CSR MAGAZINE

Cyber Security Council
Cyber Security Raad

Naar een open, veilig en welvarend digitaal Nederland • Top van Nederland aan het woord over de digitale veiligheid van Nederland, in Europa en wereldwijd.

Towards an open, secure and prosperous digital Netherlands • High level government officials and businessleaders speaking about cybersecurity in the Netherlands, across Europe and worldwide.

Jaargang 4, nummer 1, september 2018
Volume 4, Issue 1, September 2018

“De toekomst hang af van wat je nu aan het doen bent”

“The future depends on what you do today”

“De toekomst hangt af van wat je nu aan het doen bent”, een beroemde uitspraak van Mahatma Gandhi. Het is niet voor niets dat we juist deze quote hebben gepubliceerd in de CSR Meerjarenstrategie 2018-2021. De thema’s uit de meerjarenstrategie, te weten regie en sturing, groeiende (digitale) afhankelijkheid, handhaving en toezicht en nieuwe technologieën, staan centraal in deze editie van CSR Magazine. Nederland is één van de meest ICT-intensieve economieën van Europa. Digitalisering biedt enorme kansen voor de samenleving en economie, maar dan is het wel zaak te zorgen dat de digitale wereld veilig en vertrouwd blijft, nu en in de toekomst. In deze editie van CSR Magazine geven verschillende topfunctionarissen uit overheid en bedrijfsleven vanuit hun eigen expertise een visie op hoe we hier in Nederland, Europa en wereldwijd vorm aan kunnen geven. Allen zijn zij van mening dat Nederland op de goede weg is bij het verder versterken van de digitale veiligheid alsook op het gebied van onderzoek, innovatie en andere initiatieven. We zijn echter nog onvoldoende cyberready. Een rode draad in alle kritische noten die u in de artikelen kunt lezen is toch wel samenwerking. Samenwerking tussen overheid, bedrijven, organisaties en burgers is belangrijk om Nederland digitaal veilig te houden; we willen en kunnen het niet alleen. Dit stopt niet bij de grens; ook internationaal moeten we de handen ineen slaan. De recent ontwikkelde Cybersecurity Health Check is een mooi voorbeeld van samenwerking. Op verzoek van de raad hebben de vier accountantsorganisaties Deloitte, EY, KPMG en PwC hun kennis en ervaring over cybersecurity gebundeld in de Cybersecurity Health Check. Dit instrument zal in de vorm van een handreiking van de Beroepsorganisatie van Accountants (NBA) worden verspreid onder de accountants in Nederland. Verder zijn de topfunctionarissen het erover eens dat er blijvend geïnvesteerd moet worden in cybersecurity, vooral ook in kennis.

Met de investering van 95 miljoen euro in cybersecurity heeft het kabinet een eerste belangrijke stap gezet. Daarmee zijn we er nog niet; er zullen meer stappen moeten worden gezet naar de toekomst toe om ons te kunnen wapenen tegen statelijke actoren en de toenemende georganiseerde misdaad. Alleen zo kunnen we in Nederland blijvend de kansen verzilveren en innovatie bevorderen, nu en in de toekomst!

Namens de Cyber Security Raad,
Dick Schoof en Jos Nijhuis

Mahatma Ghandi famously said: 'The future depends on what you do today'. It’s no coincidence we chose to include this quote in the CSR Multi-annual strategy 2018-2021. The themes from that multi-annual strategy – supervision and guidance, growing dependence on (digital) technologies, enforcement and monitoring, and new technologies – take centre stage in this edition of the CSR Magazine. The Netherlands is one of the most ICT-intensive economies in Europe. While digitalisation offers vast opportunities for society and the economy, it is vital to ensure the digital world remains safe and reliable – now and in the future. In this edition of the CSR Magazine, various senior government officials and business leaders speak from their own expertise in offering their views on how we can realise this intent in the Netherlands, across Europe and worldwide. Each and every one of them feels the Netherlands is on the right path when it comes to reinforcing digital security, including in the areas of research, innovation and other initiatives. Still, our current cyber-readiness is insufficient. A recurring theme among the critical remarks you will encounter in these articles is that of cooperation. Cooperation between government, businesses, organisations and members of the public is vital to maintaining the cybersecurity of the Netherlands: we cannot do it alone, nor do we wish to. This does not stop at the border: international collaboration is required as well. The recently developed Cybersecurity Health Check is a fine example of such cooperation. At the council's request, the four accountancy firms Deloitte, EY, KPMG and PwC have brought all their cybersecurity-related knowledge and experience together in the Cybersecurity Health Check. This instrument will be distributed among accountants in the Netherlands in the form of guidelines issued by the Institute of Chartered Accountants (NBA). The senior executives additionally agree that there is a need for structural investment in cybersecurity, and in knowledge in particular. By investing €95 million in cybersecurity, the government has taken an important first step. Yet this will not fully suffice: more steps will have to be taken with the future in mind in order to defend ourselves against state actors and increasing organised crime. Only then will the Netherlands be able to continue to profit from economic opportunities and encourage innovation, now and in the future!

On behalf of the Cyber Security Council,
Dick Schoof en Jos Nijhuis

4 **Time to buckle up**
Ferd Grapperhaus, Minister of Justice and Security

6 **Cybersecurity in the Netherlands**
an overview

9 **Towards a digitally secure Netherlands**
Patricia Zorko, Deputy National Coordinator for Security and Counterterrorism (NCTV) and Director of Cybersecurity

12 **Digitalisation and the new government**
Sandor Gaastra, Director-General for Energy, Telecommunications and Competition at the Ministry of Economic Affairs and Climate Policy

14 **Espionage, influencing, disruption and sabotage**
Sebastian Reyn, Director-General of Integrated Policy at the Ministry of Defence

17 **Tackling cybercrime: choosing the most effective intervention**
Erik Akerboom, Chief of the Dutch National Police

21 **‘When it comes to security, there is no competition’**
Joost Farwerck, Chief Operations Officer and member of the executive board of KPN

25 **The enemy enters through the wall outlet**
Ineke Dezentjé Hamming-Bluemink, President and General Manager of FME

27 **‘A more holistic approach is needed’**
Director Petra Oldengarm and Policy Advisor Liesbeth Holterman of Cyberveilig Nederland

31 **Keeping "dry feet" in the digital era: cybersecurity is an enduring issue**
Herna Verhagen, CEO of PostNL

34 **Ambition vs. Progress: The National Cybersecurity Agenda of the Netherlands**
Melissa Hathaway, leading expert in cyberspace policy and cybersecurity

37 **A Strategy to Defend Global Innovation**
Troels Oerting, Head of Global Centre for Cybersecurity (GCC) at World Economic Forum

39 **‘Upping the ante’**
Paul Timmers, Independent advisor for digital innovation

41 **A stable and secure global internet**
Lousewies van der Laan, Member of ICANN’s International Board of Directors

Cybersecurity in the Port of Rotterdam
René de Vries, Cyber Resilience Officer, Harbour of Rotterdam

47 **Protect your most valuable digital assets with the Cybersecurity Health Check**
Firms Deloitte, EY, KPMG and PwC (BIG 4)

50 **‘Accountants have a vital role in maintaining a healthy, robust economy’**
Marco van der Vegte, Chair of the Board for the Institute of Chartered Accountants

54 **‘Think the impossible’**
Hans Folmer, Brigadier, former Commander of Defence Cyber Command (DCC)

56 **Cyber care: the healthcare of the future**
Ruben Wenselaar, CEO of Menzis

60 **Cybersecurity starts with product design**
Hans de Jong, President of Philips the Netherlands

62 **'Research into the impact of law and economics on cybersecurity is breaking new ground'**
Bernold Nieuwesteeg, Researcher at the Rotterdam Institute of Law and Economics (RILE)

64 **‘The GDPR has given citizens back their rights’**
Aleid Wolfsen, President of the Dutch Data Protection Authority (DPA)

67 **Towards an open, secure and prosperous digital Netherlands**

Ferd Grapperhaus
Minister of Justice and Security

Het afgelopen jaar is er veel bereikt op het terrein van cybersecurity. Te beginnen natuurlijk met het Regeerakkoord, waarin veel extra geld beschikbaar kwam voor dit onderwerp. Dit voorjaar heb ik namens het gehele kabinet de Nederlandse Cybersecurity Agenda (NCSA) gepresenteerd. Cybersecurity is het fundament voor digitalisering. Dit moet op orde zijn, zodat burgers en bedrijven de kansen die een digitaal Nederland biedt kunnen grijpen. De NCSA is de komende jaren leidend voor hoe wij Nederland digitaal veilig maken. En hoe er invulling wordt gegeven aan de 95 miljoen euro die dit kabinet structureel uittrekt.

TIME TO BUCKLE UP

De verantwoordelijkheid voor cybersecurity dragen we allemaal: overheid, bedrijfsleven en wetenschap. Een reden om trots te zijn op deze agenda is dan ook dat deze in samenwerking met zoveel partijen tot stand is gekomen.

Bedrijven, van groot tot klein, moeten hun bijdrage leveren en hun eigen digitale deuren goed op slot zetten. De positie van het Nationaal Cyber Security Centrum (NCSC) wordt verstevigd. We investeren in onderwijs en onderzoek. Met mijn collega's van OCW en EZK heb ik 1,5 miljoen euro vrij gemaakt om die kennisontwikkeling een extra impuls te geven.

Net zo blij ben ik met het aantal handtekeningen dat onder de in mei gesloten Nederlandse Cybersecurity Alliantie staat. Het laat zien dat cybersecurity bij velen al hoog op de agenda staat. Bedrijven als KPN en Deloitte en organisaties als ICT-Nederland en ECP hebben zich hiermee aan de uitvoering van de maatregelen uit de NCSA gecommitteerd. Via deze alliantie hopen we bestaande initiatieven, zoals het 'groot helpt klein' principe, het geven van voorlichting of het versterken van de digitale veiligheid van de gehele bedrijfsketen verder te ontwikkelen. Ik hoop op de One Conference in oktober de eerste projecten van de alliantie aan te kondigen.

We werken hard aan de nodige wet- en regelgeving. Zo is de 'cybersecuritywet' (Wetsvoorstel beveiliging netwerk- en informatiesystemen) al door de Tweede Kamer behandeld. De eerste stappen om certificering in te voeren voor dienstverleners van cybersecurity worden gezet, samen met onder andere brancheverenigingen, VNO-NCW en de bond voor verzekeraars. Mijn collega Mona Keijzer, staatssecretaris van Economische Zaken, is hard bezig met de *roadmap digitaal veilige hard- en software*.

Betekent dit dat we er zijn? Dat zeker niet. We moeten vaart maken met de uitvoering van de NCSA, we moeten vaart maken met de implementatie van nieuwe wetten en regels. Want met alleen mooie beloftes en papieren plannen komen we er niet. Kortom, schouders eronder! Ik kijk ernaar uit ook de komende jaren met alle partners in de Cyber Security Raad te werken aan een digitaal veiliger Nederland.

Ferd Grapperhaus
minister Justitie en Veiligheid

"De verantwoordelijkheid voor cybersecurity dragen we allemaal"
"Responsibility for cybersecurity falls to each and every one of us"

Much has been achieved this year with regard to cybersecurity. Beginning, of course, with the coalition agreement in which we increased the budget for cybersecurity substantially. Apart from the extra budget, I also presented the National Cybersecurity Agenda (NCSA) this spring. Cybersecurity serves as the basis for digitalisation. If we want our businesses and citizens to fully grasp the opportunities of the digitalisation of the Netherlands, we need a solid basis of cybersecurity. The coming years, the NCSA will be the leading agenda in making the Netherlands cyber secure. It will also be the guideline in how we will spend the extra budget of 95 million euros.

Responsibility for cybersecurity falls to each and every one of us: government, business and science. An additional reason to be proud of this agenda, therefore, is that so very many parties had a hand in its creation.

Businesses, whether large or small, must do their part and ensure their digital doors remain tightly locked. The position of the National Cyber Security Centre (NCSC) is being strengthened. We are investing in education and research. Together with my colleagues of the Ministry of Education and the Ministry of Economic Affairs , I invested an extra 1.5 million euros to give the development of knowledge a much needed impuls.

I am equally pleased with the number of companies and organisations willing to form the Dutch cybersecurity alliance with us, launched in May. The number of signatures demonstrate that cybersecurity is already a priority for many. Businesses such as KPN and Deloitte and organisations such as ICT Netherlands and ECP have committed themselves to implementing the measures from the NCSA. Through the alliance, we also intend to further develop existing initiatives such as bigger businesses helping the smaller ones, the sharing of information between companies and efforts to increase digital security in the entire business chain. I hope to announce the alliance's first projects at the One Conference in October.

We are working hard to draft the necessary legislation and regulations. The 'Cybersecurity Act' (the proposed Network and Information Systems Security Act), for instance, has already been debated in the House of Representatives. Initial steps are now being taken – together with other sector organisations, VNO-NCW and the Dutch Association of Insurers – to implement certification for cybersecurity service providers. My colleague, State Secretary Mona Keijzer of Economic Affairs and Climate Policy, is making progress on the Digitally Secure Hardware and Software Roadmap.

Does that mean we can rest easy? Absolutely not. On the contrary: we must speed up the process of introducing the NCSA and we must accelerate the implementation of new legislation and regulations. Because we cannot get there with only fine words and plans on paper.

In short: time to buckle up! I look forward to working together with all partners in the Cyber Security Council, in years to come as well, as we strive towards a more digitally secure Netherlands.

Ferd Grapperhaus, Minister of Justice and Security

CYBERSECURITY IN NEDERLAND

Nederland is één van de meest ICT-intensieve economieën van Europa. Digitalisering biedt enorme kansen voor de samenleving en economie, maar dan is het wel zaak te zorgen dat de digitale wereld veilig en vertrouwd blijft, nu en in de toekomst. Om hier in Nederland, Europa en wereldwijd vorm aan te kunnen geven zijn verschillende strategische veiligheidsdocumenten en strategieën opgesteld. Welke documenten en strategieën zijn dit en hoe staan deze met elkaar in verbinding? De Cyber Security Raad (CSR) heeft voor u een overzicht gemaakt.

Nederlandse Cybersecurity Agenda (NCSA), 2018
Doel: De NCSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.
De agenda staat nauw in verbinding met het **Cybersecuritybeeld Nederland (CSBN) 2018**, dat inzicht geeft in de dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid.

Verordening voor de nieuwe Europese cybersecuritystrategie (eerste conceptversie), 2017
Doel: De strategie moet bijdragen aan een veiliger en veerkrachtiger Europese digitale economie als onderdeel van de Digital Single Market Strategy.

De NCSA kent een nauwe samenhang met verschillende andere strategische veiligheidsdocumenten en strategieën op het terrein van digitalisering en cybersecurity, te weten:

Notitie 'Wereldwijd voor een veilig Nederland', Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022, Ministerie van Buitenlandse Zaken, 2018
Doel: Een internationale aanpak voor de veiligheid van Nederland. Ook een innovatieve cyberaanpak met cyberdiplomatie maakt onderdeel uit van deze strategie.
- De notitie is een vervolg op de internationale Cyberstrategie **'Digitaal bruggen slaan' (2017)**

Nationale Digitaliseringsstrategie, ministerie van Economische Zaken en Klimaat (EZK), 2018
Doel: Het verdienvermogen van Nederland verder versterken en zorgen voor betere digitale vaardigheden en cyberveiligheid in de maatschappij.
- Daarnaast heeft het ministerie van EZK de **Roadmap Digitaal Veilige Hard- en Software (2018)** uitgebracht. In dit rapport zijn maatregelen bijeengebracht die moeten leiden tot een aanzienlijke verbetering van de digitale veiligheid van hard- en software.

de National Cyber Security Research Agenda III (NCSRA III) van dcypher, 2018
Doel: Het leveren van een bijdrage aan de cybersecurity van verschillende sectoren met de uitvoering van één nationale cybersecurityonderzoeksagenda.

NL DIGIbeter Agenda Digitale Overheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Over de kansen en uitdagingen in de digitale samenleving. Deze agenda is opgesteld op basis van het **adviesrapport 'Maak Waar'** van de Studiegroep Informatiesamenleving en Overheid van het ministerie van BZK over het functioneren van de digitale overheid in relatie tot de snelle digitalisering van de samenleving.

Later dit jaar volgen nog de volgende cyberstrategieën:
- Defensie Cyber Strategie, Ministerie van Defensie
- Integrale aanpak cybercrime, Ministerie van Justitie en Veiligheid.

Dit voorjaar is de kabinetsbrede Nederlandse Cybersecurity Agenda (NCSA) gepresenteerd. Zeven ambities die omgezet moeten worden in concrete maatregelen om cyberdreigingen het hoofd te bieden en Nederland digitaal veilig te maken. Patricia Zorko, plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en directeur Cybersecurity, geeft haar visie op een digitaal veilig Nederland aan de hand van de NCSA.

The government-wide National Cybersecurity Agenda (NCSA) was presented this spring. It contains seven ambitions that will be converted into specific measures in order to respond to cyber threats and make the Netherlands digitally secure. Patricia Zorko, Deputy National Coordinator for Security and Counterterrorism (NCTV) and Director of Cybersecurity, sets out her vision for a digitally secure Netherlands based on the NCSA.

Patricia Zorko
Deputy National Coordinator for Security and Counterterrorism (NCTV) and Director of Cybersecurity

OP WEG NAAR EEN DIGITAAL VEILIG NEDERLAND

TOWARDS A DIGITALLY SECURE NETHERLANDS

‘WE SIGN UP FOR CYBERSECURITY’

De omvang en ernst van de digitale dreiging in Nederland zijn nog steeds aanzienlijk en blijven zich ontwikkelen. Het Cybersecuritybeeld Nederland 2018 laat dit opnieuw zien. Reden te meer voor een snelle start van de uitvoering van de maatregelen uit de NCSA. Het kabinet erkent de noodzaak ook en investeert daarom de komende vier jaar 280 miljoen euro extra om de dreiging het hoofd te bieden en de digitale weerbaarheid in ons land te verhogen. Zorko: “We moeten dus niet alleen, maar kunnen nu simpelweg meer doen. En we zijn voortvarend aan de slag gegaan! Letterlijk én figuurlijk hebben publieke en private organisaties ‘ingetekend’ om Nederland digitaal veilig te maken.”

Cybersecurity Alliantie

Meer dan 150 vertegenwoordigers van grote en kleine organisaties hebben op 24 mei hun handtekening gezet onder een zin die actie en samenwerking beloofd: ‘We sign up for cybersecurity’. Volgens Zorko is hiermee het startschot gegeven voor de Nederlandse Cybersecurity Alliantie. “In deze alliantie verbinden publieke en private partijen zich om de maatregelen uit de NCSA vorm te geven op die thema’s waar sprake is van een gezamenlijke verantwoordelijkheid. We zien al veel mooie initiatieven van bedrijven om Nederland digitaal veilig te maken. Het groot helpt klein principe, het versterken van de digitale veiligheid van de gehele bedrijfsketen of simpelweg bieden van voorlichting aan het MKB. De Cybersecurity Alliantie bouwt hierop voort. Door het bieden

The scope and severity of digital threats facing the Netherlands are still considerable and continue to evolve over time. The Cyber Security Assessment Netherlands 2018 (CSAN 2018) shows this development yet again. All the more reason to start swiftly with the implementation of the measures in the NCSA. As the government acknowledges this necessity, it is investing an additional 280 million euros over the next four years to deal with the threat and to improve cyber resilience across the country.

According to Zorko, ‘Not only must we do more, now we actually can do more. And we are eager to roll up our sleeves and get to work! Literally and figuratively, public and private organisations have "signed up" to improve Dutch cybersecurity.’

Cyber Security Alliance

On the 24th of May, more than 150 representatives from organisations both large and small put their signatures to a phrase that pledges action and collaboration: ‘We are signing up for cybersecurity.’ Zorko says that this action launched the Netherlands Cybersecurity Alliance: ‘Via this alliance public and private parties commit themselves to the NCSA, so they also can give shape to the measures, particularly in areas where collective responsibility is required.
We have already seen great initiatives by companies to ensure digital security in the Netherlands, such as the principle of large businesses helping smaller ones, strengthening digital security in the entire business chain or simply providing information to SMEs. The Cyber Security Alliance aims to build on this work. By providing insights and monitoring initiatives in the area of cybersecurity, the alliance is supplying key information on where additional public-private action is required to achieve breakthroughs. We want to create a movement that will spread across the Netherlands like an oil slick.’

The NDN is growing

What started out as a small technical project has grown since 2017 into a large national

“We zijn goed begonnen op weg naar een digitaal veilig Nederland. Ik teken ervoor!"

“We are off to a good start on the road towards a digitally secure Netherlands. I am signing up for that!”

van inzicht en overzicht in initiatieven op het gebied van cybersecurity zorgt de alliantie voor zicht op waar aanvullende publiek-private actie nodig is om doorbraken te realiseren. We willen een beweging creëren die zich als een olievlek over Nederland verspreidt.”

Het NDN groeit

Wat ooit begon als een klein technisch project, groeide vanaf 2017 uit tot een groot landelijk programma: het Nationaal Detectie Netwerk (NDN). Het NDN is een netwerk van publieke en vitale organisaties dat zich richt op het onderling delen van cyberdreigingsinformatie. Zorko: “Op dit moment zijn 39 rijksoverheidsorganisaties en 20 vitale organisaties aangesloten. Het programma is in een nieuwe fase terechtgekomen, waardoor we nu met meer mensen gerichte en grote stappen kunnen maken. Onze ambitie is om dit jaar tien rijksoverheidsorganisaties en zeker vijf vitale organisaties aan te sluiten. In 2019 gaan die aantallen nog eens flink omhoog.”

Extra impuls aan kennis en innovatie

Zorko geeft aan dat er al flinke stappen zijn gezet in het vergroten van de kennisbasis van cybersecurity. “Ook onze cybersecurityspecialisten ‘maken’ we samen. Een belangrijk kader hiervoor is de derde editie van de Nationale Cyber Security Research Agenda die ik in juni in ontvangst heb genomen. Gezien de urgentie, is er voor 2018 en 2019 door het kabinet extra geld beschikbaar gesteld voor kennis en innovatie: 3,5 miljoen en oplopend tot 5,5 miljoen in 2020.” Daarnaast ontwikkelt de Nederlandse Organisatie van Wetenschappelijk Onderzoek (NWO) momenteel een nationale cybersecurity-onderzoeksoproep van ca. 5 miljoen euro. Zorko: “De oproep wordt opgesteld in samenwerking met het Nationaal Regieorgaan voor Praktijkgericht Onderzoek SIA, het platform dcypher, Team ICT en de Topsector Creatieve Industrie. Op deze manier faciliteren we brede – interdisciplinaire – onderzoekssamenwerking op het gebied van cybersecurity.”
Het woord Agenda uit de naam NCSA suggereert volgens Zorko actie, afspraken en samenwerking. “Wat mij betreft zijn we goed begonnen op weg naar een digitaal veilig Nederland. Ik teken ervoor!’, aldus Zorko.

programme: the National Detection Network (NDN). The NDN is a network of organisations within the Dutch critical infrastructure and public organisations focused on sharing information about cyber threats. Zorko elaborates: ‘So far, 39 central government bodies and 20 critical organisations have joined up. The programme has entered a new phase; because we have more people, we can now be more focused and make major strides. Our ambition is to connect another ten central government bodies and at least five critical organisations by the end of this year. Those numbers will be even higher in 2019.’

