. Improve the Dutch valorisation and innovation climate;
5. Actively link up with EU policies that relate to digital autonomy, and use the EU funds available for this purpose.

These actions are necessary to strengthen our position in the short term, so that we can guarantee digital autonomy for cyber resilience today and in the future, fight cybercrime and allow everyone in the Netherlands to continue to rely on the safety and continuity of our digital society.

BACK TO TOP

"We moeten meer Europese slagkracht ontwikkelen en komen tot uniforme aanpakken."

'We should give Europe more clout and develop uniform approaches.'

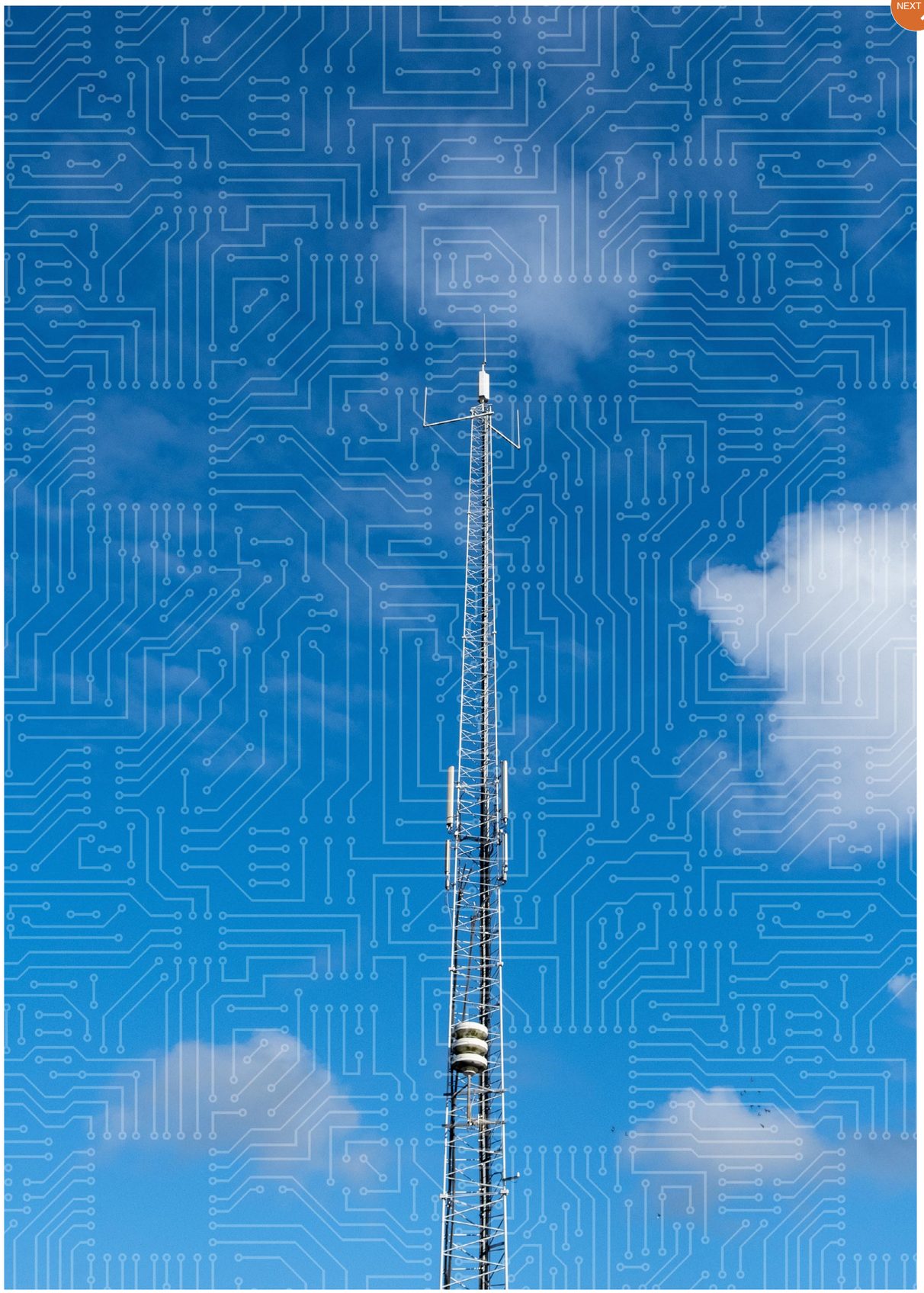


Photo: De Beeldunie

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.

Beefing up the cyber resilience of 27 European Member States is no easy task. Meeting the challenges of the future requires a certain level of ambition. ‘There’s plenty of strategy in place, but the next few years will be all about execution, execution, execution,’ VVD MEP Bart Groothuis explains from Brussels.

NIS2, AN AMBITIOUS UPDATE OF THE EUROPEAN CYBER SECURITY DIRECTIVE

Bart Groothuis
Dutch member of the European Parliament

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.”

Photo: Arenda Oomen

“Het uitwisselen van gegevens is heel belangrijk voor de cybersecurity-community en dat is waar ik het uiteindelijk voor doe.”
‘Exchanging data is extremely important to the cybersecurity community in key areas, which is my main area of concern.’

At the intersection of geopolitics and technology
Groothuis has been working in Brussels for almost two years now. ‘I work at the intersection of geopolitics and technology, but I'm mainly focused on new threats. Before this, I spent seven years working as head of cybersecurity at the Dutch Ministry of Defence. Parliament needs someone to take the lead on legislative dossiers; that's what a rapporteur does. It's my job to find a majority on the basis of the content, and I enjoy that role. I get to use all my ideas and expertise on cybersecurity.’

Major expansion
Groothuis read the Cyber Security Council's recommendations and noticed that nine out of ten were incorporated in the NIS2, Brussels' directive on cybersecurity. ‘The NIS2 directive will eventually become law in the Netherlands and all 27 other EU Member States. We already have a 2016 law in the form of the NIS, but that's proven to be flawed. The details vary from country to country, so everyone has to follow different guidelines. The NIS2 is an updated version of that legislation and is far more ambitious in scope. Last time around, there was still debate as to whether Europe actually had any say on cyber resilience at all. Those days are long gone, though.’

The directive mainly needs to be more ambitious, but in which aspects? Groothuis anticipates changes in three key areas. ‘As a first step, we need to significantly expand the scope. The companies and entities we used to refer to as “vital” are now referred to as “important and essential”. It all depends on the services you provide to society. If you've got a staff of more than 50 and a turnover of over 10 million euros, you fall within this scope. If you're smaller but provide essential services, such as cloud services, then you're also included. That means you'll be expected to take certain cybersecurity measures. For example, you'll be required to report any incidents or threats. The number of European entities will grow to around 160,000 as a result of the changes.

The way we exchange information is also set to change. There has been a lot of uncertainty about the issue of liability since the introduction of the General Data Protection Regulation (GDPR). Are you actually allowed to share personal data? Do we have any way of finding out where domains are registered? The NIS2 aims to provide a solid legal basis, so that international companies and governments can also exchange data with each other again. That's extremely important to the cybersecurity community, which is my main area of concern. We need to make sure they feel represented in Brussels.’

Cybersecurity in the boardroom
‘Thirdly, we're going to make cybersecurity *chefsache*, in line with the Cyber Security Council's recommendations. This German word means it's an issue that needs to be discussed at the boss' table – in the boardroom at CEO level. We've decided it would be a good idea to make senior management personally liable. Non-compliance will be subject to serious fines: 2% of your annual turnover if you demonstrably failed to take the necessary measures. Why 2%? Ransomware attacks often demand 2% of the company's annual turnover. Companies will face a choice: do I hand over that money to a bunch of Russian ransomware attackers, do I give it to the government in the form of a fine or do I invest it in security and cybersecurity?’

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.

“We moeten niet meer reactief reageren, maar proactief handelen”
‘It's time to be proactive rather than just responding to events’

Europe needs to be proactive
Cyber resilience is becoming an increasingly important issue across Europe. Groothuis regards the NIS as the main cornerstone, but we are seeing a range of other initiatives towards improved cyber resilience. ‘The second would be the introduction of the Cyber Resilience Act. That's one piece of the puzzle that's still missing, and it concerns connected devices – devices that can connect to the Internet. In future, you'll be able to hold software and hardware developers personally liable for shoddy products. The third change – and this is the aspect I'm most enthusiastic about – will be on an operational level. It's part of our cybersecurity strategy and focuses on DNS capability. In the event of a large-scale attack like the one on Petya at the port of Rotterdam, we'll be able to block an entire domain. It's a very simple, yet effective tool.

That's what we need to be doing more at the European level: it's time to be proactive rather than just responding to events. We know exactly where these attacks are coming from, so we should use that knowledge to pre-empt the problems. That also applies to the Netherlands. We'll have to get our hands dirty and push the legal envelope from time to time, but we don't have any other options.

If you really want to pursue an ambitious strategy, you'll have to operationalise your goals. We've developed plenty of strategy, but the execution is still lacking. That's what we need to focus on in the coming years. *Make it happen.*

We've laid the legal groundwork in Brussels, but the Dutch government now needs to show political willpower and resolve. Passively sharing information was important for a while, but it's time for something new.’

Groothuis acknowledges that the Netherlands led the way for a long time. ‘There was a lot of energy. However, we've started falling behind and actually regressing in recent years. In the UK, all cybersecurity issues are handled through a single organisation. The situation isn't that clear here in the Netherlands: the National Cyber Security Centre (NCSC) might handle some cases, while the Police or the General Intelligence and Security Service (AIVD) might handle others. We're currently developing a European framework, and you can tell that those services have really been consolidated in 17 countries. Here in the Netherlands, things are still fragmented though.’

In search of like-minded countries and regions
The EU will face plenty of challenges moving forward. Groothuis emphasises the need to invest. ‘The next few years will see a focus on deep security. It's basically the most important precondition for digital autonomy. It's all very well sourcing from other countries and partners, but you need to secure your own core interests.

For example, we need to be focused on cryptography. The Netherlands should just decide: we need our own cryptography platform, and it should be developed by the AIVD and produced by a Dutch company. That way, you have control over the entire process. A few years ago, the Ministry of Foreign Affairs was still using Kaspersky antivirus software from Russia. They basically had access to every email sent by diplomats, which is obviously unacceptable. The Netherlands will have to make some serious investments if we want deep security.

At a European level, we'll have to build alliances with like-minded countries and regions. We can't keep sourcing products and services for our critical industries from geopolitical opponents. Why should we be using Chinese facial recognition software? The same goes for technologies like 5G.

The NIS2 will also include legal requirements for supply chain review. That means we can block Chinese, Iranian or Russian products if we don't trust them. We can apply our own jurisdiction to determine what is and isn't allowed on our markets.

“Als je echt deep security wilt, moet je daar ook als Nederland in investeren.”
‘The Netherlands will have to make some serious investments if we want deep security.’

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 gezichtsherkennings-software 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."

BACK TO TOP

"We moeten het probleem bij de bron aanpakken"

'We need to tackle this problem at the source'

Finally, we're starting to understand ransomware as more than a criminal revenue model; it's also a Russian foreign policy instrument. Almost all ransomware is developed there, as every European intelligence service will tell you.

Brussels needs to take Joe Biden's lead in terms of dealing with Vladimir Putin. For the first time in 60 years, their last talks didn't focus on nuclear weapons; they discussed ransomware and cyberattacks.

The EU has also established a Cyber Diplomacy Box in order to impose sanctions on Russia and empower the Member States, but we aren't putting it to much use yet. That's a diplomatic problem as well as a cybersecurity issue. We need to address that if we want to get our house in order. I also wish the Cyber Security Council would take a more active role in the debate. We need to tackle this problem at the source.'

Time to move fast

Joe Biden signed the *Improving the Nation's Cybersecurity* Executive Order last May in response to a series of cyber incidents. Groothuis takes this as a cue to start moving fast. 'It's like playing whack-a-mole. Let me give you an example: Dutch banks joined forces when Internet banking was experiencing a wave of fraud and malware. They managed to reduce crime by 90% in the space of three months. However, crime levels in surrounding countries actually went up during that period. If the Americans are moving to enact fast-track legislation, we need to move fast as well. Our US counterparts are mainly focused on targeting the software supply chain. That could also yield results here in the EU, which is why we incorporated it in the NIS2.'

In Groothuis' view, 2022 will be a pivotal year. 'The French has taken over the EU presidency since January. We're going to try and wrap this up for this coming year. It will then be submitted to the Dutch parliament, which will have to work out the details. We'll find out where the Netherlands stands in relation to the new directive then.'

Photo: Hollandse Hoogte

VICE ADMIRAL BOUDEWIJN BOOTS

Nieuw lid van de Cyber Security Raad (CSR)

New member of the Dutch Cyber Security Council (CSR)

Recht door zee en koersvast. Marine. Kritisch, cynisch soms, maar constructief. Betrokken leider, verbindend en soms ongeduldig. Relativerend, voornamelijk door een lach. Sinds maart 2021 is vice-admiraal Boudewijn Boots de plaatsvervangend Commandant der Strijdkrachten. Met deze plaatsing op het ministerie van Defensie werd hij de eennahoogste militair van de Nederlandse krijgsmacht. Sindsdien is hij ook lid van de raad. Boudewijn Boots heeft hiermee een bekend gezicht binnen de raad opgevolgd, de huidige Commandant der Strijdkrachten, generaal Onno Eichelsheim.

Gets to the point and stays the course. A Navy man. Critical, even cynical on occasion, yet constructive. A dedicated leader who forges connections and can be impatient at times. Maintains perspective, often through humour. *Vice admiral Boudewijn Boots has been Deputy Chief of the Netherlands Defence Staff since March 2021. With this appointment at the Dutch Ministry of Defence, he became the second-highest ranking military officer in the Dutch armed forces. He has been a member of the CSR since that date as well. In that capacity, Boudewijn Boots succeeded a familiar face within the Council: the current Chief of Defence, General Onno Eichelsheim.*

Kunt u uzelf voorstellen en een korte beschrijving van uw profiel geven?
"Ik heb een rijke operationele achtergrond als marineofficier en heb tussen de uitzendingen en varende functies door gewoond op Curaçao en in Engeland. Als eskadercommandant van een van de permanente internationale vlootverbanden van de NAVO, heb ik in 2019 mijn operationele aanwezigheid op zee afgerond. In dat jaar opereerde ik in de Middellandse, Egeïsche en Zwarte Zee, de zuidflank van het verdragsgebied van de NAVO. Hierin voelde ik letterlijk de spanning in een regio met actuele en potentiële conflicten, migratiestromen en de angst voor oorlog en onveiligheid. Of dat veel verschilt met de huidige cyberdreigingen waarmee Nederland onafgebroken geconfronteerd wordt? Nauwelijks. Afgezien van het fysieke gedeelte van de dreiging, moeten wij ons heel bewust zijn van de cybergevaren die wij als samenleving elke dag weer lopen. Daar moeten we gezamenlijk en non-stop tegen strijden."

Would you mind introducing yourself and sharing a brief description of your background?
'I have a wealth of operational experience as a Marine officer and – between deployments and jobs at sea – have lived on Curaçao and in England. As squadron commander of one of NATO's permanent international joint fleets, I concluded my operational presence at sea in 2019. In that year, I served in the Mediterranean, Aegean and Black Seas, on the southern flank of the NATO treaty zone. While there, I literally felt the tension in a region facing current and potential conflicts, migration flows and the fear of war and insecurity. As for whether that is very different than the current digital threats the Netherlands is persistently dealing with today, I'd say: hardly. Apart from the physical component of the threat, we must maintain a keen awareness of the cyber threats our society faces each and every day. We must mount a coordinated and non-stop fight against them.'

Photo: Arenda Oomen

Wat is voor u het belang van de CSR en wat is uw missie als raadslid van de CSR?
"Voorheen was militair optreden beperkt tot operaties op land, op zee en vanuit de lucht. Heel overzichtelijk, maar alleen daarmee bereiken we niet onze doelen. Het gaat nu juist om het multidomein optreden. Daarom erkennen we binnen Defensie naast land, zee en lucht, ook cyber, space en informatie als 'nieuwe' domeinen. Het belang van de CSR is voor mij klip en klaar: alleen door het combineren van publiek en privaat, civiel en militair en dit te koppelen aan onderwijs en wetenschap kunnen wij ervoor zorgen dat wij Nederland cyberweerbaar en cyberveilig houden. Dat is mijn missie als raadslid van de CSR."

Why do you consider the CSR to be important and what is your mission as a council member of the CSR?
'In the past, military action has been confined to operations carried out on land, at sea and from the air. This is simple enough, but will not be enough to achieve our objectives. What is needed now are multi-domain operations. To that end, we in the Ministry of Defence now recognise not only land, sea and air but also the 'new' domains of cyber, space and information. Personally, I feel that the importance of the CSR could not be more obvious: only by combining public and private, civilian and military parties, and then linking these to others in education and science, will we be able to preserve the digital resilience and digital security of the Netherlands. That is my mission as a CSR council member.'

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.

As an officer in the Royal Netherlands Navy, I must first point out the nautical origin of the term 'cyber'. The ancient Greek word kubernetes *means 'helmsman'. In 2021, however, that etymology has been entirely forgotten and we associate 'cyber' with anything having to do with computers and computer networks. And yet the ancient nautical meaning can still prove valuable when we consider the digital resilience of the Netherlands, our digital autonomy and the role of the Ministry of Defence in that area.*

'DIGITAL SECURITY HAS BECOME AN IRONCLAD NECESSITY FOR PRESERVING OUR WAY OF LIFE AND OUR FREEDOM'

"Het cyberdomein is, net als internationale wateren, toegankelijk voor iedereen; het is een global commons."

'Like international waters, the digital realm is accessible to all: it is a global commons.'

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.

Vice-admiraal Boudewijn Boots
Plaatsvervangend Commandant der Strijdkrachten

BACK TO TOP

First, the meaning of the Greek root word quite accurately describes the role I feel the Cyber Security Council (CSR) should play in the national cyber-landscape: that of helmsman. The helmsman holds a steady course, monitors the ship's condition and advises the captain on any opportunities and threats that may appear on the horizon. So, too, does the CSR advise the Dutch government with regard to developments and threats in the digital domain. Yet we can only do so through an effective mix of government, public-private, scientific, civilian and military parties. We are in grave need of the totality of these parties' perspectives and expertise, because our opponents make no distinctions when they attack our vital interests.

This brings us to the threats on the horizon. Like the rest of society, the Dutch Ministry of Defence is becoming increasingly digitalised. Guided by the principle of Data-driven Action, data and information are becoming central to the way we operate. In turn, our networks and IT systems are becoming increasingly vital to our effectiveness. This presents opportunities, but also threats. First and foremost, we must preserve the security of our own systems and networks so that we may use them to achieve our operational objectives and to protect the strategic interests of the Netherlands.

Just as the Dutch navy has protected trading fleets for centuries, the Dutch Ministry of Defence as a whole has a protective duty with regard to Dutch society and its interests. Digital infrastructure and services make up a large portion of our economy, our country is home to one of the largest internet hubs in the world and our society continues to become increasingly digitalised. Digital security has therefore become an ironclad necessity for preserving our way of life and our freedom. As a reliable partner in our national cybersecurity structures, the Dutch Ministry of Defence is committed to protecting that digital security. This, however, does not absolve private parties from their responsibility for ensuring their own security is up to scratch.

Like international waters, the digital realm is accessible to all: it is a global commons. This complicates the notion of national sovereignty, as threats – particularly in the digital domain – do not stop at national borders. That is also why we emphatically pursue partnerships with our allies in NATO and the EU. Within NATO, we have established agreements under the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) initiative with regard to the use of military digital capabilities, and within the EU we are working on joint capabilities such as Cyber Information Domain Coordination Cell or Cyber Rapid Response Teams as part of the Permanent Structured Cooperation (PESCO) initiative. In addition, the Dutch Ministry of Defence is participating in various cybersecurity exercises and training programmes in the European or NATO context.

But let us return to ancient Greece for a moment. In order to guard themselves from attack by enemy vessels – who deployed ramming tactics to break the fleet's formation – the Greek triremes would arrange themselves in a circular *kyklos* for protection. From this position, the Greeks were able to anticipate the movements of their opponent while keeping the core of their fleet, their vital interests, safe. A weak spot in the *kyklos* was a vulnerability for the assembled fleet. While the Ministry of Defence is one of the ships that make up the circle, we are most definitely unable to do it alone. In cooperation with public and private partners in the Netherlands, and with our international military partners in NATO and the EU, we must ensure the circle holds tight. Together, we form a *kyklos* around Dutch society: we are protecting the things we cherish.

Photo: Arenda Oomen

‘CYBERSECURITY DESERVES MAYOR'S FULL ATTENTION’

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 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.

Sjoerd Potters is Mayor of the Municipality of De Bilt and responsible for cybersecurity issues on behalf of the municipal executive. Despite having a background in law rather than cybersecurity, he does not consider that any reason to shy away from the issue. On the contrary, digitalisation and cyber resilience affect so many other domains that they deserve the Mayor's full attention. Potters is well aware that we are vulnerable to digital disruptions. He also realises that we often fail to grasp the extent of the threat. So how do we address those issues, and what role should mayors and municipalities be playing? We met to discuss these and other matters.

Sjoerd Potters
Mayor of the Municipality of De Bilt

In De Bilt, cybersecurity is part of the Mayor's responsibilities. As Potters points out, this approach was adopted for good reason: ‘Talk to any technical specialist, and they'll tell you the impact of a cyber incident is far greater than you'd expect. Incident resolution is also a complex process. You can't just switch off the server and expect everything to work again. We need to make sure that awareness spreads beyond the IT sector. However, the cybersecurity community tends to be very insular. Cyber specialists often focus on their own field of expertise, while outsiders are quick to dismiss the issue as "complicated" and "a job for the experts". However, the digital and physical domains have become increasingly intertwined in recent years, and cyber incidents can have a major impact on society. That's why the issue deserves the Mayor's full attention. I feel it's my responsibility to bridge the gap between those two domains.’

‘Cybersecurity incidents are increasingly affecting the “real” world and are occurring more frequently. If the digital realm is shut down, residents will be affected far more badly than would have been the case ten years ago. We won't be able to issue passports, traffic lights and bridges won't work and benefits won't be paid, with all the associated consequences. The notion of a ransomware or DDoS attack might sound abstract to a lot of people. Still, if the attack crashes a server that controls traffic lights, you can expect to see real-world consequences. When that happens, people suddenly realise the seriousness of the situation and start taking action on a different level.’

Disaster drills

‘We have an effective crisis management structure in place to deal with incidents that affect the physical domain. However, cyberthreats are constantly evolving, leading to all sorts of potential new scenarios. We simulated a digital incident with physical implications in collaboration with the Dutch Ministry of the Interior and Kingdom Relations this year. As it turned out, our response mechanisms for incidents in the physical domain are actually pretty solid. However, the intersection between both domains did leave room for improvement.’

‘We're used to addressing digital issues internally through the Chief Information Security Officer (in short CISO) and – if necessary – an external expert, but it's actually crucial to engage with external parties. We should be quicker to mobilise the resources that already exist in the physical domain. That's why we'll be kicking off future disaster and incident training drills with a digital component instead of situations like an LPG tank that's about to explode. Obviously, those exercises also need to tie in to the physical realm. So, how are we managing the transition from digital to physical? Will we be able to build awareness of the potential risks before it's too late? And will we have adequate crisis response mechanisms in place? We're working to connect those two worlds. As far as I'm aware, most

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 fysiek 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 afgelopen 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.”

Photo: De Beeldunie

municipalities aren't doing that yet.’

Embedding processes in the organisation
‘We apply and implement the Government Information Security Baseline, which is the minimum standard for all municipalities. It's a useful tool: you don't have to figure everything out on your own. As Mayor, I'm in close touch with the Chief Information Security Officer (CISO). We communicate on an almost weekly basis. Although I am responsible for cyber resilience, it's obviously not my exclusive domain. We need to make sure there's broader support within the municipal administration.’
‘The Municipal Executive discusses the issue at fixed moments in the planning and control cycle. I've found it can be quite hard to get the other members on board. They also tend to view the issue as highly technical and aren't fully aware of the risks. That's why we've decided to organise a cybersecurity training course for the entire Municipal Executive soon. We want to make sure the council has all the information it needs to hold effective discussions on cyber resilience and the necessary investments. That's why we’ve appointed two council rapporteurs, who receive updates along with the CISO during separate sessions. They have a lot of expertise on digitalisation and cyber resilience and are happy to share it with the council.’

Transparency creates awareness
Potters previously urged municipalities to share more information on cyber incidents: ‘Thankfully, municipalities generally don't mind sharing information on embarrassing incidents these days. We're far more likely to inform each other when something goes wrong. That's partly due to the incident in the Municipality of Hollandse Kroon. The municipal authorities were very open at the time, and I see that as a sign of strength. It was an important learning experience for us, and we discussed it in detail in the Municipal Executive: what kind of preparations have we made? It

“We moeten een cyberincident aanvliegen als een klassieke ramp”

‘We need to approach cyber incidents as if they were conventional disasters’

Borging binnen de organisatie
“De Baseline Informatieveiligheid Overheid wordt bij ons toegepast en uitgevoerd. Alle gemeenten hanteren die als ondergrens. Het is 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 bespreken we 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.

really helped to raise awareness of the issue.’

