CSR Cyber Security Raad

MEERJARENSTRATEGIE 2018-2021

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

Mahatma Gandhi (1869 - 1948)

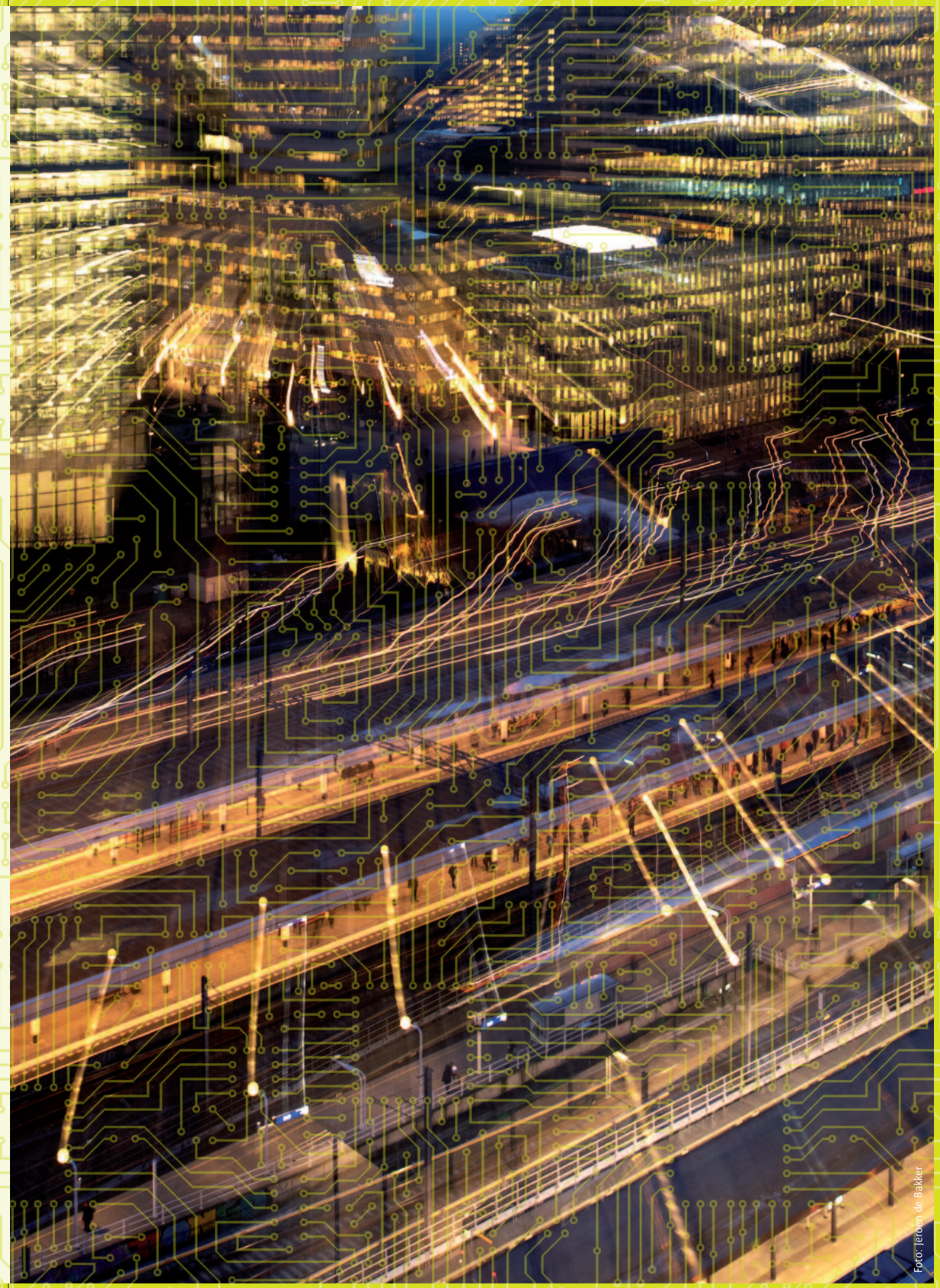

Foto: Jeroen de Bakker

VOORWOORD

Nederland bevindt zich in de voorhoede als het gaat om digitalisering; we hebben een van de grootste internetknooppunten ter wereld en we beschikken over razendsnelle, breedband telecomnetwerken. Hierdoor zijn we een van de meest ICT-intensieve economieën van Europa en staan we momenteel zevende in de wereld en vierde in Europa (2017). Om onze digitale positie vast te houden, kunnen we het ons niet permitteren om stil te zitten. Wereldwijd is een toename te zien in het aantal cyberaanvallen. Ook Nederland is en blijft een aantrekkelijk doelwit voor actoren. Toch is het urgentiegevoel onder politici, bestuurders, ondernemers en burgers nog lang niet altijd hoog genoeg. De awareness en het urgentiebesef in ons land is te laag. Vooral de menselijke factor blijkt een zwakke schakel binnen cybersecurity.

In de afgelopen jaren heeft de Cyber Security Raad (CSR) daarom nadrukkelijk ingezet op het op de agenda krijgen van cybersecurity in Nederland, publiek én privaat. Enerzijds door adviezen te geven en onderzoek te laten doen en anderzijds door onderwerpen voor het belang van cybersecurity in de media te brengen en bij te dragen aan de bewustwording. Voorbeelden zijn de adviezen 'Cybersecurity in het onderwijs en bedrijfsleven', 'Naar een landelijk dekkend stelsel van informatieknooppunten' en ‘Naar een veilig verbonden digitale samenleving’ en de rapporten ‘Internet of Things: kansen, bedreigingen en maatregelen’ en ‘De economische en maatschappelijke noodzaak van meer cybersecurity – Nederland digitaal droge voeten’. Ook heeft de CSR boardroomgesprekken gehouden bij verschillende organisaties in Nederland om de urgentie van cybersecurity op de agenda te zetten en organiseert de raad bijeenkomsten en seminars om met bestuurders over cybersecurity-thema's in gesprek te gaan. Tot slot stimuleert de CSR de oprichting van gelijksoortige raden met publiek-privaat-wetenschappelijke samenstelling in andere EU-landen. Hiertoe heeft de raad onder andere gesprekken gevoerd in Denemarken en België.