Additional incentive for knowledge and innovation

Zorko says that substantial steps have already been made in increasing the cybersecurity knowledge base. ‘We are even "creating" our own cybersecurity specialists. An important context in this regard is the third edition of the National Cyber Security Research Agenda, which was presented in June. Given the urgency, the government will make extra budget available for knowledge and innovation in 2018 and 2019: 3.5 million euros, totalling to 5.5 million euros by 2020.’ In addition, the Netherlands Organisation for Scientific Research (NWO) is currently developing a national call for cybersecurity research proposals, worth around 5 million euros. So as Zorko says, ‘the call for proposals will run in collaboration with the National Body for Practice-Oriented Research (SIA), the dcypher platform, Team ICT and the Creative Industry Top Sector. We hope that this approach will facilitate broad, possibly interdisciplinary research collaboration in the area of cybersecurity.’
To Zorko, the word ‘agenda’ in the NCSA’s name suggests action, agreement and collaboration. ‘In my view, we are off to a good start on the road towards a digitally secure Netherlands. I am signing up for that!’

Het regeerakkoord is er duidelijk over: Nederland kan digitaal koploper worden van Europa en het kabinet gaat werk maken van digitalisering in de zorg, de mobiliteit en het openbaar bestuur. Bovendien worden de 'noodzakelijke basisvoorwaarden' cybersecurity, privacy, digitale vaardigheden en innovatie aangepakt. In de recent verschenen Nederlandse Digitaliseringsstrategie, de Nederlandse Cybersecurity Agenda (NCSA) en de Roadmap Digitaal Veilige Hard- en Software (DVHS) krijgt die ambitie gestalte. Sandor Gaastra, directeur-generaal Energie, Telecom en Mededinging van het ministerie van Economische Zaken en Klimaat (EZK), vertelt erover.

The government coalition agreement is clear on the matter: as the Netherlands has the potential to be a digital leader in Europe, the government intends to work hard on digitalisation in healthcare, mobility and public administration. It also intends to tackle the 'necessary boundary conditions' – cybersecurity, privacy, digital literacy and innovation. This ambition is encapsulated in the recently released Dutch Digitalisation Strategy, the National Cybersecurity Agenda (NCSA) and the Digitally Secure Hardware and Software Roadmap (DVHS). Sandor Gaastra, Director-General for Energy, Telecommunications and Competition at the Ministry of Economic Affairs and Climate Policy, gives us his take on the topic.

Sandor Gaastra
Director-General for Energy, Telecommunications and Competition at the Ministry of Economic Affairs and Climate Policy and member of the Cyber Security Council

DIGITALISERING EN HET NIEUWE KABINET:

DIGITALISATION AND THE NEW GOVERNMENT:

HIGH AMBITIONS, COMPLEX TASKS, INTENSIVE COLLABORATIONS

Samenwerking en platforms
"De digitalisering in Nederland gaat hard", vertelt Gaastra. "Het grensoverschrijdend dataverkeer steeg tussen 2005 en 2014 met een factor 45 en investeringen in ICT zijn goed voor 20% van de groei van het BNP. In de Nederlandse Digitaliseringsstrategie staat wat nodig is om de vruchten van digitalisering te kunnen plukken voor economische groei en maatschappelijke ontwikkeling." De strategie gaat over onderzoek en innovatie, werk en vaardigheden én over 'moeilijke' vraagstukken rond concurrentie (dominante digitale platforms) en ethiek ('alwetende' algoritmen). Gaastra: "Dat hebben we onder meer vertaald in het MKB-Actieplan, de 'Implementatieagenda Smart Industry' en publiek-private kennisopbouw rond onder meer kunstmatige intelligentie, blockchain en quantum computing."

Collaborations and platforms
'Digitalisation in the Netherlands is advancing at a rapid pace,' says Gaastra. 'Cross-border data traffic increased by a factor of 45 between 2005 and 2014, while investment in ICT accounted for 20% of GDP growth. The Dutch Digitalisation Strategy sets out what is required in order to reap the benefits of digitalisation for economic growth and social development.' The strategy covers research and innovation, work and skills and 'difficult' issues around competition (dominant digital platforms) and ethics ('all-knowing' algorithms). According to Gaastra: 'All that and more has been translated into the SME Action Plan, the Smart Industry Implementation Agenda, and public-private knowledge-building around issues such as artificial intelligence, blockchain technologies and quantum computing.'

There is also a downside to digitalisation: issues with security and privacy. As Gaastra points out: 'You only need to pick up a newspaper to see the stories. Everyone can remember the terminal in Rotterdam that was hacked, causing 300 million euros worth of damage. Less attention was given to the digital break-in at a university in which the personal data of 17,000 people were made public, including their national insurance number and bank account details. While the financial damage in that case was less substantial, the damage to trust in digital technology was just as serious. Ultimately, the security and reliability of digital connections and information will determine whether we can reap the benefits of digitalisation.'

Digitalisering heeft ook een keerzijde: problemen met veiligheid en privacy. Gaastra: "Je hoeft de krant maar open te slaan. Iedereen kan zich die terminal in Rotterdam herinneren die werd platgehackt, met een schade van € 300 miljoen als gevolg. Minder aandacht is er voor de digitale inbraak bij een universiteit waardoor de persoonsgegevens van 17.000 mensen, inclusief hun burgerservicenummer en bankrekening op straat kwamen te liggen. Daar is de financiële schade minder groot, maar minstens zo erg is de schade aan het vertrouwen in digitale technologie. Uiteindelijk bepalen de veiligheid en betrouwbaarheid van digitale verbindingen en informatie of we de vruchten van digitalisering kunnen plukken."

Alliantie en boegbeeld
Het hoofdstuk over veiligheid in de digitaliseringsstrategie bestrijkt een fors terrein; van hacken en phishing tot veilig online winkelen voor iedereen. De titel is veelzeggend: 'Weerbaarheid van burgers en organisaties versterken'. Gaastra: "Cybersecurity vereist samenwerking tussen burgers, bedrijven, organisaties, toezichthouders en departementen. Het Digital Trust Center dat onlangs is gestart, gaat ons daarbij helpen. Het is een door EZK en het ministerie van Justitie & Veiligheid, ofwel J&V, gerund platform voor onafhankelijke informatie over cybersecurity-problemen én voor cybersecurity-samenwerkingsverbanden van bedrijven."

Samenwerking was ook het sleutelwoord bij de presentatie van de NCSA in mei dit jaar. CEO's sloten zich aan bij de Cybersecurity Alliantie van de agenda en wierpen zich op als boegbeeld van een van de acties uit de agenda. En er zijn meer voorbeelden: Schiphol bouwt het Cyber Synergie Schiphol Ecosysteem (CYSSEC) uit, Rabobank organiseert cyberweerbaarheidbijeenkomsten voor het MKB en KPN en andere telecomaanbieders gaan DDOS-aanvallen bestrijden in de Dutch Continuity Board. Ook onderdeel van de NCSA. Ook onderdeel van de NCSA is de Roadmap DVHS. Gaastra: "Iedere dag worden duizenden dingen aan het internet gehangen, van slimme thermostaten tot complete machineparken. Met de afhankelijkheid van het internet groeien ook de risico's, terwijl de gebruikers daar nauwelijks grip op hebben. EZK en J&V hebben in de roadmap een aanpak uitgewerkt met onder meer Europese certificering voor internetapparaten, een monitor voor onveilige apparaten en een publiekscampagne over cyberhygiëne. Samen met de betrokken partijen gaan de ministeries deze roadmap uitvoeren."

De ambities en aanpak staan op papier. Gaastra waarschuwt: "Papier is geduldig, maar ik niet. Samen aan de slag!"

"Met de internetafhankelijkheid groeien ook de risico's, terwijl de gebruikers daar nauwelijks grip op hebben."

"Dependence on the Internet leads to risks, which users barely understand."

regulators and government departments. The Digital Trust Centre that was set up recently will help with that. It is a platform run by the Ministry of Economic Affairs and Climate Policy in conjunction with the Ministry of Justice and Security, which provides independent information about cybersecurity issues and promotes cybersecurity partnerships between businesses.'

Collaboration was also the keyword for the NCSA presentation in May. A number of CEOs joined the Cybersecurity Alliance to implement the agenda and each of them volunteered to be a standard bearer for one of the actions on the agenda. There are even more examples: Schiphol Airport is developing the Cyber Synergy Schiphol Ecosystem (CYSSEC), Rabobank is organising cyber resilience meetings for SMEs, and KPN and other telecommunications providers have agreed to fight DDoS attacks through the Dutch Continuity Board. Another part of the NCSA is the DVHS Roadmap. As Gaastra points out: 'Every day, thousands of items are connected to the Internet, from smart thermostats to entire fleets of machines. Dependence on the Internet leads to risks, which users barely understand. In the Roadmap, the Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security have developed an approach which includes European certification for Internet devices, monitoring for unsafe devices and a campaign for public awareness of cyber sensibility. The ministries will implement this roadmap in cooperation with the relevant parties.'

The ambitions and approach have been put on on paper. Gaastra warns: 'Paper is patient, but I am not. What we need now is joint action!'

Voor Defensie is het digitale domein, naast het land, de lucht, de zee en de ruimte, het vijfde domein voor militair optreden. De nieuwe Defensie Cyber Strategie die in ontwikkeling is, geeft in de komende jaren richting, samenhang en focus aan de integrale aanpak voor de ontwikkeling van het militaire vermogen in het digitale domein. Sebastian Reyn is Directeur-Generaal Integraal Beleid bij het ministerie van Defensie en daarmee verantwoordelijk voor de cyberstrategie.

For the Ministry of Defence, cyber space is the fifth domain of military operations, alongside land, air, sea and space. Over the next few years, the new Defence Cyber Strategy that is being developed will provide direction, cohesion and focus for the development of military capability in the digital domain. Sebastian Reyn is the Director-General of Integrated Policy at the Ministry of Defence and is thus responsible for the cyber strategy.

Sebastian Reyn
Director-General of Integrated Policy at the Ministry of Defence and member of the Cyber Security Council

SPIONAGE, BEÏNVLOEDING, VERSTORING EN SABOTAGE

ESPIONAGE, INFLUENCING, DISRUPTION AND SABOTAGE

CONSTANT VIGILANCE IS REQUIRED FROM THE MINISTRY OF DEFENCE

Het Cybersecuritybeeld Nederland 2018 is helder: digitale aanvallen van statelijke actoren met als doel spionage, beïnvloeding, verstoring en sabotage, vormen de grootste digitale dreiging voor de nationale veiligheid. Volgens Reyn vraagt dit om een constante inspanning van Defensie. “We moeten hier actief tegen optreden en vanuit Defensie nóg alerter zijn op dreigingen als het gaat om het bewaken en beveiligingen van onze netwerken en systemen. We leven in een kennisintensief land met een uitstekende digitale infrastructuur en een internationaal politiek profiel. Dat maakt ons een interessant doelwit.”

Defensie Cyber Commando
Om de krijgsmacht effectief te kunnen laten opereren in het digitale domein is een aantal jaren geleden het Defensie Cyber Commando (DCC) opgericht. Reyn vertelt dat deze bal is gaan rollen toen het digitale domein officieel als vijfde militair domein werd erkend. “Het belangrijkste moment was toch wel de NAVO-top in Warschau in 2016. Na een jarenlange lobby heeft ook de NAVO het digitale domein erkend als operationeel domein. Kortgezegd betekent dit dat de NAVO haar verdedigende en afschrikkende taken net zo effectief gaat invullen in het digitale domein als in de ‘traditionele’ domeinen. In deze gedigitaliseerde tijd betekent dat veel voor onze veiligheid”, benadrukt Reyn. “De NAVO is nog steeds de hoeksteen van het Nederlandse internationale veiligheidsbeleid, nu ook in het digitale domein.”

The Cyber Security Assessment Netherlands 2018 is clear: cyber attacks by state actors for the purposes of espionage, influencing, disruption and sabotage are the greatest digital threat to national security. According to Reyn, these threats require constant vigilance from the Ministry of Defence: 'We must take action to counter this threat, and the Ministry of Defence must be more alert to threats than ever as it monitors as well as protects our networks and systems. Since we live in a knowledge-intensive country with superb digital infrastructure and an international political profile, we are an interesting target.'

Defence Cyber Command
To ensure that the armed forces can operate effectively in the digital domain, the Defence Cyber Command (DCC) was founded a number of years ago. Reyn says that the official recognition of cyber space as the military domain accelerated this development. 'The key moment was the 2016 NATO summit in Warsaw. After years of lobbying, NATO recognised cyber space as an operational domain. In other words, NATO can carry out its defensive and deterrent activities just as effectively in the digital domain as in the "traditional" domains.' Reyn emphasises: 'Its significance to our security in this digitalised age is high. NATO is still the cornerstone of the Dutch international security policy, which now pertains to the digital domain as well.'

Cyberstrategy
The government has set aside additional funds in each year for the Ministry of Defence to invest in cyber defence and IT. According to Reyn: 'This funding will strengthen the Ministry of Defence across the board. We are developing a cyberstrategy to give this process direction, which we expect to publish this autumn. I cannot really say much about it yet. In any case, current developments in the digital domain require active defensive measures from the Ministry. After all, we want to prevent actors from penetrating our networks and threatening our national security. That aspect has an impact on how we shape military concepts such as deterrence. Such a subject certainly has a role to play in the new strategy. We will not be going it alone. By definition, Dutch cybersecurity requires a collective effort from citizens and businesses as well as the government. We want to make a significant contribution to that process.'

The Ministry of Defence’s Cyber Strategy is closely linked to the National Cybersecurity Agenda (NCSA). 'The Ministry of Defence was involved in the creation of the NCSA,' Reyn continues. 'The same applies to the Common Foreign and Security Policy established by the Ministry of Foreign Affairs. Both documents mention a role for the Ministry of Defence. We developed this strategy further in the Ministry of Defence’s Cyber Strategy, while we also involved our public and private partners in that process.' Reyn emphasises that this public-private collaboration is key to keeping the Netherlands safe in the digital domain: 'We are neither able nor willing to do it alone. I brought my colleagues from the Cyber Security Council into the process as well. That approach provided a significant boost to our understanding of each other’s expertise and expectations. In turn, they brought specific knowledge and experience about the digital domain. We have got a fantastic network there, which we can use at the Ministry of Defence as we respond to all the challenges that we are facing.'

Cyberstrategie
Het kabinet trekt structureel tot enkele tientallen miljoenen euro’s extra uit voor Defensie voor investering in cyberdefensie en ICT. “Hiermee gaan we Defensie over de gehele breedte versterken en daartoe ontwikkelen we een cyberstrategie die naar verwachting dit najaar zal verschijnen”, vertelt Reyn. “Heel veel kan ik hier nog niet over zeggen. De huidige ontwikkelingen in het digitale domein vragen in ieder geval om een actieve verdediging door Defensie. We willen immers voorkomen dat actoren ons netwerk binnendringen. Dit heeft ook invloed op de manier waarop we bijvoorbeeld militaire concepten als afschrikking vorm gaan geven. Een onderwerp als dit gaat zeker een rol spelen in de nieuwe strategie”, vertelt Reyn. “We gaan dit niet alleen doen. De digitale veiligheid van Nederland is per definitie een gezamenlijke inspanning van burgers, bedrijven én de overheid. Daar willen wij een belangrijke bijdrage aan leveren.”

De Defensie Cyberstrategie is nauw verbonden aan onder andere de Nederlandse Cybersecurity Agenda (NCSA). “Defensie is betrokken geweest bij de totstandkoming van de NCSA”, vervolgt Reyn. “Dat geldt ook voor de Geïntegreerde Buitenland en Veiligheidsstrategie van Buitenlandse Zaken. In beide documenten is de rol van Defensie aangehaald. Wij werken dit verder uit in de Defensie Cyber Strategie en daar betrekken ook wij onze publieke én private partners bij. Deze samenwerking is belangrijk om Nederland digitaal veilig te houden; we willen en kunnen het niet alleen”, benadrukt Reyn. “Ook mijn collega’s van de raad betrek ik hierbij. Dat levert een flinke ‘boost’ op voor de wederzijdse kennis over elkaars kwaliteiten en verwachtingen. Ook nemen zij op hun beurt specifieke kennis en ervaring mee over het digitale domein. Daar hebben we een fantastisch netwerk dat we als Defensie goed kunnen gebruiken voor het aangaan van alle uitdagingen waar we voor staan!”

ERIK AKERBOOM

Nieuw lid van de Cyber Security Raad

New member of the Cyber Security Council (CSR)

“Ons werk ‘digitaliseert’ op nagenoeg elk vlak”

“We are increasingly active in the digital arena”

Erik Akerboom is per 1 maart 2016 benoemd tot eerste hoofdcommissaris van de politie, ook wel korpschef genoemd. In die functie geeft hij leiding aan de Nederlandse politie. In 2017 is Akerboom toegetreden als raadslid van de CSR.

Erik Akerboom has been the first head of the National Police since 1 March 2016, also referred to as Police Chief. As such, he is in charge of the entire Dutch police force. Akerboom became a member of the CSR in 2017.

Nederland is en blijft een interessant doelwit voor cybercriminelen. Het inzichtelijk krijgen van de (economische) schade van cybercrime blijft lastig. Welke rol speelt cyber voor de Nationale Politie?

Cyber heeft voor de politie twee kanten: in de eerste plaats digitaliseert ons werk op nagenoeg elk vlak. Natuurlijk vooral op het gebied van de opsporing. Daarbij zullen voorkomen en verstoren in toenemende mate belangrijke interventies zijn. Maar ook op het gebied van handhaving digitaliseert ons werk. Deze ontwikkeling vraagt een groot innovatievermogen van het korps, samen met publieke en private partners. De andere kant betreft de cybersecurity van onze eigen organisatie. Die moet ook op orde zijn. In de CSR komen beide aspecten aan de orde.

Wat is voor u het belang van de CSR?

De kracht van de CSR zit hem in het feit dat we als publieke en private partijen gezamenlijk met de wetenschap onze adviezen uitbrengen. De CSR speelt zo een grote rol in het agenderen van cybersecurity. Daarbij moeten we oog hebben voor de economische belangen en die van de veiligheid en privacy. De gemengde samenstelling van de raad zorgt voor evenwichtige adviezen.

The Netherlands continues to be an attractive target for cybercriminals and it remains challenging to obtain insight into the extent of economic damage and other damage arising from cybercrime. What is the role played by cyber as regards the National Police?

As far as the police are concerned, there are two aspects to cyber . In the first place, we are increasingly active in the digital arena, especially when it comes to detection, of course. In addition, prevention and disruption will become increasingly important interventions in our arsenal. Our enforcement activities are increasingly digitalising as well. This development requires a significant innovation effort from the force and its public and private partners. Secondly, cybersecurity also affects our own organisation. We must be cybersecure as well. The CSR unites both aspects.

Why do you consider the CSR to be important?

The strength of the CSR is that public and private parties issue advice together with the scientific sector. This allows the CSR to keep cybersecurity at the top of the agenda. Moreover, we have a duty to weigh economic interests, as well as security and privacy interests. The mixed composition of the CSR ensures that its recommendations achieve the right balance.

De cijfers van de politie en die van het CBS laten een daling zien van de geregistreerde criminaliteit in 2017. Ze tonen eveneens een verschuiving van traditionele misdrijven naar cybercrime. Meer mensen zijn tegenwoordig slachtoffer van hackers dan van fietsendieven. “De software om digitale misdaden te plegen is online te koop en betaalbaar. Dieven, fraudeurs en oplichters hebben de koevoet en gladde praatjes ingeruild voor kwaadaardige software pakketten”, vertelt Erik Akerboom, Korpschef van de Nederlandse Politie.

Police figures as well as Statistics Netherlands (CBS) figures show a decline in the number of reported crimes in 2017. They also show a shift from traditional crime to cybercrime. In today’s society, more people fall victim to hackers than to bicycle thieves. ‘The software you need to commit digital crime is available online and affordable. Thieves, fraudsters and con artists have traded in crowbars and smooth talk for malicious software packages’, according to Police Chief Erik Akerboom of the Dutch National Police.

Erik Akerboom
Chief of the Dutch National Police and member of the Cyber Security Council

TACKLING CYBERCRIME: CHOOSING THE MOST EFFECTIVE INTERVENTION

Daarmee blijft volgens Akerboom de urgentie voor een effectieve, integrale aanpak van cybercrime en gedigitaliseerde criminaliteit. Akerboom: “Wij zijn er voor de bescherming van de burger. Op straat maar ook online. Het vertrouwen in de politie is hoog en ik wil dat dat zo blijft.”

Opsporen

Ruim 800 digitaal specialisten van de politie speuren dagelijks naar de sporen die elke crimineel tegenwoordig achterlaat. Alle ‘offline misdrijven’ hebben immers nu ook een digitale component. “Maar opsporen alléén is niet (meer) voldoende om ons online te beschermen”, vervolgt Akerboom. “Om cybercrime te bestrijden kunnen voorkomen en verstoren soms effectiever zijn. Dat is ook terug te zien in de aanpak van het Team High Tech Crime en cybercrimeteams in de regionale politie-eenheden. Die waren vorig jaar goed voor 43 complexe cybercrime-onderzoeken. Een jaar eerder waren dit er 32. Die teams

As a result, Akerboom considers an effective, integrated approach to cyber and digital crime as urgent as ever. Akerboom: ‘We are here to protect the population, both in the streets and online. Confidence in the police is high and I would like it to remain so.’

Detect

Every day, more than 800 digital specialists employed by the police look for the traces that all criminals currently leave behind. After all, all ‘offline crime’ now also has a digital component. ‘However, detection on its own is no longer enough to protect us online’, Akerboom continues. ‘If we want to combat cybercrime, it may sometimes be more effective to prevent and disrupt. This is the strategy pursued by the National High Tech Crime Unit and the cybercrime teams of the regional police forces. Last year, they carried out 43 complex cybercrime investigations, up from 32 the previous year. These teams focus on detecting suspects, disrupting their criminal activities and earning models, and preventing people from becoming victims of cybercrime.’