‘The municipality of De Bilt is part of a consortium of six or seven municipalities,’ Potters continues. ‘The municipal CISOs form a pool. They exchange lots of knowledge and information and can stand in for each other if necessary. We regularly conduct tests together to identify vulnerabilities and keep our defences as strong as possible. That tends to yield useful information, which we can then put to good use. For example, we recently discovered that our systems could be breached in just two steps through vulnerabilities at another municipality, despite our own house being in order. That came as a shock, and we obviously took measures right away. We also set up a crisis team to deal with potential incidents. We know who is responsible for what and who to call if we need more expertise. Our technical staff are in close contact with the National Cyber Security Centre (NCSC) through the Municipal Information Security Service. Almost all municipalities now have similar arrangements. Effective communication between the CISO, administrators and the NCSC is essential. The lines of communication need to be clear and short.

In Potters' view, cyber resilience is heavily dependent on the other parties in your network. ‘That includes executive agencies and service providers as well as other municipalities. For example, we recently had a data breach involving the speed camera system in one of our villages. As it turned out, hackers could easily access licence plate details. We had a data processing agreement with the external party, so everything seemed secure on paper. Still, you can't just sign an agreement and lean back; you need to monitor the situation by asking the right questions. A national quality standard for digital service providers would be helpful in that sense. I mean, we also have a Food and Consumer Product Safety Authority. They monitor all kinds of things that most people don't necessarily understand in the

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 is cyberweerbaarheid een belangrijk aandachtspunt en ik zie 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."

BACK TO TOP

"Cyberdreiging neemt toe, daar moeten we ons veel meer samen en integraal op voorbereiden"

'Cyberthreats are on the rise, and we need to prepare for them on a much more collective and holistic basis"

public interest. Secure digital services are also in the public interest.'

National Cyber Resilience Strategy
As Potters points out, we are seeing a growing number of cyberthreats from multiple sources: 'As a society, we need to prepare on a much more collective and holistic basis. Our role as municipalities will depend on the source of the threat. The central government will have to provide a coordinated response to any attacks by state actors, but municipalities need to manage the resulting social impact. At a local level, municipalities need to have their house in order, carry out exercises within the security region and reach agreements. We need to approach cyber incidents as if they were conventional disasters.'
'Municipalities take the lead during physical incidents, but cyber incidents are obviously less clearly defined. The role of the security regions and municipalities isn't always clear, so you need to make solid agreements. As far as I know, those agreements are currently still missing. We're just waiting for the other shoe to drop, and that's a shame. I should point out that the COVID-19 pandemic has taught us a lot about agreements between the national government, the security regions and the municipalities. It hasn't always been clear who is responsible for what, and I hope and expect that the lessons learned will eventually trickle down to the cybersecurity domain. Cyber resilience is a top priority for the Association of Netherlands Municipalities, and I definitely think municipalities have an important role to play. However, I also believe digitalisation and cyber resilience are important enough to justify the creation of a separate ministry. That would really demonstrate the government's commitment to the issue and lend it a presence in the public debate. It could also help to raise awareness.'

NEXT

Photo: ANP

Frank Breedijk
Ethical hacker DIVD

Chris van 't Hof
Co-founder DIVD

A SAFER INTERNET AND SOCIETY WITH DUTCH-STYLE APPROACH

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.

In the Netherlands, every day an organisation falls victim to an attack by cyber criminals. In October 2021, a digital attack on the VDL industrial group made the headlines. Worldwide 105 companies were affected, including several in the Netherlands. For example, operations at car manufacturer NedCar in Born largely came to a standstill due to the attack. More recently, Log4J, an important software tool for a wide range of Internet applications, was found to have a serious vulnerability. However, by far the majority of hacks, vulnerabilities and ransomware attacks do not attract any publicity at all. As one of the measures to enhance society's cyber resilience, the Dutch government has created a nationwide system of information exchanges (LDS). One of the organisations involved in the LDS is the Dutch Institute for Vulnerability Disclosure (DIVD), whose experts are critical of the network but hopeful about its future.

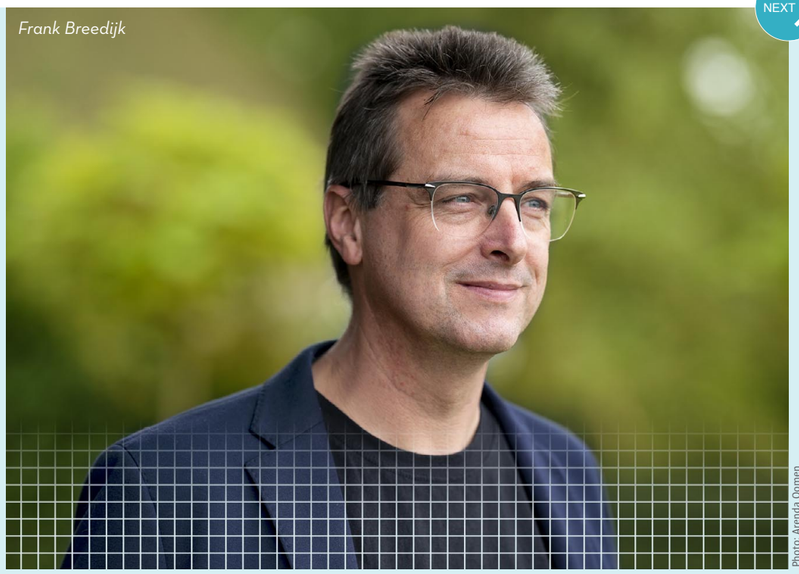

Frank Breedijk

Photo: Arenda Oomen


Chris van 't Hof

Photo: Arenda Oomen

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.''

DIVD aims to increase digital security by warning organisations about vulnerabilities in their digital systems before malicious hackers can exploit them. Chris van 't Hof, one of the founders of DIVD, and Frank Breedijk, an ethical hacker who has been involved with DIVD since its launch, tell us about their motivations, their mission and what they believe are the future roles of DIVD and the government in this context.

From vulnerability to hack

Chris explains what makes their task so urgent: 'We scan the whole of the Internet, exposing vulnerabilities in the process. We see the number of potential victims, are surprised that so very few victims become known and realise that the majority of organisations that are hacked don't make the news.'

What does make the news are the really big cases, such as the vulnerability of software tool Log4J and that of software supplier Kaseya. Their software was hacked by REvil, a group which is thought to be based in Russia. The DIVD hackers had already detected eight vulnerabilities in the software, and reported them to Kaseya, two months before the attack. The problem was that the patch (a system update to close security gaps) was not ready in time. That particular leak in the system meant there were millions of potential victims and eventually caused several thousands of real victims. Kaseya worked with DIVD and several other parties to find solutions for the hack.

According to Van 't Hof, the Kaseya case clearly demonstrates why an LSD is so important and why DIVD serves a real purpose: 'There is a need for a party that scans the Internet and reports the vulnerabilities found – a task that is not addressed very effectively within the system at the moment.'

Within the LDS framework, public and private parties join forces to exchange information and knowledge about cybersecurity issues so as to prevent digital disruption and make the

“We opereren in een niche waarin de overheid en het bedrijfsleven (nog) niet kunnen acteren.”

‘We operate in a niche in which the government and the business communicatie cannot act, at least not for the present.’

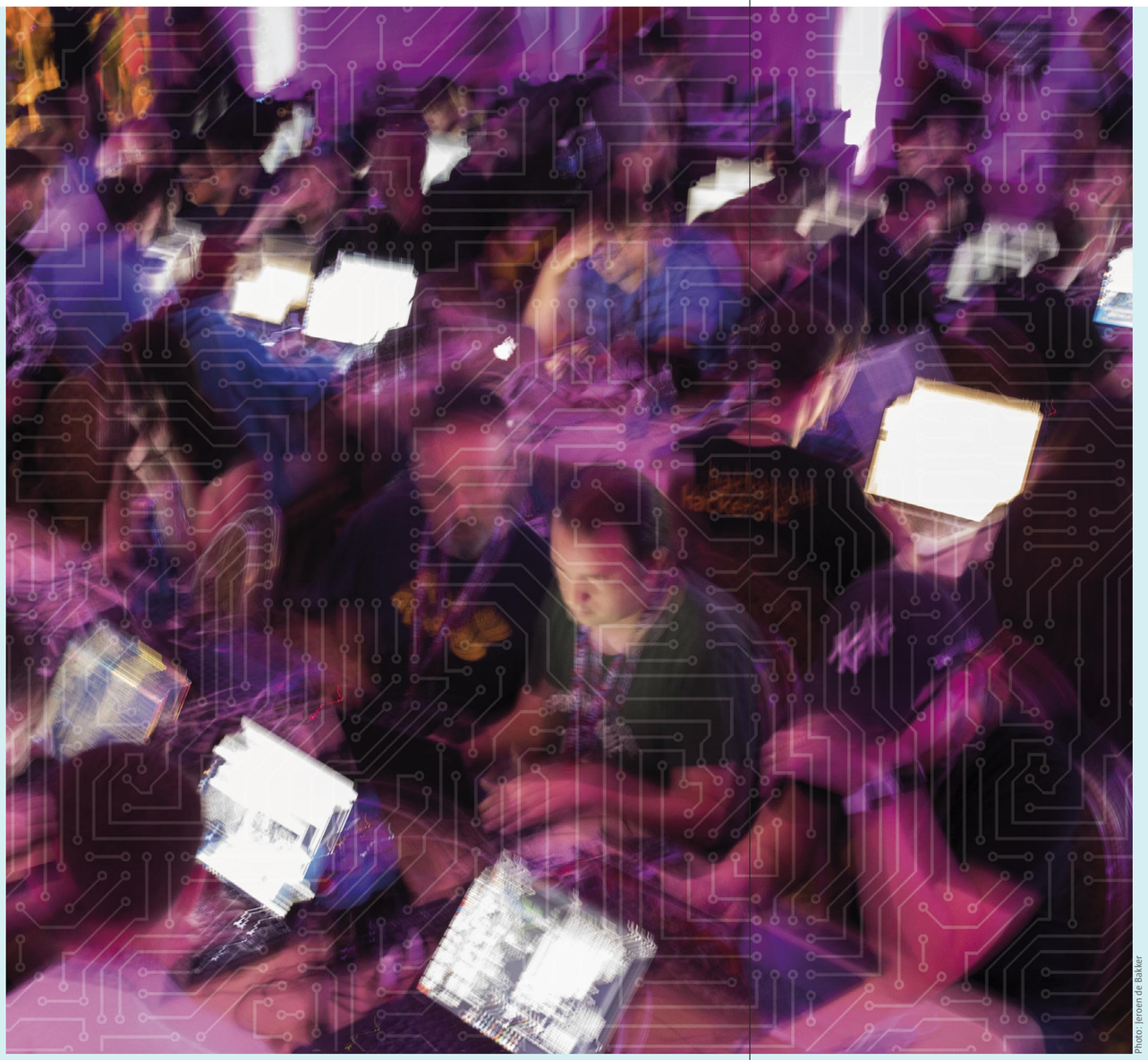


Photo: Jeroen de Bakker

Netherlands more cyber resilient. This includes parties such as CERTs (Computer emergency response teams), sectoral and regional partnerships, the National Cyber Security Centre (NCSC) and the Digital Trust Center (DTC). Van 't Hof points out however that many organisations in the Netherlands are not covered by the LDS: ‘Think of small and medium-sized businesses, for instance, websites of sports clubs and allotment gardens, or small webshops. Our research helps to fill these gaps in the LDS, because we scan them all.’

Sharing information is key

Van 't Hof and Breedijk welcome the new developments surrounding the LDS, including the establishment of an innovative public-private partnership. After all, the government is bound by laws and regulations, resulting in limitations in terms of what they can do. Both believe that the bill amending the Security of Network and Information Systems Act (Wbni), which will help flesh out the LDS, is a reason for optimism. They are also positive about the way the government is addressing the vulnerability in software tool Log4J. Here, the NCSC did take on the role of national coordinator. They do however believe that time is running out and that faster action is essential, which cannot be achieved, they say, without private initiative.

Van 't Hof: ‘Our initiative is a partnership with the government, but we can't expect the government to organise it. Public bodies cannot simply scan systems for vulnerabilities and report them of their own accord. They face limitations, for example under the General Data Protection Regulation (GDPR) and also the Wbni. We however operate on the basis of case law according to which scanning and reporting is permitted if it serves a public interest, is proportional and cannot be done in any other way.’

When asked whether the government shouldn't take over their tasks, Van 't Hof and Breedijk have a clear answer: ‘We operate in a niche in which the government and the business community cannot act, at least not for the present, so we’re making a very concrete contribution to national security. Since keeping the Internet secure is a task that serves the public interest, it should be a responsibility of the government, just like the way they have addressed the vulnerability in software tool Log4j. However, as long as DIVD is able to perform that task in a manner that is impossible for the government, we have a clear raison d’être.’ Will the government take over their task? Breedijk: ‘In that case we'll find another problem for us to tackle as a haven for creative and ethical hackers.’

Collaboration government and DIVD

‘You could compare us with the Red Cross. The fact that they exist doesn't mean we can do away with ambulances and hospitals. The Red Cross is able to reach places where the government cannot or doesn't want to go,’ says Breedijk.

The fact that an independent organisation takes up this task, Van 't Hoff adds, is also important for another reason. ‘We're talking about an incredible amount of data, which means you also obtain a great deal of power. Such power in the hands of a government body or a business could easily result in a situation where they might also use that power for other purposes than cybersecurity. It's important and possible to avoid even the appearance of such a situation, by assigning the task to an independent organisation like DIVD.’

It is up to DIVD to alert all organisations to their respective vulnerabilities and potential leaks. Breedijk compares a warning by DIVD with an air-raid siren. ‘If you don't want to hear the air-raid siren, you may soon be in big trouble. The same applies to our reports: you are free to ignore them, but we'll keep sending them as soon as we detect a vulnerability.’

The Netherlands has taken the lead

‘During the Dutch Presidency of the EU in 2016, everybody came to

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.

this country to study our approach to Coordinated Vulnerability Disclosure,’ says Van 't Hof. 'We were really taking the lead in that area, and still are; the Dutch consensus culture in the digital realm is unique. In many other countries, in contrast, there are only two options: either a total ban on scanning and reporting, meaning that you'll soon find yourself the subject of legal action, or the government claiming that hacking is so rampant that any policy to fight it would be useless.’ For both DIVD representatives, the fact that the Dutch government permits DIVD to do what it is doing and even collaborates with them is a clear sign of the government's positive attitude. The coordination and collaboration are unique and, together, constitute a good and essential step on the path towards increased Internet security.

Idealistic hackers

Van 't Hof cites promoting the public good as one important motive that drives all contributors to DIVD: 'As we all share this sense of justice, we're a group of like-minded individuals working together for a common cause: making the Internet, and our society at large, a safer place.’ Breedijk adds: ’Once people no longer trust the Internet, you might as well shut it down. While in fact the Internet is beautiful and important, also for society as a whole. Security is a basis for trust.’

Van 't Hof: ’Nor should you underestimate the fun, creativity and inspiration you get from working for DIVD, with all the wonderful people you collaborate with. DIVD staff usually work in ICT themselves, but within DIVD they are totally free to do what they want to do and are really good at, for a noble societal cause.’ Breedijk adds: ‘It's great to be able to share this passion with others and to put your heart and soul into it.’

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.’’

BACK TO TOP

“Het is nu drie voor twaalf en daarom is er meer snelheid nodig.”

‘Time is running out and faster action is essential.’

Over DIVD

Dutch Institute for Vulnerability Disclosure (DIVD) is een onderzoeksinstituut dat het internet afspeurt op zoek naar kwetsbaarheden. Wanneer de hackers, die allemaal op vrijwillige basis hun werk voor DIVD uitvoeren, een dergelijke kwetsbaarheid in de systemen vinden, waarschuwen ze de betrokken organisaties. Zo willen ze voorkomen dat hackers met slechte intenties de kwetsbaarheden gebruiken voor criminele doeleinden. Voor de oprichting van DIVD gebeurde dit werk ook al door de individuele hackers, maar met het oprichten van de stichting worden financiële zaken en de aansprakelijkheidskwesties collectief en makkelijker geregeld

DIVD werd twee jaar geleden opgericht door Victor Gevers, Astrid Oosenbrug en Chris van ’t Hof. Frank Breedijk is ethisch hacker vanaf de oprichting. Hij vertelt dat er nu zo’n 60 actief betrokken DIVD’ers zijn. ‘’Daardoor ontstaat er een web of trust. Door het persoonlijke contact kennen en vertrouwen we elkaar. De samenwerking is gebaseerd op ethiek en maatschappelijke verantwoordelijkheid, dit is een belangrijke gemeenschappelijke factor.’’

About DIVD

The Dutch Institute for Vulnerability Disclosure (DIVD) is a research institute that scans the Internet for vulnerabilities. The hackers all work for DIVD on a voluntary basis. As soon as they detect a vulnerability in a system, they warn the organisation involved. In this way they aim to prevent malicious hackers from exploiting the vulnerability for criminal purposes. Before DIVD was founded, there were hackers who performed this task on an individual basis, but the foundation has made it easier to arrange financial and liability issues collectively.

DIVD was founded two years ago by Victor Gevers, Astrid Oosenbrug and Chris van ’t Hof. According to Frank Breedijk, who has been involved as an ethical hacker from the start, they now have a workforce of around 60 active DIVD staff. ’This has created a “web of trust”. The personal contact means that we know and trust each other. Our collaboration is based on ethics and social responsibility; this is an important factor that unites us.’

Photo: Arenda Oomen

RACE FOR INNOVATION IN CYBER DOMAIN

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, afgelopen juni 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."

A major effort to reinforce and improve our research, education and innovation will be crucial in ensuring the Netherlands' continued cyber resilience and digital autonomy. The Dutch Cyber Security Council (CSR) reached this conclusion in its 'A comprehensive approach to cyber resilience' advisory report, published last year. Eddy Boot, who took over as director of dcypher last June, hopes his collaborative platform will play an important role in this process. 'All stakeholders will have to change their approach and behaviour if we aim to collaborate effectively.'

Eddy Boot
Director dcypher

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.

Samenwerking vanaf het startschot

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

"Alleen met echt nieuwe soorten oplossingen kunnen we de huidige problemen het hoofd bieden."

'We won't be able to face up to the current problems without developing genuinely innovative solutions.'

Boot, who has gained extensive experience in public-private partnerships during his two decades at the Netherlands Organisation for Applied Scientific Research (TNO) research institute, likes to compare the innovation process and its challenges to a relay race. 'A professor and their PhD students get started on a fundamental research project. At some point, they will inevitably pass the baton to applied researchers at an organisation like TNO. Those researchers then help to bring the innovation to fruition in collaboration with research consortia, *spin outs* or startups. They eventually pass the baton to the cyber industry, which can turn it into new products and services. In the final stage of the process, the relay baton – and thus the innovation – finds its way to the end user.'

While that all seems well and good in theory, anyone who has ever witnessed an actual relay race will instinctively understand the biggest risk: one of the runners might just drop the baton.

Innovation is vulnerable to the same danger, as evidenced by the somewhat overblown "valley of death" metaphor. Many potentially innovative products and services die in this doomed valley over the course of the innovation process. In some cases, it proves impossible to reach enough providers and end users or scale up beyond the local level. Other causes include a failure to identify existing funding opportunities.

Cooperation from the starting line

The valley of death is littered with missed opportunities, and Boot wants to change that. His solution? Innovation partnerships in the cybersecurity domain should begin at the starting line rather than the finish. 'If all the stakeholders are on board from the start, everyone will be a lot more committed to the project. That way, you can also capitalise on the fact that innovation processes are rarely linear. That non-linear aspect makes it difficult to define certain

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.”

Photo: Hollandse Hoogte

“De samenwerking rond innovatie in het cybersecuritydomein moet niet pas vanaf de finishlijn plaatsvinden, maar al bij het startschot.”

‘Innovation partnerships in the cybersecurity domain should begin at the starting line rather than the finish.’

phases of the research, innovation and valorisation process in advance or determine the ideal time for stakeholders to get involved,’ the dcypher director explains.

As the 'platform to end all platforms', Boot hopes dcypher will bring together all the parties who make a real difference at the starting line. ‘Everyone gets to carry the baton, so they all share responsibility and move towards the finish line together. The end result: the professor receives the relevant research questions at the right moment, the applied researchers have more opportunities to test the innovation in the field, cyber providers get to speed up their development processes and end users get an early start on implementing the new products and services,’ Boot elaborates.

This improved cooperation across the cybersecurity domain should help us overcome a number of problems. In Boot's analysis, we currently lack the necessary cybersecurity expertise and are failing to valorise innovations effectively. ‘The goals of dcypher are clear: more trained staff, more knowledge and applications and more valorisation’, he explains. Boot believes innovation also has a crucial role to play here. ‘We won't be able to face up to the current problems without developing genuinely innovative solutions.’

The winning team

In the relay race to make the Netherlands safer, smarter and more digitally autonomous, Boot wants to be the sports coach who assembles a winning team at the starting line. He has not been in his current position at dcypher that long. During his first months as director, Boot spent most of his time in the field trying to identify opportunities and challenges. A few things stood out: ‘I saw a lot of engagement, new ideas, grand ambitions and a willingness to collaborate. The scope and number of parties operating in the field of cybersecurity is also fairly limited, which makes the situation easier to oversee. A lot of the parties working in education, research, business and government have known each other for a long time and are familiar with the main challenges facing the sector. I also noticed there's a great need for more resources and closer cooperation in the field,' he says.

As Boot explains, the issue of cybersecurity is complicated by the fact that each individual party, organisation and authority has both its own capacities and its own limitations. ‘None of those individual parties can fully resolve the problems without the others' help. That's why we need more multidisciplinary collaboration across the entire cybersecurity innovation chain. I also believe all the parties involved will have to change their approach and behaviour if we aim to work together effectively. We will all have to respect each other's positions, perspectives and interests, which may not necessarily align all the time. Sometimes, you also need to step back and let others have their day for the sake of the greater good. It's all about formulating clear common ambitions and acting on them.’

A spider in the web

As a collaborative platform, dcypher can play an important role in bringing the sector together, Boot hopes. ‘We're an independent spider in the web. As a non-partisan intermediary, we encourage parties in the cybersecurity domain to collaborate more effectively on innovation. The resulting innovations will help to make this country's cybersecurity efforts more effective from a strategic, tactical and operational point of view. At the same time, we obviously don't have a magic formula to balance supply, demand and funding more effectively,’ he admits.

‘However, we can lead by example, mobilise the field to focus on the most urgent problems first and ultimately facilitate solutions. Finally, we can help to secure funding on the right terms and make sure the entire cybersecurity innovation chain – from education and research to business and

“Er is een gebrek aan cybersecurity-expertise en het ontbreekt bovendien aan het valoriseren van innovaties.”

‘We currently lack the necessary cybersecurity expertise and are failing to valorise innovations effectively.’

Government Support Portal

De juiste (toegang tot) financiële instrumenten is een belangrijke succesfactor om van onderzoek en innovatie daadwerkelijk tot toepassing en valorisatie te komen. Recente rapporten stellen echter ook vast dat die instrumenten niet altijd goed toegankelijk zijn of geschikt voor cybersecurity innovatie. dcypher wil het veld ondersteunen door toegang te bieden tot de juiste financiering op het juiste moment. Over de hele innovatieketen en voor onderzoek, startups, scale-ups en het midden- en kleinbedrijf. Daarvoor heeft dcypher de juiste ingangen bij onder meer NWO, RVO, EZK, Topsectoren en in de EU. Op de website van dcypher wordt momenteel een digitaal portal ingericht om gebruiksvriendelijke financieringsoverzichten te bieden, maar vooral om specifieke vragen aan specifieke oplossingen te koppelen. Deels digitaal, maar ook door gesprekken met de behoeftestellers. Op basis daarvan zal dcypher ook het gesprek voeren met de genoemde aanbieders om de financiële instrumenten meer op maat voor het veld te maken. **dcypher.nl**

Government Support Portal

We will have to ensure access to suitable financial instruments if we aim to develop applications and achieve valorisation. However, recent reports also suggest that existing instruments are not always readily accessible or suitable for cybersecurity innovation purposes. dcypher aims to empower the field by providing access to the most suitable financing instruments at the right time. These instruments should be available throughout the entire innovation chain in support of research projects, start-ups, scale-ups and small and medium-sized enterprises. dcypher has already established the necessary contacts at organisations such as the Dutch Research Council (NWO), the Netherlands Enterprise Agency, the Dutch Ministry of Economic Affairs and Climate Policy, Top Sectors and various EU institutions. A digital portal is currently being created on the dcypher website in order to provide access to user-friendly financing overviews and match specific questions with relevant solutions. This process will be conducted online and in direct consultation with potential recipients. dcypher will also use this information as a basis for discussions with the aforementioned providers in order to tailor the financial instruments more closely to the field's requirements. ***dcypher.nl***

BACK TO TOP

government – is optimally structured. Many parties have already established mutual ties and are relatively well organised. dcypher now faces the challenge of streamlining those processes and taking them to the next level by aligning supply and demand.’ As the platform's new director, Boot will continue to build on the work accomplished by dcypher's predecessor in recent years. He has defined a clear set of priorities for the next four years. ‘The platform has achieved a great deal in the field of education and research over the recent period. I want to consolidate and build on those efforts.