Daarmee zijn we er nog niet. De digitalisering neemt in de komende jaren wereldwijd verder toe en daarmee ook de afhankelijkheid van ICT. Dit biedt enorme kansen voor de Nederlandse samenleving en economie. Cybersecurity is een randvoorwaarde om deze kansen ook daadwerkelijk te kunnen verzilveren en daar moeten we in (blijven) investeren. De regering investeert structureel 95 miljoen euro in cybersecurity. Dit bedrag wordt verdeeld over verschillende departementen. Hiertoe wordt een ambitieuze cybersecurity-agenda opgesteld met onder meer aandacht voor standaarden voor Internet-of-Things-apparaten, het stimuleren van cybersecurity-onderzoek en het verbeteren van voorlichtingscampagnes op het gebied van cyberhygiëne.

Vertrouwen in de samenleving en haar structuren is van cruciaal maatschappelijk belang. Nederland moet een veilig, open en welvarende samenleving zijn en blijven. Het behouden van onze digitale positie blijft prioriteit en dit vraagt structurele aandacht van regering, politici, beleidsmakers, bestuurders, toezichthouders, bedrijven en burgers.

Iedereen heeft een verantwoordelijkheid in het gezamenlijk beschermen van onze economie, welvaart en maatschappij. Centrale aansturing is daarbij noodzakelijk en de overheid heeft hierin een belangrijke (voorbeeld)rol; burgers en bedrijven moeten zaken met de overheid veilig online kunnen doen.

De basis op orde geldt ook voor het bedrijfsleven. Cybersecurity is een verantwoordelijkheid van de boardroom. Het is belangrijk dat bedrijven hun eigen netwerken beschermen en zich weerbaar maken tegen cyberaanvallen. Daarom is het advies om minimaal tien procent van het ICT-budget aan te wenden voor cybersecurity.

Van burgers wordt tot slot een zekere mate van cyberhygiëne en eigen verantwoordelijkheid verwacht. De overheid faciliteert dit samen met het bedrijfsleven door het verbeteren van de digitale vaardigheden en het benadrukken van de zorgplichten van bedrijven en overheden richting hun gebruikers. Speciale aandacht vraagt de raad ook voor de jeugd. De jeugd is immers onze toekomst. Er moet structurele aandacht komen voor de digitale opvoeding van jongeren in zowel het basis- als het voortgezet onderwijs. Ook moet er meer aandacht voor loopbaanmogelijkheden zijn op het vlak van cybersecurity om het groeiende tekort aan cybersecurityspecialisten tegen te gaan. De CSR heeft daarom in 2016 de jaarlijkse National Cyber Security Summer School geïnitieerd.

Kortom, om Nederland in de digitale voorhoede te houden is er werk te verzetten. In de afgelopen jaren heeft de CSR al veel acties hiertoe in gang gezet en ook in de komende jaren blijven we dit doen. Jaarlijks zullen we ons actief inzetten om de bewustwording en de digitale weerbaarheid in ons land te vergroten. In de komende jaren gaat de raad actief met een aantal specifiek strategische thema’s specifiek gericht op cybersecurity aan de slag, waaronder regie en sturing, groeiende (digitale) afhankelijkheid, handhaving en toezicht en nieuwe technologieën. Hoe we tot deze thema’s zijn gekomen, leest u in de meerjarenstrategie van de CSR.

Het cyberlandschap is echter continu in beweging. Het is een permanente ratrace en dat dwingt ons om continu alert en voorbereid te zijn op alle mogelijke scenario’s. Dat geldt uiteraard ook voor ons als raad. De actualiteit bepaalt onze agenda, dus is de CSR Meerjarenstrategie 2018-2021 een levend document dat we waar nodig aanvullen en aanpassen aan actuele ontwikkelingen.

Namens de Cyber Security Raad,
De covoorzitters

Dick Schoof en Jos Nijhuis

MISSIE, VISIE EN STRATEGIE

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en het bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen.

1.1 Missie

De raad levert een bijdrage aan een open, veilig en welvarend digitaal Nederland door advisering aan het kabinet en het bedrijfsleven (via het kabinet) op het gebied van cybersecurity.

1.2 Visie

De raad draagt met zijn werkzaamheden bij aan de ambitie van Nederland om een open en veilig land te zijn met een welvarende digitale economie. De werkzaamheden zijn erop gericht Nederland weerbaarder te maken tegen cyberaanvallen en de kansen te verzilveren die een digitaal veilige economie biedt.

1.3 Strategie

De raad investeert in de effectiviteit van de adviezen. De leden worden strategisch ingezet om de impact van de adviezen te vergroten. Zo voeren zij bijvoorbeeld het woord in de media en bewaken zij de opvolging van een uitgebracht advies. Per onderwerp kiest de CSR een passende werkwijze om tot impact te komen. De raad beschikt over een gevarieerd repertoire aan werkwijzen (‘klassieke’ adviezen, handreikingen, gesprekken en bijeenkomsten) die afgewogen worden ingezet. De raad houdt ook scherp oog voor de impact van de producten en adviezen die hij uitbrengt. Daartoe stelt de CSR een strategisch plan op zodat de raad op de voet kan volgen in hoeverre de producten en adviezen een bijdrage leveren aan een veilig, open en welvarende samenleving.

1.4 Taken van de raad

De raad heeft drie taken die bijdragen aan het behalen van de missie. Bij de uitvoering van deze taken worden de volgende uitgangspunten gehanteerd:

1. De raad opereert alleen initiërend en zal niet structureel de uitvoering van initiatieven ter hand nemen.
2. De raad adviseert het kabinet en het bedrijfsleven (via het kabinet) over strategische cybersecurity-onderwerpen. Deze adviezen zijn richtinggevend en zetten aan tot handelen. De adviezen zijn gericht op de overheid en private sectoren (niet op individuele bedrijven).
3. De raad produceert niet alleen 'klassieke' adviezen, maar werkt ook met andere producten en activiteiten, zoals handreikingen, gesprekken en bijeenkomsten.

De taken van de raad:

1. **Het gevraagd en ongevraagd verstrekken van strategisch advies over cybersecurity aan het kabinet en het bedrijfsleven (via het kabinet).**

2. **Het volgen van trends en nieuwe technologische ontwikkelingen en deze waar nodig vertalen in strategische adviezen over mogelijke maatregelen om de risico's voor cybersecurity te verkleinen en de economische kansen te vergroten.**

3. **Het initiëren en/of versnellen van relevante initiatieven binnen Nederland en de Europese Unie die een aantoonbare bijdrage leveren aan het verhogen van het cybersecurityniveau in Nederland.**

Ad 1 Het gevraagd en ongevraagd verstrekken van strategisch advies over cybersecurity aan het kabinet en het bedrijfsleven (via het kabinet).