Disrupt

One notable success of the National High Tech Crime Unit has been the dismantling of Hansa Market after a lengthy international investigation. Akerboom: ‘That was one of the largest illegal marketplaces on the dark web. Also, by taking down webstresser.org, which sold DDoS attacks on a wide scale, we were able to prevent more civilians, schools and businesses from becoming a target.’

There were more successes: in April this year, the cybercrime teams shut down a forum where men from across the globe exchanged stolen nude pictures of thousands of mainly Dutch girls and young women. ‘That investigation began with the report of a single victim’, Akerboom recounts. ‘By accident, she came across pictures of herself on the internet after her cloud storage had been hacked into. The eventual outcome was the arrest of several suspects and the seizure of the forum’s server.’

“Criminele hackers en oplichters zijn de struikrovers van de 21ste eeuw.”

“Criminal hackers and fraudsters are the highwaymen of the 21st century”

richten zich op het opsporen van verdachten, het verstoren van hun criminele activiteiten, het verdienmodel en het voorkomen van slachtofferschap.”

Verstoren

Zo ontmantelde het Team High Tech Crime – na een langlopend, internationaal onderzoek – Hansa Market. Akerboom: “Dit was één van de grootste illegale marktplaatsen op het darkweb. En door het offline halen van webstresser.org, die op grote schaal ddos-aanvallen verkocht, konden we voorkomen dat nóg meer burgers, scholen en bedrijven werden gedupeerd.”

En er werden meer successen geboekt; in april dit jaar haalden de cybercrimeteams een forum uit de lucht waarop mannen wereldwijd gestolen naaktfoto’s van duizenden hoofdzakelijk Nederlandse meisjes en jonge vrouwen uitwisselden. “Dit onderzoek begon met de aangifte van één slachtoffer”, vertelt Akerboom. “Zij ontdekte per toeval foto’s van zichzelf op internet nadat haar online opslag was gehackt. Uiteindelijk leidde het tot de aanhouding van meerdere verdachten en de inbeslagname van de server waarop het forum draaide.”

Samenwerken

Net zoals in de Nederlandse Cybersecurity Agenda loopt samenwerking als een rode draad door de aanpak van cybercrime van de politie. Akerboom: “Die samenwerking is essentieel voor een effectieve bestrijding. En het stopt niet bij de grens, internationaal moeten we ook de handen ineen slaan met zowel publieke als private partijen. Ik ben trouwens een groot voorstander van coalities waarvan de samenstelling per zaak kan verschillen. Met het Openbaar Ministerie en elf private partners werken we inmiddels samen aan de bestrijding van de zogenoemde *tech support scam*. Wereldwijd zijn daar al veel mensen slachtoffer van geworden. Een samenwerking als deze vergroot de kennis van elkaars werk en het inzicht in elkaars belangen. Hierdoor kunnen we gerichtere interventies plegen. Uiteindelijk leidt dit tot een effectievere aanpak en een veiliger samenleving.”

Nederland is verwikkeld in een razendsnelle wedloop van technisch vernuft. “Criminele hackers en oplichters zijn de struikrovers van de 21ste eeuw. Om hen te bestrijden moeten we blijvend investeren in mensen, kennis en vaardigheden. Dat houdt nooit op”, aldus Akerboom.

Collaborate

As in the Dutch National Cybersecurity Agenda, collaboration is a key theme of the police’s cybercrime approach. Akerboom: ‘Collaboration is essential to fight crime effectively, and it does not stop at the border: international collaboration with both public and private parties is also required. In that respect, I am a strong advocate of flexible coalitions that change composition on a case-by-case basis. We are currently working with the Public Prosecution Service and 11 private partners to tackle the so-called “tech support scam”, which has claimed many victims across the world. Collaborations such as these help increase awareness of each other’s work and lead to greater insight into each other’s interests, allowing us to make more targeted interventions. In the end, this will lead to a more effective approach and a safer society.’

The Netherlands is engaged in an ever faster technological arms race. ‘Criminal hackers and fraudsters are the highwaymen of the 21st century. In order to defeat them, we must continue to invest in human capital, knowledge and skills. This is never-ending’, Akerboom stresses.

JOOST FARWERCK

Nieuw lid van de Cyber Security Raad
New member of the Cyber Security Council (CSR)

Joost Farwerck is Chief Operations Officer en lid van de Raad van Bestuur van KPN. Daarnaast is hij lid van de raad van bestuur van Nederland-ICT en lid van het uitvoerend comité van VNO-NCW. In 2017 is Farwerck als raadslid toegetreden tot de Cyber Security Raad namens Nederland ICT.

Joost Farwerck is Chief Operations Officer and member of the executive board of KPN. In addition, he is a member of the executive board of Nederland ICT and member of the executive committee of VNO NCW. In 2017, Farwerck joined the CSR as a member on behalf of Nederland ICT.

Nederland ICT is belangenbehartiger en vertegenwoordiger van de Nederlandse ICT sector. Welke rol speelt cyber hierbij?
Vertrouwen in veiligheid en de betrouwbaarheid ervan is cruciaal. Niet alleen voor de reputatie van de sector zelf, maar vooral ook voor de maatschappij als geheel. Het gaat dan niet alleen over de veiligheid en betrouwbaarheid van de verbindingen, maar ook over de veiligheid van onze spullen en software. Alleen door samen te blijven werken aan technologie die veilig en betrouwbaar is en de privacy van gebruikers respecteert, houden we voldoende draagvlak om ook in de toekomst volop te kunnen blijven profiteren van digitalisering. Dat is nodig om al onze maatschappelijke uitdagingen voor bijvoorbeeld klimaat, zorg en mobiliteit het hoofd te kunnen bieden.

Wat is voor u het belang van de CSR?
Nederland beschikt over de modernste telecom en ICT infrastructuur waarmee we in Europa voorop lopen, maar dit is ook uiterst interessant voor cybercriminelen. Daarom is het goed dat bedrijfsleven, overheid en wetenschap in Nederland samenkomen in de CSR. Door het kabinet gevraagd en ongevraagd advies te geven en toe te zien op de uitvoering van de nationale cybersecurity strategie helpt de raad Nederland digitaal te beschermen.

“Nederland beschikt over de modernste telecom- en ICT-infrastructuur waarmee we in Europa voorop lopen, maar dit is ook uiterst interessant voor cybercriminelen.”
The Netherlands boasts Europe’s most advanced telecom and ICT infrastructure, but at the same time this makes us a target for cybercriminals’

Nederland ICT represents and defends the interests of the Dutch ICT sector. What is the role played by cyber in that respect?
Faith in security and its reliability is crucial not only to the reputation of the sector itself, but also and principally to society at large. Security and reliability are not limited to connections, but also extend to devices, equipment, hardware and software. Only by continuing to work together on safe and reliable technology that is respectful of user privacy can we maintain the infrastructure we need to continue to reap the full rewards of digitalisation in the future. Only then can we tackle all of the challenges facing society, such as climate change, care, healthcare and mobility.

Why do you consider the CSR to be important?
The Netherlands boasts Europe s most advanced telecom and ICT infrastructure, but at the same time this makes us a target for cybercriminals. So it is sensible for the Dutch business and academic sectors and the government to join forces in the CSR. The CSR helps to keep the Netherlands digital infrastructure safe by providing the government with both solicited and unsolicited advice and monitoring the implementation of the National Cybersecurity Strategy.

Met de in mei gepresenteerde Nederlandse Cybersecurity Agenda (NCSA) zet het kabinet in op versterking van de samenwerking tussen overheid en bedrijfsleven voor een veiliger digitaal Nederland. Joost Farwerck, lid van de Cyber Security Raad (CSR) namens Nederland ICT en lid van de Raad van het Bestuur bij KPN, was één van de eerste ondertekenaars van de publiek-private Cybersecurity Alliantie van de NCSA en pleit voor verregaande samenwerking.

In May, the Dutch government published the Dutch National Cybersecurity Agenda (NCSA) with the aim of strengthening the collaboration between government and the business sector to achieve a more secure digital Netherlands. Joost Farwerck, member of the Cyber Security Council (CSR) on behalf of Nederland ICT and member of the executive board of KPN, was one of the first signatories of the NCSA’s public-private Cybersecurity Alliance and advocates extensive cooperation.

Joost Farwerck
Chief Operations Officer, member of the executive board of KPN and member of the Cyber Security Council

‘WHEN IT COMES TO SECURITY, THERE IS NO COMPETITION’

Het is de missie van Nederland ICT om samen met verschillende partijen Nederland te ontwikkelen tot de beste digitale economie van Europa. Volgens Farwerck heeft iedereen er belang bij dat cybersecurity in Nederland zo goed mogelijk is georganiseerd. “Door zoveel mogelijk de samenwerking te zoeken kunnen we daadwerkelijk dreigingen het hoofd bieden, zodat Nederland er beter en veiliger van wordt. Het is van groot belang dat de overheid met de private sector en wetenschap samen optrekken. De dreigingen zijn zo fors dat we deze alleen kunnen aanpakken wanneer we samenwerken. Door van elkaar te leren, door informatie te delen over bijvoorbeeld kwetsbaarheden en elkaar te helpen tijdens grote cybersecurity-incidenten. We hebben elkaar daarvoor hard nodig”, vertelt Farwerck.

Er gebeurt heel veel

Het is volgens Farwerck goed om te zien dat de verschillende ministeries (EZK, JenV en BZK) in het Nederland ICT’s mission is to work with a number of parties to turn the Netherlands into Europe’s foremost digital economy. Farwerck argues that it is in everyone’s interest to make the Dutch cybersecurity infrastructure as well organised as possible. ‘By actively seeking to collaborate as often as possible, we will be able to respond efficiently to threats and make the Netherlands more secure. It is vitally important that the government joins forces with the private and scientific sectors in this regard. The threats are so dangerous that we will only be able to tackle them if we work together. We can do this by learning from each other, sharing information about such topics as vulnerabilities and assisting each other during serious cybersecurity incidents. We really need each other’, Farwerck says.

Significant activity

Farwerck regards the fact that the Ministry of Economic Affairs and Climate Policy, Ministry of Justice and Security and Ministry of the Interior and Kingdom Relations are currently collaborating more closely than ever on digitalisation and digital security dossiers as a positive development. Farwerck: ‘The past few months have seen the publication of a number of policy recommendations that are fortunately closely intertwined, such as the NCSA, the Digitally Secure Hardware and Software Roadmap and the Dutch Digitalisation Strategy. However, this significant activity also involves a certain level of risk: how do we convert all of our ambitions into action and how do we keep private stakeholders involved? To this end, the government should remain in contact with the private sector, ensure that it remains actively involved and consider the possible impact of policies on businesses.’

Stronger together

For years, the Dutch ICT sector has been working together as one on continuous security upgrades. Farwerck: ‘We are stronger together. The key point is that when it comes to security, there is no such thing as competition. The

huidige kabinet meer dan ooit samenwerken op de dossiers die raken aan digitalisering en digitale veiligheid. Farwerck: “Afgelopen maanden is een aantal beleidsadviezen gepubliceerd die, gelukkig, sterk in elkaar grijpen, zoals de Nederlandse Cybersecurity Agenda, ofwel NCSA, de roadmap veilige digitale hard- en software en de Nationale Digitaliseringsstrategie. Er is dus volop beweging, maar daarin schuilt ook enig risico. Want hoe zetten we alle ambities om in acties en hoe zorgen we ervoor dat private partijen aangesloten blijven? Dat vraagt om een overheid die het bedrijfsleven opzoekt, betrekt en rekening houdt met de mogelijke impact van beleid op de bedrijven.”

Samen bereik je meer

De Nederlandse ICT-sector werkt al jaren samen aan het continu verbeteren van de veiligheid. Farwerck: “Samen bereik je meer. Belangrijker nog is dat als het om veiligheid gaat, je géén concurrenten hebt. Er zijn goede voorbeelden te noemen. Zo zijn meerdere Nederlandse providers betrokken bij de Dutch Continuity Board, waar gewerkt wordt aan maatregelen om de impact van DDoS-aanvallen op de Nederlandse kritieke infrastructuur te beperken en diensten bij verstoring zo snel mogelijk weer beschikbaar te maken. Daarin werken concurrenten als KPN, VodafoneZiggo en T-Mobile nauw met elkaar samen om Nederland nog veiliger te maken.

Quantum computing

Nieuwe technologische ontwikkelingen volgen elkaar in rap tempo op en daar moeten we ook in Nederland goed op inspelen. Zo is Farwerck ervan overtuigd dat quantum computing grote gevolgen zal hebben voor de manier hoe cybersecurity is georganiseerd. Farwerck: “De rekenkracht zal zo groot zijn dat veel huidige methoden van encryptie niet meer toepasbaar zullen zijn. Dat lijkt misschien nog ver weg, want kwantumcomputers worden op korte termijn niet verwacht. Toch moeten we hier nu samen mee aan de slag want we weten dat landen als China en de VS hier hard aan werken. Niet alleen vanuit een onderzoeksperspectief naar de mogelijkheden van quantum computing, maar ook naar de effecten, bijvoorbeeld op het gebied van internetveiligheid.”

Ook op praktisch gebied kan de overheid een belangrijke rol spelen. Het is te prijzen dat de overheid bij haar ICT-inkoop cybersecurity randvoorwaardelijk wil maken. Anderzijds ligt hier volgens Farwerck ook een uitdaging. “Tot op heden is vooral op prijs aanbesteed. Dit vereist dus ook dat de overheid anders moet gaan inkopen. Als er beperkingen zijn op het gebied van wet- en regelgeving dan moeten deze snel worden aangepakt”, aldus Farwerck.

“Het is van groot belang dat de overheid met de private sector en wetenschap samen optrekken”

“It is vitally important that the government joins forces with the private and scientific sectors in this regard”

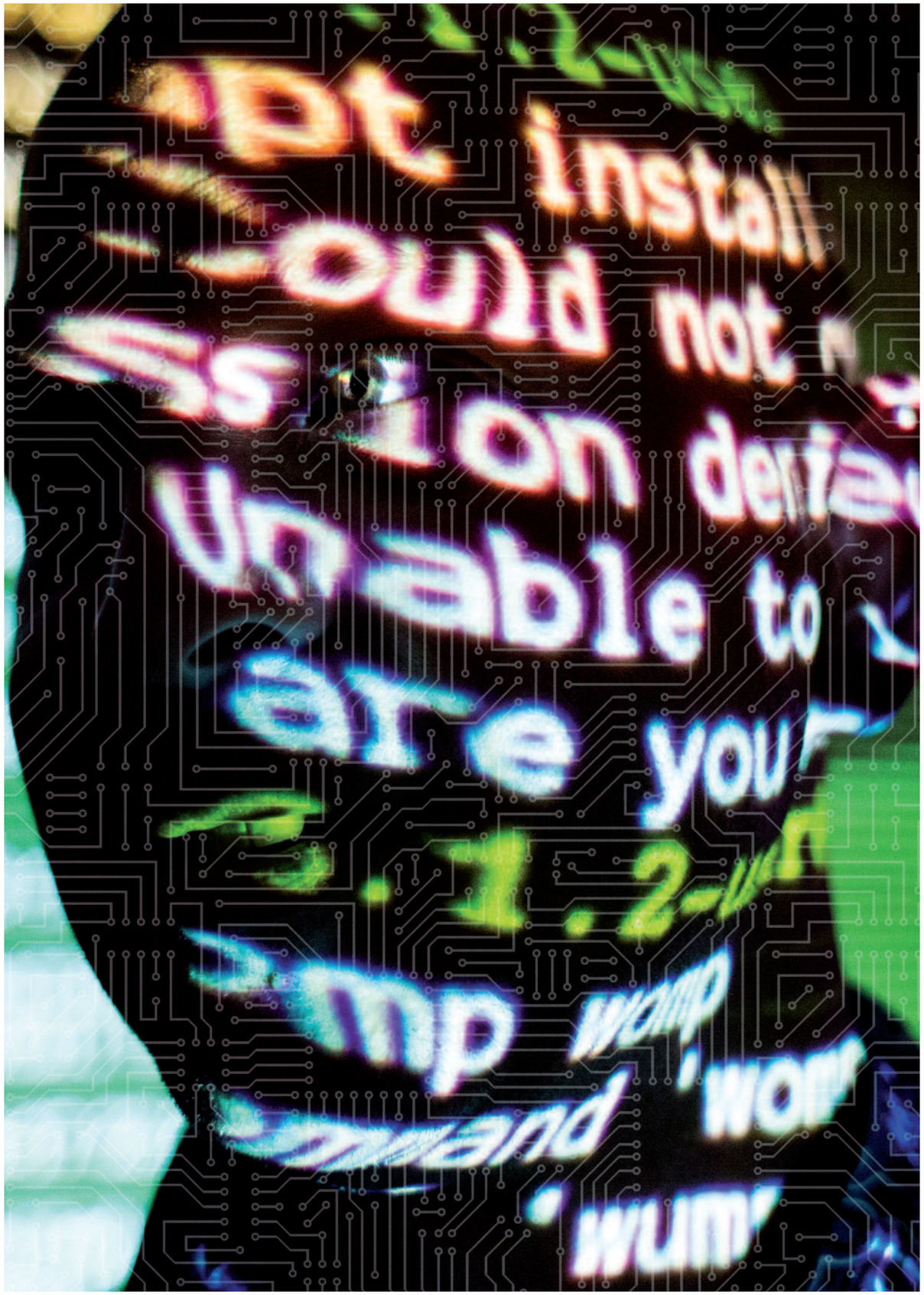
---

examples are legion. To name but one, internet service providers in the Netherlands have established the Dutch Continuity Board, which works on measures to limit the impact of DDoS attacks on Dutch critical infrastructure and to make services that have been disrupted available again as soon as possible. As part of this initiative, competitors such as KPN, VodafoneZiggo and T-Mobile work closely together to make the Netherlands more secure.’

Quantum computing

New technological developments occur in rapid succession and it is vital for the Netherlands to keep pace. Farwerck highlights the example of quantum computing, which he is convinced will have major consequences for the way cybersecurity is organised. Farwerck: ‘Computing power will become so vast that many current encryption methods will become obsolete. As quantum computers are unlikely to become available in the short term, this may seem a long way off. However, we know that countries such as China and the US are working hard on this, so we need to prepare for this together straight away – not just by carrying out research into the possibilities of quantum computing, but also by investigating its impact on such areas as online security.’

The government is able to play a key role in practical terms as well. It is commendable that the government has announced its intention to make cybersecurity a prerequisite for its ICT procurement. Yet Farwerck points out that this also represents a challenge. ‘Until now, the main procurement consideration has been price. This new policy will require the government to change its acquisition strategy. Any legal and regulatory obstacles should be addressed without further ado’, Farwerck argues.



INEKE DEZENTJÉ HAMMING-BLUEMINK

Nieuw lid van de Cyber Security Raad
New member of the Cyber Security Council (CSR)

“digitaal veilig data-uitwisseling is essentieel voor onze concurrentiepositie”
“A digitally secure exchange of data is vital to maintaining our competitive position”

Ineke Dezentjé Hamming-Bluemink is sinds november 2011 voorzitter en algemeen directeur van FME. Naast haar rol als voorzitter FME en raadslid van de CSR is Ineke Dezentjé Hamming-Bluemink onder andere voorzitter Smart Industry, neemt ze deel aan Team ICT en de High Level Industrial Round Table 2030.

Ineke Dezentjé Hamming Bluemink has been Chair and General Manager of FME since November 2011. In addition to her role as President of FME and member of the CSR board, Ineke Dezentjé Hamming Bluemink also serves as President of Smart Industry and participates in Team ICT and the High Level Industrial Round Table 2030.

Waarom is cyber een belangrijk thema voor de maakindustrie?
Digitalisering van de Nederlandse technologische industrie maakt bedrijven in toenemende mate afhankelijk van ICT. Cyberincidenten vormen een concrete dreiging voor het innovatie en verdienvermogen van de technologische industrie. Daarom moeten we bedrijven digitaal weerbaar maken. Het realiseren van digitaal veilige data uitwisseling in de toeleverancierskеten is essentieel voor onze concurrentiepositie.

Wat is voor u het belang van de CSR?
De CSR signaleert wat er op Nederland afkomt en helpt bij het verhogen van de cybersecurity in ons land. In de raad is de gouden driehoek ofwel triple helix vertegenwoordigd en dat zorgt dat we vanuit de verschillende invalshoeken de cybersecurity ontwikkelingen kunnen beschouwen en daardoor tot afgewogen adviezen komen.

Why are cyber issues important to makers and manufacturers?
The digitalisation of the Dutch technological sector is making businesses increasingly dependent on ICT. Cyber incidents pose a concrete threat to the innovative ability and earning potential of the technological sector. We must therefore ensure businesses become digitally resilient. Achieving a digitally secure exchange of data within the supply chain is vital to maintaining our competitive position.

Why do you consider the CSR to be important?
The CSR observes and reports potential challenges to the Netherlands and helps strengthen cybersecurity in our country. The golden triangle or triple helix is represented in the council s membership, which allows us to view cybersecurity developments from a range of perspectives and therefore to arrive at well considered recommendations.

Ineke Dezentjé Hamming-Bluemink
President and General Manager of FME
and member of the Cyber Security Council

THE ENEMY ENTERS THROUGH THE WALL OUTLET

Nederlanders hebben bluetooth en wifi uitgevonden. Nu we middenin de vierde industriële revolutie zitten, moeten we ook de hotspot zijn op het gebied van cybersecurity. Nederland moet digitaal nog veiliger worden, want de bedreigingen zijn groot.

Onze technologische industrie beschikt over hoogwaardige kennis, waardoor de sector extra kwetsbaar is voor digitale dreigingen en economische spionage. Ook kennisintensieve MKB-bedrijven in de technologische industrie en technostarters die innovatieve ideeën en producten ontwikkelen, zijn regelmatig doelwit van actoren die auteursrechtelijk werk en intellectuele eigendommen willen stelen. Het zet onze concurrentiepositie onder druk.

Aanval

Het veranderende IT-landschap en de toename van IoT-apparatuur zorgen ervoor dat informatiebeveiliging voor bedrijven in de technologische industrie steeds meer is verweven met alle primaire bedrijfsprocessen. De gevolgen van een cyberaanval gaan dan ook veel verder dan omzetderving. Het schaadt het vertrouwen van de medewerkers, (toe)leveranciers én klanten. FME helpt ondernemers op allerlei manieren om digitaal veilig te zijn. Via Smart Industry bijvoorbeeld, lanceerden we eerder dit jaar de Cybersecurity Scan, die zich richt op de productieomgeving (het operationele technologische domein) en inzicht geeft in de cyberveiligheid van het bedrijf. Smart Industry heeft als ambitie om in Nederland in 2021 het meest flexibele, veilige en het best digitaal verbonden productienetwerk van Europa te hebben.

