Rathenau Instituut

Cyberweerbaar met nieuwe technologie

Kans en noodzaak van digitale innovatie

Rapport

Auteurs
Pieter van Boheemen[1], Geert Munnichs[1], Linda Kool[1], Gijs Diercks[1], Jurriën Hamer[1] & Anouk Vos[2]

[1] Rathenau Instituut
[2] Radically Open Security B.V.

Foto omslag
Maarten Hartman / Hollandse Hoogte

Bij voorkeur citeren als:
Rathenau Instituut (2020). *Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie.* Den Haag (auteurs: Boheemen, P. van, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos)

Voorwoord

Sommige mensen zetten een heel deel van hun leven in de cloud. Ook bedrijven en overheden doen dat, soms gaat het zelfs om vitale delen van de samenleving. Deze groeiende afhankelijkheid van vaak buitenlandse *cloud providers* creëert nieuwe risico's: uitval van functionaliteit bij verstoring, en verlies van controle en zeggenschap over data en dataverwerking. Omdat digitale kwetsbaarheden van aard veranderen, moeten we voortdurend investeren in cyberweerbaarheid. Ook nieuwe digitale ontwikkelingen, zoals *machine learning* en de komst van de kwantumcomputer, nopen daartoe.

Dit rapport, dat we schreven op verzoek van de Cyber Security Raad en dat past bij het thema Digitale Samenleving uit ons Werkprogramma, onderzoekt de kansen van nieuwe technologische ontwikkelingen voor de nabije toekomst, en hoe deze kunnen worden benut om de cyberweerbaarheid van Nederland te verhogen. Hiervoor deden we literatuuronderzoek, hielden we interviews en organiseerden we workshops met deskundigen, stakeholders en beleidsmakers.

We ontdekten dat cyberweerbaarheid is als het menselijk immuunsysteem. Dat is niet in staat alle aanvallen buiten de deur te houden. Het immuunsysteem rekent met indringers en interne incidenten af, of probeert ze onder de duim te houden. Wie gezond is, en preventieve maatregelen neemt, slaagt daar beter en langer in.

Nieuwe technologieën als (opnieuw) machine learning, post-kwantumcryptografie, LiFi, 5G-netwerken of gedistribueerde systemen bieden kansen om de cyberweerbaarheid te verhogen. Maar dat geldt ook voor veel bestaande technologieën, die nog onvoldoende worden benut. De overheid kan daarbij het voortouw nemen, bijvoorbeeld door breed sterke vormen van encryptie toe te passen en te investeren in de verdere ontwikkeling van machine learning en post-kwantumcryptografie.

Dit rapport geeft bouwstenen op grond waarvan de Cyber Security Raad een advies kan uitbrengen aan het kabinet.

Dr. ir. Melanie Peters
Directeur Rathenau Instituut

Samenvatting

Inleiding
De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en bestaat uit vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich in om de cyberweerbaarheid in Nederland te verhogen. De raad heeft het Rathenau Instituut verzocht onderzoek te doen naar de manier waarop nieuwe technologieën kunnen bijdragen aan het verhogen van de cyberweerbaarheid in Nederland. Het onderzoek moet bouwstenen aanleveren op grond waarvan de CSR een advies kan uitbrengen aan het kabinet.

Voor het onderzoek is ingegaan op:
- de technologische ontwikkelingen die Nederland op de middellange termijn (2-8 jaar) te wachten staan;
- de gevolgen daarvan voor bestaande cyberkwetsbaarheden;
- de kansen die nieuwe technologische mogelijkheden bieden om de cyberweerbaarheid te verhogen;
- de voorwaarden waaraan moet worden voldaan om die kansen te benutten; en
- de lessen die kunnen worden getrokken uit ervaringen in het buitenland.

Speciale aandacht gaat hierbij uit naar publieke organisaties en aanbieders van vitale diensten.

Het onderzoek richt zich op nieuwe technologische ontwikkelingen.[1] Technologie krijgt echter pas betekenis door de manier waarop de mogelijkheden ervan worden benut in de maatschappelijke praktijk. Dat betekent ook dat technologische ontwikkelingen mede vorm krijgen door allerlei niet-technologisch aspecten, zoals cybervaardigheden van gebruikers, organisatorische processen en wet- en regelgeving. Het onderzoek naar het benutten van de kansen die nieuwe technologische ontwikkelingen bieden, besluit daarom met deze bredere voorwaarden.

Relevante technologische ontwikkelingen
Het onderzoek richt zich op de technologische ontwikkelingen die de komende jaren naar verwachting in de praktijk relevant zullen worden voor de cyberweerbaarheid van Nederland. Het richt zich niet op technologische ontwikkelingen die alleen in academische zin ‘nieuw’ zijn.

1 Zie bijlage 1 voor een toelichting op de technologische begrippen die in dit rapport worden genoemd. In deze samenvatting zijn deze met een * gemarkeerd.

Ter verduidelijking hiervan twee voorbeelden. De kwantumcomputer* zal de komende jaren onvoldoende ver ontwikkeld zijn om in de praktijk te kunnen worden gebruikt. Maar de verwachte komst ervan is voor deze studie relevant, omdat reeds de komende jaren maatregelen moeten worden genomen om IT-systemen te beschermen tegen het risico van een aanval met een kwantumcomputer. Omgekeerd is het *Internet of Things* (IoT)* op zich geen nieuwe technologische ontwikkeling, maar dwingt de grote vlucht die het de komende jaren zal nemen, om opnieuw te doordenken hoe Nederland met de kwetsbaarheden ervan moet omgaan. De verdere ontwikkeling van IoT wordt daarmee relevant voor dit onderzoek.

Digitalisering maakt samenleving kwetsbaar
Dit onderzoek gaat tevens in op de kwetsbaarheden die gepaard gaan met de digitalisering van de samenleving. Maatregelen die de cyberweerbaarheid moeten versterken, kunnen namelijk niet los worden gezien van deze kwetsbaarheden en daarmee samenhangende cyberdreigingen.

Door de voortschrijdende digitalisering van de samenleving raken de online en de offline wereld steeds verder met elkaar verweven. Daardoor worden steeds meer data digitaal verwerkt, bevatten steeds meer apparaten digitale technologie en worden steeds meer diensten digitaal geleverd. De verdere uitrol van IoT jaagt deze ontwikkeling verder aan. Dat is problematisch, omdat de cyberweerbaarheid veelal niet op orde is. Dat maakt IT-systemen en -applicaties kwetsbaar voor uitval, storingen en aanvallen.

Groeiende afhankelijkheid van externe partijen
Een belangrijke ontwikkeling die ook gevolgen heeft voor de cyberweerbaarheid, is de groeiende afhankelijkheid van eindgebruikers voor het goed functioneren van digitale producten en diensten van buitenlandse technologiebedrijven. Zo worden steeds meer digitale diensten door verstrekkers van cloudtechnologie* geleverd. Dit creëert nieuwe risico's: uitval van functionaliteit bij verstoring, en verlies van controle en zeggenschap over data en dataverwerking.

Ook voor de (verdere) ontwikkeling en implementatie van nieuwe technologieën als *machine learning*, kwantumcomputing*, satelliet- en 5G-netwerken* geldt dat grote buitenlandse bedrijven vooroplopen. Nederland en de EU dreigen daardoor nog sterker afhankelijk te worden van buitenlandse partijen.

Verhoging cyberweerbaarheid met nieuwe technologie
Nieuwe technologieën als *machine learning*, post-kwantumcryptografie*, LiFi*, kwantumcommunicatie*, 5G-netwerken en gedistribueerde systemen* bieden kansen om de cyberweerbaarheid te verhogen. Zo maakt *machine learning* het

naar verwachting mogelijk om automatisch kwetsbaarheden in software op te sporen en te herstellen. En post-kwantumcryptografie moet dataversleuteling mogelijk maken die bestand is tegen aanvallen waarbij gebruik wordt gemaakt van de rekenkracht van een kwantumcomputer. Deze technologieën zijn nog wel in ontwikkeling en worden nog maar beperkt toegepast.

Gebruik van automatische detectie en herstel van kwetsbaarheden of van post-kwantumcryptografie is overigens niet alleen een kans, maar ook een noodzaak. Zo zal, voordat de kwantumcomputer het mogelijk maakt om bestaande vormen van encryptie* te breken, een grootschalige migratie naar post-kwantumcryptografie moeten hebben plaatsgevonden, om zeker te zijn van de veiligheid van data.

Nieuwe technologieën scheppen nieuwe kwetsbaarheden
Nieuwe technologische ontwikkelingen scheppen ook nieuwe kwetsbaarheden. Zo vergemakkelijkt *machine learning* het uitvoeren van cyberaanvallen, doordat bestaande kwetsbaarheden automatisch en op grote schaal kunnen worden ontdekt en uitgebuit. Nieuwe technologieën kunnen ook een bron zijn van nieuwe kwetsbaarheden. Zo kan *machine learning* worden ingezet voor de manipulatie van beeldmateriaal (*deep fakes**). Bovendien hebben nieuwe technologieën eigen kwetsbaarheden. Zo is *machine learning* gevoelig voor datavervuiling; kwaadwillende partijen kunnen die kwetsbaarheid misbruiken door een *machine learning*-systeem met opzet te voeden met verkeerde data.

Verhoging cyberweerbaarheid met bestaande technologie
Het heeft ook maar beperkt zin om in te zetten op nieuwe technologieën als niet tegelijkertijd op grotere schaal gebruik wordt gemaakt van reeds voorhanden zijnde technologieën om de cyberweerbaarheid te verhogen. Zo valt er nog veel winst te halen met het nemen van basisveiligheidsmaatregelen (sterke wachtwoorden, 2-factor-authenticatie*), encryptie, het gebruik van Privacy Enhancing Technologies (PETs)*, opendatastandaarden*, *open source software** en veiligere communicatieprotocollen.

Voorwaarden voor benutten technologische kansen
Voor het benutten van de kansen die bestaande en nieuwe technologieën bieden om de cyberweerbaarheid te verhogen, moet aan een aantal voorwaarden zijn voldaan. Allereerst veronderstelt de inzet van maatregelen om de cyberweerbaarheid te verhogen een adequate risicoanalyse, op bestuursniveau, van data en processen die voor een organisatie kritiek zijn: welke ‘kroonjuwelen’ behoeven maximale beveiliging; welke risico’s zijn acceptabel?

Daarnaast kan de overheid als grote afnemer van digitale producten en diensten een belangrijke voorbeeldfunctie vervullen, bijvoorbeeld door breed PETs* toe te

passen. Bovendien kan de overheid met behulp van wetgeving, certificering en standaardisatie leveranciers stimuleren om beter beveiligde digitale producten en diensten op de markt te brengen. De Nederlandse overheid – of: de EU – zou zich nadrukkelijk moeten mengen in de besluitvorming over internationale standaarden, die van groot belang zijn voor internationale maatregelen op het gebied van cyberweerbaarheid.

Versterken van digitale autonomie

Voor het tegengaan van de risico's die samenhangen met de groeiende afhankelijkheid van buitenlandse technologiebedrijven, zijn er diverse opties.

1. Door standaard gebruik te maken van maatregelen als sterke encryptie, opendatastandaarden of gedistribueerde systemen, kunnen risico's worden tegengegaan, zoals ongewenste inzage in data, *vendor lock-in** en Single Points of Failure.*
2. Een tweede optie is het stellen van strengere eisen in de inkoopvoorwaarden aan leveranciers van digitale producten en diensten. Bijvoorbeeld door van clouddienstverleners te verlangen dat opgeslagen data standaard worden versleuteld, om ongewenste inzage te voorkomen. De Rijksoverheid en de aanbieders van vitale diensten zouden hierin een leidende rol kunnen – of: moeten – spelen.
3. Een derde optie om te ontsnappen aan een te grote afhankelijkheid van buitenlandse partijen, is door meer eigen IT-bedrijvigheid in Nederland en Europa te creëren.

Stimuleren innovatieklimaat

De laatste optie veronderstelt een daadkrachtiger kennis- en innovatiebeleid, met meer focus in de Nederlandse Cyber Security Research Agenda (NCSRA) van de Rijksoverheid. Ook is een gunstiger innovatieklimaat nodig. De overheid kan bijvoorbeeld aanbestedingsprocedures aantrekkelijker maken voor innovatieve startups. De overheid en aanbieders van vitale diensten zouden zich daarnaast sterker kunnen opstellen als *launching customer*. De vooraanstaande, Nederlandse kennispositie op het gebied van post-kwantumcryptografie biedt ook kansen om eigen IT-bedrijvigheid te ontwikkelen. Zo kunnen producten en diensten worden ontwikkeld om de migratie naar kwantumbestendige versleuteling te ondersteunen.

Een extra reden om in ieder geval een minimum aan eigen IT-bedrijvigheid te ontwikkelen, is de behoefte aan maximale beveiliging van 'kroonjuwelen' als staats- en bedrijfsgeheimen – bijvoorbeeld door gebruik te maken van sterke vormen van post-kwantumcryptografie. De Rijksoverheid en aanbieders van vitale diensten moeten daarvoor producten en diensten kunnen afnemen van vertrouwde marktpartijen, die belangrijke waarden als privacy en autonomie onderschrijven.

Benutten kansen post-kwantumcryptografie en *machine learning*
De overheid kan op diverse manieren de toepassing van nieuwe technologieën als *machine learning* en post-kwantumcryptografie ondersteunen. Daarvoor is het nodig te blijven investeren in de kennisontwikkeling op deze gebieden. Daarnaast moet de samenwerking worden gefaciliteerd tussen kennisinstellingen en organisaties die werken aan de ontwikkeling van innovatieve oplossingen voor vraagstukken op het gebied van cyberweerbaarheid. Organisaties die niet over eigen onderzoekscapaciteit beschikken, en aangewezen zijn op het aanbod van marktpartijen, moeten desgewenst inhoudelijk worden ondersteund bij de beoordeling van een passend marktaanbod.

Succesvolle inzet van nieuwe technologie vereist beschikbare expertise
Het kunnen benutten van de kansen van bestaande en nieuwe technologieën voor verhoging van cyberweerbaarheid vereist de benodigde capaciteit en expertise. Vanwege het chronische tekort aan experts op dit gebied, is het nodig meer te investeren in IT-opleidingen.

Inhoud

Inleiding

De digitale samenleving is een kwetsbare samenleving. Op allerlei manieren kunnen digitale producten en toepassingen worden gehackt, verstoord of gemanipuleerd. Data kunnen worden gestolen of vervalst, computers kunnen heimelijk worden aangestuurd, desinformatie kan worden verspreid en uitval van IT-systemen kan maatschappelijke ontwrichting veroorzaken. Van telefoons tot auto's en van financiële transacties tot patiëntendossiers: al deze toepassingen digitaliseren en dit gaat gepaard met digitale kwetsbaarheden.

Nieuwe digitale ontwikkelingen, zoals *machine learning*, het steeds massalere gebruik van clouddiensten en de komst van de kwantumcomputer, verdiepen deze kwetsbaarheden. Zo kan door het gebruik van *deep fakes* desinformatie een ontwrichtende uitwerking krijgen op het democratische proces van publieke nieuwsvoorziening en meningsvorming. En de steeds belangrijkere positie van cloudaanbieders kan leiden tot een groeiende afhankelijkheid van gebruikers van die aanbieders en daarmee gepaard gaande veiligheidsrisico's.

Tegelijkertijd bieden nieuwe ontwikkelingen ook kansen. Met *machine learning* kunnen sneller kwetsbaarheden worden gedetecteerd, en gemakkelijker hersteld. Door clouddiensten komt de beveiliging van digitale systemen in handen van professionals. En gedistribueerde systemen kunnen het risico verminderen van grootschalige uitval.

Deze studie onderzoekt de betekenis van technologische ontwikkelingen voor de nabije toekomst, en hoe ze kunnen worden benut om de cyberweerbaarheid van de Nederlandse samenleving te verhogen.

1.1 Doel en vraagstelling

Dit rapport vloeit voort uit een verzoek van de Cyber Security Raad (CSR) aan het Rathenau Instituut om onderzoek te doen naar de wijze waarop nieuwe technologieën kunnen bijdragen aan het verhogen van de cyberweerbaarheid in Nederland. De CSR is een nationaal en onafhankelijk adviesorgaan van het kabinet en bestaat uit vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich in om de cybersecurity in Nederland te verhogen. Het rapport moet bouwstenen aanleveren op grond waarvan de Cyber Security Raad over dit onderwerp advies kan uitbrengen aan het kabinet.

De centrale vraag van het onderzoek luidt: hoe kunnen nieuwe technologieën bijdragen aan het verhogen van de cyberweerbaarheid van Nederland, met speciale aandacht voor de publieke en private organisaties die deel uitmaken van de vitale infrastructuur?

Voor de beantwoording van deze vraag zijn we op de volgende deelvragen ingegaan:

- Welke technologische ontwikkelingen staan ons te wachten op de middellange termijn (2-8 jaar)?
- Welke gevolgen hebben de technologische ontwikkelingen voor bestaande cyberkwetsbaarheden en -dreigingen, en de huidige cyberweerbaarheid?
- Welke kansen bieden nieuwe technologische mogelijkheden om de cyberweerbaarheid te verhogen?
- Aan welke voorwaarden moet worden voldaan om de kansen te benutten?
- In hoeverre anticiperen de publieke en private organisaties die deel uitmaken van de vitale infrastructuur op nieuwe technologische mogelijkheden, en maken ze daarvan gebruik?
- Welke lessen kunnen worden getrokken uit ervaringen in het buitenland? Welke relevante ontwikkelingen zijn er binnen de EU?

1.2 Aanpak

Deze studie is tot stand gekomen op basis van literatuuronderzoek, interviews en drie workshops. Tijdens de workshops zijn de belangrijkste bevindingen van het literatuuronderzoek en de interviews besproken. De workshops vonden plaats op 31 januari, 21 februari en 17 juni 2019. Voorafgaand aan de workshops ontvingen de deelnemers een gespreksnotitie met een overzicht van de resultaten van het literatuuronderzoek, de interviews en de workshops die eerder hadden plaatsgevonden. Naar aanleiding van de workshops is op onderdelen aanvullend literatuuronderzoek verricht en zijn enkele aanvullende interviews gehouden.

Aan de interviews en de workshops is deelgenomen door deskundigen, stakeholders en beleidsmakers. De deelnemers aan de workshops bestonden deels uit dezelfde personen die ook aan de interviews hebben deelgenomen. In dit rapport verwijzen we naar hen met de term ‘de door ons geraadpleegde deskundigen’. Hierbij wordt geen onderscheid gemaakt tussen de deelnemers aan de interviews en de deelnemers aan de workshops. Deze zijn geselecteerd op basis van hun expertise van en betrokkenheid bij de diverse deelvragen van het onderzoek. De namen van de deelnemers aan de interviews en workshops staan vermeld in Bijlage 2 en 3.

Dit rapport beschrijft de opbrengst van het literatuuronderzoek, de interviews en de workshops en verbindt daaraan conclusies. De voortgang van het onderzoek is diverse keren besproken met de secretaris van de Cyber Security Raad en met leden van de Subcommissie Nieuwe Technologieën van deze Raad.

1.3 Procesobservaties

De vraagstelling van het onderzoek dwingt om vooruit te kijken naar de kansen die nieuwe technologieën op het gebied van cyberweerbaarheid de komende jaren bieden. Tijdens het onderzoek is het ons opgevallen dat deze vraag niet vanzelf sprak. Vooral tijdens de interviews bleek dat het de nodige moeite kostte om de vraagstelling van het onderzoek goed voor het voetlicht te brengen. In eerste instantie reageerden veel van de geïnterviewde deskundigen met reacties als: het gaat bij cyberweerbaarheid meer om organisatorische dan om technologische kwesties; zonder goed besef van de cyberdreigingen heeft het weinig zin om naar kansen te kijken, en zolang het nemen van basisveiligheidsmaatregelen op grote schaal achterwege blijft, heeft het weinig zin om naar nieuwe technologische mogelijkheden te kijken.

Desalniettemin waren de geraadpleegde deskundigen in tweede instantie wel degelijk bereid om nieuwe mogelijkheden te noemen waarvan de cyberweerbaarheid in de nabije toekomst kan profiteren. Aanvankelijk resulteerde dat in een breed scala aan mogelijkheden, zonder duidelijke prioritering of rangorde. Hierin speelde mee dat er verschillende opvattingen bestonden over wat onder ‘nieuwe technologie’ moet worden verstaan. Waar de één ‘nieuw’ in meer academische zin opvatte, met een nadruk op grensverleggend onderzoek, kreeg bij de ander de term een meer op de praktijk gerichte betekenis, waarbij de aandacht primair uitgaat naar nieuwe toepassingsmogelijkheden.

De drie workshops hebben een belangrijke rol gespeeld in het duiden en structureren van de veelsoortige opbrengst van het literatuuronderzoek en de interviews. Dit heeft mede geleid tot de hieronder staande, inhoudelijke afbakening van de studie.

1.4 Afbakening

Voor de afbakening van het onderzoek is een helder begrip nodig van wat we in deze studie verstaan onder de term nieuwe technologie. Dit begrip moet het ook mogelijk maken onderscheid te maken tussen voor de vraagstelling van het

onderzoek meer en minder relevante, ‘nieuwe’ technologische ontwikkelingen. Deze paragraaf beschrijft tot welke afbakening van het onderzoek we zijn gekomen.

Nieuwe technologie
De vraagstelling van dit onderzoek richt zich op de gevolgen van nieuwe technologische ontwikkelingen voor de bestaande praktijk die gericht is op het cyberweerbaar maken van de Nederlandse samenleving, en hoe die praktijk van die ontwikkelingen kan profiteren. De betekenis van de technologische ontwikkelingen wordt daarmee gerelateerd aan de relevantie die ze hebben voor de bestaande, en zich verder ontwikkelende praktijk. Deze studie richt zich dus niet op technologische ontwikkelingen die alleen academisch gezien grensverleggend zijn.

Rol van technologie
Hierbij moet worden bedacht dat technologie nooit op zichzelf staat. Ze krijgt pas betekenis door de manier waarop de technologische mogelijkheden invulling krijgen en worden gebruikt binnen een maatschappelijke praktijk – en dit laatste betekent in dit geval: het geheel aan inspanningen die burgers, bedrijven en overheden plegen om de Nederlandse samenleving cyberweerbaar te maken. Dat betekent ook dat technologische ontwikkelingen mede vorm krijgen door allerlei niet-technologische aspecten, zoals cybervaardigheden van gebruikers, organisatorische processen binnen bedrijven en overheden, en wet- en regelgeving.[2] Niet voor niets gaat deze studie ook in op de voorwaarden waaraan moet zijn voldaan, willen de kansen kunnen worden benut die nieuwe technologische ontwikkelingen bieden.

Relevante technologische ontwikkelingen
Door de betekenis van nieuwe technologie te relateren aan de relevantie ervan voor de praktijk, wordt het ook mogelijk af te bakenen welke technologische ontwikkelingen wel en niet in dit onderzoek worden meegenomen.

Dit kan worden verduidelijkt aan de hand van het voorbeeld van de kwantumcomputer. Naar verwachting zal de kwantumcomputer de komende acht jaar onvoldoende ver zijn ontwikkeld om succesvol in de praktijk te kunnen worden gebruikt. Maar de verwachte komst van de kwantumcomputer op de langere duur vergt wel dat reeds de komende jaren maatregelen worden genomen om IT-systemen te beschermen tegen het risico van een hack waarbij gebruik wordt gemaakt van de rekenkracht van een kwantumcomputer. Daarmee worden de mogelijke gevolgen van de – nu nog futuristische – inzet van de kwantumcomputer relevant voor de cyberweerbaarheid voor de komende jaren.

---

2 Zie ook het Cybersecurity Capacity Maturity Model (CMM) van de University of Oxford, Global Cyber Security Capacity Centre - University of Oxford. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition. Oxford.*

Omgekeerd is het *Internet of Things* (IoT) op zich geen nieuwe technologische ontwikkeling (Gabbai, 2015). Maar vanwege de grote vlucht die het de komende jaren naar verwachting zal nemen, dwingt het ons om opnieuw te doordenken hoe met de kwetsbaarheden ervan moet worden omgegaan. De verdere ontwikkeling van IoT wordt daarmee relevant voor dit onderzoek.