Revenue potential

He mentions valorisation as an important new aspect: 'the revenue potential of cybersecurity innovations. Boot: ‘We want to get products and services to market faster by accelerating knowledge development, strengthening the cyber industry and boosting end-user absorption. Among other activities, we're currently developing a digital portal to improve the accessibility of funding sources and make them more convenient for the cybersecurity field (see box). We're also organising a matchmaking event for EU businesses and research institutes and developing multi-year roadmaps to encourage long-term cooperation on research, application and economic activity throughout the innovation chain. It's time to get things moving. Or, as MEP Bart Groothuis recently told dcypher: strategy is execution, and execution is strategy.’

Photo: Nationale Beeldbank

Bibi van den Berg
Professor Cybersecurity Governance
Leiden University, chairman ACCSS

Aiko Pras
Professor Cybersecurity Twente
University, co-chair ACCSS

‘THE NETHERLANDS SHOULD DECIDE WHERE IT STANDS’

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 het 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 het ACCSS (en tevens lid van de Cyber Security Raad namens de wetenschap) en Aiko Pras, professor cyberveiligheid aan de Universiteit Twente en vicevoorzitter van het ACCSS.

The ACademic Cyber Security Society (ACCSS – pronounced as ‘access’), founded in February 2021, is an association of scientists in the Netherlands that focus on cybersecurity. Since its foundation, over 90 scientists and 8 research institutes have joined ACCSS and the organisation expects considerable further growth in the years ahead. This is important not just for science, but also for the Dutch cybersecurity strategy. We discussed this with Bibi van den Berg, Professor of Cybersecurity Governance at Leiden University and chair of ACCSS (and a member of the Dutch Cyber Security Council on behalf of the scientific community) and Aiko Pras, Professor of Cybersecurity at the University of Twente and vice-chair of ACCSS.

Photo: Arenda Oomen

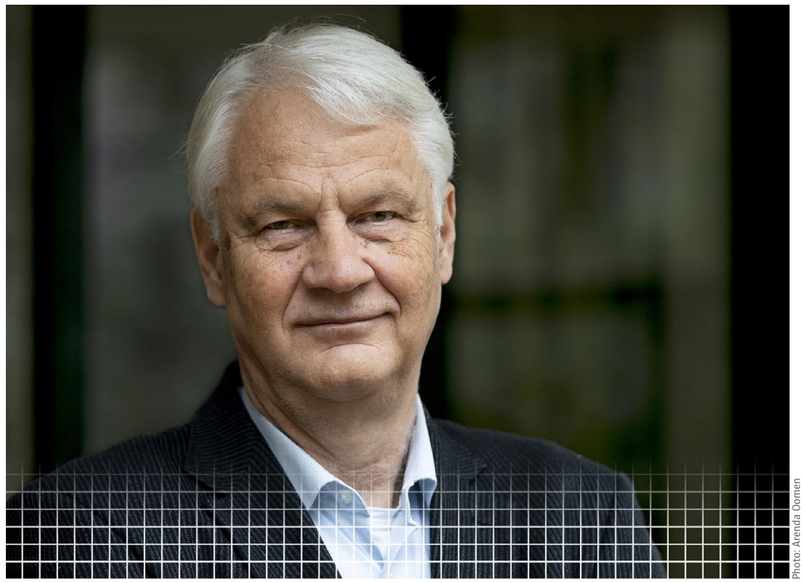


Photo: Arenda Oomen

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

The former dcypher, a network organisation for cybersecurity, closed down in October 2020. Among other things, this also meant the end of an important platform for connecting cybersecurity scientists. ACCSS has since filled the void. This is why Bibi van den Berg regards connection as an important task for the association: ‘ACCSS was born out of the idea that cybersecurity scientists in the Netherlands need a permanent platform from where they can build their own network.’

According to Van den Berg, this also explains why ACCSS connects experts from across the spectrum – natural sciences, arts & humanities and social sciences. ‘Cybersecurity is a multidisciplinary domain that transcends boundaries within the academic world. Unfortunately, contacts among many scientists are occasionally less than perfect, even though they are dealing with the same scientific issues. Our aim was to create a place where scientists can easily get in touch with each other for project or subsidy applications.’

Aiko Pras agrees that one important task of ACCSS is to unite scientists: ‘Analysis of the cybersecurity threats ahead of us shows that they are growing much faster than many people thought possible for a long time. There's a growing awareness that our society is under threat. At the same time, there's a severe shortage of experts who can give advice on the matter. This is why it's important for us scientists to unite, so that we can do more research and improve education.’

Improving findability

A second key task of ACCSS, alongside connection, is to improve findability. Van den Berg: 'Some cybersecurity scientists have excellent visibility in the media, in the public debate and among research sponsors. However, this does not apply to all of them. This is all the more reason to cherish a place that provides a single channel for anyone wishing to contact cybersecurity scientists.’ The need for such a place became apparent soon after it was created: ‘From the word go, parties contacted ACCSS asking for assistance, for example in assigning projects. They had the resources but didn't know where to go. In such cases, ACCSS takes on the role of a broker, finding the right scientist for the right project. We don't only serve university professors in this way. For example, we now also have a group of PhD students combining work and research for the government.’

Speaking in one voice

The third pillar is visibility. ACCSS has offered opportunities for scientists to make themselves heard better and more frequently. ‘It is important for us to contribute a scientific perspective to the many plans and agendas that are being developed,’ says Van den Berg. ‘Of course, scientists may have different views on certain issues; there should always be room for diverging insights. But on certain topics it's important to speak in one voice. Thanks to ACCSS, that voice can be heard in the debate. ‘Last summer, for example, ACCSS urged public parties not to pay a ransom in ransomware attacks, and in September it called for information about data leaks to be made public for further investigation. The organisation is currently drafting a proposal for a Growth Fund to promote research and education in the field of cybersecurity. The fund should provide a budget for research and training.

ACCSS is also collaborating with dcypher, which was re-launched in the autumn of 2021 and now comes under the Dutch Ministry of Economic Affairs and Climate Policy. Van den Berg explains: ‘dcypher is currently drafting a research and education agenda, and we're contributing to that effort. That's why we also regard ourselves as one of the key subcontractors of dcypher.’ According to Pras, they are actually much more than a subcontractor. ‘The big advantage of ACCSS is that we're outside of the existing hierarchy, for example within the government. This gives us a stronger position and more influence. So actually dcypher really needs us very much.’

Photo: Nationale Beeldbank

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."

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 cybersecurity-wetenschappers 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."

Connecting worlds
Are there any untapped opportunities for collaboration between scientists? For Pras, the answer is clear: 'In the past, the technical aspects of cybersecurity were always very well coordinated. We met and we collaborated. The current issues however are far less technical in nature. Think of fake news, for example. In those areas, cybersecurity is only just emerging. We're seeing all sorts of little groups popping up with their own specialisations. Cybersecurity is new to all of them, and they don't know each other either. So how can we get the players in the non-technical domain together?'

Van den Berg adds: 'It's also about making connections between the technical and non-technical people. I have a strong network in non-technical subjects, but it's in trying to connect with the scientists where things often go wrong. Still, it's essential to have everyone around the table. In addition, a multidisciplinary approach is a requirement in many research projects. Therefor you need to be able to find the right people for that.'

Identifying and formulating the right questions
Scientific knowledge and insights are important in today's cybersecurity landscape. This is because science has a number of valuable characteristics. Van den Berg explains: 'Scientists are up to date on the latest developments and recent knowledge, also – and particular – on matters that haven't yet reached the general public. In addition, we contribute independent expertise. Advice from companies is at times motivated by commercial interests. That's much less of a problem with scientists.' According to Pras, scientists are also important to help identify and formulate the right questions. 'Talks between the government and sectors often involve the question of what cybersecurity measures need to be taken in a particular sector. The problem is that it's very difficult to identify such measures when cybersecurity is not your core task. Even so, the issue is a source of great concern in many sectors. It is precisely in talks like this that scientists can make an important contribution.' Van den Berg agrees on the importance of science in public-private partnerships: 'As a university professor I'm frequently asked to help organisations and businesses formulate their questions. It's all so early and new; many organisations lack a clear overview of the questions they need to answer to make sure everything is in order.'

The consensus model carried too far
Both professors have their doubts about the current state of cybersecurity in the Netherlands. Pras does see some bright spots: 'From a scientific angle, several initiatives and research projects being conducted in the Netherlands have attracted considerable praise and are doing an absolutely wonderful job.' However, Pras is less positive about the bigger picture: 'Compared with the situation in many other countries, and how they are using and funding science and education to promote innovation in the field of cybersecurity, we've still got a long way to go.' Van den Berg agrees, adding that we are witnessing the slow erosion of the Dutch knowledge economy in terms of cybersecurity, with low investment resulting in what she calls a brain drain. This is why she believes it is urgent for education to receive more funding and more attention: 'This is not just about young university students or post-masters, it's also about Lifelong Learning. The cybersecurity domain is attracting more and more employees from other roles and positions who have to learn the ropes on the job. We should join forces with knowledge centres and educational institutions to create far more training programmes for professionals. Some universities have already taken steps in that direction, but the effort needs to be scaled up.' Pras concurs: 'Education is being taken for granted. However, we do need to broaden our view. Rather than just focusing on research universities and universities of applied sciences, we should also offer options for transfer students from other degree programmes or school levels.

"ACCSS verbindt zowel bèta, alfa en gamma-wetenschappers voor cybersecurity."

'ACCSS connects scientists from across the spectrum – natural sciences, arts & humanities and social sciences – for cybersecurity'

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."

De 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, password-managers en back-up-strategieën. Zeker belangrijk, maar aan de grote dingen die we ook nodig hebben, komen we daardoor niet toe."

"De Nederlandse kenniseconomie op het gebied van cybersecurity wordt langzaam uitgehold, waarbij lage investeringen leiden tot een braindrain."

'We are witnessing the slow erosion of the Dutch knowledge economy in terms of cybersecurity, with low investment resulting in what we call a brain drain.'

Perhaps we should start right at the beginning, at primary school.'

The two professors are also critical when it comes to research. According to Van den Berg, research projects are often assigned without sufficient prior consultation with scientists. 'There's too much reliance on the market to fill existing needs. More often than not, nobody bothers to find out whether scientists are already addressing those needs, or have any use for market solutions.' This is why Van den Berg calls for broadening the research agenda. 'I'm not suggesting we should formulate our own proposals, but I do believe we are now going too much in the opposite direction. As a result, a great deal of research is not covered, such as fundamental research and research into cutting edge technologies.'
Pras agrees that there is a mismatch between supply of and demand for research. 'What's the kind of research that pays? Mainly research motivated by current issues: ransomware, password managers and back-up-strategies. While these issues are certainly important, they do prevent us from tackling other big problems that also require our attention.'

What does the Netherlands stand for?

The two professors agree that at the political level, there is room for considerable improvement. According to Pras, this is mainly due to the way the government takes decisions: 'I note that our wonderful consensus-based decision-making model no longer works. We've carried it too far; nobody dares to take any decision any more. Compared with other EU countries, there's a lot to be said but at least things are moving there, witness the construction of a competence centre in Romania, for instance.' Pras points out that the lack of effective action involves a number of risks: 'The Netherlands is running on an old economy. The new economy is an IT economy, with platforms such as Booking.com and Thuisbezorgd. We need to build a cybersecurity infrastructure that is able to support such an economy, and find

"Er liggen genoeg plannen en strategieën, het is tijd dat we dingen gaan uitvoeren."

'We have enough plans and strategies now; it's time to put them into practice.'

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."

BACK TO TOP

the right people to operate it. If we don't, we're bound to discover ten or fifteen years from now that everything has moved to other countries. If all you do is talk without making any investments, nothing will happen.'

Van den Berg agrees it is now time for the Netherlands to adopt a more proactive attitude. 'The big question that we need to answer in the Netherlands is 'What do we stand for?'. Once you've answered that question, you can take steps. Cybersecurity is currently assigned to various different government ministries, which inevitably means that many aspects will be overlooked.' This is why ACCSS, like the Dutch Cyber Security Coalition in its latest advisory report, calls for greater coordination on this topic. Van den Berg: 'Compare this with a theme such as water. We have appointed a Delta Programme Commissioner to cover this theme, quite separate from the various ministries, who works on a plan for the next 25 years. We are a world leader on water management, because we have simply decided that this should be a key focus for us.'

Time to get to work

Van den Berg is surprised that the Netherlands does not do the same when it comes to cybersecurity: 'The basic conditions in the Netherlands are good, We're a small country, our Internet density is high and we have many bright minds. We're able to create a perfect ecosystem, but somebody will need to take the initiative.' Pras adds: 'We can build a strong position for ourselves, not by offering tax benefits but thanks to that very ecosystem.' The main message of both professors, therefore, is that we need to get started: 'We have enough plans and strategies now; it's time to put them into practice. But we do need an overarching vision for that.'

EVERY ENTERPRISE IS CRITICAL

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 gebruik maakt 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'.

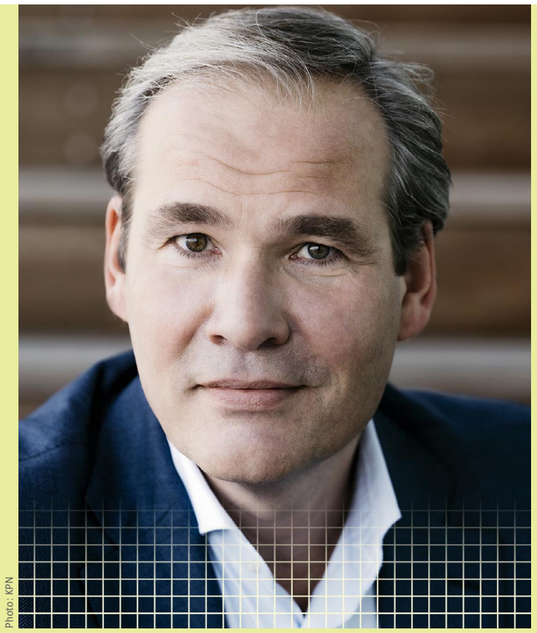


Photo: KPN

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.

Joost Farwerck
CEO en voorzitter van de Raad van Bestuur van KPN, lid van de CSR namens de vitale sectoren

"We mogen het midden- en kleinbedrijf niet uit het oog verliezen. Deze ruggengraat van de Nederlandse economie is immers ook vitaal."

'We mustn't lose sight of small and medium-sized enterprises. They are the backbone of the Dutch economy, after all, which makes them critical as well.'

BACK TO TOP

Since the second week of December 2021, a software vulnerability referred to in the media as Log4j or Log4Shell has resulted in an extremely grave security risk for anyone who makes use of digital services, both in the Netherlands and worldwide. In the Netherlands, the National Cyber Security Centre (NCSC) has therefore recommended that government bodies and businesses implement patches or workarounds as quickly as possible and – more importantly – that they prepare themselves for potentially large-scale exploitation of this vulnerability by malicious parties. This has once again demonstrated the vulnerability of our digital society.

There is much work to be done if we are to achieve a secure and resilient digital infrastructure – work that will never be complete. Cybersecurity will never be finished. This is especially true of the critical sectors whose proper functioning is of fundamental importance to Dutch society. Potential cyber-attacks on power plants, the port of Rotterdam, bridges and locks (to name just a few examples) could have unprecedented economic and social consequences. Cybersecurity, in other words, is a matter for the top brass and the resilience of critical sectors is of national importance. Cooperation and the sharing of information between the business and scientific communities and the government are vital. This must also include the improvement of risk and threat analyses and joint exercises. To that end, I support the proposed amendment to enable broader access to information on threats and incidents pertaining to systems. A better understanding of the risks will lead to more effective protection and make the Netherlands more resilient.

Efforts to enhance digital resilience are like a game of cat-and-mouse. Malicious actors have objectives, tactics and techniques that are constantly changing. Cyber-attacks are a very real problem. While the government and the business community are doing much to combat this, it is not yet enough. Businesses need assistance from the government to repel and detect criminals. Research conducted by the Dutch Cyber Security Council (CSR) shows that the Dutch government is investing less heavily in digital resilience than neighbouring countries. Belgium, for instance, has earmarked a sum 14 times greater than what the Netherlands is investing. As a result, the Netherlands is in danger of losing control and falling behind in a digital world that is by definition international, and where attackers consistently seek out the weakest point. The CSR has advocated for increasing Dutch investments in digital resilience and aligning them better with those of the countries surrounding us. The coalition agreement states that the government will invest in a 'broad, long-term approach to cybersecurity.' This is a good first step, and it is important that we capitalise on this momentum. In doing so, it is vital that we do not lose sight of small and medium-sized enterprises (SMEs). They are the backbone of the Dutch economy, after all, which makes them critical as well. As it currently stands, SMEs often lack the resources to effectively protect themselves – scalable solutions for digital resilience could help in this regard.

Ultimately, cybersecurity succeeds or fails based on a strong awareness of the opportunities and risks. Preserving our digital resilience in the coming years will require heightened vigilance and action. This is something we must undertake together, through the coordinated efforts of an involved government, knowledge institutions and the business community, of which SMEs are an essential part.

Joost Farwerck
Chair of the Executive Board and CEO of KPN, CSR member representing the vital sectors

Angeline van Dijk
Chief Inspector-Director of
Radiocommunications Agency
Netherlands

De weerbaarheid van vitale processen is een van de vijf speerpunten waar volgens de Cyber Security Raad in geïnvesteerd moet worden. Nederland moet immers kunnen vertrouwen op de veiligheid daarvan. Agentschap Telecom bracht eerder dit jaar een rapport uit over de energietransitie en het cruciale belang daarin van het mee ontwikkelen van de digitale infrastructuur. Zo kan bijvoorbeeld alleen een slim elektriciteitsnet vraag en aanbod van duurzaam opgewekte elektriciteit goed afstemmen. En daarbij is cybersecurity weer een randvoorwaarde, want met verdergaande digitalisering wordt ook het aanvalsoppervlak voor kwaadwillenden vergroot. Angeline van Dijk, directeur-hoofdinspecteur van Agentschap Telecom wil daarom samen optrekken met netbeheerders, leveranciers van apparatuur en energie en overheden.

The resilience of vital processes is one of the five key priority areas in which the Cyber Security Council feels investments are in order. The Netherlands, after all, must be able to rely on the security of those processes. Earlier this year, Radiocommunications Agency Netherlands published a report on the energy transition and the vital importance of ensuring that development of the country's digital infrastructure keeps pace with that transition. Only then will it be possible for a smart power grid to effectively coordinate the supply of and demand for renewable energy. Here, too, cybersecurity is a precondition for success, as increasing digitalisation also enlarges the potential target for attacks by malicious parties. Chief Inspector-Director of Radiocommunications Agency Netherlands Angeline van Dijk therefore wishes to coordinate joint action with grid operators, suppliers of devices and energy and government bodies.

‘A RAPIDLY DIGITALISING SOCIETY MAKES CYBERSECURITY A TOP PRIORITY’

Radiocommunications Agency Netherlands is working toward a securely connected Netherlands that can depend on reliable telecommunications and IT networks. This entails monitoring and oversight with regard to the coverage of mobile operators, the security of digital infrastructure, the safe completion of excavation work, the utilisation of frequency in shipping and aviation, the roll-out of 5G and many other matters related to digital resilience and cybersecurity. Van Dijk: ‘We possess unique knowledge in this area. After two years in charge of the Agency, my employees still impress me on a regular basis. And this expertise is no luxury. More and more, the Netherlands is becoming a digital mainport – a role that requires a strong foundation. As the guardians of the ecosystem of digital infrastructure, devices and service, we are that foundation.’

Supervision also includes identification, reporting and placement on the agenda

Our entire society is digitalising.

Photo: Agentschap Telecom

Agentschap Telecom (AT) werkt aan een veilig verbonden Nederland, dat kan rekenen op betrouwbare telecommunicatie- en IT-netwerken. Het houdt onder meer toezicht op de dekking van mobiele operators, de veiligheid van digitale infrastructuur, het veilige verloop van graafwerkzaamheden, het frequentiegebruik in de scheep- en luchtvaart, het uitrollen van 5G en vele andere zaken op het gebied van digitale weerbaarheid en cybersecurity. Van Dijk: “De kennis die we in huis hebben is uniek. Na twee jaar aan het hoofd van Radiocommunications Agency Netherlands sees that society's dependence on various forms of digitalisation is extensive and growing, as is the interconnectedness of those forms, accompanied by an increase in threats and disruptions, both real and potential. Van Dijk: ‘This certainly applies to one of the most drastic changes affecting the Netherlands now and in the coming years, the energy transition. This year, based on our broad mandate, we have issued a report concerning what is needed to achieve this transition in a safe and responsible way. As a supervisory body, we do more than just review an event after the fact to see whether things were done correctly or not. We also have a duty to identify and report issues and ensure they are placed on the agenda in good time. To that end, we conduct research into the application and impact on the electrical-power chain and the risks of electric devices that are connected to both the power grid and the internet (such as charging stations, heat pumps, solar-power systems or home batteries). Through participation in national and international regulatory bodies, we work to achieve standardisation of digitally secure devices and services. We are additionally intensifying our research into potentially disruptive devices and, if necessary, will ensure such devices are withdrawn from the market. In this way, we are embracing our own responsibility as a supervisory authority with regard to the energy transition.’

Digital blueprint

Radiocommunications Agency Netherlands is concerned about the decentralised approach to the energy transition in the Netherlands. Regional plans of action are not always effectively aligned to one another and there seems to be a lack of guidance and oversight. Van Dijk: ‘Like the Dutch Cyber Security Council, we are in favour of an integral approach to identified risks. New and existing issues call for integral coordination and cooperation with parties within the government and

het Agentschap ben ik nog regelmatig onder de indruk van mijn eigen medewerkers. En die kennis van zaken is geen luxe. Nederland wordt steeds meer een digitale mainport en dat vraagt om een goed fundament. Dat fundament zijn wij, als hoeders van het ecosysteem van digitale infrastructuur, apparaten en diensten."

Toezicht is ook signaleren en agenderen
De gehele samenleving digitaliseert. AT ziet een toenemende en diepgaande maatschappelijke afhankelijkheid en verknoping van verschillende vormen van digitalisering en tegelijkertijd een toename van dreigingen en (potentiële) verstoringen. Van Dijk: "Dat geldt zeker ook voor een van de grootste omwentelingen die Nederland nu en in de komende jaren doormaakt, de energietransitie. Vanuit onze brede verantwoordelijkheid hebben wij dit jaar ons rapport uitgebracht over wat ervoor nodig is om die transitie op een veilige en verantwoorde manier te maken. Als toezichthouder kijken wij niet alleen achteraf of iets goed of fout is gegaan, het is juist ook onze taak om zaken bijtijds te signaleren en agenderen. Daarom doen we onder andere onderzoek naar de toepassing en impact op de elektriciteitsketen en de risico's van elektrische apparatuur, die zowel aan het elektriciteitsnet als het internet gekoppeld is (zoals laadpalen, warmtepompen, zonne-energiesystemen of thuis-accu's). Vanuit nationale en internationale gremia werken we aan de standaardisatie van cyberveilige apparatuur en diensten. Bovendien intensiveren we ons onderzoek naar mogelijk verstorende apparatuur. Indien nodig halen we die van de markt. Zo pakken we als toezichthouder onze eigen verantwoordelijkheid in de energietransitie."

Digitale grondplaat
Het AT is bezorgd over de decentrale aanpak van de energietransitie in Nederland. Regionale plannen sluiten niet altijd goed op elkaar aan en er lijkt een gebrek aan sturing en overzicht. Van Dijk: "Net als de Cyber Security Raad zijn we voor een integrale benadering van geïdentificeerde risico's. Nieuwe en bestaande vraagstukken vragen om integrale afstemming en samenwerking met partijen binnen de overheid en het bedrijfsleven, zowel nationaal als internationaal. Daarvoor is het opstellen van een digitale grondplaat, waarmee de totale *governance* van het digitale stelsel van beleid, uitvoering en toezicht in kaart wordt gebracht, behulpzaam. Daarmee worden verantwoordelijkheden, afhankelijkheden en eventuele hiaten zichtbaar."

"Wij zien een toenemende en diepgaande maatschappelijke afhankelijkheid en verknoping van verschillende vormen van digitalisering en tegelijkertijd een toename van dreigingen en (potentiële) verstoringen."

'We see that society's dependence on various forms of digitalisation is extensive and growing, as is the interconnectedness of those forms, accompanied by an increase in threats and disruptions, both real and potential.'

the business community, at both the national and international level. To that end, it would be useful to establish a digital blueprint in order to set out the entire governance of the digital system of policy, implementation and supervision. This will render responsibilities, dependencies and any gaps visible as well.'

Energy transition and cyber risks
Van Dijk: 'The energy transition shares many aspects with our own work field, with regard to physical infrastructure, the continuity and integrity of critical infrastructures and secure devices and services. From radio and other devices to excavation, and from quantifying usage (metrology) to supervision of companies such as energy suppliers. As Digital Infrastructure Authority, we are an important player in the digital ecosystem that we now see taking shape. We are working to restructure ourselves to reflect that ecosystem – so that we are optimally aligned, responsive to developments and in contact with the right parties. Because new risks and vulnerabilities are emerging. New and innovative parties such as 'flexibility operators', 'aggregators' and 'changepoint operators' are arriving on the scene, while increasing digitalisation in the energy sector is resulting in greater cyber risks. It is possible to overload the energy grid by simultaneously switching huge numbers of hacked devices on or off. This could ultimately lead to a complete shutdown. The use of Artificial Intelligence (AI) for purposes such as managing and monitoring the energy balance on the grid yields both opportunities and risks as well.