Maar we moeten ook kennis blijven ontwikkelen én in huis houden. De sterke groei van de digitale economie zorgt voor een nijpend tekort aan IT- en aanverwante specialisten. In samenwerking met het ministerie van Defensie en de Regionale Opleidingscentra zorgen we voor meer aandacht voor cyberveiligheid in de mbo-opleiding Veiligheid & Vakmanschap (VeVa). De samenwerking tussen Defensie en de technologische industrie zorgt daarnaast voor een ‘trusted environment’, waarin we kennis makkelijk kunnen uitwisselen en we snel kunnen schakelen indien nodig. Daarnaast faciliteert en ondersteunt de technologische industrie cyberreservisten en wordt er samen geoefend tijdens de NAVO Cyber Coalition, waarbij zowel militaire als civiele systemen digitaal worden aangevallen.

Both Bluetooth and Wi-Fi are Dutch inventions. Now that the fourth industrial revolution is well underway, the Netherlands must be the top cybersecurity hotspot as well. It is vital that our country enhance its digital security, as the threats are severe.

Our technological industry possesses high-quality knowledge, rendering the sector especially vulnerable to digital threats and economic espionage. Knowledge-intensive SMEs in the technological sector and tech start-ups working to develop innovative ideas and products are also frequent targets for actors looking to steal copyrighted work and intellectual property. This puts pressure on our competitive position.

Attack

As a result of the changing IT landscape and the growing number of IoT devices, information security is becoming increasingly integrated into all primary business processes of companies in the technological industry. This also means that the consequences of a cyber attack extend much further than loss of income. Such an attack damages the trust placed in a company by its employees, suppliers and customers.

FME helps business owners maintain digital security on a variety of fronts. To give one example of a Smart Industry project, we successfully launched the Cybersecurity Scan earlier this year. This scan focuses on the production environment (the operational technological domain) and provides insight into the cybersecurity of a given business. The goal of Smart Industry is to see the Netherlands attain the most flexible, secure and also best-connected digital production network in Europe by 2021.

Yet it is important that we continue to develop knowledge and retain it as well. The rapid growth of the digital economy has resulted in a major shortage of IT specialists and related professionals. In cooperation with the Ministry of Defence and the regional education and training centres, we are

Kansen
Digitalisering biedt enorme mogelijkheden. We kunnen een steeds ouder wordende bevolking gezond en vitaal houden en de overgang naar een schonere en duurzame energievoorziening versnellen. We kunnen de samenleving veiliger maken en de beschikbaarheid en veiligheid van voedsel voor de wereldbevolking garanderen. Maar om de kansen die digitalisering biedt blijvend te kunnen benutten, is het noodzakelijk dat we ons met vertrouwen in de digitale wereld kunnen bewegen. Nadenken over de gevolgen van een cyberincident op basis van risicoanalyse en anticiperen op een eventuele aanval, is voor elke onderneming, organisatie en overheid een must. Alleen zo kunnen we Nederland klaarstomen voor de toekomst. Met een technologische industrie die in het hart van de samenleving staat.

“We moeten de hotspot zijn op het gebied van cybersecurity”
“We must be the top cybersecurity hotspot”

ensuring greater attention to cybersecurity in the ‘VeVa’ secondary vocational training programme (*Veiligheid & Vakmanschap*, or Security & Expertise). Another result of the partnership between the Ministry of Defence and the technological sector is a trusted environment in which we can easily exchange knowledge and, when necessary, quickly respond to changing circumstances. The technological sector also facilitates and supports ‘cyber-reservists’ and participates in joint exercises involving mock digital attacks on both military and civilian systems during the NATO Cyber Coalition.

Opportunities
Digitalisation offers enormous opportunities. It can enable us to keep an increasingly greying population healthy and vital and speed up the transition to a cleaner, more sustainable energy supply. It can help us make society safer and guarantee the availability and safety of food for the global population. If we are to successfully exploit the opportunities from digitalisation in the long term, we must be able to operate confidently in the digital world. It is absolutely vital that every business, organisation and government consider the consequences of a cyber incident based on a risk analysis and strive to anticipate potential attacks. It is the only way to effectively prepare the Netherlands to meet future challenges: with a technological sector centred firmly at the heart of our society.

Begin dit jaar is de brancheorganisatie Cyberveilig Nederland opgericht, een initiatief van acht cybersecurity-dienstverleners. Doel van de organisatie is de digitale weerbaarheid van Nederland te vergroten en daarnaast de kwaliteit en transparantie binnen de groeiende cybersecurity sector te verhogen. Petra Oldengarm, directeur, en Liesbeth Holterman, beleidsadviseur, vormen het gezicht van Cyberveilig Nederland. Samen geven zij een reflectie op de verschillende cybersecurity-strategieën. “Het mag allemaal wel wat holistischer”, vertelt Oldengarm.

The industry organisation Cyberveilig Nederland (Digitally Secure Netherlands), an initiative of eight cybersecurity service providers, was founded at the start of this year. The aim of the organisation is to improve the Dutch digital resilience as well as to increase the quality and transparency of the growing cybersecurity sector. Director Petra Oldengarm and Policy Advisor Liesbeth Holterman are the public face of Cyberveilig Nederland. Together, they share their reflections on the various cybersecurity strategies. 'A slightly more holistic approach is needed,' says Oldengarm.

Petra Oldengarm and Liesbeth Holterman
Director Cyberveilig Nederland and Policy Advisor Cyberveilig Nederland

‘A MORE HOLISTIC APPROACH IS NEEDED’

Zowel Oldengarm als Holterman zijn positief over de strategieën die er nu liggen. Ze kunnen zich goed vinden in veel facetten die genoemd zijn, zoals de veiligheid van het Internet of Things en de Roadmap Digitaal Veilige Hard- en Software. De onderlinge samenhang van alle strategieën verdient volgens beiden nog wel de aandacht. “Het is nu te versnipperd”, vertelt Oldengarm. “Cybersecurity is vandaag de dag zo verweven in al onze processen en dat vraagt om een integrale en brede aanpak. Het mag geen dossier van één ministerie zijn. We hebben een holistische visie nodig en daarvoor moeten we uit onze koker stappen.” Holterman vult aan: “Het is een gemiste kans als we dit niet doen. In de digitaliseringsagenda van het ministerie van Economische Zaken en Klimaat zijn zoveel mooie kansen voor de economie beschreven die vragen om een integrale aanpak. Alleen zo kan je de randvoorwaarden voor digitalisering goed beetpakken en de basis van cybersecurity aanpakken op alle niveaus.”

Laaghangende fruit
Vanuit de brancheorganisatie willen Oldengarm en Holterman zich hier ook hard voor maken. Daarom sluit Cyberveilig Nederland zich ook aan bij de Cybersecurity Alliantie. Oldengarm: “Het is een goed initiatief

Both Oldengarm and Holterman feel positive about the strategies currently in place. They mention a number of aspects which they welcome, including the security of the Internet of Things or the Digitally Secure Hardware and Software Roadmap. Both agree that the interconnectedness of the various strategies deserves more attention. 'Things are too fragmented at present,' says Oldengarm. 'Cyber-security is now interlocked into so many processes that a compre-hensive, integrated approach is essential. It is not a matter than can be dealt with by a single ministry. A holistic approach is needed, which means that we need to think outside the box.' Holterman adds: 'If we do nothing, it will be a real missed opportunity. While the digitalisation agenda established by the Ministry of Economic Affairs and Climate Policy describes so many great opportunities for the economy, they all require an inclusive approach. It is the only way to really create the necessary preconditions for digitalisation and solidify the foundation for cyber-security at all levels.'

Low-hanging fruit
Oldengarm and Holterman intend to work hard on promoting this issue, using the industry organisation as a platform. As part of this strategy, Cyberveilig Nederland has joined the Cyber Security Alliance. As Oldengarm says: 'It is a good initiative, to which a number of different parties have already committed. The question now is how we can give meaning and substance to the agenda. There are many different forums in the Netherlands, so how can we make sure that this

waar verschillende partijen zich aan hebben gecommitteerd. De vraag is nu wel hoe we gezamenlijk inhoud en invulling aan de agenda kunnen geven. Er zijn verschillende gremia in Nederland, dus hoe zorgen we ervoor dat dit initiatief ook meerwaarde heeft? Deze doe-modus is voor ons belangrijk!" Op de vraag wat er moet gebeuren om dit ook daadwerkelijk te bereiken, is Holterman stellig. "Hang een prijskaartje aan de ambities uit de Nederlandse Cybersecurity Agenda en maak duidelijk waar de prioriteiten liggen. Op die manier maak je het concreet en open je de discussie waarmee je energie creëert." Dit vraagt volgens Oldengarm wel om mensen die de vertaalslag kunnen maken van strategie naar de praktijk. "Personen die kunnen schakelen van strategisch, naar tactisch en operationeel niveau." Het is best lastig om deze personen te vinden, beseft Oldengarm. "Door een vertaalslag te maken, blijf je niet hangen in alleen een visie of een strategie. Je komt dan tot concrete plannen en je kunt het laaghangende fruit daadwerkelijk 'pakken' en ontstaat er meer energie voor vervolg."

Informatiedeling

Over de toekomst van een digitaal veilig Nederland zijn beiden positief gestemd. Holterman: "De mate van vertrouwen in elkaar, in Nederland en Europa, is zowel publiek als privaat gigantisch. Af en toe vinden we elkaar lastig, maar uiteindelijk praten we met elkaar en zitten we in de juiste modus." Oldengarm vult aan: "Ik ben er daarmee van overtuigd dat als er iets gebeurt dat we over de juiste mensen beschikken om een digitale crisis op te lossen." Aandachtspunt blijft volgens beiden informatiedeling. "De komst van het Digital Trust Center is een goede start, omdat dit de informatievoorziening aan alle Nederlandse bedrijven bevordert. De uitdaging blijft om ervoor te zorgen dat de informatieknooppunten aan elkaar worden geknoopt en dat er geen dubbele knopen worden gelegd", legt Holterman uit. "... en dat ze niet in de knoop raken!", vult Oldengarm tot slot aan.

"We moeten uit onze koker stappen"

'We need to think outside the box.'

initiative adds real value? The way in which we approach the matter is important to us!' Holterman has firm opinions on what needs to happen in order to achieve this goal: 'Put a price tag on the ambitions in the National Cyber Security Agenda and make it clear what the priorities are. That approach will make the agenda more tangible and start a discussion which will create a buzz.'
According to Oldengarm, this process requires people who are able to translate strategy into practice: 'People who can make the shift from a strategic level to a tactical and operational level.' She realises that it can be pretty tough finding such people. "To implement a transition, you need to avoid having only one vision or one strategy. This attitude then allows you to come up with specific plans, so you can really grab the low-hanging fruit and generate a buzz which will facilitate the next step.'

Information sharing

Both women are positive about the future of a digitally secure Netherlands. According to Holterman: 'There is a huge level of mutual trust in the Netherlands and across Europe, within both the public and private sectors. Although we get on each other's nerves from time to time, we sit down at the end of the day to talk it through and find a way forward.'
'I am convinced that if something happens,' Oldengarm adds, 'we have the right people to resolve a digital crisis.' Both agree that the focus must be on sharing information: 'Setting up the Digital Trust Centre was a good start,' says Holterman, 'because it can provide information to all Dutch businesses. The challenge now is to make sure that the information hubs are tied together and there are no double knots.' 'And that they do not get tangled!' Oldengarm adds.

In oktober 2016 bracht Herna Verhagen, CEO van PostNL, haar adviesrapport ‘De economische en maatschappelijke noodzaak van meer cybersecurity, Nederland digitaal droge voeten’ uit. Voor dit onafhankelijke onderzoek dat ze op verzoek van de Cyber Security Raad heeft uitgevoerd, sprak ze onder meer met diverse cyberexperts om de economische en maatschappelijke noodzaak van meer cybersecurity te onderzoeken. Nu bijna twee jaar later geeft zij haar visie op de huidige stand van zaken.

Herna Verhagen, CEO of PostNL, released her report entitled ‘The economic and social need for more cybersecurity: Keeping “dry feet” in the digital era’ in October 2016. For this independent study, which she conducted at the request of the Cyber Security Council, she spoke with a wide range of cyber experts and other specialists to investigate the economic and social need for more cybersecurity. Now, nearly two years later, she shares her views about the current state of affairs.

Herna Verhagen
CEO of PostNL

NEDERLAND DIGITAAL DROGE VOETEN

KEEPING “DRY FEET” IN THE DIGITAL ERA

CYBERSECURITY IS AN ENDURING ISSUE

Nederland loopt voorop in de digitale wereld en is één van de meest ICT-intensieve economieën van Europa, zo blijkt uit het rapport van Verhagen. Digitalisering biedt enorme kansen voor de samenleving en economie, maar dan is het wel zaak te zorgen dat de digitale wereld veilig en vertrouwd blijft. Volgens Verhagen is er maar één manier om de cybersecurity op orde te brengen: samenwerken! “Gezien het aantal cyberincidenten en de toegenomen dreiging sinds oktober 2016, zijn mijn adviezen ook in 2018 helaas nog onverminderd van kracht”, vertelt Verhagen.

Actieprogramma

Om de cybersecurity te versterken en de digitale weerbaarheid te vergroten is een meerjarig actieprogramma inclusief investeringsagenda noodzakelijk, zo schreef Verhagen. Een

The Netherlands is leading the way in the digital world and has one of the most IT-intensive economies in Europe, as Verhagen’s report showed. While digitalisation offers enormous opportunities for society and the economy, it makes it all the more important to ensure that the digital world is (and remains) safe and reliable. According to Verhagen, there is only one way to make cybersecurity a reality: collaboration! 'Given the number of cyber incidents and the increased threat since October 2016, my recommendations are unfortunately still as relevant as ever in 2018.'

Action programme

Verhagen wrote that in order to strengthen cybersecurity and improve digital resilience, a multi-year action programme including an investment agenda is necessary. This action programme should be drawn up by the government, in collaboration with the private organisations and local authorities. According to Verhagen, the action programme needed to address a number of specific matters. For instance, the government must set a good example by including digital security and protection of privacy as key priorities in its own digital (business) operations. In addition, the powers of the Dutch investigative, intelligence and security services must be modernised. Verhagen also recommends that the government plays a role in encouraging and – if necessary – compelling the private sector to take its own responsibility, as well as introducing and encouraging supply chain responsibility between companies: 'It is important that the private sector has its affairs in order as well and complies with the preconditions for cybersecurity. The statutory duty of care for IT products and services must also be enforced, as it would be for any other type of product. Among other reasons, cyber threats exist because unsafe products and services are available on the market, due to a lack of regulations and the pressure of "time to market". In my view, the government has an important role to play in remedying this issue. The introduction of an accreditation or

“Het bedrijfsleven moet ongeveer 10% van het jaarlijkse ICT-budget besteden aan cybersecurity”

'The business community should invest around 10% of their annual IT budget on cybersecurity.'

certification system would also increase the security of IT products and services and reduce the threat.' Finally, Verhagen suggests that the government and the business community should invest around 10% of their annual IT budgets on cybersecurity.

The collective ambition is there

Verhagen sees many of her recommendations reflected in actions and initiatives and in particular the ambitions from the National Cybersecurity Agenda (NCSA). As she points out: 'The Minister of Justice and Security is the coordinating Minister for cybersecurity. While the agenda and the collective ambition are there, both now need to be fleshed out and translated into actions and measures, backed up by funding. In my view, the 95 million euros of corresponding funding which the government has earmarked in the coalition agreement is a good first step. However, if you look at neighboring countries and the importance of cybersecurity, you can see that it requires additional investment. I commit to actively supporting the implementation of the NCSA.'

Much progress still to be made

Verhagen understands that several of strategies exist: 'There are many different sides to cybersecurity and every party looks at it from a different perspective or with different responsibilities. As long as we work with the collective ambition of strengthening cybersecurity and the government keeps a watchful eye on the higher goal (acting as a coordinator), it is not really a problem. However, it is not just the government that needs to act; every company and organisation has its own primary responsibility. If companies do not invest in their cybersecurity, companies will undoubtedly put their business processes and thus their own competitive position at risk in the long run. Security as a prerequisite or ‘licence to operate’ in the production process should be a natural part of the corporate governance code. In my opinion, there is much progress still to be made.'

actieprogramma dat door het kabinet in samenwerking met het bedrijfsleven en decentrale overheden wordt opgesteld. Het actieprogramma moest volgens Verhagen een aantal concrete zaken adresseren. Zo moet de overheid het goede voorbeeld geven door (digitale) veiligheid en bescherming van privacy op te nemen als speerpunten in de eigen digitale bedrijfsvoering. Daarnaast moeten de bevoegdheden van de Nederlandse opsporings-, Inlichtingen- en Veiligheidsdiensten worden gemoderniseerd. Ook adviseert Verhagen dat de overheid een rol moet hebben in het stimuleren en zo nodig afdwingen van de eigen verantwoordelijkheid bij de private sector alsook het introduceren en stimuleren van de zogenaamde ‘ketenverantwoordelijkheid’ tussen bedrijven. “Het is belangrijk dat ook de private sector zijn zaken op orde heeft en voldoet aan de randvoorwaarden voor cybersecurity”, stelt Verhagen. “Ook moet er invulling worden gegeven aan de wettelijke zorgplicht van ICT-producten en -diensten. Zoals dat geldt voor ieder ander product. Cyberdreigingen ontstaan onder andere omdat er onveilige producten en diensten op de markt beschikbaar komen, vanwege gebrek aan eisen en de druk van ‘time to market’. De overheid heeft wat mij betreft een sturende rol om dit te verhelpen. Ook het introduceren van een accreditatie- of certificeringssystematiek verhoogt de veiligheid van ICT-producten en – diensten en doet de dreiging daarmee afnemen” Tot slot stelt Verhagen dat overheid én bedrijfsleven ongeveer 10% van het jaarlijkse ICT budget moeten besteden aan cybersecurity.

De gezamenlijke ambitie is er

Veel van haar aanbevelingen ziet Verhagen terug in acties, initiatieven en zeker in de ambities uit de Nederlandse Cyber Security Agenda ofwel de NCSA. Verhagen: “De coördinatie op cybersecurity is belegd bij de minister van Justitie en Veiligheid. De agenda en de gezamenlijke ambitie is er. Nu moet het een en ander wel verder worden uitgewerkt in acties en maatregelen, mét bijbehorende financiering. De 95 miljoen euro die het kabinet structureel heeft vrijgemaakt in het regeerakkoord is daarin wat mij betreft het eerste stapje. Maar als je kijkt naar landen om ons heen en het belang van cybersecurity, vraagt dat om meer middelen. Ik maak mij hard om een bijdrage te leveren aan de uitwerking van de NCSA.”

Nog veel terrein te winnen

Dat er verschillende strategieën bestaan, begrijpt Verhagen. “Er zitten verschillende kanten aan cybersecurity en elke partij bekijkt dit vanuit een andere invalshoek of verantwoordelijkheid. Zolang we werken aan de gezamenlijke ambitie om cybersecurity te versterken en het kabinet zicht houdt (coördinatie) op het hogere doel, is dat niet erg. Niet alleen de overheid is daarbij aan zet; elk bedrijf of organisatie is zelf primair verantwoordelijk. Wanneer bedrijven niet investeren in hun cybersecurity brengt dat op den duur hun bedrijfsprocessen en daarmee de eigen concurrentiepositie ontegenzeggelijk in gevaar. Security als randvoorwaarde of ‘license to operate’ in het productieproces moet een vanzelfsprekend onderdeel van de ‘corporate governance code’ zijn. Daar is nog veel terrein te winnen is mijn opvatting”, benadrukt Verhagen.

‘Groot helpt klein’

Volgens Verhagen is het belangrijk dat bedrijven hun eigen netwerken beschermen en zich weerbaar maken tegen cyberaanvallen. “In de private sector zijn grote ondernemingen veelal voldoende ‘cyber aware’ en wordt cybersecurity gezien als een randvoorwaarde voor het voortbestaan van de onderneming”, vervolgt Verhagen. “Dat geldt in soms mindere mate voor de kleine(re) ondernemingen. Vanwege de toenemende connectiviteit en ketenafhankelijkheid zorgt dat voor een risico in de gehele keten. Daarom moet invulling worden gegeven aan ‘ketenverantwoordelijkheid’. Zo kan een grote onderneming met veel kennis en expertise in huis, de kleine onderneming in de keten helpen om meer secure te worden, bijvoorbeeld door kennis beschikbaar te stellen ofwel ‘groot helpt klein’. Dat is niet alleen een advies dat ik geef, maar ook zelf, in mijn rol als CEO van Post NL, actief in mijn keten toepas.”

Onderwijs en onderzoek zijn cruciaal om de kennispositie van Nederland te bewaken; ons land is immers een kenniseconomie. We moeten ervoor waken dat we in de toekomst afhankelijk zijn van experts en kennis uit landen om ons heen. Verhagen: “Het stemt mij daarom positief dat het kabinet heeft toegezegd structureel te investeren in cybersecurity-onderzoek en dat daar een eerste financiële impuls aan wordt gegeven.”

Beweging in de goede richting

“Kortom, we zijn er niet”, sluit Verhagen af. “Cybersecurity is een blijvend thema. Maar we maken wel een beweging in de goede richting. En ik blijf mij actief bezighouden met het onderwerp, omdat ik geloof in de kansen die digitalisering ons (bedrijfsleven en maatschappij) biedt, mits we die digitale wereld veilig houden.”

‘Major businesses helping small(er) businesses’

Verhagen believes that companies must protect their own networks and ensure that they have the capacity to build resilience against cyber-attacks. 'In the private sector, major businesses often are adequately "cyber aware" and while cybersecurity is seen as a prerequisite for the survival of the business. The same does not always apply equally to small(er) businesses. However, with increasing connectivity and supply chain interdependencies, risks now affect the entire chain. For this reason, "chain responsibility" must be enforced. Through this a large business with a lot of in-house knowledge and expertise can help the small businesses in its chain in becoming more secure; for example, by making its knowledge available in accordance with the principle that major businesses should help small(er) businesses. It is not merely a recommendation, as CEO of PostNL, I actively apply this principle in the chain.

Education and research are crucial to protect the Dutch knowledge position; after all, our country has a knowledge economy. We must take steps to ensure that we do not become dependent on experts and knowledge from surrounding countries in the future. Verhagen adds: 'I am therefore pleased that the government has pledged to make ongoing investments in cybersecurity research and that it will be providing an initial financial stimulus.'