Kwantumcomputer als enige *nieuwe* technologie
Zoals het voorbeeld van IoT al laat zien, liggen een aantal technologische ontwikkelingen die in deze studie worden besproken in het verlengde van eerdere ontwikkelingen. Dat geldt bijvoorbeeld ook voor het gebruik van cloudtechnologie, dat zich niet langer vooral richt op dataopslag, maar meer en meer ook op het leveren van diensten. De kwantumcomputer is in dit onderzoek de grote uitzondering: het is de enige technologische ontwikkeling die in meerdere opzichten het predicaat ‘nieuw’ verdient. Ze is niet alleen academisch grensverleggend, maar zal naar verwachting ook de bestaande praktijk vergaand transformeren.

Verdere selectie technologische ontwikkelingen
Deze studie biedt geen totaaloverzicht van allerlei nieuwe technologische ontwikkelingen, maar beperkt zich tot een selectie van de meest relevante ontwikkelingen voor de vraag hoe de cyberweerbaarheid kan worden verhoogd. Om enig inzicht te geven in de afwegingen die aan deze selectie ten grondslag liggen, volgen hier twee voorbeelden.

Ten eerste gaan we niet in op ontwikkelingen op het gebied van blockchain. We zien blockchain als een afgeleide toepassing, die gebruik maakt van de mogelijkheden die encryptie en gedistribueerde systemen bieden. Deze twee, meer basale, technologieën bespreken we wel.

Ten tweede gaan we niet in op ontwikkelingen op het gebied van gebruikersomgevingen en andere interactietechnologie, zoals wearables, digitale spraakassistenten en Virtual Reality. Hiervoor geldt een vergelijkbaar verhaal. Het rapport bespreekt de technologieën die van belang zijn voor de weerbaarheid van de systemen die aan deze interactietechnologie ten grondslag liggen. In het geval van digitale spraakassistenten als Siri, Alexa en Google Assistent zijn dit bijvoorbeeld ontwikkelingen op het gebied van *machine learning* en Privacy Enhancing Technologies.

Paragraaf 1.5 biedt een overzicht van de technologieën die in dit rapport worden besproken.

Cyberweerbaarheid
We gebruiken in dit rapport de term cyberweerbaarheid (*cyber resilience*) in plaats van het begrip cybersecurity. Cyberweerbaarheid is een relatief nieuwe term. Ze kent de nodige gelijkenis met de term cybersecurity, en de begrippen worden ook regelmatig door elkaar gebruikt. Met de term cybersecurity wordt doorgaans gedoeld op het voorkomen van schade door verstoring, uitval of misbruik van IT. De schade kan moedwillig gebeuren (bijvoorbeeld bij een cyberaanval), onbedoeld (bijvoorbeeld door een software update die verkeerd uitpakt), door een menselijke fout of een combinatie hiervan. De term cybersecurity roept associaties op met de metafoor van het fort, dat ondoordringbaar moet zijn voor aanvallen en verstoring van buitenaf.

Met de term cyberweerbaarheid gaat het niet alleen om het voorkomen van schade, maar ook om het vermogen te reageren op een aanval en eventuele schade te herstellen (Ministerie van Veiligheid en Justitie, 2013). Het is een dynamischer begrip, dat tot uitdrukking brengt dat er niet gestreefd wordt naar absolute veiligheid (ENISA, 2017). Honderd procent veiligheid bestaat immers niet (Rathenau Instituut, 2017). Voorop staat dat continuïteit in dienstverlening kan worden geborgd op het moment dat een aanval plaatsvindt of schade optreedt (Björck et al., 2015; IT Governance UK, 2019). Cyberweerbaarheid vertoont gelijkenis met het beeld van het menselijk immuunsysteem (Wlodarczak, 2017). Net als het menselijk lichaam zijn digitale systemen niet hermetisch afgesloten. Het immuunsysteem is ook niet in staat alle aanvallen buiten de deur te houden. Het immuunsysteem rekent met indringers af, of probeert ze voldoende onder de duim te houden.

Het gebruik van de term cyberweerbaarheid weerspiegelt een groeiend bewustzijn dat het internet een onveilige omgeving is, en een hermetisch afgesloten fort onmogelijk te bouwen is. Het wordt daarom belangrijker om zo goed mogelijk aanvallen en verstoringen te voorkomen, en wanneer die plaatsvinden, in staat te zijn ze op te sporen, in te dammen en ervan te herstellen. Dat laat onverlet dat de basis – ‘het fort’ – zo stevig mogelijk moet zijn.

Weerbaarheid en kwetsbaarheid
Voor het streven de cyberweerbaarheid te verhogen, is het van belang voldoende zicht te hebben op de kwetsbaarheden van IT-gerelateerde producten, diensten en systemen. Maatregelen die de cyberweerbaarheid moeten versterken, kunnen niet los worden gezien van deze kwetsbaarheden en daarmee samenhangende cyberdreigingen. We besteden in deze studie dan ook de nodige aandacht aan de kwetsbaarheden die samenhangen met bestaande en nieuwe technologische ontwikkelingen in het digitale domein.

De cyberdreigingen betreffen zowel aanvallen van kwaadwillende partijen, zoals cybercriminelen, als storingen en uitvalsincidenten. In deze studie worden de aard en omvang van bestaande cyberdreigingen, die in diverse rapporten reeds in kaart zijn gebracht, als bekend verondersteld (Rathenau Instituut, 2017; ITU, 2017; Europol, 2018; McAfee, 2018; NCTV, 2019a).

1.5 Overzicht besproken technologieën

Op basis van de resultaten van het literatuuronderzoek, de interviews en de workshops, en gebruikmakend van de hierboven beschreven afbakening van het onderzoek, zijn we tot de volgende selectie gekomen van te bespreken technologieën. Hierbij maken we een onderscheid tussen (relatief) nieuwe technologieën – die nog niet breed worden toegepast of nog volop in ontwikkeling zijn – en reeds langer bestaande en in gebruik zijnde technologieën. Zie Tabel 1 voor het overzicht.[3]

Tabel 1 Overzicht besproken technologieën

Nieuwe technologie	Kans verhoging cyberweerbaarheid
Machine learning	• Automatische monitoring van complexe IT-systemen • Automatische detectie van kwetsbaarheden, storing, uitval en aanvallen • Automatische respons op incidenten • Automatische detectie van *deep fake* video's
Post-kwantumcryptografie	• Kwantumcomputerbestendige versleuteling van data
Kwantumcommunicatie	• Veiligere communicatie d.m.v. detectie van afluisteren
5G-netwerken	• Betrouwbaarder en veiliger dataverkeer • Toekomstbestendige authenticatie
LiFi	• Lokaal veiligere communicatie d.m.v. lichtsignalen
Gedistribueerde systemen	• Decentrale architectuur IT-systemen vermindert risico van grootschalige uitval

3 Zie bijlage 1 voor een nadere toelichting van deze technologieën.

Bestaande technologie	Kans verhoging cyberweerbaarheid
Basisveiligheidsmaatregelen	• Verhoging weerbaarheid tegen (automatische) aanvallen
Cloudtechnologie	• Verhoging weerbaarheid d.m.v. professionele clouddiensten
Privacy Enhancing Technologies	• Beperking verspreiding van (persoons)gegevens • Beperking schade bij datalek en diefstal
Encryptie	• Versleuteling van data
Secure multi-party computation	• Uitwisseling data zonder volledige openheid van zaken
Digitale ondertekening	• Bestrijding desinformatie • Veiligere aanvoerketens
SecDevOps	• Inbouwen cyberweerbaarheid in ontwerpproces van digitale producten en diensten
Veiligere communicatie-protocollen	• Verhoging basale weerbaarheid van het internet
Open standaarden en *open source software*	• Vermindering risico van afhankelijkheid door *vendor lock-in*

1.6 Leeswijzer

De volgende hoofdstukken beschrijven de opbrengst van het onderzoek. De indeling van de hoofdstukken volgt grofweg de volgorde van de hierboven genoemde deelvragen van het onderzoek. Hoofdstuk 2 beschrijft de kwetsbaarheden die gepaard gaan met de voortschrijdende digitalisering van de samenleving, en de nieuwe digitale kwetsbaarheden die samenhangen met nieuwe technologische ontwikkelingen. Hoofdstuk 3 brengt in kaart welke kansen nieuwe technologieën bieden om de cyberweerbaarheid te verhogen. Hoofdstuk 4 doet hetzelfde voor de kansen die bestaande, maar onderbenutte technologieën bieden. Hoofdstuk 5 beschrijft de voorwaarden waaraan moet zijn voldaan, willen publieke organisaties en aanbieders van vitale diensten gebruik kunnen maken van deze kansen om de cyberweerbaarheid te verhogen. Daarbij wordt tevens ingegaan op relevante ervaringen in het buitenland. Hoofdstuk 6 presenteert de belangrijkste conclusies van het onderzoek.

2 Digitalisering maakt de samenleving kwetsbaar

Zoals in het inleidende hoofdstuk is gesteld, kunnen maatregelen die de cyberweerbaarheid moeten versterken niet worden losgezien van de kwetsbaarheden van IT-gerelateerde producten, diensten en systemen. Het streven naar verhoging van de cyberweerbaarheid vereist dan ook inzicht in die kwetsbaarheden.

Dit hoofdstuk beschrijft de kwetsbaarheden die gepaard gaan met de voortschrijdende digitalisering van de samenleving. Daarnaast laat het zien hoe nieuwe technologische ontwikkelingen, zoals *machine learning* of het groeiende gebruik van clouddiensten, bestaande kwetsbaarheden kunnen vergroten, of tot nieuwe kwetsbaarheden kunnen leiden. Nieuwe technologieën kunnen bovendien zelf een bron zijn van nieuwe kwetsbaarheden. Zo is het gebruik van *machine learning* vatbaar voor het risico van datamanipulatie.

2.1 Groeiende digitale verbondenheid maakt kwetsbaar

Sinds enkele decennia is sprake van een voortschrijdende digitalisering van de samenleving, met een steeds sterkere verwevenheid van de online met de offline wereld. Steeds meer data worden digitaal opgeslagen, steeds meer apparaten bevatten digitale technologie en steeds meer diensten worden digitaal geleverd. Ontwikkelingen als de verdere uitrol van het Internet of Things jagen deze ontwikkeling verder aan. Vanwege het steeds omvangrijkere karakter hiervan wordt ook wel gesproken over ‘het internet van alles’.

De voortschrijdende digitalisering betekent ook dat er steeds meer digitale doelwitten zijn die kwaadwillende partijen kunnen aanvallen, en er steeds meer digitale producten en diensten worden gebruikt die vatbaar zijn voor uitval en (ver)storing. Dit creëert uiteenlopende veiligheidsrisico’s. In toenemende mate kunnen die ook fysieke gevolgen krijgen, zoals bij de digitale aansturing van sluizen of de opkomst van *smart homes* of zelfrijdende auto’s. Zo kan het digitaal manipuleren van sluizen of van remsystemen in zelfrijdende auto’s tot grote fysieke schade leiden.

Ondanks de groeiende aandacht voor de risico's die gepaard gaan met de digitalisering van de samenleving, is het met de cyberweerbaarheid vaak droevig gesteld. Zo worden basisveiligheidsmaatregelen vaak niet of onvoldoende genomen.

Vanwege de toenemende verwevenheid van allerlei (digitale) processen ontstaan daarnaast steeds verdergaande ketenafhankelijkheid tussen organisaties. Kwetsbaarheden bij de ene organisatie kunnen daardoor gevolgen krijgen voor de cyberweerbaarheid van de andere organisatie.

In deze paragraaf beschrijven we de hier genoemde ontwikkelingen in meer detail. We gaan hierbij tevens in op ontwikkelingen op het gebied van cybercrime.

2.1.1 Het internet van alles

Sinds de jaren negentig van de vorige eeuw is het internet enorm gegroeid. Steeds meer apparaten worden op het internet aangesloten en vormen samen een Internet of Things. In 2018 waren er wereldwijd 17 miljard apparaten met het internet verbonden: 10 miljard smartphones, tablets, laptops en pc's en 7 miljard andere apparaten als slimme thermostaten, digitale implantaten als een pacemaker of een insulinepomp, en auto's. Het aantal IoT-apparaten zal in de komende vijf jaar waarschijnlijk minstens verdubbelen (Lueth, 2018).

5G-netwerken maken de verdere uitrol van het Internet of Things mogelijk. De term 5G staat voor de vijfde generatie draadloze of mobiele systemen. Deze kunnen gegevens in grotere hoeveelheden en met minder vertraging transporteren. Dit kan de functionaliteit van veel digitale toepassingen verbeteren, bijvoorbeeld door zelfrijdende auto's sneller van informatie te voorzien.

Het is hierbij belangrijk op te merken dat digitale toepassingen en apparaten ook met elkaar kunnen communiceren. Zo kan een zelfrijdende auto alleen zijn route bepalen als hij voortdurend gevoed wordt met de juiste informatie. Als een satelliet of een sensor langs de weg verkeerde informatie verstrekt kan dat ongelukken veroorzaken. De onderlinge verbondenheid van digitale apparaten kan dan ook de risico's op manipulatie, verstoring en uitval vergroten.

In de energiesector is een vergelijkbaar risico waarneembaar. De toename van decentrale opwekking en de groeiende vraag naar energie-intensieve oplaadpunten voor elektrische voertuigen maken digitaal beheer van het energienetwerk onontkoombaar. Dat brengt nieuwe risico's met zich mee, zoals storingen en uitval (Raad voor de leefomgeving en infrastructuur, 2018).

Kortom: er is een ‘internet van alles’ ontstaan, waardoor talloze producten en diensten digitaal zijn verbonden en vatbaar zijn voor aanvallen, storing en uitval.

2.1.2 De groei van digitaal beschikbare data

De groeiende digitalisering van de samenleving gaat gepaard met grote dataverzamelingen. Rijkswaterstaat monitort het waterpeil met een uitgebreid netwerk met sensoren; zoekmachines op internet houden het surfgedrag van gebruikers bij; en nieuwe auto’s slaan lokaal of bij de fabrikant veel meer gegevens op dan auto’s die 10 jaar oud zijn (Automotive Insiders, 2018). Bedrijven, overheden en andere organisaties vergaren steeds meer gegevens van klanten en cliënten: meer data leidt tot meer inzicht en tot beter op de behoefte van de persoon afgestemde producten en diensten – is de gedachte. De commerciële waarde van al die informatie voor bijvoorbeeld adverteerders maakt het mogelijk om digitale producten en diensten kosteloos aan te bieden aan gebruikers (Zuboff, 2019).

Het verzamelen van al deze data is niet zonder risico’s. De afgelopen jaren zijn met regelmaat grote datasets op straat komen te liggen. Zo zijn persoonsgegevens gelekt van 500 miljoen Marriott-hotelgasten (Ortiz, 2018), 150 miljoen MyFitnessPal-app gebruikers (Flinkle & Balu, 2018) en 87 miljoen Facebookgebruikers (Lapowsky, 2018). De lekken onderstrepen de kwetsbaarheid van centrale databases en het risico van almaar groeiende dataverzamelingen. Cybercriminelen en andere kwaadwillende partijen kunnen daarvan gebruikmaken, bijvoorbeeld door met gelekte data een doelwit te chanteren of berichtgeving te manipuleren. Hoe meer data mensen online zetten, hoe groter de kans is dat gegevens ongewenst worden ingezien of misbruikt.

2.1.3 Lage basisveiligheid

De groeiende verbondenheid met internet is vanuit het perspectief van cyberweerbaarheid problematisch, omdat ook relatief eenvoudige basisveiligheidsmaatregelen vaak niet worden genomen. Digitale apparaten en diensten worden vaak door leveranciers slecht of onvoldoende beveiligd, en niet van updates voorzien (Bulletproof, 2019). Het ontbreekt leveranciers veelal aan economische prikkels om te investeren in cyberweerbaarheid. De prijsconcurrentie op producten is groot, en de gebruiker vraagt niet naar veiligere producten (Rathenau Instituut, 2017).

Daarnaast nemen gebruikers vaak onvoldoende maatregelen om hun producten en diensten te beveiligen. Ze maken bijvoorbeeld gebruik van zwakke wachtwoorden, maken geen back-ups van belangrijke bestanden en stellen software-updates uit (Van der Grient & Konings, 2018).

Dit creëert grote veiligheidsrisico's, aangezien het manipuleren of verstoren van digitale apparaten ernstige gevolgen kan hebben. Met het internet verbonden apparaten kunnen ook worden gebruikt voor een cyberaanval. Ze kunnen worden gehackt en worden ingezet als onderdeel van een botnet, dat wordt gebruikt voor een massale DDoS-aanval (Hilton, 2016).

2.1.4 Ketenafhankelijkheid

Steeds meer IT-systemen en -toepassingen zijn met elkaar verbonden. Organisaties nemen vaak netwerkgebaseerde producten of diensten af van andere partijen. Dat kan gaan om zaken als software, hardware, dataopslag of clouddiensten. Geen enkele organisatie is meer in staat om alle taken volledig zelf uit te voeren. De kwetsbaarheid die deze afhankelijkheid van andere partijen met zich meebrengt, wordt vaak onderschat. De zwakste schakel in de keten kan namelijk verstoringen van functies verderop in de keten veroorzaken (Rathenau Instituut, 2017). Om de kwetsbaarheid in aanvoerketens te illustreren wordt nogal eens verwezen naar de anekdote van de hackers die de systemen van een casino binnen wisten te dringen via het aansturingsysteem van het aquarium (Schiffer, 2017).

Door deze ketenafhankelijkheid worden de diverse maatschappelijke en economische sectoren ook steeds meer met elkaar verbonden. De cyberweerbaarheid van bijvoorbeeld de energie- of transportsector kan dan ook steeds minder los worden gezien van die van andere partijen in de keten. Het vaak gemaakte onderscheid tussen 'vitale sectoren' en overige sectoren, wordt hierdoor steeds moeilijker houdbaar. In plaats hiervan hanteert de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) inmiddels de termen 'vitale infrastructuur', 'vitale processen' en 'vitale aanbieders' (NCTV, 2018).

2.1.5 Ontwikkelingen op het gebied van cybercrime

De voortschrijdende digitalisering van de samenleving schept allerlei mogelijkheden voor criminaliteit, terwijl de bestrijding ervan daar geen gelijke tred mee houdt. Cybercriminaliteit is niet alleen vaak lonend, cybercriminelen hebben tevens vaak weinig te vrezen. Doordat aanvallen vaak moeilijk te herleiden zijn tot een

specifieke persoon of organisatie, is opsporing en vervolging lastig. Ook als een criminele activiteit wordt onderbroken, kunnen de daders het dikwijls elders of op een andere manier opnieuw proberen. Zolang de pakkans laag blijft en het risico van vervolging ook, zal de dreiging die uitgaat van cybercriminaliteit niet afnemen.

Het plegen van cybercriminaliteit wordt ook steeds eenvoudiger. Cybercrime-as-a-service is in opkomst: cyberaanvallen en door criminelen overgenomen computers kunnen steeds gemakkelijker op ondergrondse marktplaatsen worden gekocht, waardoor de expertise om een aanval zelf uit te voeren niet meer nodig is (McAfee, 2018).

Daarnaast specialiseren cybercriminelen zich: waar de één zich bijvoorbeeld richt op spammail, legt de ander zich toe op het uitbuiten van kwetsbaarheden. Tenslotte kunnen virtuele valuta als Bitcoins cybercriminaliteit in de kaart spelen, omdat criminelen met die valuta anoniem financiële middelen kunnen verhandelen en witwassen (CipherTrace, 2018).

2.2 Nieuwe technologieën scheppen nieuwe kwetsbaarheden

Deze paragraaf beschrijft hoe het gebruik van nieuwe technologieën tot nieuwe digitale kwetsbaarheden kan leiden, of bestaande kwetsbaarheden kan vergroten. Zo vergemakkelijkt *machine learning* het uitvoeren van cyberaanvallen, doordat bestaande kwetsbaarheden automatisch en op grote schaal kunnen worden uitgebuit. Het gebruik van *machine learning* verdiept daarmee de risico's die samenhangen met bestaande kwetsbaarheden.

Nieuwe technologieën kunnen daarnaast ook zelf een bron zijn van nieuwe kwetsbaarheden. De kwantumcomputer zal het in de toekomst mogelijk maken om bestaande vormen van encryptie te breken, waardoor bestaande weerbaarheidsmaatregelen die daarvan gebruikmaken van de ene op de andere dag achterhaald zullen zijn. Ook het gebruik van *machine learning* creëert een nieuwe kwetsbaarheid, omdat de data waarop haar werking berust gemanipuleerd kunnen zijn.

2.2.1 Kunstmatige intelligentie en *machine learning*

De opkomst van kunstmatige intelligentie, ook wel *artificial intelligence* (AI) genoemd, schept nieuwe kwetsbaarheden. We lichten hieronder kort toe wat we onder AI en *machine learning* verstaan.

AI is niet nieuw. In de jaren ’50 werd het technologisch concept al verkend door wetenschappers, wiskundigen en filosofen. AI verwijst naar het bouwen van systemen die een zekere mate van intelligent gedrag vertonen (European Commission, 2019b). Daar bestaan verschillende technieken voor.

Een basale AI-techniek is *rule-based* AI. Het komt neer op het programmeren van een serie ‘als dit, dan dat’-instructies. Een voorbeeld hiervan is een computer die een waarschuwing geeft als het besturingsprogramma wordt afgesloten en er nog documenten openstaan. Veelal zien we dit niet meer als kunstmatige intelligentie, omdat we al gewend zijn aan dit ‘intelligente’ en zelfstandige gedrag van computersystemen.

Machine learning is geavanceerder dan *rule-based* AI. In plaats van vooraf gegeven instructies vormen data het uitgangspunt. *Machine learning* draait om het detecteren van patronen in bestaande data, om vervolgens in nieuwe data vergelijkbare patronen te leren herkennen. De technologie leunt sterk op statistiek.

Deep learning is een specifieke vorm van *machine learning*, die gebaseerd is op neurale netwerken – geïnspireerd op de biologie van ons brein – en verschillende lagen informatie met elkaar combineert. Een *deep learning*-algoritme voor gezichtsherkenning kan bijvoorbeeld drie lagen bevatten. De eerste laag zoekt in een afbeelding naar contrasten en kleuren. Een tweede laag combineert die informatie en zoekt naar kenmerken als randen of schaduwen. De derde laag kijkt of het specifieke kenmerken als een neus, lippen of ogen kan herkennen (Rathenau Instituut, 2019c).

De toegenomen rekenkracht van computers en de grote hoeveelheden beschikbare data hebben de ontwikkeling van *machine learning* en *deep learning* de laatste twee decennia in een stroomversnelling gebracht. Het zijn deze vormen van AI die in het huidige maatschappelijke en politieke debat volop in de belangstelling staan. Ook op het gebied van cyberweerbaarheid bestaat steeds meer belangstelling voor de mogelijkheden hiervan, zowel in offensieve als in defensieve zin. In dit rapport maken we verder geen onderscheid tussen *machine learning* en deep learning, en hanteren we de eerste term.

Machine learning kan op verschillende manieren worden ingezet om kwetsbaarheden in digitale systemen uit te buiten. Daarnaast is *machine learning* zelf kwetsbaar, doordat de data waarmee de algoritmes worden gevoed, bewust kunnen worden vervuild (Brundage et al., 2018). Deze mogelijkheden worden hieronder kort besproken.

Vergroting aanvalsoppervlak
Machine learning vergemakkelijkt het uitvoeren van cyberaanvallen. De technologie maakt het mogelijk om automatisch en op grote schaal kwetsbaarheden op te sporen in onvoldoende beveiligde systemen en IoT-apparatuur, en deze uit te buiten. Kwaadwillende partijen kunnen daarvan gebruikmaken.

Manipulatie berichtgeving
Machine learning kan daarnaast worden ingezet voor de manipulatie van tekst-, geluids- en beeldmateriaal. De laatste jaren worden deze creaties steeds overtuigender, en lastiger te onderscheiden van authentieke informatie (Brundage et al. 2018). Deze technologie kent bonafide toepassingen. Zo kan hiermee bij buitenlandse films de nasynchronisatie van het geluid gepaard gaan met aanpassing van het beeld, zodat het geheel bij de kijker natuurlijker overkomt.

