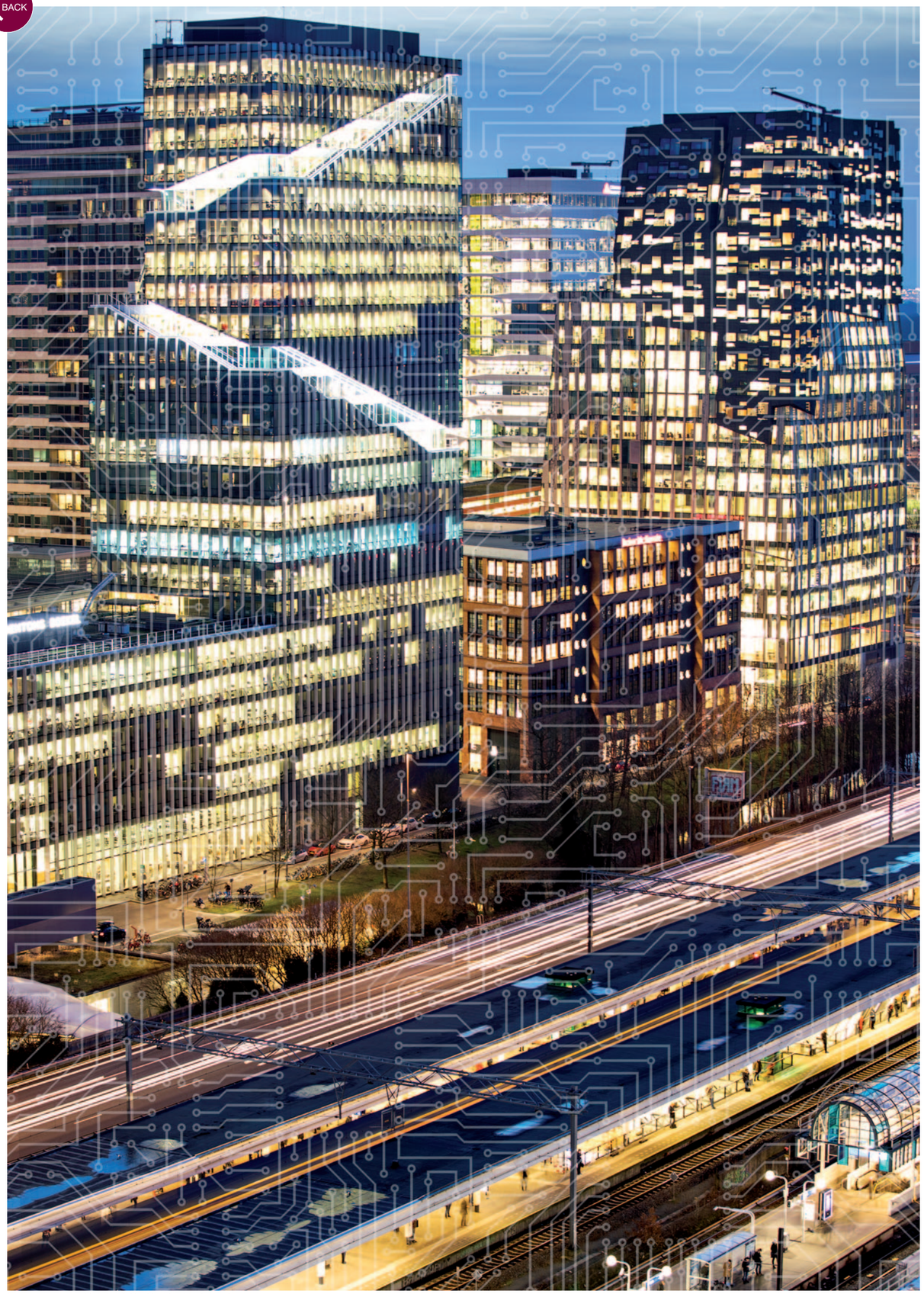
CSR MAGAZINE

Cyber Security Council
Cyber Security Raad

Het belang van de human factor voor een open, veilig en welvarend digitaal Nederland • Top van Nederland aan het woord over het belang van de human factor in relatie tot de digitale veiligheid van Nederland, in Europa en wereldwijd.

The importance of the human factor for an open, secure and prosperous digital Netherlands • High-level government officials and businessleaders speaking about the importance of the human factor in relation to cybersecurity in the Netherlands, across Europe and worldwide.

Jaargang 5, nummer 1, oktober 2019
Volume 5, Issue 1, October 2019



INHOUDSOPGAVE CONTENTS

De Cyber Security Raad

The Cyber Security Council

Van links naar rechts | *From left to right:*
Lokke Moerel, Marieke van Wallenburg, Bart Jacobs, Wiebe Draijer, Ineke Dezentjé Hamming-Bluemink, Elly van den Heuvel-Davies (secretaris/*secretary*), Hans de Jong (covoorzitter/*co-chair*), Pieter-Jaap Aalbersberg (covoorzitter/*co-chair*), Focco Vijselaar, Tineke Netelenbos, ltgen Onno Eichelsheim, Patricia Zorko, Joost Farwerck

Niet op deze foto | *Not on this picture:*
Erik Akerboom, Bibi van den Berg, Gerrit van der Burg, Michel van Eeten, Marcel Krom, Marc van der Linden, Dick Schoof

IN GESPREK MET DE NIEUWE COVOORZITTERS VAN DE CYBER SECURITY RAAD:

A CONVERSATION WITH THE NEW CO-CHAIRS OF THE CYBER SECURITY COUNCIL:

‘CYBERSECURITY MUST BECOME A MAINSTREAM ISSUE. THIS CALLS FOR LEADERSHIP’

Nederland bevindt zich wereldwijd gezien in de kopgroep als het om digitalisering gaat. Onze huidige maatschappij is in al haar facetten afhankelijk van digitale technologie en van digitale netwerken. De digitalisering van onze samenleving creëert kansen voor onze welvaart, maar brengt ook uitdagingen met zich mee. De vraagstukken over onze digitale samenleving worden immers steeds complexer; alles heeft een digitaal component. Cybersecurity is een cruciale randvoorwaarde voor een soepel verloop van de steeds verdergaande digitale samenleving alsook het belang van de human factor bij cybersecurity. Meer samenhang en verbondenheid in de aanpak ervan tussen overheid, private partijen en wetenschap is noodzaak. Ook de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) pleit in het onlangs verschenen rapport dat Nederland zich beter moet voorbereiden op een digitale ontwrichting. Hoe wil de raad hier in de komende periode aan bijdragen? Aan het woord de kersverse covoorzitters van de raad: Pieter-Jaap Aalbersberg, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en Hans de Jong, President Philips Nederland, lid van de raad namens VNO-NCW.

When it comes to digitalisation, the Netherlands is a global leader. Modern society depends in every aspect on digital technology and networks. It creates opportunities in terms of prosperity and also gives rise to certain challenges. After all, digital society is also generating increasingly complex issues, as everything has a digital component. Cybersecurity is a crucial precondition to ensuring the ever-more-digital society runs smoothly; the human factor is a vital element in relation to cybersecurity as well. Government, private parties and the scientific community should approach this issue with greater cohesion and unity. The Netherlands scientific council for governement policy also argued that the Netherlands should prepare better for a digital disruption in their recently published report. How does the council intend to contribute to this in the period ahead? We spoke to the brand-new co-chairs of the Cyber Security Council: Pieter-Jaap Aalbersberg, National Coordinator for Security and Counterterrorism (NCTV) and Hans de Jong, President of Philips Nederland, council member on behalf of VNO-NCW[1].

Beide covoorzitters zijn eensgezind. De digitale transformatie van onze samenleving vraagt volgens de raad om leiderschap en een integrale visie op de vraagstukken die hierbij komen kijken waarbij een ieder zijn verantwoordelijkheden neemt. “Het beeld zoals beschreven in het Cybersecuritybeeld Nederland 2019 benadrukt de noodzaak hiertoe”, start Aalbersberg. “Het rapport concludeert dat vrijwel alle vitale processen en systemen in Nederland volledig gedigitaliseerd zijn. De omvang van de dreiging en het achterblijven van de weerbaarheid maakt Nederland kwetsbaar voor aanvallen. Onze koploperspositie maakt dat Nederland een interessant doelwit is voor statelijke actoren en cybercriminelen. De digitale dreigingen zijn daarmee permanent, overal en nemen toe in omvang en gevolg; maatschappelijke en economische ontwrichting ligt op de loer met alle gevolgen van dien.” De Jong beaamt dit en benadrukt vooral de kansen die de digitalisering voor de economische welvaart van ons land met zich meebrengt. De Jong: “We moeten in Nederland volop inzetten op deze kansen en daarvoor is een digitaal veilige infrastructuur randvoorwaardelijk. Er zijn en worden al veel

The two co-chairs are in agreement. According to the council, the digital transformation of society calls for leadership and an integrated vision on the issues that accompany this shift, in which all parties accept their individual responsibility. 'The picture that emerges from the 2019 Cyber Security Assessment Netherlands shows how important this is,' Aalbersberg begins. 'That report concluded that almost all critical national infrastructure processes and systems in the Netherlands have been digitalised. The extent of the threat and the lack of resilience make the Netherlands vulnerable to attacks. Our status as a leader makes the Netherlands an interesting target for nation-state actors and cybercriminals. Consequently, the digital threats are permanent, ubiquitous and increasing in scope and impact. Social and economic disruption is a looming threat with potentially huge repercussions.' De Jong agrees, but underscores that digitalisation also brings opportunities for the country's economic prosperity. De Jong: 'We should take full advantage of these opportunities – and a secure digital infrastructure is a necessary precondition for doing so. Major steps to increase digital resilience are already being taken, but if you ask me, this isn’t happening fast enough. As a result, we risk losing those opportunities in the process. As I see it, the council has an important task here in terms of advising the government.'

Management & guidance

According to the co-chairs, the issues accompanying digitalisation are becoming more and more complex and international. Moreover, they are not purely technological in nature: everything has a digital component nowadays. De Jong gives 5G and artificial intelligence as examples. 'Along with plentiful opportunities, these technologies are also yielding new and fundamental security issues that require our undivided attention. As it stands, many of these issues are not being resolved, or only when it's too late.' According to Aalbersberg, this is due to the traditional method for bringing together parties in a hierarchy. 'There's no overarching and integrated vision regarding these issues, and that's an oversight the Netherlands simply cannot afford. If we are to maintain our digital resilience, we must link parties that are capable of inspiring action. Cooperation between public parties, private parties and the scientific community remains crucial in that regard. These days, everything is connected to everything else – so we also need an interconnected approach. Coordinated action is needed to respond to all developments and the opportunities they bring, which in turn requires a different kind of management and guidance and clear responsibilities with regard to cybersecurity. Cybersecurity must become a mainstream issue. This calls for leadership.' De Jong agrees on that: “Technology continues to develop at a rapid pace and issues about our digital society are becoming increasingly complex and extensive. The council therefore recognizes the importance of preparedness that the WRR has mentioned in the report. Increasing cyber resilience must be more in line with technological developments; the pace must be increased. It is important that we can continue to respond decisively to abuses and/or cyber attacks. According to De Jong businesses also still have areas for improvement on that one: “Cybersecurity presents a pre-eminent strategic challenge for boardrooms. Their IT department does of course also play an

1. Confederation of Dutch Industry and Employers

stappen ondernomen om de digitale weerbaarheid te vergroten, maar dit gaat naar mijn idee niet snel genoeg. De kansen komen daarmee onder druk te staan. Ik zie daarin een belangrijke rol weggelegd voor de raad om het kabinet hierin te adviseren."

Regie & Sturing
Volgens de covoorzitters worden de vraagstukken die de digitalisering met zich meebrengt steeds complexer, internationaler en zijn deze niet louter gerelateerd aan techniek; alles heeft een digitaal component. De Jong benoemt 5G en kunstmatige intelligentie, als voorbeeld. "Naast alle kansen, leiden deze technologieën ook tot nieuwe fundamentele veiligheidsvraagstukken die onze volle aandacht verdienen. Veel van deze vraagstukken worden nu niet of te laat opgelost." Volgens Aalbersberg komt dit door de traditionele wijze van het bij elkaar brengen van hiërarchie-partijen: "Een overkoepelende en integrale visie op de vraagstukken ontbreekt. Nederland kan zich dit niet veroorloven. We moeten partijen samenbrengen die in staat zijn om beweging te creëren om Nederland digitaal weerbaar te houden. De samenwerking tussen publieke-, private partijen en de wetenschap blijft daarin van cruciaal belang. Alles is nu met alles verbonden en dat moet ook gelden voor onze aanpak. Om in te kunnen spelen op alle ontwikkelingen en de kansen die dit met zich meebrengt is gecoördineerde actie nodig en dat vraagt om een andere wijze van regie en sturing op cybersecurity en duidelijke verantwoordelijkheden. Cybersecurity moet mainstream worden en dat vraagt om leiderschap." De Jong vult aan: "De techniek blijft zich in sneltreinvaart ontwikkelen en vraagstukken over onze digitale samenleving worden steeds complexer en omvangrijker. De raad herkent zich daarom in het belang van paraatheid dat de WRR in het rapport heeft benoemd. Het verhogen van de cyberweerbaarheid moet meer in de pas lopen met de technologische ontwikkelingen; het tempo moet omhoog. Het is belangrijk dat we slagvaardig kunnen blijven reageren op misstanden en/of cyberaanvallen." Volgens De Jong dient ook in het bedrijfsleven nog een slag te worden gemaakt: "Cybersecurity is niet alleen de verantwoordelijkheid van de IT-afdeling. Het is de verantwoordelijkheid van de boardroom. Een goede cybersecurity-aanpak raakt alle elementen in een organisatie en de boardroom dient op strategisch niveau de kaders te bepalen voor het formuleren, implementeren, bewaken en handhaven van het cybersecuritybeleid in de organisatie. Dat is overigens geen eenmalige exercitie, maar een continu proces."

Kunstmatige intelligentie
De regie en sturing moet op een andere wijze worden ingevuld; het is nu te versnipperd. De Jong benoemt kunstmatige intelligentie als voorbeeld. "Je ziet dat iedereen een beetje wakker aan het worden is en erover nadenkt om kunstmatige intelligentie een duidelijker toneel te geven; er zijn verschillende initiatieven aan het ontstaan, maar een integrale visie hierop ontbreekt. Als je kijkt naar de landen om ons heen, dan zijn zij op dit vlak al vele stappen verder en beschikken zij ook over de middelen hiervoor. Daar maak ik me echt zorgen over. We hebben daarin een inhaalslag te maken, publiek en privaat. Naar mijn idee heeft de overheid hierin nu een duidelijke stap te zetten." Aalbersberg vult aan: "Naast kunstmatige intelligentie geldt dit voor veel andere zaken. Er moet gekeken worden naar hoe publiek, privaat en wetenschap hier gezamenlijk op in kunnen zetten als het gaat om cybersecurity. Ook vanuit de raad kunnen we daaraan bijdragen."

Human factor
Een belangrijke uitdaging ten aanzien van cybersecurity ligt volgens de covoorzitters op het vlak van de human factor. Volgens Aalbersberg is het van belang dat de human factor onderdeel is van het grote geheel. "Mens en techniek zijn nauw verweven met elkaar en moeten als één geheel worden gezien. In de afgelopen jaren heeft de raad hier al vol op

important role, but the boardroom is responsible to set the parameters at strategic level for the formulation, implementation, monitoring and maintenance of their organisation's cybersecurity policy. This is not a one-off matter, but a continuous process."

Artificial intelligence
Management and guidance must be organised in a new way, as the current approach is too fragmented. One example, says De Jong, is artificial intelligence. 'Awareness is growing and everyone is thinking of ways to give artificial intelligence a more prominent role. All kinds of initiatives are being set up, but what we lack is an integrated vision for the whole. The countries around us are many steps ahead of the Netherlands in this area and have made the necessary resources available. I find this deeply concerning. We have some catching up to do there, and I think it's down to the government to make the first move.' Aalbersberg agrees, adding: 'This is true in many areas besides artificial intelligence, too. We have to look at ways for the public and private sectors and the scientific community to take concerted action when it concerns cybersecurity. We in the council can assist in that regard.'

Human factor
The co-chairs see a major cybersecurity-related challenge where the human factor is concerned. According to Aalbersberg, it is important to ensure a place for the human factor within the larger whole. 'People and technology are closely interwoven and should be considered as a single entity. This has been a great priority for the council in recent years, as is reflected in our advice on cybersecurity in education and the business community, and in the council's recommendation to discontinue the quota system for degree programmes in artificial intelligence and other, similar disciplines. The council is concerned, for instance, about the fact that we're not sufficiently preparing young people for the digital future and that we're headed for a desperate shortage of cyberspecialists. New technological developments, such as artificial intelligence, call for new knowledge and skills. We have a great need for such specialists, now and in the future. The council is insistent, therefore, that the problems with the quota system for study programmes in artificial intelligence and related disciplines such as data science and business analytics should be resolved in the short term.' De Jong concurs, and is concerned primarily for young people in the Netherlands: 'The expectation is that primary and secondary education will implement their new curriculum from 2022. After that, the schools will be given an additional term of eight years to do so. I find it quite distressing that two generations of pupils are currently not being taught digital skills. What's at stake here is, after all, the prosperity of our children and our children's children. Fortunately, we're seeing all manner of local initiatives emerging. Within the council we're also exploring possible solutions for bridging the gap that has opened up in primary and secondary education in the meantime.'

European context
Cybersecurity is a cross-border issue. Aalbersberg: 'That's why the council is advocating for more intensive cooperation with other countries and in a European context in order to present a united front against nation-state actors, hackers and cybercriminals so that we can prevent cybersecurity-related incidents. Consider issues of digital dependence, for instance: the Netherlands should take on a leading role in this regard. Only then will we be able to continue to profit from economic opportunities and encourage innovation for an open, secure and prosperous digital society.'

"Mens en techniek zijn nauw verweven met elkaar en moeten als één geheel worden gezien"

'People and technology are closely interwoven and should be considered as a single entity'

Pieter-Jaap Aalbersberg
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), covoorzitter van de raad namens de publieke sector

Sinds 1 februari 2019 is Pieter-Jaap Aalbersberg de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Hiervoor was hij politiechef van de regionale eenheid Amsterdam. Daarvoor is hij achtereenvolgens korpschef Politie Amsterdam-Amstelland en korpschef Politie IJsselland geweest. In 2014 na de ramp met vlucht MH17, gaf hij leiding aan de repatriëringsmissie in de Oekraïne.
Hij volgde de Politieacademie en hij behaalde een Executive Master of Police Management aan de Nederlandse School voor Openbaar Bestuur. Na zijn opleiding aan de Nederlandse Politieacademie was hij voornamelijk werkzaam op het gebied van intelligence en analyse en bestrijding van georganiseerde misdaad en terroristische misdrijven.

Pieter-Jaap Aalbersberg
National Coordinator for Security and Counterterrorism (NCTV), Co-chair of the council on behalf of the public sector

Pieter-Jaap Aalbersberg took office as National Coordinator for Security and Counterterrorism on 1 February 2019. Prior to this position, he was Police Chief for the Amsterdam regional unit, and before that he served consecutively as chief constable for the Amsterdam-Amstelland police region and chief constable for the IJsselland police region. In the aftermath of the flight MH17 disaster in 2014, he led the repatriation mission in Ukraine. He attended the Police Academy of the Netherlands and earned an Executive Master of Police Management from the Dutch School for Public Administration. Following his training at the Police Academy, most of his work has been in the field of intelligence and analysis and combating organised crime and terrorism.

ingezet, denk aan ons advies over cybersecurity in het onderwijs en het bedrijfsleven en het advies van de raad inzake de afschaffing van numeri fixi-systemen voor de studie kunstmatige intelligentie en aanverwante studies. Zo maakt de raad zich zorgen over het feit dat we onze jeugd onvoldoende voorbereiden op de digitale toekomst en dat we aankoersen op een schrijnend tekort aan cyberspecialisten. Nieuwe technologische ontwikkelingen, zoals kunstmatige intelligentie, vragen om nieuwe kennis en vaardigheden. Deze specialisten hebben we nu en in de toekomst heel hard nodig. De raad dringt er daarom op aan dat de numeri fixi-problematiek voor de studie kunstmatige intelligentie en aanverwante studies als data science en business analytics snel wordt opgelost." Ook De Jong is het hiermee eens en maakt zich vooral zorgen over onze jeugd: "De invoering van het nieuwe curriculum in het primair – en voortgezet onderwijs geeft scholen de mogelijkheid om dit naar verwachting vanaf 2022 in te voeren. De scholen krijgen hiervoor vervolgens nog acht jaar de tijd. Ik vind het erg zorgelijk dat twee generaties van onze jeugd nu geen les krijgen in digitale vaardigheden. Het gaat immers om de welvaart van onze kinderen en de kinderen van onze kinderen. Gelukkig zien we wel allerlei lokale initiatieven ontstaan. Ook als raad zijn we aan het nadenken over mogelijke oplossingen om de tussentijdse ontstane kloof in het primair en voortgezet onderwijs te overbruggen."

EU-verband
Cybersecurity is per definitie een grensoverschrijdend vraagstuk. Aalbersberg: "Vanuit de raad pleiten we daarom voor intensieve samenwerking met andere landen en in Europees verband om gezamenlijk een front te vormen tegen statelijke actoren, hackers en cybercriminelen om incidenten op het vlak van cybersecurity te voorkomen. Denk bijvoorbeeld aan vraagstukken over de digitale afhankelijkheid. Nederland moet hierin een vooraanstaande rol spelen. Alleen zo kunnen we in Nederland blijvend de kansen verzilveren en innovatie bevorderen, voor een open, veilige en welvarende digitale samenleving!"

BACK TO TOP

"Alles is nu met alles verbonden en dat moet ook gelden voor onze aanpak"
'These days, everything is connected to everything else – so we also need an interconnected approach'

Hans de Jong
President Philips Nederland, lid van CSR namens VNO-NCW, covoorzitter van de raad namens de private sector

Binnen Royal Philips is Hans de Jong sinds 2012 verantwoordelijk voor Philips in Nederland. In deze rol is hij o.a. mede verantwoordelijk voor de transformatie van Philips naar een Gezondheid technologie concern in Nederland. Daarnaast is hij onder andere lid van het dagelijks bestuur van VNO-NCW, FME, vicevoorzitter van de Stichting Brainport en Lid Taskforce AI. Daarvoor was hij ruim 25 jaar voor Philips internationaal actief in management-rollen waarvan acht jaar woonachtig buiten Nederland, o.a. in Hong Kong.

Hans de Jong
President of Philips Nederland, member of CSR on behalf of the Confederation of Netherlands Industry and Employers VNO-NCW, Co-chair of the council on behalf of the private sector

Since 2012 Hans de Jong is responsible for Philips in the Netherlands within Royal Philips. In this role he is, among other things, partly responsible for the transformation of Philips into an Health technology concern in the Netherlands. He is also a member of the executive committee of VNO-NCW, FME, vice-chairman of the Brainport Foundation and Member of the Taskforce AI. Before this he was 25 years internationally active for Philips in management roles, of which 8 year living abroad, among others in Hong Kong.

In februari 2019 bracht Kim Putters, directeur voor Sociaal en Cultureel Planbureau (SCP) en bijzonder hoogleraar beleid en bestuur van de zorg aan de Erasmus Universiteit Rotterdam zijn boek 'Veenbrand' uit. In zijn boek stelt Putters dat het huidige sociaal contract van onze samenleving uitgewerkt lijkt te zijn. De samenleving verandert en dat vraagt een nieuw sociaal contract voor de toekomst en een meer integrale visie op belangrijke vraagstukken die vandaag de dag spelen.

In February 2019, Kim Putters, director of the Netherlands Institute for Social Research (SCP) and endowed professor of Health Policy & Management at Erasmus University Rotterdam, published his book Veenbrand *[Peat fire]. In it, Putters posits that the current social contract within Dutch society appears to have spent its force. Society is changing, which calls for a new social contract for the future and a more integrated vision on the vital issues at play in today's world.*

Kim Putters
Director of the Netherlands Institute for Social Research (SCP) and endowed professor of Health Policy & Management at Erasmus University Rotterdam

A NEW SOCIAL CONTRACT FOR THE FUTURE

"Het begrip van het sociaal contract is terug te voeren naar de aloude filosofen", vertelt Putters. "Burgers stonden hun macht af aan de heersers in ruil voor sociale bescherming of veiligheid. Ook in de huidige moderne samenleving geldt het sociaal contract; we betalen onze belasting en premies en gaan stemmen. Hiermee geven we de macht aan de politieke leiders en in ruil daarvoor leven we in een democratie waarin we rechten hebben op bijvoorbeeld de gezondheidszorg. Het maakt dat we in vrijheid kunnen leven en dat we welvaart delen. Vertrouwen is daarbij cruciaal en dat brokkelt af als de overheid beloftes niet na kan komen en als de verbinding tussen groepen in de samenleving minder wordt." Onze samenleving is volgens Putters echter aan het veranderen. "Niet alleen onze arbeidsrelaties staan onder druk – we zijn echt op een andere manier ons werk en onze sociale relaties aan het inrichten. We communiceren anders en dat heeft sociale en culturele gevolgen. Daarmee staat ook het politieke systeem onder druk; er is twijfel over de verbinding tussen de samenleving en politici."

Informatiesamenleving

Putters is van mening dat deze ontwikkeling om een andere aansturing vraagt of in ieder geval

'The concept of the social contract can be traced back to the philosophers of yore,' says Putters. 'Citizens ceded their power to rulers in exchange for social protection or safety. The social contract applies in our modern society as well: we pay taxes and insurance premiums and turn out to vote. By doing so, we give power to the political leaders and in return we get to live in a democracy that assures us of certain rights, such as the right to healthcare. This enables us to live in freedom and enjoy shared prosperity. Trust is a vital aspect of the system, and it is eroded when the government is unable to keep its promises and when the cohesion between social groups is weakened.' According to Putter, however, society is changing. 'It is not only our employer-employee relationships that are under pressure; we are reorganising our working lives and social relationships as well. Our communication methods have changed, and this has social and cultural repercussions. It places the political system under pressure as well; there are doubts about the connection between society and politicians.'

Information society

Putters believes that this development calls for a different kind of management, or in any case greater cooperation than we are currently seeing. 'If you add up all the changes and developments, from a historical perspective it's rather like we've created a new society altogether. We're at a new crossroads in our history: the transition to an information society. Looking back, previous major shifts heralded things like the introduction of civil rights and fundamental social rights. Now just might be the time when information rights for citizens emerge.' According to Putters, our current systems are no longer well-suited to the way we organise our day-to-day lives and how we communicate this to one another. 'The same problem is evident in the political system, a model that's over 200 years old. You could easily drop a parliamentarian from a century ago into today's political arena and that person would have no trouble understanding exactly how the procedures work. But if you then sent that same individual out into society, he would be completely at a loss. This undermines people's trust in institutions. We need to rethink how we choose to organise society; we must work towards an information society in which technology, information and communication tools are managed in a different way together with citizens.'

"We staan op een nieuw kruispunt in onze geschiedenis, de transitie naar een informatiesamenleving"

'We're at a new crossroads in our history: the transition to an information society'

Core cabinet

This will also entail a new perspective and vision on the relationship between the government and citizens. In his book, Putters puts forth the idea of a 'core cabinet'. Rather than a large cohort of ministers, this would be a small cabinet of just four ministers who focus on finding solutions to the major issues of the day. His proposal: one minister for general welfare, one for inclusion and social equality, one for life course issues and one for democracy and law. Beside a minister for foreign affairs and defense and the prime minister. The idea of a core cabinet has been around for a very long time, says Putters: 'When you enter the historic chamber of the Dutch Senate, you'll see a cabinet table surrounded by seven chairs. This is no coincidence. While the idea of a more integral approach to issues might be old-fashioned, it may never have been more necessary than it is today.'

Budgets

Putters is aware that this transition cannot be realised overnight. 'So

meer samenwerking dan nu het geval is. “Als je alle veranderingen en ontwikkelingen bij elkaar optelt, dan heeft het historisch gezien alles weg van een nieuwe samenleving. We staan op dit moment op een nieuw kruispunt in onze geschiedenis, de transitie naar een informatiesamenleving. Als je terugkijkt naar onze geschiedenis dan zijn bij eerdere belangrijke veranderingen bijvoorbeeld onze burgerrechten en de sociale grondrechten ontstaan. Nu zouden dit zo maar eens de informatierechten voor burgers kunnen zijn”, vervolgt Putters. Onze huidige systemen passen volgens Putters niet meer bij de manier waarop we vandaag de dag ons dagelijkse leven organiseren en daarover communiceren met elkaar. “Dat merk je dus ook in het politieke systeem, een model dat al 200 jaar oud is. Je kunt met gemak een kamerlid van 100 jaar geleden vandaag de dag in de politieke arena plaatsen en deze persoon zal begrijpen hoe de procedures verlopen. Als je deze persoon vervolgens de samenleving instuurt, dan zal hij totaal de weg kwijt zijn. Dit zet het vertrouwen van burgers in de instituties onder druk. Het vraagt om heroriëntatie van hoe we onze samenleving willen inrichten. We moeten toewerken naar een informatiesamenleving waar technologie, informatie en communicatiemiddelen op een andere manier en met burgers samen worden gebruikt.”

Kernkabinet

Daar past ook een nieuw denken en visie op de verhouding tussen overheid en burgers bij. In zijn boek werpt Putters het idee op van een kernkabinet: in plaats van een grote ministersploeg een klein kabinet van vier ministers die zich richten op oplossingen voor de grote vragen van deze tijd. Zijn voorstel: één voor brede welvaart, één voor inclusie en sociale gelijkheid, één voor de levensloop en één voor democratie en recht. Met daarnaast bijvoorbeeld nog een minister voor buitenlandse zaken en defensie en de minister-president. Het idee van het kernkabinet is volgens Putters al heel oud: “Als je naar de aloude zaal van de eerste kamer gaat, dan staat hier een regeringstafel met daaromheen zeven stoelen. Dat was niet voor niks. Het idee van het meer integraal aanvliegen van vraagstukken is dan wellicht ouderwets, maar de noodzaak is wellicht nog nooit zo groot geweest!”.

“We hebben leiders nodig die zich durven te verbinden, de burger centraal stellen en niet primair vanuit systemen denken”

‘We need leaders who are unafraid to commit and connect, who put citizens first and who don't necessarily think in terms of systems’

Begrotingen

Putters beseft dat deze transitie niet van vandaag op morgen te realiseren is. Putters: “Naarmate we met meer politieke partijen moeten regeren en dus de macht over meerdere mensen in het kabinet verdelen, blijft het ingewikkeld om substantieel tot een minder aantal bewindspersonen te komen.” Volgens Putters kunnen er echter wel slagen gemaakt worden. “Men zou bijvoorbeeld na kunnen denken over begrotingen. In de politiek is de begroting cruciaal en sturend. De begrotingsbehandelingen en dus de gesprekken in de Kamer zullen ook themagerelateerd plaats moeten vinden”, redeneert Putters. “Als je echt een stap wilt maken, dan zou je het aantal beleidsterreinen kunnen opsplitsen tot een zeven- of achttal thema’s met bijbehorende begrotingen. Dan is het vervolgens nog de vraag hoe het daar achter te organiseren met een minister, een staatssecretaris en hun ambtenaren. Ik geloof dat dit in de politieke werkelijkheid echt verschil uit kan maken.”

Leiderschap

Op de vraag aan Putters over welk politiek leiderschap hiervoor nodig is, is Putters stellig: “We hebben leiders nodig die zich durven te verbinden, de burger centraal stellen en niet primair vanuit systemen denken. Ik zie te vaak dat bij bijvoorbeeld stelselwijzigingen burgers vaak het sluitstuk zijn terwijl zij ook de aanleiding vormden voor de wijziging. Vooral in de gezondheidszorg vind ik dit erg opvallend. Patiënten en zorgverleners geven aan met ingewikkelde bureaucratie te maken te hebben en zien door de bomen het bos vaak niet meer. Dit komt omdat er onvoldoende is nagedacht over wat we nu echt willen bereiken en of burgers die verandering mee kunnen maken. Die les moet geleerd worden; er moet veel meer de verbinding gezocht worden tussen de verandering die men wil bereiken en de burger ofwel de samenleving.” Politiek leiderschap betekent volgens Putters ook niet zo zeer om mensen zekerheid te verkopen: “Zij moeten ervoor zorgen dat burgers en bedrijven met onzekerheid om kunnen gaan en zo goed mogelijk de randvoorwaarden weten te scheppen om in de informatiesamenleving de weg te weten te vinden. Het redeneren vanuit de samenleving is een groot verschil met hoe we tot nu toe altijd onze systemen ingericht hebben.”

Uitdaging

Volgens de cultuurdimensies van Hofstede[1] komt het politieke klimaat van Nederland het meest overeen met dat van de Scandinavische landen. “Je ziet dat Nederland vaak in het cluster zit van Scandinavië, omdat wij toch een sterke gerichtheid hebben op machtsevenwicht tussen burgers en overheid. We beschikken over collectieve regelingen met afspraken over zeggenschap en de invloed die burgers daar zelf over mogen hebben, met wat Angelsaksische trekken. Aan de andere kant wordt namelijk ook geprobeerd marktprincipes en meer keuzevrijheid op allerlei terreinen te introduceren. Wij zitten dus min of meer in een gemengd model”, vervolgt Putters. “Daarom is het ook zo diffuus voor hoe we met zaken omgaan; aan de ene kant zijn we argwanend naar de overheid, maar we kiezen ook niet vol voor het marktmodel. Ergens in het midden zullen we toch een fatsoenlijke en aanvaardbare manier moeten vinden om met vraagstukken als bijvoorbeeld cybersecurity om te gaan. Daar zie ik echt een uitdaging in!”