Solar panels and charging points
The energy transition and other areas in which digitalisation is increasing can be accompanied by risks that might never occur to the average consumer. Van Dijk: 'Take, for instance, the problem of interference. Solar panels – but also numerous other appliances we use every day – can transmit interference signals. This may negatively impact even critical communication systems. A bizarre example – yet one from which we can learn a great deal – is the Waalhaven harbour in Rotterdam, where ships were "disappearing" from the radar. The culprit was revealed to be interference signals from an art installation with a large quantity of LED lights, located at the mouth of the harbour.'

Another example is measuring and registering energy consumption. That might involve smart energy meters, charging an electric vehicle at a charging point, or measuring how much hydrogen is being used. The measurement and registration of that energy consumption must be every bit as safe and reliable as at a traditional petrol-station pump.' Van Dijk: 'That is why we are currently in talks with parties such as the National Platform for the Charging-station infrastructure (NAL). And there are many other new dossiers in which we are being – and want to be – involved.'

The air and ground are filling up
In connection with the energy transition, new cables and pipes must be installed underground. This is necessary in order to expand the scope and capacity of power grids, or to create new district heat or hydrogen grids. Yet careless excavation may result in damage to the cables and pipelines that are already in the ground. Van Dijk: 'I needed some time to get used to the idea myself, but our airspace is becoming quite crowded with all these signals and waves. Just like the ground is filling up with cables. I'm concerned that in recent years, the excavation industry has not yet been sufficiently successful in reducing the incidence of digging-related damage.'

CE marking
As the transition to renewable energy progresses, the vulnerabilities will grow. Today, for instance, there are already one million households that generate their own energy using solar panels. In coming years, this number is expected to increase to around two million. Van Dijk: 'Currently, businesses are happy

Energietransitie en cyberrisico's
Van Dijk: "De energietransitie heeft veel raakvlakken met ons werk, op gebied van fysieke infrastructuur, continuïteit en integriteit van vitale infrastructuren en veilige apparaten en diensten. Van (radio-)apparatuur, tot graven, van meten van verbruik (metrologie) tot toezicht op bijvoorbeeld energiebedrijven. Als autoriteit van de digitale infrastructuur zijn we een belangrijke speler in het digitale ecosysteem dat we zien ontstaan. Wij zijn ermee bezig om ons daarnaar te herstructureren: te zorgen dat we maximaal aansluiten, meebewegen en bij de juiste partijen aanschuiven. Want er ontstaan nieuwe risico's en kwetsbaarheden. Nieuwe innovatieve partijen als 'flexibility operators', 'aggregators' of 'changepoint operators' doen hun intrede. En door de toenemende digitalisering in de energiesector nemen de cyberrisico's toe. Door gehackte apparatuur massaal en gelijktijdig in- of uit te schakelen kan overbelasting op het energienet gecreëerd worden. Dat kan uiteindelijk leiden tot uitval. Ook het gebruik van kunstmatige intelligentie (AI), bijvoorbeeld voor het aansturen en bewaken van de energiebalans op het net geeft zowel kansen, als risico's.

Zonnepanelen en laadpalen
Er spelen in de energietransitie en andere terreinen waarop digitalisering toeneemt, risico's waar de gemiddelde consument nooit aan zou denken. Van Dijk: "Neem bijvoorbeeld het probleem van interferentie. Zonnepanelen, maar ook tal van andere apparaten die we dagelijks gebruiken, kunnen stoorsignalen uitzenden. Daar kunnen zelfs vitale communicatiesystemen hinder van ondervinden. Een bizar, maar vooral ook leerzaam, voorbeeld is de Rotterdamse Waalhaven waar schepen van de radar verdwenen. Dat bleek te komen door stoorsignalen van een kunstinstallatie met veel led-licht aan de havenmonding."

Een ander voorbeeld is het meten en registreren van energiegebruik. Denk aan slimme energiemeters, het opladen van een elektrische auto aan een laadpaal, of het meten van het gebruik van waterstof. Het meten en registreren van dat energieverbruik moet net zo veilig en betrouwbaar zijn als bij het traditionele 'tanken aan de pomp'. Van Dijk: "Daarom zitten we nu bijvoorbeeld aan tafel bij partijen als het Nationaal Platform voor de Laadpaal-infrastructuur (NAL). En zo zijn er veel meer nieuwe dossiers waar we bij betrokken worden en willen zijn. "

De lucht en de grond raken vol
In verband met de energietransitie moeten er nieuwe kabels en leidingen onder de grond gelegd worden. Dat is nodig om elektriciteits-netten uit te breiden of te verzwaren, of voor de aanleg van warmte- of waterstofnetten. Maar onzorgvuldig graven kan leiden tot schade aan kabels en leidingen die al in de grond liggen. Van Dijk: "Ik moest zelf ook even aan het idee wennen, maar de lucht begint aardig vol te raken met al die signalen en golven. Net als de grond met kabels. Het baart mij zorgen dat de graafsector er de afgelopen jaren nog niet voldoende in geslaagd is graafschade te verminderen."

CE-markering
Naarmate de overgang naar duurzame energie vordert, worden de kwetsbaarheden groter. Zo zijn er nu al een miljoen huishoudens die zelf stroom opwekken via zonnepanelen. De komende jaren zal dat groeien naar zo'n twee miljoen. Van Dijk: "Nu zijn bedrijven vaak allang blij als hun nieuwe toepassingen voor de energietransitie überhaupt werken en aansluiten op de rest van het stroomnetwerk. Maar dan leggen ze de finish echt te vroeg. Ze moeten de risico's die al die nieuwe koppelingen en toepassingen met zich meebrengen in kaart hebben en zorgen voor een

"Door de toenemende digitalisering in de energiesector nemen de cyberrisico's toe."

'Increasing digitalisation in the energy sector is resulting in greater cyber risks.'

Photo: Hollandse Hoogte

enough if their new energy-transition applications work at all and can be connected to the rest of the power grid. But that means they are drawing the finish line too early in the race. They need to clearly identify the risks associated with all those new connections and applications and ensure they are sufficiently resilient. The familiar CE marking, which we are partly responsible for monitoring, used to be mainly concerned with whether a device was safe and would not cause disruptions. While that's still important, there is also growing attention for cybersecurity. For this reason, the EU has now added cybersecurity requirements to the list of standards devices must meet. This is an important step and one that is in keeping with the Digitally Secure Hardware and Software Roadmap that the Dutch Ministry of Economic Affairs and Climate Policy is developing in cooperation with Radiocommunications Agency Netherlands.

Industrial Automation & Control Systems (IACS)

When most people think of digital resilience and achieving a secure digital infrastructure, Information technology (IT) is the first thing that comes to mind. Attention for OT (Operational Technology in the business sector) is then a distant second. The CSR has proposed implementing sector-specific IACS control frameworks. This is familiar territory for Radiocommunications Agency Netherlands. Van Dijk: ‘Based on the legal framework of the Telecommunications Act and the Network and Information Systems Security Act, we apply an open standard for telecom providers, grid operators and energy companies. In cooperation with the excavation industry, we have also developed the CROW500 guideline to prevent digging-related damage to pipelines and cables. For parties such as refineries and energy suppliers, we apply a harmonised set of norms and standards in order to provide structure to the open-standard supervision. While in principle, the businesses themselves are responsible for their own risk management, our chosen approach is based on the sharing of knowledge and experience. This is why – together with the CSR and the NCSC – we organised a series of webinars on IACS, in which we addressed topics such as ISO/IEC 62443, a set of standards commonly used in the energy sector.’

New tasks: NCCA and AI

As a Digital Infrastructure Authority, the Dutch Radiocommunications Agency will remain fully dedicated to enhancing the availability, resilience and security of technical infrastructures and trust in the use and security of services and devices in the coming period. One of the Radiocommunications Agency's new tasks concerns the implementation of the European Cybersecurity Act (CSA). Van Dijk: ‘We will be assigned the role of National Cybersecurity Certification Authority (NCCA). CSA certification is currently voluntary, but will likely become mandatory at some point. By issuing certificates, we will be enhancing consumers’ peace of mind regarding the cybersecurity of the products, services and processes they use. There are also legislative changes in store, such as the new version of the Networks & Information Systems (NIS) Directive and the development of a specific Netcode on Cybersecurity. This netcode will include legislation pertaining specifically to parties who play a major role in the power grid such as grid operators and potentially, in future, other parties who have large quantities of power at their immediate disposal as well.’

‘In addition, the European Commission recently announced that every member country must have a clear point of contact for artificial intelligence. These are important societal developments that will move the Netherlands forward and increase its digital security. We at the Radiocommunications Agency are pleased to contribute to those efforts.’

“Als autoriteit in de digitale infrastructuur gaan we volop inzetten op de beschikbaarheid, weerbaarheid en veiligheid van technische infrastructuren.”

‘As Digital Infrastructure Authority, we are fully dedicated to enhancing the availability, resilience and security of technical infrastructures.’

goede weerbaarheid. De bekende CE-markering, die mede onder ons toezicht valt, ging er vroeger vooral om dat je apparaat veilig was en geen storing veroorzaakte. Dat is nog steeds belangrijk, maar daarnaast is er steeds meer oog voor cybersecurity. Vandaar dat de EU nu ook eisen voor cybersecurity heeft toegevoegd aan de eisen waar apparaten aan moeten voldoen. Dat is een belangrijke stap, die goed past in de *Roadmap veilige hard -en software* waarin het ministerie van EZK en Agentschap Telecom samen optrekken.”

Industrial Automation & Control Systems (IACS)

Bij cyberweerbaarheid en het veilig maken van de digitale infrastructuur denkt men in eerste instantie aan IT en blijft aandacht voor OT (operational technology in het bedrijfsleven) achter. De CSR heeft voorgesteld om met sectorale IACS-controleraamwerken te werken. Dit is bekend terrein voor Agentschap Telecom. Van Dijk: “Wij werken vanuit het wettelijk kader van de Telecommunicatiewet en de Wbni met een open norm richting telecomaanbieders, netbeheerders en energiebedrijven. En in samenwerking met de graafsector hebben we de CROW500-richtlijn ontwikkeld voor het voorkomen van graafschade aan leidingen en kabels. Voor bijvoorbeeld raffinaderijen en energieleveranciers werken we met geharmoniseerde standaarden en normen, om vorm te geven aan toezicht met een open norm. Ook al is risicomanagement in principe de verantwoordelijkheid van bedrijven zelf, wij kiezen voor een werkwijze van kennis en ervaring delen. Daarom hebben we bijvoorbeeld samen met de CSR en het NCSC een reeks *webinars* georganiseerd over IACS, waarbij wij onder meer aandacht hebben gegeven aan de ISO/IEC 62443, een norm die binnen de energiesector vaak gebruikt wordt.”

Nieuwe taken: NCCA en AI

In de komende periode blijft Agentschap Telecom als autoriteit in de digitale infrastructuur volop inzetten op de beschikbaarheid, weerbaarheid en veiligheid van technische infrastructuren en het vertrouwen in het gebruik en de veiligheid van diensten en apparaten. Een nieuwe taak daarin wordt de invulling die AT gaat geven aan de Europese Cybersecurity Act (CSA). Van Dijk: “Wij krijgen de rol van Nationale Cybersecurity Certificeringsautoriteit (NCCA). CSA-certificering is nu nog vrijwillig, maar wordt waarschijnlijk verplicht. Met het afgeven van de certificaten gaan wij bijdragen aan zekerheid voor afnemers van producten, diensten en processen dat de cybersecurity is gewaarborgd. Daarnaast zijn er ook veranderingen in wetgeving zoals de nieuwe versie van de Networks & Information Systems richtlijn (NIS) en de ontwikkeling van een specifieke Netcode op Cybersecurity, met specifieke wetgeving voor partijen die een grote rol spelen op het elektriciteitsnet zoals netbeheerders en mogelijk in de toekomst ook andere partijen die grote hoeveelheden vermogen ‘onder de knop’ hebben. Ook heeft de Europese Commissie onlangs uitgesproken dat er in elke lidstaat een duidelijk aanspreekpunt voor artificiële intelligentie zou moeten komen. Dat zijn belangrijke maatschappelijke ontwikkelingen die ons land verder brengen en digitaal veiliger maken. Daar denken wij als Agentschap Telecom graag over mee.”

BACK TO TOP

Perry van der Weyden
Former Chief Information Officer (CIO) at the Directorate-General for Public Works and Water Management (Rijkswaterstaat)

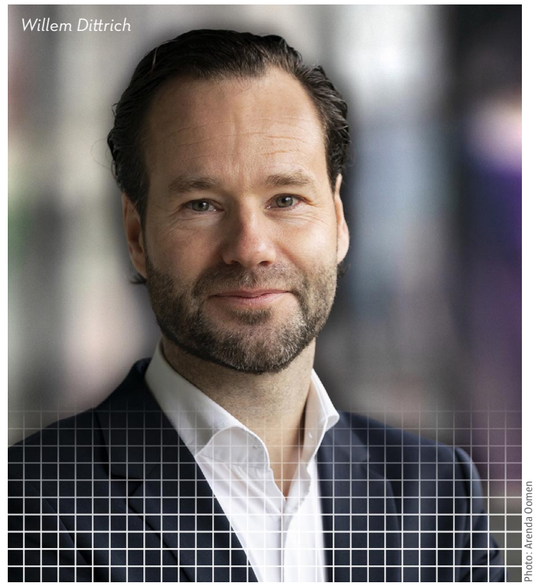
Willem Dittrich
Head of the Rijkswaterstaat Security Centre

WE'LL HAVE TO WORK TOGETHER TO DEFEND OUR DIGITAL DYKES

Perry van der Weyden werkte 7,5 jaar als hoofdingenieur-directeur Centrale Informatievoorziening Chief Information Officer (CIO) bij Rijkswaterstaat. Inmiddels heeft hij een overstap gemaakt naar de IT-dienstverlener Nedcompany, maar hij wilde graag nog ruimte maken voor ons en ingaan op wat de organisatie doet om ons land cyberweerbaar te houden. Ook zijn voormalig collega Willem Dittrich, hoofd van het Security Centre van Rijkswaterstaat, is aangesloten bij dit gesprek. In het gesprek benadrukken beide heren vooral de noodzaak om samen te werken met andere organisaties. ''Nederland beschermen tegen water kunnen we niet alleen. Zodra wij een stormvloedkering dichtdoen en er bij een sluis verderop hackers via het waterschap binnen zijn gekomen, dreigt er nog steeds gevaar.''

Perry van der Weyden spend 7.5 years working as Chief Information Officer (CIO) at the Directorate-General for Public Works and Water Management (Rijkswaterstaat). He has since joined IT service provider Nedcompany, but was keen to make time for us and discuss the organisation's efforts to keep our country cyber resilient. His former colleague Willem Dittrich, head of the Rijkswaterstaat Security Centre, also joined the conversation. Both emphasised the need to cooperate with other organisations. 'We can't protect the Netherlands against flooding on our own. We can close a storm surge barrier, but we'll still be at risk if hackers manage to open a nearby lock by hacking into the water board.'


Perry van der Weyden
Photo: Eric Fecken


Willem Dittrich
Photo: Arenda Oomen

Toen Van der Weyden zevenenhalf jaar geleden begon bij Rijkswaterstaat was IT nog een ondersteunende afdeling binnen de organisatie. Onder zijn leiding is IT geïntegreerd in het primaire proces. Een werkend en veilig IT-systeem is essentieel voor het veilig, leefbaar en bereikbaar houden van Nederland. Rijkswaterstaat is verantwoordelijk voor de infrastructuur die hiervoor zorgt. Denk daarbij onder andere aan het beheren van zogenoemde objecten zoals tunnels, bruggen, sluizen en ook de stormvloedkeringen.

'Wij beheren vitale objecten. Het heeft een maatschappij-ontwrichtende impact op het moment dat deze uitvallen. Bijvoorbeeld de waterkeringen moeten natuurlijk altijd blijven werken.'' Van der Weyden benadrukt dat het beheer van objecten op een integrale manier moet worden aangepakt, want zowel fysieke en digitale veiligheid als een veilige IT- en OT-omgeving zijn onmisbaar voor de algemene veiligheid. Rijkswaterstaat is niet de enige partij die vitale objecten beheert, daarom is samenwerking met de gehele keten zo belangrijk, bijvoorbeeld in het waterdomein. Van de stormvloedkeringen in het westen tot de sluizen en dijken in het oosten, het is een groot aaneengeschakeld netwerk van objecten waar verschillende partners verantwoordelijkheid hebben. Met al die partners zoekt Rijkswaterstaat samenwerking op verschillende gebieden.

"Het is een ratrace waarin kwaadwillenden naar binnen willen en wij hen buiten willen houden. Wij willen die race winnen."

'It's basically a rat race in which the bad guys are trying to get in and we're trying to keep them out. We aim to win that race.'

When Van der Weyden first joined Rijkswaterstaat 7.5 years ago, IT was still an auxiliary department. He oversaw efforts to integrate IT into the organisation's primary process. A functional and secure IT system is crucial in keeping the Netherlands safe, liveable and accessible. Rijkswaterstaat is responsible for the necessary infrastructure. This includes the management of objects such as tunnels, bridges, locks and storm-surge barriers.

'We manage vital objects. Society would be seriously disrupted if they failed. For example, our flood defences obviously need to be up and running at all times.' As Van der Weyden emphasises, we need to take a holistic approach to the management of these crucial objects: our overall security requires physical and digital security as well as a secure IT and OT environment. Rijkswaterstaat isn't the only organisation responsible for managing our vital objects, which makes cooperation with the entire chain – e.g. in the water management domain – crucial. From the storm-surge barriers in the west to the sluices and dykes in the east, our chain partners are responsible for a large, interconnected network of objects. Rijkswaterstaat aims to collaborate on a range of issues with each of these partners.

The organisation is continually working to improve cybersecurity. For example, the organisation controls objects through its own fibre-optic network rather than relying on the public Internet. Rijkswaterstaat independently monitors and secures this network with the help of its own Security Operations Centre (SOC) and network administrators. As Van der Weyden explains, Rijkswaterstaat currently monitors over 34 billion operations a week. This has not led to any major problems in recent years thanks to the organisation's strong focus on cybersecurity. However, Rijkswaterstaat is not losing focus: ''We have an ambitious mindset and operate on the assumption that an attack could happen at any time. That means that we need to

Rijkswaterstaat is zelf altijd bezig met het verbeteren van de cyber-security. Zo maakt het geen gebruik van het publieke internet voor het aansturen van objecten, maar heeft de organisatie hiervoor een eigen glasvezelnetwerk. Dit netwerk monitort en beveiligt de organisatie zelf met het Security Operations Center (SOC) en de netwerkbeheerders. Van der Weyden vertelt dat er inmiddels ruim 34 miljard handelingen per week worden bekeken. Doordat Rijkswaterstaat veel aandacht heeft voor cyberveiligheid, heeft dit in de afgelopen jaren niet tot grote problemen geleid. Toch verslapt de aandacht niet bij Rijkswaterstaat: ‘’We hebben een ambitieuze houding en gaan ervan uit dat een aanval altijd kan gebeuren. Dus moeten wij ervoor zorgen dat we weerbaar zijn als we worden aangevallen. Het is een ratrace waarin kwaadwillenden naar binnen willen en wij hen buiten willen houden. Wij willen die race winnen.’’

Willem Dittrich is als hoofd van het Security Centre van Rijkswaterstaat iedere dag bezig met deze race. Monitoring en detectie is inderdaad een van de drie hoofdtaken.', zegt hij hierover. "Die 34 miljard handelingen per week bevatten bijvoorbeeld virusscanresultaten of spam e-mails. Hieruit destilleert ons systeem wat we verder willen onderzoeken en analyseren. Dat doen we met slimme filters en met de mensen die werken in ons eigen Security Operations Center. Door voortdurend te zorgen dat onze filters up to date blijven, verzwaren we doorlopend de digitale dijken."

Photo: Nationale Beeldbank

Toch kwam uit het rapport *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* uit 2019, van de Algemene Rekenkamer, dat de cybersecurity van verschillende (vitale) waterwerken nog beter konden worden beveiligd tegen cyberaanvallen. De aanbevelingen uit het rapport zijn ter harte genomen en grotendeels geïmplementeerd, maar ook moet een aantal punten nog worden verbeterd. Van der Weyden licht toe dat de verouderde systemen niet per definitie een risico zijn voor de veiligheid doordat de systemen een stuk weerbaarder zijn dan ten tijde van het rapport. Mede dankzij de aanbevelingen uit dit rapport is de cyber-veiligheid van Rijkswaterstaat volgens hem op het juiste niveau, het houdt de organisatie scherp om constant de juiste keuzes te maken en de bijbehorende investeringen op tijd te doen.

Teamwerk

De CIO is trots op zijn zeer vakkundige team dat constant snelle ontwikkelingen doormaakt en doorvoert. Rijkswaterstaat is een van de eerste organisaties binnen de Rijksdienst waar ze professioneel aan de slag zijn gegaan met cyberveiligheid. Dit heeft ervoor gezorgd dat er veel ervaring, vakmanschap en handigheid in huis is. Het geheim om de juiste mensen aan boord te krijgen en houden? ‘’We leiden onze mensen zelf op. De IT-wereld verandert constant, waardoor werkzaamheden van bepaald personeel verdwijnen. Deze mensen kennen de Rijkswaterstaat-omgeving goed, dus we leiden ze op en zorgen dat hun ontwikkeling past bij de ontwikkeling van de organisatie.’’

Een andere reden dat IT’ers graag bij Rijkswaterstaat willen werken, is de relevantie van het werk. Binnen de organisatie zijn mensen 7 dagen per week, 24 uur per dag bezig met het draaiende houden van de Nederlandse infrastructuur. Cybersecurity levert een cruciale bijdrage aan de missie van Rijkswaterstaat: samenwerken aan een veilig, leefbaar en bereikbaar houden van Nederland.

'Het is belangrijk dat we cybersecurity zo vroeg mogelijk onderdeel maken van het ontwerp en van het asset management', vult Dittrich aan. We noemen dit Security by Design, een tweede hoofdtaak van het Security Centre.' Juist in het domein van OT was er behoefte aan een gedeeld kader voor cyberveiligheid. Daarom heeft Rijkswaterstaat samen met de waterschappen én in overleg met de markt de CSIR opgesteld: De Cybersecurity Implementatierichtlijn Objecten - Rijkswaterstaat. Kort geleden verscheen de 3.0 versie van deze CSIR. 'Door met een gezamenlijk kader te werken kun je elkaar ondersteunen in de toepassing. Richting de sector hanteer je ook één lijn en dat creëert overzicht en voorspel-baarheid., aldus Dittrich. 'Het werkt, en het werkt goed.'

Cybersecurity is binnen RWS dermate belangrijk dat dit volledig door eigen mensen wordt vormgegeven. Maar dat betekent niet dat ze niet samenwerken. Met andere cybersecurity-afdelingen binnen de overheid wordt veel kennis gedeeld, terwijl het Nationaal Cyber Security Centrum juist een coördinerende functie heeft. Ook werkt RWS samen met zeer gespecialiseerde bedrijven, die vaak een inhoudelijke analyse maken van (potentiële) problemen. Vervolgens gaan ze intern aan de slag om met deze analyse tot oplossingen te komen.

“Cybersecurity levert een cruciale bijdrage aan de missie van Rijkswaterstaat: samenwerken aan een veilig, leefbaar en bereikbaar houden van Nederland.”

‘Cybersecurity is a crucial part of Rijkswaterstaat's mission: working together to keep the Netherlands safe, liveable and accessible.’

make sure we're prepared in the event that we are attacked. It's basically a rat race in which the bad guys are trying to get in and we're trying to keep them out. We aim to win that race.’

As head of Rijkswaterstaat's Security Centre, Willem Dittrich takes part in that rat race on a daily basis. ‘Monitoring and detection is one of our three core tasks,' he explains. ‘For example, those 34 billion weekly operations might include virus scan results or spam emails. Our system sifts through that information to determine what we want to investigate and analyse in more detail. We do that with the help of smart filters and the staff at our own Security Operations Centre. We're constantly reinforcing our digital dykes by making sure our filters are up to date.’

Despite these efforts, the 2019 *Reinforcing our Digital Dykes: Cybersecurity and Vital Water Works* report by the Netherlands Court of Audit found there was still room to improve the cybersecurity of various critical and non-essential water works. While the report's recommendations have been taken to heart and largely implemented, a few points will still require improvement. As Van der Weyden explains, the obsolete systems are currently far more resilient than they were at the time of the report and do not necessarily pose a security risk. 'Rijkswaterstaat's cybersecurity is currently in good shape, partly thanks to the report's recommendations; the organisation is now aware that it must consistently make the right choices and make the necessary investments on time.'

Teamwork

The CIO is proud of his highly skilled team, which is constantly evolving and rapidly responding to new developments. Rijkswaterstaat is one of the first civil service organisations to have taken a professional approach to cybersecurity. As a result, it has a great deal of in-house experience, skill and know-how. So what is the secret to attracting and retaining the right people? ‘We train our staff in-house. The world of IT is constantly changing, which means certain types of personnel are losing their jobs. These people are thoroughly familiar with the Rijkswaterstaat environment, so we train them and make sure that their development aligns with the organisation's evolution.’