De raad geeft gevraagd en ongevraagd advies over relevante cybersecurity-onderwerpen. De adviezen zijn onderbouwd, richtinggevend, strategisch van aard en praktisch uitvoerbaar. Bijvoorbeeld de uitvoering en uitwerking van strategische beleids- en onderzoeksplannen vanuit de Rijksoverheid, zoals een (Inter)Nationale Cyber Security Strategie en de Nationale Cyber Security Research Agenda.
De raad streeft ernaar om praktische adviezen te geven en de awareness voor cybersecurity te vergroten. De leden spannen zich individueel in voor een digitaal veilig Nederland door boardroomgesprekken te voeren bij bedrijven met vitale processen voor ons land. Deze gesprekken hebben tot doel cybersecurity hoger op de agenda te krijgen. Een goede positionering van de raad is daarbij van belang.

Ad 2 Het volgen van trends en nieuwe technologische ontwikkelingen en deze waar nodig vertalen in strategische adviezen over mogelijke maatregelen om de risico's voor cybersecurity te verkleinen en de economische kansen te vergroten.

De raad anticipeert op de digitale toekomst door een visie te ontwikkelen op prioritaire cybersecurity-thema's. De technologische ontwikkelingen gaan razendsnel en nieuwe technologieën zijn een belangrijke drijfveer voor innovatie en economische groei. Cruciaal daarbij is het vermogen om technologische ontwikkelingen te (h)erkennen en te prioriteren op relevantie. De raad volgt trends en nieuwe technologische ontwikkelingen op de voet en vertaalt deze waar nodig naar strategische adviezen. De adviezen gaan onder andere over te nemen strategische maatregelen om risico's op het vlak van cybersecurity te verkleinen en economische kansen te vergroten.

Ad 3 Het initiëren en/of versnellen van relevante initiatieven binnen Nederland en de Europese Unie die een aantoonbare bijdrage leveren aan het verhogen van het cybersecurityniveau in Nederland.

De raad kan besluiten om nieuwe initiatieven in gang te (laten) zetten. Vanuit zijn positie kan de raad een (overheids)organisatie of een sector het verzoek doen een bepaald initiatief uit te voeren. De Nationale Cyber Security Summer School (NCS3) is daar een voorbeeld van. De raad kan gerichte adviezen uitbrengen die de versnelling brengen in de strategische aanpak van cybersecurity. Gezien het mondiale karakter van cybersecurity vraagt de raad in zijn adviezen ook aandacht voor een Europese en internationale aanpak.

1.5 Kernwaarden

De kernwaarden van de CSR zijn:

Onafhankelijk - De raad is onafhankelijk en stelt zich kritisch op ten aanzien van alle spelers in het cybersecurityveld (*Countervailing power*).

Algemeen belang - De leden stellen het belang van een veilig en welvarend Nederland boven het belang van hun individuele (zakelijke) belangen en opvattingen. De kracht van de publiek, private én wetenschappelijke samenwerking wordt ten volle benut.

Toekomstgericht - De leden plaatsen de vraagstukken in een strategisch en toekomstgericht perspectief. De oplossingen zijn mede gebaseerd op een visie op de toekomst.

1.6 Samenstelling

De samenstelling van de CSR is gerelateerd aan de in de programmering geformuleerde doelstellingen. De raad streeft naar een zo breed mogelijke dekking van invalshoeken op het terrein van cybersecurity. Daarom hebben achttien leden zitting volgens de verdeelsleutel 7-7-4: zeven leden uit de private sector, zeven leden uit de publieke sector en vier leden uit de wetenschap. De CSR heeft twee covoorzitters: één namens de publieke sector en één namens de private sector. De leden vertegenwoordigen een relevante organisatie of sector binnen het cybersecuritydomein. De leden worden volgens een vastgestelde procedure benoemd.

De unieke samenstelling (publiek, privaat en wetenschap) maakt het mogelijk prioriteiten, knelpunten en kansen vanuit diverse invalshoeken te benaderen. Door onze onafhankelijkheid en kritische blik houdt de raad de Nederlandse aanpak voor cybersecurity scherp en levert zo een wezenlijke bijdrage aan een veilig, open en welvarende samenleving. De standpunten van de CSR winnen door deze brede samenstelling aan kracht.

BELANGRIJKE ONTWIKKELINGEN OP HET VLAK VAN CYBERSECURITY

De afgelopen periode is een aantal toonaangevende rapporten gepubliceerd over het thema cybersecurity die het onderwerp vanuit verschillende invalshoeken belichten. Op basis van een aantal van deze rapporten heeft de raad de belangrijkste ontwikkelingen op het gebied van cybersecurity die de komende jaren zullen (blijven) spelen, geïnventariseerd. De publicaties zijn afkomstig van gerenommeerde instituten en hebben de aandacht gekregen in de Nederlandse pers. Dit hoofdstuk bevat een samenvattende analyse hiervan.

2.1 Analyse rapporten

Over het geheel beschouwd kunnen we stellen dat Nederland zich wereldwijd in de voorhoede bevindt als het gaat om digitalisering; we hebben een van de grootste internetknooppunten ter wereld en we beschikken over razendsnelle, breedband telecomnetwerken. Daarmee staat Nederland momenteel zevende in de wereld en vierde in Europa (2017) op het terrein van 'e-government development and online service delivery'. Daarmee is Nederland nog niet volledig cyberready[1]. Nederland heeft de ambitie om de economische kansen die het nieuwe tijdperk met zich meebrengt te verzilveren en onze digitale positie vast te houden; Nederland moet een veilig, open en welvarende samenleving zijn en blijven. Om dat te bereiken is er nog veel werk te verzetten. De digitale weerbaarheid in Nederland blijft volgens onderzoekers achter bij de groei van cyberdreigingen.

Groeiende (digitale) afhankelijkheid

Een belangrijk terugkerend thema in de rapporten is de groeiende afhankelijkheid van digitalisering binnen onze samenleving. Digitalisering neemt de komende jaren wereldwijd verder toe en daarmee kan ook de afhankelijkheid van ICT verder meegroeien. Niet alleen stijgt het aantal internetgebruikers al jarenlang, ook het aantal apparaten en gebruiksvoorwerpen dat verbinding heeft met het internet neemt wereldwijd zeer snel toe. Deze afhankelijkheid en het belang van cybersecurity gaan hand in hand. De nationale en economische veiligheid zijn daar mede afhankelijk van. Vertrouwen in de samenleving en haar structuren is daarmee van maatschappelijk belang. Burgers en bedrijven moeten kunnen blijven vertrouwen op de bescherming en rechtsorde die de overheid biedt. De overheid dient ook zorg te dragen voor hen die achterblijven in de maatschappij door de toenemende digitalisering.