BACK TO TOP

long as we're obliged to form a government with multiple political parties and to distribute power among more people in the cabinet, substantially reducing the number of ministers will remain a complex undertaking.' According to Putter real progress is possible. 'We could, for instance, start thinking about budgets. In politics, budgets are a crucial and determining factor. So budgetary discussions and the associated parliamentary debates should focus on specific themes as well,' Putters reasons. 'If you really wanted to take a step in the right direction, you could regroup the current policy areas into seven or eight themes, each with a corresponding budget. After that, there's still the question of how to arrange the underlying structure with ministers, state secretaries and their civil servants. I believe this could have true impact on the political reality.'

Leadership

When asked about the type of political leadership required, Putters is quite firm: 'We need leaders who are unafraid to commit and connect, who put citizens first and who don't necessarily think in terms of systems. All too often, in cases of system changes, citizens are a kind of afterthought – whereas they're supposedly what motivated the change in the first place. This is especially evident in the healthcare industry. Patients and healthcare professionals indicate that they have to deal with complicated bureaucracy and often cannot see the wood for the trees. This is because we haven't devoted enough thought to what we really want to achieve and whether citizens can go along with the changes. It's a lesson that has to be learned: we should be working much harder to bridge the gap between the change we are trying to bring about and the citizens, or society, affected by those changes.' Putters also feels that political leaders should focus more strongly on potential risks: 'They must help citizens and businesses manage uncertainty and enable them to create the best possible conditions for making their way in the information society. We should do our reasoning based on the interests of society, which is a far cry from how we've been organising our systems until now.'

Challenge

According to Hofstede's cultural dimensions theory[1], the political climate in the Netherlands most closely resembles that of the Scandinavian countries. Putters: 'The Netherlands often winds up in the same cluster as Scandinavia due to our strong focus on a balance of power between citizens and government. The Netherlands has collective schemes that include agreements on decision-making and how citizens can influence that process, with a few Anglo-Saxon features as well. But at the same time, we're also seeing efforts to introduce market forces and freedom of choice into all kinds of areas. The Dutch model, in other words, is more or less a hybrid. This also explains a certain fuzziness in our approach: on the one hand, we view the government with a measure of suspicion; yet on the other, we're not entirely committed to the free-market model either. To adequately handle issues like cybersecurity, we'll have to find a decent and acceptable medium somewhere between the two. We're in for quite a challenge in that regard.'

1 Hofstede, G. & Hofstede, G.J. (2005). *Allemaal andersdenkenden, omgaan met cultuurverschillen* [So many different perspectives: dealing with cultural differences]. Amsterdam: Uitgeverij Contact

Prof. Mr. Corien Prins
Chair of The Netherlands Scientific Council for Government Policy (WRR) and Professor of Law and Information Technology, Tilburg University

PREPARING FOR DIGITAL DISRUPTION CALLS FOR GOVERNMENT ATTENTION

Op 9 september 2019 nam secretaris-generaal Siebe Riedstra van het ministerie van Justitie en Veiligheid het eerste exemplaar van het WRR-rapport 'Voorbereiden op digitale ontwrichting' in ontvangst. In dit rapport presenteert de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) zijn analyse en adviezen op hoe Nederland voor te bereiden op een eventuele digitale ontwrichting. “Nu de digitale wereld steeds verder verknoopt raakt met fysieke infrastructuren en het sociale weefsel van onze samenleving is cybersecurity alleen niet langer voldoende”, vertelt prof. mr. Corien Prins, voorzitter van de WRR en hoogleraar Recht en Informatisering aan de Universiteit Tilburg.

On 9 September 2019, General Secretary of Justice and Security Siebe Riedstra received the first copy of the WRR report on the approach to digital disruption. In its report, The Netherlands Scientific Council for Government Policy (WRR) presents its analysis and recommendations on how best to prepare the Netherlands for any potential digital disruption. 'As the digital world is becoming increasingly intertwined with physical infrastructures and the social fabric of our society, cybersecurity alone no longer suffices,' says Corien Prins, WRR chair and Professor of Law and Information Technology at Tilburg University.

“Het Cybersecuritybeeld Nederland 2019 maakt expliciet duidelijk dat een ontwrichting van de samenleving als gevolg van digitale aanvallen op de loer ligt”
‘The Cyber Security Assessment Netherlands 2019 explicitly refers to the threat of societal disruption as a consequence of digital attacks’

Wie de trefwoorden ‘voorbereiden op een ramp’ in een zoekmachine inbrengt, krijgt als één van de resultaten een link naar de pagina van de rijksoverheid met als titel “Wat moet ik doen bij een ramp?”. Na wat doorklikken is de nodige informatie te vinden over de voorbereiding op specifiek een cyberaanval. Wat Prins opvalt is dat de meerderheid van de aldaar genoemde maatregelen ziet op het *voorkomen* van een cyberramp. “Slechts een zeer beperkt aantal gaat over maatregelen tijdens en na de ramp.

Wat eveneens opvalt is dat de laatstgenoemde maatregelen uitsluitend zien op een *digitale* ramp en wijzen op het belang van het veranderen van wachtwoorden en het installeren van nieuwe antivirussoftware” vertelt Prins.

Die insteek is volgens Prins te beperkt. “In hoog tempo zijn digitale en fysieke processen in de maatschappij met elkaar verknoopt geraakt. De kans is daarom groot dat een toekomstige cyberramp niet beperkt blijft tot het digitale

One of the hits after Googling ‘preparing for disaster' (in Dutch) is a link to a Dutch government webpage titled ‘What to do in the event of a disaster?' (in Dutch). A few further clicks will yield extensive information on how to prepare, specifically, for a cyber attack. What is striking, says Prins, is that most of the measures listed there focus on *preventing* a cyber emergency. 'Only very few of those measures concern the period during and after the emergency. It also strikes me that the measures that do cover that period only concern a *digital* disaster and highlight the importance of changing passwords and installing new anti-virus software.'

That approach is too restricted, says Prins. 'Digital and physical processes in society have become intertwined very rapidly. As a result, it's quite conceivable that a future cyber emergency will not remain limited to the digital domain, but spill over into other areas such as healthcare, transport and all sorts of infrastructures and processes - including vital ones. The examples are all too familiar: in the *WannaCry* ransomware attack, part of the British healthcare system crashed. *NotPetya* brought the production of vital medicines to a standstill and caused hundreds of millions of euros worth of damage to one of the world's biggest container shipping companies.'

Internal interaction
Fortunately, crisis and disaster management organisations are devoting more and more attention to the intensive interaction between the digital and physical spheres. Prins: 'Take, for example, the Dutch National Security Strategy 2019. Likewise, the Cyber Security Assessment Netherlands 2019 explicitly refers to the threat of societal disruption as a consequence of digital attacks. 'Both documents send a stark message: the risks in our digital society are changing and we will need to take new measures that will allow us to act effectively and limit the damage in the event of a disruptive attack.

So what are these measures that we need to take? Prins explains: 'We already have a professional crisis management organisation in place, with the associated laws and regulations, to deal with more familiar disasters and types of disruption, such as floods, epidemics or major fires. There's much less clarity though about what we should do, and what we're able to do, in the event of large-scale societal disruption caused by a digital incident.'

According to Prins, the WRR report on digital disruption that was presented to General Secretary Siebe Riedstra in September offers significant input to fill this gap. 'It deals with questions such as: Who should take the lead in the event of digital disruption? What sort of institutional organisation, or reorganisation, is required? What new authorities and resources do we need? And how can we prepare for digital disruption across our national borders? In addition to that, the WRR considers the opportunities for reconstruction of our digital society and for regaining people's trust in digital facilities.'

The WRR opens its report by asking who should act as the 'fire department' when a 'fire' breaks out in the digital world and emergency services are called. Prins: 'If you follow up on this metaphor of a traditional fire department, all sorts of questions emerge. Are we sufficiently aware of all the nearby facilities at risk? What part of the fire should we try to extinguish first, and what powers do the authorities involved have in terms of accessing premises during an emergency? Do we know what will happen if we decide to switch off digital facilities to prevent an even worse outcome? And what is the order in which we switch them on again, especially vital facilities? What is the best

approach to ensure rapid recovery after the disaster?'

Centralised standards and coordination

One of the WRR's conclusions is that digital disruption calls for more centralised standards and more government-controlled coordination. 'It is obvious that we can't prepare effectively for disruptive situations without a contribution from private parties,' Prins continues. 'For example, they could develop relevant standards and protocols. Given that private parties have interests of their own, we can't expect them to also assume full responsibility for the response to digital disruption. That responsibility clearly belongs with the government, as it does in the context of other types of societal disruption. However, the set of tools currently available to the government for shouldering that responsibility is highly inadequate. For example, the Dutch government currently has relatively few means and powers to intervene if private organisations and businesses refuse to collaborate in the event of imminent or actual disruption. In other words, there would be little the national government, the municipalities and other public bodies could do to force businesses to join the effort. And there is even less that the European Union could do, because it only plays an advisory role and has left it to the Member States to decide on strategic and operational aspects of cyber issues. Clarifying and strengthening both powers and standards at the national government level will help to create a framework for more robust coordination and, if necessary, escalation to a higher administrative level. At the same time, this will create the space needed to develop concrete measures and implement them in specific contexts. After all, the measures that need to be taken in the healthcare sector will differ from those required in, say, water supply.'

The WRR's recommendations

In short, the WRR's advice is that, as in other fields, the response to digital disruption should be based on the principle that the 'local fire department' deals with local 'fires' and that specialist 'fire brigades' should deal with the more complex 'fires'. Prins: 'Developing concrete measures at the level of specific contexts will ultimately also serve the interests of the parties involved, as this offers them more certainty when preparing for and confronting a disruptive digital event.'

The WRR has structured the general task that it assigns to the government by means of four well-known phases in preparing for disruption: preparedness, detection, response and recovery. 'Given these phases, one of the WRR's recommendations is that we should gain more insight into the dependencies involved,' Prins summarises. In addition, the WRR also recommends developing an alternative approach to and implementation of vital infrastructure, and reconsidering the way we prioritise critical national infrastructure processes in this country ('What parties, digital elements, vital processes and services does the functioning of Dutch society depend on?). Finally, the WRR has made some recommendations that would help the country get back on its feet as soon as possible after digital disruption. Important aspects in this regard are the compensation for victims and an effective reporting system for incident data.'

Broadening the cybersecurity debate

Governments have always protected the infrastructures that are crucial to keep society running. Prins: 'The advent of digitalisation however has made these infrastructures and countless other processes vulnerable in another sense. Growing digitalisation means that a response to disruption along traditional pathways and using familiar powers and instruments will no longer suffice. That's why we need to broaden the cybersecurity debate, extending it from *preventing* digital disruption to actually *preparing* for such an event, with a special emphasis on measures that ensure an effective response to digital disruption.'

Prins also points out that when preparing for digital disruption we should not limit our focus to the Netherlands alone, but coordinate our measures with other countries.

domein, maar ook consequenties heeft in ziekenhuizen, het vervoer en talloze (al dan niet vitale) infrastructuren en processen", vervolgt Prins. "We kennen inmiddels allemaal de voorbeelden: bij *WannaCry* viel een deel van de Britse gezondheidszorg uit. *NotPetya* legde de productie van belangrijke medicijnen plat en kostte één van de grootste containerrederijen ter wereld honderden miljoen euro's."

Interne wisselwerking

Gelukkig is er in de crisis- en rampenbestrijding steeds meer aandacht voor de intense wisselwerking tussen de digitale en de fysieke wereld. Prins: "Neem bijvoorbeeld de Nationale Veiligheidsstrategie 2019. Ook het Cybersecuritybeeld Nederland 2019 maakt expliciet duidelijk dat een ontwrichting van de samenleving als gevolg van digitale aanvallen op de loer ligt." De boodschap van beide documenten is duidelijk: in de digitale samenleving veranderen de risico's en moeten we nieuwe maatregelen nemen om bij ontwrichting adequaat te handelen en schade te kunnen beperken.

Maar om welke maatregelen gaat het dan precies? Prins legt uit: "Voor de omgang met welbekende rampen en vormen van ontwrichting, zoals overstromingen, epidemieën of grote branden, bestaat een professionele crisisorganisatie met een solide basis in wet- en regelgeving. Het is echter veel minder duidelijk wat we moeten en kunnen doen wanneer onze samenleving wordt getroffen door een ontwrichting die het gevolg is van een digitaal incident."

Het WRR-rapport over digitale ontwrichting dat in september aan secretaris-generaal Siebe Riedstra is overhandigd, levert volgens Prins in dit opzicht belangrijke input. "Het rapport gaat in op vragen als: wie moet het voortouw bij een digitale ontwrichting nemen, wat is er nodig in termen van institutionele (re)organisatie, nieuwe bevoegdheden en middelen? En hoe regelen we de voorbereiding op digitale ontwrichting over de landsgrenzen heen? Ook besteedt de WRR aandacht aan de mogelijkheden voor de wederopbouw van de digitale samenleving en het herstel van vertrouwen in digitale voorzieningen."

De WRR begint het rapport met de vraag wie de 'brandweer' is als er in de digitale wereld een spreekwoordelijke 'brand' uitbreekt en hulpdiensten moeten uitrukken. Prins: "Wie de metafoor van de klassieke brandweer doordenkt, komt voor talloze vragen te staan: is er voldoende zicht op nabijgelegen voorzieningen die in de gevarenzone kunnen komen? Welke prioriteiten zijn nodig bij het 'bluswerk' en welke bevoegdheden hebben de betrokken instanties om bij calamiteiten binnen te treden? Hebben we zicht op de consequenties als we digitale voorzieningen afschakelen om erger te voorkomen? In welke volgorde schakelen we voorzieningen weer aan, zeker als het vitale processen betreft? En hoe kan een snelle wederopbouw na de ramp het beste gefaciliteerd worden?"

Centrale normstelling en coördinatie

De WRR concludeert onder andere dat digitale ontwrichting vraagt om meer centrale normstelling en meer coördinatie door de overheid. "Natuurlijk kan een adequate voorbereiding op ontwrichtende situaties niet plaatsvinden zonder een bijdrage van private partijen", vervolgt Prins. "Zij kunnen bijvoorbeeld relevante standaarden en protocollen ontwikkelen. Vanwege hun afwijkende belangenoriëntaties kan tegelijkertijd niet worden verwacht dat private partijen de volledige verantwoordelijkheid voor digitale ontwrichting op zich nemen. Die verantwoordelijkheid komt bij uitstek de

"Het debat over cybersecurity dient verbreed te worden van het voorkomen van digitale ontwrichting naar ook de voorbereiding daarop"

'We need to broaden the cybersecurity debate, extending it from preventing digital disruption to preparing for such an event'

overheid toe, net zoals bij andere vormen van maatschappelijke ontwrichting het geval is. Het instrumentarium waarmee de overheid deze verantwoordelijkheid invulling kan geven, is momenteel echter zeer beperkt. Zo heeft de Nederlandse overheid relatief weinig middelen en bevoegdheden als private organisaties en bedrijven bij een dreigende of daadwerkelijke ontwrichting hun medewerking weigeren. De rijksoverheid, gemeenten en andere publieke instanties staan kortom met lege handen als ze bedrijven daartoe alsnog willen dwingen. Voor de Europese Unie geldt dit in nog grotere mate, omdat zij zich beperkt tot een adviserende rol en de strategische en operationele aspecten van cyber overlaat aan de lidstaten. Door op het niveau van de rijksoverheid zowel bevoegdheid als normstelling te verhelderen en te verstevigen, wordt een kader geboden voor stevigere coördinatie en – indien aan de orde - opschaling naar een hoger bestuurlijk niveau. Tegelijkertijd ontstaat er ruimte om de concretisering en uitvoering in specifieke contexten ter hand te nemen. De concrete maatregelen die in het domein van de zorg genomen moeten worden, zullen immers verschillen van die in de watervoorziening."

Adviezen en aanbevelingen WRR

Kortom, het advies van de WRR is dat ook bij een digitale ontwrichting het uitgangspunt moet zijn dat de 'lokale brandweer' lokale 'branden' blust en dat gespecialiseerde 'brandweerkorpsen' de meer complexe 'branden' voor hun rekening nemen. Prins: "De nadere concretisering beleggen op het niveau van de specifieke context dient uiteindelijk ook het belang van de betrokken partijen zelf, omdat het hen meer zekerheid biedt bij de voorbereiding en aanpak van een digitale ontwrichting."

De bepleite algemene opdracht aan de overheid concretiseert de WRR vervolgens aan de hand van vier welbekende fasen van de voorbereiding op ontwrichting: paraatheid, signalering, bestrijding en wederopbouw. "Met het oog op deze fasen ziet één van de aanbevelingen die de WRR doet op het verkrijgen van meer zicht op afhankelijkheden: van welke partijen, digitale elementen, processen en diensten het functioneren van vitale processen is de Nederlandse samenleving afhankelijk?", vat Prins samen. "Verder adviseert de WRR om tot een alternatieve benadering en invulling van vitale infrastructuur te komen. Ook moet overwogen worden om de prioritering van vitale processen aan te passen. Tenslotte doet de WRR enkele aanbevelingen om zo snel als mogelijk na een digitale ontwrichting weer 'op te krabbelen'. Belangrijk bij dat laatste zijn de compensatie van slachtoffers en een effectief meldingssysteem van incidentendata."

Debat cybersecurity verbreden

Sinds jaar en dag beschermen overheden de infrastructuren die belangrijk zijn voor de continuïteit van onze samenleving. Prins: "Met de komst van digitalisering zijn deze infrastructuren en talloze andere processen op een andere manier kwetsbaar geworden. Met de groeiende digitalisering is ook de aanpak van een ontwrichting langs de klassieke lijnen en met de vertrouwde instrumenten en bevoegdheden niet langer voldoende. Het debat over cybersecurity dient dan ook verbreed te worden van het voorkomen van digitale ontwrichting naar ook de voorbereiding daarop, met bijzondere aandacht voor maatregelen die een effectieve aanpak van digitale ontwrichting waarborgen."

De voorbereiding op digitale ontwrichting dient volgens Prins zowel in ons eigen land plaats te vinden als in afstemming met andere landen. "Wie zich voorbereidt op een digitale ontwrichting kan reeds vooraf maatregelen nemen om de gevolgen van deze gebeurtenis zoveel als mogelijk te beperken en zo snel als mogelijk weer op te krabbelen. Niet alleen de individuele belangen van overheden, bedrijven en burgers staan op het spel, maar ook het vertrouwen dat zij hebben in onze digitaliserende economie en samenleving", sluit Prins af.

BACK TO TOP

"Met de groeiende digitalisering is de aanpak van een ontwrichting langs de klassieke lijnen en met de vertrouwde instrumenten en bevoegdheden niet langer voldoende"

'Growing digitalisation means that a response to disruption along traditional pathways and using familiar powers and instruments will no longer suffice'

'Preparing for digital disruption allows us to take measures in advance to limit the consequences of the event and recover as quickly as possible. What is at risk is not just the individual interests of governments, companies and citizens but also, crucially, their trust in our digitalising economy and society,' Prince concludes.

De Algemene Rekenkamer controleert of de Rijksoverheid zijn werk op een rechtmatige en doelmatige manier uitvoert. Daartoe doet het onafhankelijk onderzoek, waarna het openbaar rapporteert aan het parlement. President Arno Visser: “De belastingbetaler moet waar krijgen voor zijn geld. Dat gaat verder dan louter euro’s en cijfers, maar ook bijvoorbeeld over thema’s als cybersecurity. Daar valt nog veel in te verbeteren, op alle niveaus.”

The Netherlands Court of Audit checks to ensure the Dutch government is carrying out its duties in a lawful and effective manner. To that end, it conducts independent investigations, the results of which are presented to parliament in public reports. President Arno Visser: ‘Taxpayers deserve to receive value for their money. That means more than just euros and figures – it extends to themes such as cybersecurity as well. There’s a great deal of room for improvement there, at every level.’

Arno Visser
President of the Netherlands Court of Audit

CYBERSECURITY IS A MATTER FOR THE TOP BRASS

Digitale veiligheid al jaren hoog op de agenda
De Algemene Rekenkamer is de onafhankelijke externe controleur van rijksoverheid wiens positie in de grondwet is vastgelegd. Het is de enige organisatie van buitenaf die overal bij mag om onderzoek te doen. In combinatie met een brede taakopvatting resulteert dat in een organisatie met veel interesse in digitale veiligheid. Visser: “Wij maken onze eigen agenda, waarbij we rekening houden met maatschappelijke ontwikkelingen. Digitale veiligheid staat niet alleen anno 2019, maar de afgelopen vijftien jaar al heel hoog op onze agenda.”

Digital security has been a top priority for years
The Netherlands Court of Audit is the independent external controller whose role is set out in the country's constitution. It is the only external organisation entitled to unlimited access for the purpose of its investigations. This, combined with a broad interpretation of its remit, yields an organisation with an intense interest in digital security. Visser: ‘We draw up our own agenda, in which we take societal developments into account. Digital security has pride of place on our 2019 agenda, but it has in fact been among our top priorities for years.’

Visser explains that there has been some development within the theme of digital security. ‘We began conducting our investigations fifteen years ago. We found that many people who were operating the Dutch government's IT systems were either unqualified or lacking in the necessary expertise. There are still vast improvements to be made there. We then began examining the critical national infrastructure processes in all departments, at which point we discovered all manner of problems. Recently, we launched a series of special investigations aimed specifically at the vital sectors. Last year, for instance, we published the results of an investigation into the cybersecurity of our water management structures.’

The human factor
Visser asserts that there is more to cybersecurity than technology alone. ‘The human factor is vital to achieving effective cybersecurity. There are three levels here. First of all, organisations must have enough people on staff. We see that the government is frequently understaffed, as a result of which some executive services depend on external parties for 50% or more of their personnel needs. Next, the people you have hired must also be properly qualified for their jobs. They need to have mastered yesterday's technology, of course, but should also – and more importantly – be ready to work with the technology of today and tomorrow. And lastly, effective

Visser geeft aan dat er binnen het thema digitale veiligheid wel sprake is van ontwikkeling. “Vijftien jaar geleden zijn we begonnen met onze onderzoeken. Toen bleek met name dat de mensen die IT-systemen bedienen bij de Rijksoverheid daar vaak ofwel niet bevoegd toe zijn, ofwel de expertise niet voor hebben. Daar is nog een wereld in te winnen. Daarna zijn we vitale systemen bij alle departementen gaan controleren, waarbij we tegen allerlei problemen aanliepen. En recent zijn we begonnen met bijzondere onderzoeken, specifiek in vitale sectoren. Afgelopen jaar hebben we bijvoorbeeld een onderzoek gepubliceerd over de cyberveiligheid bij onze waterschapswerken.”

De menselijke factor
Bij cyberveiligheid gaat het volgens Visser niet alleen om technologie: “Voor een goede cyberveiligheid is de menselijke factor cruciaal. Dat speelt op drie niveaus. Ten eerste moeten organisaties voldoende mensen in dienst hebben. Vaak zie je dat de overheid te weinig personeel in dienst heeft, waardoor sommige uitvoeringsdiensten voor 50% of meer afhankelijk zijn van externen. Vervolgens moeten de mensen die je in dienst hebt ook nog eens goed gekwalificeerd zijn. Ze moeten niet alleen de technologie van gisteren in de vingers hebben, maar ook en vooral de technologie van vandaag en morgen. Ten slotte is het cruciaal dat de medewerkers ook goed gescreend zijn. Overheidsdiensten maken gebruik van informatie die beveiligd moet worden, niet iedereen zou hier zomaar toegang tot moeten kunnen hebben. Dat gaat niet alleen om privacy, maar ook staatsgeheime, economische en militaire informatie.”

“Cybersecurity zou standaard bij de ministerraad besproken moeten worden”
‘Cybersecurity should be a standard topic of discussion in the Council of Ministers’

Visser is van mening dat op ieder terrein de mens de zwakste schakel is. “Wat je vandaag doet aan cyberveiligheid is morgen al achterhaald. Je moet daarom continu oefenen en jezelf verrassen: met pentests van buitenaf, mystery guests, ethische hackers van buiten, en meer. Mijn advies is om te testen, testen en nog eens testen. Je moet je eigen systemen ter discussie durven te stellen en niet alleen op de papieren werkelijkheid vertrouwen. Cyberveiligheid krijg je nooit op 100 procent, maar daar zou je wel naar moeten streven.”

Cybersecurity blijft een ingewikkelde afweging
“Voor een land als Nederland is waterbeveiliging een interessante casus. Er komen binnen dit thema twee veiligheidsdiscussies bij elkaar”, vervolgt Visser: “Beveiliging tegen het water is iets waar we ons in Nederland al honderden jaren mee bezig houden, het is een klassiek en typisch Nederlands veiligheidsonderwerp. Dat wordt tegenwoordig gecombineerd met cyber. Hoe komen die klassieke en moderne wereld bij elkaar? Veel van onze waterstaatswerken zijn gebouwd in de jaren ‘50 tot ‘70, met de technologie en de kennis van toen. Het waren stand-alone-systemen, niet gekoppeld aan een netwerk. Tegenwoordig is er de wens om informatie van de waterstaatswerken te koppelen, zodat je niet vijf keer dezelfde informatie deelt. Maar dat betekent wel dat de risico’s toenemen: als je er bij de één in kan, kan je er ook in bij de ander. Dit is het resultaat van tegengestelde belangen: je wilt wel dat systemen aangesloten zijn, maar niet dat ze een risico vormen. Aan de ene kant willen we een overheid die optimaal dienstverlenend is, aan de andere kant willen we óók een overheid die qua veiligheid optimaal is. Dat gaat niet altijd samen. Of je dan de keuze maakt voor dienstverlening of veiligheid hangt af van het soort dienst. Dat moet je iedere keer zorgvuldig afwegen: om wat voor soort informatie en welk type veiligheid gaat het?”

Chefsache
Een van de belangrijkste adviezen van Visser is dat cybersecurity meer op de bestuurstafel moet komen te liggen. “Ik spreek vaak de top van het bedrijfsleven en ik weet dat cybersecurity daar chefsache is. Er is geen grote bank of verzekeraar die het zich kan veroorloven om geen aandacht aan dit onderwerp te geven. Dat is wel een groot verschil met de politiek. Cybersecurity zou standaard bij de ministerraad besproken moeten worden en op de tafel van de ministers moeten liggen. Zodra een minister aandacht besteedt aan het onderwerp wordt er binnen ministeries direct vooruitgang geboekt.”

“Vertrouw niet alleen op de papieren werkelijkheid, durf je eigen systemen ter discussie te stellen”
‘Rather than putting blind faith in how your systems look on paper, you must be willing to subject them to scrutiny’

Daarom vindt Visser toezicht heel belangrijk. “Of het nou gaat om toezicht binnen de organisatie zelf, raden van toezicht of echt externe toezichthouders: overal moeten mensen zitten die verstand hebben van cybersecurity. Ook bij organisaties die van oudsher niet zozeer met cybersecurity te maken hebben, bijvoorbeeld binnen het onderwijs. De Algemene Rekenkamer heeft ook niet stil gezeten, onze organisatie is ook veranderd ten opzichte van tien jaar geleden.”

Visser is geen voorstander van een nieuwe algemene toezichthouder cybersecurity; je moet volgens hem geen nieuwe instituten creëren. “Ik denk dat het verstandiger is om de minister van Binnenlandse Zaken en Koninkrijksrelaties doorzettingsmacht te geven bij overheidsorganisaties als het gaat om van cybersecurity. Vergelijk het met de minister van Financiën: die mag ingrijpen als het bij een ander ministerie niet goed gaat op het gebied van financiën. Iets soortgelijks zou moeten gebeuren bij de minister van Binnenlandse Zaken en Koninkrijksrelaties.”

Het is nooit goed genoeg
Over hoe Nederland het in zijn algemeenheid doet op het gebied van cybersecurity kan Visser echter geen uitspraken over doen. “Er zijn zo veel ICS/SCADA-systemen, er zijn zo veel PCS-systemen, zo veel organisaties. We kunnen zelfs niet zeggen of de overheid het bijvoorbeeld beter doet dan het bedrijfsleven of andersom: binnen alle sectoren zijn er organisaties die voorop lopen en andere die achter lopen. Het belangrijkste is dat je je voorneemt dat het nooit goed genoeg is: stilstand is achteruitgang.”

employee screening is vital. Government services deal with information that must be kept secure, meaning not just anyone should be able to access it. This is not only a matter of privacy, but also state secrets in the form of economic and military information.’

People, says Visser, are in fact the weakest link in any given area. ‘Whatever steps you take towards cybersecurity today are sure to be obsolete tomorrow. That's why it's vital to keep conducting drills and surprising yourself with things like pen tests from outside the organisation, mystery guests, external ethical hackers and more. My advice is to test, test and test again. You must be willing to subject your own systems to scrutiny rather than putting blind faith in how they look on paper. While there's no way to achieve 100% cybersecurity, that doesn't mean it shouldn't be our goal.’

Cybersecurity remains a complicated issue
‘One interesting case for a country like the Netherlands is the issue of water security, a theme that brings together two separate security debates,’ Visser continues. ‘We in the Netherlands have been working to protect ourselves from water-related threats for centuries: it's a traditional and typically Dutch security topic. Today, these efforts are being combined with a cyber-related aspect. The question before us is, how to best unite the traditional and modern worlds? Many of our water management structures were built in the 1950s, 60s and 70s, using the technology and knowledge available at that time. Each was a standalone system that was not linked to a larger network. Today, there's a desire to link the information from various water management structures, so we're not passing the same information back and forth half a dozen times. This does, however, entail increased risks in that, if you can gain access to one system, you'll have access to the others as well. So it's a matter of competing interests: we want the systems to be connected, but to avoid that degree of risk. On the one hand, we want a government that provides optimum service; and on the other, we also want a government that maintains an optimum level of security. These two aims are sometimes mutually exclusive. In such cases, whether you opt for service or security will depend on the type of service in question. The decision requires careful consideration each time with regard to the type of information and the type of security involved.’

Top brass
One of Visser's most important recommendations is that cybersecurity should figure more prominently on the meeting agendas of high-level executives. ‘I often meet with the top brass from the business community and I know that cybersecurity is a priority for them. It's a topic no major bank or insurance company can afford to neglect. Yet it's a quite a different matter in the political arena. Cybersecurity should be a standard topic of discussion inthe Council of Ministers and a fixed item on the ministers’ agendas. Once a minister begins to devote attention to the topic, progress within his or her ministry will immediately follow.’

Visser therefore considers supervision and oversight to be vital. ‘Whether you're talking about supervision from within the organisation itself, supervisory councils or actual external supervisory authorities, there should be people with cybersecurity-related expertise in all bodies at all levels. That includes institutions which haven't had much involvement with cybersecurity in the past, such as those in education. The Netherlands Court of Audit itself has been busy as well – our organisation is quite different today than it was a decade ago.’

Visser is not in favour of a new supervisory authority for cybersecurity, as he is keen to avoid creating new institutions. ‘I think a wiser course of action would be to grant the Minister of the Interior and Kingdom Relations additional powers on cybersecurity issues in government organisations. This would be comparable to the Minister of Finance, who is authorised to intervene when financial foibles occur at another ministry. We should adopt a similar approach for the Minister of the Interior and Kingdom Relations.’

No such thing as good enough
With regard to an ‘overall mark’ for the Netherlands in the area of cybersecurity, Visser is unable to give a verdict. ‘There are so very many ICS/SCADA systems, so many PCS systems and so many organisations. We can't even determine, for example, whether the government is performing better than the corporate sector or vice versa. In every sector, you have organisations that are leading the pack and those that are lagging behind. The most important thing is to never settle for what you have as “good enough”: to keep up, you need to keep moving forward.’

Mariya Gabriel
European Commissioner for
Digital Economy and Society

There are many potential benefits of the digital transformation - but people will need to feel safe and confident in their digital lives if they are to reap them fully. Data is fast becoming the new global 'currency'.

PROTECTING THE DATA ECONOMY

As our towns and cities become increasingly connected, the quantity of data we produce in our daily lives continues to grow: smart meters in our homes and offices provide data on energy consumption and generation; data from public and private transport can help design better roads and networks; weather and environmental data provides precious information about our interaction with the world around us. All this data is generated by the increasing number of digital services and applications, which in turn are enriched and improved by access to this additional data.

All of this is already happening, and it is only likely to increase in the years to come. This is why over the last four years, the European Commission has worked to put in place the building blocks of a truly Digital Single Market that supports the development of new technologies and applications and at the same time ensures legal certainty and the necessary protections for consumers and businesses alike. We have proposed 30 legislative proposals. Most of them have already become law and cover everything from updated telecoms and audio-visual sector rules to new legislation on the use and protection of data.

Key digital technologies and skills will also be the focus of our work going forward: for the first time ever, the Commission has proposed a dedicated funding stream for digital as part of the next EU budget period from 2021. The Digital Europe Programme will invest over €9bn in artificial intelligence, supercomputing, cybersecurity, digital skills and the modernisation and digitalisation of the public sector.

Keeping data safe

We need to provide the legal certainty that business and research needs to develop the technologies, but just as importantly, we need citizens and businesses to be confident that the data they generate is safe. The General Data Protection Regulation (GDPR) is the most high-profile measure we have taken to address this, but it is far from the only one. We now have new rules on the free-flow on non-personalised data, on cloud computing and data storage and on the re-use of public sector information and open data; and new guidelines on the ethical use of artificial intelligence are also under development.