Maar met behulp van *machine learning* kunnen ook *deep fake* video's worden gemaakt waarin personen bepaalde uitspraken in de mond worden gelegd. Ook kan vanuit een portretfoto een bewegende video worden gegenereerd (Mehta, 2019). Zowel het stemgeluid als de bewegingen van de persoon zijn daarbij nauwelijks van echt te onderscheiden. *Deep fake* video's kunnen worden ingezet voor de verspreiding van desinformatie en misleiding van burgers, bijvoorbeeld door bekende politici uitspraken te laten doen die ze nooit hebben gedaan (Verhagen, 2019). Zo verspreidde een Vlaamse politieke partij in 2018 een video waarin de Amerikaanse president Donald Trump België lijkt op te roepen om uit het klimaatakkoord te stappen (sp.a, 2018).

De technologie is ook steeds eenvoudiger te gebruiken. In juni 2019 presenteerden onderzoekers een methode die videofragmenten automatisch voorziet van een transcript, waarna een gebruiker enkel de tekst hoeft aan te passen om een nieuwe video te genereren waarin de nieuwe tekst natuurgetrouw wordt uitgesproken door de persoon in de video (Fried et al., 2019). In de publicatie roepen de onderzoekers op tot een verantwoord gebruik van de techniek, maar misbruik ligt uiteraard op de loer. Eerder besloot het OpenAI consortium om die reden een techniek die automatisch tekstuele nieuwsberichten genereert niet te publiceren, vanwege hun bezorgdheid over de impact op de nieuwsvoorziening (OpenAI, 2019).

Kunstmatige accounts op social media (bots) kunnen de verspreiding van gemanipuleerde informatie bevorderen door deze veelvuldig te delen of te 'liken' (Rathenau Instituut, 2018b). Mede door de massale verspreiding ervan op sociale media kan desinformatie grote impact hebben op de publieke nieuwsvoorziening en de publieke opinie en, in het verlengde daarvan, maatschappelijk ontwrichtende gevolgen hebben.

De met *machine learning* toegenomen mogelijkheden om tekst-, geluids- en beeldmateriaal te manipuleren onderstrepen het groeiende maatschappelijk belang van data-integriteit.

Datamanipulatie
Ook in een tweede opzicht heeft het gebruik van *machine learning* gevolgen voor data-integriteit. Doordat de werking van *machine learning* berust op algoritmes die met data worden gevoed, is de kwaliteit van de uitkomsten van *machine learning* afhankelijk van de kwaliteit van die data. Echter, data kunnen een vooringenomenheid (*bias*) bevatten en daarmee onbedoeld of onbewust de uitkomsten van toepassingen van *machine learning* beïnvloeden.

Kwaadwillende partijen kunnen deze kwetsbaarheid misbruiken door *machine learning* systemen met opzet te voeden met verkeerde data (*data poisioning*). Aanvallers die weten hoe een *machine learning* systeem is getraind kunnen op subtiele wijze de uitkomsten manipuleren. Dit kan bijvoorbeeld door een beeldherkenningsalgoritme foto's voor te schotelen die bewerkt zijn met een bepaalde 'ruis'. Het menselijk oog ziet nog steeds hetzelfde beeld, maar het beeldherkenningsalgoritme kan ermee om de tuin worden geleid. Zo kunnen toepassingen voor medisch-diagnostische doeleinden tot verkeerde conclusies komen op basis van met ruis vervuilde scans (Finlayson et al., 2018). Ook kunnen enkele stickers op een weg het Lane Detection System van een van de modellen van Tesla het systeem doen geloven dat er sprake is van een afwijkende rijbaan, en de auto van richting laten veranderen, terwijl een menselijke autobestuurder deze stickers eenvoudigweg zou negeren (Ackerman, 2019).

2.2.2 Kwantumcomputer als gamechanger

De komst van de kwantumcomputer zal naar verwachting grote betekenis krijgen voor de cyberweerbaarheid. De term kwantumcomputer verwijst naar een computer die gebruikmaakt van natuurkundige fenomenen zoals superpositie, verstrengeling en interferentie: fundamenteel andere natuurkundige fenomenen dan die in de huidige computerchips worden gebruikt. De verwachting is dat de kwantumcomputer hiermee bepaalde wiskundige problemen sneller kan oplossen.

Dit heeft consequenties voor het kunnen breken van de huidige manieren van digitale versleuteling (encryptie). De encryptietechnieken die tegenwoordig veel gebruikt worden zijn niet bestand tegen de rekenkracht van de kwantumcomputer. Het is dan ook de verwachting dat een kwantumcomputer beveiligde data sneller kan ontsluiten en beveiligde netwerken sneller kan binnendringen.

De ontwikkeling van kwantumtechnologie staat echter nog in de kinderschoenen. Voor zover bekend is het nog niet gelukt om een bruikbare kwantumcomputer te maken en het is lastig om te voorspellen wanneer dit wel gaat lukken. Om de natuurkundige inzichten om te zetten in praktisch bruikbare chips zijn namelijk nog wetenschappelijke doorbraken nodig – waarvan onduidelijk is hoe lang die nog op zich laten wachten. Experts schatten in dat het hoogst onwaarschijnlijk is dat binnen 10 jaar een bruikbare kwantumcomputer zal zijn ontwikkeld (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al., 2019). Er zijn ook schattingen dat het nog zeker 20 tot 30 jaar kan duren. Het valt in ieder geval te verwachten dat zodra de doorbraken zijn geboekt, de kwantumtechnologie snel op de markt zal worden aangeboden, en de capaciteit om bestaande encryptie te breken zich snel zal verspreiden.

Een aantal van de door ons geraadpleegde experts vragen zich af of het wel verstandig is om de doorbraken in kwantumtechnologie af te wachten. Vanwege de verwachte tijd en de kosten die gepaard gaan met migratie naar vormen van encryptie die bestand zijn tegen de kwantumcomputer, zijn ze van mening dat organisaties zich daar nu al op moeten voorbereiden. Ze wijzen er ook op dat kwaadwillende partijen een zogenoemde *harvest and decrypt*-strategie kunnen toepassen: deze partijen verzamelen nu (versleutelde) data, om die later te kunnen ontsleutelen. Van bepaalde gevoelige data is het voorstelbaar dat onthulling, ook over 30 jaar, schadelijk kan zijn, zoals bij medische gegevens of bedrijfsgeheimen.

2.3 Groeiende afhankelijkheid van externe partijen

Ook in een tweede opzicht doen zich nieuwe kwetsbaarheden voor, die samenhangen met verschuivende afhankelijkheidsrelaties en daaraan verbonden risico’s. Burgers, bedrijven en overheden zijn voor het goed functioneren van de digitale producten en diensten waarvan ze gebruikmaken, in toenemende mate afhankelijk van externe, vaak buitenlandse partijen. Zo worden steeds meer digitale diensten door (een beperkt aantal) *cloud providers* geleverd, waardoor de eindgebruiker voor tal van functies afhankelijk wordt van de kwaliteit, continuïteit en vertrouwelijkheid van de dienstverlening.

De afhankelijkheid van externe partijen doet zich ook voor op globaal niveau. Nederland en EU kennen een beperkte eigen bedrijvigheid op het gebied van IT en cyberweerbaarheid. Zo is Nederland voor de aanleg van 5G-netwerken afhankelijk van enkele grote buitenlandse technologiebedrijven, waarbij het de vraag is welke risico's daarmee gepaard gaan op het gebied van cyberweerbaarheid.

De afhankelijkheid van Nederland en de EU van externe partijen krijgt bovendien steeds meer een geopolitieke dimensie. Nederland en EU zitten op het globale IT-speelveld niet of nauwelijks nog 'aan tafel'. Dat geldt ook voor ontwikkelingen op het gebied van *machine learning* en de kwantumcomputer. Dat roept de vraag op of Nederland en de EU niet te veel achterop raken en macht uit handen geven.

De risico's die gepaard gaan met de verschuivende afhankelijkheidsrelaties worden hieronder meer in detail besproken.

2.3.1 Clouddiensten

Steeds opnieuw blijkt dat veel eindgebruikers over te weinig expertise en capaciteit beschikken om de cyberweerbaarheid van hun IT-systemen en -apparaten op orde te krijgen. Zoals hierboven reeds aan de orde is gekomen, worden ook relatief eenvoudige basisveiligheidsmaatregelen vaak niet of onvoldoende getroffen. Dat geldt zowel voor burgers als bedrijven en overheden. Maatregelen die de cyberweerbaarheid moeten verhogen, worden dan ook steeds vaker uitbesteed aan externe partijen middels clouddiensten.

Dit heeft significante voordelen, omdat cloudaanbieders over het algemeen meer expertise en capaciteit kunnen inzetten om data en processen te beveiligen dan de eindgebruikers. De behoefte aan dit soort diensten is ook aanzienlijk. Zo laat recent onderzoek zien dat 80 procent van de ondervraagde chief technology officers (CTO's) aangeeft de cyberweerbaarheid binnen de eigen organisatie onvoldoende te kunnen borgen (Elumalai et al., 2018).

Het uitbesteden van maatregelen op het gebied van cyberweerbaarheid past in de bredere trend dat de cloud niet langer alleen wordt gebruikt om data op te slaan, maar meer en meer ook om allerlei diensten te leveren. Dat geldt zowel voor allerlei software die *as-a-service* wordt aangeboden, als voor allerlei dataverwerkings-processen die in de cloud plaatsvinden. Dat kan zo ver gaan dat een computer er vooral toe dient om het beeldscherm, het toetsenbord en de muis te verbinden met een clouddienst die alle programma's uitvoert (*desktop-as-a-service*). De verwachting is dat deze trend zich de komende jaren verder zal doorzetten.

Het uitbesteden van verantwoordelijkheden aan cloudaanbieders heeft ook een keerzijde, want het creëert nieuwe risico's: uitval van functionaliteit bij verstoring en verlies van controle en zeggenschap over data en dataverwerking.

Uitval van functionaliteit
Zodra dataverwerkingsprogramma's niet langer op de eigen computer draaien maar in de cloud hun werk doen, leidt verstoring van de clouddienst tot uitval van functionaliteit. Dit risico kan één bepaalde taak treffen, maar ook meerdere taken tegelijk. Als meerdere taken zijn ondergebracht bij één cloudleverancier, en de clouddienst wordt verstoord of niet goed functioneert, kan dat leiden tot een Single Point of Failure. Denk aan een computersysteem dat zo veel programma's extern draait dat het zonder clouddienst niet of nauwelijks bruikbaar is. En de verleiding is vaak groot om diverse taken bij één leverancier onder te brengen. Dat hangt samen met het feit dat de clouddienstverlening wordt gedomineerd door een klein aantal spelers, waaronder Amazon, Microsoft en IBM (Dignan, 2018).

Het is belangrijk de ernst van dit risico te onderstrepen: als bijvoorbeeld een ministerie of een netbeheerder veel processen via de cloud afneemt, staat of valt de geboden dienstverlening met het op orde zijn van de clouddienst. Onderzoeksbureau Gartner wijst in zijn Emerging Risk Report van 2018 dan ook op de hoge risico's die zijn verbonden aan het gebruik van clouddiensten (Morris, 2018).

Verlies aan zeggenschap en controle
Een tweede risico van het gebruik van clouddiensten betreft het verlies aan controle en zeggenschap over data en dataverwerking. Naarmate data en dataverwerking meer in de cloud plaatsvinden, wint de vraag aan belang in hoeverre de cloudaanbieder zonder toestemming van de eindgebruiker data inziet, hergebruikt, met andere partijen deelt of de manier van verwerking verandert. Dat tast de autonomie van de eindgebruiker aan, omdat hij niet langer in de gelegenheid is te bepalen wie wat met zijn data doet.

Vendor lock-in
Het toenemende gebruik van clouddiensten is overigens niet altijd een vrije keuze van de eindgebruiker. Steeds vaker dwingen leveranciers gebruikers te kiezen voor een clouddienst, omdat ze stoppen het product aan te bieden dat op de eigen computer kan draaien. De migratiekosten die gepaard gaan met het overstappen naar een andere leverancier spelen daarbij een grote rol. De gebruikers worden als het ware 'ingesloten' door de leverancier (*vendor lock-in*).

2.3.2 5G- en satellietnetwerken

Ook voor de aanleg van 5G-netwerken en satellietnetwerken is sprake van een groeiende afhankelijkheid van externe partijen.

5G-netwerken
Slechts een beperkt aantal bedrijven heeft de expertise om 5G-netwerken aan te leggen en te onderhouden. Huawei, Nokia, Ericsson, Cisco en ZTE voorzien 90% van de markt voor netwerkapparatuur (Dell'Oro Group, 2019). Rondom het gebruik van apparatuur van marktleider Huawei is veel discussie ontstaan, omdat de zorg bestaat dat het bedrijf heimelijk gegevens die over het netwerk worden verstuurd, zou kunnen onderscheppen en kunnen delen met de Chinese overheid (Kaska et al., 2019).

Ook bestaan er zorgen over de kwaliteit van het netwerk. Het Britse Huawei Cyber Security Evaluation Centre (HCSEC) rapporteerde onlangs over ernstige tekortkomingen die een gevaar vormen voor de Britse nationale veiligheid. Basale maatregelen worden volgens het Centre door Huawei nagelaten, zoals het updaten van software-elementen met bekende kwetsbaarheden. Het HCSEC wees overigens al eerder op deze onvolkomenheden (HCSEC, 2019). Het rapport laat dus ook zien dat de bestuurlijke organen die toezien op het bouwen van de 5G-netwerken er vooralsnog niet in slagen de gewenste mate van veiligheid te waarborgen, en verbetering af te dwingen.

Maar het is belangrijk om niet alle pijlen te richten op Huawei. Gegeven de omvang en complexiteit van 5G-technologie geldt voor alle leveranciers dat het heel lastig, zo niet praktisch onmogelijk is om aan te tonen dat de apparatuur geen heimelijk geplaatste kwetsbaarheden bevat (Lysne, 2018). Ongeacht de leverancier en de maatregelen die gebruikers treffen om risico's te beperken, blijft veiligheid daarom voor een deel een kwestie van vertrouwen. Het land waarin de leverancier is gevestigd speelt hierbij een rol, bijvoorbeeld vanwege de wet- en regelgeving waaraan de leverancier is gebonden (Kleinhans, 2019).

Satellietnetwerken
Het is de verwachting dat in de nabije toekomst ook satellietnetwerken een grotere rol gaan spelen in het internetverkeer. Diverse partijen, waaronder de firma's Starlink en OneWeb, zijn van plan een groot aantal satellieten te lanceren waarmee wereldwijd breedband internet kan worden aangeboden (*mega satellite constellations*). Netwerken die zich richten op het verbinden van IoT-apparatuur zijn inmiddels beschikbaar via bijvoorbeeld de firma Iridium (McLean, 2019) en het Nederlandse Hiber (Blotenburg, 2018). Het feit dat Starlink een radiolicentie heeft gekregen van de Amerikaanse Federal Communications Commission voor 2200

satellieten (Boyle, 2018) en OneWeb voor 720 satellieten (Henry, 2018) geeft een indruk van de nog te verwachte omvang van de netwerken. Ook de Chinese firma LaserFleet heeft een begin gemaakt met het aanleggen van een breedband internetverbinding in 2018 (Jones, 2018). Als deze satellietnetwerken in de toekomst kunnen concurreren met nationale netwerken, zal dit naar verwachting leiden tot een grotere afhankelijkheid van Nederland van buitenlandse partijen wat betreft de zeggenschap over en het toezicht op deze communicatienetwerken.

2.3.3 Nederland en EU raken verder achterop

Landen als de Verenigde Staten en China en grote Amerikaanse en Chinese technologiebedrijven lopen voorop met investeringen in ontwikkelingen op het gebied van artificial intelligence/*machine learning* en de kwantumcomputer. Dit beeld wordt ondersteund door cijfers van de OECD. Private investeringen in AI in Europa liggen tot wel 5 keer lager dan in de VS. Ook het feit dat China jaarlijks meer dan 500 kwantumvindingen vastlegt in patenten, terwijl Europa het slechts bij enkele tientallen houdt, wijst in die richting (EPSC, 2019).

Nederland en EU dreigen hierdoor nog verder achterop te raken en nog afhankelijker te worden van externe, buitenlandse partijen (European Commission, 2018). Ondanks recent door de EU aangekondigde investeringen in onderzoek naar kwantumtechnologie, is het maar zeer de vraag of een Europese partij uiteindelijk in staat zal zijn om een kwantumcomputer succesvol op de markt te brengen.

Een vergelijkbaar verhaal geldt voor de bedrijvigheid die de EU weet te ontwikkelen op het gebied van cyberweerbaarheid. Genormaliseerd naar het Bruto Binnenlands Product neemt de EU een negende plaats in op de internationale ranking van cybersecuritybedrijven, na Israël, de Verenigde Staten, Nieuw Zeeland, Canada, Zwitserland, Singapore, Hong Kong en India. Terwijl driekwart van de meest innovatieve cybersecuritybedrijven uit de VS komt, komt slechts één op de tien uit de EU. Dit wordt mede geweten aan een gefragmenteerde regelgeving binnen de EU en een gebrek aan standaarden (STOA, 2017).

3 Verhoging cyberweerbaarheid met nieuwe technologie

Dit hoofdstuk beschrijft hoe de inzet van nieuwe technologieën bestaande en nieuwe kwetsbaarheden kan verhelpen, en daarmee kansen biedt om de cyberweerbaarheid te verhogen. Achtereenvolgens bespreken we de mogelijkheden van *machine learning*, weerbare communicatienetwerken zoals 5G-netwerken, LiFi, kwantumcommunicatie, gedistribueerde systemen en post-kwantumcryptografie.

3.1 Defensieve inzet van *machine learning*

Het is de verwachting dat *machine learning* in de nabije toekomst, via het automatisch opsporen en herstellen van kwetsbaarheden, van groot belang zal zijn om de cyberweerbaarheid te verhogen. Ook voor het bewaren van overzicht in complexe IT-netwerken kan *machine learning* behulpzaam zijn. De verwachtingen rond de inzet van deze defensieve vormen van *machine learning* zijn hooggespannen en worden onderstreept in de Nationale Cyber Security Research Agenda. Hieronder lichten we vier vormen van een defensieve inzet van *machine learning* kort toe.

3.1.1 Automatisch in kaart brengen van IT-netwerken

Het wordt een steeds grotere opgave om overzicht te houden van het gehele netwerk van een organisatie. Het gaat dan niet alleen om fysieke apparaten en computers, maar ook om de verschillende applicaties, data en digitale diensten die daarop functioneren. Het is de verwachting dat organisaties steeds meer gebruik zullen maken van automatische systemen die het netwerk in kaart brengen en monitoren. Monitoring van de samenstelling van het netwerk is eens te meer van belang in sectoren waar die regelmatig wisselt. Dat geldt bijvoorbeeld voor onderwijs- en zorginstellingen, waar het vaak voorkomt dat mensen gebruik maken van eigen apparatuur, en deze op het systeem aansluiten (*bring your own device*). *Machine learning* moet het mogelijk maken om ook nieuwe netwerkelementen te detecteren, die voor de beheerders nog niet bekend waren.

In geval van een incident moeten netwerkbeheerders snel kunnen zien welke onderdelen van het netwerk zijn getroffen en moeten worden hersteld. Automatische monitoringsystemen kunnen hen daarin ondersteunen. Een goed overzicht van het eigen netwerk en de onderlinge afhankelijkheid van de diverse deelsystemen is ook een voorwaarde voor het gebruik van automatische responssystemen. Zonder dat overzicht is het niet verantwoord om een responssysteem over te laten gaan tot het aan- of uitschakelen van een netwerkonderdeel.

3.1.2 Automatisch opsporen en herstellen van kwetsbaarheden

Het handmatig vinden en herstellen van kwetsbaarheden in software loopt steeds meer tegen zijn grenzen aan. Tijdens het schrijven van computerprogramma's sluipen onvermijdelijk fouten in de code, die kwetsbaarheden veroorzaken. Geavanceerde computerprogramma's bevatten al snel miljoenen regels aan code, waardoor het handmatig vinden en herstellen van fouten ondoenlijk is. De verwachting is dat met behulp van *machine learning* kwetsbaarheden kunnen worden opgespoord en ook verholpen (*automatic bug fixing*).

Ook voor het verweer tegen grootschalige, snelle en nieuwe soorten aanvallen met eerder onbekende eigenschappen zal naar verwachting menselijk handelen niet langer volstaan. Geautomatiseerde detectie en respons met behulp van *machine learning* kan hiervoor uitkomst bieden.

Maar de ontwikkeling van algoritmes die automatisch kwetsbaarheden herstellen bevindt zich nog in een experimentele fase. Een spraakmakend voorbeeld hiervan is Project Mayhem. Het project is de winnaar van een competitie die het Amerikaanse Defense Advanced Research Projects Agency (DARPA) organiseerde voor de ontwikkeling van automatische programma's die kwetsbaarheden kunnen detecteren en verhelpen (Fraze, 2017). Mayhem bleek tijdens een DEFCON-conferentie hierin beter te presteren dan mensen. Het team achter Mayhem verwoordde de reden voor het succes als volgt: "What machines (currently) lack in creativity, they make up for in speed, tenacity and scale. Mayhem analyzes thousands of programs in parallel in a few hours, a task that would take a human many years of tedious work. Mayhem can find thousands of bugs and previously unknown vulnerabilities in a day running on the cloud. In the time it takes an expert to open up a file, an automated system may have looked at hundreds."[4] Project Mayhem beperkt zich tot herkenning van reeds bekende bestaande kwetsbaarheden. Het vinden van nieuwe, onbekende kwetsbaarheden blijft

4 Zie https://forallsecure.com/blog/

vooralsnog mensenwerk. Cybersecurity-experts die dit soort kwetsbaarheden kunnen vinden, blijven dus noodzakelijk.

Automatisch herstel van softwarefouten raakt aan de Softwarerichtlijn
Er bestaat daarnaast twijfel over de rechtmatigheid van het automatisch herstellen van kwetsbaarheden in software. De Richtlijn betreffende de rechtsbescherming van computerprogramma's, ook wel bekend als de Softwarerichtlijn, bepaalt dat de rechthebbende toestemming moet verlenen aan gebruikers voordat deze software mogen bewerken. Artikel 5 van deze richtlijn voorziet wel in een uitzondering, die handelingen betreft die voor de gebruiker noodzakelijk zijn om het programma te kunnen gebruiken, onder meer om fouten te verbeteren. Maar de uitzondering geldt niet voor het verspreiden van verbeterde software. Dat roept de vraag op of het automatisch herstellen van kwetsbaarheden verenigbaar is met de wettelijke bepalingen.

3.1.3 Automatische detectie van storing, uitval en aanvallen

Ook als allerlei weerbaarheidsmaatregelen zijn genomen, zullen zich incidenten blijven voordoen in digitale systemen. Detectie en herstel van incidenten zijn dan ook van groot belang. Ook hiervoor bieden nieuwe technologische maatregelen mogelijkheden.

Grote organisaties brengen hun activiteiten op het gebied van cyberweerbaarheid vaak samen in een security operation center (SOC). Voor de automatische detectie van storing, uitval en aanvallen kunnen SOCs worden uitgerust met Security Information and Event Management (SIEM) technologie. De komende jaren zal naar verwachting het gebruik van deze technologie sterk toenemen (TechNavio, 2017). De SIEM-technologie kan beheerders ook ondersteunen in het detecteren en het inschalen van meldingen van incidenten. *Machine learning* kan beheerders helpen om meldingen beter op waarde te schatten. Uit onderzoek van Verizon blijkt dat meer dan 70% van de technische meldingen van datalekken door beheerders onopgemerkt blijven (Verizon, 2018).

Vanwege de hoge operationele kosten komt het regelmatig voor dat diverse organisaties gezamenlijk gebruikmaken van één SOC. Omdat de kwaliteit van een SOC toeneemt naarmate het over meer informatie over mogelijke dreigingen kan beschikken, vormt het onderling delen van de informatie een belangrijke randvoorwaarde voor het succesvol functioneren van een SOC. Binnen de Rijksoverheid beschikken verschillende organisaties, zoals de Belastingdienst en Rijkswaterstaat, over een eigen SOC (Algemene Rekenkamer, 2019a). Ook worden

krachten van SOCs van de Rijksoverheid gebundeld in een Joint-SOC (SSC-ICT, 2019).