1 Potomac Institute for Policy Studies. (2017), The Netherlands cyber readiness at a glance, Arlington

De Nederlandse digitale infrastructuur is sterk afhankelijk van een select aantal buitenlandse organisaties, wat Nederland potentieel kwetsbaar kan maken. Steeds vaker willen overheden en bedrijven regie voeren over eigen data. Het urgentiebesef binnen de Europese Unie begint te komen om data veilig op te slaan en onder een regime van wet- en regelgeving te laten vallen om zodoende aan Europese afspraken te voldoen.

Soevereiniteit

In het digitale domein speelt soevereiniteit al langer een grote rol van betekenis. Vooralsnog zijn autoritaire landen als China en Iran (negatieve) voorbeelden van landen die de eigen soevereiniteit misbruiken door het afschermen van een 'nationaal' deel van het internet. Inmiddels spreken ook westerse landen zich uit over eigen soevereiniteit. Daarbij gaat het vooral om een betere bescherming van het internet en data, mede ingegeven door de onthullingen van Edward Snowden.

(Analoge) fallback-scenario's

De groeiende afhankelijkheid door de digitalisering van onze samenleving zal de komende jaren verder toenemen. De afhankelijkheid van de digitale technologie brengt grote risico's met zich mee voor de continuïteit van de (maatschappelijke) dienstverlening. Dit komt doordat het aantal analoge fallback-scenario's afneemt en alternatieve opties niet (meer) beschikbaar zullen zijn. Er zijn verschillende redenen toe te wijzen aan deze afname; de meest genoemde reden is de hoge kosten voor systemen.

Ethische en maatschappelijke vraagstukken

Door de groeiende afhankelijkheid vormen zich nieuwe ethische en maatschappelijke uitdagingen. Publieke waarden en mensenrechten als privacy, gelijke behandeling, autonomie en menselijke waardigheid dreigen in het geding te komen doordat huidige wettelijke kaders in voorkomende gevallen onvoldoende toekomstgericht zijn. Door technologische convergentie zijn de kaders die we gebruiken voor publieke waarden niet langer vanzelfsprekend, waardoor de bescherming van publieke waarden op dit moment onduidelijk is en soms tekort schiet. De kaders zullen minimaal in Europees verband moeten worden ontwikkeld.

Nieuwe technologieën

Nieuwe technologieën brengen kansen en risico's met zich mee. Onderzoek en innovatie spelen een belangrijke rol bij het zoeken naar oplossingen en kunnen een veilige toepassing van (nieuwe) technologieën bevorderen. Nederland moet hier actief op (blijven) inspelen door bijvoorbeeld het opbouwen van kennis en het tijdig inspelen op de consequenties – zowel positief als negatief – die deze technologieën kunnen hebben op onze digitale veiligheid, bijvoorbeeld bij ethische en publieke waarden. Een aantal voorbeelden van nieuwe technologieën die in de aankomende jaren een rol gaan spelen, zijn: robotica, blockchain, biometrie, Internet of Things (IoT), kunstmatige intelligentie, kwantumcomputing en big data.

Regie en sturing

Volgens de onderzoekers ontbreekt het op dit moment in Nederland aan voldoende sturing en regie op het terrein van cybersecurity. Voor een veilig, open en welvarende samenleving is de coördinatie en sturing zowel bij overheden zelf als voor publiek-private samenwerking belangrijk. De overheid heeft hierin een (voorbeeld)rol, maar de invulling ervan is nog niet uitgekristalliseerd. Ook is er sprake van versnippering over een groot aantal ongelijksoortige partijen. Hierdoor is onduidelijk welke partij voor welke taak verantwoordelijk is. Zo is de beleidsverantwoordelijkheid voor ICT en specifiek cybersecurity in ons land verdeeld over ten minste vijf departementen en zijn er tal van agentschappen, zelfstandige bestuursorganen (ZBO's) en toezichthouders actief.

Het afstemmen van de verschillende strategieën en agenda's is randvoorwaardelijk om een integrale aanpak te kunnen ontwikkelen[2].

(Publiek-private) samenwerking

De publiek-private samenwerking moet ook de samenwerking behelzen met niet-gouvernementele organisaties (NGO's). Voorbeelden van samenwerking zijn er in de vitale infrastructuur en de aanpak van cybercrime door de Nederlandse bankensector. Toch blijkt dat de publiek-private samenwerking op een hoger plan zou kunnen komen. Het verstevigen van deze samenwerking en het beter coördineren ervan wordt als noodzakelijk gezien. Het gaat hierbij vooral om het ontwikkelen van een cultuur waarin het delen van kennis, ervaring en het beter afstemmen van initiatieven als vanzelfsprekend wordt ervaren. Organisaties moeten op het gebied van cybersecurity nauwer samenwerken in de ketens.

Ook moet Nederland blijven samenwerken op internationaal niveau. Geen enkel land kan de vraagstukken rondom cybersecurity zelfstandig oplossen. De vraagstukken hebben een grensoverschrijdend karakter. Binnen de Europese Unie worden in toenemende mate wetten en regels gemaakt. De NIB-richtlijn (richtlijn netwerk- en informatiebeveiliging), de privacyregeling en de in september 2017 verschenen eerste conceptversie van de verordening voor de nieuwe Europese cybersecuritystrategie zijn daar voorbeelden van. Nederland zou een sterk agendazettende rol kunnen vervullen binnen de EU.

Investering cybersecurity

Om onze digitale positie vast te houden en te kunnen blijven concurreren met landen als het Verenigd Koninkrijk, Frankrijk, Duitsland en de Scandinavische landen is het van belang om meer te investeren in cybersecurity. Op dit moment investeert Nederland minder dan 0,01% van het bruto nationaal product (bnp) aan cybersecurity, terwijl concurrerende landen structureel meer investeren.