Two key policy areas in this regard are cybersecurity and digital skills. I see these two as highly complementary and very much focused on the human aspects of the digital society and economy. We have already highlighted the potential of digital technologies and the key role that data in particular plays - but what could undermine both of these would be a lack of trust on the part of citizens. If they feel that their 'digital selves' are not safe, that their data is at risk of being stolen or manipulated, or that the right checks and balances are not in place they will undoubtedly make less use of all the potential benefits the digital development is offering.

'Cyber-attacks have increased in numbers, but also in scale and geographical spread'

Cyber-attacks have increased in numbers, but also in scale and geographical spread. It is clear that the EU needs to become more resilient to cyber-attacks and create an effective cyber deterrence. The human factor plays a very important part in this. With some 95% of incidents said to be enabled by some type of human error – intentional or not - there is a strong human factor at play. Technology can only take us so far in keeping us safe in the digital world - we all need to exercise our own responsibility as well. And this means changing the way we approach our digital lives. People - but also businesses and public administrations - need to have the skills and the right tools to be able to quickly detect and actively protect themselves against attacks.

Legislative framework in place

For its part, the EU has worked hard to ensure the safety of networks and systems and to raise awareness of the risks - and the solutions - inherent in the increasingly digital world. The Network and Information Security (NIS) Directive came into force last year and is designed to build resilience against potential cyber-threats across our entire digital society and economy by obliging operators of all relevant services to adopt effective risk management practices. We will also soon start with the implementation of the new Cybersecurity Act, in force from 27 June 2019. The Cybersecurity Act reinforces the European Cybersecurity Agency, ENISA, and creates a new EU certification framework for cybersecurity. Most recently we have proposed to set up a new European Cybersecurity Competence Centre and a Network of National Coordination Centres, to enable much closer coordination of increasing public investments in cybersecurity technology and tools.

Tackling the human factor

However, investments in technology are only half of the equation. Effective cybersecurity also critically relies on the skills of the people concerned. This is why we need to develop cybersecurity education at all levels, starting from regular training of a cyber workforce and cybersecurity training for all ICT specialists. Yet it is important that cybersecurity education is not limited to IT professionals - it needs to be a key part of every area, from engineering to business management or law. And of course, the earlier we start to learn about cybersecurity, the better: more than 20% of 12-18 year olds in Europe hardly ever use computers at school and only one in six of this same age group attend schools with high speed internet connection. We need to help young people acquire the digital skills they need by making sure their schools and teachers are equipped and qualified and their schools have access to high quality internet.

According to the latest data from the Digital Economy and Society Index, a 'digital scoreboard' for the EU managed by the European Commission, more than one third of those in the active labour force do not have basic digital skills, even though most jobs require at least this basic level of knowledge. The Netherlands is one of the best performing EU countries in terms of overall digital transformation, but even so more than 20% of Dutch people do not have these basic digital skills. At the same time, there is increasing demand for advanced digital skills - including cybersecurity skills - across the economy; yet some 53% of European companies recruiting or trying to recruit digital technology experts have difficulties in doing so. This is a particular problem for the Netherlands, where that share is even higher at 69%. This figure is corroborated by the high demand of Dutch companies to welcome European trainees as part of the Commission's Digital traineeship opportunity, where the Netherlands attracted more trainees than France or Italy.

The Commission also helps to raise awareness about local and national projects or initiatives that can help people get the right skills, such as Make IT Work, a Dutch project which trains non-IT university graduates for new careers in IT. The project reflects the wider aims of the Dutch government to prioritise improving cybersecurity, the digitisation of public services and digital skills during its time in office - a key understanding that reaping the benefits of the Digital Single Market will need the right combination of trust and understanding to fully come to fruition.

BACK TO TOP

‘More than one third of those in the active labour force do not have basic digital skills’

Saskia Bruines
Alderman for Education, Knowledge Economy and International Affairs for the Municipality of The Hague

Saskia Bruines is sinds februari 2017 wethouder Onderwijs, Kenniseconomie en Internationaal van de gemeente Den Haag. Onder haar leiding zet de hofstad ambitieuze stappen als smart city. Net als andere grote steden staat Den Haag voor een aantal grote uitdagingen. Er komen elk jaar duizenden inwoners bij terwijl de stad wel bereikbaar en leefbaar moet blijven. Het stadsbestuur wil daar met digitalisering en innovatie slim mee omgaan. Zo blijft Den Haag een aantrekkelijke stad om in te wonen en werken. Wat betekent zo'n digitale samenleving voor de stad en de inwoners? We vragen het aan de Haagse wethouder.

Saskia Bruines has served as Alderman for Education, Knowledge Economy and International Affairs for the Municipality of The Hague since February 2017. Under her leadership, the royal residence has realised ambitious strides towards becoming a smart city. Like other large cities, The Hague faces several major challenges. Its population is increasing by several thousand each year while the city strives to retain its standards of accessibility and liveability. The municipal government hopes to smartly manage this development through digitalisation and innovation, ensuring that The Hague will remain an attractive city in which to live and work. But what will such a digital society mean for the city and its inhabitants? We asked alderman Bruines to share her perspective.

“WE ZETTEN DIGITALISERING EN INNOVATIE IN OM HET LEVEN VAN DE MENSEN IN DE STAD TE VERBETEREN”

‘WE ARE MAKING USE OF DIGITALISATION AND INNOVATION IN ORDER TO IMPROVE THE LIVES OF PEOPLE IN THE CITY’

THE HAGUE’S AMBITIONS AS A SMART CITY

In November 2018, The Hague won the international Smart City Award. 'In a smart city, digitalisation and innovation are utilised to improve the lives of the people who live there,' Bruines explains. 'Such efforts should focus on the inhabitants rather than the technology. Technology does, of course, have a big part to play in addressing urban issues. It is especially important in The Hague, as we expect to see significant growth in the years ahead.' The Municipality of The Hague won another award for its project ‘Living at home for longer, in good health' (*Gezond Lang Thuis*). Bruines: 'In this project, the city cooperated with businesses and elderly residents of The Hague to develop care-related home automation, i.e. domotics. Domotic solutions include not only care robots and fall sensors, but robot pets that provide companionship. Such technologies enable elderly individuals to extend the period in which they can continue living independently at home. According to the Smart City Awards jury, this is a unique project that is in keeping with the concept of a smart city'.

Digital skills

While digitalisation is changing the fabric of society, Bruines agrees it is important not to lose sight of the human aspect. 'Everyone must be in a position to benefit from the digital society, which will require new skills. To that end, lifelong learning is the new motto. That begins in schools, of course, with the implementation of digitalisation in education, but it obviously applies to all age groups.'

In november 2018 heeft Den Haag de international Smart City Award gewonnen. “In een smart city worden digitalisering en innovatie ingezet om het leven van de mensen in de stad beter te maken”, legt Bruines uit. “De inwoner staat daarbij centraal en niet de techniek. Technologie speelt een grote rol bij de aanpak van stedelijke vraagstukken. Vooral in Den Haag is dit van groot belang, want de komende jaren gaan we flink groeien.” De gemeente Den Haag heeft ook een prijs gewonnen met het project ‘Gezond Lang Thuis’. “Daarin is samen met bedrijven én Haagse ouderen zorgdomotica ontwikkeld. Denk aan zorgrobots, valsensoren, maar ook aan robothuisdieren die als gezelschap dienen. Dankzij dit soort technologie kunnen ouderen langer zelfstandig thuis wonen. Volgens de jury van de Smart City Awards is dit een uniek project dat past bij een smart city”, vervolgt Bruines.

Digitale vaardigheden
Digitalisering verandert de samenleving en het menselijke aspect mag daarbij niet uit het oog verloren worden, vindt ook Bruines. “Iedereen moet kunnen profiteren van de digitale maatschappij en daar zijn nieuwe vaardigheden voor nodig. Een leven lang leren is het nieuwe adagium. Dat begint natuurlijk op school door toepassing van digitalisering in het onderwijs, maar geldt natuurlijk voor alle leeftijdsgroepen.” Daarom organiseert de gemeente hiertoe cursussen en wordt de eigen dienstverlening toegankelijker gemaakt. Digitale inclusie is volgens Bruines een gezamenlijke opgave voor het Rijk, gemeenten, het bedrijfsleven en het onderwijs. “Betere samenwerking en afstemming is noodzakelijk en kan leiden tot mooie initiatieven met extra maatschappelijke impact. Zo voeren Haagse hbo- en mbo-studenten cybersecurity-onderzoek in de praktijk uit door concreet advies te geven aan bedrijven. Zo helpen ze mee om de digitale weerbaarheid van de lokale mkb-bedrijven te verhogen.”

Living Labs
Om nieuwe slimme oplossingen op kleinere schaal ‘in het echt’ te kunnen beproeven, organiseert de gemeente samen met bedrijven, inwoners en de overheid zogeheten Living Labs, zoals de ervaarwoning van het ‘Gezond Lang Thuis’. “Daarnaast komen er ook proefomgevingen in de openbare ruimte op straat”, vertelt Bruines. “Na deze zomer openen we bijvoorbeeld het Living Lab Scheveningen. Samen met inwoners, lokale ondernemers en het bedrijfsleven is in kaart gebracht welke slimme toepassingen we in dit gebied kunnen uitproberen. Het voordeel van de opzet van een Living Lab is dat je toepassingen op gecontroleerde wijze met bewoners kunt testen. Een geslaagde toepassing is dan eenvoudiger uit te rollen over de rest van de stad.”

Op deze wijze werkt de gemeente onder meer samen met provincie Zuid-Holland en TU Delft aan het ontwikkelen van ‘use cases’ voor dit gebied. “Met dynamisch parkeerbeheer willen we bijvoorbeeld zorgen voor een goede doorstroming”, vervolgt Bruines. “Een ander voorbeeld is het sturen van bezoekersstromen met licht en geluid tijdens grote evenementen. Vanzelfsprekend houden we daarbij rekening met de ethische en wettelijke aspecten van deze nieuwe technologie, zoals het beschermen van privacy en transparantie.”

Kennisdeling
Op de vraag aan Bruines of de kennis en ervaring uit alle projecten ook gedeeld wordt met andere steden is zij stellig. “Jazeker delen wij onze kennis. Samen met Amsterdam, Rotterdam, Utrecht en Eindhoven hebben een gezamenlijke smart city-agenda opgesteld. Elke stad is trekker van een onderwerp dat het beste bij deze gemeente past. Rotterdam trekt Sustainability, Eindhoven Smart Mobility. Healthy Urban Living hoort bij Utrecht en Amsterdam staat aan de lat voor Circularity. Als stad van Vrede en Recht is Den Haag trekker van het thema Safety & Security, zoals fysieke veiligheid, maar ook cybersecurity. Elke stad zoekt naar mooie voorbeeldprojecten in het land en we leren van elkaars ervaringen. Dit is een unieke samenwerking.” Deze samenwerking zorgt er volgens Bruines ook voor dat Nederland er internationaal goed op staat. “Ook op regionale schaal en landelijk organiseren we het delen van kennis steeds beter. Tijdens de conferentie Nederland Digitaal in maart 2019 hebben ruim honderd organisaties, bedrijven en gemeenten een gezamenlijke verklaring over Smart Society onderschreven. Daarmee hebben zij allen uitgesproken samen te werken aan een digitaal Nederland.”

Vrede, recht en veiligheid
We worden steeds afhankelijker van digitale middelen en dat zet de digitale weerbaarheid van onze samenleving onder druk en zeker ook van organisaties en bedrijven. Incidenten kunnen immers een grote impact hebben op de samenleving. Als stad van vrede, recht en veiligheid wil de gemeente Den Haag haar eigen digitale omgeving goed beschermen en een voortrekkersrol vervullen. Een mooi voorbeeld vindt Bruines de jaarlijkse hackwedstrijd van de gemeente. “Ethische hackers krijgen dan de mogelijkheden om beveiligingslekken in de gemeentelijke systemen te ontdekken. Zo testen we niet alleen onze systemen, maar laten we ook zien hoe belangrijk digitale veiligheid is voor organisaties. Dit jaar vond alweer de derde editie plaats in de centrale hal van het stadhuis.” Ook zoekt de gemeente actief de samenwerking op met publieke en private partners. Door de aanwezigheid van toonaangevende organisaties in Den Haag, zoals Europol, NATO Communications & Information Agency (NCIA), verschillende cybersecurity-onderdelen van de Rijksoverheid, TNO en de TU Delft, is er veel kennis aanwezig en wordt steeds meer

“Technologie speelt een grote rol bij de aanpak van stedelijke vraagstukken”

‘Technology has a big part to play in addressing urban issues’

And that is why municipal authorities are organising classes and taking steps to make their own services more accessible. Bruines views digital inclusiveness as a joint task for the Dutch national and municipal governments, the business community and the education sector. 'More effective cooperation and coordination is needed and can lead to exciting initiatives with added societal impact. For example, students from universities of applied sciences and secondary vocational education in The Hague are conducting cybersecurity research in practice by providing businesses with specific recommendations. In this way, they are helping to increase the digital resilience of local SMEs.'

Living Labs
In order to test new smart solutions ‘in real life’ but at a smaller scale, the city is teaming up with businesses, residents and the government in what are known as Living Labs, such as the test residence of the *Gezond Lang Thuis* project. 'Test environments will also be set up in public spaces, on the street,' says Bruines. 'After the summer, for instance, we'll open a new Living Lab in Scheveningen. We've joined forces with residents, local entrepreneurs and the business community to identify smart applications that can be tried out in this region. The advantage of the Living Lab format is that it allows you to test applications with residents in a controlled fashion. This makes it easier to then roll out a successful application across the rest of the city as well.'

The city cooperates in this way with partners including the Province of South Holland and Delft University of Technology (TU Delft) to develop ‘use cases’ specifically for this region. Bruines: 'We aim, for instance, to use dynamic parking management to ensure proper flow. Another example is using light and sound signals to guide visitor flows during large-scale events. With due regard, of course, for the ethical and legal aspects of these new technologies, such as the interests of privacy protection and transparency.'

Knowledge exchange
When asked whether the knowledge and experience gained in all these projects is to be shared with other cities, Bruines is clear. 'We will absolutely be sharing what we learn. In fact, we have drafted a joint smart city agenda together with Amsterdam, Rotterdam, Utrecht and Eindhoven. Each city will lead the way for the topic that best fits that particular municipality. Rotterdam, for instance, has been tasked with Sustainability, while Eindhoven will tackle Smart Mobility. Healthy Urban Living will be Utrecht's purview and Amsterdam will be in charge of Circularity. As the city of peace and justice, The Hague has been tasked with the theme of Safety & Security – which includes both physical security and cybersecurity. Each city also looks for good examples of projects nationwide, and we learn from one another's experiences. This collaboration is unique.' According to Bruines, the collaboration on this matter also helps promote the international reputation of the Netherlands. 'We are getting better and better at organising knowledge exchange also at the regional and national levels. During the Nederland Digitaal conference in March 2019, over one hundred organisations, businesses and municipalities signed a joint declaration on the Smart Society. By doing so, they all expressed a desire to work towards optimising digitalisation in the Netherlands.'

Peace, justice and security
As we become increasingly dependent on digital tools, the pressure on the digital resilience of society – and of organisations and businesses – is likewise increasing. After all, incidents can drastically impact our society. As the city of peace, justice and security, The Hague endeavours to protect its digital environment and play a leading role in this area. Bruines sees a good example of this in the annual hacking competition hosted by the city. 'During this event, ethical hackers are given a chance to look for vulnerabilities in the municipal systems. This enables us to not only test our systems, but to demonstrate how vital digital

samengewerkt aan nieuwe cybersecurity-oplossingen. “Dit heeft onder andere geleid tot de ontwikkeling van The Hague Security Delta”, vervolgt Bruines. “Inmiddels zijn meer dan 250 bedrijven, overheden en kennisinstellingen hierbij aangesloten om samen te werken aan innovaties voor een veilige wereld.”

Ook de bewustwording van de eigen medewerkers voor cybersecurityrisico’s is voor Den Haag een belangrijke pijler. “De ambtelijke top heeft bijvoorbeeld een cybersecurity-crisis nagebootst. En voor medewerkers hebben we het bewustwordingsspel ‘Gegevensweg?!’ geïntroduceerd. Daarmee leren de ambtenaren spelenderwijs persoonsgegevens beter te beschermen. Zo is de noodzakelijke kennis op alle niveaus aanwezig.”

Onderwijs

De Haagse Smart City Strategie staat in nauwe verbinding met de Educatieve Agenda 2018 – 2022 ‘Ontwikkel kansen in Den Haag’. Hierin hebben onderwijspartners en de gemeente een toekomstperspectief benoemd, waarbij de wederkerige relatie tussen het onderwijs en de sociale en economische ontwikkeling van de stad centraal staat. Dit is volgens Bruines een relatie die de laatste en de komende decennia steeds sterker wordt bepaald en/of gefaciliteerd door ICT. “Dat betekent dat het onderwijs een taak heeft om ervoor te zorgen dat de (toekomstige) beroepsbevolking digitaal geletterd is. Dit begint bij het zorgdragen voor digitaal geletterde docenten die via een vernieuwd curriculum gaan zorgen voor digitaal geletterde leerlingen.” Bruines vindt dat hier haast bij is geboden. “De digitale ontwikkelingen gaan razendsnel en de impact op het dagelijks leven is enorm. Toepassing van kunstmatige intelligentie, big data en robotica versnellen dit proces. De jeugd moet hier goed op worden voorbereid; zij zijn onze toekomst en moeten klaar zijn voor de arbeidsmarkt van morgen. Daarom is het zo belangrijk dat we de jeugd nu al alle benodigde skills bijbrengen. Van programmeren tot bewust en veilig gebruik van digitale middelen.” Bruines benadrukt dat er al veel gebeurt op dit vlak, maar het kan en moet sneller. Het lerarentekort in het primair - en voortgezet onderwijs dwingt ons volgens haar tot te kijken naar andere oplossingen. “Het onderwijs moet ‘anders’ georganiseerd worden en de digitalisering van het onderwijs kán daarin een grote rol spelen. Ook hier kan samenwerking met het bedrijfsleven en kennisinstellingen een meerwaarde hebben.” (Noot van de redactie: De gemeente Den Haag en de CSR gaan samen verkennen wat de mogelijkheden zijn om de inhoud van de leerlijn digitale geletterdheid uit het nieuwe curriculum te vertalen naar bijscholingsprogramma’s voor docenten in het primair - en voortgezet onderwijs in de vorm van een pilot in de gemeente Den Haag.)

“Het onderwijs heeft een taak heeft om ervoor te zorgen dat de (toekomstige) beroepsbevolking digitaal geletterd is”

‘The educational system has a duty to ensure the digital literacy of the current and future working population’

security is to organisations. This year's edition, the third, was held in the central atrium of city hall.' The city also actively pursues cooperation with public and private partners. Because leading organisations – such as Europol, the NATO Communications & Information Agency (NCIA), various cybersecurity units of the Dutch government, TNO and TU Delft – are located in The Hague, there is a wealth of knowledge present and cooperation aimed at finding new cybersecurity solutions is increasing. 'One of the fruits of this process is the development of The Hague Security Delta,' Bruines goes on. 'Over 250 businesses, government bodies and knowledge institutions are currently affiliated with the Delta for the purpose of collaborating on innovations for a secure world.'

Another important theme for The Hague is raising awareness with regard to cybersecurity risks among its own employees. 'Senior administrators, for instance, took part in a simulated cybersecurity crisis. And for employees, we introduced an awareness-raising game called *Gegevensweg?!*, which translates as Runaway data?! and offers a fun way to teach civil servants to protect their personal data. That ensures the necessary knowledge is present at every level.'

Education

The Hague Smart City Strategy is closely tied to the 2018-2022 Educational Agenda, ‘Development opportunities in The Hague’. In this document, the city and its educational partners have outlined a vision for the future that centres on the interaction between education and the social and economic development of the city. Bruines explains that this relationship has, in recent decades (and will in future decades), become increasingly defined and/or facilitated by ICT. 'In other words, the educational system has a duty to ensure the digital literacy of the current and future working population. The first step is to ensure digitally literate teachers and lecturers who will create digitally literate pupils and students via an updated curriculum.' And if you ask Bruines, this can't come a moment too soon. 'Digital developments are progressing at lightning speed and their impact on our day-to-day lives is enormous. The application of artificial intelligence, Big Data and robotics serves to accelerate this process. It's crucial that we properly prepare young people for this reality: they are our future and must be ready to enter tomorrow's labour market. That is why it's so important that we teach young people the necessary skills, running the gamut from programming to how to use digital tools prudently and securely, and that we start today.' Bruines emphasises that while a great deal is already being done in this area, these efforts can and must be speeded up. The shortage of teachers in primary and secondary education means we are obliged to consider other solutions. 'Our education system is in need of reorganisation, and the digitalisation of education could play a major part in those efforts. Here, too, cooperation with the business community and knowledge institutions can offer added value.' (Editor's note: In a pilot to be conducted in The Hague, the Municipality of The Hague and the Cyber Security Council will explore options for applying the content of the new curriculum's digital literacy learning track in continued education programmes for primary and secondary school teachers.)

BACK TO TOP

FOCCO VIJSELAAR

Nieuw lid van de Cyber Security Raad (CSR)

New member of the Dutch Cyber Security Council (CSR)

Sinds november 2018 is Focco Vijselaar is Directeur-Generaal Bedrijfsleven en Innovatie bij het ministerie van Economische Zaken en Klimaat. In deze functie is hij onder andere (mede)verantwoordelijk voor het digitaliseringsbeleid en de transitie naar een duurzame en digitale economie. Namens het ministerie van EZK is hij sinds november 2018 lid van de CSR.

Focco Vijselaar has been Director-General for Enterprise and Innovation at the Ministry of Economic Affairs and Climate Policy since November 2018. In this capacity, he bears joint responsibility for digitalisation policy in the Netherlands and the country's transition to a sustainable and digital economy. He has been a member of the Cyber Security Council on behalf of the Ministry of Economic Affairs and Climate Policy since November 2018.

Wat is voor u het belang van de CSR?
"Een goed ondernemersklimaat en een innovatieve economie vragen om een veilige digitale omgeving. Die maken we met een gezamenlijke aanpak van ondernemers, onderzoekers, maatschappelijke - en overheidsorganisaties. De raad brengt daarbij verschillende partijen én perspectieven op strategisch niveau samen. Nederland moet een veilige, open en welvarende samenleving zijn en blijven. De ontwikkelingen in het digitale domein bieden veel economische en maatschappelijke kansen die alleen kunnen worden verzilverd als Nederland digitaal veilig is."

Welke rol speelt 'cyber' voor het ministerie van Economische Zaken en Klimaat?
"Cybersecurity is een belangrijke randvoorwaarde voor het vertrouwen van bedrijven en consumenten in de digitalisering van onze economie. Een veilige digitale samenleving is dan ook één van de pijlers van de Nederlandse Digitaliseringstrategie. Meer specifiek zet EZK in op het versterken van de weerbaarheid van het midden- en kleinbedrijf en consumenten, het stimuleren van kennisontwikkeling en innovatie, het borgen van een betrouwbare en efficiënte telecominfrastructuur en het verhogen van het digitale veiligheidsniveau van hard- en software en het Internet of Things. Dit is een divers pallet aan vraagstukken die je alleen samen met partners aan kan pakken. Partners die - als gezegd - samen komen in de CSR."

Why do you consider the CSR to be important?
'A good business climate and an innovative economy require a secure digital environment. We can create that environment through a joint approach by business owners, researchers, social organisations and government bodies. To that end, the council brings together a range of different parties and perspectives at a strategic level. The Netherlands should be and remain a secure, open and prosperous society. Developments in the digital domain offer many economic and social opportunities which can only come to fruition if the Netherlands maintains cybersecurity.'

How does the Ministry of Economic Affairs and Climate Policy view the role of cybersecurity?
'Cybersecurity is a vital precondition for businesses' and consumers' confidence in the digitalisation of our economy. As such, a secure digital society is one of the pillars of the Dutch Digitalisation Strategy. More specifically, the Ministry is investing in efforts to strengthen the resilience of small and medium-sized businesses and consumers, to promote knowledge development and innovation, to ensure a reliable and efficient telecom infrastructure and to enhance the digital security of hardware, software and the Internet of Things. This is a diverse array of issues that can only be tackled in conjunction with partners. Partners who – as I said – all come together in the CSR.'

Mr. Alida Oppers
Director-General for Primary and Secondary Education at the Ministry of Education, Culture and Science
Focco Vijselaar MA
Director-General for Enterprise and Innovation at the Ministry of Economic Affairs and Climate Policy and member of the Cyber Security Council

THE BUSINESS AND EDUCATIONAL COMMUNITIES MUST JOIN FORCES TO ACHIEVE A SECURE DIGITAL NETHERLANDS

De ontwikkelingen in het digitale domein bieden veel economische en maatschappelijke kansen die alleen kunnen worden verzilverd als Nederland digitaal veilig is. Nederland heeft een goede uitgangspositie om de economische kansen van de digitale toekomst voluit te benutten en innovatie te bevorderen. De randvoorwaarden voor economisch succes moeten dan wel goed worden geborgd. Dit begint bij digitale vaardigheden én weerbaarheid vinden Alida Oppers, Directeur-Generaal Primair en Voortgezet Onderwijs bij het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en Focco Vijselaar, Directeur-Generaal Bedrijfsleven en Innovatie bij het ministerie van Economische Zaken en Klimaat (EZK). Daartoe moeten het bedrijfsleven en onderwijs de handen ineenslaan.

Developments in the digital domain offer many economic and social opportunities which can only come to fruition if the Netherlands maintains cybersecurity. The country is well-situated to exploit the economic opportunities of the digital future to the full and encourage innovation. In order to do so, however, the conditions for economic success must be effectively enforced. The starting point in such efforts must encompass both digital skills and resilience, according to Alida Oppers, Director-General for Primary and Secondary Education at the Ministry of Education, Culture and Science, and Focco Vijselaar, Director-General for Enterprise and Innovation at the Ministry of Economic Affairs and Climate Policy. To that end, it is vital that the business and educational communities join forces.

Overal in Europa is het besef doorgedrongen dat digitalisering essentieel is voor de economie van morgen. “Ook Nederland is wakker”, concludeert Vijselaar. “Vorig jaar heeft het kabinet daarom de Nederlandse Digitaliseringsstrategie gepresenteerd. Daarin hebben we twee belangrijke randvoorwaarden expliciet genoemd: digitale vaardigheden én weerbaarheid. Omdat het ontwikkelen van digitale vaardigheden voor een groot deel in het onderwijs begint, hebben we de samenwerking opgezocht met het ministerie van OCW en kijken we ook naar hoe het bedrijfsleven hieraan een bijdrage kan leveren.”

Onderwijscurriculum

Vanuit het ministerie van OCW zijn teams van leraren en schoolleiders bezig om het onderwijscurriculum te herzien voor het basis- en voortgezet onderwijs. Naar verwachting is dit curriculum in 2022 beschikbaar. “Digitale geletterdheid is hierin één van de negen leergebieden”, vertelt Oppers. “Om goed mee te kunnen doen in de samenleving zijn ict-basisvaardigheden noodzaak, maar ook informatievaardigheden, mediawijsheid en computational thinking. Deze kennis en vaardigheden krijgen straks een vaste plek in het onderwijscurriculum.” Scholen krijgen de tijd om het nieuwe curriculum in te voeren, maar kunnen er nu al voor kiezen om aan de slag te gaan met digitale geletterdheid. Oppers: “Veel scholen doen dat al. Zo heeft een Gronings schoolbestuur een eigen leerlijn digitale geletterdheid ontwikkeld. De scholen die er mee bezig zijn, lopen nu tegen verschillende vraagstukken aan, bijvoorbeeld ‘Welke vaardigheden hebben docenten nodig?’ en ‘Welke leermiddelen passen bij de onderwijskundige visie?’.” Om het onderwijs te helpen met deze vraagstukken hebben de ministeries van EZK en OCW samen met de PO-Raad, VO-raad en Kennisnet de handen ineengeslagen. Vijselaar: “Samen zijn we het Doorbraakproject Onderwijs & ICT gestart. Dat heeft ertoe geleid dat inmiddels bijna 100 schoolbesturen uit heel Nederland lid zijn van de coöperatie SIVON. De coöperatie draagt zorg voor een veilige en betaalbare internetvoorziening voor het onderwijs.”
Oppers vult aan: “Deze samenwerking zetten we nu door met de digitaliseringsagenda voor het funderend onderwijs, dat onderdeel is van de Nederlandse Digitaliseringsstrategie. Digitalisering heeft grote invloed op het hele onderwijs, niet alleen op de kennis en vaardigheden van leerlingen, maar ook op hoe leraren lesgeven en hoe scholen zichzelf organiseren.”

Digitale weerbaarheid

De digitale weerbaarheid van Nederland kan volgens Oppers en Vijselaar vergroot worden door een goede basis in het onderwijs te leggen. “Als het gaat om cybersecurity mogen we de menselijke factor niet onderschatten”, stelt Vijselaar. “Vergelijk het met de veiligheid van een huis. Je kunt met allerlei maatregelen een huis veilig maken, maar geen beveiliging is geschikt voor iemand die het huis verlaat en de deur open laat staan. Zo gaat het ook met digitale veiligheid. Daarom ben ik blij dat digitale veiligheid en privacy onderdeel uitmaken van de voorstellen van de curriculumherziening. Daarmee is het nog niet af, de leraar moet dit straks in de praktijk een plek geven.”

“Om goed mee te kunnen doen in de samenleving zijn ict-basisvaardigheden noodzaak”

‘Effective participation in society requires basic ICT skills’

Oppers is van mening dat voor de digitale weerbaarheid de randvoorwaarden in het onderwijs op orde moeten zijn. “Ook in het onderwijs moet digitalisering veilig gebeuren. Leraren werken met gevoelige informatie. Geen ouder zal willen dat de gegevens van hun kinderen op straat liggen. En geen school wil dat leerlingen hun digitale vaardigheden inzetten om hun rapporten op te poetsen. Daarom wordt de komende vijf jaar 50 miljoen aan collectieve middelen in SIVON geïnvesteerd om de digitale infrastructuur te verbeteren en te beveiligen.”

Uitdagingen

Volgens Oppers staan we nog voor grote uitdagingen om dit alles te bereiken: “Allereerst moeten leraren zelf digivaardig zijn en dat is een grote operatie. Er werken ruim 180.000 leerkrachten en docenten in het funderend onderwijs. Zij zullen leerlingen moeten onderwijzen in digitale vaardigheden.” Vijselaar is van mening dat publiek-private samenwerking helpt bij deze uitdagingen. “Instellingen en bedrijven kunnen een positieve bijdrage leveren, door het onderwijs te helpen met het scholen van leraren of door gebruik te maken van zogeheten hybride leraren, die deels voor de klas staan en deels actief zijn in het bedrijfsleven”, vertelt Vijselaar. “Dat begint bij het onderwijs zélf. De meeste bedrijven willen wel helpen, maar weten vaak niet hoe ze dit moeten doen. Ook omdat scholen, zeker basisscholen, vaak niet goed weten wat ze van het bedrijfsleven willen.” Oppers ziet veel individuele projecten tussen scholen en één bedrijf. Oppers: “Dit is weliswaar positief, maar het is versnipperd en niet duurzaam. Dat kan beter, als we de krachten bundelen, gezamenlijke doelen vaststellen en elkaar hier scherp op houden.” Oppers gelooft dat er mooie dingen kunnen gebeuren als zij erin slagen om de behoeften van scholen te verbinden met bijdragen van het bedrijfsleven. “Wat we willen is een brede en gecoördineerde inzet van scholen, bedrijven en maatschappelijke organisaties die hier energie bij voelen. In het najaar gaan we met scholen en het bedrijfsleven afspraken maken over wat we belangrijk vinden en welke bijdrage een ieder gaat leveren.”

Meerwaarde instellingen en bedrijven

Vijselaar is van mening dat iedereen uiteindelijk kan profiteren van deze samenwerking. “Bedrijven zijn op zoek naar oplossingen die impact hebben. Dat kan als initiatieven meer gebundeld zijn. Nog belangrijker is dat een breder platform het makkelijker maakt voor bedrijven om lokaal mee te helpen, bijvoorbeeld als het mkb iets wil doen voor scholen in de omgeving en zoekt naar een goede structuur hiervoor. In het Techniekpact hebben we onder andere vergelijkbare afspraken voor techniekonderwijs gemaakt; op landelijk niveau afspraken maken en het licht zetten op de goede voorbeelden. Dit helpt mensen, lokaal en regionaal, om de juiste keuzes te maken.” Oppers is het daarmee eens en vult aan dat zij met de curriculumherziening de onderwijsinhoud bij de tijd willen brengen. “Minstens zo belangrijk is dat we ook iets willen doen aan de

Parties all across Europe have realised that digitalisation will be absolutely essential to tomorrow's economy. ‘The Netherlands is fully aware as well,' Vijselaar concludes. ‘That's why the government presented the Dutch Digitalisation Strategy last year, in which we explicitly set out two crucial preconditions: digital skills and digital resilience. Since the development of digital skills largely begins at school, we've sought out cooperation with the Ministry of Education, Culture and Science and are also exploring ways for the business community to contribute.’