IT professionals are also keen to join Rijkswaterstaat because the work we do is so relevant. Our staff work 7 days a week, 24 hours a day to keep the Netherlands' national infrastructure up and running. Cybersecurity is a crucial part of Rijkswaterstaat's mission: working together to keep the Netherlands safe, liveable and accessible.

‘Cybersecurity should be integrated into the architecture and asset management processes at the earliest possible stage,’ Dittrich adds. ‘That's referred to as Security by Design, the Security Centre's second core task.' The OT domain really needed a common cybersecurity framework. Rijkswaterstaat responded by drafting the Cybersecurity Implementation Guideline (CSIR) in collaboration with the water boards and market parties: The Cybersecurity Implementation Guideline for Objects – Directorate-General for Public Works and Water Management. The 3.0 version of this CSIR was recently introduced. 'Working within a common framework allows you to support each other during the implementation phase. It also allows you to be more consistent in respect of the industry, which makes everything more transparent and predictable,' Dittrich explains. 'It works, and it works well at that.'

Cybersecurity is such an important aspect of Rijkswaterstaat's operations that the organisation does it all in-house. Still, that does not mean they are not seeking out collaborations. Rijkswaterstaat shares a great deal of knowledge with other government cybersecurity departments, while the National Cyber Security Centre plays a coordinating role. Rijkswaterstaat also collaborates with highly specialised companies

Er wordt ook intensief samengewerkt met de SOC's van andere uitvoeringsorganisaties. 'In wat we het Joint SOC noemen, zorgen we ervoor dat specialisten van verschillende uitvoeringsorganisaties kennis, kunde en ervaringen met elkaar delen.' Ook is begin 2020 het Nationaal Response Netwerk (NRN) ingericht. Dit netwerk vormt RWS samen met de Informatiebeveiligingsdienst van de Nederlandse gemeenten (IBD), de Belastingdienst, de ICT-coöperatie van onderwijs en onderzoek SURF, het Ministerie van Defensie, Rijkswaterstaat en het Nationaal Cyber Security Centrum. Deze partijen hebben in een convenant vastgelegd dat ze waar mogelijk schaarse, specialistische capaciteiten delen op de momenten dat één of meerdere deelnemers dit nodig hebben. Dittrich is blij met het NRN en hoe dit functioneert. 'Incident response is cruciaal in de security-operatie. Doordat er een NRN is kunnen we een beroep doen op elkaars inzet op het moment dat we dat nodig hebben.' Om goed voorbereid te zijn op deze samenwerking wordt er gezamenlijk geoefend en kennis uitgewisseld. 'The profit is in the proces', aldus Dittrich. 'We leren zoveel van onze gezamenlijke activiteiten. Alleen dat al maakt het meer dan de moeite waard.'

Water houdt zich niet aan grenzen

De recente overstromingen in Limburg, België en Duitsland hebben weer eens bewezen dat water zich niets aantrekt van landgrenzen. Water-beheer vraagt dus ook om internationale samenwerking. Rijkswaterstaat deelt al informatie en kennis met andere landen, maar de ambities gaan verder. In een Digital Europa Programme zou deze samenwerking nog meer gestalte krijgen, maar ook in I-STORM werkt RWS samen op het gebied van stormvloedkeringen.

Wat de overstromingen ook duidelijk maakten, is dat je achter een computer het water niet kan laten verdampen. Uiteindelijk staat alle techniek die Rijkswaterstaat beheert ten dienste van een veilig, leefbaar en bereikbaar Nederland. Ook op spannende momenten moet de techniek het doen. In de voorbereiding op uitval hanteert Rijkswaterstaat een *all hazard* benadering, of het nu gaat om uitval van elektriciteit of van het glasvezelnetwerk: er is altijd een back-up plan beschikbaar voor de bediening.

Van der Weyden realiseert zich maar al te goed dat niemand alleen staat binnen het waterbeheer. Als Waterschap niet, maar ook als Rijkswaterstaat niet. ‘’De hele keten is zo sterk als de zwakste schakel, dus het is aan ons om, samen met onze partners deze hele keten nog beter te beveiligen. We zijn hier al mee bezig en ook de bewustwording wordt steeds groter. Maar deze uitdaging blijft relevant voor de komende jaren.’’

BACK TO TOP

“We leren zoveel van onze gezamenlijke activiteiten. Alleen dat al maakt het meer dan de moeite waard.”

‘We're learning so much from our joint activities. That alone is making this all worthwile.’

that often conduct substantive analyses of existing and potential risks. The organisation then applies these analyses to develop the necessary solutions in-house.

We also work closely with the SOCs at other executive agencies. ‘The joint SOC, as we call it, offers a platform for specialists from various executive agencies to share their knowledge, expertise and experience. We also set up the National Response Network (NRN) in early 2020. The network is made up of the Dutch municipalities' Information Security Service (IBD), the Dutch Tax and Customs Administration, SURF (the ICT cooperative for education and research), the Dutch Ministry of Defence, Rijkswaterstaat and the National Cyber Security Centre. All the participating organisations have signed a covenant agreeing to share their scarce specialist resources whenever one or more of the other members need support. Dittrich welcomes the NRN and appreciates the way it functions. 'Incident response is a crucial part of any security operation. Thanks to the NRN, we can now ask each other for help when we need it. The participants are organising joint exercises and knowledge exchanges in preparation for the collaboration. 'The profit is in the process', as Dittrich puts it. 'We're learning so much from our joint activities. That alone is making this all worthwhile.'

Water does not respect borders

As the recent floods in Limburg, Belgium and Germany proved yet again, water does not respect national borders. Accordingly, effective water management also requires international cooperation. Rijkswaterstaat is already sharing information and knowledge with other countries, but our ambitions do not stop there. While the partnership will eventually culminate in a Digital Europe Programme, Rijkswaterstaat is already collaborating on storm-surge barriers as part of the ISTORM programme.

As the floods also demonstrated, you can't make water evaporate from behind a computer screen.

Photo: Nationale Beeldbank

Ultimately, all the technology Rijkswaterstaat manages is there to ensure that the Netherlands remains safe, liveable and accessible. That technology also has to work at critical moments. As a part of our preparations for outages – ranging from electricity outages to fibre-optic network failures – Rijkswaterstaat has adopted an all-hazards approach: we always have a back-up plan in place to ensure operational continuity.

As Van der Weyden knows only too well, there are no solitary actors in water management. That applies to both the water boards and Rijkswaterstaat. ‘The entire chain is only as strong as its weakest link, so it's up to us and our partners to make everything more secure. We're already working on that, and there's certainly a growing awareness of the issue. Still, it will remain a significant challenge in the years to come.’

Marleen Stikker
Co-founder Waag, a Future Lab for technology and society

‘CRITICAL TECHNOLOGICAL KNOW-HOW IS CRUCIAL’

Waag is een toekomstlab voor technologie en samenleving. Het verkent de sociale en culturele impact van nieuwe technologieën vanuit de waarden *open, fair & inclusive*. Marleen Stikker was in 1994 een van de twee oprichters van Waag. In hetzelfde jaar stond ze aan de wieg van De Digitale Stad, het eerste sociale mediaplatform in Europa, dat mede vormgaf aan het internet in Nederland.

Waag is a Future Lab for technology and society. It explores the social and cultural impacts of new technologies from a perspective based on the values of openness, fairness & inclusiveness. *Back in 1994, Marleen Stikker was one of the two founders of Waag. In that same year she also witnessed the birth of De Digitale Stad (the Digital City), the first social media platform in Europe, which helped shape the Internet in the Netherlands.*

Photo: Arenda Oomen

Stikker spreekt expliciet over het internet en niet over cyberspace: “Ik vind het merkwaardig dat cyber als een eigen domein wordt behandeld. Het lijkt te duiden op een aparte ruimte, die los staat van de fysieke ruimte. Dat was in het begin van de jaren negentig wellicht het geval, maar nu zijn alle maatschappelijke en fysieke processen verweven met digitalisering. De technologie achter deze digitalisering wordt ontwikkeld door organisaties en is niet neutraal. De kern van de vraag is: wie heeft de technologie in handen? Diegene heeft een machtspositie over anderen. Het rare is dat velen denken dat technologie ons overkomt, maar het begint met mensen die technologie maken. We moeten onszelf vragen blijven stellen: hebben we nog strategische autonomie over onze infrastructuur, hebben we nog zelfbeschikking over ons eigen leven?”

Digitale autonomie
De opvatting van Stikker is dat we als samenleving te lang technologie over ons heen hebben laten komen. Stikker: “Daardoor staat onze kritieke infrastructuur op het spel. We hebben de vrije markt vrij spel gegeven en hebben onze samenleving overgeleverd aan extractieve verdienmodellen van een steeds kleiner aantal grote spelers. Privatisering maar ook digitalisering van onder andere onze water-, voedsel-, energievoorziening, maar ook van de telecom zorgen ervoor dat we geen zicht hebben op het eigenaarschap van en geen soevereiniteit hebben over de kritieke infrastructuur.”

Dat is volgens Stikker het geopolitieke aspect van onze digitale autonomie. “Maar het treft in essentie alle lagen van de samenleving. Van grote kritieke infrastructuur, tot mkb’ers en

Stikker prefers to use the term ‘Internet’ rather than cyberspace. ‘I think it's strange for cyber to be treated as a domain in its own right. The term seems to denote a separate space, detached from physical space. While that may have been the case in the early 1990s, today all societal and physical processes have become strongly interwoven with digitalisation. The technology behind this digitalisation is developed by organisations and is not neutral. They key question is this: who is in charge of the technology? That party has power over others. The funny thing is that while many people feel that technology is something that happens to them, in reality it is people who make the technology. We need to keep asking ourselves questions like: what's the state of our strategic autonomy over our infrastructure? Are we still free to decide about our own lives?’

Digital autonomy
According to Stikker, as a society we have allowed technology to ‘happen to us’ for too long. ‘As a result, our critical infrastructure is now at stake. We have given free rein to market forces and surrendered our society to the extractive earning models of an ever shrinking number of big players. The privatisation, and digitalisation, of our water, food and energy supply, and of telecommunication services, have created a situation in which we have lost sovereignty over critical infrastructure and don't even know who owns it.’

That, according to Stikker, is the geopolitical aspect of our digital economy. ‘But it essentially affects all layers of society, from large-scale critical infrastructure to small and medium-sized businesses and the self-employed. These are becoming ever more dependent on platforms, can no longer set their own prices and service levels, and sometimes don't even know their own customers any more. Digital autonomy is a “nested problem”, it occurs both in large-scale and small-scale contexts. At the individual level, it's about the question of whether we have any self-determination left or if digital systems decide about our future.’

What makes the current approach to cybersecurity problematic, according to Stikker, is its emphasis on preserving the existing economic balance of power. ‘This also applies to the Dutch Cyber Security Council's advisory reports. They fail to address the fundamental issue: the extent of our dependence on the suppliers of those systems. Politicians are so committed to an open economy and a free market

Photo: Nationale Beeldbank

that they have ignored the necessary guarantees and limitations. In this way we have given up a significant part of our public control function. The contradiction is false. I agree we need an open economy, but one in which openness means open technology and data commons to fight monopolisation. This calls for a government that does not govern the country as a business, but one that has anchored its policies to public values.'

Let's not leave technology to the experts

Stikker has been warning for years about the power of tech companies, and urges administrators to be critical. Stikker: 'It's easy to dismiss critical attitudes towards technology. However, a critical attitude doesn't mean you are necessarily against something, but rather that you want to make progress under certain conditions. This calls for an analytical approach, and a thorough understanding of the underlying principles. Administrators should ask themselves which forms of technological innovation they are and are not prepared to accept. This means they need to have a good grasp of the issue: what purpose does this optimisation serve, and how can I justify it? Is my understanding of the issue sufficient? Who is designing this technology, who determines what we are going to use it for and who owns and controls it when it's there? This problem we are facing concerns society as a whole; it's not simply a science or engineering issue, because technology doesn't always offer a one-to-one solution to a societal problem.'

According to Stikker, it is crucial for administrators to understand that technology is not neutral. 'This insight is essential if you want to protect the strategic autonomy of the Netherlands also in this field; you shouldn't simply rely on your experts and advisers. Critical technological know-how should be a condition for anyone in an administrative position.'

zelfstandigen. Deze worden steeds meer afhankelijk van platforms, kunnen hun eigen prijzen en dienstverlening niet meer bepalen en kennen soms hun eigen klanten niet eens meer. Digitale autonomie is een *nested problem*, het doet zich in het groot en in het klein voor. Op het niveau van het individu gaat het om de vraag of we nog zelfbeschikking hebben of dat digitale systemen onze toekomst bepalen."

Het lastige van de huidige cybersecurity-benadering vindt Stikker de nadruk die wordt gelegd op het behoud van het economische krachtenveld. "Dit geldt ook voor de adviesrapporten van de Cyber Security Raad. De fundamentele vraag wordt niet geadresseerd: de mate waarin we afhankelijk zijn van de leveranciers van systemen. De politiek hecht zoveel waarde aan een open economie en vrije markt, dat noodzakelijke waarborgen en begrenzing achterwege zijn gelaten. We hebben zo veel van onze publieke controle uit handen gegeven. Het is een schijntegenstelling. Ik ben ook voorstander van een open economie, maar dan een waarbij openheid betekent dat we te maken hebben met open technologie en datacommons, waarin monopolievorming wordt tegengegaan. Dat vraagt om een overheid die het land niet bestuurt als de BV Nederland, maar een die haar beleid verankert in publieke waarden."

Technologie niet overlaten aan experts

Stikker waarschuwt al jaren over de macht van techbedrijven. Ze pleit voor een kritische houding van bestuurders. Stikker: "Het is makkelijk om kritische geluiden ten aanzien van technologie te diskwalificeren. Een kritische houding betekent niet dat je per se tegen iets bent, het betekent dat onder bepaalde voorwaarden vooruit wil. Dit vereist analyses en het kunnen doorgronden van de achterliggende principes. Bestuurders moeten bij zichzelf nagaan op welke manier ze technologische innovatie wel en niet willen inzetten. Dat vraagt om een dieper begrip van bestuurders: 'Waar optimaliseer ik voor en hoe legitimeer ik dat. Heb ik voldoende begrip van de materie? Wie ontwerpt de technologie, wie definieert waar we het voor gebruiken en wie heeft er vervolgens eigenaarschap over?' Het is een maatschappelijk probleem waar we voor staan, het is niet enkel een bèta of engineering onderwerp want echnologie is niet altijd een-op-een een oplossing voor maatschappelijke problemen."

Het is volgens Stikker cruciaal dat bestuurders begrijpen dat technologie niet neutraal is. "Als je de strategische autonomie van Nederland ook op dit vlak wil bewaken, dan kan je hier niet aan ontkomen en enkel vertrouwen op je experts en adviseurs. Kritische technologische kennis hoort voorwaardelijk te zijn om bestuurder te zijn."

Urgentie omzetten in daadkracht

Zowel Nederland als de EU zijn op dit moment afhankelijk van slechts een paar techreuzen. Stikker ziet alternatieven voor de middellange en lange termijn, maar daar zijn wel keuzes voor nodig: "De macht van deze bedrijven is ongekend en ongewenst. Een bedrijf als Amazon zit niet alleen in retail, maar ook in de farmaceutische industrie, het verzekeringswezen en dataopslag. Waarom heeft het zo lang geduurd om mededingingsregels te handhaven? Een deel van de strijd moet geleverd worden in de VS met de *break up big tech* beweging, waarbij voorkomen moet worden dat bedrijven in verschillende branches tegelijk actief kunnen zijn."

"Bij een open economie hoort een integrale visie op digitale autonomie en zelfbeschikking."

'An open economy requires an integrated vision on digital autonomy and self-determination.'

Converting a sense of urgency into effective action

Currently the Netherlands, and the EU as a whole, depend on a mere handful of technology giants. Stikker believes that alternatives are available in the medium and long term, but only if we make the necessary choices: 'The power that these companies have is unprecedented and undesirable. Amazon, for instance, isn't just a retail business, but has also spread into the pharmaceutical sector, the insurance sector and data storage. Why did it take such a long time to enforce the competition rules? Part of the battle needs to be fought on US soil, with the "break up big tech movement", to prevent companies from operating in various branches at the same time.'

But Europe and the Netherlands also have a role to play, Stikker points out. 'A lot of legislation is being drafted; think of the Digital Market Act, the Digital Services Act, the AI Act and of course the General Data Protection Regulation (GDPR). However, enforcement, which is crucial, is lacking. While we are consuming enormous volumes of digital services every day, the regulatory supervision of those services is only a fraction of the supervision of foodstuffs, for example. That's embarrassing.

One other solution is for us to create alternatives ourselves. For that to be a success, you need innovation, energy and manufacturing power. There is room for such an approach, the need is obvious. We should formulate principles that help us reintroduce public values in the digital domain – principles such as encryption by design, privacy by design, open source and interoperability. We also need different forms of ownership and different earning models, combining open source with a healthy ecosystem of various companies that supply those services. This will help us get rid of the vendor lock-in. As long as the government does not adopt this as its point of departure, sovereignty and digital autonomy will remain very distant objectives.'

“Open economie versus digitale autonomie is een schijntegenstelling.”

‘Open economy versus digital autonomy is a false contradiction.’

Maar ook Europa en Nederland hebben volgens Stikker een rol te spelen. “Er is al veel wetgeving in de maak, de digital market act, de digital services act, de AI act en natuurlijk de General Data Protection Regulation (GDPR). Maar de handhaving hiervan ontbreekt terwijl dit cruciaal is. We consumeren dagelijks enorme hoeveelheden digitale diensten, maar moeten het doen met een fractie van de toezichthouding die we bijvoorbeeld op levensmiddelen hebben. Dat is gênant.”

“Een andere oplossing is dat we zelf de alternatieven gaan maken. Maar dat vraagt wel weer om innovatie, energie en maakkracht. De ruimte is er, er is behoefte aan. We moeten principes opstellen die publieke waarden terugbrengen in het digitale domein. Principes als encryption by design, privacy by design, open source en interoperabiliteit. We moeten toe naar andere vormen van eigenaarschap en verdienmodellen, waarbij open source gecombineerd wordt met een gezond ecosysteem, van verschillende bedrijven, dat deze diensten levert. Zodat we ook af kunnen van vendor lock-in. Zolang de overheid dat niet als uitgangspunt neemt, zijn soevereiniteit en digitale autonomie nog heel ver weg.”

Stikker stelt dat er behoefte is aan systemische veranderingen in juridische bepalingen, in aanbestedingen, in interne kaders en in de principes die ten grondslag liggen aan keuzes die we maken. “Dit waarborgt dat de investeringen van honderden miljoenen in startups en nieuwe technologieën onze digitale autonomie aantasten, doordat bijvoorbeeld verkeerde partijen macht over ons uitoefenen. Er kan een grote slag gemaakt worden als het gevoel van urgentie wordt omgezet in daadkracht.”

Cybersecurity demystificeren

Er is in Nederland een groot tekort aan cyberspecialisten en kennis over cybersecurity. “We moeten het voor jong mensen aantrekkelijker en toegankelijker maken om zich hierin te specialiseren,” aldus Stikker. ‘’Dat begint al op school, waar we scholieren moeten interesseren voor het onderwerp. Ze laten zien dat cyber en digitalisering belangrijk zijn voor iedereen. Nieuwsgierigheid begint als ze weten waar ze hun opgedane kennis voor kunnen inzetten. Waarom zou je willen leren coderen als je niet weet waar je dat voor kan toepassen?”

“Veel leerkrachten zijn doodsbenauwd voor technologie en technologieonderwijs. Terwijl het niet zo ingewikkeld is. Wij organiseren cursussen waarbij we in drie dagen de angst van leerkrachten veranderen in nieuwsgierigheid. Technologie is niet abstract maar creatief en concreet. Het is niet zozeer een informatica-vak, maar een ontwerpvak. Dat kun je ook collectief op scholen doen: door leerlingen te leren knutselen, door digitale vaardigheden én maatschappelijke vraagstukken verbinden. Door technologie zien als onderdeel van het ontwikkelen van burgerschap en niet alleen als een hardcore bètavak. Wat ook enorm zal zorgen voor meer inzicht is het versterken van de rol van geesteswetenschappen en sociale wetenschappen. Zorg dat deze wetenschappen een bijdrage leveren aan het ontwerp van de toekomst, in plaats van alleen in een reflectiemodus te zitten.”

Er is volgens Stikker een enorme potentie in de samenleving om bij te dragen aan het ontwerpen van de digitale toekomst. “Maar dan moet het idee verdwijnen dat het alleen voor de slimme data-wetenschapers en *young capital* is weggelegd. Bij Waag hebben we ervaring met open sensortechnologie waarmee bewoners data genereren over hun leefomgeving. Daar hoort ook data-geletterdheid bij: hoe moet je data interpreteren? Daarin werken we samen met het RIVM. Je staat verstelt van de leergierigheid en de hoeveelheid al aanwezige kennis van mensen.”

Meldingsplicht voor cyberincidenten

Waag is een schakel tussen de fysieke en digitale samenleving. Stikker zet zich in om die twee werelden bij elkaar te brengen, maar constateert ook dat er een taboe heerst op cyberincidenten: “Men schaamt zich als er iets misgaat, als er gehackt wordt. Dat suggereert dat de veiligheid van de systemen niet op orde is. Er zou een publieke meldingsplicht moeten komen. Het is raar dat we niet weten hoeveel mensen in de problemen komen door bijvoorbeeld identiteitsfraude. Door regelmatig meldingen te maken, krijgen we een idee van de omvang van het probleem. We moeten ons instellen op het feit dat software nooit volledig veilig zal zijn. Op het moment dat nieuwe software gereleaset wordt, ontstaat er een kwetsbaarheid en een afhankelijkheid van andere systemen.”

Stikker is van mening dat er nog te weinig wordt nagedacht over technologie. “Dat zou veel meer zichtbaar moeten zijn. Zodat mensen zich af kunnen vragen: Waarom zijn onze straten, onze deurbellen en onze tandenborstels eigenlijk smart? Hoezo is informatie over mij verhandelbaar? Mijn persoonlijke integriteit moet toch beschermd zijn. We verhandelen onze organen toch ook niet. Hoe kan het dat we een app store hebben waar producten in zitten die rechtstreeks onze soevereiniteit en autonomie bedreigen? We doen nu alsof *spying software* en *facial recognition* vanzelfsprekend zijn. Dat is het niet. Dat soort spullen horen niet op straat, niet in je deurbel, en niet in je tandenborstel.”

BACK TO TOP

NEXT

According to Stikker, there is a need for systemic changes in statutory provisions, in public procurement contracts, in internal frameworks and in the principles underlying the choices we make. 'This will ensure the hundreds of millions of euros invested in start-ups and new technologies from eroding our digital autonomy, for example by allowing the wrong parties to have power over us. We can make a huge leap forward if we manage to convert this sense of urgency into effective action.’

Demystifying cybersecurity

The Netherlands is struggling with a severe shortage of cyber specialists and know-how. ‘We need to make it more attractive for young people to specialise in this field, and make it more accessible for them,’ says Stikker. ‘We should start at the schools and arouse pupils’ interest in this subject, showing that cyber and digitalisation are important for everybody. Pupils will become curious once they know how they can apply the knowledge they have acquired. Why learn to encode if you don't know for what purposes you could use that knowledge?

Many teachers feel extremely uncertain about technology and technology teaching, but it's really not all that complicated. We organise courses for teachers in which we transform those fears into curiosity, in three days. Technology is not an abstract thing; it's creative and concrete. Rather than just another computer science subject, it's really a design subject. You can address that collectively at schools, by teaching pupils some handicrafts and by connecting digital skills and societal issues. By viewing technology not just as a hardcore science subject, but as part of the development of good citizenship. One other factor that will greatly increase our understanding is strengthening the role of the humanities and social sciences. Make sure that these disciplines contribute to your design for the future, instead of staying in your reflection mode.’

Stikker points to the enormous potential in society for contributions to the design of our digital future. ‘To benefit from that potential, we will need to get rid of the notion that this is the exclusive domain of smart data scientists and young capital. At Waag we have experience with open sensor technology that enables residents to generate data about their local environment. This also requires data literacy: how to interpret those data? We collaborate with RIVM on that issue. It's just amazing how eager people are to learn, and indeed how much they already know. '

Duty to report cyber incidents

Waag serves as a link between the physical and digital domains of society. Stikker is committed to bringing these two domains together, but also notes that cyber incidents are taboo: ‘People tend to be ashamed when something goes wrong, when their systems are hacked. This suggests that there is room for improvement in terms of systems security. What we need is a public duty to report incidents. After all, it's odd that we don't know how many people get into trouble due to ID fraud, for instance. When incidents are reported on a regular basis, this will give us a better idea of the scope of the problem. We must resign to the fact that software will never be completely secure. As soon as new software is released, a vulnerability will arise, and a dependence on other systems.’

According to Stikker, technology is not getting the attention it deserves. ‘It should be far more visible so that people can wonder: why do we have all these smart streets, smart doorbells, smart toothbrushes? And why should information about my person be tradeable? Surely my personal integrity deserves maximum protection. After all, we don't trade in our organs, do we? And how is it possible that there is an app store with products that pose a direct threat to our sovereignty and autonomy? We act as though spying software and facial recognition should be taken for granted. But they shouldn’t. That sort of stuff shouldn't be installed in the streets, in your doorbell or in your toothbrush.’