Cybercriminaliteit

Nederland is en blijft een interessant doelwit voor cybercriminelen. Het inzichtelijk krijgen van de (economische) schade van cybercrime blijft lastig. Meerdere organisaties hebben gelijksoortige onderzoeken uitgevoerd, hieruit blijkt dat er geen eenduidig beeld van de schade van cybercrime is. Een recente schatting is dat cybercrime Nederlandse organisaties 10 miljard per jaar kost[3]. Cyber enabled crime en cybercrime komen relatief veel voor in Nederland. De verwachting is echter dat cybercrime over een aantal jaar in veel landen omvangrijker is dan traditionele criminaliteit[4]. Waarbij rekening gehouden moet worden met het feit dat traditionele criminaliteit doorontwikkelt waardoor het een digitaal component krijgt.

Uit het Nationaal Veiligheidsprofiel (NVP) en het Cybersecuritybeeld Nederland (CSBN) blijkt eveneens dat cyberspionage door landen als Rusland en China een steeds aannemelijker risico is, hoger dan epidemieën, natuurrampen en nucleaire ongevallen.

Ook cyberterrorisme en cybersabotage vormen een groot risico dat tot grote economische schade en maatschappelijke ontwrichting kan leiden. Om dit te voorkomen is er aandacht nodig voor Industrial Automation & Control Systems (IACS). De aandacht binnen cybersecurity voor IT is vele malen groter dan operationele technologie (OT). Steeds meer fysieke objecten

2 Nederland heeft verschillende strategieën en agenda's ontwikkeld omtrent cybersecurity. Het ministerie van Justitie en Veiligheid heeft de Cybersecurity Strategie 2.0: van bekwaam naar bewust, het ministerie van Economische Zaken en Klimaat heeft de Digitale Agenda: vernieuwen, vertrouwen en versnellen, het ministerie van Buitenlandse Zaken heeft de Internationale cyberstrategie: digitaal bruggen slaan, het ministerie van Defensie heeft de Defensie Cyber Strategie en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek heeft de National Cyber Security Research Agenda II.

3 Deloitte 'Cyber Value at Risk in The Netherlands', september 2017

4 Internet organised crime threat assessment 2017, Europol

zoals bruggen, tunnels, sluizen en ook machines zijn verbonden aan het internet. Het veilig houden van deze fysieke objecten is van belang voor de continuïteit en het veilig houden van Nederland. Het internet wordt in Nederland nog niet beschouwd als vitale infrastructuur.

Bij het bestrijden van cybercrime tegen bijvoorbeeld de georganiseerde misdaad en statelijke actoren blijkt attributie een lastig vraagstuk. Actoren maken gebruik van technische mogelijkheden waardoor het lastig is te achterhalen welke actoren betrokken zijn bij een cyberaanval. Daardoor ontkomen daders vaak aan vervolging, omdat niet altijd te achterhalen is en/of met zekerheid vast te stellen welk type actor achter een bepaalde cyberaanval zit. Een van de oorzaken hiervoor is het gebrek aan meldingen/aangiften waardoor er een incompleet beeld van cybercrime in Nederland is. Inzicht in cybercrime is noodzakelijk om effectiever erop in te kunnen spelen. De oorzaak van het lage aantal meldingen ligt onder andere in de complexiteit van het doen van aangifte. De kans op imagoschade voor het betreffende bedrijf is ook een belangrijke factor in het niet doen van aangifte.
Omdat vraagstukken op het vlak van cybersecurity een grensoverschrijdend karakter hebben is ook Europese samenwerking noodzakelijk in de bestrijding tegen cybercrime.

Basisbeveiliging

De awareness en het urgentiebesef in ons land is nog te laag. Overheid, bedrijfsleven en burgers nemen veel stappen om de digitale weerbaarheid te vergroten, maar dit gaat niet snel genoeg. Vooral de menselijke factor blijkt nog altijd een zwakke schakel binnen cybersecurity. De kansen en bedreigingen van digitalisering staan onvoldoende op ons netvlies en zijn geen integraal onderdeel van ons denken en doen. Alle overheden, ook medeoverheden, hebben een voorbeeldrol; burgers en bedrijven moeten zaken met de overheid veilig online kunnen doen. Informatie moet online beschikbaar zijn en de uitwisseling van gegevens goed beveiligd. De basisbeveiliging moet dan goed op orde zijn en netwerken beschermd tegen cyberaanvallen. Zowel binnen de overheid als in het private domein is de basisbeveiliging nog onvoldoende op orde. Op het gebied van cybersecurity zijn er al wel verschillende gerenommeerde normenkaders en baselines ontworpen[5] die bijdragen aan een goede basisbeveiliging. Daarbij is het van belang dat leveranciers zich houden aan de baseline en de levenscyclus van producten en diensten duidelijk communiceren.

Zorgplichten en toezicht

Voor fabrikanten kunnen zorgplichten en productaansprakelijkheid incentives zijn om de digitale veiligheid van hun producten serieus te nemen. De Amerikaanse Federal Trade Commission (FTC) is een voorbeeld van actief toezicht op het gebied van ICT. Nederland kent geen vergelijkbare toezichthouder die op eenzelfde wijze kan optreden tegen onvoldoende beveiligd ICT-apparatuur. De toezicht en naleving van de Meldplicht Datalekken en de beveiliging van persoonsgegevens is in handen van de Autoriteit Persoonsgegevens (AP).

Daarnaast kent de huidige wetgeving meerdere zorgplichten toe aan organisaties ten aanzien van digitale beveiliging. Het ontbreekt aan consensus over wat de basisveiligheid zou moeten inhouden. Het handhaven van wet- en regelgeving in het digitale domein behoeft meer aandacht.

Cyberwarfare

In politieke vraagstukken speelt cyberwarfare steeds vaker een rol. Zo is er volop aandacht voor digitale beïnvloeding van democratische instituties in meerdere westerse landen waaronder Nederland. Beïnvloeding van democratische waarden is een substantieel risico geworden. Net als andere landen heeft Nederland het cyberdomein toegevoegd aan de nationale veiligheidsagenda. Alle vitale belangen die de Nederlandse overheid dient te beschermen, zijn doordrongen van digitale systemen. Het cyberdomein wordt steeds meer het terrein van geopolitieke en terroristische dreigingen. Nederland heeft een begin gemaakt met de inrichting van cyberdiplomatie. Ook wordt er gewerkt aan mondiale normen op het gebied van cybersecurity vanuit de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) en de Verenigde Naties (VN). Door meer transparantie over wat wel en niet is toegestaan en hoe daarop gereageerd mag worden, worden conflicten in de toekomst beheersbaarder.