Educational curriculum

The Ministry has tasked teams of teachers and school administrators with reviewing the educational curriculum for primary and secondary education in the Netherlands. The new curriculum is expected to be available in 2022. ‘Digital literacy is one of the nine learning themes in the curriculum,’ says Oppers. ‘Effective participation in society requires not only basic ICT skills but information skills, media literacy and computational thinking. Soon, that knowledge and those skills will be permanently embedded in our educational curriculum.’ Schools will be given time to implement the new curriculum, but they can also choose to get started with digital literacy straight away. Oppers: ‘Many schools are already doing so. One school board in Groningen, for instance, has developed its own digital literacy learning track. The schools involved are now encountering various issues, such as identifying the skills that lecturers need and the learning tools that are appropriate to their educational vision.’ To help those in education find answers to these questions, the two Ministries (Economic Affairs & Climate Policy and Education, Culture & Science) are partnering with the primary and secondary education councils and Kennisnet. Vijselaar: ‘Together, we launched the Education & ICT Breakthrough project. This has led to nearly a hundred school boards across the Netherlands coming together as members of the SIVON cooperative. That cooperative is responsible for ensuring secure and affordable Internet access for the Dutch educational system.’
Oppers adds: ‘We are now extending this cooperation via the digitalisation agenda for primary education, which is part of the Dutch Digitalisation Strategy. Digitalisation strongly impacts the entire educational system – not only the knowledge and skills of pupils, but how teachers teach and how schools organise themselves as well.’

Digital resilience

According to Oppers and Vijselaar, the digital resilience of the Netherlands can be enhanced by incorporating a solid foundation into the country's educational system. ‘In matters of cybersecurity, it's important not to underestimate the human factor,’ Vijselaar says. ‘Think of it as you would home security. There are all manner of tools and tips to increase the security of your home, yet no security measure will be effective if you leave the front door open behind you. It's the same with digital security. This is why I'm pleased that digital security and privacy are also addressed in the proposed curriculum review. Which isn't the end of the story, of course: teachers will need to put those aspects into practice down the road.’
Oppers points out that the right preconditions must be in place in the educational system in order to achieve digital resilience. ‘Digitalisation in education must occur in a secure fashion. Teachers and lecturers handle sensitive information. No parent wants their child's data to be treated carelessly or leaked. And no school wants pupils to apply their digital skills to adjusting their academic results. For this reason, 50 million in public resources will be invested in SIVON over the next five years, in order to improve the quality and security of the digital infrastructure.’

Challenges

Yet Oppers sees several major challenges ahead: ‘The very first step is to see that all teachers are digitally literate – quite an operation in itself. Over 180,000 teachers work in primary and secondary education in the

overladenheid van het curriculum. Dat heeft deels te maken met de vele initiatieven die scholen aangeboden krijgen. Leraren kampen met hoge werkdruk, die deels wordt veroorzaakt door deze overladenheid. Dan helpt het niet om een wirwar aan initiatieven te hebben, die elkaar soms ook nog beconcurreren. Focus, structuur en aansluiting op de vraag van scholen is dus van belang, het onderwijs heeft hier de rol om zijn vraag goed te formuleren."

Oproep

Vijselaar legt uit dat de kern van de uitdaging niet zit in het optuigen van nieuwe initiatieven, maar juist in het versterken van bestaande trajecten en het bundelen van krachten. Hij doet een oproep aan het bedrijfsleven: "Dit najaar is een kans voor instellingen, bedrijven en andere belangstellenden die mee willen doen en zich bij ons aan willen aansluiten." Oppers vult aan: "De herziening van het curriculum is belangrijk voor zowel het onderwijs als het bedrijfsleven. Digitale geletterdheid heeft daarin een belangrijke plaats. Als de minister het vervolg van de herziening met de Tweede Kamer bespreekt, is het belangrijk dat bekend is dat de voorstellen op steun in de maatschappij kunnen rekenen. Spreekt u zich hier vooral over uit!"

"Publiek-private samenwerking helpt bij deze uitdagingen"

'Public-private partnerships can offer assistance in facing these challenges'

Netherlands. They are the ones who will have to teach their pupils digital skills.' Public-private partnerships can offer assistance in facing these challenges, says Vijselaar. 'Institutions and businesses can contribute by helping schools train teachers or through the use of so-called hybrid teachers, who spend part of their time in the classroom – teaching – while also working part-time in professional practice. But those in education must take the first step. While most businesses are willing to help, they are often unsure of how to go about it. This is often because schools – and primary schools in particular – aren't quite sure of what they want from the business community.' Oppers is aware of many individual projects involving schools and a single business. 'Although this is a positive development, it's rather fragmented and short-term in nature. We can do better if we all combine our strengths, establish shared goals and hold one another accountable for attaining them.' Oppers believes that great things can happen if the needs of schools can be linked to contributions from the business community. 'What we're trying to achieve is a broad and coordinated effort from schools, businesses and social organisations that are excited by this possibility. In the autumn, we'll be making agreements with schools and partners in professional practice regarding what our priorities are and what everyone will be contributing.'

Added value for institutions and businesses

Ultimately, to Vijselaar's mind, everyone stands to benefit from this cooperation. 'Businesses are looking for solutions that make a real impact. To that end, initiatives need to be more effectively combined. Even more importantly, such a broader platform makes it easier for businesses to help at the local level, such as when an SME wants to do something for schools in its area and is looking for an appropriate structure for its contribution. The Technology Pact includes similar agreements regarding technological education: it involves making agreements at a national level and highlighting good examples. This helps parties at the local and regional levels to make the right choices.' Oppers agrees, adding that they intend to bring the educational content up to date through the curriculum review. 'At the same time we also want to lighten the curriculum, which is currently overburdened due in part to the many initiatives schools are offered. Teachers are dealing with heavy workloads, caused in part by this surfeit of content, and so a dizzying range of initiatives – some of which are even in competition with one another – isn't exactly helpful. That's why focus, structure and coordination with the needs of schools are important. This also means parties in education have a duty to formulate their needs effectively.'

Call for action

Vijselaar explains that rather than in setting up new initiatives, the core challenge lies in strengthening existing projects and combining the strengths of various parties. He's issuing an appeal to the business community: 'This autumn, there will be an opportunity for institutions, businesses and any other stakeholders interested in participating to join us in our efforts.' Oppers adds: 'This curriculum review is important for both the educational system and the business community, assigning a prominent position to digital literacy. When the minister discusses the results of the review in the House, it is vital that everyone is aware that these proposals enjoy broad societal support. So be sure to express that clearly whenever you can!'

BACK TO TOP

EVERY CHILD SHOULD BE GIVEN THE OPPORTUNITY TO DEVELOP DIGITAL SKILLS

The idea for FutureNL, says Snellen, came into her mind when she gave computer skills training as a parent in her daughter's class. 'I noticed that there was no proper match between digital skills training at school and reality in the big world out there, let alone the reality of digital developments in the pipeline. So I started to organise guest lessons in computer programming, taught by people from the business community. The idea was that once teachers and pupils were brought up to speed on the range of possibilities ahead, this would automatically bring about a structural change.'

That proved a bit over-optimistic, but not because of insufficient demand. 'After those guest lessons, one of the first products I developed was a teaching package that I made in cooperation with Blink Educatie. It included a competition that generated so many questions that it seemed a good idea to go and find out who were actually using the teaching package. It turned out that as many as 1200 schools had already started using it in the very first month.'

Despite clearly filling a need, the package did not result in any additional, structural attention for digital skills in education. 'I decided I really needed to tackle this. Building on the guest lessons and the teaching packages we eventually developed an entirely new learning path for primary education, secondary education and teacher training colleges.'

Opportunities for all children

FutureNL has since developed into a professional organisation and already has several successes to its name. At the same time, there is still plenty of work to be done. Snellen: 'We will not really have succeeded until every child in the Netherlands has the opportunity to develop digital skills. That will enable them to deal with digitalisation more effectively in their current environment, which will also improve their prospects for the future, when every job will have a digital component. We should prepare children and students for that right now. We've opted for a two-pronged approach: a bottom-up design with activities at schools to promote change via the teachers, and a lobby aimed at politicians to persuade them to incorporate digital skills in the new curriculum. If all of that is successful, it will also motivate publishers to take over the baton. Publishers are still quite traditional in their approach, both in terms of content and form. For instance, they create textbooks that must last for five years, but digital developments are much faster than that.'

Blockades

If the urgency of promoting digital skills in education is so evident, why isn't the matter being dealt with on the required scale? Snellen believes there are several factors involved. 'I think there are some common denominators. Firstly, lack of time. Primary school teachers have a pretty busy job. And then there is fear. If you have little or no digital skills yourself, it's easy to think that you'll never learn them either. Thirdly, one in three schools simply don't have the required equipment. The

Ronilla Snellen
Co-founder and director of the FutureNL foundation

"Digitale geletterdheid moet structureel onderdeel van het onderwijs worden. Nederland heeft op dit vlak echt een achterstand in te halen." Dat zegt Ronilla Snellen, medeoprichter en directeur van de stichting FutureNL. Een organisatie die in samenwerking met scholen, overheden, universiteiten en bedrijven, leerlingen kennis laat maken met (de digitale toepassingen van) technologie en technologische vaardigheden. En dat is hard nodig want Nederland heeft nu al veel te weinig mensen beschikbaar die zijn opgeleid in bètavakken, techniek en computerwetenschappen.

'Digital literacy should be integrated into the curriculum. In this area there's a huge backlog to be dealt with in this country.' Says Ronilla Snellen, co-founder and director of the FutureNL foundation, an organisation that teams up with schools, government bodies, universities and businesses to introduce pupils to (digital applications of) technology and technical skills. This is urgent, given that science, technology and computer science graduates are already in short supply in the Netherlands.

Snellen kwam op het idee van FutureNL toen ze computerouder in de klas van haar dochter was. "Het viel me op dat het onderwijs in digitale vaardigheden onvoldoende aansloot bij de realiteit in de grote-mensen-wereld. Laat staan voor de ontwikkelingen die er op digitaal vlak nog aankomen. Daarom begon ik in de avonduren met het organiseren van gastlessen programmeren door mensen vanuit het bedrijfsleven. Dit vanuit de gedachte dat als leraren en leerlingen kennis maken met wat er allemaal mogelijk is, er vanzelf een structurele verandering op gang zou komen."

Dat laatste bleek iets te optimistisch, maar dit lag niet aan een tekort aan vraag. "Na die gastlessen was een van de eerste producten die ik ontwikkelde een lespakket dat ik maakte met Blink Educatie. Daarin zat ook een prijsvraag, waar ik zoveel vragen over kreeg dat ik maar eens ging kijken wie het lespakket allemaal gebruikten. Dat bleken in de eerste maand maar liefst 1200 scholen te zijn."

Ondanks het enorme gebruik, ontstond er geen structurele extra aandacht voor digitale vaardigheden in het onderwijs. "Ik besloot hier echt mee aan de slag te gaan. Van gastlessen, breidden we uit naar lespakketten, tot een hele nieuwe leerlijn. Voor het primair onderwijs, maar ook voor het voortgezet onderwijs en de PABO."

Kansen voor alle kinderen

FutureNL is inmiddels uitgegroeid tot een professionele organisatie en er zijn meerdere successen behaald. Er is tegelijkertijd nog veel werk te doen. "Ons werk is pas geslaagd als alle kinderen in Nederland de kans krijgen om digitale vaardigheden te ontwikkelen", aldus

Snellen. “Zodat ze hier en nu beter kunnen omgaan met digitalisering en zo meer toekomstperspectief krijgen. Elke baan in de toekomst zal digitale componenten hebben en daar moeten kinderen en studenten nu al op voorbereid worden. Dat doen we langs twee lijnen: met activiteiten op scholen om van onderaf via docenten een beweging op gang te brengen. En met een lobby richting de politiek om digitale vaardigheden op te laten nemen in het nieuwe curriculum. Als dat helemaal lukt, ontstaat ook de motivering voor uitgevers om het stokje over te nemen. Die denken nu nog erg traditioneel. Qua inhoud, maar ook qua vorm. Ze werken aan lesboeken die vijf jaar gebruikt moeten kunnen worden. De digitale ontwikkelingen gaan daar veel te snel voor.”

Blokkades

De urgentie van aandacht voor digitale vaardigheden in het onderwijs zijn evident, maar waarom wordt dit dan niet breed opgepakt? Snellen heeft hier wel ideeën over: “Ik zie een aantal gemene delers. Ten eerste tijdgebrek, als leraar op een basisschool heb je het al behoorlijk druk. Daarnaast is er angst. Als je zelf weinig tot geen digitale vaardigheden hebt, kun je al gauw denken dat je het nooit zult leren. En ten derde heeft een op de drie scholen simpelweg niet de benodigde apparatuur. Daar is inmiddels een subsidiepotje voor vanuit het ministerie van Onderwijs, Cultuur en Wetenschap, maar dat gaat nog niet hard genoeg. Daarom maken we het voor scholen en leraren zo makkelijk mogelijk. We nemen alle bezwaren die ze opbrengen mee in de ontwikkeling van ons lesmateriaal. En we sluiten goed aan op de hardware en software die scholen al gebruiken. Daarnaast linken we digitale geletterdheid altijd aan een bestaand vak. Zo wordt het niet nog een vak erbij – waar geen tijd en ruimte voor is – maar een vervanging van bestaande uren.”

Nederlandse standaard voor digitale geletterdheid

De volgende stap is om digitale geletterdheid structureel onderdeel van het onderwijs te maken. “We hebben geholpen bij de ontwikkeling van een leerlijn. Daardoor is er nu een Nederlandse standaard voor digitale geletterdheid. Het is een van onze grootste successen tot nu toe. Hierbij hielp het dat we begonnen bij wat er al stond. In Nederland werd al gewerkt met het 21st century model, waarin op het vlak van onderwijs en digitalisering gefocust wordt op mediawijsheid, informatievaardigheden, computational thinking en digitale basisvaardigheden. Door daarbij aan te sluiten, herkende iedereen het en hoefden we niet op nul te beginnen qua overtuiging.”

Nederland loopt achter

We zijn in Nederland dus bezig met een inhaalslag, maar hoe doen ‘we’ het eigenlijk ten opzichte van het buitenland? “Niet goed genoeg”, aldus Snellen. “Nederland loopt achter. Scandinavische landen, de Verenigde Staten en Canada doen het beter, maar een land als India ook. In ons systeem duurt de aanpassing van het curriculum heel lang. Terwijl digitalisering juist razendsnel gaat. Het nieuwe curriculum, waarin verschillende digitale vaardigheden nu een plek krijgen, gaat waarschijnlijk pas in 2022 van kracht en scholen krijgen zeven jaar de tijd voor de implementatie. Dat duurt veel te lang. Ik garandeer je dat de wereld er in 2030 alweer totaal anders uit ziet. De overheid en uitgevers doen te weinig nu. Het is eigenlijk gek dat wij als stichting nu een cruciale nieuwe leerlijn maken.”

Cybersecurity

Ook voor cybersecurity is een belangrijke rol weggelegd in de leerlijnen en programma’s die FutureNL ontwikkelt. “Daar zie ik wel urgentie. Ook door de overheidscampagne over nepnieuws die op dit vlak nu loopt. Maar zeker voor schooljeugd denk ik dat het belangrijk is dit tastbaar te maken. Wij hebben bijvoorbeeld een les waarin we leerlingen een fake-profiel laten onderzoeken van een jongen van 10: Chris. Chris lijkt op het eerste gezicht een bestaande jongen, met een Facebook-profiel en Youtube-kanaal, maar langzaam laten we kinderen zien dat daar niks van klopt. De kinderen zijn dan zo ontzet, dat vergeten ze niet gauw meer. Zo bereik je meer dan met posters in de bushalte of reclame op tv.

Ook werken we momenteel met de Gemeente Rotterdam aan een lespakket over cybersecurity. We bespreken daarin wat er kan gebeuren online en wat je er aan kan doen, bijvoorbeeld door ze te leren wat phishing is. Aan het einde van de les stellen de leerlingen zelf een kaart op, waarop ze hun eigen kwetsbaarheden in kaart brengen. Deze lessen zijn vanaf begin volgend jaar voor alle scholen gratis te vinden op onze website www.futurenl.org

Dit soort lessen maakt kinderen loei enthousiast. Betere digitale vaardigheden aanleren is ook gewoon leuk. En belangrijk!”

BACK TO TOP

NEXT

“Elke baan in de toekomst zal digitale componenten hebben en daar moeten kinderen en studenten nu al op voorbereid worden”

‘Every job in the future will have a digital component. We should prepare children and students for that right now’

Ministry of Education, Culture and Science has made a subsidy available for that, but progress is still too slow. That's why we are making things as easy as possible for schools and teachers and consider all their objections when developing teaching materials. We're also doing our best to connect to the hardware and software that schools are already using. What's more, we always link digital literacy training to existing subjects in the curriculum. So we use existing class hours for the training, rather than create a new, additional subject for which there's simply no time or space available.'

Dutch standard for digital literacy

The next step is to integrate digital literacy into the curriculum. 'We've contributed to the development of a learning path. As a result, we now have a Dutch standard for digital literacy. In fact this has been one of our greatest achievements thus far. We had something to build on, which helped. After all, schools in this country were already using the 21st century model, which provides for a focus in education and digitalisation on media literacy, information skills, computational thinking and basic digital skills. By connecting to a familiar model, we didn't have to start from scratch in terms of persuading people to adopt our approach.'

The Netherlands is lagging behind

So as we are trying to eliminate our backlog in digital skills training, how are we performing compared with other countries? 'Not as well as we should', is Snellen's verdict. 'The Netherlands is lagging behind Scandinavia, the United States, Canada but also countries like India. In our system it takes ages to adapt a curriculum, in stark contrast to the speed of digital developments. The new curriculum incorporates several digital skills, but it is not expected to be introduced until 2022 and schools will be given another seven years to implement it. That's far too long. By 2030 the world will be fundamentally different from what we're planning for today, mark my words. So the government and publishers should really step up their efforts. Actually it's odd that we, a foundation, are now developing this crucial new learning path.'

Cybersecurity

Cybersecurity, too, has an important role to play in the learning paths and programmes developed by FutureNL. 'We do see a sense of urgency there, encouraged in part by the campaign about fake news that the government has launched. I do feel however that we need to give concrete examples to show schoolchildren in particular how fake news can affect them. For instance, we've developed a lesson in which we ask pupils to investigate the fake profile of a ten-year-old boy, named Chris. While at first sight Chris looks like a real boy with his own Facebook profile and YouTube channel, we gradually make the children realise that he is entirely fake. That really upsets them. It's a message they're not likely to forget. This is much more effective than using posters on a bus shelter or running a commercial on TV.

We're also teaming up with the Rotterdam city council to create a teaching package on cybersecurity. In it we'll discuss the risks children run online and what they can do to protect themselves, for example by teaching them about phishing. At the end of the lesson we ask the children to map out their own vulnerabilities. Starting early next year, these teaching materials will be available to all schools free of charge from our website, www.futurenl.org.

Lessons of this kind really make the children extremely enthusiastic, as they see that improving their digital skills can actually be great fun. And it's important too!'

René Speelman
Corporate Social Responsibility Manager at Sogeti and member of the Education Working Group of NLdigital

‘DIGITAL LITERACY IS OUR SOCIAL RESPONSIBILITY’

In Nederland wordt hard gewerkt aan curriculumvernieuwing die het onderwijs beter moet laten aansluiten op de digitaliserende toekomst. Naar verwachting wordt het nieuwe curriculum voor het primair en voortgezet onderwijs in 2022 beschikbaar gesteld en krijgen de scholen tot 2030 de tijd om het curriculum in te voeren. In Denemarken zijn overheid en onderwijs al een stap verder met het invoeren van digitale geletterdheid in het onderwijs. René Speelman, manager Corporate Social Responsibility bij Sogeti en lid van de Werkgroep Onderwijs van NLdigital, is namens NLdigital op studiereis naar Denemarken geweest om inspiratie op te doen voor de implementatie van het onderwijscurriculum in Nederland.

A major effort is under way in the Netherlands to modernise the curriculum so as to prepare students more effectively for ongoing digitalisation. Expectations are that the new curriculum for primary and secondary schools will become available in 2022, and that schools will be given time until 2030 to implement it. In Denmark, the government and the education sector have already reached the next stage in introducing digital literacy training in education. René Speelman, Corporate Social Responsibility Manager at Sogeti and a member of the Education Working Group of NLdigital, has been on a study trip to Denmark on behalf of NLdigital to gain inspiration for the implementation of the modernised curriculum in the Netherlands.

Als jonge onderwijzer introduceerde Speelman de computer in de klas in de tijd van de Commodore 64, de ZX Spectrum en de P2000. “De programma’s werden vanaf een klein cassettebandje geladen”, vertelt Speelman enthousiast. “Het was magie voor de kinderen, maar ook voor veel leerkrachten. Toen ik aan mijn collega’s op een woensdagmiddag liet zien wat er allemaal mogelijk was, viel plotseling de stroom uit. Demonstratief liet de directeur van de school het rekenboekje op tafel vallen en zei: “Deze doet het altijd”. Dit was in 1985 en sinds die tijd is er gelukkig veel veranderd. Op verschillende scholen zijn leerkrachten met digipassie bezig om jonge mensen te laten ervaren hoe gaaf het is om met IT te werken. Ondanks alle digitale ontwikkelingen is IT, of beter gezegd digitale geletterdheid, tot op heden nog geen vast onderdeel in het onderwijscurriculum. Wat de kinderen moeten leren om zich in de digitale samenleving optimaal te ontwikkelen, staat nog steeds niet vast.” Het is volgens Speelman de hoogste tijd om daar wat aan te doen.

Curriculum.nu
De laatste vernieuwingen van het onderwijscurriculum dateren van vijftien jaar geleden; de periode van PDA’s, bellen en SMS-en, mondjesmaat Wifi en geen tablets. Een hele generatie is inmiddels opgegroeid zonder dat digitale geletterdheid formeel op het onderwijsprogramma stond. Inmiddels wordt er onder aanvoering van Curriculum.nu hard gewerkt om digitale geletterdheid op te nemen in het nieuwe curriculum. Dat doen ze samen met een grote groep onderwijskundigen en studenten. In Denemarken zijn overheid en onderwijs al een stap verder; hier is al ervaring opgedaan met de implementatie ervan. Om die reden nam Speelman namens de werkgroep Onderwijs van NLdigital deel aan een studiereis naar Kopenhagen. Speelman: “De werkgroep Onderwijs richt zich op het vergroten van de digitale kennis en vaardigheden in ons land en het verkleinen van het tekort aan IT-talenten. Dat gaat mooi hand in hand. Hoe meer jongeren enthousiast raken over het vakgebied, des te

Speelman introduced computers in the classroom early in his teaching career. These were the days of the Commodore 64, the ZX Spectrum an the P2000 - which still rouse his enthusiasm. ‘Those programs were loaded from a small cassette tape. It was magic - not just for he children, but for us teachers too. One afternoon, as I was showing my colleagues what they could do with a computer, all of a sudden we had a power failure. The school headmaster demonstratively dropped an arithmetic book on the table, saying: “This thing always works". That was back in 1985; I'm happy to say a great deal has changed since then. At many schools, teachers who are passionate about digitalisation are allowing kids to experience for themselves how wonderful it is to work with IT. Despite the massive developments in IT that we've seen in recent years, IT - or I should say digital literacy - has still not become a fixed component of the curriculum. There is still no consensus on what children should learn to develop to their full capacity in our digital society.’ It is high time, says Speelman, that this situation is tackled.

Curriculum.nu
The most recent round of modernisations in the curriculum took place 15 years ago; the period that saw the introduction of PDAs, mobile phones, text messaging, small-scale Wi-Fi - but no tablets. This means that a entire generation has grown up since with a curriculum that had no formal place for digital literacy. Lead by Curriculum.nu, a considerable effort is now being made to introduce digital literacy in the new curriculum, in collaboration with a large group of educationalists and students. In Denmark, the government and the education sector have already reached the next stage and gained experience with the actual implementation. This is why Speelman decided to make a study trip to Copenhagen on behalf of NLdigital's Education Working Group. Speelman: 'Our working group focuses on increasing the digital knowledge and skills in this country and reducing the shortage of IT talents. So it works both ways: the more young people become enthusiastic about the field, the greater the chance that they'll opt for a professional career in IT. We made this study trip to Denmark to see for ourselves how digitalisation is being integrated into Danish education, and to gain inspiration for implementing the curriculum here in the Netherlands.'

Integrated or separate
The influence of the government in Denmark is greater than in the Netherlands, which is reflected in a different organisation of the education system. All the same, Denmark is struggling with several issues and learning lessons that are also relevant to the Dutch education system, says Speelman. 'One of the dilemmas Denmark is trying to solve is how to offer digital literacy as a part of your curriculum. Should you integrate and combine digital skills with other subjects, or offer digital skills training as a separate subject? They're running a pilot in Denmark right now with over twenty schools offering integrated digital literacy training and another twenty schools providing digital literacy as a separate subject. I saw an example of the integrated approach during a lesson on the development of democracy and universal suffrage. The pupils were introduced to the micro:bit, a small device with a miniature LED display that they can program via their laptop or tablet and use to create a voting machine, for example. This approach allowed the teacher to

groter de kans is dat zij kiezen voor een professionele carrière in de IT. Tijdens de studiereis naar Denemarken wilden we met eigen ogen zien hoe digitalisering in het Deense onderwijs wordt geïntegreerd en inspiratie opdoen voor de implementatie van het curriculum in Nederland."

Integraal of separaat

Omdat de invloed van de overheid in Denemarken groter is, is het onderwijssysteem in dit land anders georganiseerd. Toch kampt Denemarken volgens Speelman met verschillende vraagstukken die ook leerzaam zijn voor ons onderwijssysteem. "Eén van de dilemma's waar Denemarken een antwoord op zoekt is hoe je digitale geletterdheid in het onderwijs aanbiedt. Doe je dit integraal, in combinatie met andere vakken of zet je het als separaat vak op het rooster? In Denemarken voeren ze nu een pilot uit waarbij ze op ruim twintig scholen digitale geletterdheid integraal aanbieden en op twintig andere scholen wordt het als apart vak geven. Ik heb een voorbeeld gezien van een integrale aanpak tijdens een les over de ontwikkeling van democratie en het stemrecht. De leerlingen werden geïntroduceerd met de micro:bit, een klein device met een ledschermpje die zij via hun laptop of tablet kunnen programmeren en waarmee zij bijvoorbeeld een stemmachine kunnen maken. Door deze aanpak kon de docent ook met de kinderen praten over de veiligheid van het systeem en hoe je dit onrechtmatig kunt beïnvloeden. Op deze wijze werd digitale geletterdheid van kinderen geïntegreerd met een les over kennis van de maatschappij."

Consument én producent

Het voorbeeld van de stemmachine levert volgens Speelman nog een interessant inzicht op. "In het aanbieden van digitale geletterdheid kun je perspectieven van leerlingen laten veranderen. De leerling kan als consument gebruikmaken van IT en kennismaken met de functionaliteit en het design ervan. Anderzijds kan men dezelfde leerling vragen om software te maken. Hij of zij kijkt dan met een andere bril naar IT en is opeens producent. Ze leren opeens na te denken over software, design, functionaliteit, het testen van de software en de veiligheid. Daarmee is de leerling als het ware producent."

Maatschappelijke verantwoordelijkheid

Met de bril op van NLdigital heeft Speelman ook gekeken naar de wijze waarop het IT-bedrijfsleven een rol kan spelen bij de implementatie van het nieuwe onderwijscurriculum en specifiek de module digitale geletterdheid. "Partijen als Google for Education, HP, Lego Education, Dell, Acer en Microsoft zijn bekende leveranciers in het onderwijs maar als we het commerciële belang eraf halen, blijft er dan nog een belang over?" Dat digitale geletterdheid opgenomen moet worden in het curriculum is volgens Speelman een open deur. "Om je in deze wereld goed te ontwikkelen en je talenten optimaal te benutten is een grondige kennis van de digitale mogelijkheden, onmogelijkheden, kansen en risico's noodzakelijk", claimt Speelman. "Als we nalaten kinderen op dit gebied te onderwijzen, lopen we het risico dat kinderen met meer digitale kennis later kansrijker zijn dan de kinderen met minder digitale kennis. Het besef van urgentie kan wat dat betreft nog een stuk omhoog; haast is geboden." Speelman is van mening dat de IT-sector hierin als eerste een maatschappelijke verantwoordelijkheid heeft. "Wij brengen immers de technologie op de markt en mogen ons verantwoordelijk voelen voor een goed gebruik. Daarnaast is het tekort van IT-professionals in de arbeidsmarkt al duidelijk zichtbaar. We zijn erbij gebaat dat meer jongeren enthousiast worden voor het IT-vak. Het is een goede tweede reden om krachtig te participeren in het IT-onderwijs." Rendement op korte termijn is volgens Speelman het grootst als we beginnen bij lerarenopleidingen als de Pabo. "Wat mij betreft niet met pilots zoals in Denemarken, maar geregisseerd vanuit een landelijke digiforce, zodat we met een directe betrokkenheid van het bedrijfsleven snel kunnen starten met de invoering van het curriculum en kunnen bijstellen waar nodig om het curriculum up-to-date te houden."

"Wij brengen immers de technologie op de markt en mogen ons verantwoordelijk voelen voor een goed gebruik"

'After all, we are the ones that launch the technologies, so there's every reason for us to feel responsible for how they're used'

address issues such as system security and hacking while discussing other subjects. In this example, digital literacy was integrated into a lesson on society and politics.'

Consumers and producers at the same time

Speelman points out that the example of the voting machine also yields another interesting insight. 'Providing digital literacy training allows us to alter pupils' perspectives. On the one hand, you enable them to use IT as consumers and introduce them to IT functionality and design. On the other hand, you can ask those same pupils to actually create software themselves. This will turn them into producers and will make them view IT from a different angle, teaching them to think about software, design, functionality, testing and security issues. That makes them producers rather than consumers of IT.'

Social responsibility

From his role within NLdigital, Speelman has also considered ways for the business community to contribute to the implementation of the new curriculum and, more specifically, of the digital literacy module. 'Players such as Google for Education, HP, Lego Education, Dell, Acer and Microsoft are well-known suppliers of educational tools, but I need to know what interests remain if we remove the commercial interest.' Claiming that digital literacy training needs to be incorporated into the curriculum is stating the obvious, says Speelman. 'To develop your talents to full potential in today's world, you will need to have a solid understanding of what is and what is not possible with IT, and of the opportunities and risks involved. If we fail to teach children about these things, the risk is that children with more digital knowledge will eventually have more opportunities than those with less knowledge in this field. We actually need a far greater sense of urgency in this regard; time really matters.' In Speelman's view, the IT sector itself should take the lead in terms of accepting its social responsibility. 'After all, we are the ones that launch the technologies, so there's every reason for us to feel responsible for how they're used. At the same time, the shortage of IT professionals in the labour market is clearly growing. If more young people become enthusiastic about IT as a profession, we clearly stand to benefit as a sector. That's a second good reason for us to strongly participate in IT education.' The short-term returns are the greatest, says Speelman, if we start at teacher training colleges, for example in primary education. 'I'd rather not run pilots, such as in the Danish example, but set up a nationwide digiforce that would enable us to ensure the direct involvement of businesses in quickstarting the implementation of the curriculum and adjust it where necessary to keep it up to date.'

NEXT
BACK TO TOP

CYBERSECURITY: THE IMPORTANCE OF ‘THE HUMAN FACTOR’

De digitale transformatie van organisaties, de economie en samenleving is in volle vaart gaande; we spreken ook wel van de digitale revolutie! Data is daarbij van cruciaal belang. Denk aan input voor het optimaliseren van bestaande processen of als grondstof voor nieuwe diensten. Al deze ontwikkelingen gaan in sneltreinvaart en houden direct verband met ons vermogen om in de toekomst relevant te blijven op wereldniveau. Tot nu toe zijn we als Nederland daar best goed in, getuige de top-10 positie op de lijst van meest concurrerende economieën.

Veiligheid, en cybersecurity in het bijzonder, speelt in deze ‘always on, always connected’-wereld een belangrijke rol. Als de toepassingen of databronnen niet *beschikbaar* zijn: geen omzet, nieuwe klanten en verdienmodellen en als de data niet *integer* zijn: verkeerde voorspellingen, komt daarmee snel een eind aan de dienst en het voortbestaan van de onderneming. Bovendien zijn zonder *vertrouwelijkheid* van algoritmes en adviezen de diensten eenvoudig te kopiëren en zullen klanten overlopen.

De menselijke factor is hierbij een belangrijke schakel. Zowel voor het veilig maken en houden van systemen en data én voor het op een veilige manier werken met nieuwe technologieën.

Expertise zoeken we bij de cyberspecialisten, bijvoorbeeld specialisten om systemen en data veilig te maken via beleid of specialisten voor een security operations center. De behoefte aan deze medewerkers groeit de laatste jaren explosief. Waar in 2014 nog 482 vacatures werden geplaatst voor soortgelijke functies, was dit aantal in 2017 toegenomen tot 1461.[1] Leden van CIO Platform Nederland geven aan dat het in toenemende mate lastig is om hiervoor geschikte mensen te vinden. Het groeiende tekort aan cyberspecialisten vormt een bedreiging waaraan we collectief iets moeten doen; deze vijver moet groter! Een flinke stap kan bijvoorbeeld worden gezet door meer vrouwen te stimuleren een opleiding te volgen die de opmaat vormt voor dit soort banen; dit vergt namelijk niet alleen technische, maar zeker ook sociale vaardigheden. Dus, stimuleer vrouwelijke medewerkers om zich bij te scholen, maak fondsen en tijd hiervoor beschikbaar. Enthousiasmeer dochters, kleindochters, nichtjes en andere meiden in jullie netwerk om zich in dit werkveld te verdiepen. En ook jongens blijven natuurlijk van harte welkom.