PETER ZIJLEMA

Nieuw lid van de Cyber Security Raad (CSR)

New member of the Dutch Cyber Security Council (CSR)

Peter Zijlema is General Manager bij IBM Nederland. Daarnaast bekleedt Zijlema diverse bestuurlijke functies voor onder meer NLdigital, VNO-NCW, FME en de American Chamber of Commerce in the Netherlands (AmCham NL). Hij is eveneens lid van de Raad van Advies van ECP en lid van het strategieteam van de Nederlandse AI Coalitie. Sinds juni 2021 is Peter Zijlema lid van de CSR namens NLdigital.

Peter Zijlema is General Manager at IBM Nederland. In addition, he holds various administrative positions, for example at NLdigital, VNO-NCW (the largest employers' organisation in the Netherlands), FME (the Dutch employers' organisation in the technology industry) and the American Chamber of Commerce in the Netherlands (AmCham NL). Zijlema is also a member of the Advisory Board of the ECP Platform for the Information Society and a member of the strategy team of the Netherlands AI Coalition. In June 2021, Zijlema joined the CSR on behalf of NLdigital.

Kunt u uzelf voorstellen en een korte beschrijving van uw profiel geven?
"Sinds 1997 ben ik werkzaam bij IBM en heb ik verschillende (senior) functies bekleed in zowel Nederland, Oost-Europa als de Verenigde Staten. Sinds 2014 heb ik IBM Nederland commercieel geleid en ben ik sinds 2017 ook General Manager voor IBM Nederland en Benelux. Op een inspirerende wijze wil ik IBM positioneren als relevante partner voor de digitale transformatie in de Benelux. Naast mijn functie bij IBM heb ik ook diverse bestuurlijke functies. Onder meer bij NLdigital, waar ik de portefeuilles 'Ethiek' en 'Vertrouwen/cybersecurity' onder mijn hoede heb."

Waarom is een integrale aanpak voor cyberweerbaarheid en het behoud van onze digitale autonomie zo belangrijk voor de digitale sector?
"Cybersecurity is voor mij een absolute randvoorwaarde voor innovatie. Zonder security voldoen diensten en producten niet aan de verwachtingen van investeerders, afnemers, burgers. Dit gaat ten koste van ons vertrouwen, onze digitale autonomie en ook ten koste van onze vitale processen en infrastructuur. Juist omdat dit zo'n complex vraagstuk is, vraagt dit om een integrale benadering. De huidige coronacrisis onderstreept de urgentie hiervan extra. Ik zie dat er in Nederland op veel fronten al goede stappen zijn gezet, maar de samenhang ontbreekt nog. Ook de internationale connectie moet naar mijn idee nog sterker vorm krijgen."

Welke rol ziet u hierin voor uw zelf als nieuwe raadslid van de CSR?
"In de publiek-private samenwerking vertegenwoordig ik namens NLdigital een onmisbare schakel in het cybersecurityveld: de dienstverleners en leveranciers van ICT-producten. Met mijn lidmaatschap in de CSR wil ik de kennis, kunde en capaciteit van onze achterban inzetten om de cyberweerbaarheid van Nederland verder te versterken."

Photo: Arenda Oomen

Could you introduce yourself and briefly describe your personal profile?
'I've worked for IBM since 1997 in various senior positions, in the Netherlands, in Eastern Europe and in the United States. I have been commercial director of IBM Netherlands since 2014, and also took on the role of General Manager for IBM Netherlands and the Benelux in 2017. My goal is to position IBM as a relevant partner for the digital transformation in the Benelux countries in a way that inspires people. Besides my role at IBM I also have various administrative positions, for example at NLdigital, where I am in charge of the Ethics and Trust/Cybersecurity portfolios.'

Why is an integrated approach to cyber resilience and preserving our digital autonomy so important for the digital sector?
'For me, cybersecurity is an important precondition for innovation. Without security, services and products simply fail to meet the expectations of investors, buyers and citizens. This will erode our trust, our digital autonomy and our vital processes and infrastructures. This issue calls for an integrated approach precisely because it is so complex. The current coronavirus crisis only serves to emphasise the urgency of such an approach. While I've seen considerable progress being made in the Netherlands on various fronts, we do need more coordinated action. I also believe that we should further strengthen the connection with international developments.'

How do you view your own role in this context, as a new member of the CSR?
'In the public-private partnership domain I represent a crucial link, on behalf of NLdigital, in the field of cybersecurity: the service providers and suppliers of ICT products. Through my CSR membership I intend to mobilise the knowledge, know-how and capacity of the field to further strengthen cyber resilience in the Netherlands.'

Vanuit NLdigital zien we een drietal belangrijke aandachtsgebieden waarmee een bestuurder het verschil kan maken in het realiseren van cyberweerbaarheid in Nederland. Het start al bij bewustwording. Het besef, bijvoorbeeld, dat het niet meer de vraag is óf je geraakt gaat worden door een cyberaanval, maar wanneer je wordt geraakt. En ook het bewustzijn dat het verhogen van de cybersecurity om extra investeringen vraagt. Een tweede aandachtsgebied is de keten van software, wat wil zeggen de ontwikkeling van begin tot eind, veiliger maken om te komen tot maximale veiligheid. Dat kan bijvoorbeeld door het introduceren van standaarden voor cybersecurity binnen ketens. Een derde aandachtsgebied is de verdere beweging naar 'security and privacy by design', wat neerkomt op het inbouwen van veiligheid vanaf de start van het ontwerp van een product – en dus niet achteraf.

NLdigital has identified three focus areas in which administrators can make a real difference in realising cyber resilience in the Netherlands. It starts at the awareness-raising level. Being aware, for example, of the fact that it is no longer a question of whether you will be affected by a cyberattack, but when. And being aware that a higher level of cybersecurity also calls for a higher level of investment. The second focus area is the software chain: ensuring the highest level of security throughout the entire development process. This can be achieved, for instance, by introducing cybersecurity standards within chains. The third focus area is the further shift towards 'security and privacy by design', which comes down to integrating security in the design of a product right from the start, and not as an afterthought.

CYBERSECURITY CHALLENGES CALL FOR AN INTEGRATED APPROACH

We regard security as a precondition for innovation. Security generates trust. Given the importance of security, I am committed to addressing these three focus areas and prioritising cybersecurity using the NLdigital network. That network can help create the necessary level of awareness. In addition, the network and the experience it contains may help us formulate standards and embed the ‘security and privacy by design’ principle in all forms of product and service development.

One important factor in this regard is public-private partnership for the joint development of solutions, such as the Digital Trust Center (DTC). The DTC was created by the Dutch Ministry of Economic Affairs and Climate Policy to provide cybersecurity-related advice and support to the 1.8 million companies that are beyond the scope of the National Cyber Security Centre (NCSC). In my opinion, the DTC should be granted far more resources to enable it to fulfil this task effectively. I am convinced that this will greatly help to protect companies in the Netherlands.

Many solutions available
Many solutions that will help improve security are already available. Failure to implement those solutions on a much wider scale is a missed opportunity, according to NLdigital – so we should not hesitate to use what is already at hand. At the same time, we also need an innovative approach to promote standardisation and continuous improvement throughout the chain. Once implemented, such standards will create further opportunities for automation. This will result in much shorter response times to address vulnerabilities, so that many more attacks can be prevented from causing real damage. In addition, automation will contribute to the productivity of security experts in a tight market.

Importance of integrated approach cyberresilience
Cyber resilience is not yet sufficient everywhere in the Netherlands to be able to confront increasing threats. This is a complex challenge that will have to be addressed from within all layers of Dutch society. Cybersecurity is expressly regarded from the perspective of sovereignty, in the sense that insufficient cyber resilience will erode our digital autonomy. This is why the CSR recommends an integrated approach to strengthening cyber resilience, which involves a cyber resilience coordination effort; secure products and services for citizens, businesses and the government; resilient vital processes and infrastructures; cybercrime supervision, enforcement and protection; and knowledge, research and innovation. These measures would address all of the three focus areas mentioned above.

Peter Zijlema
General Manager IBM Benelux, General Manager IBM Netherlands and CSR member representing NLdigital

“De innovatie die we nu ook nodig hebben is meer standaardisatie in de hele keten en dat dan ook continu verbeteren”
‘We need an innovative approach to promote standardisation and continuous improvement throughout the chain.’

Security zien we als randvoorwaarde voor innovatie, het zorgt voor vertrouwen. Gezien het belang van security, wil ik me inzetten om genoemde aandachtsgebieden te adresseren en cybersecurity een prioriteit maken met behulp van het netwerk van NLdigital. Dit netwerk kan mede helpen het benodigde bewustzijn te creëren. De inzet van het netwerk en hun ervaring kan tevens bijdragen om tot standaarden te komen en het ‘security en privacy by design’ principe in te bedden in alle vormen van product- en dienstontwikkeling.

Belangrijk hierbij is de publiek-private samenwerking voor de gezamenlijke ontwikkeling van oplossingen, zoals voor het Digital Trust Center (DTC). Voor het DTC dat vanuit het Ministerie van Economische Zaken en Klimaat is opgezet, om de 1,8 miljoen bedrijven buiten het werkveld van het Nationaal Cyber Security Centrum (NCSC), te adviseren en ondersteunen op het gebied van cybersecurity, moeten mijns inziens veel meer middelen vrijgemaakt worden om deze taak goed te kunnen vervullen. Ik ben ervan overtuigd dat de bedrijven van Nederland hierdoor veiliger zullen worden.

Veel oplossingen voorhanden
Op dit moment zijn al veel oplossingen beschikbaar om veiligheid te bevorderen. Vanuit NLdigital vinden we het een gemiste kans dat we deze oplossingen niet op veel grotere schaal gebruiken – dus toepassen wat reeds beschikbaar is. De innovatie die we nu ook nodig hebben is meer standaardisatie in de hele keten en dat dan ook continu verbeteren. Met geïmplementeerde standaarden kan er meer worden geautomatiseerd dan nu het geval is. Dit zal onder andere leiden tot een veel hogere reactiesnelheid bij kwetsbaarheden, waardoor schade bij veel meer aanvallen voorkomen kan worden. Bovendien draagt deze automatisering bij aan de productiviteit van security-experts in een markt van schaarste.

Belang integrale aanpak cyberweerbaarheid
Op dit moment is de cyberweerbaarheid in Nederland nog niet overal afdoende om de toenemende dreigingen het hoofd te bieden. Cyberweerbaarheid is een complexe uitdaging en moet in alle lagen van onze samenleving geadresseerd worden. Cybersecurity wordt nadrukkelijk gezien vanuit een soevereiniteitsperspectief. Dat wil zeggen dat onvoldoende cyberweerbaarheid ten koste gaat van onze digitale autonomie. De CSR adviseert daarom een integrale benadering om de cyberweerbaarheid te vergroten, wat neerkomt op regie op cyberweerbaarheid, veilige producten en diensten voor burgers, bedrijfsleven en overheid, weerbare vitale processen en infrastructuur, cybercrimetoezicht, -handhaving en -bescherming en kennis, onderzoek en innovatie. Daarmee zouden mijn drie eerdergenoemde aandachtsgebieden geadresseerd worden.

Peter Zijlema
General Manager IBM Benelux en General Manager IBM Nederland en lid van de CSR namens NLdigital

BACK TO TOP

Ciaran Martin
Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government and visiting Professor at King's College London

AN ACTIVIST STRATEGY TO BREAK WITH THE PAST

Ciaran Martin was the founding Chief Executive of the UK National Cyber Security Centre (NCSC), part of the intelligence agency Government Communications Headquarters (GCHQ). After working as a civil servant for 23 years he is now Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government and a visiting Professor at King's College London.

As Chief Executive of the NCSC Martin completed the British National Cybersecurity Strategy 2016-2021.1 'In one word the strategy was activist', Martin explains. 'We broke with some sort of Western/US led consensus that had dominated government cybersecurity for the last ten years. This consensus was a focus on the top end of the problem and then get the market to do the rest. This meant encouraging people to share information and partner with the government. There were no real details on what that meant. It was very passive, and it wasn't really working.'

A more activist approach
The 2015-16 strategy is well known for establishing the NCSC as the single point of leadership for cyber security in the UK. 'That was not particularly important in itself, but it was a change in strategy towards a more activist approach.'

This approach was visible in four main activities. The first is to really grip threats and incidents. 'We saw this with the TalkTalk hack in 2015, when a major telephone company was hacked. There were no rules on how to manage the public consequences of this incident. We could've had all the knowledge in the world, but would not be able to put it into practice because we didn't have a leadership role to reassure and communicate with the public or with the businesses affected. The establishment of the NCSC changed this.'

The second is still according to Martin a work in progress: the improvement of resilience in critical infrastructure. 'In terms of legacy infrastructure, it's pretty much impossible to do transformative change, you're only doing mitigation. But with new critical infrastructure, for instance when we build smart transit systems, we now build it with security resilience in the design based on expert advice from the NCSC.'

Intervention when the market is not working
'The final two activities are the most interesting breaks with the past', Martin explains. 'The third is direct government intervention in parts of structural internet insecurity where the market isn't working. An example of this are our actions against brand spoofing. This is a huge problem in cybersecurity, but nobody does anything about it. We found that one of the reasons for this is because fixing it doesn't pay. Brand spoofing does not seem to hurt the position of the brand. If you receive a fake e-mail from (supposedly) your supermarket you will still go there for your groceries, because it wasn't their fault.'

1 The strategy is due to be refreshed. But because of all the political difficulties with Brexit and COVID all government strategies have been delayed. The new strategy should be out soon.

Photo: NCSC Press Office

'In my view we placed far too much weight on the concept of information sharing as a solution than it can bear.'

'Therefore, the NCSC decided to act', Martin explains. 'We mandated the introduction of the DMARC protocol on all government brands, which made e-mails a lot harder to spoof. We also promoted a freely available version for businesses. What the protocol does is tell an e-mail client what an official e-mail from an organisation should look like. If it does not match do not deliver it. In 2017 we did a pilot with the Tax Authority. In one year we prevented 500 million fake attempts from being sent.'

The last activity is focused on making the internet easier to use safely. 'We won the argument on password policy. In the past every network we use would have its own password policy. Forcing you to use a long unique password and changing that password every so often. You soon end up with a multitude of different passwords. For users this makes it impossible to use the internet safely. A professor in behavioral science calculated that this was the equivalent of asking people to remember a new 600-digit number every month. We banned the phrase 'people are the weakest link in cybersecurity' and instead focused on a series of reforms to try and make the internet easier to use safely. This involves actively communicating with the public.'

The obsession with information sharing
On the topic of information exchange Martin is critical about the attention it receives in cybersecurity. 'We placed far too much weight on the concept of information sharing as a solution then it can bear. It is a useful contributory part. There is a wonderful phrase, that is not mine, but puts it very directly: 'information sharing is the thoughts and prayers of cyber security.'

Good information sharing can be effective, according to Martin, but it takes a lot of effort. 'Look at Wall Street where they have serious technical capability and money behind exchanging mutually comprehensible data. It's expensive and takes a lot of skills and effort. Just piling together information and saying: 'let's share some stuff' is less useful. I think when someone writes a PhD in 50 years about cybersecurity in the early 21st century one of the main questions would be: why was everyone so obsessed with information sharing as if it was the most important thing of all?"

Martin touches on several obstacles which hinder information sharing. "Organisations are wary of competition and legal liability. Also, people tend to look for return on investment on their activities. What can be won? Of course, the government sharing certain intelligence can really help. But I personally think that if information sharing was solving a lot of problems, it would happen more. So, it does contribute to a wider cybersecurity strategy, but many strategies are equally or more important."

According to Martin, the NCSC model for partnerships can be compared to an onion. It is a whole of nation approach but with different layers. ‘The inner ring is direct support to and service provision for defense and military assets. Parts of the NCSC make products for the ministry of defense. The next layer is government, followed by critical infrastructure where we subject resources for resilience and mitigation and provide sectoral guidance. The UK has a very flexible approach to what is critical and what is not. There can be organisations you do not know about but if something happened to them it could prove critical. Think of DNS-registrar or political institutions, which were added to the list a couple of years ago.’ The NCSC never really compiled a public list of critical infrastructure. ‘Our view is that given the nature of bureaucracy we would get it wrong and even if we did get it right, it would be outdated immediately. Layer four is everybody else. In a country of 66 million people, you don’t have the capacity to talk to everyone. But we publish information, such as small business guidance, and help them with basic protection.’

The effects of Brexit on international cooperation have been minimal, Martin explains. ‘While the relationship between heads of state might have been affected, the relationship between cybersecurity agencies improved. During Brexit talks the operational cooperation improved considerably. As an example, Martin mentions the cooperation with the Netherlands after The Hague Operation, which Martin describes as a superb piece of work by the Dutch colleagues. Perhaps it is the nature of cybersecurity that makes it less affected by Brexit. The operational environment is very apolitical. We still work closely together and will do so in the future.’

The growing concern on ransomware

For Martin the most pressing issue now in cybersecurity is ransomware. ‘Over the course of ‘20-‘21 its’ socially disruptive impact has become much more visible. Prior, it was still big business, but it was used for the quiet extortion of big wealthy companies. They just paid to make it go away. There are no disclosure requirements, so it would go by largely unnoticed. For whatever reason they’ve started going for things like national healthcare systems. Apart of the utter amorality and danger that it brings, people are noticing the impact more and more now.’

According to Martin the really concerning thing that the ’20-‘21 ransomware outbreak has done, is that it has weakened our confidence in the resilience of organisations and especially the services they provide. ‘One of the main rules in cybersecurity used to be that operational technology must never be influenced by enterprise technology. This means that hacking an e-mail system should not shut down a pipeline or a hospital. But in the last two years we have seen exactly that. That hole on our resilience is worrying. If it can be done with medium capabilities, think about what can happen if nation states are behind the controls with higher and more sophisticated capabilities.’

Martin lists three things working in favor of the criminals using ransomware. ‘First, there is a safe haven in Russia and some other countries where they can operate freely. Second is the weak resilience of organisations, which makes them more vulnerable. Organisations should ask themselves what happens when they lose their system? Can they still operate their pipeline or provide healthcare? If you can’t, work out how to do it. The third is the business model, which favors the criminals. It is easy to extort people and the payment in cryptocurrency makes it very hard to trace. We need more regulation on that, to limit or ban payments and require the disclosure of payments. After 9/11 a mayor part of the fight on terrorism was clamping down financial flows and stop the flow of money. We should do the same with cryptocurrency to battle criminals using ransomware.’

Don’t be afraid of cybersecurity

Martin concludes with some advice for organisation leaders: ‘Don’t dismiss cybersecurity as too technical. Treat it as a business risk like any other. Just focus on what cyber harms are most likely to affect your organisation and what reasonable mitigation you can put in place. Then find someone who is technically fluent to assist you. Just don’t be afraid of cybersecurity.’ He also has an advice for public policy makers: ‘We need to raise our heads a bit. The biggest problem strategically is that we allowed, through nobody’s fault, a system of technology of which we are all increasingly dependent on, which has all sorts of structural insecurities. We should demand safer technology. The same way we do for safer public transport.’

BACK TO TOP

‘Over the course of ‘20-‘21 the socially disruptive impact of ransomware has become much more visible.’

Floor Jansen
Teamleader at the National Police Force's High-Tech Crime Team (THTC)

Floor Jansen is als criminoloog, sociaal wetenschapper en cybersecurity-expert werkzaam als teamleider bij het Team High Tech Crime (THTC) van de Nationale Politie. Dankzij haar multidisciplinaire achtergrond is ze gewend om problemen van verschillende kanten te bekijken, waardoor er in haar werk als vanzelf een integrale aanpak volgt voor het bestrijden van cybercrime.

Floor Jansen works as a criminologist, social scientist and cybersecurity expert as a teamleader at the National Police Force's High-Tech Crime Team (THTC). As a result of her multidisciplinary background, she has learnt to examine problems from various angles and is naturally inclined to approach cybercrime from a holistic perspective.

WHY WAIT TILL THINGS GO WRONG?

OFFENDER PREVENTION IS A CRUCIAL PART OF CYBERSECURITY

Het THTC bestaat inmiddels meer dan tien jaar. Het werd ooit opgericht toen de Politie geconfronteerd werd met de eerste cybercrimes, en heeft zich inmiddels ontwikkeld tot een internationaal toonaangevend team van 140 man. Jansen: “Dat zijn niet alleen digitaal rechercheurs, maar ook ontwikkelaars en strategen die nationale en internationale vormen van high tech crime bestrijden. Dat doen we op innovatieve en baanbrekende manieren. Datascience gedreven opsporing is voor ons bijvoorbeeld essentieel. We sporen niet alleen op, we zetten ook in op een proactieve bestrijding van high tech crime.”

The THTC has been active for over ten years. Originally formed in response to the first cybercrime incidents, it has since evolved into an internationally renowned team of 140 people. Jansen: ‘In addition to digital investigators, it is also made up of developers and strategists working to fight national and international forms of high-tech crime. We approach those issues in innovative and ground breaking ways. For example, data science-driven detection methods are crucial to what we do. In addition to detection, we also proactively target high-tech crimes.’

This effectively involves a holistic approach to cybercrime. ‘Traditional detective work usually starts when a citizen reports a cybercrime to the police, after which the investigative machine springs into action,’ Jansen explains. ‘The THTC is already hard at work before any police reports have been filed. For example, we work to identify the main botnets and criminal actors operating around the world today. We then look for opportunities to combat those international groups and organisations from the Netherlands. Although these perpetrators aren't necessarily based in the Netherlands, they do make use of our advanced digital infrastructure. That creates opportunities for detection.’

Offender prevention

With a multidisciplinary background, Jansen is accustomed to examining problems from different angles. ‘I tend to focus on the main problem and its

Photo: Arenda Oomen

In feite is dat ook een integrale aanpak van cybercrime. “Klassiek recherchewerk begint wanneer een burger aangifte doet bij een politiebureau van bijvoorbeeld een cyberdelict, waarna de opsporing-machine gaat draaien,” legt Jansen uit. “Het THTC begint al vóórdat er een aangifte is gedaan. We zoeken bijvoorbeeld naar wat op dit moment wereldwijd de belangrijkste botnets of criminele actoren zijn. Vervolgens zoeken we naar kansen voor Nederland om die internationale groepen en organisaties te bestrijden. Die daders bevinden zich lang niet altijd in Nederland, maar ze maken wel gebruik van onze uitstekende digitale infrastructuur. Dat biedt kansen voor de opsporing.”

Daderpreventie

Het grote voordeel van de multidisciplinaire achtergrond van Jansen is dat ze gewend is om problemen van verschillende kanten te bekijken. “Ik focus mij eerder op het hoofdprobleem en de oorzaken daarvan. Daar rolt als vanzelf een integrale aanpak van cybercriminaliteit uit voort. Dat is een van de redenen waarom ik de Cyber Offender Prevention Squad (COPS)[1] van het THTC heb opgezet.”

“Waar we ons tot een paar jaar geleden beperkten tot het opsporen van cybercriminaliteit ten behoeve van vervolging, proberen we nu met de COPS een omslag te maken naar het breed bestrijden van het probleem. We doen dit door voorkomen en verstoren toe te voegen aan vervolgen. We leveren dus niet meer alleen een verdachte aan bij het Openbaar Ministerie, maar proberen een probleem te definiëren en te bedenken hoe we dat op een efficiënte manier kunnen bestrijden. Bijvoorbeeld door daderpreventie.”

Het volledige spectrum bestrijden

Daderpreventie is een heel breed begrip. Jansen legt uit hoe COPS dit oppakt: “We proberen potentiële daders af te schrikken en bij te sturen naar positieve keuzes. Dat lukt voor een bepaald deel, maar een deel van de *potentiële* daders zal toch daadwerkelijk dader worden. Voor die laatste groep, die bewust kiest voor cybercrime, proberen we cybercriminele markten te verstoren en hun positie te verzwakken. Om dit te bereiken ontwikkelen we interventies voor deze twee verschillende groepen. We voeren deze interventies uit met partners binnen onze organisatie (zoals de basisteams en de cybercrimeteams) en partners hierbuiten, zoals gemeenten en cybersecuritybedrijven. We pogen met deze aanpak schade te voorkomen, talent voor de samenleving te behouden en de rechtsketen te ontlasten.”

1 De Cyber Offender Prevention Squad (COPS) zet in op daderpreventie vanuit verschillende specialismen. Dit team bestaat uit een gedragsspecialist, interventiespecialist, digitaal specialist en de oprichter van het Britse NCA Prevent Team. Zij zoeken de samenwerking op met publieke en private partijen om preventieve interventies te ontwikkelen en hiermee daderschap van cybercrime te ontmoedigen.

“Politiecijfers over het aantal cybercrime-delicten zeggen weinig over de omvang van het probleem.”

‘Police statistics on the number of cybercrime offences don't reflect the extent of the problem.’