Digitale geletterdheid

Ten opzichte van verschillende landen blijft Nederland achter als het gaat om digitale vaardigheden. Om een veilig, open en welvarende samenleving te zijn en blijven, is het van belang dat we in Nederland structureel aandacht besteden aan de digitale opvoeding van jongeren in het basis- en voortgezet onderwijs. Dit om hen beter voor te bereiden op het digitale heden en de toekomst.
Ook moet er meer aandacht komen voor loopbaanmogelijkheden op het vlak van cybersecurity om het groeiende tekort aan cybersecurityspecialisten tegen te gaan.

5. Onder andere: Baseline Informatiebeveiliging Rijksoverheid, Baseline Informatiebeveiliging Gemeenten, Baseline Informatiebeveiliging Waterschappen, ISO27000 reeks en de NEN7510. Er wordt op dit moment gewerkt aan een Baseline Informatiebeveiliging Overheid, als vervanging van de bestaande overheidsbaselines.

2.2 Ontwikkelingen: een samenvatting

Groeiende (digitale) afhankelijkheid

- Digitalisering neemt wereldwijd verder toe en de afhankelijkheid van ICT groeit verder mee.
- Het aantal internetgebruikers stijgt alsook het aantal apparaten dat verbinding heeft met het internet.
- De Nederlandse digitale infrastructuur blijkt afhankelijk te zijn van een select aantal buitenlandse organisaties; dit kan Nederland potentieel kwetsbaar maken.
- De Europese Unie wil data veilig opslaan en onder een regime van wet- en regelgeving laten vallen.

Soevereiniteit

- Soevereiniteit speelt een grote rol van betekenis in het digitale domein.
- China en Iran zijn (negatieve) voorbeelden van landen die soevereiniteit misbruiken.
- Ook westerse landen spreken zich uit over eigen soevereiniteit; zij willen een betere bescherming van het internet en data.

(Analoge) fallback-scenario's

- Ondanks de groeiende afhankelijkheid neemt het aantal (analoge) fallback-scenario's af.
- Dit brengt grote risico's met zich mee voor de continuïteit van de (maatschappelijke) dienstverlening.
- Voornaamste reden voor de afname is de hoge kosten voor systemen.

Maatschappelijke en ethische vraagstukken

- De groeiende afhankelijkheid brengt nieuwe ethische en maatschappelijke uitdagingen met zich mee.
- Publieke waarden en mensenrechten dreigen in het geding te komen doordat huidige wettelijke kaders in voorkomende gevallen onvoldoende toekomstgericht zijn.
- Nieuwe kaders zullen minimaal in Europees verband moeten worden ontwikkeld.

Nieuwe technologieën

- Nieuwe technologieën brengen kansen en risico's met zich mee.
- Onderzoek en innovatie kunnen een veilige toepassing van (nieuwe) technologieën bevorderen.
- Nederland moet hier actief op (blijven) inspelen.
- Voorbeelden van nieuwe technologieën die in de aankomende jaren een rol gaan spelen, zijn: robotica, blockchain, biometrie, Internet of Things (IoT), kunstmatige intelligentie, kwantumcomputing en big data.

Regie en sturing

- Er is in Nederland onvoldoende sturing en regie op het terrein van cybersecurity.
- Coördinatie en sturing bij overheden en publiek-private samenwerking is belangrijk.
- De overheid heeft hierin een (voorbeeld)rol.
- Ook is er sprake van versnippering over een groot aantal ongelijksoortige partijen. Hierdoor is onduidelijk welke partij voor welke taak verantwoordelijk is.
- Het afstemmen van de verschillende strategieën en agenda's is randvoorwaardelijk voor een integrale aanpak.

(Publiek-private) samenwerking

- Publiek-private samenwerking is van belang ook met niet-gouvernementele organisaties (NGO's) en moet op een hoger plan komen.
- Er zijn verschillende goede voorbeelden in de vitale infrastructuur en de Nederlandse bankensector.
- Organisaties moeten op het gebied van cybersecurity nauwer samenwerken in de ketens door kennis en ervaring te delen en initiatieven op elkaar af te stemmen.

Investering cybersecurity

- Nederland moet meer investeren in cybersecurity om te kunnen blijven concurreren met de landen om ons heen.
- Op dit moment investeert Nederland minder dan 0,01% van het bruto nationaal product (bnp) aan cybersecurity, terwijl concurrerende landen structureel meer investeren.

Cybercriminaliteit

- Cybercrime neemt toe en wordt omvangrijker dan traditionele criminaliteit.
- Een recente schatting is dat cybercrime Nederlandse organisaties 10 miljard per jaar kost.
- Cyber enabled crime en cybercrime komen relatief veel voor in Nederland.
- Cyberspionage door landen als Rusland en China is een steeds aannemelijker risico, hoger dan epidemieën, natuurrampen en nucleaire ongevallen.
- Ook cyberterrorisme en cybersabotage vormen een groot risico als het gaat om cybersecurity.
- Aandacht is eveneens nodig voor Industrial Automation & Control Systems (IACS). De aandacht binnen cybersecurity voor IT is vele malen groter dan operationele technologie (OT).
- Attributie blijkt een lastig vraagstuk; daders ontkomen vaak aan vervolging.
- Een van de oorzaken hiervoor is het gebrek aan meldingen/aangiftes waardoor er een incompleet beeld van cybercrime in Nederland is.
- De oorzaak van het lage aantal meldingen ligt onder andere in de complexiteit van het doen van aangifte.
- Ook de kans op imagoschade voor het betreffende bedrijf is een belangrijke factor in het niet doen van aangifte.
- Europese samenwerking is noodzakelijk in de bestrijding tegen cybercrime.

Basisbeveiliging

- De awareness en het urgentiebesef in ons land is vooralsnog te laag.
- De menselijke factor blijkt nog altijd een zwakke schakel binnen cybersecurity.
- Alle (mede)overheden hebben een voorbeeldrol.
- Zowel binnen de overheid als in het private domein is de basisbeveiliging nog onvoldoende op orde.
- Er zijn wel verschillende gerenommeerde normenkaders en baselines ontworpen die bijdragen aan een goede basisbeveiliging.

Zorgplichten en toezicht

- Het handhaven van wet- en regelgeving in het digitale domein behoeft meer aandacht.
- De huidige Nederlandse wetgeving kent meerdere zorgplichten toe aan organisaties ten aanzien van digitale beveiliging.
- De toezicht en naleving van de Meldplicht Datalekken en de beveiliging van persoonsgegevens is in handen van de Autoriteit Persoonsgegevens (AP).