Inhoudelijke security expertise moet ook terecht komen in de ontwikkel- en beheerteams en bij mensen die met data science actief zijn. Zij hebben een bijzondere verantwoordelijkheid en een soms lastige positie. Enerzijds worden ze afgerekend op snel ontwikkelen van functionaliteiten en aan de andere kant dragen zij zorg voor een fatsoenlijke (lees veilige) manier van programmeren of omgang met databestanden. Een verkeerde aansturing kan al snel ertoe leiden dat ‘time to market’ belangrijker wordt dan het maken van een juiste afweging van belangen. Bijvoorbeeld over het al dan niet gebruiken van bepaalde datasets of het leggen van verbanden tussen data die ethisch wellicht niet wenselijk is. Hier ligt een cruciale rol voor bestuurders; geef de juiste incentives mee!

Een geheel andere insteek om organisaties te beveiligen is met de kracht van human capital: medewerkers en klanten. Een alerte en kritische blik op e-mail en andere berichten en signalen die door elektronische tools worden afgegeven, is van wezenlijk belang om de netwerken, systemen en data van organisaties veilig te houden. Stimuleer continu alle betrokkenen, van commissarissen en directieleden tot aan junior medewerkers. Blijf alert, beloon het stellen van vragen en melden van vreemde situaties, wees creatief in het verzinnen van manieren om iedereen bij de les te houden en geef bovenal zélf het goede voorbeeld!

Ronald Verbeek
Directeur, CIO Platform Nederland

“Het groeiende tekort van cyberspecialisten vormt een bedreiging waaraan we collectief iets moeten doen; deze vijver moet groter!”

‘The growing shortage of cyberspecialists poses a threat that we'll have to address together: this pool must be expanded!’

BACK TO TOP

The digital transformation of organisations, the economy and society is in full swing: indeed, it is often called a digital revolution! Data is a crucial factor in this transformation, as it provides both input for the optimisation of existing processes and raw material for new services. Developments in this context are moving at lightning speed and have a direct bearing on this country's ability to remain relevant at a global level in future. Until now, we have been fairly successful in this area, considering our top-ten position on the list of the world's most competitive economies.

Security, and cybersecurity in particular, play a vital role in this ‘always on, always connected’ world of ours. When applications or data sources are not *available*, sales will come to a halt, no new clients will be attracted and earning models become useless. When the data lacks *integrity*, inaccurate forecasts will result – quickly followed by an end to the service and the continued existence of the company in question. And when algorithms and advice are not *confidential*, the services will be susceptible to imitation and clients will switch providers.

The human factor is absolutely an important link, both in order to keep systems and data secure, and to make sure new technologies are utilised securely.

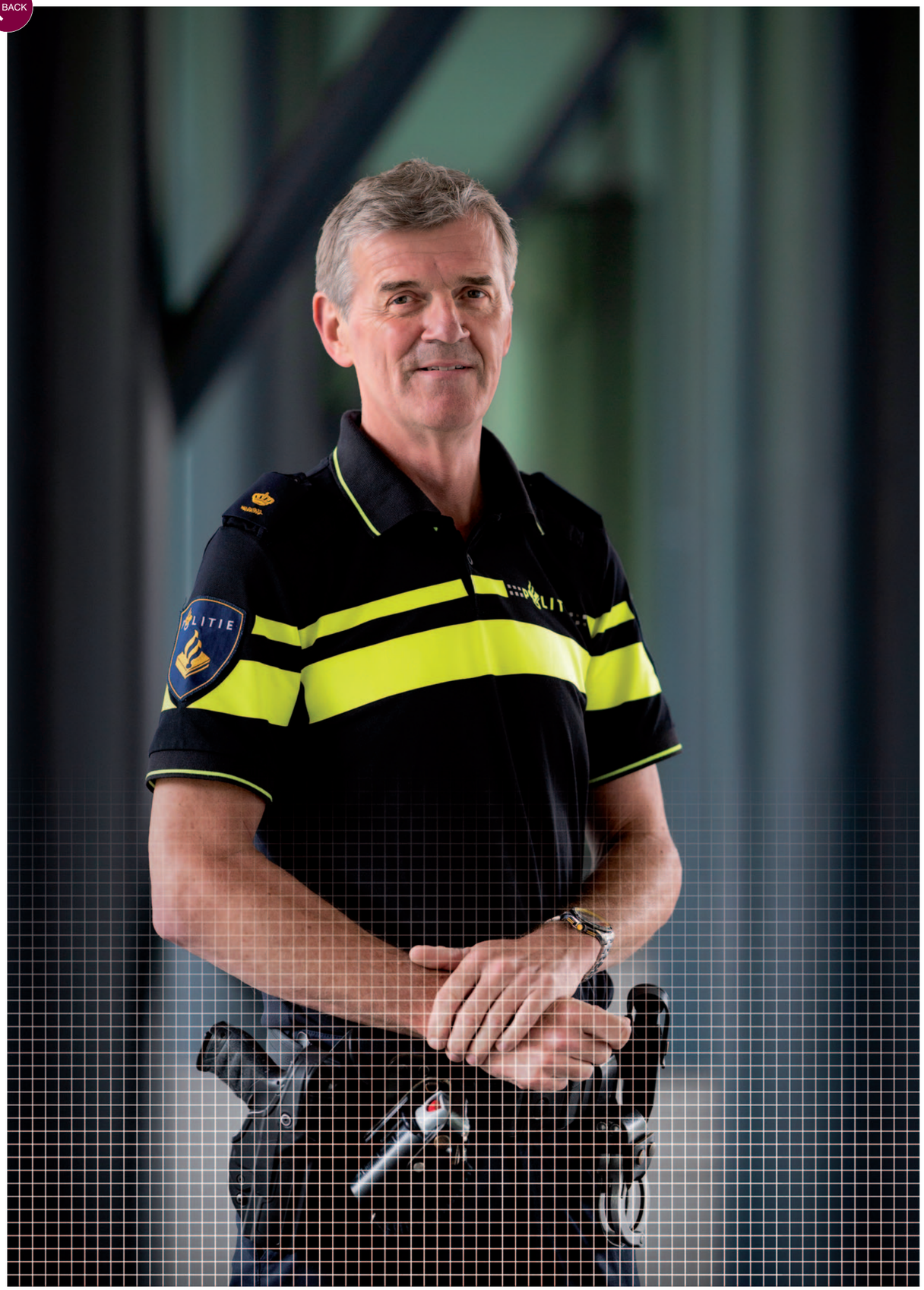
For the expertise needed to achieve system and data security through policy or a security operations centre, for instance, we turn to our cyberspecialists. The demand for such employees has increased exponentially in recent years. Whereas in 2014, 482 vacancies for such positions were posted, in 2017 this number had grown to 1461.[1] Members of CIO Platform Netherlands have warned that it is becoming increasingly difficult to find suitable candidates for these jobs. The growing shortage of cyberspecialists poses a threat that we'll have to address together: this pool must be expanded! One major contribution might, for instance, be realised by urging more women to enrol in studies that serve as the basis for this type of job, which requires not only technical skills but social skills as well. In other words: encourage female employees to pursue additional education and training, and make funding and time available for this purpose. Motivate your daughters, granddaughters, nieces and other young women in your network to learn more about this field. Young men are also welcome as ever, of course.

Substantive security expertise must also be passed on to development and management teams and people active in the field of data science. They have a special responsibility and may find themselves in a difficult position. On the one hand, they are judged by their ability to rapidly develop functionalities, while on the other they are held responsible for ensuring solid (i.e. secure) practices in programming and handling data files. Improper management can easily lead to prioritising time to market over the proper consideration of other interests involved – whether or not to use certain data sets, for example, or linking various data in a way that might be morally questionable. Board members have a crucial role here, as they should provide the right incentives.

An entirely different approach to making organisations secure relies on the strength of human capital, i.e. employees and clients. A vigilant and critical eye on emails and other messages and signals emitted by electronic tools is of critical importance in order to keep organisations’ networks, systems and data secure. All involved parties should be continuously encouraged – everyone from members of the Supervisory Board and directors to junior staff members. Stay vigilant, incentivise people to ask questions and report unusual situations, be creative in finding ways to keep everyone engaged and – above all – be sure you're setting a good example yourself!

Ronald Verbeek
Director, CIO Platform Netherlands

1. Pr-eDICT-tool van CA-ICT op basis van cijfers van Jobdigger, bewerkt door Dialogic. Zie: https://pr-edict.nl/ict-vacatures
Pr-eDICT tool from CA-ICT, using figures from Jobdigger, processed by Dialogic. See: https://pr-edict.nl/ict-vacatures



Theo van der Plas
Programme director for digitalisation and cybercrime with the National Police Force

Cybercrime neemt steeds verder toe. De verwachting is dat cybercrime over een aantal jaar omvangrijker is dan traditionele criminaliteit. Binnen vijf jaar zal de helft van alle strafzaken cybercrime-gerelateerd zijn. Theo van der Plas, programmadirecteur digitalisering en cybercrime bij de Nationale Politie, werkt in zijn team met specialisten hard om de cybercriminaliteit in Nederland te ondermijnen.

Cybercrime rates continue to rise. The expectation is that in many countries, cybercrime will surpass traditional areas of crime in scope in a number of years' time. Within five years, half of all criminal cases will be cybercrime-related. Theo van der Plas, programme director for digitalisation and cybercrime with the National Police Force, and his team of specialists are working hard to combat cybercriminality in the Netherlands.

FROM ELDERLY BRITS TO TEENAGE HACKERS

Er zijn inmiddels veel anekdotes te vertellen over cybercrime, zoals de grootste juwelenroof ooit in Engeland en waarschijnlijk door de oudste bende ooit. Van Der Plas: "De 'Grandpa Gang' werden ze genoemd", vertelt Van Der Plas. "Zeven Britse bejaarden die in 2015 twintig miljoen aan goud, juwelen en contant geld hebben gestolen. Maar de betonborende bejaarden maakten domme fouten. Zo hadden ze een vluchtauto gehuurd onder een valse naam, maar daarbij wél hun echte adres opgegeven. Ook hadden ze de beveiligingssystemen onklaar gemaakt, maar waren ze een beveiligingscamera op straat vergeten. Wat ook niet hielp was dat de bejaarde bestuurder van de vluchtauto in slaap was gevallen. De bejaarde Britten zitten inmiddels een jarenlange gevangenisstraf uit." Volgens Van Der Plas was dit verhaal voorpaginanieuws. "Heel anders dan een andere bankroof een jaar eerder", vervolgt hij. "Toen werden zo'n honderd banken wereldwijd beroofd door een bende hackers die de Carbanak Gang werd genoemd. Ze haalden nauwelijks het nieuws, terwijl dit met honderden miljoenen dollars buit, de grootste bankroof uit de geschiedenis was. De banken hebben maatregelen genomen en het vermoedelijke kopstuk van de bende in Spanje is gearresteerd, maar de bende is nog steeds actief."

1,2 miljoen slachtoffers

Ook meer recent en dichter bij huis ziet Van Der

By now there are many cybercrime-related anecdotes to be told, such as the one about the biggest jewel heist in British history and what is likely the oldest gang of crooks ever. Van Der Plas: 'People called them the Grandpa Gang: seven elderly British men who stole twenty million in gold, jewels and cash in 2015. But these concrete-drilling grandpas made some foolish mistakes. They had rented a getaway car under a false name but had given the rental company a real address. They had also disabled the security system but forgotten about a security camera on the street. Another hitch in their plan was that the driver of the getaway car, himself getting on in years, had fallen asleep. The aged British thieves are currently serving long prison sentences.' According to Van der Plas, the incident was front page news. 'It was covered quite differently than another bank robbery, one year prior,' he continues. 'In that case, a hundred banks or so around the world were robbed by a gang of hackers known as the Carbanak Gang. They hardly made the news at all, despite the fact that the hundreds of millions of dollars in loot made their crime the biggest bank robbery of all time. The banks took measures in response and the suspected ringleader was arrested in Spain, yet the gang itself continues to operate.'

1.2 million victims

More recently and closer to home, Van der Plas is observing the consequences of digital threats such as retail fraud, phishing and ransomware. 'Studies by Statistics Netherlands show that over 1.2

Plas de gevolgen van digitale dreigingen, zoals aankoopfraude, phishing en gijzelsoftware (ransomware). “Uit onderzoek van het Centraal Bureau voor de Statistiek blijkt dat vorig jaar ruim 1,2 miljoen Nederlanders slachtoffer waren van digitale criminaliteit. Jonge internetgebruikers van 12 tot 25 jaar waren met zo’n 12 procent het vaakst slachtoffer en van de 65-plussers werd daarentegen nog geen 4 procent slachtoffer. We zien klassieke criminaliteit, zoals woninginbraken en overvallen, afnemen en cybercriminaliteit toenemen.”

Overal zelfde wachtwoord

Van Der Plas maakt de vergelijking met de beveiliging van een huis. “Wie op vakantie gaat, sluit alles goed af, regelt wellicht een tijdschakelaar voor het licht. Vraagt de buren de post weg te halen. Alles om ervoor te zorgen dat het lijkt alsof je thuis bent en om inbrekers buiten de deur te houden. De digitale deur sluiten we daarentegen nog steeds onvoldoende af, bijvoorbeeld omdat die beveiligingsupdate nu even niet uitkomt of we klikken te snel op een linkje in een verdachte e-mail.” Van Der Plas geeft toe dat phishingmails die zogenaamd van de banken komen er steeds professioneler uitzien. “En als we kijken naar jongeren: zij leren online, leven online. Gamen met generatiegenoten over de hele wereld. Maar diezelfde jongeren gebruiken vaak hetzelfde wachtwoord voor verschillende websites, sociale media en games. Dat maakt het voor hackers wel heel makkelijk.”

Melden en delen

“We zien als politie ook dat mensen maar beperkt aangifte doen van cybercriminaliteit”, vervolgt Van Der Plas. “Nog geen tien procent, is een ruwe schatting. Tegelijkertijd weet ook niet iedereen dat hij of zij slachtoffer is. Onderzoek laat zien dat het merendeel van de bedrijven die gehackt zijn, dat niet weten. En als ze het wel weten doen ze vaak geen aangifte uit angst voor imagoschade.” Het melden en delen van informatie over digitale kwetsbaarheden en trends kan volgens Van Der Plas helpen om een beter beeld te krijgen. “Dan kunnen we als politie meer doen om cybercriminaliteit te voorkómen of de gevolgen ervan te beperken.”

Jongeren als dader

Samen met partners uit bedrijfsleven, wetenschap en overheid werkt de politie aan campagnes om mensen bewust te maken van online dreigingen. “We vertellen ook wat ze zelf kunnen doen om veiliger online te zijn en we richten ons ook op mogelijke daders onder jongeren met de campagne ‘Je bent één klik verwijderd van cybercrime’. Want juist onder jongeren zien we behalve veel slachtoffers, ook veel (potentiële) daders. En voor de jongere die de klik naar cybercrime al wél heeft gezet, hebben we samen met het Openbaar Ministerie en enkele private partijen ‘Hack-Right’ opgezet; de digitale versie van bureau HALT. Als een jongere bijvoorbeeld wordt gepakt voor hacken, dan volgt een verplichte stage bij een ICT-bedrijf om beter te begrijpen wat hij of zij heeft aangericht. Zo hopen we meer schade te voorkomen. Sterker nog: we hebben eerder goede ervaring opgedaan met jonge hackers, die nu organisaties bijstaan om hun cybersecurity te verbeteren.”

“Juist onder jongeren zien we behalve veel slachtoffers, ook veel (potentiële) daders”

‘We're finding not only many victims among young people, but many actual or potential culprits as well’

million people in the Netherlands were victims of digital criminality last year. Young Internet users between 12 and 25 years of age were, with 12 per cent, the most frequent victims; of those aged 65 and over, by comparison, less than 4 per cent were victimised. We're seeing a decrease in traditional crime such as burglary and robbery while the rate of cybercrime continues to increase.’

The same password for everything

Van der Plas draws a parallel with efforts to ensure home security. ‘When you go on holiday, you make sure all the doors and windows are locked, and maybe you put the lights on a timer. You ask the neighbours to keep the mail from piling up – whatever it takes to make it seem like you're at home and discourage burglars from breaking in. When it comes to digital doors and windows, on the other hand, we tend to leave all kinds of things ajar – like when carrying out the security update is inconvenient, or we thoughtlessly click on a link in a suspicious email.' Van der Plas admits that phishing emails purporting to be from banks are becoming ever more professional in appearance. ‘And if we consider young people today, they are learning online and living their lives online, playing online games with peers from all over the world. Yet members of this same generation often use the same password for different websites, social media and games. That makes them really easy targets for hackers.’

Reporting and sharing

‘We are also seeing that people have only a limited tendency to report cybercriminality at all,’ Van der Plas goes on. ‘A rough estimate says less than 10 per cent do. And at the same time, not everyone is aware that they've been victimised. Research shows that the majority of companies that are hacked don't even know it. And if they do know, they often don't report the crime to prevent reputational damage.’ According to Van der Plas, reporting and sharing information on digital vulnerabilities and trends can help provide a clearer picture of the situation. ‘That way, we in law enforcement can do more to either prevent cybercrimes or limit the consequences when they do happen.’

Van topsport naar breedtesport

Vrijwel elke strafzaak heeft tegenwoordig een digitaal component. Volgens Van Der Plas maakt dat de bestrijding van cybercrime niet alleen meer een topsport is voor een zeer gespecialiseerd team, maar ook een breedtesport. “Iedere politiecollega krijgt er mee te maken: aan de balie, wijkagenten, rechercheurs. Dus werken we er hard aan om de digitale vaardigheden en kennis van onze huidige collega’s verder te ontwikkelen. Daarnaast hebben we de komende vijf jaar 17.000 nieuwe collega’s nodig. Deze toekomstige politiemensen brengen vaak vanwege hun leeftijd en ervaring meer cyberkennis mee naar de politie.”

Mens en machine

Bij de politie worden ook stappen gezet als het gaat om datascience en kunstmatige intelligentie ofwel Artificial Intelligence (AI). Van Der Plas: “Stel: wij hebben grote hoeveelheid data van fora waar hackers contact hebben. Of we zitten op een site waar uitwisseling

away from cybercrime”. That's because we're finding not only many victims among young people, but many actual or potential culprits as well. And for young people who have already clicked their way into cybercrime, we've joined forces with the Public Prosecution Service and several private parties to launch “Hack-Right” – a digital version of the HALT programme for juvenile crime prevention. When a teenager or young adult is caught hacking, for example, they will be required to complete a traineeship with an ICT company in order to better understand the consequences of their actions. In this way, we hope to prevent further damage. As a matter of fact: past experiences with youthful hackers have proven quite positive in that some of them have become consultants helping organisations improve their cybersecurity.’

From specialists to all-rounders

These days, virtually every criminal case has a digital component. According to Van der Plas, this means that combating cybercrime is no longer a job for a highly specialised team, but rather a task for skilled all-rounders. ‘Every one of our police colleagues deals with the issue, from those with desk jobs, to community police officers to detectives. As a result, we are working hard to further develop the digital skills and knowledge of our existing colleagues. We will also need to add 17,000 new colleagues within the next five years. Thanks to their age and experience, many of these future officers will bring additional cyber-related knowledge to the police force.’

plaatsvindt van diensten voor cybercrime, denk aan gijzelsoftware of een DDoS-aanval. Met het in beslag nemen van die data haal je een hoeveelheid informatie binnen die voor geen enkel mens behapbaar is. Hoe kun je patronen ontdekken in al die informatie, hoe lopen bijvoorbeeld die criminele lijnen? Hoe verdien je aan gijzelsoftware? Je moet het immers opzetten, regelen dat het afpersgeld naar een bank gaat. Dat geld moet weer uit de illegaliteit komen. We zetten de eerste stappen op dit gebied om deze data te analyseren en te interpreteren." Van Der Plas benadrukt dat de mens altijd nodig blijft voor het analyseren en interpreteren van de gegevens, maar wél met andere vaardigheden. "We zoeken naast cyberkennis ook mensen die met deze nieuwe technieken data kunnen analyseren. Ook hier blijft de menselijke maat aan de orde: hoe zorgen we ervoor dat de collega's het nog snappen, dat zij zich verbonden blijven voelen en niet vervreemden door de invoering van technologie? Daarom hebben we in 2018 het Nationaal Politielab AI opgericht. Hier werken we samen met universiteiten om antwoord te geven op vragen als: wat kunnen we en wat mogen we als politie met kunstmatige intelligentie? En moeten we dat dan ook willen? Zo werken we met de tandem mens en machine aan een eigentijdse politie, die van vandaag en overmorgen."

People and machines

The National Police Force is also taking steps in the areas of data science and Artificial Intelligence (AI). Van Der Plas: 'Say we have collected a vast quantity of data from Internet forums where hackers get together. Or that we are monitoring a website where people trade cybercrime services such as ransomware or DDoS attacks. Seizing that data involves importing a quantity of information that no human could ever hope to process. So how can we find patterns in all that data, or connect the dots between criminal actors? To start, how does one make money using ransomware? You have to set it up and make sure the ransom payment goes into a certain bank account. That money has to be whitewashed at some point. We're now taking the first steps in this area with regard to analysing and interpreting the data.' Van der Plas emphasises that while actual humans will always be needed to analyse and interpret the data, those humans will need to have different skills in future. 'Besides cyber expertise, we're also looking for people who can apply these new technologies for the purpose of data analysis. Here, too, there is real value to be found in the human aspect: how can we ensure that our colleagues keep abreast of developments, continue to feel connected to the work and are not alienated by the introduction of new technology? In response to these issues, we founded the National Police Lab for AI in 2018. In the Lab, we team up with universities to answer questions such as: what types of artificial intelligence have possible – and lawful – applications for us to use in law enforcement? And should we be eager to use them, ethically speaking? So we're working hand in hand with people and machines to build a modern police force, both for today and many days down the line.'

"We werken met de tandem mens en machine aan een eigentijdse politie, die van vandaag en overmorgen"

'We're working hand in hand with people and machines to build a modern police force, both for today and many days down the line'

LUITENANT-GENERAAL ONNO EICHELSHEIM

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

Luitenant-generaal Onno Eichelsheim begon zijn militaire loopbaan in 1986 als cadet aan de Koninklijke Militaire Academie. Hij heeft verschillende (operationele) functies binnen Defensie vervuld. Sinds juli 2019 vervult hij als luitenant-generaal de functie van plaatsvervangend Commandant der Strijdkrachten. Sinds die maand is hij ook lid van de CSR.

Lieutenant General Onno Eichelsheim started his military career in 1986 as a cadet at the Royal Military Academy and performed various operational roles within the Ministry of Defence. Since July 2019, Eichelsheim has served as Deputy Chief of the Netherlands Defence Staff in his position as lieutenant general. In that same month he also joined the CSR as a member.

Waarom is 'cyber' belangrijk voor Defensie en in het bijzonder voor Nederland?
"Gelet op de hoofdtaken van Defensie op het gebied van de bescherming van het Nederlandse en NAVO-grondgebied, het bevorderen van de internationale rechtsorde en het ondersteunen van de civiele autoriteiten rekent ons land op Defensie als het erop aankomt. Optreden tegen digitale bedreigingen van onze veiligheid, in nationaal en internationaal verband, hoort daarbij. De internationale veiligheidssituatie verslechtert en de geopolitieke belangentegenstellingen verscherpen. Dit maakt de bijdrage die Defensie aan onze digitale veiligheid levert des te belangrijker. Defensie heeft vier entiteiten die elk een facet van het cyberdomein vertegenwoordigen: Defensie Cyber Commando (offensief en kennispartner), Defensie Cyber Security Center (security), Militaire Inlichtingen en Veiligheidsdienst (inlichtingen) en de Koninklijke Marechaussee (opsporing en handhaving)."

Wat is voor u het belang van de CSR?
"Na mijn functie als directeur MIVD kan ik concluderen dat het een absolute noodzaak is om Nederland (digitaal) veilig te maken voor de toekomst. De CSR draagt door middel van gedragen adviezen bij aan de digitale weerbaarheid van ons land. De kracht van de raad is dat vraagstukken integraal worden opgepakt. Het brede palet aan achtergronden binnen de raad en alle kennis en ervaring die daarmee gepaard gaat, zorgt ervoor dat problemen vanuit verschillende invalshoeken worden bekeken. De gedegen adviezen die hieruit volgen, worden door het kabinet opgevolgd. Dit maakt de CSR een belangrijk adviesorgaan."

Why is 'cyber' so important for the Ministry of Defence and indeed for the Netherlands as a whole?
Given the Ministry's main tasks to protect Dutch and NATO territory, promote the international rule of law and support the civil authorities, the people in this country will ultimately count on the Ministry of Defence when they need protection. So they also expect us to counter threats to our security, in a national and international context. The Ministry of Defence's contribution to our digital security has become all the more important, as the international security situation is worsening and geopolitical tensions are growing. The Ministry has four entities which each represent one facet of the cyber domain: Defence Cyber Command (offensive and knowledge partner), Defence Cyber Security Center (security), the Military Intelligence and Security Service (intelligence) and the Royal Netherlands Marechaussee (investigation and enforcement).'

Why do you consider the CSR to be important?
'Having served as director of the Military Intelligence and Security Service, I conclude that it is absolutely vital to prepare for this country's future digital security. Through its widely supported advice, the council contributes to the digital resilience of this country. The great strength of the council is that it is able to tackle issues in an integrated manner. The broad range of backgrounds of its members and all the associated knowledge and experience ensure that problems are dealt with from a holistic perspective. This results in thorough recommendations that the Cabinet cannot ignore. As such, the council is an important advisory body.'

Lieutenant General Onno Eichelsheim
Deputy Chief of the Netherlands Defence Staff at the Ministry of Defence and member of the Cyber Security Council

De digitale wereld is inmiddels een vast onderdeel van ons leven geworden met alle voordelen, gemakken en kansen die daarbij komen kijken, zowel in de persoonlijke als maatschappelijke omgeving. Daarnaast brengt de digitalisering ook uitdagingen met zich mee. De omvang en ernst van de digitale dreiging in Nederland zijn nog steeds aanzienlijk en blijven zich ontwikkelen. "Dat geldt niet alleen voor Defensie", vertelt luitenant-generaal Onno Eichelsheim, plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie en lid van de Cyber Security Raad. "Sterker nog, door het ontbreken van heldere klassieke scheidingslijnen is cyberdreiging inherent een gedeelde dreiging van individu tot samenleving, publiek en privaat. Defensie heeft hierin een belangrijke verantwoordelijkheid."

The digital world has become an integral part of our lives - with all the advantages, conveniences and opportunities that this entails, both in our personal and broader social environments. There are a number of challenges involved, however. The scope and severity of digital threats in the Netherlands remain significant and are growing. 'The problem is not limited to the Defence area', says Lieutenant General Onno Eichelsheim, Deputy Chief of the Netherlands Defence Staff at the Ministry of Defence and member of the Cyber Security Council. 'Indeed, now that many traditional dividing lines have faded, the cyber threat has become a common concern in all domains - from the individual environment to society at large, and in both the public and private sectors. The Ministry of Defence has a huge responsibility here.'

NO DIGITAL CLOUD WITHOUT THE HUMAN FACTOR

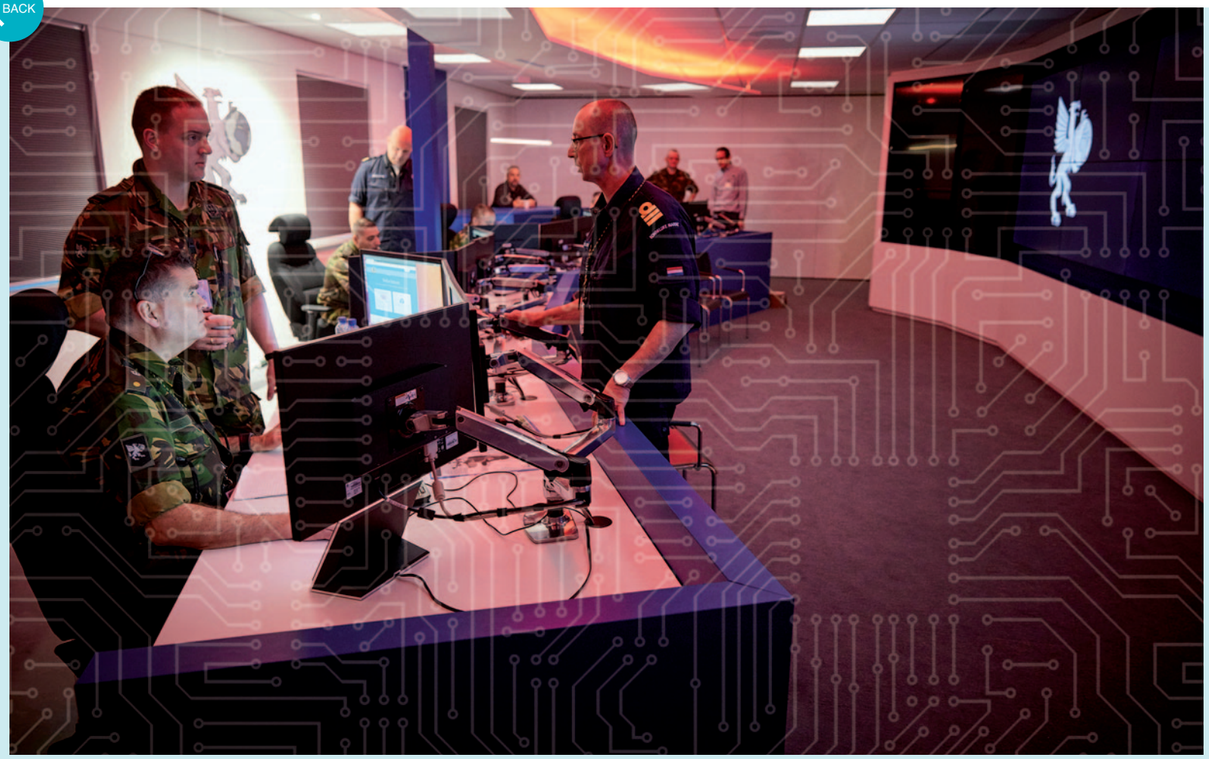
Voor Defensie was dit reden om vorig jaar een geactualiseerde versie van de Defensie Cyber Strategie (DCS) uit te brengen waarin de samenwerking tussen publieke en private organisaties een grote rol speelt. Belangrijk is de samenwerking rondom de human factor, ofwel de mens. Luitenant-generaal Eichelsheim vindt dit zelfs de belangrijkste schakel in de digitale veiligheidsketen.

In fact, it prompted the Ministry to issue an updated version of its Defence Cyber Strategy (DCS) last year, in which collaboration between public and private organisations takes centre stage. Crucially, this collaboration should focus on the human factor - in other words, on people. Eichelsheim believes this is actually the most important link in the entire digital security chain.

The Defence Cyber Strategy
Of course the DCS centres around the constitutional tasks of the armed forces - but that is not its only focus. 'Defence will ultimately have to shoulder its full responsibility, including in the cyber domain,' says Eichelsheim. 'The DCS generates digital cloud by focusing on investments in four priority areas: defensive and offensive cyber measures, cyber intelligence and collaboration. In this sense, collaboration serves as the link between the Ministry of Defence and society. While these priority areas may seem to be specific to Defence, in fact we share these issues with many other domains. That's because digital security is no longer something we can achieve on our own. We'll have to tap into the capacities, know-how and experience of others to increase resilience in all domains.'

The Ministry of Defence is currently elaborating its objectives in a detailed and practical implementation plan. Eichelsheim: 'That's why we expect the DCS will attract more publicity in the years ahead. All the actions that are being taken to achieve digital security in the Netherlands may look new, but in fact they're not new at all. With this strategy we're building on previous versions of the DCS from 2012 and the resulting activities. So we've already made considerable headway, collaborating with a variety of parties. Even so, further steps will still need to be made.'

Shared challenges – joint solutions
The days that a single party was able to counter digital threats on its own are over, says Eichelsheim, so the country needs an integrated approach - which explains the immense importance of collaboration. Is that unique? 'No, it isn't; in fact this is a major focus area of the Dutch National



“De vijver is klein en het specialisme is schaars”

‘There are not that many specialists and we're all fishing in the same small pond’

De Defensie Cyber Strategie

Met de DCS richt Defensie zich uiteraard, maar niet alleen, op de grondwettelijke taken van de krijgsmacht. “Als het erop aankomt moet Defensie, ook in het cyberdomein, haar verantwoordelijkheid nemen”, vertelt Eichelsheim. “Om digitale slagkracht te bereiken richt de DCS zich op investeringen op vier hoofdonderwerpen: defensieve- en offensieve cyber, cyber-inlichtingen en samenwerking. Samenwerking is hier de brug tussen Defensie en de samenleving. Het lijkt er wellicht op dat dit Defensie-specifieke hoofdonderwerpen zijn, maar feitelijk zijn het gezamenlijke vraagstukken. We bereiken digitale veiligheid immers niet meer alleen. We moeten integraal gebruikmaken van elkaars capaciteiten, kennis en ervaring om elkaar te versterken.”