Moving in the right direction

'All in all, we are not there yet,' Verhagen concludes. 'Cybersecurity is an ongoing issue. However, we are moving in the right direction. I will remain active working on this issue, because I believe in the opportunities that digitalisation can offer to businesses and to society in general, provided that we keep the digital world safe.'

Melissa Hathaway
leading expert in cyberspace
policy and cybersecurity

AMBITION VS. PROGRESS:

THE NATIONAL CYBER-SECURITY AGENDA OF THE NETHERLANDS

In April 2018, the Netherlands published a new National Cybersecurity Agenda: A Cybersecure Netherlands (NCSA), articulating its plan to create a more secure and resilient nation. The plan is a continuity of the country's ambitious goals, previously laid out in the 2016 *National Cyber Security Strategy 2: From Awareness to Capability (NCSS2)*. The new NCSA was developed in response to a request from the new four-party coalition government in October 2017. The new government was aware of both the digital risks and the economic and social opportunities that the Netherlands was facing in cyberspace, and understood that the country also had the potential to become the bridge between the United Kingdom (UK) and Europe after Britain's decision to exit the European Union (EU). Additionally, the government counted on the fact that the Netherlands would be perceived as a more politically stable country for conducting business during a time of increased populist movements throughout Europe. Anticipating the most advantageous results, the government agreed to further support cybersecurity initiatives, increased funding by at least 300 million euro over four years, and requested the National Coordinator for Security and Counterterrorism (NCTV) within the Ministry of Justice and Security, to develop an action plan for the way forward. (i.e. the NCSA).

Despite the seven ambitious strategic goals* contained in the NCSA, however, the document lacks a fundamental focus on the economic prosperity and future of the Netherlands' digital economy and its strengths — all of which must be underpinned by secure, trusted, and resilient cyber infrastructures and services. The action plan fails to connect the economic imperatives to the security agenda of the country — the predicate to the argument of why cybersecurity is important to the nation and society. This nexus cannot be ignored especially for a highly-digitalised country like the Netherlands — one of the top 10 most connected countries globally and a top 10 exporter of ICT goods and telecommunication services around the world with a digital economy that accounts for almost 25% of its gross domestic product (GDP). Government leaders hope for the Netherlands to become an Internet pioneer and leader in developing secure hardware and software products, but this ambition requires tighter alignment of the objectives in the NCSA to the country's national economic objectives.

The Netherlands has been steadily improving its cybersecurity posture at the national level, albeit, not at the pace of its ambitions. Some successful initiatives from the NCSS2 include:

- In February 2017, the Ministry of Foreign Affairs published an *International Cyber Strategy*;
- In April 2018, the Ministry of Economic Affairs and Climate published a *Roadmap for Digitally Secure Hardware and Software*;
- In June 2018, the Dutch Cybersecurity Platform for Higher Education and Research (dcypher) published the third edition of the *Dutch National Cyber Security Research Agenda (NCSRA III)* and advanced its initiatives for higher education;
- In June 2018, the Ministry of Economic Affairs published a *Strategy on Digitalisation*.
- In July 2018, the Ministry of Foreign Affairs launched a network of foreign service personnel responsible for cybersecurity matters and placed the first embassy officials in the UK, Japan, and the United States;
- *A Digital Trust Center* was launched to raise awareness and provide tools to small and medium enterprises (SMEs); and
- Funding was allocated to accelerate the operationalization of the Law on Computer Criminality III.

* The seven NCSA strategic goals are: (1) The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats; (2) The Netherlands contributes to international peace and security in the digital domain; (3) The Netherlands is at the forefront of digitally secure hardware and software; (4) The Netherlands has resilient digital processes and a robust infrastructure; (5) The Netherlands has successful barriers against cybercrime; (6) The Netherlands leads the way in the field of cybersecurity knowledge development and (7) The Netherlands has an integrated and strong public-private approach to cybersecurity.

Foto: Jeff Lubin

"Government leaders hope for the Netherlands to become an Internet pioneer and leader in developing secure hardware and software products, but this ambition requires tighter alignment of the objectives in the NCSA to the country's national economic objectives"

Moreover, the Ministry of Defence intends to publish a *Defence Cyber Strategy* and the Ministry of International Affairs and Kingdom relations will publish a strategy on the *Digital Agenda for Government* in 2018.

The NCSA is "closely related to these documents" but there is still no apparent overarching national architecture and vision that integrates them. National leaders should recognize that cyber readiness and preparedness begin first and foremost with an effective risk management approach that encompasses a clear understanding of their country's high-value assets and high-impact systems that require increased levels of protection — the country's most critical digital dependencies (e.g., companies, infrastructures, services, and assets)." The Netherlands has yet to carry out such a comprehensive cyber risk assessment, identify its high-value assets and high-impact systems, and design an overarching strategy to address the risks associated with them. This was exemplified in June 2017, when the port of Rotterdam — the largest port in Europe — was significantly affected and its services degraded by the NotPetya destructive malware. The Netherlands had defined critical infrastructure in 2015 "as a set of products, services, and underlying processes that is necessary for the functioning of the country [and that] must be secure and able to withstand and rapidly recover from all hazards." However, when officials began to examine the state of the port's Internet dependencies, they discovered that only the port's waterway infrastructure — and not the facilities of several enterprises that impact the national economy — had actually been deemed critical in their national cybersecurity strategy and infrastructure protection policies.

Furthermore, the Netherlands has yet to officially transpose the EU directive for the Security of Network and Information Systems (NIS) into national legislation. Only when its draft Cybersecurity Law, which was approved by the House and is pending approval by the Senate, is adopted, the Netherlands will be compliant with the EU NIS Directive. The Cyber-security Law will also codify the responsibility of Ministry of Justice and Security and the national Computer Security Incident Response Team (CSIRT) for the ensuring the security and resilience of government and vital infrastructures. This will be essential in order to review and potentially modify the list of what the country deems most "critical" (e.g., companies, infrastructures, services, and assets). For instance, the two most important gateways of commerce (i.e., Port of Rotterdam and Schiphol Airport) should be on that list. Additionally, the high-tech industry that is going to be the core of future technologies and economic growth, including 5G communications, quantum computing, and next generation micro-electronics — many of them co-located at the

Eindhoven high-tech cluster and near the technical universities — should be protected too. Risk management requires proactive anticipation of threats and continuous assessment of vulnerabilities within the country's most critical digital dependencies. The NCSA states that it will be updated again in 2021, but is that soon enough considering that, by then, the Netherlands' digital economy will already represent 25% of its GDP and possibly more?

The government committed to a structural investment of 95 million euro for cybersecurity. The investment is certainly significant for a country the size of the Netherlands, but when it is divided among multiple ministries and organizations to hire personnel, build capability and processes, and establish mechanisms for cooperation with industry, the money will not go far. Sufficient, consistent, and continuous funding, informed by national cyber risk assessments, is required to ensure successful outcomes to an ambitious agenda. Not having a central authority to manage and track the milestones against clearly-defined timeframes may reduce the effectiveness of the overall Dutch strategy. The Netherlands' approach to managing national cyber risk is still decentralized and dependent on the polder model process of cooperation. There are at least 20 different ministries and government organisations with individual and collective responsibilities for enhancing the cybersecurity posture of the Netherlands, but no one agency has overarching authority to ensure the national cybersecurity architecture is achieved. The NCSA highlights this problem and notes that civil-military cooperation should be accelerated and roles and responsibilities need clarification, but it does not propose a governance mechanism to ensure the whole-of-government executes its ambitious plan. Effective implementation of the NCSA requires leadership and governance too — clearly defining and clarifying roles, responsibilities, processes, decision rights, and accountability mechanisms.

The Netherlands has both great potential and a long way to go to become cyber ready. Its ambitious goals should not be compromised by bureaucratic structures and processes that masquerade the appearance of progress.

Melissa Hathaway
Leading expert in cyberspace policy and cybersecurity. President of Hathaway Global Strategies LLC and Senior Fellow and member of the Board of Regents at Potomac Institute for Policy Studies.

In May 2017 Melissa Hathaway and Francesca Spidalieri, published 'Cyber Readiness Index At A Glance: The Netherlands'. The report was performed by the Potomac Institute for Policy Studies (PIPS) and commissioned by the Dutch Government. It is the latest study in a series of country reports assessing national-level preparedness for cyber risks based on the Cyber Readiness Index (CRI) 2.0 methodology.

"Sufficient, consistent, and continuous funding, informed by national cyber risk assessments, is required to ensure successful outcomes to an ambitious agenda"

Troels Oerting
Head of Global Centre for Cybersecurity (GCC) at World Economic Forum

"We ensure that the internet continues to be the foremost engine for communication, prosperity, and innovation the world over"

A STRATEGY TO DEFEND GLOBAL INNOVATION

All roads to a successful digital future go through security. True security is, itself, impossible without effective cooperation and unified standards – after all, as we become more interconnected, globally, so do our risks.

These ideas were at the heart of European Commission President Jean Claude Juncker's State of the Union delivered in September of last year, where he announced the intention of the European Commission to propose new legislation to support a more secure and resilient European digital economy as part of the Digital Single Market Strategy. Likewise, these ideas are the intellectual foundation of the Centre for Cybersecurity, established in January 2018 by the World Economic Forum in order to mobilize the capabilities of a global network of partners from business, government, international organizations, academia and civil society to enhance international cybersecurity and resilience.

In our view, there are three vital tasks before us in order to effectively improve global cybersecurity and protect our businesses and institutions. We must reduce the global attack surface, contain cyberattacks as they happen, and deter malicious actors. In order to do so, we need better policies, laws, regulations and standards. Additionally, we need better cooperation at every level (from leaders to individuals, from government to businesses) and more effective deterrents to criminals and others seeking to subvert our shared networks for illicit purposes. Going it alone is no longer possible. We must act together, as force multipliers and as partners to rebuild trust globally.

With its emphasis on improving partnership and harmonizing efforts to improve security, we believe that the EC proposed regulation is an important step in the right direction.

Based on President Jean Claude Juncker's address, the proposal for regulation, delivered in May and agreed to by the Council on 8 June 2018, recognizes that agility is vital in order to meet the challenges of a constantly evolving and changing threat in cybersecurity. The regulation empowers ENISA to take a more active role in advising the EU and member states. In order to play this vital role, an additional part of ENISA's mandate is to work together with other nations and international organizations – a recognition that this is truly a global challenge and that our risks are interdependent, requiring global cooperation in order to meet our shared security burdens.

The proposed regulation also sets forth the requirements for a unified European cybersecurity certification framework, an effective standard that promotes both security and cooperation across jurisdictions. Since both security and trust are rooted in stability, harmonizing certifications is an important step in order to achieve both and thereby foster the continued growth of our economy and continued protection of our vital institutions. We have no doubt that this harmonization will help to foster more effective security, more efficiently delivered, in both public and private organizations throughout Europe.

This regulation, if adopted, will make cybersecurity coordination within Europe much more seamless and effective. The Centre for Cybersecurity looks forward to continuing our work with all of our partners in Europe and globally and we hope that this regulation will serve as a model for other regions as well. We do this, not because it is easy or because more regulation is a good in itself, but because this is what is necessary to ensure that the internet continues to be the foremost engine for communication, prosperity, and innovation the world over.

CYBER SECURITY RAAD

COLUMN

"It is about trust in industrial Internet of Things"

‘UPPING THE ANTE’

The European Commission put forward in September 2017 an ambitious upgrade of Europe’s cybersecurity strategy, a package of actions to address the explosion of threats and costs of cyber disruption and technology leaping forward. The new cyber strategy certainly does not come too early!

In its hard core is the proposed Cybersecurity Act. This firstly boosts ENISA, Europe’s Network and Information Security Agency in tasks and budget. Secondly, it puts in place an EU-wide legal framework for cybersecurity certification. This is truly new and urgently needed. It is about trust in industrial Internet of Things, smart grids, connected cars and consumer products like printers. The ambition is significant: combining cybersecurity standards with legally recognised one-stop certification and European trust labelling. This has potential international reach.

The approach is still modest, for example certification is voluntary. Member States and European Parliament still need to agree on this legislative proposal, hopefully resulting in a clear governance so that industry and Member States, with ENISA and the European Commission get to work rapidly. My experience with the Network and Information Security Directive is that all parties, from economic affairs to national security and intelligence, from public representatives to industry have to ‘get out of their box’ for a workable deal.

No surprise to hear that more will be needed. More money in the future EU budget and by countries and companies for Research & Development (including Artificial Intelligence and quantum), skills, robust infrastructure and cyber-defense. More exercises to deal with future large-scale incidents (learning from past incidents such as NotPetya), with willingness to act politically. We have to get ahead of the curve as cybercriminals and malicious states threaten our strategic autonomy, our very capability to decide on essential aspects of our longer-term future in economy, society and democracy.

Finally, rankings suggest that internationally Europe is not a laggard and in certain areas even a leader (such as in secure data protection and potentially in cyber certification). To move to pole position, we need to act upon good policy intentions, put money on the table, cooperate profoundly, walk the talk. This should be the yardstick for European cybersecurity.

Paul Timmers
Independent advisor for digital innovation, visiting fellow Oxford University and former director of the European Commission for Digital Society, Trust & Cybersecurity

(opinion in personal capacity).

De Internet Corporation for Assigned Names and Numbers ofwel ICANN is een Amerikaans bedrijf zonder winstoogmerk. ICANN helpt het internet in de wereld stabiel en veilig te houden door topleveldomeinnamen toe te wijzen en beleid te ontwikkelen voor de generieke domeinen, zoals .com en .org en landendomeinen zoals .nl (Nederland). Lousewies van der Laan is lid van de International Board of Directors bij ICANN. Met haar ging de Cyber Security Raad in gesprek over het belang van het werk van ICANN voor een digitaal veilige wereld.

The Internet Corporation for Assigned Names and Numbers (ICANN) is an American not-for-profit corporation. ICANN helps keep the internet stable and secure worldwide by assigning top-level domain names and supporting the development of policies for both generic domains, such as .com and .org, and country domains, such as .nl (the Netherlands). Lousewies van der Laan is a member of ICANN's International Board of Directors. The Cyber Security Council sat down with her to discuss the importance of ICANN's work for a digitally secure world.

Lousewies van der Laan
Member of ICANN's
International Board of Directors

LOUSEWIES VAN DER LAAN (ICANN):

A STABLE AND SECURE GLOBAL INTERNET

Van der Laan legt uit dat ICANN zich bezighoudt met de technische laag van het internet. "Het is de logische laag waar niemand over nadenkt. Want hoe komen al die pakketjes met e-mails, video's en foto's van A naar B? De pakketjes van nullen en enen moeten door allemaal kabels om snel op de plaats van bestemming te komen. Dan wil je wel dat jouw pakket op de juiste bestemming wordt afgeleverd. Daarvoor moet beleid worden gemaakt." Volgens Van der Laan kan je het vergelijken met het versturen van fysieke poststukken. "Op het moment dat er verwarring ontstaat, komen poststukken op het verkeerde adres terecht. Dit kan soms per abuis zijn, maar er kunnen ook partijen zijn die er belang bij hebben om het te misbruiken. Je moet er zeker van kunnen zijn dat als je het juiste adres invoert dat jouw bericht veilig aankomt dan wel dat je op de juiste website belandt. Dat is de basis en essentie van veilig internet."

As Van der Laan explains, ICANN is concerned with the technical layer of the internet. 'This is the logical layer that nobody gives a second thought to. This layer determines how data packages with emails, videos or pictures get from A to B. All these binary packages have to be routed through cables in order to arrive at their destination quickly. Naturally, you want your package to reach the correct destination. That requires creating policies.' Van der Laan compares it to sending tangible items through the mail. 'If the system is disrupted or the address is wrong, mail items arrive at the wrong destination. This may be by accident, but there may also be parties with an interest in abusing the system. If you enter the correct address, you must be able to rely on your message arriving safely or that you are visiting the correct website. That is the basis and the essence of a secure internet.'

Multi-stakeholder model

To achieve its aims, ICANN works with a multi-stakeholder model, in which individuals, national governments, organisations that assign IP addresses, industry, non-governmental organisations (NGOs), humans rights organisations and technical experts all play their part to arrive at a community-based, consensus-driven policymaking approach. Van der Laan: 'The stakeholders focus on solving the problems that have been identified. It's a fascinating model – everyone has their say. This is also why some governments are reluctant to fully engage, particularly autocratic governments of countries such as Russia and China. They are used to the government being in charge and not "just" being partners in a multi-stakeholder process.

According to Van der Laan, we have the multi-stakeholder model to thank for the internet working as smoothly as it does. 'If a country wants to build a website in a language that uses a non-Latin script, such as Chinese, Greek or Russian, there needs to be a policy in place in order to avoid confusion', Van der Laan explains. 'For instance, some Han Chinese characters are also used in

Multistakeholdermodel
ICANN doet dit op basis van een multistakeholdermodel waarin individuen, regeringen van landen, bedrijven die over IP-adressen gaan, commerciële bedrijven, maar ook niet-gouvernementele organisatie (NGO's), mensenrechtenorganisaties en techneuten een belangrijke rol spelen in de op de gemeenschap gebaseerde, consensusgestuurde, beleidsvormende aanpak. Van der Laan: "Het zijn de stakeholders die zich richten op de oplossingen voor de problemen die er liggen. Ik vind dit een fascinerend model; iedereen heeft inspraak. Dat is ook een van de redenen waarom regeringen het soms lastig vinden, vooral autocratische regeringen als Rusland en China. Die zijn gewend dat de regeringen de baas zijn en niet dat zij een van de partners in een multistakeholderproces zijn."

Dat het internet goed werkt, komt volgens Van der Laan juist omdat het volgens het multistakeholdermodel is opgebouwd. "Wanneer een land een website wil maken in niet-Latijnse scripts, denk aan Chinees, Grieks of Russisch, dan moet hier beleid voor worden gemaakt om te voorkomen dat er verwarring op ontstaat", vertelt Van der Laan. "Zo zijn bepaalde symbolen in het Han Chinees bijvoorbeeld hetzelfde als in het Japans. Een bericht die verzonden wordt vanuit Tokyo zou dan wel eens ergens in Beijing kunnen landen, terwijl dit niet de bedoeling was. Dus daar moet beleid op worden gemaakt en processen voor worden afgesproken. En dat lukt gewoon! De technici zijn bij ons de echte experts en geven de doorslag. Zij weten op welke manier dit het veiligst kan. En als er consensus is, dan is dat het nieuwe wereldwijde beleid over welke symbolen te gebruiken zijn. Zo heeft Irak onlangs .irak in het Arabisch ingevoerd."

AVG
Net als het internet zijn ook de multistakeholders global. "Daarom vinden de vergaderingen wereldwijd plaats", vervolgt Van der Laan. "Wat we heel graag willen is dat die verbindingen overal blijven lopen en dat de technische laag blijft werken zonder dat er bijvoorbeeld een firewall wordt opgezet door een land als China. De vergaderingen wisselen daarom af in alle regio's." Tijdens de laatste vergadering is er veel over de Algemene verordening gegevensbescherming (AVG) gesproken. Van der Laan: "Voor het registreren van domeinnamen en IP-adressen, wordt de database Whois – uitgesproken als 'hoe is' – gebruikt. Hierin zijn gegevens verwerkt, zoals de naam en contactgegevens van de eigenaar, de provider en gegevens van servers. ICANN heeft verplicht gesteld dat deze database voor iedereen toegankelijk is. Met de komst van de AVG is dit nu in strijd met de Europese wetgeving. ICANN is neutraal en kan hiervoor geen nieuw beleid maken. De oplossing moet uit de multistakeholdercommunity komen. En dat is een echte uitdaging, want op dit moment zijn er voor- en tegenstanders. Zo zijn er discussies over hoe we ervoor kunnen zorgen dat bepaalde groepen, zoals politie en andere specifieke diensten, wel toegang houden tot de database."

Soevereiniteit
In het digitale domein en zeker op het internet speelt soevereiniteit al langer een grote rol van betekenis. Landen als China en Iran gebruiken hun eigen soevereiniteit door het afschermen van een 'nationaal' deel van het internet. "Helaas kan ICANN hier weinig aan doen, we hebben alleen een technisch mandaat om te zorgen dat het internet werkt en gaan dus niet over de content", vervolgt Van der Laan. "Net als dat internet goede mensen met elkaar verbindt, verbindt het ook slechte mensen met elkaar. Regeringen en politieke leiders beschikken niet altijd over technische skills om problemen als terrorisme of mensensmokkel goed op te lossen en nemen dan grovere maatregelen. De censuur in China is daar een voorbeeld van." Het Internet Governance Forum (IGF) is volgens Van der Laan het wereldwijde platform waar deze discussies wel gevoerd moeten worden. Zelf is Van der Laan ambassadeur van het NL IGF. "Ze vergaderen een keer per jaar en tussentijds heb je de lokale fora per regio. In Europa is dat de EuroDIG. Ik vind het jammer dat er vooralsnog weinig oplossingen uit zijn voortgekomen. De EuroDIG komt volgend jaar in juni naar Nederland. Dit is een mooie kans voor ons als land om het goede voorbeeld te geven en te laten zien hoe het kan. Wij zijn een rechtsstaat, we begrijpen wat democratie is, lopen voor op mensenrechten en worden mondiaal ook zo gezien. Wij moeten kunnen laten zien hoe de nieuwe digitale economie en technologische wereld eruit komt te zien en hoe we daar met elkaar de vruchten van kunnen plukken!"

"Nederland moet tijdens de EuroDIG laten zien hoe het kan"
"EuroDIG is a chance for the Netherlands to share our experience with effective multi-stakeholderism"

Japanese. Theoretically, this might cause a message sent from Tokyo to end up in Beijing unintentionally. We need to make policy and agree processes to avoid this – and we manage to do this! Technicians, mostly volunteers, who are the real experts, have the final say. They know how to achieve this in the most secure manner possible. Once we have arrived at a consensus on how to use certain characters, it becomes a new global policy. This is how Iraq was recently able to launch .iraq in Arabic, for example.'

GDPR
Just like the internet, the multi-stakeholders operate on a global scale. 'That is why all meetings involve attendees from across the globe', Van der Laan continues. 'Ideally, we want to prevent any disruption to existing connections and keep the technical layer in working order, without countries such as China erecting firewalls or other obstacles. That is why we meet in all regions in turn.' At the last meeting, the main topic of discussion was the General Data Protection Regulation (GDPR). Van der Laan: 'Domain names and IP addresses are registered on the basis of the Whois database. This contains data such as the name and contact details of the site owner, the provider and server data. ICANN has made it mandatory for countries to ensure that this database is publicly accessible. However, the GDPR has made this illegal under EU law. As a neutral party, ICANN is unable to solve this through a new policy; the solution must come from the multi-stakeholder community. This represents a real challenge, as there are both proponents and opponents of open access at the moment. Some of the discussions focus on how we can ensure access to the database for certain groups, such as the law enforcement and providers of certain other services.'