Cyberwarfare

- In politieke vraagstukken speelt cyberwarfare steeds vaker een rol.
- Beïnvloeding van democratische waarden is een substantieel risico geworden.
- Nederland heeft, net als andere landen, het cyberdomein toegevoegd aan de nationale veiligheidsagenda en een begin gemaakt met de inrichting van cyberdiplomatie.
- Ook wordt er gewerkt aan mondiale normen op het gebied van cybersecurity vanuit de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) en Verenigde Naties (VN).
- Meer transparantie over wat wel en niet is toegestaan en hoe daarop gereageerd mag worden, maakt conflicten in de toekomst beheersbaarder.

Digitale geletterdheid

- De jeugd is onze toekomst: meer structurele aandacht voor digitale opvoeding in het onderwijs is gewenst.
- Meer aandacht is nodig voor loopbaanmogelijkheden op het vlak van cybersecurity om het groeiende tekort aan cybersecurityspecialisten tegen te gaan.

2.3 Bronvermelding

De analyse in dit hoofdstuk is gebaseerd op een literatuurstudie van de volgende rapporten en publicaties:

- Centraal Planbureau (2017), Risicorapportage cyberveiligheid economie, Den Haag;
- Gartner (2016), Special Report: Cybersecurity at the Speed of Digital Business, Stamford;
- Gartner (2017), Hype Cycle for Threat-Facing Technologies, 2017, Stamford;
- Kool, L., J. Timmer, L. Royakkers, & R. van Est (2017), Opwaarderen - Borgen van publieke waarden in de digitale samenleving, Den Haag, Rathenau Instituut;
- Munnichs, G., Kouw, M., & Kool, L. (2017), Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid, Den Haag, Rathenau Instituut;
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017), Cybersecuritybeeld Nederland 2017, Den Haag, Nationaal Coördinator Terrorismebestrijding en Veiligheid;
- Potomac Institute for Policy Studies (2017), The Netherlands cyber readiness at a glance, Arlington;
- Verhagen, H. (2016), De economische en maatschappelijke noodzaak van meer cybersecurity, Den Haag;
- Wetenschappelijke Raad voor het Regeringsbeleid (2015), De publieke kern van het internet, Den Haag/Amsterdam: Amsterdam University Press;
- Wetenschappelijke Raad voor het Regeringsbeleid (2017), Veiligheid in een wereld van verbindingen, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid;
- World Economic Forum (2017), The Global Risks Report 2017, Geneva: World Economic Forum;
- World Economic Forum (2018), The Global Risks Report 2018, Geneva: World Economic Forum.

Foto: Jeroen de Bakker

MEERJARENSTRATEGIE CSR

De urgentie is helder. Nederland kan voortbouwen op een solide basis die in het verleden is gelegd. We kunnen echter niet achterover leunen en moeten actief blijven werken aan het niveau van cybersecurity om de vooraanstaande positie te behouden en de economische kansen die een digitaal veilige economie biedt, te verzilveren. Daarbij is het identificeren van de strategische vraagstukken en tijdig daarop inspelen van groot belang. Ook in de komende jaren draagt de Cyber Security Raad (CSR) hieraan bij conform onze missie, visie en strategie.

De analyse in het voorgaande hoofdstuk bevat een overzicht van belangrijke (technologische) ontwikkelingen die risico's met zich meebrengen voor een veilig, open en welvarende samenleving. De CSR heeft deze ontwikkelingen vertaald naar een viertal strategische thema's waarmee de raad in de komende vier jaar aan de slag gaat om onze digitale positie te behouden en in de voorhoede te blijven als het gaat om digitalisering. Daarmee draagt de raad bij aan het versterken van de cybersecurity van Nederland. Aan de hand van de gekozen strategische thema's zal de raad gevraagd en ongevraagd strategisch advies verstrekken aan het kabinet en private partijen (via het kabinet) op het gebied van cybersecurity. Uiteraard blijft de raad ook inspelen op actuele thema's die in dit complexe domein kunnen ontstaan.

Aanvullend op de meerjarenstrategie brengt de CSR een tweejaarlijks werkprogramma uit waarin de strategische thema's vertaald zijn naar concrete acties.

De strategische thema's zijn:

1. **Regie en sturing**
2. **Groeiende (digitale) afhankelijkheid**
3. **Handhaving en toezicht**
4. **Nieuwe technologieën**

Ad 1 Regie en sturing

Voor een veilig, open en welvarende samenleving is de coördinatie en sturing zowel bij overheden zelf als voor publiek-private samenwerking belangrijk. De overheid heeft hierin een (voorbeeld)rol, maar de invulling ervan is nog niet uitgekristalliseerd. Dit heeft geleid tot een beperkte coördinatie en sturing. De beleidsverantwoordelijkheid voor ICT en specifiek

cybersecurity is verdeeld over tenminste vijf departementen. Daarnaast zijn er tal van agentschappen, zelfstandige bestuursorganen (ZBO's) en toezichthouders actief. Er is (politiek) geen eenduidig aanspreekpunt. Het versterken van de cybersecurity in Nederland vraagt om een goede coördinatie en sturing. Dat begint met het afstemmen van de verschillende strategieën en agenda's. Zo heeft het ministerie van Justitie en Veiligheid de Cybersecurity Strategie 2.0: van bekwaam naar bewust, het ministerie van Economische Zaken en Klimaat heeft de Digitale Agenda: vernieuwen, vertrouwen en versnellen, het ministerie van Buitenlandse Zaken heeft de Internationale cyberstrategie: digitaal bruggen slaan, het ministerie van Defensie heeft de Defensie Cyber Strategie en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek heeft de National Cyber Security Research Agenda II. De CSR zal hiertoe een adviserende rol vervullen.

Ad 2 Groeiende (digitale) afhankelijkheid

De digitalisering neemt de komende jaren verder toe en daarmee groeit de afhankelijkheid van ICT in onze samenleving. Zo krijgen we steeds meer internetgebruikers en is er ook een toename te zien in het aantal apparaten en gebruiksvoorwerpen dat verbinding heeft met het internet (Internet of Things). Steeds meer aandacht gaat ook uit naar Industrial Automation & Control Systems (IACS), systemen die binnen vitale en industriële sectoren worden gebruikt voor de automatische monitoring en besturing van vooral fysieke processen.