Defensie werkt op dit moment de doelstellingen verder uit, geconcretiseerd in een implementatieplan. “De aankomende jaren zal men dan ook meer horen over de DCS”, vervolgt Eichelsheim. “De acties om een digitaal veilig Nederland te bereiken lijken allemaal nieuw, maar dat zijn ze niet. De strategie bouwt voort op de eerdere uitgaven van de DCS (2012) en de activiteiten die daar vervolgens uit zijn voortgevloeid. We hebben dus al veel stappen gezet in samenwerking met verschillende partijen. Meer stappen blijven echter noodzakelijk.”

Gedeelde uitdagingen – gezamenlijke oplossingen

Een integrale aanpak is volgens Eichelsheim noodzakelijk. Hij ziet dat niemand de digitale dreigingen nog alleen aan kan. Daarom is samenwerking voor Eichelsheim van groot belang. Is dat uniek? “Nee, het is niet uniek aangezien het een belangrijk onderwerp in de Nederlandse Cybersecurity Agenda is.
Een belangrijke factor die voor mij alle doelstellingen in de DCS en zeker ook de NCSA onmiskenbaar verbindt, is de mens ofwel de human factor. Hierbij denken we al snel aan de cyberspecialist, de nerd, de hacker. En dat is ook deels waar. Deze specialisten hebben we zeker nodig binnen Defensie om ons te kunnen wapenen tegen eventuele dreigingen. Helaas zijn we daar niet de enige in, de vijver is klein en het specialisme is schaars.” Bij deze gemeenschappelijke uitdaging komt wat Eichelsheim betreft de samenwerking nadrukkelijk om de hoek kijken. “De uitdaging vraagt om adaptieve oplossingen. Een goed voorbeeld daarvan bij Defensie is de inzet van cyberreservisten.”

Eichelsheim legt uit dat cyberreservisten hun dagelijks specialistenwerk combineren met een parttime baan binnen Defensie. “Sinds 2018 heeft het Defensie Cyber Commando de CYBERRES-eenheid waar cyberspecialisten zijn ondergebracht”, vertelt Eichelsheim. “De reservisten werven we binnen het bedrijfsleven; het wervingsprogramma is zelfs in samenwerking met het bedrijfsleven opgezet. Het ontwikkelen van kennis en de inzet van capaciteiten is de win-win van deze samenwerking. De cyberreservisten zetten we in binnen de krijgsmacht. De kennis en ervaring die zij opdoen, nemen ze mee terug naar hun eigen organisatie. Ik zie dit soort adaptieve samenwerkingen noodzakelijkerwijs groeien in ons gezamenlijk belang.”

De human factor als zwakke plek

Naast de cyberspecialist is voor Eichelsheim ook de ‘gewone’ dagelijkse gebruiker van digitale middelen een belangrijk onderdeel van de human factor. Eichelsheim: “Naast technische bedreigingen is de mens zelf vaak een zwakke plek in de beveiliging. Veelal onbewust doen we dingen, al dan niet extern geïnitieerd, die ons en onze systemen kwetsbaar maken. De medewerker beweegt zich privé natuurlijk ook in het digitale en maatschappelijke domein.”
Daarom vindt Eichelsheim het belangrijk om aandacht te blijven besteden aan die ‘gewone’ medewerker die we allemaal hebben binnen onze organisatie. “Samenwerking kan hierbij nadrukkelijk meerwaarde opleveren. We hebben een gezamenlijke verantwoordelijkheid in het weerbaar maken van de maatschappij op het vlak van cybersecurity. Zo dienen we een gedeeld belang, het veilig houden van Nederland. We zijn immers zo sterk als onze zwakste schakel. We kunnen van elkaar leren en moeten niet solistisch op zoek gaan naar oplossingen. Het uitwisselen van praktijkvoorbeelden en *lessons learned* is wat mij betreft dan ook cruciaal.”

Eichelsheim benadrukt dat de kracht tevens zit in het consistent herhalen van een gezamenlijke (publiek-private) boodschap om de maatschappelijke bewustwording te verhogen. “Het is mij in ieder geval gedurende mijn loopbaan duidelijk geworden dat investeren in de awareness van de medewerker een belangrijke schakel is in onze digitale veiligheid. Binnen Defensie besteden we dan ook specifiek aandacht aan deze kant van de human factor. Zo geven we iedere medewerker een awareness training, het ‘digitale rijbewijs’, waarbij zij bewust worden gemaakt van cyberdreigingen en wat ze daarmee moeten doen. Daarnaast worden binnen de organisatie cursussen gegeven die dieper ingaan op awareness. Ik merk dat door deze inspanningen defensiemedewerkers anders omgaan met het gebruik van bijvoorbeeld sociale media en dat is goed nieuws.”

Veilig houden wat ons dierbaar is

Binnen Defensie wordt dus nadrukkelijk aandacht besteed aan het uitbreiden en bestendigen van de digitale veiligheid van Nederland. Volgens Eichelsheim kan dit alleen door samenwerking, zowel interdepartementaal als met de publieke, private en wetenschappelijke omgeving. “De brug die ik nadrukkelijk zoek, en die ons blijvend verbindt, is samenwerking. Niemand van ons kan de huidige en toekomstige dreigingen alleen pareren. De mens speelt daarin voor mij een dominante rol en de human factor is waar we gezamenlijk aan moeten blijven werken om te beschermen wat ons dierbaar is en om de BV Nederland te versterken.”

Meer informatie over de mogelijkheden rondom cyberreservisten vindt u via www.werkenbijdefensie.nl/cyberreservist-worden

BACK TO TOP

Cybersecurity Agenda. One major aspect that clearly connects all the objectives of the DCS and certainly also those of the NCSA is the human factor - by which I mean, people. And that's not just the cyber specialists, the nerds and hackers. Of course, they're involved too. We absolutely need such specialists at the Ministry of Defence to be able to ward off any threats. But we're not the only party with such needs. There are not that many specialists and we're all fishing in the same small pond.’ That, says Eichelsheim, is what makes collaboration so crucial in our attempts to counter this shared threat. ‘It’s a challenge that calls for adaptive solutions. For example, take the deployment of cyber reservists at the Ministry of Defence.’

Cyber reservists, Eichelsheim explains, are able to combine their specialist tasks with a part-time job at the Ministry. ‘In 2018, Defence Cyber Command launched its CYBERRES unit for cyber specialists. We recruit the reservists within the business community; in fact, we set up the recruitment programme in collaboration with businesses. It's a win-win situation, as all the parties involved benefit from the knowledge we develop in this way and the capabilities we deploy. We use the cyber reservists for tasks within the armed forces, where they will gain knowledge and experience that they can also use in their own organisations. These kinds of adaptive collaborations are inevitable and they're growing, which is in our collective interest.’

The human factor as the weakest link

Besides the cyber specialist, another crucial component of the human factor, says Eichelsheim, is the ‘ordinary’ individual who uses digital tools on a daily basis. Eichelsheim: ‘Alongside technical threats, a weak spot in our security defences tends to be the individual user. As users we do all sorts of things, often unwittingly, and possibly prompted by external factors, that increase our own vulnerability and that of our systems. Of course, employees also enter the digital and societal domain in a private capacity.’ That is why Eichelsheim believes it is important to retain our focus on the ‘ordinary’ employee within any organisation. ‘Collaboration can have a very clear added value in this regard. After all, we share responsibility for increasing society's resilience in terms of cybersecurity - to promote a shared interest, which is to keep the Netherlands safe. We're only as strong as the weakest link in our chain. We can learn from each other and should avoid looking for solutions without involving others. I really believe that exchanging examples from practice and lessons learned is absolutely crucial.’

Our strength, Eichelsheim emphasises, also lies in consistently repeating a common public-private message to raise awareness. ‘What I've learned in my career is that investing in awareness among individual employees is an important link in our digital security. That's why we're focusing specifically on this aspect of the human factor at the Ministry of Defence. For example, every employee completes an awareness training programme for a digital 'driving licence' to alert them to cyber threats and how to deal with them. We also provide internal courses for more in-depth awareness training. One effect of these efforts is that Defence employees have adapted their approach to social media. That's good news.’

Protecting the things we cherish

So it is clear that within the Ministry of Defence there is a great deal of attention for expanding and consolidating digital security in the Netherlands. According to Eichelsheim this can only be achieved through collaboration - both among the various government ministries and with the public, private and academic communities in society at large. ‘The bridge that I am so emphatically trying to find and that will unite us permanently is collaboration. None of us is able to ward off existing and future threats all on his own. In my view, human beings play a dominant role in this regard, which is why we'll need to continue sharing our focus on the human factor to protect the things we cherish and strengthen the Dutch economy.’

For more information about training as a cyber reservist, visit www.werkenbijdefensie.nl/cyberreservist-worden

WIEBE DRAIJER

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

Wiebe Draijer (54) is bestuursvoorzitter van de Rabobank en bestuurslid van de Nederlandse Vereniging van Banken. In juni 2019 werd Draijer benoemd als lid van de CSR namens de financiële sector.

Wiebe Draijer (54) is the chairman of the Managing Board of Rabobank and a member of the Board of the Dutch Banking Association. In June 2019, he was appointed to the Cyber Security Council as a representative of the financial sector

Waarom is 'cyber' een belangrijk thema binnen de financiële sector?
"Doordat we altijd bezig zijn met geld en financiële transacties zijn we een grote pot met honing voor criminelen. Voor cybercriminelen is dat niet anders. Die proberen alleen niet met behulp van een koevoet een bank binnen te komen, maar gebruiken hele obscure technologische manieren en constructies. We moeten hen een stap voor zien te blijven. Op het gebied van cyber moeten we daarom als sector voorop lopen."

Wat is voor u het belang van de CSR?
"We kunnen met de raad zaken agenderen en verder helpen. Het is soms opzienbarend hoe onvoorbereid veel organisaties en bedrijven waren en zijn op dit terrein en hoe onbewust men is van het risico dat men loopt. Bijvoorbeeld in het MKB rondom Intellectual Property (IP) in de landbouw, toevallig een onderwerp waar we bij de Rabobank ook veel mee bezig zijn. Onze landbouwkennis is juridisch goed beveiligd, maar extreem kwetsbaar voor cybercriminaliteit. Een rapport zoals Herna Verhagen onder andere in opdracht van de raad daarover heeft afgeleverd is daarom heel belangrijk: haar diagnose was spot on."

Wat is uw persoonlijke speerpunt binnen de CSR?
"Dat is de ontwikkeling en introductie van veilige identificatiemiddelen voor het maatschappelijke domein. Ik denk dat authenticatie een terrein is waar we al heel ver mee zijn. Er is technologie beschikbaar en daar maken wij binnen de financiële sector ook al gebruik van. Waarom is dit dan zo moeilijk te vertalen naar andere diensten? Dat is een terrein waarin ik me ga verdiepen als lid van de CSR. Volgens mij zijn we hierin verder dan het publieke debat laat zien."

Why are cyber issues important within the financial sector?
'As everything in the financial sector revolves around money and financial transactions, we act like a huge magnet for criminals. This includes cybercriminals. The only difference is that rather than forcing their way into a bank with a crowbar, cybercriminals use obscure technologies and set-ups. We really need to stay ahead of them. This is why it is crucial for us to take the lead as a sector in the cyber field.'

Why do you consider the CSR to be important?
'The CSR enables us to place issues on the agenda and help them forward. It's quite surprising to see how many organisations and companies are and have always been careless in this regard, and how little they are aware of the risks they are running. Take the issue of Intellectual Property in agriculture SMEs – which happens to be a subject we're involved in with quite intensively here at Rabobank. While our expertise in the field of agriculture is very well protected in a legal sense, it remains extremely vulnerable to cybercrime. That's what makes reports like the one delivered by Herna Verhagen on behalf of the council and others so important. Her diagnosis was spot on.'

What is your own main area of focus within the CSR?
'My main focus is the development and introduction of safe means of identification in the public domain. We've made enormous progress in the field of authentication. The technologies are available and we're already using them in the financial sector. So why is it proving so hard to translate this to other services? That's an issue I am going to investigate as a member of the council. I think we're further ahead in this area than is commonly assumed in the public debate.'

Wiebe Draijer
Chairman of the Managing Board of Rabobank, member of the Board of the Dutch Banking Association and member of the Cyber Security Council

Wiebe Draijer is bestuursvoorzitter van de Rabobank en bestuurslid van de Nederlandse Vereniging van Banken. In juni 2019 werd Draijer benoemd als lid van de Cyber Security Raad namens de financiële sector. Een sector waarin de strijd tegen cybercriminaliteit hoog op de agenda staat: "Het is als dansen met de vijand. Je moet steeds drie stappen slimmer zijn en kunnen voorspellen wat er morgen staat te gebeuren. Als Nederlands bancair stelsel zijn we daar goed en proactief mee bezig."

Wiebe Draijer is the chairman of the Managing Board of Rabobank and a member of the Board of the Dutch Banking Association. In June 2019, he was appointed to the Cyber Security Council as a representative of the financial sector – where efforts to combat cybercime are high on the agenda. 'It's like dancing with the enemy. It is crucial that you stay ahead of them, that you outwit them and anticipate their next move. The Dutch banking sector is quite effective and proactive in doing just that.'

THE FINANCIAL SECTOR IS A MAGNET FOR CRIMINALS

Spotlight
De financiële sector staat volgens Draijer doorlopend in de spotlight van criminelen en criminele organisaties, maar ook van statelijke actoren. "We zijn altijd bezig met geld, waarde en transactionele diensten. Een grote pot met honing voor criminelen. We bevinden ons daardoor in meerdere opzichten aan de voorkant van wat er speelt in de wereld op het gebied van cybersecurity en cybercriminaliteit. Dat betekent aan de ene kant dat we elke dag bezig zijn om de ontwikkelingen bij te houden en om criminelen een stap voor te zijn. Daarnaast vervult de financiële sector een poortwachtersrol in het tegengaan van cybercrime gerelateerde aspecten, zoals helderheid over herkomst vermogen, witwaspraktijken en de veilige introductie van de richtlijn PSD2. Dat vraagt om goede regulering, nieuwe technologische ontwikkelingen, en constante oplettendheid."

Goede samenwerking is daarvoor onmisbaar. "Dat doen we zowel op formeel als informeel niveau en met verschillende partijen", aldus Draijer. "Formeel werken financiële instellingen bijvoorbeeld samen in het Financieel Expertise

Magnet
The financial sector never ceases to attract the interest of criminals, criminal organisations and nation-state actors alike, says Draijer. 'In this sector everything revolves around money, value and transactional services. It really is a magnet for criminals. As a result, we're right on the front line of what's going on in the world of cybersecurity and cybercrime. That means we're working each and every day to keep abreast of developments and remain ahead of criminals. At the same time, the financial sector serves as a gatekeeper in combating cybercrime-related practices, for example by demanding clarity about the origins of capital, fighting money laundering practices and ensuring the safe introduction of the revised Payment Services Directive. This calls for effective regulation, new technologies and constant vigilance.'

To achieve that, effective collaboration is essential. 'We collaborate both in formal and informal settings, and with a variety of parties', says Draijer. 'At the formal level, for instance, financial institutions have joined forces in the Financial Expertise Centre (FEC) and there are specific public-private initiatives such as FI ISAC for the confidential exchange of information about incidents, threats, vulnerabilities and best practices.' Alongside that there are numerous informal contacts between institutions and with public bodies. Draijer: 'That's really important. Given the speed of developments within cybersecurity and cybercrime, it's crucial for the right people to be able to find each other immediately. And we really act shoulder to shoulder as sector partners in those collaborative projects, so that we can all learn from each other directly. That's clearly a shared interest.'

It is not just criminals however, but also the media that closely monitor the financial sector. Media reports about the sector appear almost on a daily basis. But that's all in the game, says Draijer. 'Cybercrime in the financial sector is a hot topic, and financial institutions are more or less a sitting target. I'm not sure if that's entirely fair, but we do recognise the urgency there and

Centrum ofwel FEC en zijn er specifieke publiek-private initiatieven zoals de FI ISAC, waarin we (vertrouwelijk) informatie uitwisselen over incidenten, bedreigingen, kwetsbaarheden en *best practices*." Daarnaast is er ook veel informeel contact tussen instellingen en met overheidsorganisaties. "Dat is ook nodig", vindt Draijer. "Voor een onderwerp waarbinnen de ontwikkelingen zo razendsnel gaan als cybersecurity en cybercrime, is het belangrijk dat de juiste mensen elkaar snel weten te vinden. We staan in die samenwerkingen als sector ook echt schouder aan schouder, zodat we direct van elkaar kunnen leren. Er is een duidelijk gedeeld belang."

De financiële sector staat niet alleen in de spotlight van criminelen maar ook van de media. Zij berichten bijna dagelijks over het onderwerp. Dat is volgens Draijer echter niet iets om verongelijkt over te zijn. "Cybercrime in de financiële sector is een *hot topic* en als financiële instellingen zijn wij geregeld de kop van jut. Je kan dat oneerlijk vinden, maar dit is juist een terrein waar we de directe noodzaak zien en onze verantwoordelijkheid nemen. Hier moeten we voorop lopen en daarom hebben we ook flinke stappen gezet. Daar kunnen we trots op zijn."

Dillema's

Cybersecurity in de financiële sector brengt ook dilemma's met zich mee. Daar is Draijer zich maar al te goed van bewust. "We hebben als bank een verantwoordelijkheid om innovatie aan te jagen en ten dienste te staan van klanten en tegelijkertijd moeten we blijven bedenken hoe criminelen hier misbruik van kunnen maken. Denk bijvoorbeeld aan onze Rabo-scanner. We hebben daarmee een van de veiligste manieren van online betalen ter wereld geïntroduceerd, maar hoe zorgen we tegelijkertijd voor het grootste gebruiksgemak? Daar moeten we constant de balans in blijven zoeken. Veel innovaties zijn gericht op het verhogen van gemak, maar gemak mag niet overslaan in een lagere drempel voor criminelen om daar misbruik van te maken."

De strijd tegen cybercriminaliteit en voor cybersecurity brengt volgens Draijer ook een aantal ethische dillema's met zich mee. "Het is gemakkelijk om cybercriminaliteit heel zwart-wit te zien, maar het is veel complexer dan dat. Neem bijvoorbeeld de blockchain-technologie en cryptocurrency zoals Bitcoin. Bitcoin wordt inmiddels door veel mensen gezien als een middel waar cybercriminelen misbruik van maken. Tegelijkertijd zitten er heel veel voordelen in de technologie van blockchain en Bitcoin voor allerlei toepassingen. Hoe moet je dan als financiële instelling omgaan met zo'n technologie? Het is voor ons een uitdaging om daar de tanden in te zetten."

Authenticatie en de menselijke kant

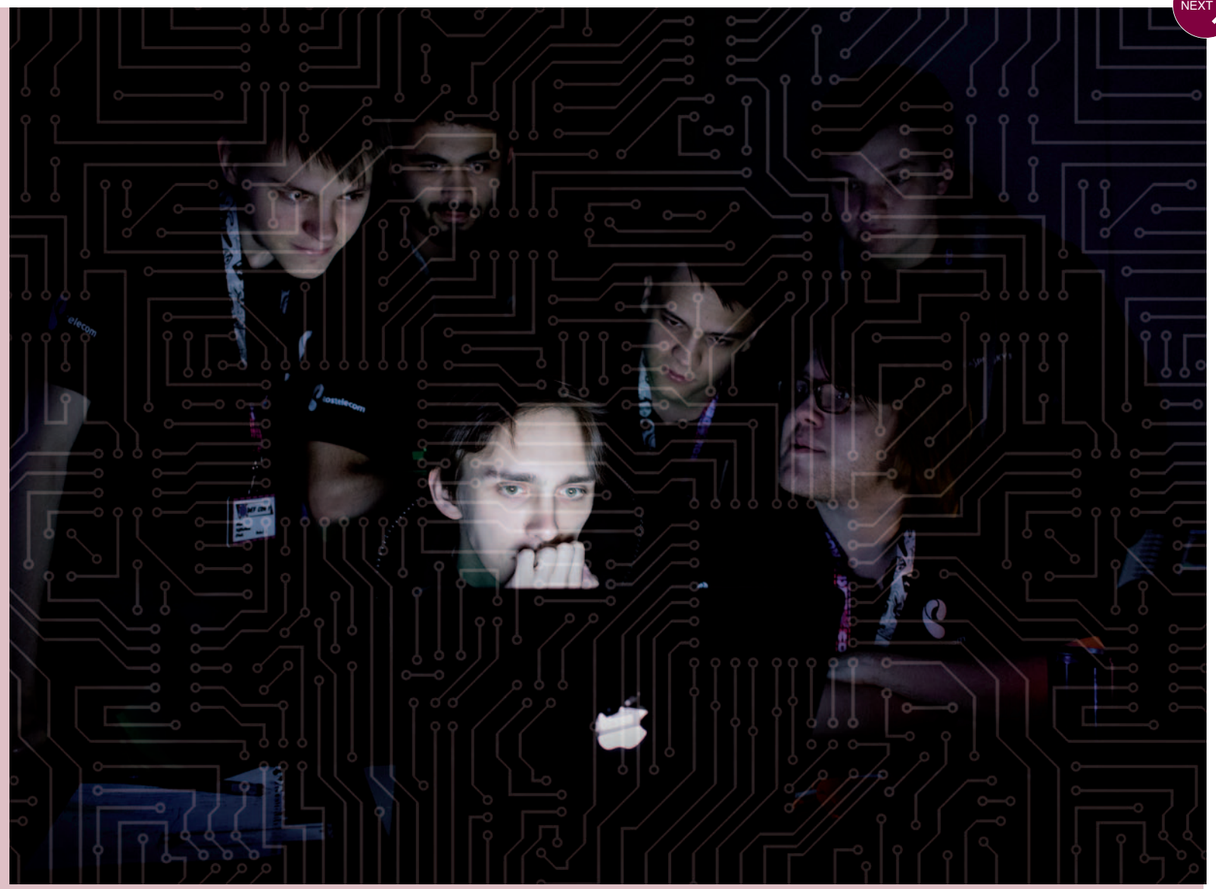
Sinds juni 2019 is Draijer namens de financiële sector ook lid van de Cyber Security Raad. Een van zijn aandachtspunten is de ontwikkeling en introductie van veilige identificatiemiddelen in het maatschappelijke domein. Die middelen kunnen een belangrijke rol vervullen in de strijd tegen cybercriminaliteit. "Ik denk dat authenticatie een terrein is waar we al heel ver mee zijn", zegt Draijer. "Er is technologie beschikbaar en daar maken wij binnen de financiële sector ook al gebruik van. Waarom is dit dan zo moeilijk te vertalen naar andere diensten? Dat is een terrein waarin ik me ga verdiepen als lid van de CSR. Volgens mij zijn we hierin verder dan het publieke debat laat zien."

En wat te denken van de menselijke kant van cybersecurity? Volgens Draijer is daar nog veel ontwikkeling in nodig. "In een van mijn vorige banen als consultant deed ik ooit onderzoek naar menselijk gedrag, waarbij we een matrix ontwikkelden met op de X-as de mate van werkelijk risico en op de Y-as de hoogte van het gepercipieerde risico. Linksboven stond vliegen, terwijl dat juist een van de veiligste manieren van transport is. Rechtsonder vond je de huiselijke omgeving, terwijl juist enorm veel ongelukken gebeuren op bijvoorbeeld een keukentrapje. Als je die matrix nu zou maken voor cybersecurity, dan kan je menselijk gedrag vergelijken met dat keukentrapje. Men onderschat het risico. De manier waarop we omgaan met wachtwoorden, updates, onze camera en de installatie van beveiligingssoftware is cruciaal. Het zijn kleine dingen die grote effecten hebben."

Als leidinggevende van een financiële instelling begrijpt Draijer dit maar al te goed, daarom investeert zijn bank in bewustwording en trainingen voor zowel medewerkers als klanten. "Het gaat vaak echt om de dagelijkse dingen die ervoor zorgen dat je veilig bent. Hoe vaak verander je je wachtwoord? Heb je goede bescherming? Kijken mensen mee op je scherm in de trein? Daarom hebben we voor medewerkers interne trainingen, voeren we bewustwordingscampagnes en doen we praktische updates. Ook testen we onszelf geregeld. We zijn daardoor bijvoorbeeld met een andere bril naar onze organisatie en medewerkers gaan kijken. Denk aan de manier waarop we medewerkers screenen en maatregelen die we nemen om kwetsbaarheden zoveel mogelijk in te dammen. Ook onze klanten zijn een belangrijke doelgroep in onze aanpak. We leren hen altijd te dubbelchecken wanneer ze een betaalverzoek of e-mail krijgen met een factuur en waarschuwen hen voor bestaande en nieuwe technieken van cybercriminelen."

"Vaak hebben kleine dingen grote effecten"

'Small issues often have a huge impact'



BACK TO TOP

shoulder our responsibility. We need to take the lead there and have actually made significant strides already. We have reason to be proud of that.'

Dilemmas

Cybersecurity in the financial sector has also created a number of dilemmas. Draijer is very much aware of that. 'As a bank, we have a responsibility to drive innovation and serve our clients, while remaining alert to any loopholes that would allow criminals to abuse those services. Our own Rabo scanner is a case in point. With it, we've introduced one of the safest online payment systems in the world, but we'll constantly have to balance this against the need to ensure optimum user-friendliness for our clients. Many innovations aim to increase user-friendliness, but we should take care that by making services easier to use we do not also lower the threshold for abuse.'

According to Draijer, the efforts to fight cybercrime and promote cybersecurity also entail a number of ethical dilemmas. 'We tend to view cybercrime as a black-and-white issue, but actually it's a lot more complex than that. For example, consider blockchain technology and cryptocurrencies such as Bitcoin. Many people are now aware that the bitcoin system is open to abuse by cybercriminals. At the same time however, blockchain and bitcoin technologies offer a wealth of benefits for a whole range of applications. So as a financial institution we need to find a way to deal with such technologies. That's a real challenge for us to tackle.'

Authentication and the human aspect

In June 2019, Draijer joined the Cyber Security Council as a member on behalf of the financial sector. In that role, one of his areas of focus is the development and introduction of safe means of identification in the public domain. Those means potentially play an important role in the battle against cybercrime. 'We've made enormous progress in the field of authentication', says Draijer. 'The technologies are available and we're already using them in the financial sector. So why is it proving so hard to translate this to other services? That's an issue I am going to investigate as a member of the council. In fact I think we're further ahead in this area than is commonly assumed in the public debate.'

As for the human aspect of cybersecurity, Draijer believes there is still a great deal of progress to be made. 'In one of my previous jobs as a consultant I conducted research into human behaviour. We developed a matrix plotting the actual risk on the X axis and the perceived risk on the Y axis. Flying ended up in the top-left quadrant, even though it is actually one of the safest forms of travel. And the home environment ended up bottom-right, despite the enormous number of accidents happening just there, on your stepladder in the kitchen for instance. If we were to make a similar matrix for cybersecurity risks, human behaviour would take the place of that stepladder. People tend to underestimate the risk. The way we deal with passwords, updates, our camera and security software is crucial. These are all small issues but their impact is huge.'

A senior executive of a financial institution, Draijer is all too aware of that, and that is why his bank is investing in training for both employees and clients. 'More often than not, out digital security depends on simple, everyday precautions. For example, how often do I change my password? Am I well protected? Does anyone watch my screen when I'm travelling on the train? We provide internal training courses for our staff, run awareness campaigns and perform practical updates to eliminate risks of this nature. We also run regular tests of our own practices, which has made us view our own organisation and our employees from a different perspective, for instance in terms of our staff screening practices and the measures we take to minimise vulnerabilities. With our approach we also, and crucially, target our clients, teaching them to always double-check payment requests or emails with an enclosed invoice, and alerting them to existing and novel techniques used by cybercriminals.'

MARC VAN DER LINDEN

Nieuw lid van de Cyber Security Raad (CSR)

New member of the Cyber Security Council (CSR)

Sinds februari 2017 is Marc van der Linden de CEO van Stedin Groep. Daarvoor was hij lid van de raad van bestuur van Eneco. Bij Eneco bekleedde Van Der Linden diverse functies waaronder die van directeur van Eneco Energy Projects, directeur van Eneco Installatiebedrijven en directeur van Eneco Wind. Van Der Linden is tevens voorzitter van Netbeheer Nederland. Sinds eind 2018 is hij lid van de CSR.

Marc van der Linden has been CEO of Stedin Group since February 2017. Before that, he was a member of Eneco's Executive Board. Van der Linden held various positions at Eneco, including that of director of Eneco Energy Projects, director of Eneco Installation Companies and director of Eneco Wind. Van der Linden is also chair of Netbeheer Nederland. He has been a member of the Cyber Security Council since late 2018.

Waarom is 'cyber' een belangrijk thema voor de vitale sectoren en Stedin specifiek?

"Een goede energievoorziening is cruciaal voor het functioneren van de Nederlandse maatschappij. Als de dreigingen toenemen, dan neemt voor ons ook het belang toe om onze infrastructuur goed te beschermen. Daarnaast hebben wij ook een zorgplicht om de persoonsgegevens van onze klanten te beschermen."

Wat is voor u het belang van de CSR?

"Het sterke van de CSR is dat de raad is samengesteld uit experts vanuit de wetenschap, de publieke - en private sector. Die driehoek maakt het mogelijk om strategische vraagstukken en knelpunten vanuit verschillende perspectieven te bekijken en hierop een integrale visie te ontwikkelen. Ook het zoeken van de samenwerking met vergelijkbare organisaties in andere landen heeft voor ons een sterke meerwaarde, want ook de energie-infrastructuur houdt zich niet aan landsgrenzen."

Why are cyber issues important to the critical sectors and to Stedin in particular?

'An effective energy supply is crucial to the functioning of Dutch society. As threats increase, so too does the importance of protecting our infrastructure. We also have a duty of care when it comes to protecting our customers' personal data.'

Why do you consider the CSR to be important?

'The CSR's strength is that it is made up of experts from scientific practice and the public and private sectors. That triad enables us to examine strategic issues and obstacles from various perspectives and to develop an integrated vision in response. We also feel there's strong added value in seeking out cooperation with similar organisations in other countries, as the energy infrastructure isn't constrained by national borders.'

Marc van der Linden
CEO of Stedin Group and member of the Cyber Security Council

De mens is juist de sterkste schakel in de strijd tegen cybercriminaliteit, vindt Marc van der Linden, CEO van Stedin Groep. Sinds drie jaar zwaait hij de scepter bij het Rotterdams netwerkbedrijf en verlegde met een nieuwe strategie Stedins focus op toekomstig netbeheer. En daar past aandacht voor cybersecurity uitstekend bij.

People are in fact the strongest link in the fight against cybercrime, says Marc van der Linden, CEO of Stedin Group. He's been in charge of the Rotterdam-based grid operator for three years now and has introduced a new strategy that is shifting Stedin's focus to future grid management. Which fits in well, obviously, with attention to cybersecurity.

YOUR STRONGEST GATEKEEPERS ARE YOUR STAFF

Samenwerken met netbeheerders

Cybersecurity heeft bij Stedin de hoogste prioriteit. Met de toename van de dreiging hiervan nemen ook de voorzorgsmaatregelen toe. "Het is een soort wedloop", vertelt Van Der Linden. "Als netbeheerder werken we veel samen met de andere netbeheerders. Die samenwerking heeft twee doelstellingen. We willen de weerbaarheid van onze energiesystemen hoog en gelijk houden, zodat er binnen de netbeheerders geen zwakke broeders zijn. En we willen onze (schaarse) middelen niet dubbel inzetten. Het helpt niet als we onafhankelijk van elkaar wielen uitvinden of onnodige inkopen doen."

Cooperation with grid operators

At Stedin, cybersecurity is a top priority. As the threat of cybercrime expands, so too do the preventative measures. 'It's a kind of arms race,' Van der Linden says. 'As a grid operator, we frequently cooperate with the other grid operators out there. This cooperation is aimed at two objectives. We want to keep the resilience of our energy systems high and uniform, so there are no weak links among the grid operators. And secondly, we want to avoid redundancy in how we apply our scarce resources. No one benefits when we all try to invent the wheel for ourselves or make unnecessary purchases.'

Van der Linden emphasises the fact that electrical cables don't stop at national borders. 'In our sector, there's an infamous case involving Ukraine. In late 2015, a (most likely) Russian cyberattack shut down several energy plants, causing a blackout that affected all of Western Ukraine. Such events make European cooperation a vital necessity – and for that reason we've set up the Energy Network Cyber Security, or ENCS. Many European grid operators are members. We all share experiences and set up joint research projects.'

Human factor

Recently, Stedin Group was alarmed to find itself the target of a cyberattack that relied on phishing emails asking for log-in details. Van der Linden: 'When you have 4,000 people working at your company, you know that such emails will get at least a handful of responses. Still, the phishing scam

Van Der Linden benadrukt dat elektriciteitskabels niet stoppen bij de grenzen. “In onze wereld is de casus van Oekraïne infaam. Eind 2015 legde een (vermoedelijk) Russische cyberaanval enkele energiecentrales plat, waardoor West-Oekraïne zonder stroom zat. Daarom is Europese samenwerking ook een noodzaak en dat doen we in het Energy Network Cyber Security ofwel ENCS. Hierin zitten veel Europese netbeheerders. We delen ervaringen en stippelen gezamenlijke onderzoeken uit.”