“Het klassieke opsporen en vervolgen is een effectief middel, maar niet heel efficiënt. Het is de integrale blik waarmee we naar de problematiek hebben gekeken, waarbij het daderpreventieteam cybercrime voorkomt, ook naast het strafrecht. Met 140 man in het THTC heb je de capaciteit om een bepaald aantal daders per jaar op te sporen en te vervolgen. Als je aan daderpreventie of verstoring doet, dan is het mogelijk om veel meer effect te sorteren en het probleem aan de voorkant te bestrijden. Preventie is vaak schaalbaarder, proportioneler en efficiënter”

Samenwerking loont

Niet alle cybercrime is het werk van geharde criminelen, een deel wordt uitgevoerd door verveelde jongeren die de gevolgen van hun gedrag niet helemaal overzien. Tijdens de coronacrisis zag Jansen deze vorm van cybercrime toenemen: “Met name tijdens de lockdowns, toen iedereen binnen moest zitten, was er meer verveling. Daardoor nam zowel de motivatie als de gelegenheid toe. Daarom hebben we proactief positieve alternatieven ontwikkeld, zoals *Gamechangers*: speciale games om jongeren uit de cybercriminaliteit te houden. Met behulp van uitdagingen leren ze cybercrime te herkennen en wordt geprobeerd te voorkomen dat zij (onbedoeld) dader worden. Dit project is opgezet met verschillende coalitiepartners, zoals Deloitte, ESL gaming en Stichting Hack in the Class.”

“We werken altijd zoveel mogelijk met partners samen. De verantwoordelijkheid om cybercrime te voorkomen ligt namelijk niet alleen bij de politie. Stichtingen, bedrijven, publieke organisaties: iedereen heeft een verantwoordelijkheid. Met de COPS brengen we partijen bij elkaar, zodat iedereen vanuit zijn eigen informatiepositie een steentje bij kan dragen.”

Structurele financiering en aandacht

Er zijn volgens Jansen verschillende succesvolle voorbeelden van een integrale aanpak van cybercrime. “Een mooi succesproject is *Hack_Right*,

1 The Cyber Offender Prevention Squad (COPS) applies knowledge from various disciplines to develop effective offender prevention measures. The team consists of various intervention specialist, eg a behaviourist, a digital specialist, multiple criminologists and a British expert on offender prevention. They develop preventive interventions in collaboration with public and private parties in an effort to deter potential cybercriminals.

underlying causes. That sort of approach naturally leads to a more holistic cybercrime strategy and inspired me to set up the THTC's Cyber Offender Prevention Squad (COPS).[1]’

‘A few years ago, we only monitored cybercrime with the aim of prosecution. These days, COPS is transitioning to a more comprehensive approach. In addition to prosecution, we're shifting our focus to prevention and disruption. That means we're not just handing over suspects to the Public Prosecution Service any more; we're trying to define specific problems and figure out how to combat them effectively. Amongst other methods, we're now focusing on offender prevention.’

Full-spectrum crime prevention

Offender prevention is a very broad term. Jansen explains COPS' approach: ‘We try to deter potential offenders and steer them towards more positive choices. Those efforts will turn certain offenders, but a certain percentage of potential offenders will ultimately still end up committing crimes. The latter group makes a conscious choice to engage in cybercrime, so we aim to disrupt cyber-criminal markets, devalue offenders’ profiles, products and platforms, and raise barriers for offenders to commit crime. We develop separate interventions for these two groups, which we then implement in cooperation with internal partners (such as the basic teams and cybercrime teams) and external parties such as municipalities and cybersecurity firms. This approach is aimed at preventing damage, retaining talent for broader society and easing the burden on our legal system.’

‘Traditional investigation and prosecution methods are effective, but not very efficient. We examined the issue from a more holistic perspective and developed an approach that includes both criminal law and cybercrime prevention by the Offender Prevention Team. The THTC has a staff of 140, so we only have enough capacity to track down and prosecute a certain number of offenders each year. Offender prevention and disruption methods can be far more effective and allow us to tackle the problem at the source. Prevention tends to be more scalable, proportional and efficient.’

Collaboration pays off

Cybercrime is not always committed by hardened criminals; some offenders are just bored kids who do not really understand the consequences of their actions. Jansen noticed a rise in this form of cybercrime during the COVID-19 pandemic: ‘People were especially bored during the lockdowns, when everyone was forced to stay indoors. As a result, there was both more motive and more opportunity. We decided to respond proactively and developed positive alternatives like Gamechangers: games aimed at deterring young people from cybercrime. The games present a series of challenges, teaching them how to recognise cybercrime and avoid becoming perpetrators, whether unwittingly or otherwise. The project was developed in collaboration with various coalition partners, such as Deloitte, ESL gaming and the Hack in the Class Foundation.’

‘We always work with partners whenever we can. After all, the police aren't the only ones responsible for preventing cybercrime. Foundations, companies, public organisations: everyone has a responsibility here. COPS brings all those stakeholders together so that everyone can contribute from their own information position.’

een initiatief voor daders tussen de 12 en 23 jaar die voor het eerst een cyberdelict hebben gepleegd. *Hack_Right* is een alternatieve of aanvullende straf waarbij recidivepreventie het doel is. Het is opgezet door onder andere de politie, het OM, de Raad voor de Kinderbescherming, Reclassering, Bureau en Halt. Bijzonder aan *Hack_Right* is dat de private sector heeft meegewerkt aan de ontwikkeling en meewerkt aan de uitvoering van *Hack_Right*. De deelnemers gaan aan de slag voor en bij een cybersecurity-afdeling en worden hierbij begeleid door deze bedrijven. Zij hebben dus een heel belangrijke rol in de recidivepreventie."

"Een ander succes is stichting *HackShield*, waar de overheid medefinancier van is. *HackShield* is een online game voor jongeren tussen de 8 en 12 jaar om niet alleen zichzelf, maar ook hun omgeving te beschermen tegen cybercrime. Het is een soort digitale scouting, waar veel publieke partners zoals gemeenten en politie aan meewerken. De stichting heeft de game ontwikkeld en de politie heeft onder andere meegewerkt aan de politiequest 'Online Grenzen'. In deze quest leren jongeren hoe ze cybercrime kunnen herkennen en hoe ze kunnen voorkomen dat ze hiervan zelf dader of slachtoffer worden."

Dit soort initiatieven worden volgens Jansen op dit moment nog niet structureel ondersteund. "Het hangt vaak aan elkaar van donaties, ook vanuit het bedrijfsleven. Structurele ondersteuning in zowel financiële zin als aandacht is nog heel mager. Dat geldt over de hele linie. Ook bij de politie is daderpreventie slechts een klein onderdeel, daar zou meer structureel aandacht en financiering voor moeten zijn. Want preventie zonder opsporing is tandeloos, maar opsporing zonder preventie is eindeloos."

Er is in 2019 een eenmalige investering van €30 miljoen gedaan die ten dele is gebruikt voor de integrale aanpak van cybercrime. Jansen: "Die boost was heel hard nodig. De recherche is hiermee versterkt; we hebben nu bijvoorbeeld 10 regionale cybercrime units. De volgende stap is dat de handhavingskant van de politie ook in positie komt op het onderwerp cybercrime. In de offline wereld investeert de politie heel veel in preventie. Wie spijbelt, snoep steelt of een bushokje vernielt, wordt hierop meteen aangesproken en er wordt ingegrepen. Online vandalisme, diefstal en vernieling wordt nauwelijks opgemerkt, laat staan dat hierin wordt ingegrepen. Jongeren bouwen op deze manier razendsnel een cybercriminele carrière op buiten het zicht om van ouders, school en de politie. Slechts een deel van hen wordt opgespoord als ze echt veel schade aanrichten. We moeten zorgen dat het niet zo ver komt. We moeten zorgen dat wijkagenten ook online surveilleren en bijsturen. Maar dit roept veel vragen op. Waar? En hoe? Welke mogelijkheden en restricties gelden er voor de politie? Wat is de rol van het OM en de burgemeester? En welke competenties hebben agenten nodig om te handhaven op het internet? De politie concurreert ook met techbedrijven in de zoektocht naar de juiste mensen, dat is nieuw voor onze organisatie. Talent is schaars, we vissen allemaal in dezelfde vijver. Om nieuw talent voor het versterken van de handhaving op cybercrime te werven, is structureel budget nodig."

Voorkomen meer effect dan oplossen
Ondanks de gemaakte voortgang, blijft het aantal cybercrime-incidenten en -delicten toenemen. Op de vraag of een integrale aanpak het tij kan keren geeft Jansen een genuanceerd antwoord: "Aan de ene kant moeten we de integrale aanpak intern bij de politieorganisatie verder versterken. Zorg ervoor dat verschillende onderdelen van de politie samenwerken om cybercrime te bestrijden, en laat het niet over aan een groepje specialisten bij de recherche. Maar bij die integrale aanpak moeten we ook externe partijen betrekken. Dat is een les voor iedereen: zorg dat je altijd samenwerkt met partijen die een rol hebben in de aanpak van cybercrime of die simpelweg hun verantwoordelijkheid pakken. Elke organisatie overziet een ander stukje van het probleem, elke organisatie heeft andere expertise, een ander mandaat en een ander netwerk. Het bij elkaar brengen van die expertise is echt de sleutel in het succesvol aanpakken van cybercrime, je bereikt een effect dat je anders zelf niet had kunnen bereiken."

De politie werkt hiervoor ook samen met andere handhavingsinstellingen, zoals het OM, het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). "We zijn een paar jaar geleden gestart met het platform *NoMoreRansom*. Dat is typisch een voorbeeld van een integrale aanpak waar allerlei organisaties een stukje aan bijdragen. Dit heeft zich doorontwikkeld in de Ransomware Taskforce, waarbij er verder wordt gekeken dan ransomware incidenten oplossen. Dat leidt immers tot veel te weinig effect. In plaats daarvan probeert de Ransomware Taskforce eerst de spaghetti van ransomware-varianten en ransomware-dienstverlening in kaart te brengen, om zo te achterhalen welke partijen het belangrijkste zijn. Die worden vervolgens in samenwerking met de private industrie geselecteerd, om daarna die criminele groepering of dat proces zo goed mogelijk te bestrijden. Het neerhalen van het Emotet-botnet voorkomt veel meer ransomware-besmettingen dan we ooit achteraf hadden kunnen oplossen."

Versterking handhavingsketen
Er wordt met andere woorden al veel samengewerkt aan een integrale aanpak van cybercrime. Toch ziet Jansen ook nog kansen om de handhavingsketen verder te versterken. "De start van het COPS-team belichaamt dat. Onze missie is ook om te zorgen dat de handhavingsketen veel meer wordt betrokken bij het onderwerp cyber, en dan niet alleen reactief maar ook op een proactieve manier. Het is zonde om steeds maar te wachten tot het mis gaat, vervolgens op te sporen en criminelen te berechten. Dan blijf je dweilen met de kraan open. Daderpreventie en de versterking van de handhavingsketen is een manier om die kraan te repareren."

"Zorg dat je altijd samenwerkt met partijen die een rol hebben in de aanpak van cybercrime."
'Make sure to always work closely with the organisations fighting cybercrime.'

"We zijn gezamenlijk verantwoordelijk om cybercrime te voorkomen."
'The fight agains cybercrime is a collective effort.'

Structural funding and attention
Jansen highlights some successful examples of this holistic approach to cybercrime. 'The Hack_Right initiative is a great example: the project targets first-time cybercrime offenders between the ages of 12 and 23. Hack_Right is an alternative or supplementary form of punishment aimed at preventing recidivism amongst first time cyber offenders and was developed by parties including the police, the Public Prosecution Service, the Child Care and Protection Board, the Probation Service and Halt. Uniquely, Hack_Right was developed in cooperation with private sector parties, who are also helping to execute the initiative. Participants work for corporate cybersecurity departments, who also provide them with guidance. Those private sector parties play a crucial role in preventing recidivism.'

'The HackShield Foundation – an initiative co-funded by the government – is another success story. HackShield is an online game for children between the ages of 8 and 12 and teaches players how to protect themselves and their environment against cybercrime. It's basically a form of digital scouting involving a host of public sector partners such as municipalities and the police. The game was developed by the foundation with the help of the police, who contributed to the "Online boundaries" police quest and other content. The quest teaches young people how to recognise cybercrime and avoid becoming perpetrators or victims themselves.'

In Jansen's view, these types of initiatives are not yet getting the structural support they need. 'Everything tends to depend on donations, some of which come from the business community. There's still very little structural support in terms of both finances and attention for the issue. That applies across the board. The police also aren't very active in terms of offender prevention; that will require more systematic attention and funding. After all, prevention without detection is ineffective, but detection without prevention is a never ending story.'

A one-off €30 million investment in 2019 was partly used to develop a holistic approach to cybercrime. Jansen: 'We really needed that boost. It helped us to reinforce our criminal investigation department; for example, we now have ten regional cybercrime units. As a next step, the police's enforcement arm needs to focus their efforts on cybercrime. The police are investing a great deal in prevention in the offline realm. Anyone who skips classes, steals candy or vandalises a bus shelter is immediately held to account and disciplined. By contrast, online acts of vandalism, theft and destruction are hardly ever detected, let alone acted upon. As a result, young people can quickly forge a career as cybercriminals out of sight of their parents, schools and the police. They are generally only detected if they cause a great deal of damage. We need to prevent them from reaching that point in the first place. We should make sure community police officers are also monitoring their behaviour online and providing guidance. Still, this does raise a host of new questions. Where? How? What options do the police have at their disposal, and what restrictions do they face? What role should the Public Prosecution Service and the Mayor play? What competences will police officers need to enforce the law online? The police are also competing with tech companies in their search for the right staff, which is something our organisation has never faced before. Talent is scarce, and we're all fishing in the same pool. We'll need structural resources if we aim to recruit new talent and improve our cybercrime enforcement efforts.'

Prevention more effective than cure
Despite our progress, the number of cybercrime incidents and crimes is still growing. When asked whether a holistic approach could turn the tide, Jansen gives a nuanced answer: 'On the one hand, we need to keep pushing for a more holistic approach within the police organisation. Make sure the

“Er ligt heel veel expertise en kennis in de handhavingsketen besloten: elke organisatie heeft zijn eigen manier van werken. Waarom zou die kennis niet werken voor de aanpak van cybercrime? Die organisaties kennen de weg in cyberspace alleen nog niet voldoende. Daar ligt een rol voor ons in besloten, om de handhavingsketen te ondersteunen zodat zij hun werkwijze ook online kunnen toepassen. Dat gaat verder dan alleen kennis delen en cybercrime signaleren, maar gaat juist om de vraag wat de handhavingsketen kan doen om te interveniëren. Ik kan mij voorstellen dat een organisatie als de AIVD dat op hun eigen niveau al doet, maar dan heb je het meer over statelijke actoren. Wij doen iets vergelijkbaar, maar dan veel meer op microniveau. Het is nodig dat op alle niveaus de handhavingsketen online veel meer ruimte inneemt. Dat de sirenes die je in een wijk hoort, ook online te horen zijn. Ongeacht of die zichtbare handhaving nu door de blauwe wijkteams van de Politie, door de MIVD of de AIVD wordt uitgevoerd, het gaat er om dát het gebeurt.”

BACK TO TOP

Photo: Hollandse Hoogte

“Het bij elkaar brengen van expertise is echt de sleutel in het succesvol aanpakken van cybercrime.”

‘You need to bring al expertise together to tackle cybercrime effectively.’

different police divisions are working together to fight cybercrime and don't leave it all up to a small group of specialists in the criminal investigation department. However, we should also involve external parties in this holistic approach. That should be a lesson to everyone involved: always work with parties involved in the fight against cybercrime or others that are simply prepared to take responsibility for the issue. Each organisation oversees a different aspect of the problem, and they all have their own areas of expertise, mandates and networks. You need to bring all that expertise together if you aim to tackle cybercrime effectively; that way, you'll be able to achieve a level of impact that you couldn't have otherwise.’

The police are also working with other enforcement agencies, such as the Public Prosecution Service, the National Cyber Security Centre (NCSC), the Digital Trust Center (DTC), the Military Intelligence and Security Service (MIVD) and the General Intelligence and Security Service (AIVD). ‘We launched the NoMoreRansom platform a few years ago. It's a typical example of a holistic approach involving a wide range of organisations. The platform eventually evolved into the Ransomware Taskforce, which doesn't just focus on resolving ransomware incidents. After all, that kind of one-sided approach is far too ineffective. Instead, the Ransomware Taskforce starts by identifying the jumble of ransomware variants and ransomware services in order to pinpoint the most important actors. They are then singled out in collaboration with private sector partners in order to target the criminal group or process as effectively as possible. The effort to take down the Emotet botnet prevented far more ransomware infections than we ever could have resolved after the fact.’

Strengthening enforcement chain

Clearly, there have already been significant joint efforts to develop a holistic approach to cybercrime. However, Jansen still sees further scope to strengthen the enforcement chain. ‘The launch of the COPS team would be a good case in point. As part of our mission, we also work to involve the law enforcement chain much more closely in cyber issues. We want to encourage a proactive approach rather than a purely reactive one. It would be a waste to just keep waiting for things to go wrong and then tracking down and prosecuting the perpetrators. That's like filling a bucket full of holes. Offender prevention and efforts to strengthen the enforcement chain can help us mend that bucket.’

‘The enforcement chain contains a great deal of expertise and knowledge: every organisation has its own particular approach and methods. Why not harness that knowledge in the fight against cybercrime? However, those organisations still don't know their way around the cyber arena that well. That's where we come in: we need to support the enforcement chain so that they can also apply their methods online.’

‘It's not just about knowledge sharing and detecting cybercrime; we need to figure out how the enforcement chain can intervene most effectively. I would imagine an organisation like the AIVD is already doing that at their own level, but those are state actors. We're doing something comparable, but aimed at (wannabe) criminals. The enforcement chain really needs to expand its online presence at every level. You need to make sure the sirens you hear on the street are also audible online. It doesn't matter whether these visible forms of enforcement are carried out by community police teams, the MIVD or the AIVD: as long as it gets done.’

THEO HENRAR

Nieuw lid van de Cyber Security Raad (CSR)

New member of the Dutch Cyber Security Council (CSR)

Op 17 juni 2021 is Theo Henrar aangetreden als voorzitter van FME, de ondernemersorganisatie voor de technologische industrie. Daarnaast is Henrar ook voorzitter van de Raad van Commissarissen van Zeehaven IJmuiden. Sinds zijn benoeming als voorzitter bij FME is Theo Henrar ook lid van de CSR namens FME.

On 17 June 2021, Theo Henrar was appointed President of FME, the employers' organisation for the technology industry. Henrar is also President of the Supervisory Board of IJmuiden Seaport. Since being named president of FME, Theo Henrar has additionally served as CSR member representing FME.

Kunt u uzelf voorstellen en een korte beschrijving van uw profiel geven?
"Als ambassadeur van de industrie vind ik mijn benoeming als voorzitter van FME een heel mooi vervolg van mijn carrière. Mijn kennis en ervaring die ik tijdens mijn loopbaan heb opgedaan, komt daarbij goed van pas. Zo heb ik verschillende functies bekleed bij Tata Steel/ Corus Group de industrie, zowel in de verkoop als in de productie en productieplanning en als algemeen manager in Nederland en het Verenigd Koninkrijk. Na de fusie tussen Hoogovens en British Steel tot Corus Group heb ik de European Market Unit gereorganiseerd en was ik managing director van veertig staalservice centers in het Verenigd Koninkrijk en het Europese vasteland. Daarna werd ik in 2007 algemeen directeur van Corus Packaging Plus met vestigingen in het Verenigd Koninkrijk, Noorwegen, België en Nederland. In 2008 werd ik benoemd tot directievoorzitter van Tata Steel Nederland/Corus Nederland. Tijdens mijn militaire diensttijd heb ik ook gediend als reserveofficier als secretaris van de directeur Algemene Zaken van het Ministerie van Defensie."

Would you mind introducing yourself and sharing a brief description of your background?
'As an ambassador for the industrial sector, I view my appointment as President of FME as a fine next step in my career. The knowledge and experience I have amassed during my career will serve me well in this capacity. I have, for instance, held various positions with Tata Steel/Corus Group, both in sales and in manufacturing and production planning, including a position as General Manager in the Netherlands and the United Kingdom. After Hoogovens and British Steel merged to form Corus Group, I oversaw the reorganisation of the European Market Unit and was Managing Director of 40 steel service centres in the United Kingdom and on the European mainland. In 2007, I then became General Manager of Corus Packaging Plus, which has branch locations in the United Kingdom, Norway, Belgium and the Netherlands. In 2008, I was named Executive Chairman of Tata Steel Netherlands/Corus Netherlands. During my time as a reserve officer in the military, I also served as secretary to the Director of General Affairs at the Dutch Ministry of Defence.'

Photo: Arenda Oomen

Onlangs bent u aangesteld als voorzitter FME, wat is u missie als het gaat om de cyberweerbaarheid van onze samenleving en wat neemt u daarvan mee in uw rol als lid van de CSR?
"De digitale en fysieke wereld zijn stevig met elkaar vervlochten. Hierdoor leiden digitale incidenten steeds vaker tot ernstige verstoring van belangrijke (industriële) processen. Het is onmogelijk om deze incidenten en de hierop volgende maatschappelijke ontwrichting in alle gevallen te voorkomen.
Ik ben ervan overtuigd dat de bewustwording van deze reële dreiging continu gestimuleerd moet worden. Dit stelt private organisaties en betrokken publieke instanties in staat om te anticiperen op de uitval van belangrijke processen. Het is dan ook erg belangrijk om de digitale en fysieke respons in crisissituaties te oefenen. De resultaten van oefeningen kunnen worden gebruikt om rollen, mandaten of in te zetten middelen binnen publieke en private organisaties op elkaar af te stemmen. Dit draagt bij aan het verhogen van de digitale weerbaarheid van de samenleving als geheel."

Wat is de toegevoegde waarde van een integrale aanpak cyberweerbaarheid voor uw achterban?
"Een integrale aanpak voor de cyberweer-baarheid van onze samenleving is van groot belang. Bedrijven staan immers allang niet meer op zichzelf, maar maken deel uit van een ecosysteem binnen grote, vaak internationale, toeleveringsketens. Daarom is het belangrijk om ook binnen de EU met elkaar op te trekken. Cybercriminelen houden zich immers niet aan landsgrenzen. Als lid van de raad zal ik vooral aandacht blijven vragen voor de beperkte omvang van de hulpmiddelen die middelgrote en kleine bedrijven tot hun beschikking hebben. Inzetten op de intensivering van publiek-private samenwerking is de snelste route naar een betere weerbaarheid van het Nederlandse bedrijfsleven."

You were recently appointed President of FME. What is your mission with regard to the digital resilience of our society and how do you intend to incorporate this into your role as a member of the CSR?
'The digital and physical worlds are firmly intertwined. Because of this, digital incidents are more often resulting in serious disruptions to important processes, both industrial and otherwise. It is impossible to prevent such incidents – and the ensuing social disruption – in every single case. I firmly believe that we must constantly foster awareness of this very real threat. Doing so will enable private organisations and the relevant public authorities to anticipate interruptions to vital processes. It is similarly important to rehearse the digital and physical response to be taken in crisis situations. The results of these drills can be used to coordinate the roles, mandates and resources available for deployment within public and private organisations. This, in turn, will contribute to enhancing the digital resilience of society as a whole.'

How will an integral approach to digital resilience add value for your constituents?
'An integral approach to the digital resilience of our society is of vital importance. After all: companies have long since ceased to operate independently of one another. Instead, they are part of an ecosystem that exists within large, often international supply chains. In that light, it is important to coordinate our approach at the level of the EU as well. We know that cybercriminals are not deterred by national borders. As a member of the CSR, my primary focus will be drawing continuous attention to the limited scope of the resources medium-sized and small enterprises have at their disposal. Investing in the intensification of public-private partnerships is the fastest route to achieving greater resilience for the Dutch business community.'

Cyberaanvallen zijn aan de orde van de dag. De nog steeds voortdurende coronapandemie heeft er bovendien voor gezorgd dat het aantal in rap tempo steeds verder toeneemt. Het dwingt bedrijven een digitale inhaalslag te maken om het werken op afstand mogelijk te maken. Daarmee zijn we steeds meer digitaal afhankelijker geworden. Tegelijkertijd wordt Nederland geconfronteerd met nieuwe dreigingen, een toename van cybercrime en neemt het aantal incidenten toe. Zo is het aantal cyberaanvallen in het afgelopen jaar opnieuw enorm gestegen. Het meest recente voorval vond plaats bij de VDL Groep die werd geraakt door gijzelsoftware. Hierdoor kwam een groot deel van de productie stil te liggen. Ditzelfde overkwam vorig jaar ook de Mandemakers Groep (DMG). Daarnaast herinneren we ons allemaal nog de beruchte 'kaashack' van een grote supermarktketen waarbij de hack voor lege kaasschappen in de supermarkt heeft gezorgd.

Cyber-attacks have become a daily occurrence – and the ongoing COVID-19 pandemic is yielding a further, rapid increase in the number of incidents. The pandemic has forced businesses to take a digital leap forward in order to facilitate remote working. This has increased the digital dependence of the Netherlands. At the same time, the country faces new threats, an increase in cybercrime and a growing number of incidents. Once again, the number of cyber-attacks has risen tremendously over the past year. The most recent incident was a ransomware attack aimed at the VDL Group, which brought the majority of their production activities to a standstill. The same thing happened to the Mandemakers Group (DMG) last year as well. And no doubt we all remember the infamous 'cheese hack' of a major supermarket chain, which resulted in empty cheese cases in their stores.