De afhankelijkheid van de digitale technologie brengt grote risico's met zich mee. Deze worden veelal veroorzaakt door de toenemende cybersecurityproblemen. Het toenemende aantal potentiële doelwitten als gevolg van de groei van clouddiensten en het Internet of Things (IoT) verhoogt ook de risico's. Ook zijn alternatieve opties niet (meer) beschikbaar. Dit kan Nederland potentieel kwetsbaar maken op het terrein van de continuïteit van (maatschappelijke) dienstverlening en brengt de vooraanstaande positie van ons land als het gaat om cybersecurity in het geding.

Ad 3 Handhaving en toezicht

Het handhaven van wet- en regelgeving in het digitale domein van onze samenleving behoeft meer aandacht. In tegenstelling tot andere landen beschikt Nederland niet over een toezichthouder die bijvoorbeeld op kan treden tegen onvoldoende beveiligd ICT-apparatuur. Het toezicht en de naleving van de Meldplicht Datalekken en de beveiliging van persoonsgegevens is formeel geregeld via de Autoriteit Persoonsgegevens (AP). Het certificeren van producten en diensten kan hier mogelijk een oplossing bieden. Willen we als land in de voorhoede blijven als het gaat om cybersecurity, dan zal de handhaving en toezicht hierop goed ingericht dienen te worden.
Opsporing en vervolging van cybercriminelen moet hoog op de agenda staan. De achterstand in kennis en mankracht dient te worden weggewerkt. Ook moet het melden van cybercrime voor burgers en bedrijven een stuk eenvoudiger worden.

Ad 4 Nieuwe technologieën

Nieuwe technologische toepassingen gaan razend snel. Bij nieuwe technologieën zouden security- en privacy-by-design uitgangspunten moeten zijn. Veel producenten willen hun 'smart products' vaak te snel lanceren. Ze willen allemaal als eerste op de markt zijn, zonder eerst de digitale veiligheid van deze producten te borgen. Het belang van standaardisatie en certificering neemt hierdoor toe. De raad wil aandacht besteden aan de mogelijkheden die nieuwe technologieën te bieden hebben, het verzilveren van kansen en bedreigingen het hoofd te bieden. Onderzoek en innovatie kunnen hier mogelijk een oplossing in bieden. Nederland moet hier actief op (blijven) inspelen door bijvoorbeeld het opbouwen van kennis en het tijdig inspelen op de consequenties – zowel positief als negatief – die deze technologieën kunnen hebben op onze digitale veiligheid, bijvoorbeeld bij ethische en publieke waarden.

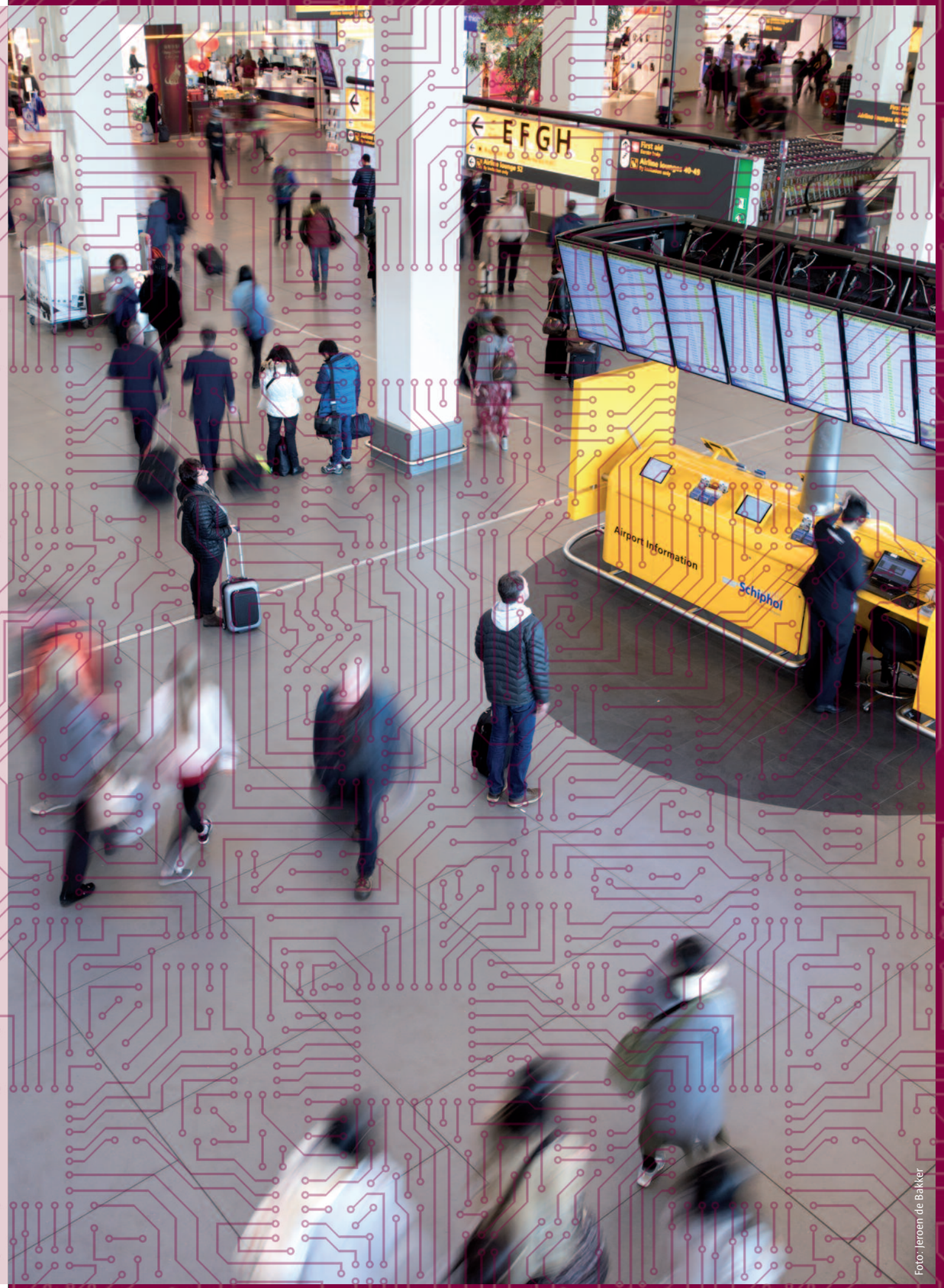

Foto: Jeroen de Bakker