Sovereignty
Sovereignty has been an issue of major significance within the digital domain for some time now, particularly with regard to the internet. Countries such as China and Iran use their sovereignty to screen certain sections of the 'national' part of the internet. 'There is nothing that ICANN can do about this. We only have a technical mandate to ensure that the internet works and have no say as regards content', Van der Laan explains. 'The internet makes no distinction between connecting well-intentioned people and those with malicious intent, just like telephone lines. Governments and political leaders do not always possess the technical skills to tackle problems such as terrorism or human trafficking, so they fall back on cruder measures. Chinese censorship is an example.' According to Van der Laan, the right global platform for having these discussions is the Internet Governance Forum (IGF). However, Van der Laan finds the concrete results from IGF disappointing. She is an ambassador for the Dutch IGF herself. 'IGFs are convened once a year, with regional fora convened in the interim. The forum for Europe is EuroDIG. Next June, EuroDIG will be convened in the Netherlands. This is a great chance for our country to step up and share our experience with effective multi-stakeholderism. We are a democracy under the rule of law and are globally recognised as a defender of human rights. We must be able to demonstrate what the new digital economy and world of technology will look like and how we can reap its benefits together!'

In de Haven van Rotterdam is cybersecurity een relatief nieuw begrip. Zeker in vergelijking met de bankensector, die het onderwerp al jaren hoog op de agenda heeft staan. Banken testen elkaar zelfs. René de Vries, (Rijks)havenmeester Rotterdam, zorgt 24 uur per dag voor orde en veiligheid in de haven van Rotterdam, ook als het gaat om cybersecurity.

For the Port of Rotterdam, cybersecurity is a relatively new concept – particularly compared to the banking sector, which has been dealing with this topic extensively for years. Nowadays, banks even test each other. René de Vries, the Port of Rotterdam's harbour master, is responsible for maintaining order in the Port of Rotterdam and keeping it secure 24 hours a day – also when it comes to cybersecurity.

René de Vries
Cyber Resilience Officer
Harbour of Rotterdam

CYBERSECURITY IN THE PORT OF ROTTERDAM

"HET HEEFT TIJD NODIG OM TOT EEN VOLWASSEN, ONTWIKKELD EN BREED GEDRAGEN SYSTEEM TE KOMEN"

'BUILDING A MATURE, FULLY DEVELOPED AND BROADLY SUPPORTED SYSTEM TAKES TIME'

De Vries vergelijkt cybersecurity in zijn haven nu graag met de ontwikkeling die de International Ship & Port Security ofwel ISPS heeft doorgemaakt. "De International Maritime Organisation, ofwel IMO, heeft naar aanleiding van de aanslagen van 9/11 een ISPS-code opgesteld. Deze VN-regelgeving zorgt ervoor dat de (toegangs)beveiliging van terminals en schepen goed is geregeld en beschermd tegen terroristische dreigingen. In Rotterdam gaat dat om 190 terminals met naar schatting zo'n 5.000 tot 6.000 medewerkers. Waar we met Port Security in 2004 stonden, staan we nu met cybersecurity, of beter gezegd cyberresilience", vertelt De Vries. Volgens hem is het onmogelijk om 100% van cyberincidenten te voorkomen. "Zeker omdat zeven op de tien cyberincidenten een menselijke trigger hebben. Daarom willen we juist de nadruk leggen op de weerbaarheid van bedrijven. Dat bedrijven weten wat ze moeten doen als systemen zijn geraakt of informatie niet meer betrouwbaar is. Dat ze weten wie ze moeten bellen en welk crisisplan er in werking treedt. Beperk de schade en zorg dat je zo snel mogelijk terug naar de dagelijkse operatie kan", vervolgt De Vries.

Bewustwording

Wat De Vries van Port Security heeft geleerd, is dat het tijd nodig heeft om tot een volwassen, ontwikkeld en breed gedragen systeem te komen. De Vries: "Wij hebben daar inmiddels de eerste stappen voor gezet. We zijn begonnen met een verkenning in 2013 en een bewustwordingscampagne voor onze klanten van FERM in 2016. FERM is een publiek-private samenwerking waar ik het ambassadeurschap vervul als Port Cyber Resilience Officer. Vanuit FERM willen we zoveel mogelijk concrete tips, trucs, formats en nieuws aan onze klanten leveren." De Vries beseft dat niet elk bedrijf de mogelijkheid heeft een Information Security Officer aan te nemen, een consultant in te huren of bedrijven weten gewoonweg niet welke stappen te nemen. Zo ook binnen de haven van Rotterdam. "Ook die bedrijven maken onderdeel uit van een keten die digitaal is verbonden. Een keten die zo sterk is als de zwakste schakel", legt De Vries uit.

notPetya

Cybersecurity blijft volgens De Vries een onderwerp waar bedrijven terughoudend in zijn om echt in te investeren. Dit gebeurt vaak pas

"Beperk de schade en zorg dat je zo snel mogelijk terug naar de dagelijkse operatie kan."
"The objective is to limit the damage and return to normal as soon as possible"

De Vries likes to compare cybersecurity in 'his' port with developments in International Ship & Port Security (ISPS) legislation. 'Following 9/11, the International Maritime Organisation [IMO] elaborated an ISPS code. This UN guideline provides a regulatory framework regarding security and access protection for both terminals and vessels to protect them against terrorist attacks. Here in Rotterdam, we have 190 terminals employing between 5,000 and 6,000 staff. Just as we developed Port Security in 2004, we are now developing cybersecurity, or rather cyber resilience', De Vries says. He maintains that it is impossible to avoid 100% of all cybercrime incidents. 'Especially because seven out of ten cybercrime incidents are a result of human error. This is why we want to stress the resilience aspect for businesses. Resilient businesses know what to do if their systems are impacted or information is no longer reliable. They know who to call and which crisis plan to fall back on. The objective is to limit the damage and return to normal as soon as possible', De Vries continues.

Raising awareness

The Port Security project taught De Vries that building a mature, fully developed and broadly supported system takes time. De Vries: 'We have now taken the first steps. A preliminary investigation carried out in 2013 was followed up with an awareness campaign for our FERM customers in 2016. FERM is a public-private partnership that I promote in my capacity as Port Cyber Resilience Officer. It functions as a platform to deliver as many specific tips, tricks, formats and news items to our customers as possible.' De Vries is well aware that not all businesses have the resources to employ an Information Security Officer, hire a consultant or develop the know-how to understand which steps to take. The Port of Rotterdam is no different. 'All these businesses are links in a digital chain. This chain is only as strong as its weakest link', De Vries explains.

notPetya

According to De Vries, cybersecurity remains an area that many businesses are reluctant to really invest in. Many only do so after a serious incident. 'Businesses underestimate the risks and believe they will not be affected, or they overestimate their own capabilities because they think they possess the right know-how or have taken the right measures. Alternatively, they may be at the mercy of international head offices and have little say themselves', De Vries explains. 'Businesses may be impacted even if they are not the primary target of an attack. We saw this during the notPetya ransomware attack in July last year, which affected businesses worldwide. One of the victims in our port was APM Terminals, a subsidiary of Maersk. The lesson we learnt is that cybercrime incidents can have repercussions in the real physical world. We also had to correct some reports in the media, because it wasn't the Port of Rotterdam or the entire Maasvlakte that had been hacked, but a single company with two terminals. Both

als het een keer goed mis is gegaan. “Bedrijven onderschatten het risico en denken dat dit hen niet overkomt of overschatten zichzelf, omdat ze van mening zijn de juiste kennis in huis te hebben of de juiste maatregelen treffen. Het kan ook zijn dat ze afhankelijk zijn van internationale hoofdkantoren en daarmee zelf weinig invloed hebben”, vertelt De Vries. ”Bedrijven kunnen ook slachtoffer worden als ze niet zelf gericht worden aangevallen. Dat zagen we bij de notPetya ransomware in juni vorig jaar waarbij bedrijven wereldwijd zijn geraakt. Onder andere APM Terminals, dochteronderneming van Maersk hier in onze haven werd toen getroffen. Wat we hiervan hebben geleerd is dat een cyberincident dus echt fysieke gevolgen kan hebben. We hebben toen ook het beeld in de media moeten rechtzetten, omdat niet de Haven of de Maasvlakte was gehackt, maar één bedrijf met twee terminals. Na ruim een week waren beide terminals weer operationeel. Wij hebben in de eerste dagen gericht informatie en handelingsperspectief kunnen sturen naar bedrijven in de haven, onder andere door de goede samenwerking met het Nationaal Cyber Security Centrum.”

Haven Cybermeldpunt

NotPetya heeft er mede toe geleid dat de vrijblijvendheid wat betreft cybersecurity in de haven Rotterdam in de komende jaren zal afnemen doordat er meer juridisch wordt vastgelegd. De Vries: “Zo heeft Burgemeester Aboutaleb in juni van dit jaar het Haven Cybermeldpunt geopend. Dit meldpunt staat open voor alle bedrijven en gebruikers in de haven, maar kent een verplicht karakter voor de 190 terminals. Uiteraard willen we niet elke phising mail gemeld krijgen, maar wel de IT-verstoring die impact heeft op de digitale veiligheid van de haven. Zo brengen we cyberveiligheid en fysieke veiligheid dichter bij elkaar!”

terminals were fully operational again after little more than a week. During the first few days of the aftermath, we were able to supply businesses in the harbour with targeted information and action plans, thanks in part to the excellent cooperation of the National Cyber Security Centre.’

Port Cyber Hotline

Partly as a result of the notPetya affair, cybersecurity at the Port of Rotterdam will assume a more formal character over the next few years, thanks to the introduction of new legislation. De Vries: ‘To this end, Mayor Aboutaleb launched the Port Cyber Hotline last year. This hotline can be used by all of the port’s businesses and users, but reporting cybercrime incidents is mandatory for the 190 terminals. Obviously, they do not need to report every single phishing email, but we should be notified of any IT disruptions with an impact on the port’s digital security. That way, we can bring cybersecurity more into line with physical security!’

PROTECT YOUR MOST VALUABLE DIGITAL ASSETS WITH THE CYBERSECURITY HEALTH CHECK

Cybersecurity op de agenda brengen van organisaties, blijft hoognodig. De Cyber Security Raad (CSR) heeft de accountantsorganisaties Deloitte, EY, KPMG en PwC (hierna BIG 4), benaderd met vraag of zij een Cybersecurity Health Check wilden ontwikkelen voor middelgrote ondernemingen om richting te geven aan hun cybersecuritybeleid. Veel organisaties vinden het lastig om grip op de zaak te krijgen.

Getting cybersecurity onto an organisations agenda remains a matter of critical importance. The Cyber Security Council (CSR) approached the accountancy firms Deloitte, EY, KPMG and PwC (hereinafter: BIG 4) to ask whether they would like to develop a Cybersecurity Health Check for medium sized businesses to help them steer their cybersecurity policy. Many organisations find getting a grip on the issue tricky.

Organisaties zijn op allerlei manieren digitaal met elkaar verbonden. Dat biedt veel kansen. Zeker in Nederland: één van de meest ICT intensieve economieën ter wereld, met een digitale productie van bijna 23 procent van het bruto binnenlands product.

Tegelijkertijd brengt deze digitale verbondenheid risico s met zich mee. Als een organisatie, publiek of privaat, groot of klein, haar digitale zaakjes niet op orde heeft, schaadt dat niet

Organisations are digitally interconnected in all kinds of ways, which presents manifold opportunities. Particularly in the Netherlands one of the most ICT intensive economies in the world, with a digital production level of nearly 23% of gross domestic product.

Yet this digital interconnectedness also entails risks. If an organisation (public or private, large or small) does not have its digital affairs in order, then this will undermine trust not only in itself but in the Netherlands and the Dutch business community as a whole. Hence cooperation and sharing knowledge and experiences are essential to safeguard sound, secure data traffic. The recently developed Cybersecurity Health Check is an example of this. In close cooperation with the CSR, the accountancy and consultancy offices of the BIG 4 combined their cybersecurity knowledge and experience in the Cybersecurity Health Check.

alleen het vertrouwen in haarzelf maar ook in de BV Nederland. Samenwerken en kennis en ervaringen uitwisselen is dan ook essentieel om veilig en integer dataverkeer te waarborgen. De recent ontwikkelde Cybersecurity Health Check is hier een voorbeeld van. In nauwe samenwerking met de CSR hebben de accountants en advieskantoren van de BIG 4 hun kennis en ervaring over cybersecurity gebundeld in de Cybersecurity Health Check.

Concrete handvatten
Het doel van de health check is om cyberkennis en ervaringen met een breder publiek te delen. De checklist biedt concrete handvatten aan organisaties om inzicht te krijgen in hun staat van cyberbeveiliging. En dat is essentieel. In de huidige digitale wereld is het immers niet de vraag of een organisatie te maken krijgt met een cyberincident, maar wanneer. Actie ondernemen om de kans op een incident te verkleinen, is daarom niet voldoende. Maatregelen om de aanval snel te detecteren en hier vlot op te reageren, zijn even belangrijk. Dit helpt namelijk om de impact van de aanval zo klein mogelijk te houden. Accountants kunnen een belangrijke bijdrage leveren aan de bewustwording in de organisatie ten aanzien van digitale risico s. Voor hen biedt de health check handvatten om het gesprek over cybersecurity aan te gaan.

Vijf domeinen
De Cybersecurity Health Check bestaat uit vijf domeinen:

- Identificatie: Het vaststellen van de digitale kroonjuwelen, de belangrijkste risico s als hierop een cybersecurityaanval plaatsvindt en wie de verantwoordelijkheid draagt voor cybersecurity.
- Bescherming: Het in kaart brengen van de maatregelen, niet alleen technisch maar ook omtrent bewustwording, die zijn getroffen om de digitale kroonjuwelen te beschermen.
- Detectie: Het detecteren van dreigingen, identificeren van incidenten en uitvoeren van beveiligingstesten.
- Reactie: Het paraat hebben van een communicatie en crisisplan en deze regelmatig testen met behulp van een gesimuleerd cyberincident.
- Herstel: Het inrichten van back up voorzieningen en een herstelplan om zo snel mogelijk weer up en running te zijn.

Digitale voorsprong
Wij roepen alle organisaties op om aan de hand van deze checklist kritisch te kijken welke elementen zij wel en niet in huis hebben, met deze resultaten aan de slag te gaan en dit ook te bespreken met hun accountant en adviseur. Ook is het omgekeerde van belang: accountants die op basis van het document het gesprek aangaan met ondernemingen. De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) heeft medewerking toegezegd door de Cybersecurity Health Check onder haar vlag te publiceren en te verspreiden onder hun leden. Ook de SRA en vijf middelgrote accountantskantoren werken graag mee aan dit initiatief. De Cybersecurity Health Check is te vinden op de site van het Digital Trust Center (DTC).
Dit is geen eenmalige exercitie. De Cybersecurity Health Check is niet enkel bedoeld om achterstallig onderhoud aan te pakken. Juist als organisaties regelmatig de check uitvoeren, kan hun beveiliging continu op hoog niveau blijven. Dat is noodzakelijk om zowel organisaties zelf als de BV Nederland een digitale voorsprong te geven.

Concrete guidelines
The aim of the health check is to share cybersecurity knowledge and experience with a wider audience. The checklist offers concrete guidelines to organisations, providing them with insight into the state of their cybersecurity. And that is essential, as in today s digital world the question is not whether an organisation will fall victim to a cyber incident but when. Hence taking action to reduce the probability of an incident will not suffice. Measures to ensure swift detection of and a rapid response to the attack are just as important. After all, these will help minimise the attack s impact. Accountants can go a long way towards raising awareness of digital risks within the organisation. For them, the health check provides guidelines for dialogue on cybersecurity.

Five spheres
The Cybersecurity Health Check comprises five spheres:

- Identification: Ascertaining the most valuable digital assets, the most significant risks if a cybersecurity attack is mounted on these, and who bears responsibility for cybersecurity.
- Protection: Charting the measures taken (not only in technical terms but also with regard to raising awareness) to protect the most valuable digital assets.
- Detection: Detecting threats, identifying incidents and performing security testing.
- Response: Having a communication and crisis plan in place and regularly testing it by means of cyber incident drills.
- Recovery: Setting up backup facilities and drawing up a recovery plan to be up and running again within the shortest possible time frame.

Digital edge
We call upon all organisations to cast a critical eye over the elements they do or do not have in house using this checklist, and to set to work on the results and discuss them with their accountant and advisor. This is also important from the opposite perspective, that of accountants engaging in dialogue with organisations. The Royal Netherlands Institute of Chartered Accountants (NBA) has extended its cooperation by publishing the health check and disseminating it among its members. The SRA and five medium sized accountancy firms are happy to collaborate on this initiative. The Cybersecurity Health Check is featured on the site of the Digital Trust Center (DTC).
This is not a one off exercise. The health check is not simply intended to address overdue maintenance. Regularly performing the check will enable organisations to keep their security up to scratch at all times. This is necessary to give both organisations themselves and the Netherlands as a whole a digital edge.

In Nederland hebben accountants een belangrijke signalerende en waarschuwende rol in de samenleving. Marco van der Vegte, bestuursvoorzitter van de Nederlandse Beroepsorganisatie van Accountants (NBA), vindt dat van hen verwacht mag worden dat zij alert zijn op bedreigingen voor de economie. “Ik vind eerlijk gezegd dat we nog scherper moeten worden op onze rol rondom cybersecurity. Dit onderwerp hebben we daarom prominent in onze eigen sectorbrede Vernieuwingsagenda gezet”, vertelt Van der Vegte.

In the Netherlands, accountants play a vital role in society with regard to identifying and reporting risks. Marco van der Vegte, President of the Board for the Institute of Chartered Accountants (NBA), feels they can rightfully be expected to keep an eye out for threats to the economy. ‘To be honest, I feel we should be more vigilant in our role with regard to cybersecurity. That’s why we’ve ensured this topic figures prominently in our own sector-wide Innovation Agenda’, Van der Vegte explains.

Marco van der Vegte
President of the Board for the Institute of Chartered Accountants

‘ACCOUNTANTS PLAY A VITAL ROLE IN MAINTAINING A HEALTHY, ROBUST ECONOMY’

Accountants zijn in de visie van Van der Vegte de hoeders van een gezonde en sterke economie. “We zitten immers overal aan tafel in de BV Nederland. Niet alleen vanuit de controlepraktijk bij grote organisaties met een openbaar belang, maar ook in het mkb, binnen de overheid en als accountants in business in leidinggevende functies bij uiteenlopende organisaties. Alle accountants hebben een belangrijke rol in het vergroten van het bewustzijn van cybercrime-gerelateerde bedrijfsrisico’s.” Dat meer scherpte nodig is, blijkt volgens Van der Vegte wel uit het voorbeeld van de laatste jaarlijkse Accountantsdag. “We hebben toen live een accountantskantoor laten hacken. Veel accountants in de zaal waren verbaasd dat het zo gemakkelijk ging.”

Publieke management letter
Van der Vegte vindt het belangrijk om te blijven communiceren over de gevolgen van een cyberaanval. Ook het besef dat het iedereen kan overkomen moet volgens hem breder worden. “Voor elke online organisatie geldt niet zozeer de vraag of men wordt gehackt, maar wanneer en hoe vaak. En hoe snel

To his mind, accountants play a vital role in maintaining a healthy, robust economy. ‘After all, we’ve got a hand in practically every business operating in the Netherlands. Not just with regard to auditing services for large organisations with a public interest, but also in SMEs, in government and as accountants in business in leadership positions at a wide range of organisations. All accountants have an important part to play in increasing awareness of cybercrime-related corporate risks.’ According to Van der Vegte, an example from the most recent annual Accountants Day makes it clear that greater vigilance is in order. ‘On that day, we arranged for a live hack of an accountancy firm. Many of the accountants in attendance were surprised by how easily it succeeded.’

Public management letter
Van der Vegte feels it is important to maintain open communication regarding the consequences of a cyber attack. He thinks the realisation that it can happen to anyone deserves wider attention as well. ‘For any online organisation, the question is not so much if you will be hacked, but when and how often. And how quickly you will be able to respond. Organisations must have hard and soft measures in place to make all employees aware of potential cyber attacks and to instruct them on what to do in the event of such an attack.’
The accountant is the logical choice to act as trusted advisor to the Board in this area. Every organisation should be aware that cybercrime poses one of the more severe risks that a company can face. A risk of the same magnitude as fire or fraud. Van der Vegte: ‘Accountants have a responsibility to point this out to executives, repeatedly if necessary. Whether at their request or not. In 2016, the NBA published a public management letter in which the most important factors were set out. Therefore the Cyber Security Council (CSR) approached the accountancy firms Deloitte, EY, KPMG and PwC, also know as the BIG 4, to develop a Cybersecurity Health Check. The NBA will publish the health check and disseminate it

“Alle accountants hebben een belangrijke rol in het vergroten van het bewustzijn van cybercrime-gerelateerde bedrijfsrisico’s”

“All accountants have an important part to play in increasing awareness of cybercrime-related corporate risks”

daarop gereageerd kan worden. Er zijn harde en zachte maatregelen nodig in een organisatie om elke werknemer attent te maken op mogelijke cyberaanvallen en te instrueren wat ze moeten doen als het toch gebeurt.”
De accountant is de logische ‘trusted advisor’ van het bestuur op dit onderwerp. Elke organisatie moet zich realiseren dat cybercrime een van de grotere risico’s is die de organisatie kunnen bedreigen. Net als fraude of brand. Van der Vegte: “Accountants hebben een rol om bestuurders bij de les te houden in dit opzicht. Gevraagd en ongevraagd. Daartoe hebben de vier grootste accountantsorganisaties Deloitte, EY, KPMG en PwC op verzoek van de Cyber Security Raad de Cybersecurity Health Check opgesteld. De NBA zal dit instrument onder haar vlag publiceren.”

Kamervragen

Onlangs zijn er kamervragen gesteld over de aandacht in accountantsverklaringen voor cyberbeveiliging en IT. Die aandacht zou te gering zijn. Volgens Van der Vegte is de accountant wettelijk verplicht een oordeel te vellen over de betrouwbaarheid en de continuïteit van de ICT-systemen in een organisatie. “De conclusies zijn voor het maatschappelijk verkeer niet zichtbaar, omdat deze worden opgenomen in een management letter”, vertelt Van der Vegte. “Of er veel of weinig aandacht wordt gegeven aan cyberbeveiliging en IT kan dus niet ontleend worden aan de controleverklaring van een organisatie. Niettemin is het zeker goed om te onderzoeken of meer expliciete aandacht voor dit onderwerp in de accountantsverklaring zinvol is. Die handschoen pak ik graag samen op met de betrokken ministeries, maar ook met NOREA, de beroepsorganisatie van IT-auditors.”