WE CANNOT AFFORD TO RELAX

Direct and indirect losses
Along with the growing number of cyber-attacks, the losses incurred are increasing as well. It is incredibly difficult to gain a picture of the total losses caused by cybercrime, as these losses are both direct and indirect. What's more, not all businesses file a police report when they have been victimised by cybercriminals. Annual reports from Europol, however, show that in some countries, cybercrime and cyber-enabled crime are already much more common than traditional forms of criminality. I think this offers a good idea of the expanding size of the problem.

We cannot afford to relax
So far, the Netherlands has been spared drastic consequences as a result of cyber-attacks. Both public and private parties are investing and working hard to achieve a digitally resilient society. Despite the positive steps we are taking, the digital resilience of the Netherlands is not yet sufficient in all areas – and this leaves us vulnerable. We therefore cannot and must not sit back and relax: what will happen, for example, if every hospital in the country is attacked at once? Or what might happen if all the systems connected to our water grid are hacked, or how about our traffic systems or payment transactions? These are scenarios that could lead to a national disaster. If we are to remain an open, free and prosperous society in the future, more extensive action must be taken soon. The Dutch Cyber Security Council (CSR) has issued a great recommendation in this area and I sincerely hope that the new government will follow up on their advice.

Sharing is the new ownership
As a new CSR member representing FME, I endorse the recommendations issued by the council. I'd also like to touch on a few points specifically. At FME, our motto is 'sharing is the new ownership'. I consider it crucial that information regarding digital threats be made available to all businesses and organisations, both critical and non-critical, with special attention to small and medium-sized enterprises. Fortunately, there is a legislative amendment in the pipeline that will ensure our ability to achieve a nationwide network with actual, nationwide coverage. But none of us can do this alone. Only by cooperating and exchanging information can we strengthen the digital resilience of the Netherlands, together. Cyber exercises are also important in this regard, and we at FME deliver a vital contribution to such drills. Last year, for example, FME worked with the Dutch Ministry of Defence to organise a cyber exercise, which participants found to be quite valuable. In addition to knowledge and experience about what to do – and more importantly, what not to do – in case of a cyber-attack, such exercises also help strengthen mutual trust and shared knowledge with regard to cybersecurity.
The Netherlands has a strong need for this knowledge in particular, as the growing shortage of cybersecurity specialists poses an urgent challenge. More and more Dutch experts with cyber-related talents in the scientific and social domains are choosing to move abroad, simply because there is more money available for research, education and innovation in other countries. This is not conducive to rectifying our existing shortage of sufficiently qualified specialists in the field of cybersecurity. It is therefore absolutely imperative that we halt the current academic brain drain.

Theo Henrar
President FME, CSR member representing FME

"Ondanks alle goede stappen die we zetten, is onze cyberweerbaarheid nog niet overal voldoende op orde en dat maakt ons kwetsbaar."
'Despite the positive steps we are taking, the digital resilience of the Netherlands is not yet sufficient in all areas – and this leaves us vulnerable.'

Naast een toename van het aantal cyberaanvallen, stijgt ook het schadebedrag steeds verder. De totale schade van cybercrime is ontzettend moeilijk zichtbaar te maken. Dit komt omdat er sprake is van zowel directe als indirecte schade. Daarnaast doen ook niet alle bedrijven aangifte wanneer zij slachtoffer zijn geworden van cybercriminelen. Jaarverslagen van Europol laten echter zien dat *cybercrime* en *cyber enabled crime* in sommige landen al veel groter is dan traditionele vormen van criminaliteit. Dit geeft naar mijn idee wel een goed beeld van de toenemende omvang.

Niet achteroverleunen
Tot op heden hebben cyberaanvallen in ons land nog geen grootse gevolgen gehad. Er wordt dan ook door zowel publieke als private partijen hard gewerkt en geïnvesteerd in een cyberweerbare samenleving. Ondanks alle goede stappen die we zetten, is onze cyberweerbaarheid nog niet overal voldoende op orde en dat maakt ons kwetsbaar. We kunnen en mogen daarom niet achteroverleunen, want wat gebeurt er als alle ziekenhuizen in Nederland bijvoorbeeld gelijktijdig aangevallen worden? Of wat gebeurt er als alle systemen voor ons waternet gehackt worden of wat te denken van onze verkeerssystemen of het betalingsverkeer? Het zijn scenario's die kunnen leiden tot een nationale ramp. Om ook in de toekomst een open, vrije en welvarende (digitale) samenleving te zijn, moeten er snel grotere stappen gezet worden. De Cyber Security Raad (CSR) heeft hierover een mooi advies uitgebracht en ik hoop van harte dat het nieuwe kabinet hier gevolg aan gaat geven.

Delen is het nieuwe hebben
Als nieuw lid van de CSR namens FME onderschrijf ik het advies dat de raad heeft uitgebracht. Een aantal punten wil ik daarbij specifiek aanhalen. Vanuit FME is ons credo 'delen is het nieuwe hebben'. Ik vind het van groot belang dat informatie over cyberdreigingen voor alle bedrijven en organisaties beschikbaar is, vitaal en niet-vitaal, met extra aandacht voor het midden- en kleinbedrijf. Gelukkig is er een wetswijziging in de maak dat ervoor gaat zorgen dat we het landelijk dekkend stelsel ook echt dekkend kunnen gaan maken. Maar daarvoor hebben we elkaar nodig. Alleen door samenwerking en informatiedeling kunnen we met elkaar de cyberweerbaarheid van Nederland versterken. Cyberoefeningen zijn daarbij ook van groot belang en daar leveren we vanuit FME een belangrijke bijdrage aan. Zo heeft FME vorig jaar samen met het ministerie van Defensie ook een cyberoefening georganiseerd, die door de deelnemers als zeer waardevol is ervaren. Naast alle kennis en ervaring over wat wel en vooral niet te doen bij een cyberaanval, dragen dergelijke oefeningen ook bij aan het vergroten van onderling vertrouwen en kennis over cybersecurity. Vooral die kennis hebben we in Nederland heel hard nodig, want het toenemende tekort aan cybersecurityspecialisten is een prangend probleem. Zo vertrekt steeds meer wetenschappelijk en maatschappelijk Nederlands cybertalent naar het buitenland, omdat daar simpel weg meer geld beschikbaar is voor onderzoek, onderwijs en innovatie. Dit komt het huidige tekort aan voldoende gekwalificeerde specialisten in het cybersecuritydomein niet ten goede. Deze huidige academische *braindrain* moeten we daarom echt een halt toegeroepen.

Theo Henrar, Voorzitter FME

BACK TO TOP

Juhan Lepassaar
Executive Director of the European Union Agency for Cybersecurity, ENISA

CERTIFYING CYBERSECURITY PREPAREDNESS ON EU-LEVEL

Juhan Lepassaar, Executive Director of the European Union Agency for Cybersecurity (ENISA), has dedicated most of his career to the European Union in his home country of Estonia, in the EU affairs department of the Government Office. But also in Brussels, where he worked for the European Commission with Vice-President Andrus Ansip who was responsible for the Digital Single Market. He joined ENISA as Executive Director on 16 October 2019.

When ENISA was founded in 2004, there was a need to strengthen the overall level of cybersecurity in the European Union (EU). There was also a need to support the development and implementation of cybersecurity policies according to Lepassaar. 'Despite the uncertainties in the beginning, ENISA managed to build a strong reputation over the years. ENISA is working on different cybersecurity fronts and cooperates today with national cybersecurity authorities, with EU institutions, bodies and agencies, but also with private stakeholders around essential cybersecurity priorities for the European Union. With the Cybersecurity Act of 2019, the Agency's mandate expanded further in the area of operational cooperation when a large-scale cross-border cyber crisis occurs and provides a role to ENISA to draft EU cybersecurity certification schemes.'

Supporting European countries to be cyber secure

ENISA has been supporting Member States in the development and review of their cybersecurity strategies. The Agency has also been organising trainings and exercises involving Computer Incidents Response Teams (CSIRTs) and is engaged in a number of initiatives to support the cybersecurity community at large. Lepassaar: 'In short, ENISA has developed into a fully fledge organisation supporting the Member States and the EU Institutions, agencies and bodies. In doing so we have reached this level of maturity I see today and which is absolutely essential for the new tasks ahead of us.'

Photo: Enisa

The Cybersecurity Act (CSA, which came into effect on 27 June 2019) marks a new era in terms of the evolution of ENISA and of the positioning of the EU in the global cybersecurity landscape. What are these new roles? Lepassaar explains that ENISA supports the European Commission in relation to its cybersecurity certification policy which aims at enhancing the level of trust in the digital single market. 'In accordance with the provision of the CSA, ENISA received the request on common criteria for products known as EUCC (Common Criteria based European Candidate Cybersecurity Certification Scheme) for the use in chips and smart cards. ENISA transmitted this first scheme to the European Commission for approval in May this year. We are also developing a candidate scheme on cloud services. This EU Cloud Services cybersecurity certification scheme was in its first draft published for public consultation at the end of December 2020. Another development. In January 2021 the EC came with the request for the development of a new certification scheme for 5G and therefore ENISA is working on the establishment of ad hoc working group on 5G.Additionally to certification, ENISA has a new role that includes the analyses of main trends in the cybersecurity market on both the demand and supply sides.'

> 'The Cybersecurity Act marks a new era in terms of the evolution of ENISA and of the positioning of the EU in the global cybersecurity landscape.'

Significance and opportunities of EU-wide certification

The EU cybersecurity certification framework lays down the conditions needed to increase trust and security in ICT products, services and processes. Lepassaar declares that the digital single market can only thrive if there is general public trust that all such products, services and processes provide a certain level of cybersecurity. 'In order to implement such new certification framework at EU level, ENISA seeks international interoperability and compliance with international standards, and assists public authorities in the Member States as well as the Commission.'

Drawing up cybersecurity certification schemes at EU level serves the purpose of providing criteria to carry out high-level conformity assessments to establish how products, services

and processes meet specific requirements. Lepassaar: ‘Each scheme will specify one or more level(s) of assurance such as basic, substantial or high on the basis of the level of risk associated with the envisioned use of the product, service or process. The extensive research and consultation performed will allow to draft comprehensive schemes tailored to the needs of Member States with whom ENISA engages to the purpose of geographically defragmenting the internal market. Union-wide mechanisms of certification will allow European businesses to compete at national, Union and global level.’

Minimum standards on cybersecurity

The Cybersecurity Act does not include instruments to force suppliers to adhere to minimum cybersecurity standards. Instead, it foresees a series of measures to facilitate and promote the uptake of cybersecurity standards, Lepassaar explains. ‘First, it foresees the aforementioned development of EU certification schemes for ICT products, processes or services. An EU certification scheme will contain several elements e.g. security requirements, specification of approved evaluation methods, etcetera. Certifications issued under such schemes are expected to be recognised in all Member States, thus certifying that specified security requirements are met. This will make it easier for enterprises to trade across borders and for users to understand the security features of products and services. In other words, EU certification schemes are expected to also represent an incentive for suppliers to adhere to cybersecurity standards. Second, ENISA facilitates the establishment and take-up of European and international standards for risk management and for the security of ICT products, services and processes in general. In collaboration with Member States and industry, ENISA provides advice and guidelines regarding standards as well as the technical areas related to the security requirements for operators of essential services and digital service providers. Third, ENISA assists in the development and implementation of Union policy and law. In this context the role of ENISA is to facilitate the implementation of the NIS directive, requiring specific entites - such as operators of essential services - minimum security levels to be maintained based on cybersecurity standards. Last but not least, the CSA gives ENISA the mandate to raise public awareness on cybersecurity risks and threats, and to provide guidance on good practices for businesses. Awareness raising actions are important to inform suppliers on the cybersecurity risks associated with their activities.’

ENISA has only just submitted the first candidate cybersecurity scheme on Common Criteria based European Candidate Cybersecurity Certification Scheme (EUCC) to the European Commission for approval. Lepassaar: 'It is too early to say something about the results like the number of countries and suppliers certifying their products and services. For the moment Member States who developed national certification schemes are already certifying these. Certification obviously attracts the attention of suppliers who wish to add an extra layer of assurance to their customers. ENISA cooperates closely with Member States and with industry to decide on requirements and the way forward for the benefit of the EU as a whole.’

The Cybersecurity Act makes cybersecurity certification voluntary unless Union law or Member State law includes provisions to the contrary. According to Lepassaar the European Commission will regularly assess the efficiency and use of the adopted EU cybersecurity certification schemes and whether an EU scheme is to be made mandatory through Union Law. ‘The first assessment is expected to be carried out by 31st December 2023. It is on the basis of these assessments that the Commission will be deciding which products, services and/or processes covered by an existing scheme which will have to be covered by a mandatory certification scheme.’

Guiding Small and Medium-sized Enterprises (SMEs)

Over the past two years ENISA has issued a number of recommendations and reports to guide SMEs. In addition, ENISA just released a “SecureSME tool” meant to facilitate the navigation into the different tips, guidelines and recommendation of ENISA on cybersecurity for small and medium-sized companies. Lepassaar: ‘For instance, it is important for SMEs to develop an incident response plan which would include guidelines, define roles and responsibilities to ensure that incidents are responded to in an adequate, timely and professional way. SMEs can investigate tools to monitor and create alerts should suspicious activity or security breaches occur. Securing devices by keeping software patched and up to date is another recommendation. These are only examples from the cybersecurity guide for SMEs ENISA recently published and made available in another ten European languages. Besides, ENISA supports Member States in the development of the national cybersecurity strategies to be in line with the new cybersecurity strategy of the Union and thus raise standards to a similar high level of security across Member States as provided for by the NIS directive. ENISA has recently issued a National Capabilities Assessment Framework (NCAF) in order to help EU Member States self-measure the level of maturity of their national cybersecurity capabilities.’

‘The Cybersecurity Act makes cybersecurity certification voluntary unless Union law or Member State law includes provisions to the contrary’

Challenges and opportunities

The digital world is a fast one is the opinion of Lepassaar. ‘This is why ENISA needs to be even faster. Part of our job at ENISA is to spot and anticipate the challenges lurking in the corner and track the opportunities at hand. Some of the challenges, except for the development of the certification schemes include Artificial Intelligence, 5G and possibly post-quantum cryptography. Artificial Intelligence, even if not new in itself has not yet been fully analysed in terms of cybersecurity.’ Lepassaar explains that it is highly complex, given its nature and its very different and wide applications. ‘Cryptography and post-quantum cryptography are very serious and I would say quite sensitve topics too. In this area, we need to anticipate the future, even if we cannot be sure what it holds. Quantum computing, if it ever becomes a reality, will be threatening the security of the technologies we use today because it will have the capacity to break into our current security systems. We do not want to jeopardise our digital resilience and to do that we need to build it today as wisely as possible. As I said, technologies develop extremely fast. We need to keep in mind that anything we use today might become completely obsolete and inefficient tomorrow because of emerging new equipments and technologies. So, I would say that to enhance digital resilience of products and services, ENISA’s role is to correctly assess the threat landscape and to disseminate information on the best security controls and good practices. Beyond these practical aspects, the challenge is to ensure Member States are equipped with up-to-date knowledge and tools to allow informed decision-making to drive the policy initiatives.’

‘In the end, I would say that, the way ENISA has evolved and the level of cooperation we have reached today across the EU has really open the door to a lot of opportunities in terms of information sharing and created important synergies.’

‘Quantum computing, if it ever becomes a reality, will be threatening the security of the technologies we use today.’

BACK TO TOP

NEXT

Photo: Nationale Beeldbank

SAMENSTELLING CYBER SECURITY RAAD (CSR)

COMPOSITION OF THE DUTCH CYBER SECURITY COUNCIL (CSR)

PRIVATE SECTOR
PRIVATE SECTOR

Mw. mr. drs. S.C. (Sylvia) van Es (covoorzitter)
President Philips Nederland, lid van CSR namens VNO-NCW

Mrs S.C. (Sylvia) van Es LLM
President Philips the Netherlands, CSR member representing VNO-NCW

Mw. drs. C. (Claudia) de Andrade-de Wit
CIO, Directeur Digital & IT Haven Rotterdam, lid van CSR namens het CIO Platform

Mrs C. (Claudia) de Andrade-de Wit MA
CIO, Director Digital & IT Port of Rotterdam and boardmember CIO Platform, CSR member representing CIO Platform

Dhr. W. (Wiebe) Draijer
Voorzitter van de groepsdirectie van de Rabobank en bestuurslid van de Nederlandse Vereniging van Banken, lid van CSR namens de financiële sector

Mr W. (Wiebe) Draijer
Chair of the group management of Rabobank and council member of the Dutch Banking Association, CSR member representing the financial sector

Dhr. mr. J. (Joost) Farwerck
CEO en voorzitter van de Raad van Bestuur bij KPN, lid van CSR namens de vitale infrastructuur

Mr J.F.E. (Joost) Farwerck LLM
CEO KPN and Chairman of KPN's Board of Management, CSR member representing the vital sectors

Dhr. mr. Th.J. (Theo) Henrar
Voorzitter FME (ondernemers-organisatie voor de technologische industrie), lid van CSR namens FME

Mr Th.J. (Theo) Henrar LLM
President FME (the Dutch employers' organisation in the technology industry), CSR member representing FME

Mw. T. (Tineke) Netelenbos
Voorzitter ECP, lid van CSR namens ECP, Platform voor de Informatie-samenleving

Mrs T. (Tineke) Netelenbos
Chair of ECP, Platform for the information society

Dhr. mr. P. (Peter) Zijlema
General Manager IBM Benelux / Country General Manager IBM Netherlands, lid van CSR namens NLdigital

Mr P. (Peter) Zijlema LLM
General Manager IBM Benelux / Country General Manager IBM Netherlands, CSR member respresenting NLdigital

PUBLIEKE SECTOR
PUBLIEKE SECTOR

Dhr. P.J. (Pieter-Jaap) Aalbersberg EMPM (covoorzitter)
Nationaal Coördinator Terrorisme-bestrijding en Veiligheid (NCTV)

Mr P.J. (Pieter-Jaap) Aalbersberg EMPM (co-chair)
National Coordinator for Security and Counterterrorism

Dhr. drs. E.S.M. (Erik) Akerboom MPM
Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Mr E.S.M. (Erik) Akerboom MA EMPM
Director-General of the General Intelligence and Security Service (AIVD)

Dhr. vice-admiraal B.G.F.M. (Boudewijn) Boots
Plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie

Mr Vice Admiral B.G.F.M. (Boudewijn) Boots
Deputy Commander of the Armed Forces, Ministry of Defence

Dhr. mr. G.W. (Gerrit) van der Burg
Voorzitter van het College van procureurs-generaal

Mr G.W. (Gerrit) van der Burg LLM
Chairman of the Board of Prosecutors-General

Dhr. mr. H.P. (Henk) van Essen
Korpschef Politie

Mr H.P. (Henk) van Essen, LLM
National Police Chief

Dhr. drs. F.W. (Focco) Vijselaar
Directeur-Generaal Bedrijfsleven en Innovatie bij het ministerie van Economische Zaken en Klimaat

Mr F.W. (Focco) Vijselaar MA
Director-General Industry and Innovation, Ministry of Economic Affairs and Climate Policy

Mw. drs. M. (Marieke) van Wallenburg
Directeur-Generaal Overheids-organisatie bij het ministerie van Binnenlandse Zaken en Koninkrijks-relaties

Mrs M. (Marieke) van Wallenburg MA
Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations

WETENSCHAPPELIJKE SECTOR
SCIENCE SECTOR

Mw. prof. dr. B. (Bibi) van den Berg
Hoogleraar Cybersecurity Governance verbonden aan het Institute of Security and Global Affairs van Universiteit Leiden

Mrs prof. dr. B. (Bibi) van den Berg
Professor of Cybersecurity Governance attached to the Institute of Security and Global Affairs, Leiden University

Dhr. prof. dr. M.J.G. (Michel) van Eeten
Hoogleraar Cybersecurity TU Delft

Mr prof. dr. M.J.G.(Michel) van Eeten
Professor Governance of Cybersecurity, Delft University of Technology

Dhr. prof. dr. B.P.F. (Bart) Jacobs
Hoogleraar Computerbeveiliging Radboud Universiteit Nijmegen

Mr prof. dr. B.P.F. (Bart) Jacobs
Professor of Software Security and Correctness, Radboud University Nijmegen

Miranda Koopman

Mw. prof. mr. E.M.L. (Lokke) Moerel
Senior Of Counsel Morrison & Foerster LLP, Hoogleraar Universiteit Tilburg

Mrs prof. E.M.L. (Lokke) Moerel LL.M.
Senior of Counsel Morrison & Foerster & Professor Global ICT Law, Tilburg University

SECRETARIS
SECRETARY

Mw. drs. E.C. (Elly) van den Heuvel-Davies

Mrs E.C. (Elly) van den Heuvel-Davies MA

e.c.van.den.heuvel@cybersecurityraad.nl

BACK TO TOP

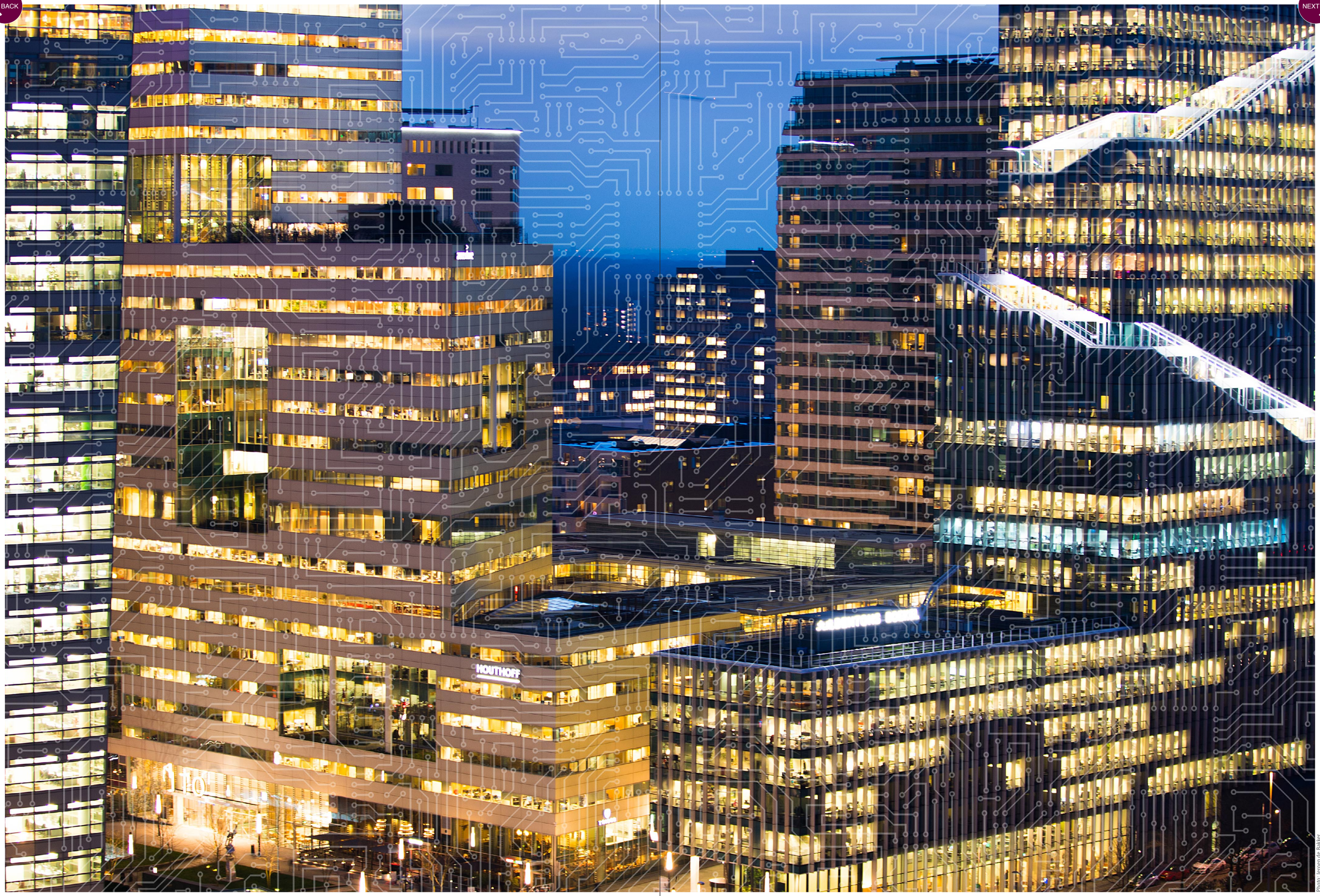


Photo: Jeroen de Bakker

Colofon | Colophon

Opdrachtgever | Commissioning party: **Cyber Security Raad Nederland** | Dutch Cyber Security Council
Hoofdredactie | Chief editor: **Elly van den Heuvel-Davies (secretaris |** secretary)
Concept en (eind)redactie | Concept and (final) editing: **Heidi Letter, Ouiam Yachou**
Met dank aan | With thanks to: **Marije van Schaik (CSR), Tim Puts (CSR), Sandra Veen (CSR), BKB**
Fotografie | Photography: **Arenda Oomen Fotografie, Jeroen de Bakker, ANP foto, Hollandse Hoogte, Nationale Beeldbank, De Beeldunie, Agentschap Telecom, KPN, ENISA, Eric Fecken. NCSC Press Office (UK)**
Vertalingen | Translations: **Metamorfose Vertalingen • Opmaak** | Layout: **BKB • Drukwerk** | Printwork: **Xerox**

February 2022

CSR
Cyber Security Council
Cyber Security Raad