Automatische detectie van incidenten is overigens niet foutloos. Een medewerker zal regelmatig moeten checken of afwijkingen die het systeem vindt, ook daadwerkelijk incidenten zijn, en de aard en ernst ervan moeten beoordelen. Zeker bij gerichte, geavanceerde aanvallen zal menselijk beoordelings- en handelingsvermogen nodig blijven om te voorkomen dat aanvallers grote schade aanrichten. Cybersecurity-experts met verstand van zaken blijven dus onverminderd nodig.

Monitoring en detectie is overigens niet alleen bedoeld voor grote organisaties. Voor thuissituaties en het MKB worden diverse producten aangeboden die vergelijkbare technieken toepassen. Zo heeft de firma Slatman IT een app ontwikkeld waarmee gebruikers inzicht kunnen krijgen in het gedrag van de apparatuur in hun (thuis)netwerk. De app informeert gebruikers over veiligheidsrisico's. Een vergelijkbare dienst biedt het Nederlandse Dyne in het open source project Dowse, dat met subsidie van het SIDN-fonds wordt ontwikkeld (SIDN-fonds, 2018). Voorlopig vormt de extra werklast die dit soort producten voor de gebruiker met zich meebrengt wel een drempel voor grootschalig gebruik ervan door MKB-ers en thuisgebruikers.

Behavioural analytics
Voor relatief eenvoudige vormen van detectie wordt *machine learning* overigens al langer gebruikt. Zo kan het gedrag van gebruikers in digitale systemen automatisch worden geanalyseerd (*behavioural analytics*). Met behulp van *machine learning* kan op grote schaal afwijkend gedrag worden onderkend. Banken gebruiken deze aanpak al jaren om ongebruikelijke pintransacties te signaleren en te blokkeren. Met behulp van *behavioural analytics* wordt het ook steeds beter mogelijk om op basis van persoonlijke kenmerken als typesnelheid en muisbewegingen individuele gebruikers te identificeren. Deze technologie kan daarmee een aanvulling vormen op andere authenticatietechnieken. Een gebruiker die bijvoorbeeld toegang heeft tot de financiële administratie, maar daar normaal gesproken geen gebruik van maakt, kan op het moment dat hij overgaat tot deze actie om extra identificatie worden gevraagd. Deskundigen verwachten dat deze mogelijkheden een grote bijdrage kunnen leveren aan de verhoging van de cyberweerbaarheid (Hill, 2017).

3.1.4 Automatische respons op aanvallen

Zodra duidelijk is dat een incident in een digitaal systeem schade aanricht, is het zaak om daar zo snel mogelijk op te reageren. Vanwege de steeds grotere schaal

waarop incidenten plaatsvinden, biedt automatisering ook hier uitkomst. Aanvallers kunnen bijvoorbeeld gebruikmaken van netwerken bestaande uit grote hoeveelheden geïnfecteerde apparatuur, die in aantal kunnen oplopen tot honderdduizenden, zoals het Mirai-botnet (Fruhlinger, 2018). Een handmatige reactie geven op zulke massale aanvallen is eigenlijk niet te doen.

Technologieën die hiervoor uitkomst kunnen bieden zijn veelal gebaseerd op klassieke verdedigingsstrategieën. Zo kunnen aanvallers worden afgeleid, zodat ze worden beziggehouden en de verdedigers in de gelegenheid worden gesteld om een zwakke plek te vinden bij de aanvaller (*honey pot*). Aanvallen kunnen ook worden afgeslagen of worden ontweken door de route naar het doelwit digitaal te verleggen. Verder is het mogelijk om het onderdeel van het systeem waarop de aanval is gericht, tijdelijk uit te schakelen of los te koppelen (*containment*). Gezien de snelheid waarmee aanvallen kunnen plaatsvinden, is het de verwachting dat de automatisering van dit soort verdedigingsstrategieën de komende jaren verder zal toenemen.

Het onklaar maken van de aanvalsmiddelen of de aanvaller is soms de meest doeltreffende manier om een aanval af te slaan. Automatische offensieve technieken zijn dan ook in opkomst. Organisaties die deze methoden toepassen bevinden zich wel op het grensvlak van wat wettelijk is toegestaan (Higgins, 2017). De Wet Computercriminaliteit ziet het binnendringen van computersystemen zonder toestemming van de eigenaar als computervredebreuk. Het hacken van aanvalsmiddelen is wel toegestaan zodra deze zich binnen het eigen netwerk bevinden. In de praktijk zijn de grenzen daarvan vaak lastig vast te stellen, omdat interne en externe systemen steeds nauwer met elkaar verweven raken. Verder bestaat de vrees dat offensieve technieken kunnen leiden tot een risicovolle escalatie van aanvallen en tegenaanvallen (Higgins, 2017). Gezien deze moeilijkheden is de verwachting dat menselijk handelen onderdeel zal blijven van deze processen.

Voor inlichtingen- en veiligheidsdiensten met de bevoegdheid om offensieve technieken in te zetten, spelen deze beperkingen in mindere mate. De Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) stelt wel beperkingen aan de inzet van een automatische respons. Zo moeten tapbevoegdheden ‘zo gericht mogelijk’ worden ingezet.

3.2 *Machine learning* tegen *deep fakes*

Behalve voor het automatisch opsporen en herstellen van kwetsbaarheden en voor een automatische respons op aanvallen, kan *machine learning* worden ingezet bij

de bestrijding van gemanipuleerd beeldmateriaal (*deep fakes*), en de verspreiding ervan.

Voor de bestrijding van *deep fakes* zijn inmiddels diverse mogelijkheden ontwikkeld. Zo berekent het MediFor-systeem van DARPA een integriteitsscore voor nieuwsberichten op basis van diverse kenmerken. Daarbij wordt gekeken naar sporen van manipulatie in beeld- en videomateriaal; het analyseren van lichtinval (belichting van gezichten, reflecties van lampen); en door, bijvoorbeeld, de weersomstandigheden op een foto te vergelijken met de weersmetingen op dat moment, op die plek. Ook voor het detecteren van valse accounts en automatische bots die massaal berichten verspreiden op social media wordt *machine learning* ingezet, bijvoorbeeld met behulp van Botometer (Karatas, 2017).

Het ligt in de lijn der verwachting dat ook in de detectie van *deep fakes* een wedloop zal ontstaan. Zodra *machine learning* systemen worden ingezet om gemanipuleerde beelden te detecteren, zullen aanvallende partijen proberen om de systemen die beeld- en videomateriaal manipuleren, daarop aan te passen.

De effectiviteit van technische detectie van gemanipuleerde berichtgeving is afhankelijk van het moment waarop het wordt ingezet. Zodra desinformatie eenmaal is verspreid, is het lastig om deze teniet te doen. Doordat social mediaplatformen als Twitter, Snapchat en Facebook gericht zijn op een zo snel mogelijke verspreiding van informatie, is het de vraag hoeveel ruimte ze bieden voor preventieve filtering. Van andere mediaplatformen, zoals online nieuwssites, kan eerder worden verwacht dat zij gebruik gaan maken van detectiesystemen tegen *deep fakes*.

3.3 Weerbare communicatienetwerken

Een belangrijk onderdeel van cyberweerbaarheid betreft de beschikbaarheid, betrouwbaarheid en beveiliging van gegevensoverdracht via communicatienetwerken. Op dit gebied doen zich diverse nieuwe technologische ontwikkelingen voor, zoals de opkomst van 5G-netwerken, LiFi, satellietnetwerken en kwantumcommunicatie. Elk van deze ontwikkelingen brengt kansen met zich mee voor het verhogen van de cyberweerbaarheid. Omdat we ervan uitgaan dat Nederland geen eigen omvangrijke satellietnetwerken zal bouwen in de komende 8 jaar, laten we die technologische ontwikkeling hier buiten beschouwing.

3.3.1 5G-netwerken bieden voordelen

5G biedt naast een snellere verbinding met het netwerk en een grotere datacapaciteit ook diverse mogelijkheden om de beschikbaarheid, betrouwbaarheid en beveiliging van het dataverkeer te verhogen (Shafi, 2017; Norrman et al., 2018). We zullen hier vooral ingaan op een aantal verschillen tussen 5G- en 4G-netwerken. 5G-communicatietechnologie is overigens een verzamelnaam voor een scala aan verbindingen, waarvan een aantal nog in ontwikkeling is[5].

5G voorziet in Ultra-Reliable Low Latency Communication (URLLC), dat ervoor moet zorgen dat bij kritieke systemen data met zo min mogelijk vertraging en fouten heen en weer worden gezonden. 5G-apparaten kunnen bijvoorbeeld sneller van antenne wisselen, waardoor de overdracht van informatie naar mobiele apparaten betrouwbaarder verloopt. Dit is bijvoorbeeld van belang voor zelfrijdende auto's of het op afstand aansturen van operatierobots.

Een groot verschil met 4G is de mogelijkheid die 5G biedt om datastromen te scheiden (*network slicing*). Dit maakt het bijvoorbeeld mogelijk om beter te bepalen wie toegang krijgt tot welke data. *Network slicing* maakt ook nieuwe verdienmodellen mogelijk. Aanbieders kunnen diensten aanbieden die variëren in hoeveelheid data, overdrachtssnelheid, verbindingssnelheid en betrouwbaarheid. Afhankelijk van de gewenste mate van cyberweerbaarheid kunnen eindgebruikers verschillende keuzes maken. 5G biedt ook de mogelijkheid om communicatie binnen een netwerk beter te versleutelen.

Een ander verschil tussen 5G en 4G is de overstap naar virtuele simkaarten. Bij 5G is het niet langer nodig om gebruik te maken van een fysieke simkaart. Netwerk operators kunnen in plaats daarvan een eigen authenticatiemethode kiezen, op basis van softwarecertificaten, tokenkaarten of andere sleutels. Nieuwe methoden kunnen later worden toegevoegd aan de 5G Authentication and Key Agreement (5G AKA). Dat maakt het 5G-netwerk toekomstbestendiger. Daar staat tegenover dat het ontbreken van een fysiek element in de authenticatiemethode de betrouwbaarheid ervan mogelijk kan verlagen.

Het is de bedoeling dat 5G ook nieuwe maatregelen treft tegen afluisteren, waaronder het uitsluiten van IMSI-*catching*. IMSI-*catching* is een methode waarbij een aanvaller lokaal een nieuwe zendmast toevoegt aan een netwerk, waarmee de verbinding kan worden getapt. In 5G-netwerken moeten zendmasten elkaar

5 Met name de standaarden zijn nu in ontwikkeling. Hier zijn een groot aantal organisaties bij betrokken, zoals de 3rd Generation Partnership Project (3GPP), de Internet Engineering Task Force (IETF), GSM Association (GSMA), European Telecommunications Standards Institute (ETSI) working group en het Open Network Automation Platform (ONAP).

onderling authentiseren, waardoor valse zendmasten kunnen worden uitgesloten. Recent onderzoek toont echter aan dat ook 5G kwetsbaar is voor IMSI-catching (Whittaker, 2019). Maar zoals eerder vermeld, is 5G-technologie nog in ontwikkeling. Het is dus goed mogelijk dat tegen de tijd dat de technologie op grote schaal zal worden gebruikt, deze kwetsbaarheid zal zijn verholpen.

Rondom 5G-netwerken is ten slotte veel discussie ontstaan over de aanwezigheid van ‘achterdeurtjes’ in de apparatuur of software van leveranciers. In het kader daarvan is het belangrijk om te beseffen dat de Nederlandse Telecommunicatiewet telecomproviders verplicht voorzieningen te treffen die het mogelijk maken om hun diensten te tappen (*lawful interception*). Het tappen van internetcommunicatie wordt namelijk van belang geacht in de strijd tegen misdaad en terrorisme. Maar het inbouwen van de mogelijkheid om de communicatie te tappen, biedt ook andere, kwaadwillende partijen de gelegenheid daarvan gebruik te maken.

Al met al valt niet op voorhand te bepalen of de nieuwe mogelijkheden die 5G-netwerken bieden zullen leiden tot weerbaardere communicatienetwerken dan 4G-netwerken. Dat zal in de praktijk moeten blijken.

3.3.2 LiFi biedt voordelen in specifieke situaties

LiFi is een techniek waarbij licht wordt gebruikt om data over te dragen tussen apparaten. De data-overdracht wordt technisch mogelijk gemaakt door LED-lampen zeer snel aan en uit te schakelen, met een frequentie die door het menselijk oog niet wordt opgemerkt. De techniek wordt al op de markt aangeboden door de firma PureLifi.

LiFi-communicatie biedt vooral kansen onder specifieke omstandigheden. In situaties waar het afluisteren van radiosignalen moet worden voorkomen, kan deze technologie van pas komen. LiFi maakt het namelijk mogelijk om data zeer lokaal te delen: omdat licht niet door muren heen kan, blijft het signaal binnenskamers. Verder kan licht, in tegenstelling tot radiosignalen, onder water grote afstanden overbruggen. Ook in vliegtuigen en andere omgevingen waar elektromagnetische interferentie een gevaar vormt, biedt LiFi mogelijk uitkomst. Op het jaarlijkse LiFi-congres stond het gebruik ervan in de luchtvaart volop in de aandacht.[6]

Het Agentschap Telecom wijst in een rapport uit 2018 op andere voordelen van LiFi. Het wordt gezien als een alternatief voor het veelgebruikte WiFi. Daar waar veel WiFi-netwerken samenkomen, zoals in steden en drukke gebieden, ontstaat

6 Zie https://lificongress.com/

het risico op storingen. LiFi kan in die gevallen uitkomst bieden. Het agentschap signaleert wel dat er nog geen universele standaard bestaat voor LiFi-communicatie, en dus ook nog geen overeenstemming over het te gebruiken type authenticatie en encryptie. Het is voor de cyberweerbaarheid van belang dat deze aspecten in een standaard worden uitgewerkt voordat de technologie op grote schaal wordt toegepast (Van der Gaast et al., 2018).

3.3.3 Kwantumcommunicatie merkt afluisteren op

Kwantumtechnologie maakt het mogelijk om informatie tussen twee plekken over te dragen, zonder dat de informatie onopgemerkt kan worden afgeluisterd. De natuurkundige wetten bepalen namelijk dat observatie van een kwantumobject onherroepelijk een verandering van het signaal teweegbrengt. Een verzender kan dus meteen de overdracht staken als van afluisteren sprake lijkt te zijn.

Al meer dan 10 jaar zijn er systemen te koop die van kwantumcommunicatie gebruikmaken, bijvoorbeeld van de firma ID Quantique. Deze systemen werken met glasvezelverbindingen tot enkele honderden kilometers. Chinese wetenschappers meldden in 2017 dat zij er in geslaagd waren om over een afstand van 1200 kilometer informatie uit te wisselen met een kwantumcommunicatiesatelliet (Liao et al., 2017). In Nederland is het initiatief genomen om tussen Amsterdam, Delft, Leiden en Den Haag een kwantumcommunicatienetwerk te bouwen. Tevens is een Europese samenwerking van start gegaan met als doel om in zeven Europese landen, waaronder Nederland, een kwantumcommunicatienetwerk te realiseren. Dit Europese initiatief bevindt zich nog in de planningsfase (DG CONNECT, 2019b).

Belangrijke nadelen van kwantumcommunicatiesystemen zijn de kosten en afmetingen. Een kwantumcommunicatiesysteem past (nog) niet in smart phones of IoT-apparaten. Het toepassingsgebied van kwantumcommunicatie blijft vooralsnog beperkt tot industriële en overheidstoepassingen waarbij het risico op afluisteren tot het minimum moet worden beperkt.

3.4 Gedistribueerde systemen ter preventie van Single Points of Failure

Gedistribueerde systemen maken het mogelijk om een grootschalige uitval van IT-systemen te voorkomen. Dit risico doet zich vooral voor bij Single Points of Failure, waarbij diverse, bijvoorbeeld geschakelde systemen voor hun functioneren afhankelijk zijn van één onderdeel. Als dat ene onderdeel uitvalt, vallen de daarvan

afhankelijke systemen ook uit. In plaats van gebruik te maken van één dienstverlener of één computersysteem, worden bij een gedistribueerd systeem data en software verdeeld over diverse aanbieders en systemen. Gedistribueerde systemen kunnen hierdoor blijven functioneren, ook als een deel van de aanbieders en systemen niet beschikbaar is.

Zo maakt het Interplanetary File System (IPFS) een gedistribueerde dataopslag mogelijk, zonder gebruik te maken van centraal beheerde datacenters. Stukjes en beetjes van de data en de aansturing daarvan worden verdeeld over een groot netwerk zonder centraal punt. Decentralisatie kan zelfs zover gaan dat systemen zo worden ingericht dat ze ook zonder aansturing door mensen blijven functioneren. Er wordt dan gesproken van gedistribueerde autonome organisaties (*distributed autonomous organisations*).

Binnen grote organisaties worden gedistribueerde systemen reeds volop ingezet. Zo biedt Netflix zijn videodienst aan via een gedistribueerd systeem van tienduizenden computers (Chella, 2018). Het gebruik ervan in samenwerkingsverbanden tussen organisaties bevindt zich echter nog in een experimentele fase. Het gebrek aan een centraal aanspreekpunt maakt het bijvoorbeeld lastig voor publieke organisaties om zich ertoe te verhouden.

3.5 Post-kwantumcryptografie

Zoals in het vorige hoofdstuk uiteen is gezet, maakt de kwantumcomputer de huidige versleutelingstechnologie van de ene op de andere dag ouderwets en ineffectief. De kwantumcomputer kan dan ook worden beschouwd als een gamechanger. De komst van de kwantumcomputer dwingt dan ook tot het ontwikkelen van nieuwe, sterkere cryptografische standaarden. Deze zogeheten post-kwantumcryptografie, die gebruikmaakt van complexere en grotere sleutels, moet de rekenkracht van kwantumcomputers kunnen weerstaan. Hoewel het waarschijnlijk nog enige tijd zal duren voordat een in de praktijk bruikbare kwantumcomputer voorhanden is, is het voor een aantal organisaties al wel van belang zich voor te bereiden op migratie naar post-kwantumcryptografie.

Internationale prijsvraag NIST

Het is op dit moment nog onduidelijk welke vorm van post-kwantumcryptografie wereldwijd zal worden toegepast. Diverse partijen zijn bezig met de ontwikkeling van een standaard. Het Amerikaanse National Institute of Standards and Technology (NIST) heeft een internationale prijsvraag uitgeschreven met als doel het ontwikkelen, evalueren en standaardiseren van één of meer kwantumbestendige cryptografische algoritmes. Het duurt mogelijk tot 2024 voordat

NIST met een eindoordeel komt, dat naar verwachting zal worden overgenomen door de belangrijkste spelers in het digitale domein (NIST CSRC, 2019).

De vraag is hier op zijn plek waarom de EU in deze een afwachtende houding aanneemt en het initiatief bij het Amerikaanse NIST laat. Het European Telecommunications Standards Institute (ETSI) of de Internationale Standaardisatie Organisatie (ISO) lijken immers ook geschikte partijen om een standaardisatieproces te initiëren.

Kwantummigratie als opgave

Vanwege de onzekerheid over de standaard(en) voor post-kwantumcryptografie, is het vooralsnog onduidelijk wat de migratie naar deze sterke vorm van encryptie met zich mee zal brengen. Volgens experts komt het in ieder geval neer op een omvangrijke opgave (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al., 2019).

Daarbij moet worden bedacht dat zodra een partij erin slaagt een krachtige kwantumcomputer te maken, dit het wereldwijde einde zal betekenen van de beschermende werking van de gebruikelijke encryptietechnologie. Een eerdere, wereldwijde vervanging van een encryptiestandaard laat zien hoe lang het kan duren voordat zo'n overstap volledig is gemaakt. Nadat in 2005 een kwetsbaarheid werd gevonden in de populaire MD5-encryptietechnologie, nam Microsoft pas in 2014 het besluit om deze technologie uit te schakelen in Windows (Microsoft, 2014). Voor een afzonderlijke organisatie mag het nog relatief eenvoudig zijn om een nieuwe, kwantumbestendige encryptiestandaard in te voeren om haar digitale systemen te beveiligen. Maar tegelijkertijd moet de brede omgeving van de organisatie waarmee ze digitaal in verbinding staat, eenzelfde stap maken. Pas dan kan de oude standaard worden uitgeschakeld.

De migratie naar kwantumbestendige encryptie zou wel eens 20 jaar in beslag kunnen nemen. Zodra er overeenstemming bestaat over de standaarden, zullen deze moeten worden geïmplementeerd in allerlei programmeertalen, protocollen en chips. Vervolgens moeten leveranciers die gaan gebruiken in hun producten. Daarna – leert de ervaring – kan het nog vele jaren duren voordat de meerderheid van de internetsystemen van updates zijn voorzien (Saffman, 2016).
Bovendien moet worden bedacht dat de migratie niet alleen een kwantumbestendige versleuteling van gevoelige data van bedrijven en overheden betreft, maar ook de versleuteling of vernietiging van alle kopieën die gebruik maakten van oude encryptietechnologie. Veel organisaties zullen dan pas beseffen hoe wijd hun gegevens zijn verspreid.

Het is verder van belang om te beseffen dat alle informatie die vandaag de dag over het internet wordt verstuurd en gebruik maakt van de gangbare encryptie, kan worden ontvreemd, en ontsleuteld zodra een krachtige kwantumcomputer voorhanden is.

Het is daarom van belang om nu al te anticiperen op de komst van de kwantumcomputer, voor de bescherming van gevoelige persoonsgegevens en bedrijfsgeheimen. Van patiëntendossiers tot concurrentiegevoelige informatie is het voorstelbaar dat inzage door ongewenste partijen ook over 30 jaar grote gevolgen kan hebben. Alleen al om deze reden is het raadzaam om de migratie naar post-kwantumcryptografie zo snel mogelijk in gang te zetten.

Die technieken voor een kwantumbestendige versleuteling zijn nu al voorhanden. Voor sommige doeleinden – zoals het beveiligen van staatsgeheimen – worden deze ook al gebruikt.

Monitoring
Vanwege de grote onzekerheid over de termijn waarop een werkende kwamtumcomputer kan worden verwacht en de grote impact daarvan, is het van belang ontwikkelingen op dit gebied nauwlettend te monitoren (Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing et al., 2019).

4 Verhoging cyberweerbaarheid met bestaande technologie

Dat het maar beperkt zin heeft om in te zetten op allerlei nieuwe technologieën, wanneer niet tegelijkertijd op grotere schaal gebruik wordt gemaakt van reeds voorhanden zijnde technologieën ter versterking van de cyberweerbaarheid, is al in de inleiding genoemd; het was een belangrijke reactie van de geïnterviewde deskundigen op de onderzoeksvraag. Inderdaad bieden reeds bestaande, maar onderbenutte technologische maatregelen kansen om de cyberweerbaarheid te verhogen.

In dit hoofdstuk bespreken we achtereenvolgens de belangrijkste voorbeelden hiervan: basisveiligheidsmaatregelen als sterke wachtwoorden en software updates; biometrische identificatie; Privacy Enhancing Technologies; encryptie; digitale ondertekening van berichten; Secure Development and Operations; veiligere aanvoerketens; veiligere communicatieprotocollen; en open standaarden en *open source software*.

4.1 Basisveiligheidsmaatregelen

Zoals in Hoofdstuk 2 reeds is aangegeven, valt er met het oog op de cyberweerbaarheid nog veel winst te halen met basisveiligheidsmaatregelen. Dat geldt zowel voor burgers, bedrijven als overheden. Het uitblijven van deze maatregelen maakt IT-systemen en -apparaten kwetsbaar voor cyberaanvallen. Die kwetsbaarheid wordt alleen maar groter als aanvallers gebruik kunnen maken van nieuwe technologische mogelijkheden als het automatisch opsporen en uitbuiten van kwetsbaarheden met behulp van *machine learning*.

De basisveiligheidsmaatregelen zijn al vaak beschreven. Hieronder vallen maatregelen als het gebruik van sterke wachtwoorden, 2-factor-authenticatie, het tijdig installeren van software-updates en het maken van back-ups van belangrijke bestanden (NCTV, 2019b; Rathenau Instituut, 2017).

De praktijk leert dat eindgebruikers vaak moeilijk te bewegen zijn om van deze maatregelen gebruik te maken (Van der Grient & Konings, 2018). Jaar na jaar constateert het Cybersecuritybeeld Nederland dat er onvoldoende actie wordt ondernomen om de basisveiligheid te verbeteren.