Kroonjuwelen

Het streven naar steeds betere IT-audits juicht Van der Vegte van harte toe. “Alles beveiligen is echter onmogelijk. De focus dient op de kroonjuwelen gericht te worden. Dat zijn de meest kritische data en processen. Daarbij is de mens vaak de zwakste schakel en cultuur en gedrag verdienen daarom aandacht. Ook in de keten kunnen zwakke schakels zitten: leveranciers die zich niet aan bepaalde basisnormen houden, kunnen een bedreiging voor de organisatie vormen”, aldus Van der Vegte.

among our members. Also the SRA and five medium-sized accountancy firms are happy to collaborate on this initiative.’

Parliamentary questions

Recently, questions were asked in Parliament about the attention paid to cybersecurity measures and IT in accountant’s statements. That attention was alleged to be insufficient. Van der Vegte explains that an accountant is legally obligated to issue a judgement regarding the reliability and continuity of the ICT systems in an organisation. ‘Rather than being revealed to society at large, these conclusions are included in a management letter instead’, says Van der Vegte. ‘In other words, there’s no way to tell from an organisation’s audit report whether they are devoting a great deal or very little attention to cybersecurity. Nonetheless, it’s definitely a good idea to explore whether it would be useful to pay more explicit attention to the topic in the accountant’s statement. I’m happy to take up this issue together with the relevant ministries, as well as with NOREA, the professional association for IT auditors.’

Crown jewels

Van der Vegte is wholeheartedly pleased with efforts to make IT audits ever-more effective. ‘It’s impossible to secure everything, however. The focus should be squarely on the “crown jewels”, that is the most critical data and processes of an organisation. People themselves are often the weakest link as far as that goes, which is why organisational culture and behaviour deserve attention as well. The chain can contain weak links, too – suppliers who fail to comply with certain basic standards can pose a threat to the organisation’, says Van der Vegte.

‘THINK THE IMPOSSIBLE’

“Singularity is het moment dat machines slimmer worden dan mensen”

“The singularity is the moment when machines become smarter than humans.”

Nadat ik in San Francisco geland ben passeer ik security en douane. Ik stap in een Uber die mij naar Cupertino brengt. In het hotel heb ik mijn eerste kennismaking met nieuwe technologie. Mocht ik mijn tandenborstel vergeten zijn of een flesje water nodig hebben, dan komt een robot die brengen. De receptie is echter nog gewoon bemenst. De daaropvolgende week zal ik horen dat alles gaat veranderen. Hier in Silicon Valley mag ik een week het *executive program* van de Singularity University volgen. Niet mijn eerste kennismaking; ik heb in Nederland enkele jaren geleden al eens een symposium hierover bijgewoond. *Singularity* is, eenvoudig gezegd, het moment dat machines slimmer worden dan mensen. De vraag is of je na een week ondergedompeld te zijn in verhalen over wat er technologisch allemaal mogelijk is, je ook een *believer* wordt van dit gedachtegoed. Het gaat overigens niet alleen over kunstmatige intelligentie of quantum computing, uitdagingen waarover ik in het NRC in februari 2017 al eens iets heb gezegd, maar over technologische ontwikkelingen in het algemeen. Kern van het verhaal is dat we als samenleving voor grote uitdagingen staan als het gaat om bijvoorbeeld energie, milieu, voedsel, water en gezondheid. Daarvoor moeten we creatieve oplossingen zoeken en technologie gaat ons daarbij helpen, zeker gezien de huidige of toekomstige exponentiele ontwikkelingen. Ben ik een *believer*? Ja, ik geloof dat technologie zich verder zal ontwikkelen en dat we nog niet weten wat er over tien jaar mogelijk is. Maar ik besef ook terdege dat dit de afgelopen decennia niet anders is geweest. De maatschappij is mee veranderd, vaak zonder dat we ons dat realiseren. Velen denken dat de wet van Moore zijn langste tijd heeft gehad, maar ik denk dat die voorlopig niet afzwakt. Rekenkracht zal exponentieel blijven toenemen met alle ontwikkelingen die daar aan vast zitten. Die notie vraagt dat we daar nu al rekening mee houden, ook in cybersecurity. Huidige security oplossingen zullen in de toekomst onvoldoende blijken te zijn. Als we ons dat realiseren moeten we nu al in ontwerpen rekening houden dat het aanpasbaar en schaalbaar is. Zeker gezien een toekomst met *the internet of everything*. Het is een *global* uitdaging, die meer vraagt dan een local oplossing. Dat vraagt om een creatieve aanpak, of, zoals tijdens het programma werd onderwezen, *think the impossible* , zowel vanuit dreigingen als vanuit kansen.

Hans Folmer, Brigade generaal, voormalig commandant Defensie Cyber Commando (DCC)

Folmer ontving voor zijn werk uit handen van minister Ank Bijleveld Schouten het Ereteken voor Verdienste in Zilver.

As soon as I landed in San Francisco, I went through customs and security, then took an Uber to Cupertino. I had my first encounter with cutting edge technology in the hotel. If I had forgotten my toothbrush or wanted a bottle of water, a robot would bring me one. While the reception desk was still staffed by humans, I found out over the following week that everything was about to change. I was here in Silicon Valley to attend Singularity University s week long executive programme. It was not my first experience of the singularity, as I had attended a symposium on the subject in the Netherlands several years ago. Simply put, the singularity is the moment when machines become smarter than humans. The question is whether you could start to believe this idea after a week immersed in stories about all the things that are possible with technology. Incidentally, the singularity is not only about artificial intelligence or quantum computing, which challenges I already discussed in Dutch Daily NRC back in February 2017 it is about technological developments in general. The crux of the matter is that we as a society are facing major challenges in areas such as energy, the environment, food, water and health. We need to find creative solutions and technology can help with that process, particularly in the light of current and future exponential developments. Am I a believer? Yes, I believe that technology will continue to develop and that we have no idea what will be possible ten years from now. However, I am also fully aware that this fact has already been true for several decades. Society has changed as well, often without us realising it. Whereas many people think that Moore s Law has had its day, I believe that it will still apply for the time being. Processing power will continue to increase exponentially, with all the developments that will undoubtedly be associated with it. We are forced to take this fact into account, including in cybersecurity matters. In future, our current security solutions will prove insufficient. Once we realise this, we need to start thinking about designing systems that are adjustable and scalable; particularly in light of a future that includes the Internet of Everything. This global challenge requires more than just a local solution. It requires a creative approach or, as they taught us in the programme, it requires us to think the impossible with regard to both threats and opportunities.

Hans Folmer
Brigadier
Former Commander of Defence Cyber Command (DCC)

In recognition of his work, Folmer was awarded the Silver Decoration of Merit by Minister Ank Bijleveld Schouten.

RUBEN WENSELAAR

Nieuw lid van de Cyber Security Raad

New member of the Cyber Security Council (CSR)

“Voor de zorgsector zijn digitale toepassingen essentieel”

'Digital applications are essential for the healthcare sector.”

Ruben Wenselaar is voorzitter van de Raad van Bestuur van zorgverzekeraar Menzis en bestuurslid van Zorgverzekeraars Nederland. In 2017 is hij toegetreden als lid van de CSR.
Na zijn studie bedrijfseconomie werkte Ruben Wenselaar bij uiteenlopende organisaties in management- en directiefuncties op het vlak van financiën, ICT en Human Resource Management. In 2002 werd Ruben directievoorzitter van Amicon zorgverzekeraar. In 2004 trad hij toe tot de Raad van Bestuur van Menzis, dat ontstond na de fusie van Amicon met Geové.

Ruben Wenselaar is the CEO of the Board of Directors of Menzis, a health insurer, and member of the Board of the Association of Dutch Health Insurers. He was appointed to the CSR in 2017. After completing a degree in Business Management, Ruben Wenselaar held management and executive positions in various organisations within the fields of finance, IT and human resource management. Ruben was appointed Chair of the Board of the health insurer Amicon in 2002. In 2004, he joined the Board of Directors of Menzis, which was formed from the merger of Amicon and Geové.

Wat is voor u het belang van de CSR?
Ik zie dat cybersecurity economisch en maatschappelijk zeer relevant is, maar dat het nog in de kinderschoenen staat. Ik vind het een uitdaging om cybersecurity naar een hoger niveau te tillen, met als doel om voordelen van de digitale wereld in brede zin in Nederland te kunnen benutten. Vanuit mijn rol als raadslid van de CSR kan ik daar aan bijdragen.

Waarom is cyber een belangrijk thema voor de zorgsector?
Voor de zorgsector zijn digitale toepassingen essentieel om de zorg voor alle Nederlanders in de toekomst toegankelijk te houden. De druk op de arbeidsmarkt vereist zeker in deze sector vernieuwende oplossingen. Om die toekomst te verwezenlijken is cybersecurity instrumenteel.

Why do you think that the CSR is important?
Although I can see the critical relevance of cybersecurity at an economic and social level, it is still in its infancy. I think that we are facing a large challenge in trying to lift cybersecurity to a higher level, with the aim of enabling the Netherlands to harness the benefits of the digital world in a broad sense. In my role as a member of the CSR, I can make an important contribution to this issue.

Why is cyber an important theme for the healthcare sector?
Digital applications are essential for the healthcare sector to ensure that healthcare remains accessible for all Dutch people in future. Pressure on the labour market is driving the need for innovative solutions in this sector. Cyber security will be instrumental in achieving that future.

ICT is niet meer weg te denken in de zorg. Patiëntgegevens worden digitaal opgeslagen en gedeeld, medische apparatuur wordt digitaal aangestuurd en het aantal e-healthtoepassingen groeit snel. Het risico op kwetsbaarheden in ICT-systemen groeit daarmee ook, net als dreigingen van buitenaf: phishing, ransomware, hacking etc. Digitale toepassingen gaan de gezondheidszorg fundamenteel veranderen.

ICT in healthcare is here to stay. Patient data are stored and shared digitally, medical equipment is digitally controlled and the number of e-health applications is growing rapidly. As a result, the risk of vulnerabilities in IT systems is also growing, along with external threats: phishing, ransomware, hacking, and so on. Digital applications will change healthcare fundamental.

Ruben Wenselaar
CEO of Menzis and member of the Cyber Security Council

INNOVATIE EN DIGITALISERING ZIJN NOODZAKELIJK VOOR DE TOEKOMST VAN DE ZORGSECTOR

THE FUTURE OF THE HEALTHCARE SECTOR REQUIRES INNOVATION AND DIGITALISATION

CYBER CARE: THE HEALTH-CARE OF THE FUTURE

Veel van deze vernieuwingen zijn zeer gewenst, aldus Menzis-bestuurder en lid van de Cyber Security Raad (CSR) Ruben Wenselaar. “Denk aan ingrijpende innovaties zoals zorg op afstand”, vertelt Wenselaar. “Voor een consult met een medisch deskundige of zelfs het verzenden en bespreken van gezondheidsmetingen hoeft de patiënt niet langer uit huis.” Maar er zijn meer kansen volgens Wenselaar: “Steeds meer medisch apparatuur kan met elkaar ‘communiceren’ en met het Internet of Things kunnen we de zorg een stuk efficiënter maken. Dit heeft veel voordelen voor de patiënt, denk aan vaker hulp vanuit thuis, dus meer flexibiliteit en door efficiënte inzet en deling van wereldwijde kennis zelfs een hogere kans op genezing.”

Borgen privacy en opslag gegevens

Niet onbelangrijk vindt Wenselaar dat innovaties helpen de zorg betaalbaar te houden. Uiteraard

Many of these innovations are highly desirable, according to Ruben Wenselaar, CEO of Menzis and member of the Cyber Security Council (CSR). 'Consider radical innovations such as remote care,' says Wenselaar. 'Patients no longer have to leave the house in order to consult a medical expert or even send and discuss medical examination results.' Wenselaar sees even greater opportunities still: 'Medical devices can increasingly "communicate" with each other, while the Internet of Things will allow us to make healthcare substantially more efficient. This development has many benefits for patients, such as more frequent help at home, which results in greater flexibility. Through the efficient use and worldwide sharing of knowledge, they may even have a better chance of recovery.'

Safeguarding privacy and data storage

Wenselaar thinks it significant that innovations are helping healthcare to remain affordable. An initial investment is required, of course. 'However, we can also see risks, which are twofold. First, there is a need for safeguarding privacy. Medical data is increasingly "travelling" across the network. This situation requires careful authentication and secure transport of the data. Organisations must take care of these things. The second risk concerns data storage. It is a crucial question where the data are located, including in a physical sense, and how they are secured.'

Wenselaar gives an example of this kind of risk. 'Suppliers of physical

na een initiële investering. “Maar we zien ook risico’s. Die zijn tweeledig. Ten eerste het borgen van de privacy. Steeds meer medische gegevens ‘reizen’ over het netwerk. Dat vereist een zorgvuldige authenticatie en veilig transport van de data. Organisaties moeten hiervoor garant staan. Ten tweede, de opslag van de gegevens. Cruciaal is waar de gegevens staan, óók in fysieke zin, en hoe ze worden beveiligd.”

Wenselaar geeft een voorbeeld van zulke risico’s: “Leveranciers van fysieke medische apparatuur hebben veelal nog geen ervaring met de security daaromheen. Dat gat moet gedicht worden. Het is prachtig dat apparatuur aansluiting kan vinden op het netwerk, maar de veiligheid moet waterdicht zijn. Denk bijvoorbeeld aan apparatuur die op afstand kan ondersteunen bij chirurgie. Zo kan een gespecialiseerde neurochirurg vanuit Japan in de nabije toekomst een operatie uitvoeren in Nederland. Nu al kijken chirurgen op afstand mee. Het moet dan uiteraard onbestaanbaar zijn dat zulke instrumenten kunnen worden gehackt.”

Solide samenwerking

Nederland heeft de ambitie om internationaal bij de top te blijven horen op het vlak van digitalisering in de zorg. “We hebben een goede infrastructuur liggen en de nodige kennis in huis. Er bestaat een solide samenwerking tussen publiek, privaat en wetenschap. De CSR is daar een voorbeeld van. Het Zorg-Computer Emergency Respons Team ofwel Z-CERT, geeft dit in de zorgsector vorm. Bij een *security breach* kunnen zij, met hulp van andere CERTS, zo nodig wereldwijd, signaleren en problemen tackelen. Maar om op topniveau mee te blijven doen moet de overheid verder in beweging komen. Rondom cybersecurity geeft Nederland nog geen 6 miljoen euro uit aan cybersecurity-onderzoek, terwijl Duitsland € 50 miljoen uitgeeft. Onze buren hebben ook een kennisinstituut, wij niet. Dat leidt tot *braindrain*. We dreigen dus achter te gaan lopen.” Daarnaast vindt Wenselaar dat de Nederlandse zorgsector nog trager is dan andere branches in het vrijmaken van budgetten voor het implementeren en beheren van cybersecurity-maatregelen. “Daar moet veel meer aandacht voor zijn. Zorgorganisaties richten zich nog steeds te veel op de fysieke kant van patiëntveiligheid, de cyberkant wordt nog te vaak onderschat.”

“Met het Internet of Things kunnen we de zorg een stuk efficiënter maken”

“The Internet of Things will allow us to make healthcare substantially more efficient.”

medical equipment often have no experience in ensuring the security of that equipment. This gap must be addressed. While it is great that equipment can connect to the network, the security must be foolproof. Consider equipment that provides remote support during surgery, for example. In the near future, it could allow a specialist neurosurgeon from Japan to perform an operation in the Netherlands. Surgeons are already observing from a distance. Obviously, it must be impossible to hack such instruments.'

Solid collaboration

It is the ambition of the Netherlands to solidify its position as a global leader in the field of digitalisation in healthcare. 'We have good infrastructure in place and we have access to the necessary knowledge locally. In addition, we have a solid collaboration between the public and private sectors as well as academia. The CSR is a good example of this process. The Computer Emergency Response Team for Healthcare, or Z-CERT, gives shape to this collaboration in the healthcare sector. In case of a security breach, Z-CERT can report on and tackle problems with the help of other ‘CERTs’ and at a global level if necessary. However, if we are to retain our leading position, the government must do more to help. With regard to cyber-security, the Netherlands has set aside less than 6 million euro for cybersecurity research, while Germany is spending 50 million euro. Our neighbours also have a dedicated knowledge institute, which we lack. This situation has resulted in a brain drain, so there's a risk that we could fall behind.’

Wenselaar also thinks that the Dutch healthcare sector has been slower than other sectors to release budgets for implementing and managing cybersecurity measures: 'There needs to be a much greater focus in this area. Healthcare organisations still focus too much on the physical side of patient safety, while the digital side is too often underestimated.'

Over Z-CERT

Z-CERT is het expertisecentrum op het gebied van cybersecurity in de zorg. Z-CERT heeft specifieke kennis van hard- en software en medische technologie in de zorg en ondersteunt zorgverleners op het moment dat ze worden getroffen door een incident. Daarnaast biedt de stichting diensten om de weerbaarheid van de sector op het gebied van cybersecurity te vergroten.

De deelnemers aan Z-CERT vormen een netwerk om gezamenlijk uitdagingen als ransomware, phishing, datalekken of hacken aan te pakken. Het netwerk is snel groeiende en bestaat behalve de deelnemers uit brancheorganisaties, leveranciers, andere CERT’s, internationale contacten, (hackers)communities etc. Zo wordt informatie verzameld die nodig is om risico’s of dreigingen snel te signaleren en de deelnemers te adviseren hoe ze daarmee om kunnen gaan.

De stichting is opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU) en GGZ Nederland (GGZ). Samen met de branches werkt Z-CERT aan het Actieplan Informatiebeveiliging Patiëntgegevens.

Op dit moment zijn de diensten van Z-CERT beschikbaar voor ziekenhuizen (UMC, STZ, algemeen en categoraal) en GGZ-instellingen. Momenteel vinden de pilots plaats voor uitbreiding van de doelgroep naar langdurige zorg (Actiz) en gehandicaptenzorg (VGN), Zelfstandige klinieken(ZKN), Ambulancediensten (AZN) en medische laboratoria (SAN). Daarnaast wordt een sectoraal dreigingsbeeld voor de zorgsector opgesteld, die in oktober gepresenteerd zal worden. Op termijn wordt dit uitgebreid naar de hele zorgsector.

About Z-CERT

Z-CERT is the centre of expertise when it comes to cybersecurity in healthcare. Z-CERT possesses specific knowledge of hardware, software and medical technology within the healthcare industry and offers support to care providers in the event an incident has occurred. The foundation also provides services aimed at strengthening the sector's resilience as it relates to cybersecurity.

Together, Z-CERT participants form a network which enables members to tackle shared challenges such as ransomware, phishing, data breaches and hacking. The network is growing rapidly and includes not only participants from sectoral organisations but suppliers, other CERTs, international contacts and communities (including hackers), and so on. It is a means of gathering the information needed to quickly identify risks and/or threats and to advise participants on how best to respond to those risks.

The foundation began as an initiative of the Dutch Hospital Association (NVZ), the Netherlands Federation of University Medical Centres (NFU) and the Dutch Mental Healthcare Association (GGZ). Together with the sectors, Z-CERT is drafting an Action Plan on the Information Security of Patient Data.

Z-CERT's services are currently available to hospitals (UMC, STZ, general and specialised) and mental healthcare institutions. At the moment, pilots are underway in connection with expansion of the target group to include long-term care (Actiz), care and support for people with a handicap (VGN), independent clinics (ZKN), ambulance services (AZN) and medical laboratories (SAN). In addition, a sectoral threat assessment for the healthcare sector is being prepared and is scheduled for presentation in October. This will ultimately be expanded to include the entire healthcare sector.

‘SECURITY-BY-DESIGN’ DIENT TOEGEPAST TE WORDEN OP DE COMPLETE LEVENSCYCLUS

‘SECURITY-BY-DESIGN’ MUST BE APPLIED TO THE ENTIRE LIFE CYCLE

CYBERSECURITY STARTS WITH PRODUCT DESIGN

De strategische concurrentiepositie van bedrijven is, in toenemende mate, sterk afhankelijk van data, digitale innovatie, en consumentenvertrouwen. Cyberaanvallen, zoals de gijzelsoftware ‘WannaCry’ waarbij wereldwijd meer dan 230.000 computers in 150 landen besmet raakten, laten zien dat zelfs de grootste en meest geavanceerde organisaties kwetsbaar zijn voor verstoringen. Ook de National Health Service in het Verenigd Koninkrijk werd hierdoor getroffen. Als aanbieder van gezondheidstechnologie richt Philips zich op het verbeteren van de gezondheid van mensen en het bereiken van betere zorgresultaten. Aan het woord Hans de Jong, president Philips Nederland.

The strategic competitive position of companies depends to an increasingly significant degree on data, digital innovation and consumer confidence. Cyber attacks, such as the ransomware ‘WannaCry’ that has infected more than 230,000 computers in 150 countries, show that even the largest and most advanced organisations are vulnerable to disruptions. The National Health Service in the United Kingdom has also been affected by this ransomware. As a provider of health technology, Philips is focused on improving people’s health and achieving better healthcare outcomes. Hans de Jong, President of Philips the Netherlands, shares his thoughts.

Hans de Jong
President of Philips the Netherlands

"Digitalisering van de zorg is een integraal onderdeel van onze strategie"

“Digitalisation of healthcare is an integral part of our strategy.”

Philips maakt gebruik van geavanceerde technologieën en diepgaand inzicht in klinische toepassingen en de behoeften van consumenten om geïntegreerde oplossingen te ontwikkelen. Deze zogenaamde ‘connected healthcare’ is volgens De Jong essentieel in de transformatie van de gezondheidszorg om betere zorg tegen lagere kosten mogelijk te maken. “Nu al investeren wij 60% van het 1,7 miljard euro budget van Research & Development in software-ontwikkeling. Digitalisering van de zorg is een integraal onderdeel van onze strategie. Want onderling met elkaar verbonden, digitale apparaten zijn essentieel voor het verder verbeteren van de efficiëntie van onze dienstverlening waarbij de kwaliteit van de dienstverlening toeneemt terwijl de kosten afnemen.”

Digitaal ecosysteem

Dit digitale ecosysteem leidt echter ook tot een grotere digitale kwetsbaarheid. De Jong: “De persoonlijke gegevens van patiënten en de beschikbaarheid en betrouwbaarheid van digitale zorgsystemen vormen, in potentie, een belangrijk doelwit voor cybercriminelen. Binnen Philips zijn we ons bewust van de zorgen van onze klanten en de cruciale rol die cybersecurity hierin heeft. Naarmate ziekenhuisnetwerken, klinische databanken, medische hulpmiddelen en patiëntmonitoringsystemen meer geïntegreerd raken, neemt ook de kans op kwetsbaarheden en misbruik daarvan toe.”