Human factor

Onlangs werd Stedin Groep opgeschrikt door een cyberaanval middels phishing e-mails waarin om inloggegevens gevraagd werd. Van Der Linden: “Als er 4000 mensen bij je bedrijf werken, dan weet je dat ze wel een paar keer beet hebben. Die phishing-actie heeft er toe geleid dat wij versneld een extra controlesysteem hebben ingebouwd in ons bedrijf: een extra verificatie via je werktelefoon.”
Van Der Linden vindt het belangrijk dat als collega’s beseffen dat ze opgelicht zijn via zo’n phishing e-mail om het slachtoffer te ondersteunen, de schade te beperken en door te gaan met de bedrijfsvoering. “Iedereen kent het gevoel van schaamte, want iedereen is wel eens opgelicht. Het is belangrijk dat je het taboe afhaalt van de slachtofferrol. Juist dan moet je als leidinggevende schouder aan schouder staan met het slachtoffer.”

Van Der Linden gelooft niet dat mensen de zwakste schakel zijn in het systeem. “Je kunt veel afvangen door techniek, maar uiteindelijk zijn de medewerkers je beste filters. Ze zijn juist je sterkste poortwachters. In die positie moet je ze wel brengen. Want techniek alleen lost niet alles op. Je kunt allerhande tools aanreiken. Maar je moet ook weten hoe je die spullen moet gebruiken. Vergelijk het met autorijden. Die gordel en die spiegels zijn niet veilig, maar het *gebruik* ervan.”

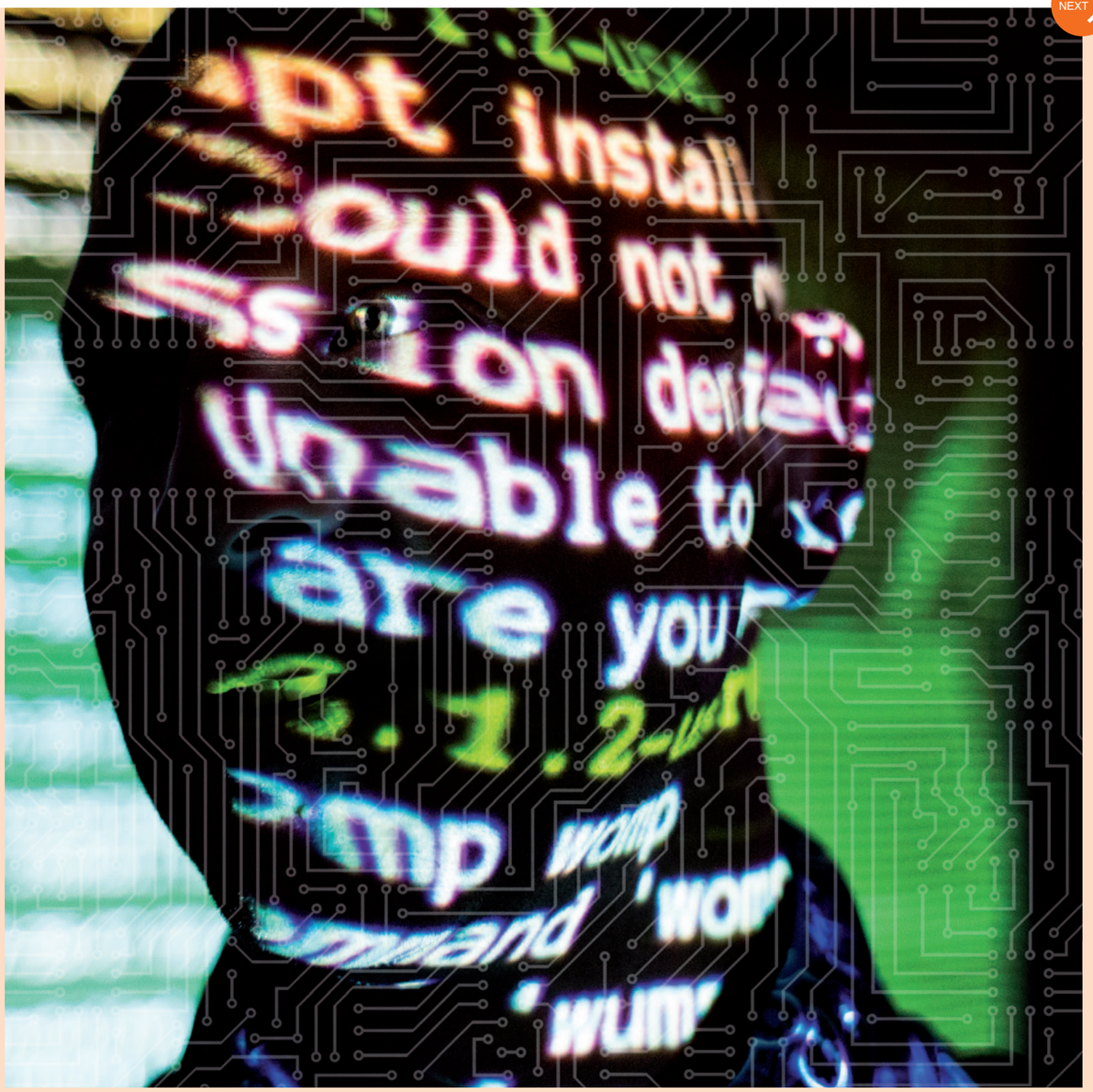
Jong geleerd

Mede hierom zijn binnen Stedin alle medewerkers door een e-learningproces geleid. “En die kennis en vaardigheden onderhouden we”, vervolgt Van Der Linden. “Van nieuwe medewerkers wordt ook verlangd dat zij deze cursus volgen. Het maakt je scherper en creëert awareness. Het e-mailadres van de verzender standaard checken, niet automatisch op linkjes klikken of attachments openen. Het zijn kleine tips, maar als iedereen binnen het bedrijf het tussen de oren heeft, dan hou je een hoop ellende buiten de deur.”

Van Der Linden zou het niet gek vinden als we in Nederland nog vroeger zouden beginnen met die awareness. “Vroeger op de basisschool moest je je verkeersdiploma halen van Veilig Verkeer Nederland. Waarom doen we niet ook zoiets in het cyberdomein: dat je uiteindelijk een diploma krijgt, zodat je weet hoe je je veilig digitaal kunt rondbewegen?”
Die awareness zetten ze bij Stedin niet alleen van onderuit in, maar ook vanuit de top. “Afgelopen maand vond onze halfjaarlijkse strategische sessie plaats met onze Raad van Bestuur en alle directeuren. Daarin hebben wij een volle middag besteed aan cyberdreigingen en de rol van het Stedin-bestuur daarin. We hebben de Oekraïne-hack uitvoerig gesimuleerd en stap voor stap bekeken welke acties wij al hebben genomen om dit scenario – dat zich uiteraard gradueel ontvouwde – te voorkomen. Ook hier stond de human factor centraal: hoe kunnen wij onze mensen ondersteunen?”

“Moet je Russische en Chinese softwarebedrijven bij voorbaat uitsluiten?”

‘Should Russian and Chinese software providers be excluded from even participating?’



did prompt us to accelerate the roll-out of an additional internal control system: an extra verification step via employees’ work phones.'
Van der Linden feels it’s important to support colleagues once they know they have fallen victim to a phishing email, and to help limit the damage and carry on with operational tasks. 'We all know the feeling of shame, since everyone has been scammed at one point or another. It's important to lift the taboo surrounding victimisation. Especially in cases like this, it's important for the manager to express solidarity with the victim.'

Van der Linden doesn't believe that people are inevitably the weakest link in any system. 'While it's true that technology can deflect a lot of problems, ultimately your employees are the most effective filters you have. They're your strongest gatekeepers. You do have to position them that way, though, because technology alone won't solve all your problems. You can provide all kinds of tools, but you also need to know how to use them properly. Think of it like a car. The seatbelt and mirrors don't make the car safe – actually *using* them does.'

Early start

This is part of the reason that all Stedin employees are required to complete an e-learning programme. 'We work to keep the knowledge and skills they gain up to date,' Van der Linden continues. 'New employees are expected to complete the course as well. It makes them more vigilant and creates awareness of the need to always check the e-mail address of the sender and avoid automatically clicking on links or opening attachments. These are simple tips, but if everyone in the organisation has committed them to memory they can save you a great deal of trouble.'

Van der Linden doesn't see any reason why we shouldn't get an early start on cultivating awareness in the Netherlands. 'Primary-school children used to be required to earn an official traffic safety diploma. Why shouldn't we have something similar for cyber issues – let children work towards a diploma so that they know how to safely navigate in the digital world?' At Stedin, that awareness is cultivated not only at the lower levels but in the uppermost echelons of the company as well. 'We held our semi-annual strategic session last month, with the Executive Board and all directors in attendance. An entire afternoon was dedicated to cyber threats and the role of Stedin's administrators in that regard. We created a detailed simulation of the Ukraine hack and examined, step by step, the actions we have already taken to prevent such a situation, which naturally unfolded gradually. Here, too, the human factor was a primary concern: how can we best support our people?'

Sector-transcending

As a grid operator, Stedin is well aware of its role and responsibility in helping the Netherlands arm itself against cyberattacks. Van der Linden: 'In consultation with our supervisory authority, the Radiocommunications Agency Netherlands, we are seeking the most effective way for us to fulfil our duty of care. To that end, we're quite pleased with the Network and Information Systems Security Act (Wbni), as it offers us plenty of tools for doing so. The Act sets out a reporting obligation and a duty of care in terms of implementing security measures. It's a way to exchange information regarding the threats already at play in one sector but not yet in another.'

Van der Linden recognises the value of this sector-transcending approach. Stedin Group is therefore taking part in the Critical Infrastructure Committee, which was set up on the initiative of VNO-NCW. 'The committee's common denominator is critical infrastructure: finance, telecom, water and major industries,' Van der Linden continues. 'Within the committee, we discuss matters such as the tension that exists between the need to have an open tender procedure and the need to protect ourselves from threats by state actors. What's the best approach? Should Russian and Chinese software providers be excluded

Sectoroverstijgend
Stedin is zich bewust van de rol en verantwoordelijkheid die zij als netbeheerder hebben om Nederland te wapenen tegen cyberaanvallen. Van Der Linden: “In samenspraak met onze toezichthouder Agentschap Telecom kijken wij hoe wij het beste kunnen voldoen aan onze zorgplicht. Wij zijn wat dat betreft blij met de Wet Beveiliging Netwerk- en Informatiesystemen, die ons voldoende handvatten geeft. Deze wet voorziet in een meldplicht van incidenten en een zorgplicht, het treffen van beveiligingsmaatregelen. Zo deel je met elkaar de gevaren die bij ene sector spelen, maar bij de andere nog niet.”

Van Der Linden hecht waarde aan die sectoroverstijgende aanpak. Daarom heeft Stedin Groep ook zitting in de Commissie Vitale infrastructuur, een initiatief van VNO-NCW. “Deze commissie heeft als gemeenschappelijkheid vitale infrastructuur: financiën, telecom, water, grote industrieën”, vervolgt Van Der Linden. “We bespreken hierin bijvoorbeeld de spanning die heerst tussen open aanbestedingen en bescherming tegen de dreiging vanuit statelijke actoren. Hoe ga je daarmee om? Moet je Russische en Chinese softwarebedrijven bij voorbaat uitsluiten? Dit is een lastig dilemma.”

Schaap met vijf poten
Binnen Stedin is men volgens Van Der Linden soms te veel op zoek naar multidisciplinariteit: “Naar het schaap met de vijf poten. Iemand die verstand heeft van processen, van de techniek, inkoop, awareness, wetgeving. Maar cybersecurity zit in alles. Iedereen heeft een noodzakelijk puzzelstukje van de grote cyber-legpuzzel. Als je je dat realiseert, dan ben je beter af met een schaap met vier poten. Want met drie van zulke schapen krijg je de gewenste multidisciplinariteit. Uiteindelijk is onze maatschappij multidisciplinair opgebouwd en niet alleen door ICT’ers, maar ook vanuit bijvoorbeeld de financiële, sociale, economische en juridische sector. Waarom zou je die dan niet multidisciplinair beschermen? We hebben het samen opgebouwd; we moeten het ook samen beschermen. Daarom heb ik de verantwoordelijk van cybersecurity binnen onze Raad van Bestuur ook niet bij één persoon belegd. Bij ons zijn de taken onderling goed verdeeld op het cyberdomein, maar op zo’n manier dat we er allemaal mee te maken hebben en allen verantwoordelijk zijn. Onze cybersecurity-afdeling is de ruggengraat; onze afdelingen vormen het zenuwstelsel.”

from even participating? It's a tricky dilemma.'

Unicorn
Van der Linden feels that Stedin Group is sometimes overly concerned with the multidisciplinary aspect: 'They're looking for the impossible; for someone who's an expert on processes, technology, purchasing, awareness and legislation. But cybersecurity is part of everything. Everyone has their own vital piece of the larger cyber puzzle. Once you understand that, you're better off with regular experts. Three of them will give you the multidisciplinary knowledge you're after. Ultimately, Dutch society has a multidisciplinary structure that includes not only ICT expertise, but also know-how from the financial, social, economic and legal sectors. So why shouldn't we take a multidisciplinary approach to its protection? We built this thing together, and we should safeguard it together as well. That is precisely why I haven't tasked just one individual on our Executive Board with responsibility for cybersecurity. In our Board, the cyber-related tasks are evenly distributed, but in such a way that we all deal with these issues and all bear responsibility in this area. Our cybersecurity department is the backbone and our respective departments are the central nervous system.'

“Je kunt veel afvangen door techniek, maar uiteindelijk zijn de medewerkers je beste filters”
‘While it's true that technology can deflect a lot of problems, ultimately your employees are the most effective filters you have’

BACK TO TOP

Greet Prins
Former member of the Council for Health and Society (RVS), chair of the Executive Board for Philadelphia Zorg and member of the Senate of Dutch Parliament for the Christian Democrats

WAARDE(N)VOLLE ZORGTECHNOLOGIE:

VALUABLE AND VALUE-DRIVEN CARE TECHNOLOGY:

AN EXPLORATORY OPINION ON THE OPPORTUNITIES AND RISKS OF ARTIFICIAL INTELLIGENCE IN THE HEALTHCARE SECTOR

Kunstmatige intelligentie doet zijn intrede in onze samenleving, zo ook in de zorgsector. Het leidt naar de mening van de Raad voor Volksgezondheid en Samenleving (RVS) tot waardevolle technologie. Kunstmatige Intelligentie kan de kwaliteit en de toegankelijkheid van de zorg verbeteren, maar dan moet de overheid wel een scherp oog in het zeil houden, is de conclusie uit het door de RVS in februari 2019 gepubliceerde verkennend advies, getiteld 'Waarde(n)volle zorgtechnologie'. "Het rapport is een verkennend advies, omdat zoveel nog niet bekend en nog onzeker is, maar wel een advies omdat wij van oordeel zijn dat afwachten geen optie is", vertelt Greet Prins, voormalig raadslid van de RVS en tevens voorzitter Raad van Bestuur bij Philadelphia Zorg en lid van de CDA-fractie in de Eerste Kamer.

Artificial intelligence (AI) is making its way into society, including the healthcare sector. The Council for Health and Society (RVS) is of the opinion that this will result in valuable technology. AI has the potential to enhance the quality and accessibility of care – yet the government would do well to keep a close eye on its development. This is the conclusion of the exploratory opinion published by the RVS in February 2019, entitled 'Waarde(n)volle zorgtechnologie' [Valuable and value-driven care technology]. 'The report is an exploratory opinion because so much remains unknown and uncertain, yet it is an opinion nevertheless, as we feel that wait-and-see is not a viable option here,' says Greet Prins, former RVS board member, chair of the Executive Board for Philadelphia Zorg and member of the Senate of Dutch Parliament for the Christian Democrats.

Kunstmatige intelligentie wordt volgens Prins nu al toegepast in de zorgsector. "Het brengt veel kansen met zich mee voor de zorgsector, zoals klantvriendelijkheid en toegankelijkheid. Denk aan ingrijpende innovaties, zoals zorg op afstand, maar ook diagnose op afstand. Dankzij de digitalisering kunnen we de zorg een stuk efficiënter maken. Dit heeft veel voordelen voor de patiënt, zoals meer flexibiliteit en meer snelheid. Met alle nieuwe digitale toepassingen kan men bijvoorbeeld een analyse opvragen en er zijn al expertsystemen die aangeven net zo goed een diagnose te kunnen stellen als een zorgprofessional." Prins geeft aan dat de kennis en kunde met behulp van kunstmatige intelligentie dankzij zijn uitgebreide algoritme significant meer is dan de kennis die één enkele zorgspecialist heeft'.

Medisch oog

Prins benadrukt echter dat dit niet betekent dat daarmee de rol van de zorgprofessional in de toekomst overbodig is. "Integendeel, de 'human and intuitive touch' blijft nodig. Het gaat immers niet alleen om een specifieke aandoening, maar ook om de patiënt in zijn totale context. Ik ben

Prins explains that AI is already being used on a large scale in the healthcare sector. 'It offers many potential benefits for the sector, for instance by improving customer-friendliness and accessibility. These benefits include major innovations, such as remote care and remote diagnosis. Digitalisation allows us to make the healthcare sector much more efficient. This offers many advantages for patients, including greater flexibility and speed. The new digital applications make it possible to request and view an analysis, for instance, and some expert systems are already nearly as good as a healthcare specialist when it comes to providing a diagnosis.' Prins feels that the knowledge and expertise of an algorithm more than outweigh the lack of an 'intuitive human touch' from a healthcare specialist.

Medical eye

Prins emphasises that the role of healthcare professionals will remain important. 'On the contrary, the human and intuitive touch remains necessary. After all, it is not only about a specific disorder but also about the patient in his overall context. In fact, I believe the two serve to reinforce one another: artificial intelligence contributes to the quality of the care. It gives the healthcare professional more time and space for the conversation and dialogue with the patient and it keeps the healthcare professional alert. Take, for example, a case where there's a discrepancy between a physician's diagnosis, based on observations, and that of the system's algorithms. In such a case, the algorithms challenge the physician to verify his diagnosis and see whether any errors have been made. Healthcare specialists will also remain vital in terms of providing proper guidance for patients and communicating with them. These are matters that can't be entrusted to a machine. Thanks to technology, healthcare providers will be able to focus more strongly on the human aspect of their work and bring an even higher level of quality to that role.'

Digital literacy

According to Prins, understanding digital applications and handling them in a safe and responsible way requires certain knowledge on the part of healthcare professionals. 'This knowledge must of course be amassed and maintained somehow. These days, the pace of development is so quick that in one year's time, the world can look very different than it does today. It's important that healthcare professionals know what they can – and can't – expect from applications such as robots. The professionals need to be able to effectively judge when to intercede. I like to compare it to the adaptive cruise control in my car. I can't always blindly trust the cruise control; sometimes I have to take action myself.' The RVS has therefore recommended setting up a programme for monitoring developments in the area of AI, and for generating and exchanging relevant knowledge. Prins: 'On the one hand, this programme addresses the healthcare professionals. Attention to artificial intelligence should be integrated into healthcare degree and training programmes, as healthcare providers need to know how algorithms work and what they can do with them. On the other hand, of course, it also addresses members of the public. They, too, should understand what AI is, what the potential uses are and how to deal with it in their own lives. To that end, it's vital that we make digital literacy a structural part of primary and secondary education in the Netherlands. Much has been said about it, but speed is desirable given the digital developments today I really hope that educational institutions will take

van mening dat het elkaar versterkt; kunstmatige intelligentie draagt bij aan de kwaliteit van de zorg, geeft de zorgprofessional meer tijd en ruimte voor het gesprek en de dialoog met patiënten en het daagt de zorgprofessional uit. Bijvoorbeeld als een arts een andere diagnose stelt op basis van wat hij waarneemt en dit niet overeenkomt met wat de computer zegt. Het daagt de arts uit om nog zorgvuldiger te kijken naar wat klopt en wat niet klopt. Ook blijft een zorgspecialist dus hard nodig als het gaat om de begeleiding en de communicatie met de patiënt. Dat zijn zaken die je niet aan een machine over kan laten. Dankzij de techniek kunnen zorgverleners zich meer richten op het menselijke aspect van hun werk en deze rol nog kwalitatiever invullen."

Digitale vaardigheden

Het veilig en verantwoord omgaan met digitale toepassingen en het begrijpen ervan vraagt volgens Prins wel de nodige kennis van de zorgprofessionals. "Deze kennis moet worden opgebouwd en onderhouden natuurlijk. De ontwikkelingen vandaag de dag gaan immers zo snel dat de wereld volgend jaar weer heel anders kan zijn dan vandaag. Het is belangrijk dat zorgprofessionals weten wat ze van een toepassing als bijvoorbeeld een robot kan verwachten en wat juist niet. Ze moeten goed in kunnen schatten wanneer ze moeten ingrijpen. Ik vergelijk het altijd met de adaptive cruisecontrol van mijn auto. Daar kan ik ook niet altijd blind op vertrouwen. Soms is het nodig dat ik zelf ingrijp." Vanuit de RVS is daarom onder andere geadviseerd om programmatisch ontwikkelingen op het vlak van kunstmatige intelligentie te volgen, kennis te genereren en kennis te delen. Prins: "Enerzijds heeft dit betrekking op de zorgprofessionals. In de zorgopleidingen moet daarom structureel aandacht zijn voor kunstmatige intelligentie, want zorgverleners moeten weten hoe algoritmes werken en wat ze hiermee kunnen doen. Anderzijds geldt dit natuurlijk ook voor de burgers. Ook zij moeten begrijpen wat het is, wat ze ermee kunnen en hoe ze er mee om kunnen gaan. Daarom is het belangrijk dat digitale geletterdheid structureel onderdeel wordt in het basis- en voortgezet onderwijs. Er wordt al veel over gesproken, maar snelheid is gewenst gezien het tempo van de digitale ontwikkelingen vandaag de dag. Ik hoop dan ook echt dat onderwijsinstellingen de handschoen oppakken zodra er een nieuw curriculum beschikbaar wordt gesteld."

"Kunstmatige intelligentie draagt bij aan de kwaliteit van de zorg en het daagt de zorgprofessional uit"

'Artificial intelligence contributes to the quality of the care and keeps the healthcare professional alert'

Kwaliteit en betrouwbaarheid

Naast het programmatisch volgen van ontwikkelingen op het vlak van kunstmatige intelligentie is de RVS in zijn rapport ook kritisch over de uitdagingen die er liggen op het vlak van kwaliteit en betrouwbaarheid van digitale toepassingen. De kwaliteitseisen die aan alle toepassingen worden gesteld, zijn volgens de raad vaak onvoldoende. "Dat moet anders", bevestigt Prins. "Veel digitale toepassingen worden buiten Nederland ontwikkeld en op de markt gebracht. Deze aanbieders opereren voor een belangrijk deel buiten het formele zorgsysteem, maar meer direct richting de burger en dus is er voor hen geen noodzaak om een toelating op grond van de Wet Toelating Zorginstellingen aan te vragen. Daarmee vallen de toepassingen buiten de kwaliteits- en veiligheidseisen die wij in ons land hanteren. Ook de CE-markering voor toelating van deze toepassingen tot de (Europese) markt is nu ontoereikend. Met andere woorden, de snelheid waarmee kunstmatige intelligentie zijn intrede doet in de zorgsector past niet meer bij onze huidige wet- en regelgeving. De overheid heeft hierin een belangrijke wettelijke taak om eisen van kwaliteit en betrouwbaarheid af te dwingen. Denk bijvoorbeeld aan de digitale veiligheid van een toepassing."

Datacontinuïteit

Heel belangrijk vindt de RVS ook de garantie van datacontinuïteit: "Bedrijven en zelfs ziekenhuizen kunnen failliet gaan", geeft Prins aan. "In dat geval moeten patiënten over hun gegevens kunnen blijven beschikken. De downloadmogelijkheid die wij adviseren, maakt het voor burgers mogelijk om hun gegevens in zorgsystemen altijd op te vragen en te downloaden. Dit kan gecombineerd worden met een van overheidswege opgelegde 'health data escrow' of een erkenning voor bedrijven die een dergelijke escrow-regeling hebben. Deze zorgt ervoor dat gegevens en de broncode van de programma's beschikbaar blijven op het moment dat een bedrijf ermee stopt. Ook voor de digitale veiligheid van deze basisgegevens mag meer aandacht komen in de zorgsector."

Europese samenwerking

Net als voor cybersecurity geldt ook voor dit thema dat de vraagstukken een grensoverschrijdend karakter hebben. Daarom vindt de RVS het belangrijk dat er samengewerkt wordt op Europees niveau als het gaat om het ontwikkelen van uitgangspunten en principes voor kunstmatige intelligentie. De meeste toepassingen worden in andere landen ontwikkeld. Dus hoe kunnen we ervoor zorgen dat deze toepassingen ook voldoen aan de eisen die wij in Nederland stellen? "Als enkel land is het lastig om dit voor elkaar te krijgen. De kans van slagen is groter wanneer de Europese Unie hierin positie neemt. De Nederlandse regering en het parlement zullen dus actief moeten deelnemen aan deze ontwikkeling in Europees verband en waar nodig initiatief moeten nemen om ervoor te zorgen dat de Nederlandse opvattingen worden gehoord en een plaats krijgen in de op te stellen richtsnoeren en het rechtskader", aldus Prins.

BACK TO TOP

up the gauntlet as soon as the new curriculum becomes available.'

Quality and reliability

In addition to calling for a monitoring programme for developments in AI, the RVS report also takes a critical view of the challenges in connection with the quality and reliability of digital applications. According to the council, the quality standards to which all applications are held are often insufficient. 'This has to change,' Prince confirms. 'Many digital applications are being developed and marketed outside the Netherlands. Because these providers largely operate outside the formal healthcare system, but more directly towards the citizen, they have no need to seek admission under the Care Institutions Accreditation Act. As a result, the applications are exempt from the standards for quality and safety we adhere to in the Netherlands. The CE marking that grants these applications admission to the European market is now insufficient too. In other words, our current laws and regulations can't keep up with the speed with which artificial intelligence is making its way into the healthcare sector. The government has a vital statutory task to enforce quality and reliability standards – for instance, where the digital security of an application is concerned.'

Data continuity

Another crucial aspect, according to the RVS, is guaranteeing data continuity. 'Businesses and even hospitals can go bankrupt,' says Prins. 'And when they do, patients must have ongoing access to their medical data. The download opportunity we recommend would make it possible for citizens to request and download their data from healthcare systems. This could potentially be combined with a government-mandated "health data escrow" or a quality mark for organisations that have such an escrow scheme in place. Such a mark ensures that the source code of the data remains available when a company stops using it. It wouldn't be a bad idea for the healthcare sector to devote greater attention to the digital security of that data, either.'

European cooperation

As with cybersecurity, the issues related to this theme are inherently cross-border in nature. According to the RVS, it is important to promote cooperation at a European level when it comes to developing the basic guidelines and principles for artificial intelligence. The majority of applications are being developed by other countries. How, then, can we ensure these applications will also comply with requirements we have established in the Netherlands? 'This is difficult for an individual country to achieve. But when the European Union adopts a standpoint on the matter, the chances of success increase. In other words, the Dutch government and parliament must actively participate in this development at a European level, and take initiative where needed in order to ensure that Dutch perspectives are heard and incorporated into the guidelines and legal frameworks to be drafted,' Prins concludes.

Marieke van Wallenburg
Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations and member of the Cyber Security Council

SECURITY IS A PUBLIC VALUE

De overheid werkt in het contact met de burger en het bedrijfsleven steeds digitaler. Dat is een ontwikkeling die zeker niet ten einde is gekomen. Ook zien we dat de accenten in de ICT-technologie sterk veranderen. Vijfentwintig jaar geleden begon het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) na te denken over het toepassen van de digitale snelweg: het internet. Vandaag de dag wordt veel gesproken over de kansen die, bijvoorbeeld kunstmatige intelligentie, blockchain, bitcoins en drones bieden. Ook zien we dat overheden, bedrijven en instellingen telkens investeren in nieuwe technische mogelijkheden omdat ze kansen zien voor het verbeteren van hun taken, diensten of producten. Marieke van Wallenburg, Directeur-Generaal Overheidsorganisatie bij het ministerie van BZK, geeft haar visie op een digitaal veilig Nederland aan de hand van de 'NL DIGIbeter Agenda Digitale Overheid'.

The contact between the government on the one hand and citizens and the business community on the other is becoming increasingly digitalised. And we certainly haven't seen the end of this trend. The priorities in ICT technology are visibly and drastically shifting as well. Twenty-five years ago, the Ministry of the Interior and Kingdom Relations began to consider how to make use of the 'digital highway': the Internet. Today, much of the discussion centres on the opportunities presented by artificial intelligence, blockchain, bitcoins, drones and other technologies. We are also seeing governments, businesses and institutions making repeated investments in new technical possibilities in order to further improve their work, services or products. Marieke van Wallenburg, Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations, shares her vision for digital security in the Netherlands based on the Dutch Digital Government Agenda.

De menselijke factor
Publieke waarden zoals privacy, zelfbeschikking en gelijkheid moeten volgens Van Wallenburg blijvend worden gewaarborgd bij al deze ontwikkelingen. "We mogen de menselijke factor niet uit het oog verliezen. In juli 2018 is de 'NL DIGIbeter *Agenda Digitale Overheid*' gepresenteerd. De agenda gaat over de kansen die de technologie biedt en dat we die moeten benutten. Ik zie de agenda als onderdeel van een drieluik, met daarin ook de Nederlandse Digitaliseringsstrategie en de Nederlandse Cybersecurity Agenda ofwel de NCSA."

Het ministerie van BZK heeft in goede samenwerking met andere overheden, maatschappelijke organisaties etc., initiatieven ontplooid om te zorgen dat burgers en bedrijven beter gebruikmaken van digitale overheidsdiensten en dat deze diensten ook beter aansluiten bij de praktijk bij burgers en bedrijven. Van Wallenburg: "Ik noem er een paar. Voor zo'n tweeënhalf miljoen Nederlanders is het gebruik van digitale middelen een probleem, aangezien zij er niet of nauwelijks mee overweg kunnen. Daarom hebben we het thema Digitale Inclusie handen en voeten gegeven door er concrete acties aan te verbinden, bijvoorbeeld via uitbreiding van het programma Tel mee met Taal. Het doel van dit programma is om niet alleen laaggeletterdheid aan te pakken, maar ook aandacht te hebben voor het ontwikkelen van digitale vaardigheden. In juli 2019 zijn de eerste vijftien informatiepunten Digitale Overheid geopend waar iedereen terecht kan met vragen en op (de digitale) weg geholpen worden. Steeds zijn we kritisch op de gebruiksvriendelijkheid van onze digitale producten. Voordat we 'live' gaan, testen we

The human factor
Van Wallenburg feels that public values such as privacy, self-determination and equality must be permanently safeguarded in all such developments. 'We mustn't lose sight of the human factor. The Dutch Digital Government Agenda was presented in July 2018. It centres on the opportunities technology offers, and the need for us to seize those opportunities. I think of the agenda as part of a three-pronged approach that also includes the Dutch Digitalisation Strategy and the National Cybersecurity Agenda, or NCSA.'

Together with other governments, social organizations and so forth the Ministry of the Interior and Kingdom Relations has developed initiatives to help citizens and businesses make more effective use of government services and ensure that the services themselves are better aligned to the needs of those citizens and businesses. Van Wallenburg: 'I'll give you some examples. The use of digital resources poses an obstacle for some two and a half million people in the Netherlands, as they are more or less digitally illiterate. That's why we've tried to give the theme of Digital Inclusion flesh and blood by linking it to tangible actions, such as expanding the "Tel mee met Taal" programme. This programme aims to not only address the problem of functional illiteracy but to devote attention to the development of digital skills as well. Additionally, the first fifteen Digital Government information centres were opened in July 2019. These are open to anyone with questions or who needs help in getting started with digital literacy. We keep a critical eye on the user-friendliness of our digital products. Before going live, we always conduct evaluations in a test environment with actual users. That's important and we will continue to do so.'

And there are even more initiatives that address the needs of people who lack digital skills. Van Wallenburg: 'The MijnOverheid government portal launched an app in December 2018 to receive messages from the government by

altijd eerst in een oefenomgeving met gebruikers. Ik vind dit belangrijk en we blijven hiermee doorgaan."

Er zijn meer initiatieven waarbij we als overheid rekening houden met mensen die niet digitaal vaardig zijn. Van Wallenburg: "In december 2018 werd de Berichtenbox-app van MijnOverheid gelanceerd en op dit moment wordt de DigiD-app gebruiksvriendelijker gemaakt om ervoor te zorgen dat ook mensen die minder digivaardig zijn, deze kunnen gebruiken. We maken de dienstverlening persoonlijker door te kijken vanuit de optiek van levensgebeurtenissen. Er zijn sinds de zomer enkele tientallen checklists voor levensgebeurtenissen gemaakt, die op Rijksoverheid.nl staan. Die checklists geven advies en melden verplichtingen bij trouwen, bij pensioen of bijvoorbeeld bij het krijgen van een kind. Het helpt de burger op weg om zaken direct te kunnen regelen."

En veilig!
Ook de digitale veiligheid bij dit alles is volgens Van Wallenburg een belangrijk aandachtspunt, omdat de overheid hierin een voorbeeldrol te vervullen heeft. "Van de overheid mag een hoge mate van zorgvuldigheid worden verwacht ten aanzien van de bescherming van gegevens van burgers en bedrijven vanwege de plicht die zij oplegt tot het verstrekken van gegevens", vertelt Van Wallenburg. "Het is zeker zo dat iedere organisatie bij de overheid zelf verantwoordelijk is voor de eigen informatieveiligheid. Daarnaast zijn er ook zaken die we met elkaar moeten regelen, omdat het basale zaken zijn en het efficiënt is om dat gezamenlijk te regelen. Immers, Rijks- of overheidsorganisaties zijn digitaal aan elkaar verbonden waardoor het beveiligingsniveau van een individuele overheidsorganisatie effect heeft in de gehele keten." Al deze maatregelen zijn als overheidsverplichting vastgesteld in de Baseline Informatiebeveiliging Overheid (BIO). "Alle overheidslagen hebben zich aan de BIO verbonden. De publicatie van de BIO in de Staatscourant is de bezegeling van een lang traject waar heel veel mensen aan hebben meegewerkt: een mijlpaal waar ik trots op ben!", vertelt Van Wallenburg.