4.2 Biometrie

Het gebruik van biometrie is sterk in opkomst. Biometrische technieken, zoals een vingerafdruk of gezichtsscan, maken het voor gebruikers mogelijk om in te loggen op bijvoorbeeld hun smartphone zonder gebruik te hoeven maken van een wachtwoord. Op korte termijn lijkt dit winst te kunnen opleveren, omdat het een sterkere beveiliging oplevert dan de vaak zwakke wachtwoorden die gebruikers instellen. Maar tegelijkertijd worden hiermee nieuwe kwetsbaarheden geïntroduceerd. Zo kunnen met het algoritme DeepMasterPrints vingerafdrukscanners worden misleid (Hern, 2018). En onderzoekers wisten met een 3D-print van hun hoofd de gezichtsherkenning van populaire smartphones om de tuin te leiden (Major, 2018).

Hierbij moet worden bedacht dat de gevolgen van een biometrie-hack groter kunnen zijn dan bij gebruik van een wachtwoord met tekens of een pincode. Een wachtwoord of pincode kan worden veranderd als ze zijn gelekt of achterhaald, voor een gehackte vingerafdruk of irisscan is dat niet mogelijk. Uit biometrische scans kunnen bovendien gevoelige eigenschappen van een persoon worden afgeleid, zoals een diabetesdiagnose op basis van een irisscan (Pultarova, 2017), of andere gezondheidsinformatie. Er kunnen dan ook serieuze vraagtekens worden geplaatst bij de wenselijkheid van een grootschalig gebruik van biometrie voor identificatiedoeleinden.

4.3 Privacy Enhancing Technologies

Hoe meer (persoons)gegevens op het internet worden gedeeld, hoe groter de kans dat deze gegevens worden gelekt of gehackt. Inperking van de grote hoeveelheden gegevens die worden gedeeld, kan de cyberweerbaarheid dan ook substantieel verhogen. Er zijn diverse Privacy Enhancing Technologies (PETs) voorhanden die dit mogelijk maken. Voorbeelden hiervan zijn zoekmachines als DuckDuckGo en Startpage, die zoektermen van gebruikers niet opslaan, en de chatdienst SnapChat, die de sporen van gebruikers na gebruik kan wissen.

Een in Nederland ontwikkeld voorbeeld van een PET is het Identity Management System I Reveal My Attributes (IRMA). Het stelt gebruikers in staat om zelf hun digitale identiteit te beheren en alleen die gegevens te verstrekken die voor een bepaald doel nodig zijn. Zo moet bij de aankoop van alcoholische dranken een verkoper kunnen vaststellen dat een klant de wettelijk vastgestelde minimumleeftijd heeft. Het voldoen aan de minimumleeftijd is een voorbeeld van een persoonlijk ‘attribuut’. IRMA stelt de gebruiker in staat om alleen het bewijs te tonen dat aan deze leeftijdseis wordt voldaan, in plaats van een traditioneel identificatiebewijs

zoals een rijbewijs, waarop allerlei andere persoonlijke informatie staat. Het systeem minimaliseert daarmee de uitwisseling van gegevens.

Een ander voorbeeld van een PET betreft het opensourceproject Social Linked Data (Solid), van de internetpionier Tim Berners Lee. Solid zet ontwikkelaars van software ertoe aan om de dataopslag gescheiden te houden van de dataverwerking. Gegevens die aan Solid worden toegevoegd, kunnen worden beheerd in een Personal Online Data Store (Pods). Gebruikers kunnen vervolgens zelf bepalen wanneer en waarvoor de gegevens in hun Pods worden gebruikt, bijvoorbeeld om zich te identificeren (Solid, 2019).

4.4 Encryptie

Met behulp van encryptie kunnen (persoons)gegevens dusdanig worden versleuteld dat ze alleen leesbaar zijn voor degenen die beschikken over de juiste sleutel. Encryptie wordt veel gebruikt om data te beveiligen die via netwerken worden verzonden en om gevoelige gegevens op computers, servers en mobiele apparaten te beschermen. Ook Privacy Enhancing Technologies maken voor hun informatiebeveiliging gebruik van encryptie.

Het is de verwachting dat encryptie in de komende jaren niet alleen in de privésfeer zal worden gebruikt, zoals in chatapps als Whatsapp, Signal en Telegram, maar ook in zakelijke communicatie. Daarnaast is de versleuteling van gegevens in opslag, bijvoorbeeld in clouddiensten, in opkomst.

Secure multi-party computation
Een kanttekening bij het gebruik van encryptie betreft het kunnen uitwisselen van gegevens met andere partijen. Veel gebruikte encryptietechnieken vereisen dat informatie eerst wordt ontsleuteld voordat deze kan worden gedeeld of verwerkt. Eenmaal ontsleuteld, is de informatie kwetsbaar voor cyberaanvallen. Ontwikkelingen op het gebied van zogenoemde homomorfe encryptie bieden hiervoor uitkomst. Gebruikers kunnen dankzij deze techniek versleutelde gegevens verwerken zonder ze eerst te moeten ontsleutelen. De kans op ongewenste inzage wordt zodoende verkleind.

Deze techniek komt bijvoorbeeld van pas in situaties waarin partijen belang hebben bij het kunnen beschikken over elkaars gegevens, maar geen inzage willen geven in al hun informatie. Dat kan bijvoorbeeld het geval zijn als meerdere partijen gegevens willen uitwisselen over cyberkwetsbaarheden en -aanvallen, maar niet op individueel niveau willen prijsgeven dat ze doelwit zijn van een bepaalde aanval.

Secure multi-party computation stelt de partijen in staat informatie te delen, zonder dat de gegevens te herleiden zijn tot een bepaalde partij.

Kwetsbaarheden in encryptietechnologie
Een tweede kanttekening bij het gebruik van encryptie betreft het risico dat de versleuteling wordt gebroken. De meest bekende methode hiervoor is een *brute force* aanval, een aanval met brute kracht. Een aanvaller probeert in dit geval net zo veel sleutels uit tot de juiste is gevonden. Hoe meer rekenkracht een aanvaller heeft, hoe groter de kans dat het zal lukken.

Een andere methode om encryptie te kraken zijn *side-channel* aanvallen, die zich richten op de directe omgeving waarin het programma opereert. Stroomverbruik, elektromagnetische velden of geluid kunnen bijvoorbeeld informatie bieden waaruit de juiste sleutel kan worden afgeleid. Ook kan een aanvaller gebruikmaken van *social engineering*: door middel van psychologische beïnvloeding van betrokken personen kunnen zij worden verleid de encryptiesleutel prijs te geven of de inhoud van de versleutelde informatie bekend te maken.

Zoals eerder aangegeven, zal de komst van de kwantumcomputer het op termijn mogelijk maken om op grote schaal bestaande vormen van encryptie te breken.

Belemmering voor opsporing
Een derde kanttekening bij het gebruik van (sterke) encryptie betreft het gebruik dat criminelen of terroristische groeperingen ervan kunnen maken om hun communicatie te beveiligen, en daarmee te ontsnappen aan opsporingsinspanningen van politie en justitie. Sommige overheden roepen daarom op tot ‘verantwoorde encryptie’. Deze kan door bijvoorbeeld technologiebedrijven worden doorbroken wanneer sprake is van een gerechtelijk bevel. In Australië is een wet aangenomen die technologiebedrijven daartoe dwingt (Scott, 2018). Maar het is omstreden of en hoe zulke verantwoorde encryptie kan worden gerealiseerd. De Nederlandse regering is hier geen voorstander van (Minister van Veiligheid en Justitie & Minister van Economische Zaken, 2016).

4.5 Digitale ondertekening ter bestrijding van *deep fakes*

In het vorige hoofdstuk is aangegeven dat *machine learning* kan worden ingezet ter bestrijding van *deep fake* manipulatie van beeldmateriaal. Maar deze vorm van desinformatie kan ook worden bestreden met bestaande, relatief eenvoudige technologische middelen. Zo kunnen nieuwsbronnen gebruikmaken van digitale ondertekening van berichten, foto’s en video’s. Digitale ondertekening stelt de lezer

of kijker in staat om de herkomst van berichten – en daarmee de betrouwbaarheid van de berichtgeving – te verifiëren. De technologie is breed toepasbaar. Ook gebruikers die e-mails, berichten op social media of andere digitale documenten te verzenden, kunnen ervan gebruikmaken. Maar op dit moment gebeurt dit slechts op kleine schaal.

Maar net als bij de meeste andere technologieën, staat of valt digitale ondertekening met een correcte implementatie ervan. Zo werden onlangs kwetsbaarheden onthuld in de ondertekening van e-mails in Mozilla Thunderbird (Mozilla, 2019), en bleek de betrouwbaarheid van digitaal getekende PDFs onvoldoende gewaarborgd (Stewart, 2019). Deze methode voorkomt ook niet dat mensen, al dan niet onbewust, onbetrouwbare digitale documenten ondertekenen en daarmee meewerken aan het verspreiden van desinformatie.

Bovendien wordt digitale ondertekening pas een effectief middel tegen de verspreiding van desinformatie als ze op grote schaal wordt toegepast. Overheidsinstanties kunnen hierin het voortouw nemen, door digitale ondertekening te stimuleren of op te leggen. Voor mediabedrijven hanteert de EU momenteel een beleid gebaseerd op zelfregulering. Wanneer dit onvoldoende werkt, kan worden overgestapt op meer dwingende regelgeving (EC Media Convergence and Social Media Unit 1.4, 2019).

4.6 Meer structurele aandacht voor cyberweerbaarheid

De cyberweerbaarheid is er in het bijzonder bij gebaat als op een meer structurele manier wordt voorkomen dat digitale kwetsbaarheden ontstaan. We bespreken hier drie voorbeelden, die divers van aard zijn: SecDevOps, waarbij al in het ontwerpproces aandacht wordt besteed aan het belang van cyberweerbaarheid; veiligere aanvoerketens, waarbij breder wordt gekeken dan de eigen organisatie; en veiligere communicatieprotocollen, die op een basaler niveau de cyberweerbaarheid beogen te verhogen.

4.6.1 SecDevOps voor een integraal ontwerpproces

Goed beveiligde producten en diensten beginnen bij een goed ontwerpproces. Secure Development and Operations (SecDevOps) moeten een integrale aanpak van IT-gerelateerde organisatieprocessen mogelijk maken.[7] Hierbij werken binnen een organisatie de security-afdeling, de developmentafdeling en de operationele

7 Zie https://www.devsecops.org/

afdelingen samen om kwetsbaarheden te verkleinen in de softwareontwikkeling en in de uitrol daarvan (Pal, 2018). De uitrol betreft bijvoorbeeld de manier waarop een leverancier software-updates aanbiedt aan eindgebruikers. Ook die kan kwetsbaarheden bevatten. Zo brachten onderzoekers van Kaspersky Lab onlangs aan het licht dat gebruikers van populaire Asus-apparatuur tot voor kort het risico liepen om via de update-tool van Asus te worden aangevallen (GreAT & AMR, 2019).

SecDevOps richt zich op het automatiseren en integreren van beveiligingsprocessen in het gehele ontwikkelproces, van ontwerp tot implementatie bij de gebruiker. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van technische middelen die proactief code scannen op kwetsbaarheden en signaleren waar in systemen kan worden binnengedrongen (*vulnerability testing en penetration testing*). SecDevOps-technieken kunnen ook worden gebruikt voor een automatische audit van een nieuwe software versie. Zo is Jenkins een onder software ontwikkelaars populair systeem om nieuwe software te schrijven. Hiermee kan automatisch software worden gecontroleerd op de tien meest voorkomende kwetsbaarheden die zijn geïdentificeerd door de Open Web Application Security Project (OWASP) foundation.

Voor een grootschalige toepassing van SecDevOps is het van belang dat dit soort technieken gebruiksklaar wordt aangeleverd. Publieke sectoren zouden het gebruik ervan kunnen afdwingen door het op te nemen in inkoopvoorwaarden.

Bij het ministerie van Defensie staat het werken volgens SecDevOps-methoden al op de radar. Zo heeft het Joint IV Commando (JIVC), dat verantwoordelijk is voor de IT-voorzieningen, de methode opgenomen in het programma Gereedstelling Nieuwe IT, zoals is te lezen in recente vacatures (Werken bij de Overheid, 2019).

4.6.2 Veiligere aanvoerketens

Naarmate organisaties hun eigen beveiliging beter op orde hebben, richten aanvallers hun vizier vaker op toeleveranciers van die organisaties. Organisaties doen er dan ook goed aan breder te kijken dan de eigen cyberweerbaarheid.

Zo kan de aanvoer van nieuwe software worden beveiligd door het installatiebestand te voorzien van een digitaal watermerk (*hash*). Dit is een vorm van digitale ondertekening. Gebruikers kunnen met behulp van zo'n watermerk eenvoudig controleren of het installatiebestand is gemanipuleerd. Softwaredistributiesystemen als Google Play en Apple Appstore voeren dit soort controles automatisch uit.

Ook op het niveau van de hardware zijn controles mogelijk. Zo controleert de T2-chip in Apple's iMac Pro of de computer alleen van vertrouwde software gebruikmaakt gedurende het opstartproces (Apple Support, 2019).

Andere – niet technologische – maatregelen om de cyberweerbaarheid van leveranciers te verhogen liggen op het terrein van certificering, inkoopvoorwaarden en toezicht. Zo stelt het ministerie van Defensie in zijn Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) strenge voorwaarden aan leveranciers.

4.6.3 Veiligere communicatieprotocollen

De technische infrastructuur van het internet bestaat uit diverse technologische 'lagen' (*layers*). Niet alleen in de hogere applicatielagen bevinden zich kwetsbaarheden, maar ook op meer basale niveaus. De meer basale IT-infrastructuur betreft onder andere communicatieprotocollen, zoals verbindingsprotocollen (voor de uitwisseling van data tussen netwerkelementen), netwerkprotocollen (voor de uitwisseling van data tussen bron en bestemming), en applicatieprotocollen (voor de uitwisseling van informatie tussen applicaties). Andere basale elementen betreffen hardware, firmware en operating systems. Doorgaans gebruiken meerdere applicaties dezelfde basale infrastructuur. Technologische innovaties die kwetsbaarheden verhelpen op deze 'diepere' niveaus, kunnen dan ook van grote betekenis zijn voor de verhoging van de cyberweerbaarheid.

Nederlandse kennisinstellingen als TU Delft, UTwente, SURF en TNO werken aan verbeterde communicatieprotocollen. Om deze daadwerkelijk ten goede te laten komen aan de cyberweerbaarheid, dienen ze op grote schaal te worden geïmplementeerd. Maar dat lukt niet altijd, of maar ten dele. Zo bestaat er een veiliger alternatief voor het veelgebruikte Internet Protocol (IP) versie 4, namelijk IP versie 6 (IPv6). Toch is dit nieuwe protocol de afgelopen 10 jaar tot slechts 25% van het wereldwijde web doorgedrongen (Google, 2019).

Ook de nieuwe versie van het IP-protocol bevat overigens kwetsbaarheden. Het protocol functioneert namelijk zo dat de digitale adressen van gebruikers vaak voor alle deelnemers van het internet zichtbaar en bereikbaar zijn. Een alternatief protocol als RINA schermt de digitale adressen juist af, wat de veiligheid ervan ten goede komt. Daarnaast verlangt het IP-protocol van beheerders dat zij zelf maatregelen treffen om belangrijke data te beveiligen. Dat kan anders: een protocol als Named Data Networking (NDN) neemt de beveiliging van data juist als uitgangspunt. Ook het project Scalability, Control and Isolation on Next-Generation

Networks (SCION) verdient vermelding. In dit alternatieve netwerkprotocol vormen belangrijke principes als controle, transparantie en weerbaarheid de basis van de communicatie. Deze alternatieve protocollen bevinden zich nog wel in een experimentele fase.

Het op grote schaal vervangen van een communicatieprotocol door een nieuwere versie blijkt in de praktijk weerbarstig. Dat geldt nog sterker voor de overstap naar een geheel ander communicatieprotocol. Het valt te vergelijken met het invoeren van rechts rijden in het Verenigd Koninkrijk. Het vervangen van een communicatieprotocol kan alleen succesvol worden uitgevoerd als een grote meerderheid van de deelnemers in een netwerk daarmee instemt, of als zowel het oude als het nieuwe systeem gelijktijdig blijven werken. Voor veel reeds in gebruik zijnde apparatuur en software is het echter niet mogelijk om het communicatieprotocol te vervangen. Een volledige, wereldwijde overstap valt dan alleen te bewerkstelligen door deze apparatuur en software in zijn geheel te vervangen.

Vanwege de grote moeite die het kost om veiligere communicatieprotocollen te implementeren, worden wereldwijd op dit vlak maar kleine stapjes gemaakt. De voortgang wordt tevens bemoeilijkt doordat het intergouvernementele overleg over het wereldwijde beheer van het internet is vastgelopen. In 2017 eindigde de bijeenkomst van de VN Group of Governmental Experts (UN-GGE) zonder slotverklaring. Sindsdien zijn wel diverse publiek-private initiatieven ondernomen, zoals het Cyber Security Tech Accord in 2018. Maar wereldwijde voortgang op dit gebied vergt vooral een breed gedeelde, meer concrete normstelling en handhaving (Rathenau Instituut, 2019b)
.

De overstap naar een ander communicatieprotocol kan worden vergemakkelijkt wanneer een grote speler binnen het digitale domein zich daarachter schaart. Zo besloot Google enkele jaren geleden het gebruik van het HTTPS-protocol aan te moedigen. In de browser Chrome wordt tegenwoordig een waarschuwing getoond als gebruikers een website zonder HTTPS bezoeken. In reactie hierop hebben aanbieders van websites besloten om in rap tempo het HTTPS-protocol te implementeren (Sheridan, 2018). In enkele jaren is het gebruik van HTTPS gestegen naar meer dan 90% van alle websites (Google, 2019).

Voor het gebruik van veiligere standaarden als HTTPS en IPv6 geldt in de Nederlandse publieke sector een ‘pas toe of leg uit’-beleid bij de aanschaf van producten of diensten voor een bedrag vanaf 50.000 euro (Forum Standaardisatie, 2019). In de praktijk blijkt hier lang niet altijd gehoor aan te worden gegeven. Zo schiet een groot aantal websites van Nederlandse ziekenhuizen hierin tekort (Van

der Laan, 2019). Experts roepen op tot meer dwingende maatregelen vanuit de overheid om de naleving te bevorderen (Schneier, 2018).

4.7 Opendatastandaarden en *open source software*

Zoals bij het toegenomen gebruik van clouddiensten al ter sprake kwam, gaan eindgebruikers bij de aanschaf van digitale producten of diensten vaak verbanden aan waarvan ze de gevolgen lang niet altijd kunnen overzien. Zo komt het regelmatig voor dat gebruikers worden geconfronteerd met een wijziging van de voorwaarden waaronder een digitale dienst of product door de leverancier wordt aangeboden. Vervolgens moeten zij een afweging maken tussen aanvaarding van de veranderde voorwaarden, of het maken van kosten die gepaard gaan met de overstap naar een andere leverancier. Dit kan ook ten koste gaan van de cyberweerbaarheid, omdat gebruikers niet altijd het best beveiligde product krijgen aangeboden.

Door gebruik te maken van opendatastandaarden en *open source software* kan het voor een gebruiker gemakkelijker worden om naar een andere leverancier over te stappen, omdat in dat geval de kosten daarvan lager zijn. Aanbieders zouden zo ook meer worden gedwongen hun producten en diensten te verbeteren. Er bestaan verschillende gradaties in de mate van openheid, variërend van inzage in de programmatuur tot vrijheid tot het maken van aanpassingen daarin en het verspreiden daarvan. Naarmate de gebruiker meer keuzevrijheid geniet, neemt de afhankelijkheid van een leverancier af.

De Wet hergebruik overheidsinformatie (Who) beoogt het gebruik van opendatastandaarden te bevorderen. Zo is het voor (semi-)overheidsorganisaties verplicht om het Open Document Format (ODF) te gebruiken voor tekstbestanden, in plaats van software-specifieke formats als Docx van Microsoft Word. De door ons geraadpleegde deskundigen merken op dat de wet voor opendatastandaarden niet altijd wordt nageleefd. Het gebruik van *Open source software* wordt binnen de overheid weliswaar gestimuleerd, maar is niet als norm gesteld (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2014).

Niet per definitie veilig
Het gebruik van open standaarden en *open source software* draagt overigens niet vanzelf bij aan een hogere cyberweerbaarheid. Dat liet de *HeartBleed* kwetsbaarheid in 2014 zien. Deze kwetsbaarheid trof 66% van alle wereldwijde webdiensten, maar bleef lange tijd onopgemerkt, hoewel iedereen toegang had tot de broncode van de software en de kwetsbaarheid had kunnen vinden.

Ook kwaadwillende partijen kunnen hierdoor beter zicht krijgen op de kwetsbaarheden die zich daarin voor kunnen doen, en daar hun voordeel mee doen. Veel initiatieven op dit gebied worden daarnaast door vrijwilligers gedragen, die ook het onderhoud ervan verrichten. Een gebrek aan onderhoud kan ten koste kan gaan van de veiligheid. Software en standaarden moeten namelijk continu onderhouden worden, om recent ontdekte kwetsbaarheden te verhelpen.

5 Voorwaarden voor benutten technologische kansen

Dit hoofdstuk beschrijft de voorwaarden die van belang zijn voor het benutten van de kansen die bestaande en nieuwe technologieën bieden om de cyberweerbaarheid te verhogen. De aandacht gaat hierbij vooral uit naar de overheid en naar aanbieders van vitale diensten.

5.1 Cyberweerbaarheid begint met risicoanalyse

Het gebruik van technologische maatregelen ter verhoging van de cyberweerbaarheid veronderstelt een adequate risicoanalyse op bestuursniveau van voor een organisatie kritieke data en processen, die maximale beveiliging behoeven. Op basis van deze risicoanalyse moet ook een afweging plaatsvinden van welke onderdelen en processen van de organisatie met het internet moeten worden verbonden, en welke niet. Daarnaast is speciale aandacht nodig voor grote databestanden met gevoelige gegevens.

Afwegingen horen thuis op bestuursniveau
De afweging over digitalisering van organisatieprocessen en over de noodzaak van verbondenheid met het internet, wordt vaak gezien als een technologisch vraagstuk, dat vooral op de IT-afdeling thuishoort. Maar aan de beslissing om te digitaliseren en op welke manier, moet een risicoanalyse op bestuursniveau vooraf gaan: welke gegevens en processen zijn kritisch voor de organisatie (‘kroonjuwelen’), en moeten maximaal worden beveiligd? Welke risico’s zijn acceptabel? En hoe moeten de voordelen van verbondenheid met het internet worden afgewogen tegen de nadelen ervan?

Toetsingskaders om risico’s in kaart te brengen en informatie over de effectiviteit van maatregelen om risico’s te verminderen, kunnen organisaties helpen bij het maken van deze afwegingen. Vooralsnog ontbreekt het in Nederland aan een breed gedeelde, systematische benadering voor het maken van een adequate risicoafweging (NCTV, 2019a). Rijkswaterstaat heeft hiervoor op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een eigen normenkader ontwikkeld: de Cybersecurity Implementatierichtlijn Objecten Rijkswaterstaat (CSIR) (Algemene Rekenkamer, 2019a).

Kritieke databestanden
Diverse door ons geraadpleegde deskundigen geven aan dat daarnaast meer aandacht moet uitgaan naar kritieke databestanden met gevoelige gegevens, bijvoorbeeld als het gaat om gezondheidsdata of omvangrijke registers met persoonsgegevens. Door grote hoeveelheden data over burgers samen te brengen in een databestand, kan een datalek of hack grote maatschappelijke gevolgen krijgen.

Gevoelige gegevens zouden beter moeten worden beveiligd, bijvoorbeeld door gebruik te maken van sterke vormen van versleuteling of Privacy Enhancing Technologies (PETs). In het geval van medische data pleiten diverse partijen voor de introductie van het ‘patiëntgeheim’. De patiënt moet daarmee meer mogelijkheden krijgen om data niet automatisch te delen met bijvoorbeeld partijen buiten het medisch domein (Hooghiemstra, 2018; Rathenau Instituut, 2019d; Patiëntenfederatie, 2019).