Systematische aanpak

Bij Philips is men van mening dat effectieve cybersecurity niet langer volstaat met het beschermen van individuele apparaten. Een systematische aanpak is volgens De Jong vereist, waarbij organisaties rekening houden met de risico’s waar en hoe de apparaten worden gebruikt en de digitale zorgplichten die hierbij horen. “We werken dan ook volgens een ‘security-by-design’ principe dat we toepassen op de complete levenscyclus van alle oplossingen die we aanbieden. Dit betekent dat we beveiligingsprincipes toepassen vanaf de tekentafel waar het product wordt ontworpen en ontwikkeld. Het ‘security-by-design’-principe is ook zichtbaar bij het testen en implementeren en wordt opgevolgd met robuuste beleidsregels en procedures voor monitoring, effectieve updates en, waar nodig, incidentresponsmanagement”, vertelt De Jong. “Het Philips Product Security & Services Office werkt hierbij nauw samen met toonaangevende cybersecurity-onderzoekers en testfaciliteiten over de hele wereld, waaronder het Amerikaanse Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) en het Nederlandse expertisecentrum voor cybersecurity in de zorg Z-Cert.”

Philips uses advanced technologies and in-depth insight into clinical applications and consumers’ needs to develop integrated solutions. According to De Jong, this ‘connected healthcare’ is essential in the transformation of healthcare in order to enable better care at a lower cost: ‘We are already investing 60% of our 1.7-billion-euro Research & Development budget in software development. Digitalisation of healthcare is an integral part of our strategy. Because interconnected digital devices are essential to further improve the efficiency of our services, in which the quality of services increases while costs decrease.'

Digital ecosystem

However, this digital ecosystem also leads to a greater cybersecurity vulnerability. According to De Jong: 'The personal data of patients as well as the availability and reliability of digital care systems could potentially be a key target for cyber criminals. At Philips, we are conscious of our customers’ concerns and of the crucial role played by cybersecurity in alleviating those concerns. As hospital networks, clinical databases, medical devices and patient monitoring systems become more integrated, the possibility of vulnerabilities and misuse also increases.'

A systematic approach

Philips believes that effective cybersecurity is no longer sufficient to protect individual devices. De Jong says that a systematic approach is required, in which organisations take into account where and how the devices will be used, as well as what the resulting risks and the associated digital duties of care are: 'We work according to a "security-by-design" principle, which we apply to the entire life cycle of all solutions that we offer. In other words, when we apply security principles, we are starting at the drawing board where the product is designed and developed. This "security-by-design" principle can also be seen in our testing and implementation, and it is followed up with robust policy rules as well as procedures for monitoring, effective updates and incident response management, where necessary. The Philips Product Security & Services Office works closely with leading cybersecurity researchers and test facilities throughout the world, including the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and Z-Cert, the Dutch expertise centre for cyber-security in healthcare.'

‘RESEARCH INTO THE IMPACT OF LAW AND ECONOMICS ON CYBERSECURITY IS BREAKING NEW GROUND’

In mijn promotieonderzoek geef ik oplossingsrichtingen voor overheid, bedrijfsleven en wetenschap, zodat slimmer geïnvesteerd kan worden in cybersecurity. Ik onderzocht nieuwe juridische instrumenten, zoals de mogelijkheid om tegen cyberrisico te verzekeren, de optie om de risico s voor cybersecurity onderling te delen middels pooling en de meldplicht datalekken in de Algemene verordening gegevensbescherming ofwel de AVG.

Laten we het allereerst hebben over de meldplicht datalekken, sinds kort onderdeel van de AVG (die nu flink op het publieke netvlies staat). Cruciaal voor het welslagen van de meldplicht is dat helder is wanneer een datalek wel en wanneer niet gemeld moet worden. Een te ruim afgestelde meldplicht datalekken geeft een verhoogd risico op meldingsmoeheid en onnodige maatschappelijke kosten. Een goed afgestelde meldplicht kan ons daarentegen veel leren over de wijze waarop bedrijven met cybersecurity omgaan. Dan is het wel belangrijk dat al die informatie over datalekken niet in een digitale bureaula verdwijnt zonder dat we daar wat van kunnen leren. Daarom ben ik zeer content met het voornemen in het CSR werkprogramma 2018 2019 om wetenschappelijk onderzoek te laten uitvoeren naar het effect van openbaar melden van datalekken in Nederland binnen de kaders en mogelijkheden van de meldplicht datalekken en de AVG.

Ten tweede is er nog veel verbeterpotentieel op het gebied van de markt voor cyberverzekeringen. Die markt kan flink beter en gestroomlijnder. Ik vroeg bijvoorbeeld namens zes bedrijven tien verschillende cyberpolissen aan. Wat bleek? Verzekeraars stellen nauwelijks cybersecurity eisen aan het MKB vóór het afsluiten van een verzekering. Ook zijn de verzekeringen te ingewikkeld. Premies en polisvoorwaarden verschillen op veel details en de waarde hiervan kan moeilijk worden ingeschat. In mijn onderzoek kostte het bijvoorbeeld ruim drie maanden om alle cyberverzekeringen te vergelijken. Ondoenlijk voor een MKB er. Een basisverzekering zou bijvoorbeeld kunnen helpen om het vergelijken makkelijker te maken.

Tenslotte nog een onconventionele oplossing: een pool voor bedrijven om onderling hun cyberrisico te delen. Een soort Broodfonds voor cyberrisico s dus: bedrijven hebben een aandeel in elkaars risico. Als een deelnemer in de pool dus cyberschade heeft, dragen de andere deelnemers bij. Dit aandeel in elkaar geeft dus een extra stimulans om kennis te delen, want je wilt natuurlijk ook het risico bij de ander beperken. Deze cyberriskpool wordt nu door mij op haalbaarheid onderzocht in samenwerking met verschillende Nederlandse hoge onderwijsinstellingen.

Al met al is onderzoek naar de impact van recht en economie op cybersecurity akkeren op een nog vrijwel braakliggend terrein. Een terrein dat het verdient om verder bewerkt te worden om Nederland weerbaarder te maken tegen cyberaanvallen.

mr. dr. ir. Bernold Nieuwesteeg, Directeur bij het Centre for the Law and Economics of Cyber Security (CLECS) en onderzoeker bij het Rotterdam Institute of Law and Economics (RILE)

“Verzekeraars stellen nauwelijks cybersecurity-eisen aan het MKB”
“Insurers set hardly any cybersecurity requirements on SMEs.”

In my doctoral research, I presented potential solutions for government, academia and industry to make smarter investments in cybersecurity. I studied new legal instruments, such as the possibility of insuring against cyber risks, the option of sharing cybersecurity risks through pooling and the data breach notification obligation in the General Data Protection Regulation (GDPR).

To start, I will talk about data breach notification obligation that recently became part of the GDPR (which, in turn, is very much on the public radar at present). It is crucial to the success of the notification obligation that it is clear when disclosing a data breach is or is not required. If the obligation to notify data breaches is defined too broadly, it increases the risk of notification fatigue and unnecessary social costs. Conversely, a well calibrated obligation to notify can teach us a lot about the way in which companies are handling cybersecurity. To this end, it is highly important that no information about data breaches disappears into a digital drawer before we have a chance to learn from it. For this reason, I am so pleased with the commitment in the work programme established by the Cyber Security Council (CSR) for 2018 2019, which includes commissioning academic research into the effects of public disclosure of data breaches in the Netherlands within the contexts and parameters of the data breach notification obligation as well as the GDPR.

Furthermore, there is great potential for improvement in relation to the cyber insurance market. That market could be made substantially better and more streamlined. For example, I have applied for ten different cyber policies on behalf of six companies. What happened? Insurers set hardly any cybersecurity requirements on SMEs before agreeing to provide insurance. The categories of coverage are also too complex. When you look at the details of premiums and policy conditions, there is wide variation and it is hard to estimate the value of the insurance. In my research, for example, it took me around three months to compare all the various cyber insurance policies. Small business owners do not have that kind of time. A basic insurance could help make it easier to compare policies.

Finally, here is another unconventional solution: a pool in which companies can share their cyber risks. A kind of solidarity fund or collective insurance scheme for cyber risks: companies hold a stake in each other s risk. So if one participant in the pool is harmed by a cyber attack, the other participants help them out. This cooperative approach provides an extra incentive to share knowledge, because you obviously want to limit other companies risks. I have already studied the feasibility of such a cyber risk pool , in collaboration with various higher education institutions across the Netherlands.

All in all, research into the impact of law and economics on cyber security is mostly breaking new ground. This ground deserves further attention to increase the resilience of the Netherlands in the face of cyber attacks.

Dr Bernold Nieuwesteeg
Director of the Centre for the Law and Economics of Cyber Security (CLECS) and
Researcher at the Rotterdam Institute of Law and Economics (RILE)

Sinds 25 mei 2018 is de nieuwe Algemene verordening gegevensbescherming (AVG) van kracht. De AVG zorgt ervoor dat de dezelfde privacywetgeving in de hele Europese Unie geldt. Voorheen hadden alle lidstaten nog hun eigen nationale wetten, gebaseerd op de Europese privacyrichtlijn uit 1995. Met de komst van de AVG hebben alle lidstaten hun nationale wetgeving om moeten zetten, zo ook Nederland. In hoeverre draagt de AVG bij aan een digitaal veilig Nederland? En in is in de AVG aandacht voor cybersecurity? Daarover ging de Cyber Security Raad (CSR) in gesprek met Aleid Wolfsen, voorzitter Autoriteit Persoonsgegevens (AP).

On 25 May 2018, the new General Data Protection Regulation (GDPR) entered into effect. The GDPR ensures that the same privacy legislation is applied throughout the European Union. Up until now, all Member States have had their own national laws, based on the 1995 European Privacy Directive. With the arrival of the GDPR, all Member States – including the Netherlands – have had to amend their national legislation. To what extent is the GDPR contributing to digital security in the Netherlands? And what does the GDPR have to do with cybersecurity? The Cyber Security Council (CSR) talked to Aleid Wolfsen, President of the Dutch Data Protection Authority (DPA).

‘THE GDPR HAS GIVEN CITIZENS BACK THEIR RIGHTS’

Aleid Wolfsen
President of the Dutch Data Protection Authority (DPA).

Volgens Wolfsen staat Nederland er goed voor in verhouding tot de andere lidstaten. Een week voor de invoering van de AVG heeft de Eerste Kamer een klap gegeven op de uitvoeringswet waarmee Nederland op tijd klaar was. Dit was ook nodig vertelt Wolfsen: “Nederland is in Europa relatief een van de meest digitale landen en dat legde ook een grote verplichting op ons land. Als het gaat om digitaal betaalverkeer voor bedragen onder de vijftig euro is Nederland bijvoorbeeld koploper. Je kunt overal betalen met je pinas en veel mensen maken gebruik van toepassingen als ‘Tikkie’. Dit geeft veel competitieve voordelen, maar ook verplichtingen en risico’s als het gaat om cybersecurity. Het is belangrijk dat de beveiliging dan ook in orde is.”

Cybersecurity

De AVG-wetgeving draagt bij aan cybersecurity. “Privacy is een vorm van dataprotectie, en dataprotectie is inmiddels de moeder van alle grondrechten. De AVG zorgt voor de veiligheid van persoonsgegevens bij instellingen. Wij letten op de beveiliging van persoonsgegevens-systemen. Om deze te beschermen moet je adequate organisatorische en technische maatregelen treffen”, vertelt Wolfsen. “Dit is afhankelijk van het soort gegevens, denk bijvoorbeeld aan geloof, politieke activiteiten, gezondheid en seksuele voorkeur. De AVG bevat strenge normen hiervoor.”

Organisaties zijn in bepaalde situaties verplicht een functionaris voor de gegevensbescherming (FG) aan te stellen. Wolfsen: “De FG heeft een bijzondere positie in de organisatie. Deze persoon moet erop toezien dat de organisatie normconform werkt en dat alle juiste maatregelen zijn getroffen om data goed te beschermen.”

Drempel weg

Met alle maatregelen die de wet bevat, heeft de AVG een positieve invloed op het voorkomen van lekken of diefstal van persoonsgegevens. “Ook de eisen voor de meldplicht zijn strenger geworden”, vervolgt Wolfsen. “Zo is de drempel waarbij boetes kunnen worden opgelegd verdwenen; een lek moet nu sneller gemeld worden. De meldplicht is belangrijk omdat de beveiliging is aangescherpt en we dit ook

According to Wolfsen, the Netherlands is in a good position compared to the other Member States. The Senate approved the implementation act one week before the introduction of the GDPR, ensuring that the Netherlands was ready on time. This action was necessary, as Wolfsen explains: 'The Netherlands is one of the most digitalised countries in Europe, which places a significant obligation on our country. For instance, if you look at electronic payment traffic for amounts under fifty euros, the Netherlands comes out on top. You can use your bank card to make payments anywhere, while many people use apps such as Tikkie. While this situation provides many competitive benefits, there are also obligations and risks related to cybersecurity. It is important for the security levels to be up to par.'

Cybersecurity

The GDPR contributes to cyber-security. 'As privacy is a form of data protection, data protection is now the mother of all fundamental rights. The GDPR ensures the security of personal data held by institutions. We make sure that the systems storing personal data are secure.' As Wolfsen explains, to protect personal data, you must have adequate organisational and technical measures in place: 'It depends on the type of data, such as religious beliefs, political activities, health or sexual preference. The GDPR contains strict rules for these types of data.'

In certain situations, organisations are required to appoint a Data Protection Officer (DPO). Wolfsen explains: 'The DPO occupies a special position in the organisation. This person has to ensure that the organisation operates in conformity with the rules and that all proper measures are taken to protect data.'

Removal of the threshold

With all the measures contained in the law, the GDPR is having a positive influence on the prevention of leaks and theft of personal data. 'The obligations to report have become tougher as well,' says Wolfsen. 'For instance, the threshold for the imposition of fines has gone; breaches must now be reported more quickly. The obligation to report is important because security has been tightened and we must be able to monitor it. So it actually benefits the institution concerned for breaches to be reported.' Wolfsen reports that close to a majority of reports come from the healthcare sector, though many also come from the financial sector and government bodies: 'People in the healthcare sector are very happy to make reports, which I find commendable. They want security above all, because they are working with such sensitive and confidential personal data.'

So far, the DPA has not imposed any fines. 'We have imposed penalties, though,' continues Wolfsen. 'In addition, we have received several hundred complaints, which we are investigating. We need to ascertain whether the individuals affected by a data breach should have been notified and, if so, whether they were in fact notified. Finally, we are investigating whether the breach is symptomatic of any structural security issues.'

Public reports

Although the details of individual reported data breaches are confidential in the Netherlands, the DPA is still able to provide general information on the number of reports within individual sectors. When asked whether he would support public reporting, which is required in some states in the USA, Wolfsen is adamant: 'I think that our current law is fine. Nobody can be named and shamed, so I think public reporting is unnecessary. However, I think it a different story when you are talking about the

“Privacy is een vorm van dataprotectie, en dataprotectie is inmiddels de moeder van alle grondrechten”

'As privacy is a form of data protection, data protection is now the mother of all fundamental rights.'

moeten kunnen controleren. Het is dus ook in het voordeel van de desbetreffende instelling dat deze lekken worden gemeld.” Wolfsen vertelt dat bijna het merendeel van de meldingen uit de zorgsector komt, naast de financiële sector en openbaar bestuur. “In deze sector is men zeer meldbereid en dat vind ik prijzenswaardig. Ze willen vooral ook zekerheid, juist omdat ze hier met bijzondere en veel vertrouwelijke persoonsgegevens werken.”

Tot op heden heeft de AP nog geen boetes uitgedeeld. “Wel zijn er dwangsommen opgelegd”, vervolgt Wolfsen. “Ook hebben we een aantal honderd klachten ontvangen die we onderzoeken. We gaan dan na of betrokkenen bij een datalek geïnformeerd hadden moeten worden en of het inderdaad gemeld had moeten worden. Ook onderzoeken we of er een structureel beveiligingsprobleem achter zit.”

Openbare meldingen

In Nederland zijn de gegevens over individueel gemelde datalekken vertrouwelijk. Wel kan de AP in het algemeen informatie geven over het aantal meldingen binnen specifieke sector(en). Op de vraag of Wolfsen voorstander zou zijn van openbaar melden zoals dat in sommige staten van de Verenigde Staten het geval is, is Wolfsen stellig. “Ik vind zoals het nu in de wet staat goed. Het mag geen schandpaal worden, dus openbaar melden vind ik niet nodig. Ik vind het een ander verhaal wanneer het de kwetsbaarheid van landelijke systemen betreft en het daarmee invloed heeft op de nationale veiligheid. Het raakt dan de infrastructuur van de samenleving.”

Balans

Nederland streeft naar een vrije, veilige en welvarende samenleving. Deze drie kernwaarden komen om verschillende redenen steeds meer onder druk te staan. Door de digitale ontwikkelingen komen fundamentele waarden: transparantie en privacy soms met elkaar op gespannen voet te staan. Wolfsen: “De AVG-wet brengt balans in het behouden van kernwaarden als transparantie en privacy in dit digitale tijdperk. De digitalisering van de samenleving brengt naar mijn idee vooral welvaart en levensplezier met zich mee voor de burger. Anderzijds zijn er ook zeer serieuze risico’s waar we rekening mee moeten houden. We zijn ontzettend kwetsbaar; alles is aan elkaar gekoppeld. En mensen geven nog veel te ondoordacht ergens toestemming voor. Kwetsbaarheden in systemen zijn niet altijd te voorkomen. De oplossing ligt in het adequaat reageren, melden en oplossen van een datalek. Belangrijker nog is het voorkomen ervan. Als het gaat om cybersecurity blijkt de mens vaak de zwakste schakel. We moeten ons bewust worden van het feit dat je voorzichtig moet omgaan met je eigen persoonsgegevens en ook met die van een ander. Daarom is de AVG zo belangrijk, die maakt de rechten van burgers weer krachtig!”

Digitale opvoeding

Het bewust worden van de risico’s die het digitale tijdperk met zich meebrengt kan volgens Wolfsen het beste op een vroege leeftijd worden gedaan. Wolfsen: “Voor ons was dit reden om de campagne ‘Privacy gaat iedereen wat aan’ te starten op een basisschool. De jeugd is immers onze toekomst. Daarom is het belangrijk om ze van jongs af aan op alle fronten ‘digitaal’ op te voeden. Je hoeft niet te kunnen programmeren, maar je moet wel weten hoe de digitale wereld werkt. Een leidinggevende of bestuurlijke positie bekleden is vandaag de dag bijna onmogelijk wanneer je zelf geen kennis hebt van de digitale wereld”, aldus Wolfsen.

---

vulnerability of national systems, where there is an impact on national security. In this case, it affects the infrastructure of society.'

Balance

The aim of the Netherlands is to be a free, secure and prosperous society. These three key values are increasingly coming under pressure for a variety of reasons. The fundamental values of transparency and privacy are sometimes at odds with each other as a result of current digital developments. Wolfsen asserts: 'The GDPR brings balance to the preservation of core values such as transparency and privacy in the digital era. In my view, the primary fruits of the digitalisation of society for citizens are prosperity and happiness. By contrast, there are also very serious risks that we must consider. We are extremely vulnerable, as everything is connected to everything else. People nonetheless continue to give their consent for too many things without thinking about it. Vulnerabilities in systems cannot always be prevented. The solution is to address, report and resolve data breaches appropriately. Even more important is preventing breaches. When it comes to cybersecurity, humans are generally the weakest link. We need to be conscious of the fact that we have to handle our own personal data, as well as other people’s data, with great care. For this reason, the GDPR is so important – it has given citizens back their rights!'

Digital competency

According to Wolfsen, awareness of the risks associated with the digital era is best instilled at an early age. As he says: 'We launched the "Privacy affects everyone" campaign in a primary school to this very end. Young people are our future. For this reason, it is important to train them from an early age to be digitally competent on all fronts. While you may not need to understand coding, you do need to know how the digital world works. These days, occupying a position as a manager or government official is almost impossible if you do not understand anything about the digital domain.'

TOWARDS AN OPEN, SECURE AND PROSPEROUS DIGITAL NETHERLANDS

This is a short summary of the advices given by the authors in this edition of CSR Magazine towards en open, secure and prosperous digital Netherlands.

Cybersecurity requires a **comprehensive and wide-ranging approach**. It is a **shared responsibility** of government, the business community and academia. It should not be a topic addressed by a single ministry.

National and international **collaboration** is essential to address matters effectively.

The agenda and the shared ambition exist. What is now required is the implementation in the shape of **actions and measures**, including the required **funding**.

Points for attention remain **sharing knowledge, information and experience**. The newly established Digital Trust Center is an excellent starting point, as it promotes information provision to Dutch businesses.

Increasing connectivity and chain dependency have led to the need for **chain responsibility** being assumed.

Cybersecurity must become part of the **audit procedure**. In addition, cybersecurity must form part of **procurement**.

Children are the future, so a greater structural focus in primary and secondary education on **developing digital competency** is necessary.

People still often remain the weakest link. Therefore, structural attention to raising consciousness remains necessary.

The rapid growth of the digital economy has resulted in a major shortage of IT specialists and related professionals. As a result, more **investment in academic knowledge** is needed.

We need to anticipate the consequences of an exponential increase in **computing power**, including the consequences for cybersecurity.

When designing products and systems, we need to ensure there are **adaptable and scalable security solutions**. This is a *global* challenge, which requires more than a *local* solution.

Colofon | Colophon

Opdrachtgever: Cyber Security Raad Nederland | Commissioning party: **Dutch Cyber Security Council**
Hoofdredactie | Chief editor: **Elly van den Heuvel (secretaris |** secretary)
Concept en (eind)redactie | Concept and (final) editing: **Heidi Letter**
Met dank aan | With thanks to: **Andrea Bakker (CSR), Rene Corbijn (Nederland ICT), Nicole Mallens (VNO NCW), Siep van Sommeren (CSR), Ester Valk (CSR), Ronald Verbeek (CIO Platform), Christel Verloop en Lodewijk van Zwieten (OM)**
Fotografie | Photography: **Jeroen de Bakker, Miranda Koopman, Jeff Lubin, Arenda Oomen**
Vertalingen | Translations: **Metamorfose Vertalingen** • **Opmaak |** Layout: **BKB** • **Drukwerk |** Printwork: **Xerox/OBT**

September 2018

CSR
Cyber Security Council
Cyber Security Raad