Gezamenlijke acties
"Het werk is zeker nog niet klaar", vervolgt Van Wallenburg. "Afgelopen najaar zijn we nieuw acties gestart om in gezamenlijkheid de informatieveiligheid bij de overheid en bij de Rijksdienst te vergroten. Het gaat in totaal om achttien verschillende acties, te veel om allemaal te benoemen en toe te lichten. We zetten onder andere in op het gezamenlijk vergroten van de feitelijke veiligheid, bijvoorbeeld door een versnelde uitrol van het Nationaal Detectie Netwerk voor de Rijksdienst en door te onderzoeken hoe we voor burgers en bedrijven de herkenbaarheid van overheidswebsites en e-mail kunnen vergroten." Alle acties van BZK hiertoe staan niet op zichzelf en zijn nauw verbonden met de NCSA. Van Wallenburg: "Een mooi voorbeeld is er ten aanzien van het Landelijk dekkend stelsel. In dat verband geven we de komende tijd een impuls aan het overheidsbreed oefenen met incidenten op het gebied van digitale veiligheid."

Beveiliging is niet alleen techniek
Dat beveiliging vaak wordt gezien als een technische aangelegenheid vindt Van Wallenburg niet terecht. Volgens haar begint het met nadenken over wat de waarde van je eigen processen is. "Zijn het je kroonjuwelen? Zitten er persoonsgegevens bij? Zijn er processen die vrijwel niet verstoord mogen raken? Met daarin informatie die echt onaangetast moet blijven? En last but not least, informatie die echt niet in

"Je mag niet verwachten dat burgers zonder meer weten wat ze moeten doen om de echte zware jongens en meiden te weren"

'It is hardly fair to expect citizens to just know, on their own, what they must do in order to keep the real bad guys (and girls) out'

e-mail and, as we speak, the DigiD app is being made more accessible and usable so that even less tech-savvy individuals will be able to use it. We're making the service more personal by taking an approach based on life events. This summer, several dozen life-event checklists have been created and published on Rijksoverheid.nl. These checklists offer advice and inform readers of their obligations in case of an event such as marriage, retirement or the birth of a child. This lends citizens a helping hand in managing such matters for themselves.'

And secure, too!
Van Wallenburg points out that digital security is an important area for attention here as well, as the government has an exemplary function in this area. 'Because the government obligates citizens and businesses to submit certain data, the government can rightfully be expected to exercise a high degree of care when it comes to protecting that data,' Van Wallenburg explains. 'It is clear that every organisation within the government itself bears responsibility for its own information security. There are also certain aspects we must arrange in coordination with one another, because they are fundamental and it is more efficient to manage them jointly. After all, the central government and other governmental organisations are digitally linked – meaning the security level of each individual governmental organisation will have repercussions for the entire chain.' Each of these measures has been established as a governmental obligation in the Government Information Security Baseline [BIO: Baseline Informatiebeveiliging Overheid]. Van Wallenburg: 'Every layer of government has pledged to comply with the BIO. Its publication in the Government Gazette marked the successful completion of a long journey made possible by the efforts of a great many people: a milestone of which I'm terribly proud!'.

Joint actions
'Our work, however, is certainly far from done,' Van Wallenburg continues. 'Last autumn, we

MARIEKE VAN WALLENBURG

Nieuw lid van de Cyber Security Raad (CSR)

New member of the Cyber Security Council (CSR)

Marieke van Wallenburg (1974) is Directeur-Generaal Overheidsorganisatie (DGOO) bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Sinds maart 2019 is zij lid van de CSR.

Marieke van Wallenburg (1974) is Director-General for Public Administration at the Ministry of the Interior and Kingdom Relations. She has served as a member of the CSR since March 2019.

Waarom is 'cyber' een belangrijk thema voor het ministerie van BZK?
"Cybersecurity is voor het Ministerie van BZK een belangrijk thema, omdat digitale dreigingen een grote maatschappelijke impact hebben. Het onderwerp cybersecurity krijgt binnen het ministerie volop aandacht, om te beginnen bij de Algemene Inlichtingen en Veiligheidsdienst (AIVD), maar ook vanuit de coördinerende rol die BZK heeft voor de overheid als geheel en de Rijksdienst in het bijzonder. Het ministerie is verantwoordelijk voor het stellen van informatiebeveiligingsregelgeving en –kaders, zoals de Baseline Informatiebeveiliging Overheid."

Wat is voor u het belang van de CSR?
"De raad geeft de mogelijkheid om de toekomstige uitdagingen in cybersecurity te bespreken met alle sleutelspelers. Om de dreigingen van nu en de toekomst te weerstaan, moeten we samen optrekken. Daarom heeft het voor mij ook meerwaarde dat in de CSR naast de publieke partijen ook private partijen en de wetenschap vertegenwoordigd zijn."

Why are cyber issues important to the Ministry of the Interior and Kingdom Relations?
'Cybersecurity is an important priority at the Ministry of the Interior and Kingdom Relations because digital threats have major societal impact. The Ministry is devoting serious attention to theme of cybersecurity, primarily within the General Intelligence and Security Service (AIVD), but also via its coordinating role on behalf of the Dutch government in general and the Dutch Civil Service in particular. The Ministry of the Interior and Kingdom Relations is responsible for establishing data security regulations and frameworks, such as the Government Information Security Baseline.'

Why do you consider the CSR to be important?
'The council provides an opportunity to discuss future cybersecurity-related challenges with all key players. If we are to ward off threats, now and in the future, we will have to join forces. For this reason, I find it valuable that the CSR includes representatives from not only public parties but private parties and the scientific community as well.'

verkeerde handen mag vallen? Kortom, waar zou je als bestuurder wakker van moeten liggen? Ik zie gelukkig wel dat bestuurders zich veelal bewust zijn van het belang van cybersecurity."

Meer zelfredzaamheid
We nemen meer en meer kennis van alle gevaren die uitgaan van internetcriminelen en van statelijke actoren. Dat is ook nodig om mensen daartegen in beweging te krijgen. "Maar dan moeten we het die mensen ook gemakkelijker maken om er zelf iets tegen te kunnen doen", stelt Van Wallenburg. "Veilig faciliteren, security by design. Ik denk dat dat nog beter kan. Je mag nu niet verwachten dat burgers zonder meer weten wat ze moeten doen om de echte zware jongens en meiden te weren. Dat is voer voor specialisten. Hoewel ik snap dat hun betrokkenheid belangrijk is en blijft, zou ik willen dat mensen in staat worden gesteld meer zelf bij te dragen aan het vergroten van hun eigen veiligheid." Van Wallenburg maakt daarbij de vergelijking met de auto: "Vijftig jaar geleden hadden auto's geen gordels, airbags en hoofdsteunen. Nu wel, maar dat betekent niet dat je niet meer na hoeft te denken, je moet je gordels zelf omdoen, je moet je hoofdsteunen op de juiste hoogte brengen en bij een babyzitje op de voorbank moet je zelf de airbag uitzetten. Naast de veiligheid "onder de motorkap", is dit soort zaken er dus ook. En dat zou ik in de ICT ook willen zien: meer effectieve zelfredzaamheid."

Tot slot
Van Wallenburg is zich ervan bewust dat dit alles geen eenvoudige opgave is. "We moeten ons maximaal inspannen om de publieke waarden te waarborgen, samen met het vergroten van de zelfredzaamheid. Dat is wereldwijd de grootste uitdaging als het gaat om de menselijke factor."

"Van de overheid mag een hoge mate van zorgvuldigheid worden verwacht ten aanzien van de bescherming van gegevens van burgers en bedrijven"

'the government can rightfully be expected to exercise a high degree of care when it comes to protecting data of citizens and businesses'

launched new actions to collectively enhance information security within the Dutch government and Civil Service. A total of eighteen distinct actions were involved – too many to list and describe them all here. We are taking steps to strengthen actual security, such as committing the civil service to an accelerated roll-out of the National Detection Network and by exploring ways to make government websites and e-mails more recognisable for businesses and members of the public.' The Interior Ministry's actions in this area are not isolated measures; they are closely affiliated with the activities of the NCSA. Van Wallenburg: 'A great example of this involves the nationwide network. That's where, in the coming period, we'll be providing extra support to government-wide incident drills in in the field of digital security.'

Security is more than technology alone
Many people view security as a technical matter: a misconception, if you ask Van Wallenburg. To her mind, the very first step should be to consider the value of your own processes. 'Are they your crown jewels, as it were? Do they involve personal data? Are there any processes that should never be interrupted if you can help it? With information in them that must remain absolutely unaffected? And – last but not least – is there information that must never be allowed to fall into the wrong hands? In short: what are the things that should keep you, as an administrator, awake at night? Luckily, most administrators seem to be well aware of the importance of cybersecurity.'

Greater self-reliance
We learn more and more from every danger aspect placed before us by cyber criminals and state actors. And learning is necessary if we are to move people to action against these threats. 'But we also still need to make it easier for them to take action on their own,' Van Wallenburg says. 'Secure facilitation and security-by-design: I think there's room for improvement here. At present it's hardly fair to expect citizens to just know, on their own, what they must do in order to keep the real bad guys (and girls) out. That's a job for a specialist. While I understand that expert involvement is important, and will remain so, I'd like to see the general public empowered to contribute more effectively to efforts to increase their own security.' Van Wallenburg likens the situation to a car: 'Fifty years ago, cars didn't have seatbelts, air bags or headrests. Today, they do – but that doesn't mean drivers no longer need to use their head. You still have to fasten your seatbelt, adjust your headrest and switch off the air bag when you put a child's car seat in the front passenger seat. Besides the car's built-in safety features, you have behavioural aspects like this to consider as well. And that's precisely what I'd like to achieve in ICT: greater and more effective self-reliance.'

In conclusion
Van Wallenburg is aware that none of these tasks are easy. 'We must devote maximum effort to safeguarding public values, while at the same time enhancing self-reliance. This is the greatest challenge worldwide in terms of the human factor.'

NEXT

BACK TO TOP

Professor Monica Whitty
Full-time chair in Human Factors in cybersecurity at the University of Melbourne and committee member of the Global Futures Council on CyberSecurity for the World Economic Forum.

THE IMPORTANCE TO TRAIN INDIVIDUALS INTO EMPLOYING SECURE ONLINE HABITS

There has been much governmental, individual and business concern about the growing number and costs of cyber-dependent and cyber-enabled crimes and the harms associated with these crimes. Harms reported upon include economic, identity and/or privacy-related, health, as well as psychological harms, such as stress and anxiety. Harms can be experienced by individuals, and by collective units like nation states. Businesses are often treated as national units, but large businesses tend to be transnational in their business and tax arrangements, wherever they are headquartered. Harms from ransomware can range from patients' health if healthcare systems are taken down, to the state's security to economic and reputational harms to business. Harms from hacking might include loss of business, reputational harm, or even the bringing down of a nation's critical infrastructure – which could lead to severe devasting effects.

Cyberfrauds (also referred to as advance-fee scams) are one type of cyber-enabled crime, which I have researched over the last 12 years. Victims of cyberfrauds are often left feeling traumatized from criminals who have groomed them and tricked them out of money (even when small sums of money are involved). These scams existed as postal mail scams prior to the advent of the Internet; however, the Internet has opened the floodgates to these scams, where criminals can target many more victims and draw from a range of tools to trick victims into believing they are authentic individuals. In the classic Advanced-fee scam, also referred to as the 'Nigerian email scam', an individual receives an e-mail from a stranger who claims to have a large sum of funds trapped or frozen for a variety of reasons (e.g., unclaimed estate, corrupt executive, dying Samaritan). In each case, they offer the recipient rich rewards for helping government officials or family members out of an embarrassing or legal problem. Other examples include investment, inheritance, lottery, and romance scams.

Although often considered as trivial crimes, these types of crimes can leave victims feeling depressed, anxious, and socially isolated, with some individuals known to have committed suicide. Some of these scams have involved victims, unknowingly, involved as money mules or drug mules. To give an example of one such victim:

This victim befriended a fake persona of a Captain in the US army (who, unbeknownst to her was, in fact, a cybercriminal) whom she met via Skype. Over the time she was communicating with the criminal she was sent a number of photographs of a real Captain (which were stolen photograms from the Internet). For two years, the victim communicated with the Captain daily. She felt fully absorbed by the relationship, and at a certain point, the criminal asked for her hand in marriage – which she accepted. Simultaneously, the victim was repeatedly asked for money to help pay for crises such as medical expenses after the Captain was supposedly shot by the Taliban. Shortly after, the criminal declared that he could retire and live with the victim. However, to do so, the victim was asked to go to another country, where she was told she would meet the Captain's Commander and collect and sign the Captain's retirement papers. During this trip, the victim was planted with class A drugs which were detected on her during her return travels. When she learnt that she had been scammed the victim was completely surprised and shocked by what had happened to her.

The general public often trivialize scams, believing that only stupid, naïve individuals could ever fall for one of these scams. However, my research demonstrates that many different types of individuals are caught up in scams – often including professional and well-educated individuals. Unfortunately, knowing about scams and how they work does not necessarily prevent scam victimization. Victims of scams have often heard about the scam that tricked them into giving up their money.

Governments often spend large resources into developing raising awareness campaigns – in the hope that individuals and businesses will recognize a scam, thereby avoiding the con. However, criminals are very clever at appearing authentic and distracting victims for long enough so that they do not have time to check the facts. Instead, I argue that cybersecurity educational programmes need to train individuals into employing secure online habits; for example, using a reverse image search on all people they meet online. Moreover, businesses have a corporate responsibility to improve on their scam detection techniques (if they can't spot a scam why do they expect that their customers are able to do so), and to train users into using their sites safely.

BACK TO TOP

'Victims of cyberfrauds are often left feeling traumatized from criminals who have groomed them and tricked them out of money (even when small sums of money are involved)'

Delphine Chevallier
consultant, trainer and publisher,
Thalia NeoMedia

Graduated in general management (ESCP Europe), Mathematics and Economics (University Paris-IX) and Digital Strategies (INSEAD), I am part of this manager generation who have gone through major and rapid work transformation as technology invaded the workplace. Developing then my career as HRD in major international organisations, I then had the privilege to transform people and organisations to operate effectively in a digital era.

'CYBERATTACK'

Working with end users I started to figure out two issues :

1. the knowledge gap between the technicians and the people using the technology for their day-to-day job,
2. the effort for people to switch from human interactions to IT ones.

Developing then my career in HR and Learning & Development in major international organizations, I have had the privilege to observe the impact of digitalisation on all company's positions, which frequently has led to redundancy plan as technology was not only replacing human tasks but also doing the job more rapidly. People had thus been facing significant learning challenges to adapt their skills and develop brand new competencies from scratch, for the same job or to find a new one.

With the raise of smartphone and WiFi, together with increased capacity storage on servers and software mobility, the organisational disruption has been so massive and rapid, that human brain has been facing an unprecedent challenge to adapt. An increased number of people in organisations and in society, have been unable to really acquire new skills and related behaviors to work safely with the technology. Last but not least, when leading system implementation as part of my job, colleagues working on the technical side of those projects, were sharing with me in confidence the fact that, because of the increased complexity in project governance in matrix organizations, the multiple systems interactions combined with accelerated data flow has become extremely challenging to monitor.

Let's step back for a few seconds: organisations and people over the past few years had to radically switch their ways of working and interacting (inside and outside organisations) from a slow, controlled, processed, heavily structured and divided model with few data, to a fast, fluid, experienced based, blurry but at the same time open environment with high volume of data. With a huge number of benefits (easy access to information, interactions with customers, value chain transparency just to name a few). But the downside puts the whole society at risk of losing more than we think as digital has invaded the work place and our personal life.

When a major incident occurs (such as cyberattack or network interruption or hardware damages), individuals are put more than ever in a stressful situation. Here are some words I have heard recently from people who have experienced such an event: « it made me hysterical not to be able to access my data », « I was even more upset as my clients and stakeholders were still moving ahead, sending e-mails, working normally; and I was at a standstill without access to anything. I felt like being excluded », « I have lost 2 years of my life », « I turn crazy as I realized I was unable to work anymore », « I had no clue what to do to be able to do my work ».

Emotions generated by IT interruption are even stronger as they hit individuals in their belief of being invulnerable in a digital world which is,

'An increased number of people in organisations and in society, have been unable to really acquire new skills and related behaviors to work safely with the technology'

to a certain extent, disconnected from reality. When systems stop, it put us back in an environment (here and now, at our desk, colleagues working next door, paper and pen) we have unconsciously put distance with. Alongside from my work in various large multinational firms, I started to establish my profile as a publisher, using the power of story telling to accelerate learning. The book "Cyberattack", was published in French in the Fall 2018. Inspired from real events (NotPeya attack), it tells the story of an employee who is suddenly moving from hyper digital activity to do her job to silence and vacuum. The reader becomes progressively aware of cyber war threat which leads to everyone's vulnerability.

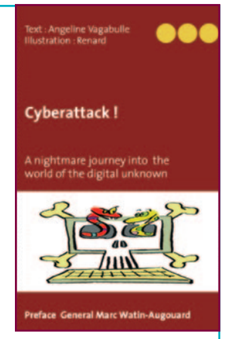
The story is highlighting the importance of preparing people to emotionally go through such event with distance and calm. This is not an easy task, in a business world largely dominated by rationality and algorithm. After years of focusing on digitalising tasks were we really thinking we were building a more efficient environment without any disturbing emotions and mood swings? Did we forgot that a human still sits behind the machine? Isn't it a choc to realize that the digital labyrinth created might have increased our level of risks ? How could have we missed that technology augments also the power of malicious people using all the rifts present in the skills set of employees and in the increased data flow of interactions?

In the context described above, a cyberattack (or a major IT incident), is a very brutal, violent experience for individuals suddenly facing their own vulnerability and the beyond comprehension organisational one. If not prepared in behaving in such a chaotic context, the inability of ensuring operations continuity can lead to the loss of a business in just a second.

Should you want to rather take this as an opportunity to become stronger, making the most of digital without the inevitable related risks, ask yourselves those critical questions :

1. Do the people involved in my core business operations still have the minimum know-how to run them manually? Have they recently practiced to run them without any digital support?
2. Do all employees, whatever their department and position, know what to do every day to protect our digital organisation's assets? Do they have practiced recently to work during few hours without any access to digital tools?

If you have positive answers to those questions, then your organisation, through its people, is mature enough to ensure well protected digital operations. The brutality and the damages technology can generate is proportionate to the illusion algorithms have given you to control your business.



In a world where digital hyper-connection reigns supreme, what would happen if someone were to destroy our computer networks?

On June 27th 2017, a global cyberattack strikes multinational corporations across the globe.

Angeline, a long time paid-up member of the rat race, suddenly finds herself thrown into the heart of catastrophic computerized chaos. Within a split second, the hyperactivity of the digital networks becomes the black silence of the big void. No information, no news. And worst of all, no way to communicate. After the initial shock, the question of how to restart the machine becomes the priority.

Is Angeline's giant global company merely a colossus with feet of clay? How is one to continue working when all their tools have been destroyed?

Let yourself be carried away by this true and deeply human story that plunges you into the throes of the great disconnection.

"Cyberattack ! *A nightmare journey into the world of the digital unknown*"
Text : Angeline Vagabulle, Illustration : Renard,
Thalia NeoMedia / DG Editions les Funambulles
Prefaced by General Marc Watin-Augouard, Founder and co-director of the International Cybersecurity Forum and Director of the Ecole des Officiers de la Gendarmerie Nationale Research Center.

Elly van den Heuvel-Davies
Secretary of the Cyber Security Council

ALL ASPECTS OF THE HUMAN CONDITION IN RELATION TO CYBER SECURITY

Dit jaar staat de human factor centraal in CSR Magazine. Een bewuste keuze van de raad omdat, hoe je het ook wendt of keert, de mens centraal staat in de digitale wereld; als burger, consument, slachtoffer, dader, sterkste schakel en zwakste schakel. Maar ook als ontwerper. Laten we vooral niet vergeten dat kunstmatige intelligentie, algoritmen, robotica en ook privacy en security by design vooralsnog mensenwerk is. Het digitale tijdperk vraagt nieuwe kennis en vaardigheden van ons als mens in alle facetten en van de komende nieuwe generatie(s). Dit vraagt om een aanpak over de hele linie. We weten dat onze kwetsbaarheid en afhankelijkheid toenemen, maar toch zijn we daar nog onvoldoende op ingericht.

This year, CSR Magazine is focusing on the human aspect. This was a conscious decision on the council's part, because no matter how you look at it, humans are at the core of the digital world: as citizens, consumers, victims, criminals and both the strongest and weakest link. But also as the architects of it all. We should never forget fact that artificial intelligence, algorithms, robotics and even privacy and security-by-design are – for the time being – human inventions. The digital era calls for new knowledge and skills in all aspects of the human condition, and will ask them of future generations as well. This requires a single, united approach. We know that our vulnerability and dependency are increasing, but we have not yet taken sufficient steps in response.

Readiness
To avoid falling behind, we must anticipate future digital developments in a timely and effective manner. This is precisely our intention in the council: to adopt an integral approach with the leadership to match. The necessity of such an approach is reflected in a recently published WRR report, which concludes that the threat of digital disruption is real and we must adopt a state of readiness. That 'state of readiness' is a fine phrase, one that encompasses everything we need to be: *vigilant, willing, prepared, well-practised, combative, careful and adept*. When you see this combination of attitudes, you might think: 'But surely those are valuable qualities in any era?' And you'd be absolutely right. Down through the centuries, we have had to be prepared to fight for our economic and societal interests. And if Dutch investigative journalist Huib Modderkolk is to be believed, a digital war has been raging for quite some time now – it's just that no one is aware of it. This touches on the core of all major digital issues: much of what is happening in the digital world is barely visible to the majority of people, and yet we are right in the thick of it.

Today's cybersecurity issues are complex, and most can no longer be solved at a national level. An integral European approach is needed, one with a vision for the future and a focus on public-private partnerships, in recognition of a broad desire to make real investments in our shared digital future. A digital web is being spun around our day-to-day lives, and we're hardly aware that it's happening. The physical and digital worlds are becoming ever more closely intertwined and we are growing increasingly dependent on the Internet. At the same time, with technology becoming ever more intimate in nature, the boundary between man and machine is gradually blurring.[1] Combined with the lightning pace at which technological developments are taking place, the message is clear: we ain't seen nothing yet. Looking ahead to anticipate and respond to new developments in a timely manner is a habit that must become ingrained in society as a whole. The council believes it has an important role to play in this area.

Rock and a hard place
Luckily, there is a growing realisation in both this country and the European Union that we must work to meet these challenges and to protect what we hold dear. There is much at stake for citizens of the EU: after all, ours is an open, free and prosperous society founded around our standards and values. Right now, Europe finds itself between a rock and a hard place. On the one hand, the Big 5 (Google, Amazon, Facebook, Microsoft and Apple) from the United States rule the Internet: they view us primarily as consumers and have already collected more information on us than we can possibly imagine. A lack of European alternatives means they can easily continue to hold sway over us. And on the other hand, to the East you have the People's Republic of China, where the state controls all areas of life and views its citizens as subjects. The sovereign Internet helps the Chinese government to issue good marks to citizens for demonstrating exemplary behaviour.

Paraat
We zullen tijdig en effectief moeten anticiperen op toekomstige digitale ontwikkelingen om niet achterop te raken. Dat is ook waar we als raad op in gaan zetten: een integrale aanpak met bijpassend leiderschap. Dat dit nodig is, blijkt ook uit het onlangs gepubliceerde WRR-rapport waarin wordt geconcludeerd dat digitale ontwrichting op de loer ligt en dat we paraat moeten zijn. Een mooi woord 'paraat', het heeft alles in zich wat we momenteel nodig hebben: *alert, bereid, gereed, niet ongeoefend, strijdbaar, voorzichtig en vaardig*. Als je deze combinatie aan gemoedstoestanden ziet, denk je: 'Maar dat is toch van alle tijden?' En zo is het ook! Door de eeuwen heen hebben we klaar moeten staan om te strijden voor onze economische en maatschappelijke belangen. En als we Huib Modderkolk moeten geloven, is er al lange tijd een digitale oorlog gaande, maar niemand ziet het. Daarmee raakt hij de kern van de grote digitale vraagstukken; veel van wat zich in de digitale wereld afspeelt, is voor de meeste mensen nauwelijks zichtbaar en toch zitten we er middenin.

De cybersecurity-vraagstukken zijn complex en kunnen in veel gevallen niet meer op nationaal niveau worden opgelost. Ook op Europees niveau is een integrale aanpak nodig met een toekomstvisie en waarin publiek-private samenwerking centraal staat alsook de wil van de samenleving om daadwerkelijk te investeren in onze digitale toekomst. Zonder dat we het echt in de gaten hebben, wordt er om ons dagelijks leven heen een digitaal web gespannen. De fysieke en de digitale wereld raken steeds meer met elkaar verweven en we worden steeds afhankelijker van het internet. Ook wordt technologie steeds intiemer en vervaagt langzamerhand de grens tussen mens en machine[1]. De technologische ontwikkelingen gaan razend snel; *we ain´t seen nothing yet*. Vooruitkijken en tijdig anticiperen op nieuwe

1. Est, R.van, m.m.v. V. Rerimassie, I van Keulen en G. Dorren, Intieme technologie: de slag om ons lichaam en gedrag, Den Haag, Rathenau Instituut 2014
Est, R. van, in cooperation with V. Rerimassie, I. van Keulen and G. Dorren, Intimate technology: the battle for our body and behaviour, The Hague, Rathenau Institute, 2014

ontwikkelingen moet ingebed zijn in onze hele samenleving. De raad ziet hier een belangrijke rol voor zichzelf weggelegd.

Twee vuren

Gelukkig groeit in ons land en in de Europese Unie het bewustzijn om te werken aan de uitdagingen en om te beschermen wat ons lief is. Er staat ook veel op het spel voor EU-burgers. Het gaat om een open, vrije en welvarende samenleving waarin onze normen en waarden centraal staan. Europa zit op dit moment tussen twee vuren. Enerzijds beheersen de Big 5 (Google, Amazon, Facebook, Microsoft en Apple) uit de Verenigde Staten het internet; zij zien ons vooral als consumenten en hebben inmiddels meer informatie over ons verzameld dan we kunnen bevatten. Door het gebrek aan Europese alternatieven kunnen zij ons makkelijk in hun greep houden. Anderzijds heb je de volksrepubliek China in het oosten waar de staat het voor het zeggen heeft en de burgers als onderdanen ziet. Het soevereine internet helpt de Chinese staat een handje bij het uitdelen van een rapportcijfer aan de burger voor voorbeeldig gedrag.

Noch de VS, noch China zitten stil als het gaat om het exploreren van de digitale mogelijkheden, voor goede en minder goede praktijken. China ziet de kansen die digitalisering kan bieden heel scherp en kondigt in ‘Made in China 2025’ aan China te zullen transformeren in een ‘manifactoring superpower’ in onder meer robotics, luchtvaarttechniek, kwantum computing. Het plan is duidelijk niet bedoeld als een inhaalslag, maar om andere economieën voorbij te streven. Ondertussen dringen buitenlandse technologiebedrijven diep in de haarvaten van onze samenleving door hun concepten van smart cities te implementeren in de VS, Canada en in Nederland. Steden moeten worden voorzien van sensoren, robots, zelfrijdende auto´s en digitale diensten. Dat heeft uiteraard zo zijn aantrekkelijke kanten en zal het dagelijkse leven waarschijnlijk comfortabeler maken. Maar beseffen we daarbij wel voldoende dat onze privacy, cybersecurity en onafhankelijkheid hiermee behoorlijk onder druk komen te staan? Het feit dat met de komst van internet of things alles met elkaar en met het internet is verbonden, maakt ons nog kwetsbaarder. In de media wordt hier regelmatig de noodklok over geluid door cyberexperts. De roep om een sterke regierol en voldoende investering vanuit de overheid wordt steeds sterker.

Het is bemoedigend om te zien dat ook Europa niet stil zit. Het Franse evenement International Cybersecurity Forum (FIC) is met ruim 10.000 bezoekers waarschijnlijk het grootste cybersecurity-congres in Europa. FIC heeft zich voorgenomen om het over de EU-boeg te gooien en daarmee een grotere gemeenschappelijke bijdrage te leveren aan de weerbaarheid van Europa. Als voorzitter van het Advisory Board lever ik daar vanuit Nederland een bijdrage aan. Het thema van de conferentie in januari 2020 is niet verrassend: *the human factor*. Ook openen de Fransen de aanval op Facebook met hun oproep om de Libra te weren uit de EU. Europa zet na het bouwen van een betere verdedigingslinie met behulp van de NIB-richtlijn en de Algemene verordening gevensbescherming (AVG) in op vermindering van de digitale afhankelijkheid. Het World Economic Forum (WEF) heeft met de oprichting van een eigen Cyber Security Centrum een actieve rol op zich genomen om de cyberweerbaarheid op mondiaal niveau te verhogen. Er is duidelijk werk aan de winkel. De awareness is bij veel andere landen te laag. Mijn collega WEF-adviseur uit Zuid-Afrika staat bijvoorbeeld nog aan het begin: *een Afrikaan zal zijn laatste eten delen met een gast, dus waarom zijn ‘wagwoord’ niet?* Toegegeven we zijn in Europa verder, maar dat betekent niet dat we achterover kunnen leunen. We moeten juist nu als (EU-)land doorpakken en zorgen dat de digitale basis echt op orde komt. Dat geldt ook voor het opvoeren van het tempo om de weerbaarheid te verhogen. Ook hier zal de raad de komende periode op inzetten. *Haast is geboden.*

“De roep om een sterke regierol en voldoende investering vanuit de overheid wordt steeds sterker”

‘The call for a strong leadership role and sufficient investment from the government is becoming increasingly urgent’

Neither the US nor China is wasting any time when it comes to exploring further digital possibilities – for both ethical and less-than-ethical practices. China has a clear picture of the opportunities digitalisation can offer. In ‘Made in China 2025’, it has announced that it intends to transform the country into a manufacturing superpower in a range of sectors, including robotics, aviation technology and quantum computing. This plan is clearly intended not as a means for catching up, but for surpassing the success of other economies. Meanwhile, international tech companies are infiltrating the bloodstream of our society by implementing their smart city concepts in the US, Canada – and the Netherlands. Cities must be equipped with sensors, robots, self-driving cars and digital services. Some aspects of this are appealing, of course, and will likely make our daily lives more comfortable. But are we sufficiently aware that these applications also place considerable pressure on our privacy, cybersecurity and independence?

With the rise of the Internet of Things, all devices will become connected not just to the Internet, but with each other, which renders us even more vulnerable. Cyber experts frequently sound the alarm about this issue in the media. The call for a strong leadership role and sufficient investment from the government is becoming increasingly urgent.

It is encouraging to see that Europe is not sitting on its hands, either. With over 10,000 visitors, the International Cybersecurity Forum (FIC) in France is probably the largest cybersecurity conference in Europe. FIC intends to approach the issue via the EU and by doing so, to make a larger joint contribution to the resilience of Europe. As chair of the Advisory Board, I will be contributing to these efforts from here in the Netherlands. The theme of the conference planned for January 2020 is, unsurprisingly, the human factor. The French are also launching their attack on Facebook with their call to ban the Libra from the EU. Having already built a better line of defence through the NIS Directive and the General Data Protection Regulation (GDPR), Europe is now turning its attention to reducing its digital dependence. By establishing its own Cyber Security Centre, the World Economic Forum (WEF) has readily assumed an active role in increasing digital resilience at the global level. Clearly there is work to be done. The level of awareness in many other countries is too low. My fellow WEF adviser from South Africa, for instance, has only just begun: *People in Africa are willing to share their last bit of food with a guest, so why not their password?* While here in Europe, we're admittedly further along in the process, that doesn't mean we can just sit back and relax. Especially at this point in time, we – as a country and as an EU Member State – must persevere and ensure that our digital foundation is truly sound. This also applies to accelerating the timeline for increasing resilience. The council will be working towards this goal, too, in the coming period. *We have little time to lose.*

NEXT

BACK TO TOP

Colofon | Colophon

Opdrachtgever | Commissioning party: **Cyber Security Raad Nederland | Dutch Cyber Security Council**
Hoofdredactie | Chief editor: **Elly van den Heuvel-Davies (secretaris |** secretary)
Concept en (eind)redactie | Concept and (final) editing: **Heidi Letter (CSR)**
Met dank aan | With thanks to: **Andrea Muntslag-Bakker (CSR), Raymond Bierens (CSR), Soesma Malaha (CSR), Siep van Sommeren (CSR), BKB**
Fotografie | Photography: **Arenda Oomen Fotografie, Jeroen de Bakker, Jiri Büller, Frank van Beek Fotografie, ANP foto, Nationale Beeldbank, De Beeldunie en Nationale Politie**
Vertalingen | Translations: **Metamorfose Vertalingen** • **Opmaak |** Layout: **BKB** • **Drukwerk |** Printwork: **Xerox/OBT**

October 2019

CSR
Cyber Security Council
Cyber Security Raad