5.2 Voorbeeldfunctie overheid

De overheid verkeert in de positie om een leidende en voorbeeldstellende rol te vervullen op het gebied van cyberweerbaarheid. Als grote afnemer van digitale producten en diensten en als grote dienstverlener kan de overheid grote invloed uitoefenen op het algehele weerbaarheidsniveau. Voorbeelden daarvan zijn het standaard gebruikmaken van multifactor-authenticatie, sterke versleuteling van gevoelige gegevens en Privacy Enhancing Technologies (zie kader 1: Privacy Enhancing Technologies verheffen tot standaard). Ook kan de overheid van publieke nieuwsmedia verlangen dat zij hun berichten digitaal ondertekenen, om het risico van verspreiding van nepnieuws en desinformatie te tegen te gaan.

Cyberweerbaarheid overheid onvoldoende op orde
Er moet nog wel het nodige gebeuren, wil de overheid deze voorbeeldrol kunnen vervullen. Zo constateert de Algemene Rekenkamer in een recent rapport ‘grote problemen’ in de informatiebeveiliging bij meerdere organisaties binnen de Rijksoverheid. Deze organisaties voldoen niet aan alle maatregelen op het gebied van cyberweerbaarheid die voor de Rijksoverheid verplicht zijn gesteld. Het aantal onvolkomenheden is volgens de Rekenkamer zelfs toegenomen ten opzichte van het jaar daarvoor. Dit wordt mede veroorzaakt door een gebrek aan expertise bij ministeries (Algemene Rekenkamer, 2019b).

Om sterker te kunnen sturen op een cyberweerbare overheid en een voorbeeldfunctie van de overheid, lijkt er veel voor te zeggen om de verantwoordelijkheid daarvoor meer bij één partij samen te brengen. Meerdere door

ons geraadpleegde deskundigen zijn van mening dat de verantwoordelijkheden voor cyberweerbaarheid te veel verdeeld zijn over de diverse ministeries. Zij zijn voorstander van meer coördinatie en sturing. Het is de vraag of het recente Coördinatiebesluit, dat meer bevoegdheden op dit gebied bij het ministerie van Binnenlandse Zaken legt, hiervoor toereikend is. Vanuit de behoefte aan meer coördinatie is er in het Verenigd Koninkrijk voor gekozen om de verantwoordelijkheid voor de cyberweerbaarheid van de nationale overheid bij één ministerie te leggen.

Kader 1 Privacy Enhancing Technologies verheffen tot standaard

Voor een brede toepassing van PETs heeft de Rijksoverheid een sleutelpositie, vanwege haar rol in het beheren van dossiers, verstrekken van identiteitspapieren en het digitaal inloggen op overheidsdiensten met DigiD. Bijvoorbeeld het aanbieden van een PET als de KopieID app maakt al verschil. Die stelt gebruikers in staat om onnodige informatie op een kopie van een identiteitsbewijs te verbergen en de kopie te voorzien van een watermerk.

Om een breed gebruik van PETs te bevorderen moeten ze betrouwbaar, transparant en gebruiksvriendelijk zijn, en voldoende bekendheid genieten bij gebruikers.

Anticipatie op nieuwe technologieën

Om een voorbeeldrol te kunnen spelen, moet de overheid ook in voldoende mate anticiperen op de mogelijkheden die nieuwe technologieën bieden om de (eigen) cyberweerbaarheid te verhogen.

Tijdens dit onderzoek bleek het lastig om een duidelijk beeld te krijgen van het bewustzijn dat in de publieke sector – en ook breder: bij aanbieders van vitale diensten – bestaat van de mogelijkheden die nieuwe technologieën bieden. De door ons geraadpleegde deskundigen laten zich daarover vooral in algemene bewoordingen uit. Ze maken zich zorgen over de overheid en over sectoren als de zorg en het onderwijs. De zorgen over de overheid worden mede ingegeven door de kritische bevindingen van de Commissie Elias en het adviesrapport ‘Maak Waar!’ van de Studiegroep Informatiesamenleving en Overheid. Hun inschatting is dat die bevindingen nog steeds relevant zijn, en dat de inzet van nieuwe

technologie ter verhoging van de cyberweerbaarheid in de publieke sector achterblijft.

Maar dit beeld gaat niet op voor alle vitale aanbieders. Volgens de geraadpleegde deskundigen staat cyberweerbaarheid wel hoog op de agenda binnen de financiële, telecom- en energiesectoren en wordt binnen deze sectoren ook gebruikgemaakt van de mogelijkheden die nieuwe technologieën bieden. Deskundigen die in deze sectoren werken zijn zich ook goed bewust van de kansen die bijvoorbeeld *machine learning* bieden om de cyberweerbaarheid te verhogen.

5.3 Wet- en regelgeving

Een tweede manier voor de overheid om het algehele niveau van cyberweerbaarheid te verhogen is door leveranciers te stimuleren om beter beveiligde digitale producten en diensten op de markt te brengen. We bespreken hier drie veelgenoemde instrumenten die de overheid daarvoor ter beschikking staan: wetgeving – bij voorkeur met behulp van op open normen, certificering, en standaardisatie.

5.3.1 Open wettelijke normen en toezicht

Vanwege de snelle technologische ontwikkelingen op het gebied van IT verdient het de voorkeur om bij wet- en regelgeving te werken met ‘open’ wettelijke normen. Zo kent de Wet Beveiliging Netwerken- en Informatiesystemen (Wbni) uit 2018 een zorgplicht toe aan vitale aanbieders en digitale dienstverleners (zoals onlinemarktplaatsen en clouddienstverleners). De wet stelt dat aanbieders ‘passende en evenredige technische en organisatorische maatregelen’ moeten treffen om de opgeslagen of verwerkte gegevens te beveiligen. Het gebruik van open normen voorkomt dat reeds voordat een wet van kracht is geworden, de daarin vastgelegde eisen zijn achterhaald.

Toezicht op open normen
Het gebruik van open normen vereist duidelijke kaders en een adequaat toezicht. Toezichthouders moeten met behulp van richtlijnen nader invulling geven aan de open normen en toezien op naleving ervan. Dat betekent een belangrijke rol voor toezichthouders als het Agentschap Telecom, de Autoriteit Consument en Markt en de Autoriteit Persoonsgegevens. Zij dienen daarvoor ook voldoende te zijn uitgerust, zowel wat menskracht betreft als expertise.

Afstemming toezicht
Omdat digitalisering steeds meer domeinen treft, overschrijden digitale producten en diensten steeds vaker de grenzen van juridische domeinen, waardoor ze onder verschillende toezichthouders kunnen vallen. Richtlijnen voor consumentenproducten, digitale dienstverleners, goederen met een digitaal element, alsook sectorspecifieke wetgeving, kunnen in één product, zoals een auto of 'lifestyle app', samenkomen. Adequaat toezicht op zulke producten vraagt om samenwerking en afstemming van toezichthouders, zowel binnen nationaal als internationaal verband. Een van de vragen die hierbij speelt, is welke instantie autoriteit heeft op welk deelgebied. Dat vraagt ook om onderzoek naar de mogelijkheden van (inter)nationale afstemming en samenwerking. Binnen de Nationale Cyber Security Research Agenda vormt onderzoek naar governance-vragen een van de aandachtsgebieden. Ook het Europese onderzoeksproject CyberSec4Europe richt zich op dat soort vragen (DG CONNECT, 2019a).

De internationale consumentenorganisaties Consumers International en BEUC uiten kritiek op de manier waarop de toezichthouders in de EU-lidstaten invulling geven aan de bescherming van de consument in het digitale domein. Volgens hen besteden de toezichthouders te weinig aandacht aan privacybescherming en informatiebeveiliging, en is hun aanpak vaak te gefragmenteerd (Coll & Simpson, 2016). Toezichthouders zouden op een meer integrale manier moeten kijken naar de bescherming van digitale consumentenrechten, met ook aandacht voor zaken als rechtvaardigheid en eerlijke machtsverhoudingen (Consumers International et al., 2017).

5.3.2 Certificering

Certificering is een tweede instrument waarmee de overheid leveranciers kan stimuleren om beter beveiligde digitale producten en diensten op de markt te brengen. Afnemers kunnen daarmee nagaan of digitale diensten en producten aan bepaalde minimumeisen voldoen.

In 2018 is de Europese Cybersecurity Act aangenomen. Deze voorziet in een Cybersecurity Certificates Framework voor digitale producten en diensten. Het is de verwachting dat het van ontwikkelaars van IoT-apparatuur zal vragen om het principe van security-by-design toe te passen. De certificering zal worden uitgevoerd op vrijwillige basis en kent drie niveaus: basaal, substantieel en hoog. Het Framework moet nog worden geïmplementeerd in nationale wet- en regelgeving. Het is daarom nog onduidelijk hoe de Europese Cybersecurity Act precies zal uitwerken. Er is door de EU gekozen voor vrijwillige certificering om hogere kosten voor markttoegang te voorkomen (Stupp, 2018a).

Consumentenorganisaties hebben hierover hun teleurstelling geuit (Stupp, 2018b). Ook meerdere door ons geraadpleegde deskundigen geven het belang aan van een verplichte certificering.

Een tweede aanknopingspunt voor certificering in het digitale domein is de Europese richtlijn voor radioapparatuur, die in 2017 is herzien. De richtlijn regelt het CE-keurmerk. De hieraan verbonden voorschriften regelen zaken als gebruiksveiligheid, het voorkomen van interferentie en storingsgevoeligheid. Nederland wil zich in EU-verband inzetten om via deze richtlijn ook minimale veiligheidseisen te stellen aan IoT-apparatuur (Ministerie van EZK, 2018).

Bewezen veilig?
Er moet wel een belangrijke kanttekening worden geplaatst bij het gebruik van certificering voor leveranciers van digitale producten en diensten. Vooralsnog is het immers niet mogelijk om de veiligheid van producten en diensten onomstotelijk aan te tonen (*provable secure*). In plaats daarvan kunnen leveranciers en gebruikers gebruikmaken van contractuele afspraken, kunnen tests worden uitgevoerd en kunnen leveranciers inzicht bieden in de door hen gebruikte programmatuur. Onderzoek naar de mogelijkheden om de veiligheid van producten en diensten aan te tonen zijn vooralsnog een academische aangelegenheid. Dit maakt ook deel uit van de National Cyber Security Research Agenda (Dcypher, 2018).

In de cryptografie is het wel mogelijk dat ontwikkelaars wiskundig bewijs leveren voor de veiligheid van hun versleuteling. Van de versleutelingstechniek RSA – die de basis vormt voor het ‘groene slotje’ in de browser – is bijvoorbeeld bekend op welk wiskundig principe de versleuteling is gebaseerd. De mate van informatiebeveiliging die het RSA-algoritme claimt te bieden, kan dus onafhankelijk worden gecontroleerd.

5.3.3 Internationale standaardisatie

Een derde instrument waarmee de overheid leveranciers kan bewegen om beter beveiligde digitale producten en diensten op de markt te brengen, is door middel van (internationale) standaardisatie. Standaarden zijn van groot belang voor internationale maatregelen op het gebied van cyberweerbaarheid.

Marktpartijen aan het roer
Tot nog toe komen standaarden in het digitale domein vooral vanuit de markt tot stand, zonder dat daaraan een formeel standaardisatieproces vooraf is gegaan. Zo zijn communicatieprotocollen zoals HTTP en IP in het verleden vooral door hun populariteit in het gebruik tot standaard uitgegroeid. Daar waar wel sprake is van

een standaardisatieproces, hebben grote technologiebedrijven doorgaans een dikke vinger in de pap. Zij beschikken vaak over de benodigde expertise om technisch-inhoudelijke bijdragen te leveren en zijn ook bereid de benodigde menskracht in te zetten om de bijeenkomsten bij te wonen en daarmee invloed uit te oefenen op het standaardisatieproces. Overheden blijven daar over het algemeen bij achter.

Er bestaan weliswaar internationale beleidsfora, zoals Internet Corporation for Assigned Names and Numbers (ICANN), Internet Governance Forum (IGF), International Telecommunication UnionI (ITU) en Internet Society (ISOC), maar deze hebben vooralsnog niet of nauwelijks zeggenschap over de globale internetinfrastructuur (Van Eeten, 2017).

Internationale rol overheden
Lange tijd werd het ook als onhaalbaar gezien om internationaal beleid te voeren op het gebied van cyberweerbaarheid. Dat werd mogelijk ingegeven door het feit dat het hierbij al snel om duizenden partijen gaat, die in vele landen actief zijn. Met de recente opkomst van een beperkt aantal dominante spelers, zoals clouddiensten en platformbedrijven, die een groot deel van de internationale markt bedienen, is een situatie ontstaan waarin internationale beleidsmaatregelen meer effect zouden kunnen hebben.

De prijsvraag van het Amerikaanse NIST, gericht op het ontwikkelen van een standaard voor post-kwantumcryptografie, laat ook zien dat overheden wel degelijk een internationale rol van betekenis kunnen spelen. Dat blijkt ook uit de wereldwijde werking die uitgaat van de Algemene Verordening Gegevensbescherming van de Europese Unie (AVG, of: General Data Protection Regulation (GDPR). Gezien het grote belang van de internationale fora waarin wordt beslist over internationale richtlijnen en standaarden, zou de Nederlandse overheid – of nog beter: de EU – zich daar nadrukkelijker in moeten mengen. Dat moet er tevens toe leiden dat die richtlijnen en standaarden voldoende recht doen aan belangrijke Europese waarden als veiligheid, privacy en autonomie.

Ook een relatief klein land als Nederland kan overigens invloed uitoefenen op internationale standaarden. Zo is Nederland marktleider op het gebied van laadpalen voor elektrische auto’s. Hiermee heeft het invloed op keuzes die wereldwijd doorwerken. Zo heeft het autoconcern Tesla zich aangepast aan de laadpalen van het Nederlandse FastNed, door adapters te leveren waarmee de Tesla ook in Nederland gemakkelijk kan worden opgeladen (De Jong, 2019). Alhoewel dit voorbeeld niet gaat over cyberweerbaarheid, laat het wel zien dat een klein land door voorop te lopen in ontwikkelingen en een bepaalde standaard te introduceren, internationaal navolging kan krijgen.

5.4 Versterken van digitale autonomie

In dit onderzoek hebben we gezien dat er een trend gaande is waarbij steeds meer diensten door cloudleveranciers worden aangeboden. Dat kan leiden tot een verhoging van de cyberweerbaarheid, omdat clouddienstverleners doorgaans meer kennis en capaciteit in huis hebben om systemen te beveiligen dan gebruikers. Maar, zoals we zagen, kan dat ook leiden tot een groeiende afhankelijkheid van cloudleveranciers en tot de daarmee gepaard gaande risico's als uitval van functionaliteit bij verstoring, en verlies van controle en zeggenschap over data en dataverwerking.

De door ons geraadpleegde deskundigen delen de mening dat deze afhankelijkheidsrisico's ongewenst zijn. Maar ze verschillen van mening over de mogelijkheden om deze afhankelijkheid te verkleinen – en dat betekent ook: de digitale autonomie van gebruikers te vergroten. Een aantal van hen vindt dat Nederland – en breder gezien: Europa – te weinig inzet op de ontwikkeling van eigen IT-bedrijvigheid. Kansrijke Nederlandse of Europese startups worden te vaak door grote buitenlandse technologiebedrijven opgekocht en te gelde gemaakt, wat de afhankelijkheid van die bedrijven alleen maar verder vergroot. Door sterker in te zetten op eigen bedrijvigheid en innovatie zou de afhankelijkheid van externe partijen kunnen worden verminderd. Die bedrijvigheid en innovatie kunnen overigens ook afkomstig zijn van 'sociale ondernemingen', non-profitorganisaties of publieke IT-dienstverleners.

Anderen zijn van mening dat de bijdragen van Nederlandse of Europese leveranciers van digitale producten en diensten op het gebied van cyberweerbaarheid zich niet zullen kunnen meten met de maatregelen van grote technologiebedrijven, die wereldwijd vooroplopen in R&D. Zie ook de uitspraak van Jeff Moss, oprichter van de hackersconferentie Black Hat, dat er wellicht twintig bedrijven in staat zijn om een substantiële bijdrage te leveren aan het wereldwijd vergroten van de cyberweerbaarheid (Sheridan, 2018). Ongewenste afhankelijkheid zou dan ook beter kunnen worden tegengegaan door nationaal of in EU-verband hogere eisen te stellen, gekoppeld aan inkoopvoorwaarden, aan de betrouwbaarheid en continuïteit van de dienstverlening.

Een derde mogelijkheid om ongewenste afhankelijkheid tegen te gaan en digitale autonomie te vergroten, bestaat uit het gebruik van technische maatregelen als PETs, encryptie en open standaarden en *open source software*. Met de eerste twee maatregelen kan ongewenste verspreiding en ongewenst hergebruik van data worden voorkomen; met de laatste twee kan een al te sterke afhankelijkheid van één cloudleverancier worden verminderd.

De diverse opties hoeven elkaar overigens niet uit te sluiten. Het streven naar meer IT-bedrijvigheid in Nederland of Europa en een betere bescherming daarvan tegen overnames, kunnen samengaan met het stellen van hogere veiligheidseisen – zoals het standaard gebruik van PETs en encryptie – als inkoopvoorwaarde.

5.4.1 Digitale autonomie versterken met technische maatregelen

Het gebruik van technische maatregelen als Privacy Enhancing Technologies en encryptie kan de verspreiding en het (her)gebruik van data door andere partijen voorkomen, en daarmee bijdragen aan behoud van controle en zeggenschap over data en dataverwerking. Daarnaast kan het gebruik van open standaarden en *open source software* bijdragen aan het tegengaan van ongewenste afhankelijkheid van een cloudleverancier en het risico van vendor lock-in, omdat het voor de eindgebruiker gemakkelijker worden om naar een andere leverancier over te stappen.

Het gebruik van PETs, encryptie en *open source software* zijn voor de hand liggende mogelijkheden om de digitale autonomie van de gebruiker te versterken, omdat het reeds bestaande, maar onderbenutte mogelijkheden betreft.

De door ons geraadpleegde experts verschillen wel van mening over de noodzaak om uit oogpunt van cyberweerbaarheid – bijvoorbeeld – de data van de Rijksoverheid op te slaan in datacentra binnen de eigen landsgrenzen. Terwijl sommigen van mening zijn dat daardoor meer controle kan worden uitgeoefend op de veiligheid en betrouwbaarheid van de dataopslag, zijn anderen van mening dat het weinig uitmaakt waar data worden opgeslagen, zolang deze maar zwaar genoeg zijn versleuteld.

Voor dit laatste is het wel van belang dat die versleuteling maximaal kan worden vertrouwd, en dat wil zeggen: door vertrouwde partijen wordt ontwikkeld en geïmplementeerd. Dit is in elk geval nodig voor de beveiliging van kritieke data van overheid en bedrijfsleven, zoals staatsgeheime informatie, of de ‘kroonjuwelen’ van bedrijven.

5.4.2 Digitale autonomie versterken met strengere inkoopvoorwaarden

Een tweede optie om de ongewenste effecten van de afhankelijkheid van buitenlandse partijen tegen te gaan en digitale autonomie te vergroten, is strengere

eisen stellen in de inkoopvoorwaarden op het gebied van cyberweerbaarheid en controle en zeggenschap over data en dataverwerking. Zo kunnen Nederlandse en Europese partijen van clouddienstverleners verlangen dat opgeslagen data niet door de leverancier of door derde partijen kunnen worden ingezien, bijvoorbeeld door data standaard te versleutelen. Het ministerie van Defensie stelt al langer specifieke voorwaarden aan leveranciers, onder andere op het gebied van cyberweerbaarheid (zie kader 2: ABDO inkoopvoorwaarden IT-leveranciers).

Kader 2 ABDO inkoopvoorwaarden IT-leveranciers

Leveranciers van het ministerie van Defensie moeten voldoen aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO). Het Te Beschermen Belang (TBB) speelt hierbij een belangrijke rol. Het kent vier niveaus, die gerelateerd zijn aan de mogelijke schade die het gevolg is van kennisname door niet-gerechtigde partijen. Afhankelijk van het TBB-niveau worden andere eisen gesteld aan de leverancier.

Sinds 2017 is in de ABDO een hoofdstuk gewijd aan IT-beveiliging. De hierin opgenomen eisen hebben betrekking op organisatorische maatregelen, zoals het aanstellen van een cyberbeveiligingsfunctionaris, en technische maatregelen, bijvoorbeeld op het gebied van encryptie en cloudcomputing. De eisen zijn concreet en lezen als een checklist.

De ABDO-voorwaarden vormen volgens diverse door ons geraadpleegde deskundigen een goed voorbeeld van het stellen van strengere voorwaarden aan leveranciers van digitale producten en diensten. Maar anderen vragen zich af of alle ABDO-voorwaarden wel leiden tot de hoogst mogelijke weerbaarheid (Olsthoorn, 2017). De ABDO vereist bijvoorbeeld dat opdrachtnemers uitsluitend medewerkers met de Nederlandse nationaliteit op vertrouwensfuncties plaatsen. Die voorwaarde is alleen zinvol als er voldoende Nederlanders voorhanden zijn die beschikken over de voor de functie benodigde kwaliteiten.

Volgens diverse door ons geraadpleegde deskundigen moeten de Rijksoverheid en de aanbieders van vitale diensten een leidende rol spelen bij het stellen van strengere eisen aan cyberweerbaarheid. Daartoe zouden ze hun krachten moeten bundelen en gezamenlijk inkoopvoorwaarden moeten opstellen. Anderen wijzen erop op dat met het oog op de benodigde marktmacht, inkoopwaarden beter op Europees niveau kunnen worden afgestemd. De European Union Agency for

Cybersecurity (ENISA) heeft ook richtlijnen opgesteld voor inkoopbeleid (ENISA, 2014).

Inkoopvoorwaarden 5G
In Nederland bestaat toenemende aandacht voor de gevolgen van het aan te leggen 5G-netwerk voor de cyberweerbaarheid. De Taskforce Economische Veiligheid van de NCTV heeft hierover onlangs een advies uitgebracht, dat door de regering in juli 2019 is overgenomen. Telecomaanbieders worden hierdoor verplicht aanvullende beveiligingsmaatregelen te nemen om hun netwerk te beschermen, waaronder het stellen van extra hoge eisen aan leveranciers van diensten en producten in de kritieke onderdelen (Ministerie van Justitie en Veiligheid, 2019). Welke onderdelen dat betreft is niet bekend (Hijink, 2019).

Deze gang van zaken is in lijn met het Europese beleid op het gebied van 5G-netwerken, dat aanstuurt op aanvullende voorwaarden op het gebied van cyberweerbaarheid. Dit beleid wijkt af van het door de Verenigde Staten voorgestane beleid om leveranciers uit landen met een ‘offensief’ cyberprogramma te weren. Behalve de Verenigde Staten, hebben Australië, Nieuw Zeeland en Japan besloten om vanwege die reden de Chinese leverancier Huawei te weren (Tao, 2018). Wat de aanvullende voorwaarden die de EU voorstaat behelzen, is op dit moment nog niet duidelijk.

In Duitsland heeft een vergelijkbare discussie plaatsgevonden. Dat heeft er begin 2019 toe geleid dat strengere eisen worden gesteld aan bedrijven die willen meedingen naar de 5G-frequentieveiling (Bundesnetzagentur, 2019). De eisen zijn opgesteld door de Duitse toezichthouders voor telecommunicatie en dataprotectie. De eisen behelzen onder andere het certificeren van kritieke componenten door het Duitse BSI, periodieke beveiligingstesten en het voorkomen van ‘monoculturen’.[8]

Op Europees niveau is een voorstel ontwikkeld voor afstemming van nationale inkoopvoorwaarden. In maart 2019 heeft de Europese Commissie voorgesteld om te komen tot een gezamenlijke Europese benadering voor de beveiliging van 5G-netwerken (European Commission, 2019a).

5.4.3 Digitale autonomie versterken met eigen IT-bedrijvigheid

Een derde optie om te ontsnappen aan een al te grote afhankelijkheid van grote buitenlandse partijen, is door binnen Nederland en Europa meer eigen IT-

8 Voor de complete lijst met eisen, zie https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190307_SL.html

bedrijvigheid te ontwikkelen. Dat veronderstelt wel dat binnen Nederland en Europa de ontwikkeling van IT-bedrijvigheid, en in het bijzonder de ontwikkeling en implementatie van nieuwe technologieën die de cyberweerbaarheid verhogen, meer als speerpunt moet worden gezien. Zoals hierboven al opgemerkt, kan die bedrijvigheid behalve van private ondernemingen, ook afkomstig zijn van onder andere non-profitorganisaties of publieke IT-dienstverleners.

Nederland is hiervoor op zich genomen niet te klein – zoals nogal eens wordt beweerd. Zeker niet wanneer deze rol wordt gezien binnen de context van grotere samenwerkingsverbanden als de NAVO of de EU. Het feit dat een nog kleiner land als Estland binnen de NAVO een eigen rol kan spelen op het gebied van cyberweerbaarheid, laat zien dat omvang van een land niet allesbepalend is. De door ons geraadpleegde deskundigen wijzen er wel op dat Estland zich in een bijzondere situatie bevindt. De continue dreiging en ervaring met (Russische) cyberaanvallen in Estland wordt vaak genoemd als een bepalende factor. Dit heeft geleid tot een hoog gevoel van urgentie om aan cyberweerbaarheid te werken, die breed wordt gedeeld.

Focus in kennis- en innovatieagenda

Om meer eigen IT-bedrijvigheid te ontwikkelen – die primair gericht is op verhoging van de cyberweerbaarheid – is een daadkrachtiger kennis- en innovatiebeleid nodig. De Nederlandse regering heeft daartoe met de Kennis en Innovatieagenda 2020-2023 een aanzet gegeven. De missie cyberveiligheid vormt hierbinnen één van de 25 missies (Ministerie van Economische Zaken en Klimaat, 2019). De Nederlandse Cyber Security Research Agenda (NCSRA) heeft hiervoor een belangrijke inhoudelijke leidraad gevormd.

De door ons geraadpleegde deskundigen zijn evenwel van mening dat het bij de NCSRA ontbreekt aan voldoende focus om werkelijk verschil te kunnen maken. De overheid zou gerichter moeten kiezen op welke (deel)gebieden de Nederlandse kennisinstellingen internationaal voorop moeten lopen, om vervolgens de verworven kennis te vermarkten.

Ook het innovatiebeleid is gediend bij meer focus. In Nederland is de financiering van innovatie vooral generiek van aard. Al jaren wordt circa 90% van de innovatiebestedingen uitgegeven in de vorm van generieke fiscale steun (Rathenau, 2018). Een van de weinige niet-fiscale instrumenten, de Small Business Innovation Research (SBIR), biedt mogelijkheden om meer focus aan te brengen. Maar vooralsnog wordt dit instrument over de volle breedte van de NCSRA ingezet (zie kader 3: SBIR Cyber Security stimuleert IT-bedrijvigheid over volle breedte NCSRA).

Kader 3 SBIR Cyber Security stimuleert IT-bedrijvigheid over volle breedte NCSRA

Het Small Business Innovation Research Cyber Security programma stelt subsidie beschikbaar voor onderzoek naar de haalbaarheid en ontwikkeling van innovaties (RVO, 2017). 90% van het budget wordt gefinancierd door het Fonds voor interne veiligheid van de Europese Unie (ISF); 10% door een bijdrage van de NCTV.

De NCSRA vormt de leidraad voor de SBIR. Via een aanbestedingsprocedure worden ondernemers opgeroepen bij te dragen aan het realiseren van de hoofddoelen van het overheidsbeleid op het gebied van cyberweerbaarheid. Deze hoofddoelen zijn breed geformuleerd.

Uit een analyse van 43 geselecteerde projectvoorstellen blijkt dat ook een breed scala aan initiatieven financiering krijgt. Ongeveer de helft van de voorstellen is gericht op een technische vorm van informatie- of netwerkbeveiliging, en betreft bijvoorbeeld een authenticatietechniek, app of cloudtechnologie. Daarnaast richt ongeveer een derde van de projectvoorstellen zich op het ontwikkelen van managementinstrumenten. Deze vergaren bijvoorbeeld informatie over data, netwerken en kwetsbaarheden, en maken die vervolgens inzichtelijk. De resterende voorstellen betreft hoofdzakelijk trainings- en bewustwordingsprojecten.

De SBIR-beoordelingscommissie hanteert impact, technologische haalbaarheid, economisch perspectief en prijs van de offerte als criteria. Daaruit spreekt geen voorkeur voor een bepaalde technologie of voor een bepaalde verdeling tussen technologische en meer organisatorische voorstellen.

Het bovenstaande roept de vraag op welke precieze ambities de Nederlandse regering heeft met haar kennis- en innovatiebeleid op het gebied van cyberweerbaarheid.

Overheid als launching customer
Ter stimulering van de eigen IT-bedrijvigheid kan de overheid daarnaast fungeren als *launching customer*. Dit betekent dat de overheid als risicodrager financieel investeert in beloftevolle startups, sociale ondernemingen en non-profitorganisaties; en als grote afnemer succesvolle digitale producten en diensten afneemt en daarmee bijdraagt aan de opschaling van de innovatieve ondernemer of organisatie. Ook aanbieders van vitale diensten zouden zich meer kunnen opstellen als launching customer.

Hierbij moet in acht worden genomen dat de IT-sector wordt gekenmerkt door relatief veel startups en mkb-bedrijven. Om innovaties te bevorderen en daar de vruchten van te kunnen plukken, is het belangrijk gunstige voorwaarden te scheppen voor innovatieve organisaties. Dat vergt onder andere aandacht voor aanbestedingsprocedures. Volgens een aantal door ons geraadpleegde deskundigen houden aanbestedingsprocedures vaak te weinig rekening met start-ups. Aanbestedingen zouden voor hen veelal te groot en te complex zijn, waardoor vooral grotere partijen zich hiervoor kwalificeren.

Om innovatie te bevorderen zou de overheid dan ook meer ruimte moeten creëren voor kleine ondernemingen en non-profitorganisaties. Dat vormt ook een van de doelstellingen van de nog op te richten Cyber Innovation Hub, waarin ministeries, kennisinstellingen en bedrijven samenwerken aan vraagstukken op het gebied van cyberweerbaarheid (Rathenau Instituut, 2019a).

Naast de reguliere overheidspartijen is er ook een mogelijke rol weggelegd voor de inlichtingendiensten. Samenwerking tussen kleine, startende ondernemingen en de inlichtingen- en veiligheidsdiensten komt in Nederland weinig voor. Dit komt doordat producten, medewerkers en de onderneming een strenge screening moeten ondergaan alvorens zij in het geheime domein mogen opereren. In de praktijk zijn kleine ondernemingen zelden in staat om die procedures te doorlopen.

DARPA als voorbeeld
In het licht van de hier genoemde innovatievoorwaarden, maakt het Amerikaanse militaire innovatieagentschap DARPA gebruik van een interessante vorm van samenwerking met technologieontwikkelaars. Zo is DARPA als launching customer al in een vroeg stadium betrokken bij het proces van kennisontwikkeling naar innovatie. DARPA legt in deze fase ook geen screeningsvoorwaarden op aan de partijen waarmee het samenwerkt. De samenwerking vindt buiten het geheime domein plaats. Daarvoor zijn geavanceerde simulatieomgevingen ontwikkeld (DARPA, 2008).

In 2018 besloot Duitsland een organisatie op te richten met een soortgelijke missie als DARPA (Delcker, 2018). Volgens de Duitse regering moet deze organisatie er toe leiden dat Duitsland minder afhankelijk wordt van buitenlandse leveranciers. Het budget van 200 miljoen euro voor een periode van vijf jaar staat echter nog in schril contrast met het jaarlijkse budget van nagenoeg 3 miljard euro van DARPA.

Waardengedreven innovatie
Een bijkomend, maar niet onbelangrijk argument voor het ontwikkelen van een eigen Nederlandse of Europese positie op de wereldwijde IT-markt, is de leidende positie van de Europese Unie als het gaat om normatief geladen regulering van IT-ontwikkelingen. Zie ook de wereldwijde werking die de GDPR heeft gekregen. Die normatieve kracht kan de Europese Unie uitbouwen, door zwaarder in te zetten op de ontwikkeling van IT-gerelateerde producten en diensten waarin recht wordt gedaan aan waarden als veiligheid, privacy en autonomie (Dobbe & Stikker, 2019). Daarmee kan het Europese bedrijfsleven zich onderscheiden van het Amerikaanse, Chinese en Russische bedrijfsleven.

5.5 Post-kwantumcryptografie biedt kansen op IT-bedrijvigheid

Vanuit Nederland doen meerdere partijen mee aan de NIST-prijsvraag die is gericht op het vaststellen van een internationale standaard voor post-kwantumcryptografie. Met onder andere de Radboud Universiteit, CWI Amsterdam, TU Eindhoven en Philips beschikt Nederland op dit gebied over een stevige kennisbasis.

Deze internationaal vooraanstaande, Nederlandse kennispositie biedt kansen om op het gebied van post-kwantumcryptografie eigen IT-bedrijvigheid te ontwikkelen. Met behulp van de expertise van Nederlandse kennisinstellingen kunnen producten en diensten worden ontwikkeld die de toekomstige, grootschalige migratie naar kwantumbestendige versleuteling kunnen ondersteunen.

In andere landen wordt hierop reeds ingezet, zoals blijkt uit de activiteiten van het Britse bedrijf PQShield, en de ondersteuning die het van de Britse overheid krijgt. Vooruitlopend op de migratie naar post-kwantumcryptografie bereidt deze onderneming zich voor op de ontwikkeling van producten, onder andere door experts aan zich te binden. In Nederland is van een dergelijke inzet nog geen sprake.

5.6 Benutten kansen post-kwantumcryptografie en *machine learning*

Het bovenstaande roept de vraag op wat er nodig is om de kansen die nieuwe technologieën bieden, te kunnen benutten. Wat vraagt dat van betrokken overheden, bedrijven en kennisinstellingen? We kijken daarbij vooral naar post-kwantumcryptografie en *machine learning*, en naar de Rijksoverheid en aanbieders van vitale diensten.

Omgang met technologische innovatie
Bedacht moet worden dat weliswaar op beperkte schaal reeds toepassingen beschikbaar zijn van *machine learning* en post-kwantumcryptografie, maar dat voor beide geldt dat de technologie nog volop in ontwikkeling is. Wat post-kwantumcryptografie betreft, is hiervoor de reeds genoemde prijsvraag van het NIST van belang, die gericht is op het ontwikkelen van cryptografiestandaarden. Omdat de toepassingen ervan nog volop in ontwikkeling zijn, is het nu niet mogelijk aan te geven hoe deze precies vorm zullen krijgen, en wat er in concrete praktijksituaties nodig is om ze adequaat te kunnen implementeren.

Wel kan het een en ander worden gezegd over de wijze waarop organisaties anticiperen op zich ontwikkelende technologische mogelijkheden en daarvan gebruikmaken. Uit dit onderzoek komt naar voren dat er grote verschillen bestaan in de omgang van vitale aanbieders met technologische innovaties. Grote organisaties die beschikken over een eigen onderzoeksafdeling zijn in de gelegenheid om verder vooruit te kijken naar toekomstige technologische ontwikkelingen, en in samenwerking met kennisinstellingen te werken aan de ontwikkeling van innovatieve oplossingen voor vraagstukken op het gebied van cyberweerbaarheid. Het gaat hierbij bijvoorbeeld om het voorkomen van vervuiling of bias in de datasets waarmee slimme algoritmes worden getraind. De toepassingen die hieruit voortvloeien dienen vervolgens nog wel binnen de eigen organisatie te worden geïmplementeerd.

Voor de samenwerking met kennisinstellingen is het hierbij nodig dat de organisatie in kwestie voldoende zicht heeft op waar nieuwe kennis en producten worden ontwikkeld; daarvoor de benodigde expertise in huis heeft; en intern over experimenteerruime beschikt. Voor de externe deskundigen waarmee wordt samengewerkt is het van belang dat zij de organisatie voldoende kennen en de vraagstukken waarvoor die zich gesteld ziet. Dat geldt bijvoorbeeld voor een organisatie als de AIVD, die in samenwerking met (Nederlandse) kennisinstellingen de mogelijkheden onderzoekt van het gebruik van *machine learning* voor detectiedoeleinden. De samenwerking kan baat hebben bij een geografische en culturele ‘nabijheid’ van de organisatie met de kennisinstellingen (Boschma, 2005;

Rathenau Instituut, 2018a). Maar deze nabijheid lijkt voor samenwerking geen noodzakelijke voorwaarde.

Maar niet alle aanbieders van vitale diensten beschikken over eigen onderzoekscapaciteit. Ze zijn voor innovatieve producten of diensten aangewezen op het aanbod van marktpartijen. Zij hebben vooral behoefte aan expertise waarmee ze het marktaanbod op waarde kunnen schatten, inclusief de vraag of de producten en diensten daadwerkelijk een oplossing bieden voor de weerbaarheidsvraagstukken waarmee zij op dat moment te maken hebben, of naar verwachting in de nabije toekomst mee te maken zullen krijgen. Omdat voor de aanschaf van de benodigde producten en diensten een aanbestedingsplicht geldt, worden deze uit het wereldwijde marktaanbod betrokken. Grote, internationale leveranciers van digitale producten en diensten kunnen daarbij overigens ook voorzien in lokale ondersteuning.

Ondersteuning door de overheid
De overheid kan op diverse manieren de toepassing van nieuwe technologieën als *machine learning* en post-kwantumcryptografie ondersteunen. In de eerste plaats is het nodig te blijven investeren in de kennisontwikkeling binnen kennisinstellingen op het gebied van *machine learning* en post-kwantumcryptografie. Daarnaast moet samenwerking tussen kennisinstellingen en organisaties waar mogelijk worden gefaciliteerd. Organisaties die niet over eigen onderzoekscapaciteit beschikken, moeten desgewenst inhoudelijk worden ondersteund bij de beoordeling van een passend marktaanbod. De bestaande Information Sharing and Analysis Centres (voor vitale aanbieders) en het Digital Trust Center (voor niet-vitale aanbieders) kunnen daarvoor worden gebruikt.

Helderheid over wettelijke kaders
Zoals in Hoofdstuk 3 is aangegeven, is het de vraag of het gebruik van *machine learning* voor het automatisch herstellen van kwetsbaarheden en voor een automatische respons op aanvallen verenigbaar is met de Softwarerichtlijn, respectievelijk de wettelijke bepalingen op het gebied van computervredebreuk. De overheid doet er dan ook goed aan daar helderheid over te verschaffen.

5.7 Succesvolle inzet van nieuwe technologie vergt beschikbare expertise

Misschien wel de belangrijkste voorwaarde voor het benutten van de kansen die bestaande en nieuwe technologieën bieden voor de verhoging van cyberweerbaarheid is het kunnen beschikken over voldoende expertise. Dat geldt voor de volle breedte van het spectrum: voor de ontwikkeling en implementatie van

deze technologieën moeten overheden, aanbieders van vitale diensten, overige bedrijven en toezichthouders over voldoende menskracht en expertise beschikken.

Maar er bestaan grote zorgen over een gebrek aan expertise. Meerdere door ons geraadpleegde deskundigen wijzen op een groot en aanhoudend tekort in Nederland aan deskundigen op het gebied van cyberweerbaarheid. Volgens de internationale beroepsvereniging ISACA kampte in 2018 de helft van de cybersecurity-organisaties met een tekort (ISACA, 2018). Volgens beroepsvereniging ISC2 bestaat dit tekort wereldwijd uit 3 miljoen professionals (ISC2, 2018). Nederlandse bedrijven beschouwen het gebrek aan expertise ook als een grote belemmering voor het gebruik van *machine learning* (AINED, 2018).

Vanwege dit tekort aan experts, is het dan ook nodig meer te investeren in IT-opleidingen, zowel op mbo-, hbo- als universitair niveau. Eerder heeft de Cyber Security Raad al opgeroepen om meer IT-professionals op te leiden (Broekhuizen, 2018).

6 Conclusies

Op basis van de in de voorafgaande hoofdstukken beschreven bevindingen, komen we tot de volgende conclusies.

6.1 Kansen van nieuwe technologie

Nieuwe technologieën bieden kansen om cyberweerbaarheid te verhogen
Machine learning, post-kwantumcryptografie, 5G-netwerken, LiFi, kwantumcommunicatie en gedistribueerde systemen zijn nieuwe technologieën die kansen bieden om de cyberweerbaarheid van Nederland te verhogen. Met *machine learning* wordt het mogelijk om op grote schaal en automatisch kwetsbaarheden in software op te sporen en te herstellen. Ook kan *machine learning* worden ingezet ter bestrijding van *deep fake* manipulatie van beeldmateriaal. Post-kwantumcryptografie maakt een dusdanig sterke versleuteling van data mogelijk dat deze bestand zijn tegen aanvallen waarbij gebruik wordt gemaakt van de rekenkracht van een kwantumcomputer. 5G-netwerken bieden de mogelijkheid om communicatienetwerken beter te beveiligen. Daarnaast maken LiFi en kwantumcommunicatie veiligere vormen van digitale communicatie mogelijk, die moeilijker zijn af te luisteren. Ten slotte kan met behulp van gedistribueerde systemen de weerbaarheid worden verhoogd tegen uitval van functionaliteit bij verstoring. De genoemde technologieën zijn nog wel in ontwikkeling en kennen nog maar beperkt toepassing.

***Machine learning* en post-kwantumcryptografie: kans én noodzaak**
Nieuwe technologieën zoals automatische detectie en herstel van kwetsbaarheden of het gebruik van post-kwantumcryptografie bieden niet alleen kansen om de cyberweerbaarheid te verhogen. Gebruik ervan is ook een noodzaak, wil de cyberweerbaarheid van Nederland gelijke tred houden met de mogelijkheden van kwaadwillende partijen om op hun beurt gebruik te maken van nieuwe technologieën.

De ontwikkelingen op het gebied van kwantumcomputing brengen die noodzaak het duidelijkst naar voren: voordat de kwantumcomputer het mogelijk maakt om bestaande vormen van cryptografie te breken, zal een grootschalige migratie naar post-kwantumcryptografie moeten hebben plaatsgevonden. Een vergelijkbaar verhaal geldt voor de inzet van *machine learning* voor automatische detectie en respons: de verwachting is dat vanwege de massale en geavanceerde aanvallen

die *machine learning* in de nabije toekomst mogelijk maakt, deze niet meer met alleen mensenhanden kunnen worden bestreden.

6.2 Kansen van bestaande technologie

Basisveiligheidsmaatregelen blijven onderbenut
Het heeft maar beperkt zin om de kansen van nieuwe technologieën te benutten voor verhoging van de cyberweerbaarheid, als niet tegelijkertijd op grotere schaal gebruik wordt gemaakt van reeds voorhanden zijnde technologieën. Ook bestaande, maar onderbenutte technologieën bieden kansen om de cyberweerbaarheid van Nederland te verhogen.

Dat geldt ook voor de weerbaarheid tegenover geavanceerde aanvallen, waarbij bijvoorbeeld offensief gebruik wordt gemaakt van *machine learning*. Basisveiligheidsmaatregelen (zoals sterke wachtwoorden en software updates) en andere voorhanden zijnde maatregelen (encryptie, digitale ondertekening van berichten) kunnen substantieel bijdragen aan de weerbaarheid tegen het automatisch opsporen en uitbuiten van digitale kwetsbaarheden of de verspreiding van *deep fake* beeldmateriaal. Het is dan ook problematisch dat zulke, reeds voorhanden zijnde maatregelen onvoldoende worden benut. De overheid zou dan ook sterker moeten sturen op gebruik van deze mogelijkheden om de cyberweerbaarheid te verhogen.

Veel winst mogelijk door aandacht voor structurele weerbaarheid
Daarnaast kan de technische infrastructuur van het internet op een basaler niveau weerbaarder worden gemaakt. Door in het ontwerp van systemen en applicaties structureel aandacht te besteden aan cyberweerbaarheid kan veel worden gewonnen. Denk hierbij aan het gebruik van veiligere hardware en communicatieprotocollen. Ook hiervoor geldt dat gebruik ervan door de overheid moet worden afgedwongen.

6.3 Nederland en Europa raken achterop

Nederlandse en Europese partijen zijn voor hun digitale producten en diensten in hoge mate afhankelijk van grote buitenlandse – vooral Amerikaanse en Chinese – technologiebedrijven. Dat geldt ook voor allerlei toepassingen die de cyberweerbaarheid moeten verhogen. Een belangrijke trend hierbij is dat eindgebruikers (burgers, bedrijven, overheden) maatregelen op het gebied van cyberweerbaarheid steeds vaker uitbesteden aan – buitenlandse – cloudleveranciers. Dat creëert een groeiende afhankelijkheid van die partijen, en

creëert nieuwe risico's: uitval van functionaliteit, Single Points of Failure en verlies aan zeggenschap en controle over data en dataverwerking.

Ook voor de (verdere) ontwikkeling en implementatie van nieuwe technologieën als *machine learning*, kwantumcomputing en 5G-netwerken geldt dat grote buitenlandse bedrijven vooroplopen. Nederland en de EU dreigen dan ook achterop te raken.

6.4 Opties voor versterken digitale autonomie

Voor het tegengaan van de risico's die samenhangen met de groeiende afhankelijkheid van Nederlandse en Europese partijen van buitenlandse technologiebedrijven en het versterken van de eigen, digitale autonomie, bestaan diverse opties: gebruikmaken van technische maatregelen als Privacy Enhancing Technologies, encryptie en open standaarden; strengere inkoopvoorwaarden stellen aan digitale producten en diensten; en het ontwikkelen van eigen IT-bedrijvigheid.

Versterking autonomie met technische maatregelen
Door standaard gebruik te maken van maatregelen als Privacy Enhancing Technologies, sterke encryptie, opendatastandaarden en *open source software* en gedistribueerde systemen kunnen risico's als ongewenste inzage in data, *vendor lock-in* en Single Points of Failure worden tegengegaan.

Versterking autonomie met strengere inkoopvoorwaarden
Een tweede optie om de afhankelijkheidsrisico's tegen te gaan, is het stellen van strengere eisen in inkoopvoorwaarden aan de leveranciers van digitale producten en diensten. Bijvoorbeeld door van clouddienstverleners te verlangen dat opgeslagen data standaard wordt versleuteld, zodat ze niet door de leverancier of door derde partijen kan worden ingezien.

Versterking autonomie met eigen IT-bedrijvigheid
Een derde optie om te ontsnappen aan een te grote afhankelijkheid van buitenlandse partijen, is door het creëren van meer eigen IT-bedrijvigheid in Nederland en Europa.

6.5 Stimuleren eigen IT-bedrijvigheid

Post-kwantumcryptografie biedt kansen op eigen bedrijvigheid
Nederlandse kennisinstellingen beschikken over vooraanstaande kennis op het gebied van post-kwantumcryptografie. Door deze kennis te vermarkten, ontstaan mogelijkheden om eigen IT-bedrijvigheid te ontwikkelen. In plaats van daarmee te wachten totdat het Amerikaanse National Institute for Standards and Technology (NIST) standaarden heeft geformuleerd voor post-kwantumcryptografie, zou Nederland – of beter nog: de EU – daar op korte termijn initiatieven op kunnen ontplooien.

De benodigde tijd voor een grootschalige migratie naar het gebruik van post-kwantumcryptografie en het risico van *harvest and decrypt*-aanvallen onderstrepen de urgentie om reeds op korte termijn gevoelige data met sterke encryptie te versleutelen, en daarbij waar mogelijk gebruik te maken van kwantumbestendige cryptografie. Deze urgentie vormt een extra reden om niet te wachten op de uitkomsten van de NIST-prijsvraag, die mogelijk pas in 2024 bekend worden.

Eigen kroonjuwelen eerst
Een extra reden om in ieder geval een minimum aan eigen IT-bedrijvigheid te ontwikkelen is de behoefte aan maximale beveiliging van ‘kroonjuwelen’ als staats- en bedrijfsgeheimen en overige kritieke databestanden – bijvoorbeeld door gebruik te maken van sterke vormen van (post-kwantum)cryptografie. De Rijksoverheid en aanbieders van vitale diensten moeten daarvoor producten en diensten kunnen afnemen van vertrouwde marktpartijen, die belangrijke waarden als privacy en autonomie onderschrijven. Hoewel dat niet per se hoeft te betekenen dat hiervoor producten en diensten worden afgenomen van Nederlandse of Europese leveranciers, kan dat wel helpen.

6.6 Voorwaarden voor benutten kansen

Om de kansen te benutten die nieuwe en bestaande technologieën bieden om de cyberweerbaarheid in Nederland te verhogen, moet aan de volgende voorwaarden worden voldaan.

Bevorderen innovatieklimaat
Voor het creëren van meer eigen IT-bedrijvigheid is een gunstiger innovatieklimaat nodig. De overheid kan daaraan bijdragen door aanbestedingsprocedures aantrekkelijker te maken voor innovatieve startups; door als overheid als launching customer te fungeren; en door te blijven investeren in kennisontwikkeling en in de samenwerking tussen kennisinstellingen en het bedrijfsleven.

Meer focus in onderzoeks- en innovatieagenda
Het streven naar meer eigen IT-bedrijvigheid is daarnaast gebaat bij een daadkrachtiger kennis- en innovatiebeleid, met meer focus in de Nederlandse Cyber Security Research Agenda (NCSRA). De overheid zou samen met het bedrijfsleven en kennisinstellingen gerichter moeten kiezen voor kennisgebieden waarop Nederlandse kennisinstellingen voorop moeten lopen – om vervolgens de verworven kennis te vermarkten.

Gezien de in Nederland aanwezige kennis op het gebied van post-kwantumcryptografie en het belang van een maximale beveiliging van staatsgeheimen en bedrijfsgeheimen van vitale aanbieders, ligt het voor de hand om onderzoek naar de verdere ontwikkeling en implementatie van sterke vormen van encryptie te stimuleren.

Daarnaast is het van belang dat Nederland – en Europa – onderzoek (blijven) stimuleren naar de verdere ontwikkeling en het gebruik van *machine learning*, gedistribueerde systemen en veiligere hardware, producten en communicatieprotocollen.

Invloed op richtlijnen en standaarden
Vanwege de grote invloed van internationale richtlijnen en technologiestandaarden op het algehele weerbaarheidsniveau, is het van belang dat de Nederlandse overheid – en nog beter: de EU – daarover meebeslist in internationale fora. Dat moet ook garanderen dat belangrijke Europese waarden als privacy en autonomie voldoende recht worden gedaan.

Voorbeeldfunctie overheid
Als grote afnemer van digitale producten en diensten en als grote dienstverlener zou de overheid het goede voorbeeld moeten geven door standaard gebruik te maken van basisveiligheidsmaatregelen als 2-factor-authenticatie; door in haar diensten waar mogelijk gebruik te maken van Privacy Enhancing Technologies; en door van publieke nieuwsmedia te verlangen dat zij hun berichtgeving digitaal ondertekenen.

De overheid en de aanbieders van vitale diensten zouden daarnaast een leidende rol moeten spelen in het stellen van strengere inkoopvoorwaarden aan digitale producten en diensten. Om meer marktkracht te ontwikkelen zouden de inkoopvoorwaarden bij voorkeur binnen EU-verband niveau moeten worden afgestemd.

Om deze voorbeeldfunctie te kunnen vervullen, lijkt meer centrale sturing binnen de overheid nodig, bijvoorbeeld door de verantwoordelijkheid voor de cyberweerbaarheid van de Rijksoverheid bij één ministerie te leggen.

Investeren in expertise

Het benutten van de kansen die nieuwe en bestaande technologieën bieden voor het verhogen van de cyberweerbaarheid staat of valt tenslotte met het kunnen beschikken over voldoende expertise. Zowel overheden, aanbieders van vitale diensten, overige bedrijven als toezichthouders moeten daarvoor over voldoende capaciteit en expertise beschikken. Vanwege het chronische tekort aan experts, is het dan ook hard nodig om meer te investeren in cybersecurityopleidingen.

Literatuurlijst

Ackerman, E. (2019). *Three Small Stickers in Intersection Can Cause Tesla Autopilot to Swerve Into Wrong Lane*. https://spectrum.ieee.org/cars-that-think/transportation/self-driving/three-small-stickers-on-road-can-steer-tesla-autopilot-into-oncoming-lane

AINED. (2018). *AI voor Nederland*. https://www.vno-ncw.nl/sites/default/files/aivnl_20181106_0.pdf

Algemene Rekenkamer. (2019a). *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*. https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

Algemene Rekenkamer. (2019b). *Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde.* https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde

Apple Support (2019). *About the Apple T2 Security Chip.* https://support.apple.com/en-us/HT208862

Automotive Insiders. (2018). *Branchemonitor Schadesector beschikbaar – Automotive Insiders*. https://automotiveinsiders.nl/onderzoek/

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). *Cyber Resilience – Fundamentals for a Definition*. Advances in Intelligent Systems and Computing, 353, 311–316. https://doi.org/10.1007/978-3-319-16486-1_31

Blotenburg, S. (2018). *Startup lanceert minisatelliet: "Begin van een wereldwijd IoT-netwerk"*. https://www.rtlz.nl/business/artikel/4493866/hiber-internet-things-nanosatelliet-telecom-netwerk-iot

Boschma, R. (2005). *'Proximity and Innovation: A Critical Assessment'*, Regional Studies, Volume 39, Issue 1. https://www.tandfonline.com/doi/abs/10.1080/0034340052000320887

Boyle, A. (2018). *FCC approves SpaceX's plan to provide broadband services with Starlink satellites.* https://www.geekwire.com/2018/fcc-approves-spacexs-plan-provide-broadband-services-starlink-satellites/

Broekhuizen, K. (2018). *Noodklok over Nederlandse braindrain bij cybersecurity.* Financieel Dagblad. https://fd.nl/economie-politiek/1251379/noodklok-over-nederlandse-braindrain-bij-cybersecurity

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … & Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. arXiv:1802.07228 [cs]. http://arxiv.org/abs/1802.07228

Bulletproof. (2019). *Annual Cyber Security Report 2019*.

Bundesnetzagentur. (2019). *Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks*. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190307_SL.html

Chella, V.K. (2018). *Cassandra serving netflix @ scale*. https://www.slideshare.net/VinayKumarChella/cassandra-serving-netflix-scale

CipherTrace Cryptocurrency Intelligence. (2018). *2018 Q3 Cryptocurrency Anti-Money Laundering Report* (p. 22).

Coll, L., & Simpson, R. (2016). *Connection and protection the Internet of Things and challenges for consumer protection*. https://www.consumersinternational.org/media/1292/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing, Computer Science and Telecommunications Board, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, & National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum Computing: Progress and Prospects* (E. Grumbling & M. Horowitz, Red.). https://doi.org/10.17226/25196

Consumers International, ANEC, BEUC & ICRT. (2017). *Securing consumer trust in the Internet of Things*. https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf

DARPA. (2008). *Prizes for Advanced Technology Achievements.* https://www.grandchallenge.org/grandchallenge/docs/DDRE_Prize_Report_FY07.pdf

Dcypher. (2018). *National Cyber Security Research Agenda III (NCSRA III) 2018*. https://www.dcypher.nl/national-cyber-security-research-agenda-iii-ncsra-iii-2018

De Jong, M. (2019). *Charging with a Tesla Model S/X*. *http://support.fastned.nl/hc/en-gb/articles/205418987-Charging-with-a-Tesla-Model-S-X*

Delcker, J. (2018). *Germany to launch US-style agency to develop cyberdefense*. https://www.politico.eu/article/germany-to-launch-darpa-style-agency-to-develop-cyber-defense/

Dell'Oro Group (2019). *Key Takeaways - Worldwide Telecom Equipment Market 2018*. http://www.delloro.com/delloro-group/telecom-equipment-market-2018

DG CONNECT (2019a). *Four EU pilot projects launched to prepare the European Cybersecurity Competence Network*. https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

DG CONNECT. (2019b). *The future is quantum: EU countries plan ultra-secure communication network*. https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

Dignan, L. (2018). *Top cloud providers 2018: How AWS, Microsoft, Google, IBM, Oracle, Alibaba stack up*. https://www.zdnet.com/article/top-cloud-providers-2018-how-aws-microsoft-google-ibm-oracle-alibaba-stack-up/

Dobbe, R. & M. Stikker (2019). 'Vergeet China en Silicon Valley', *NRC Handelsblad* 13 & 14 april 2019.

EC Media Convergence and Social Media Unit 1.4. (2019). Tackling online disinformation. https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Elias, T. (2014). *Parlementair onderzoek ICT-projecten bij de overheid*. https://www.tweedekamer.nl/kamerstukken/detail?id=2014Z17985&did=2014D36603

Elumalai, A., Sprague, K., Tandon, S., & Yee, L. (2018). *Ten trends redefining enterprise IT infrastructure*. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Modernizing%20IT%20for%20digital%20reinvention/Modernizing-IT-for-digital-reinvention-Collection-July-2018.ashx

ENISA. (2014). *Security Guide for ICT Procurement*. https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement

ENISA. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU*. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-eu-common-security-and-defence-policy-csdp-challenges-and-risks-for-the-eu

European Political Strategy Centre. (2019). *Rethinking Strategic Autonomy in the Digital Age*. https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf

European Commission. (2018). *State of the Union 2018 – Cybersecurity: Commission proposes to invest in stronger and pioneering cybersecurity capacity in the EU*

European Commission. (2019a). *A common EU approach to the security of 5G networks*. https://ec.europa.eu/commission/news/common-eu-approach-security-5g-networks-2019-mar-26_en

European Commission. (2019b). *A definition of Artificial Intelligence: main capabilities and scientific disciplines.* https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Europol. (2018). *Internet Organised Crime Threat Assessment 2018*.

Finlayson, S. G., Chung, H. W., Kohane, I. S., & Beam, A. L. (2018). *Adversarial Attacks Against Medical Deep learning Systems*. arXiv:1804.05296 [cs, stat]. http://arxiv.org/abs/1804.05296

Flinkle, J., & Balu, N. (2018). *Under Armour says 150 million MyFitnessPal accounts breached*. Reuters. https://uk.reuters.com/article/us-under-armour-databreach-idUKKBN1H532W

Forum Standaardisatie (2019). *Lijst open standaarden.* https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

Fraze, D. (2017). *Cyber Grand Challenge (CGC).* https://www.darpa.mil/program/cyber-grand-challenge

Fried, O., Agrawala, M., Tewari, A., Zollhöfer, M., Finkelstein, A., Shechtman, E., … Theobalt, C. (2019). Text-based editing of talking-head video. ACM Transactions on Graphics, 38(4), 1–14. https://doi.org/10.1145/3306346.3323028

Fruhlinger, J. (2018). *The Mirai botnet explained: How IoT devices almost brought down the internet*. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Gabbai, A. (2015). *Kevin Ashton Describes "the Internet of Things"*. https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/

Global Cyber Security Capacity Centre - University of Oxford. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)* - Revised Edition. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf

Google (2019). *IPv6*. Geraadpleegd 16 april 2019, van: https://www.google.com/intl/en/ipv6/statistics.html

Google. (2019). *Google Transparency Report*. https://transparencyreport.google.com/https/overview?hl=en

GreAT, & AMR. (2019). *Operation ShadowHammer*. https://securelist.com/operation-shadowhammer/89992/

Henry, C. (2018). *SpaceX won't seek U.S. rural broadband subsidies for Starlink constellation.* https://spacenews.com/spacex-wont-seek-u-s-rural-broadband-subsidies-for-starlink-constellation/

Hern, A. (2018*). Fake fingerprints can imitate real ones in biometric systems – research*. The Guardian. https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research

Higgins, K. (2017). *New Tool Debuts for Hacking Back at Hackers in Your Network*. https://www.darkreading.com/attacks-breaches/new-tool-debuts-for-hacking-back-at-hackers-in-your-network/d/d-id/1330121

Hill, M. (2017). *Behavioral Analytics in Cybersecurity*. https://www.infosecurity-magazine.com:443/editorial/behavioral-analytics-in/

Hilton, S. (2016). *Dyn Analysis Summary Of Friday October 21 Attack*. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Hijink, M. (2019). *Details van 5G-netwerk met Huawei blijven mistig*. https://www.nrc.nl/nieuws/2019/07/01/details-van-5g-netwerk-met-huawei-blijven-mistig-a3965775

Hooghiemstra, T. (2018). *Informationele zelfbeschikking in de zorg*. https://research.tilburguniversity.edu/en/publications/informationele-zelfbeschikking-in-de-zorg

Huawei Cyber Security Evaluation Centre. (2019). *Huawei cyber security evaluation centre oversight board: annual report 2019*. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

ISACA. (2018). *State of Cybersecurity 2018*. https://cybersecurity.isaca.org/state-of-cybersecurity

ISC2. (2018). *Cybersecurity Workforce Study*. https://www.isc2.org:443/Research/Workforce-Study

IT Governance UK. (2019). *Cyber Resilience*. https://www.itgovernance.co.uk/cyber-resilience

ITU. (2017). *Global Cybersecurity Index*.

Jones, A. (2018). *Spacety a Chinese Startup Plans Launch of Four Satellites on October 29*. http://satnews.com/story.php?number=2063954306

Karataş, A., & Şahin, S. (2017). *A Review on Social Bot Detection Techniques and Research Directions*.

Kaska, K., Beckvard, H., & Minárik, T. (2019). *Huawei, 5G and China as a Security Threat* (p. 26). Tallin: NATO Cooperative Cyber Defence Centre of Excellence.

Kleinhans, J.-P. (2019). *5G vs. National Security*. https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf

Lapowsky, I. (2018). Facebook Exposed 87 Million Users to Cambridge Analytica. *Wired*. https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

Liao, S.-K. et al. (2017). *Satellite-to-ground quantum key distribution*. Nature, 549(7670), 43–47. https://doi.org/10.1038/nature23655

Lueth, K.L. (2018). *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating*. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Lysne, O. (2018). *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* https://www.springer.com/de/book/9783319749495

Major, M. (2018). *A Look at How Easily 3D-Printed Heads Can Hack Facial Recognition*. https://interestingengineering.com/a-look-at-how-easily-3d-printed-heads-can-hack-facial-recognition

McAfee (2018). *McAfee Labs 2019 Threats Predictions Report.* https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/

McLean, V. (2019). *Iridium Declares Victory; $3 Billion Satellite Constellation Upgrade Complete*. http://www.spacedaily.com/reports/Iridium_Declares_Victory_3_Billion_Satellite_Constellation_Upgrade_Complete_999.html

Mehta, I. (2019). *Samsung's new AI can create talking avatars with a single photo*. https://thenextweb.com/artificial-intelligence/2019/05/23/samsungs-new-ai-can-create-talking-avatars-with-a-single-photo/

Microsoft (2014). *Microsoft Security Advisory 2862973*. https://docs.microsoft.com/en-us/security-updates/securityadvisories/2014/2862973

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. (2014). *Open overheid*. https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/open-overheid

Ministerie van Economische Zaken en Klimaat. (2019). *Missies voor het* topsectoren- en innovatiebeleid. https://www.rijksoverheid.nl/documenten/publicaties/2019/04/26/missies

Ministerie van Economische Zaken en Klimaat, Ministerie van Justitie en Veiligheid. (2018). Roadmap Digitaal Veilige Hard- en Software. https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software

Ministerie van Justitie en Veiligheid. (2019). *Kamerbrief Maatregelen bescherming telecomnetwerken en 5G.* https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/kamerbrief-maatregelen-bescherming-telecomnetwerken-en-5g

Ministerie van Veiligheid en Justitie. (2013). *Nationale Cyber Security Strategie 2*. https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2

Minister van Veiligheid en Justitie, & Minister van Economische Zaken. (2016). Kabinetsstandpunt encryptie. Geraadpleegd 7 augustus 2019: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail

Modderkolk, H. (2019). *Grapperhaus stuurt na Volkskrant-publicatie alsnog kritisch AIVD-advies over 5G naar de Kamer.* https://www.volkskrant.nl/gs-b820d00f

Morris, S. (2018). *Cloud Computing Tops List of Emerging Risks*. Geraadpleegd 15 april 2019: https://www.gartner.com/smarterwithgartner/cloud-computing-tops-list-of-emerging-risks/

Mozilla (2019). *Security vulnerabilities fixed in Thunderbird 60.5.1.* https://www.mozilla.org/en-US/security/advisories/mfsa2019-06/

NCTV. (2018). Factsheet weerbare vitale infrastructuur.

NCTV. (2019a). Cybersecuritybeeld Nederland CSBN 2019.

NCTV. (2019b). *Uw Eigen Veiligheid*. https://www.nctv.nl/binaries/WEB_117467_NCTV_UwEigenVeiligheid_A5_tcm31-371131.pdf

NIST CSRC (2019). *Workshops and Timeline - Post-Quantum Cryptography*. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

Norrman, K., Nakarmi, P., & Fogelström, E. (2018). *5G security - enabling a trustworthy 5G system [White paper]*. https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system

Olsthoorn, P. (2017). *Fox-IT moet Nederlands blijven van Defensie*. https://www.netkwesties.nl/957/fox-moet-nederlands-blijven-defensie.htm

OpenAI. (2019). *Better Language Models and Their Implications*. https://openai.com/blog/better-language-models/

Ortiz, E. (2018). *Marriott says data breach compromised info of up to 500 million guests*. NBC News. https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041

OWASP IoT Security Team. (2018). *OWASP IoT Top 10 2018*. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

Pal, G. (2018, april 2). *Secdevops or devsecops or devops next-generation (NG) – What is your take on devops?* https://www.csoonline.com/article/3267633/secdevops-or-devsecops-or-devops-next-generation-ng-what-is-your-take-on-devops.html

Patiëntenfederatie Nederland. (2019). *Het Patiëntgeheim*. https://www.rijksoverheid.nl/documenten/rapporten/2019/01/17/het-patientgeheim

Pultarova, T. (2017). *Picture of Health: Can AI Eye Scan Reveal What Ails You?* https://www.livescience.com/61171-artificial-intelligence-eye-scan.html

Raad voor de Leefomgeving en Infrastructuur. (2018). *Stroomvoorziening onder digitale spanning*. https://www.rli.nl/publicaties/2018/advies/stroomvoorziening-onder-digitale-spanning

Rathenau Instituut (2017). *Een nooit gelopen race – Over cyberdreiging en versterking van weerbaarheid*. Den Haag (auteurs: Munnichs, G., M. Kouw & L. Kool). https://www.rathenau.nl/nl/digitale-samenleving/een-nooit-gelopen-race

Rathenau Instituut (2018a). *Bedrijf zoekt universiteit – De opkomst van strategische publiek-private partnerships in onderzoek.* Den Haag (auteurs: Tjong Tjin Tai, S.Y., J. van den Broek, T. Maas, T. Rep & J. Deuten). https://www.rathenau.nl/nl/vitale-kennisecosystemen/bedrijf-zoekt-universiteit

Rathenau Instituut (2018b). *Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland.* Den Haag (auteurs: Keulen, I. van, I. Korthagen, P. Diederen & P. van Boheemen). https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws

Rathenau Instituut (2019a). *Kennis in het vizier – De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur*. Den Haag (auteurs: Diercks,

G., J. Deuten & P. Diederen). https://www.rathenau.nl/nl/vitale-kennisecosystemen/kennis-het-vizier

Rathenau Instituut (2019b). *Cyberspace zonder conflict – De zoektocht naar de-escalatie van het internationale informatieconflict*. *Den Haag (auteurs:* Hamer, J., R. van Est & L. Royakkers). https://www.rathenau.nl/nl/digitale-samenleving/cyberspace-zonder-conflict

Rathenau Instituut (2019c). 'Zo brengen we AI in de praktijk vanuit Europese waarden.' Website Rathenau Instituut, 19 maart 2019 (auteurs: Jong, R. de, L. Kool & R. van Est) https://www.rathenau.nl/nl/digitale-samenleving/zo-brengen-we-ai-de-praktijk-vanuit-europese-waarden

Rathenau Instituut (2019d). *Gezondheid centraal – Zorgvuldig data delen in de digitale samenleving*. Den Haag (auteurs: Niezen, M., R. Edelenbosch, L. van Bodegom & P. Verhoef). https://www.rathenau.nl/nl/maakbare-levens/gezondheid-centraal

RVO (2017). *3e tender SBIR Cyber Security*. https://www.rvo.nl/subsidies-regelingen/sbir/overzicht-sbir-oproepen/3e-tender-sbir-cyber-security

Saffman, M. (2016). *"Quantum Computing with atomic qubits and Rydberg interactions: progress and challenges,"* Journal of Physical B: Atomic, Molecular and Optical Physics, 49, 202001

Schiffer, A. (2017). *How a fish tank helped hack a casino*. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (1 edition). New York: W. W. Norton & Company.

Scott, J. (2018). *Australia Passes Law Targeting WhatsApp and Signal*. https://www.bloomberg.com/news/articles/2018-12-06/australia-moves-toward-passing-law-targeting-whatsapp-signal

Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., Silva, P. D., … Wunder, G. (2017). *5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice*. IEEE Journal on Selected Areas in Communications, 35(6), 1201–1221. https://doi.org/10.1109/JSAC.2017.2692307

Sheridan, K. (2018). *Google Engineering Lead on Lessons Learned From Chrome's HTTPS Push*. Dark Reading.

SIDN fonds (2018). *Dowse*. https://www.sidnfonds.nl/projecten/dowse

Solid (2019). *How It Works.* https://solid.inrupt.com/how-it-works

sp.a. (2018). "Trump heeft een boodschap voor alle Belgen... #Klimaatpetitie https://t.co/Kf7nIaDOKj" Twitter. https://twitter.com/sp_a/status/998089909369016325

SSC-ICT (2019). *In het digitale hart van de Rijksoverheid*. https://www.ssc-ict.nl/actueel/nieuws/2019/soc.aspx

Stewart, R. (2019). *Digital signatures in PDF applications exploited by researchers*. https://cyware.com/news/digital-signatures-in-pdf-applications-exploited-by-researchers-2df0bc66

STOA. (2017). *Achieving a sovereign and trustworthy ICT industry in the EU*. http://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2017)614531

Studiegroep Informatiesamenleving en Overheid. (2017). *Maak Waar!* https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar

Stupp, C. (2018a). *National governments reach breakthrough deal on voluntary cybersecurity certification*. https://www.euractiv.com/section/cybersecurity/news/national-governments-reach-breakthrough-deal-on-voluntary-cybersecurity-certification/

Stupp, C. (2018b). *Plan for EU cybersecurity certification receives Parliament approval*. https://www.euractiv.com/section/cybersecurity/news/plan-for-eu-cybersecurity-certification-receives-parliament-approval/

Tao, L. (2018). *Japan latest country to exclude Huawei, ZTE from 5G roll-out*. https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government

TechNavio. (2017). *Global Security Information and Event Management Market 2017-2021.* https://www.technavio.com/report/global-it-security-global-security-information-and-event-management-market-2017-2021

Van der Gaast, S., Xu, H., Koonen, T., & Tangdiongga, E. (2018). Optical Wireless Communication: Options for extended spectrum use [Rapport]. https://www.agentschaptelecom.nl/documenten/rapporten/2018/02/07/onderzoek-lifi

Van der Grient, R., & Konings, F. (2018). *Nationaal Cybersecurity Bewustzijnsonderzoek 2018*. https://www.alertonline.nl/cybersecurityonderzoek

Van der Laan, S. (2019). *Nederlandse ziekenhuizen kwetsbaar voor cyberaanvallen*. https://www.elsevierweekblad.nl/kennis/achtergrond/2019/02/nederlandse-ziekenhuizen-kwetsbaar-voor-cyberaanvallen-163181w/

Van Eeten, M. (2017). *Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity*. Digital Policy, Regulation and Governance, 19(6), 429–448. https://doi.org/10.1108/DPRG-05-2017-0029

Verhagen, L. (2019). *Overal hangen beveiligingscamera's. Hoe betrouwbaar zijn de interpretaties die computers maken van de beelden?* Geraadpleegd 7 augustus 2019, van: De Volkskrant website: https://www.volkskrant.nl/gs-bef1fd8b

Verizon (2018). *Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/dbir/

Werken bij de Overheid (2019). *Manager Release • Ministerie van Defensie*. Geraadpleegd 15 april 2019, van: https://www.werkenbijdeoverheid.nl/vacatures/manager-release-DEF-2019-0859

Whittaker, Z. (2019). *New flaws in 4G, 5G allow attackers to intercept calls and track phone locations*. http://social.techcrunch.com/2019/02/24/new-4g-5g-security-flaws/

Wlodarczak, P. (2017). *Cyber Immunity - A Bio-Inspired Cyber Defense System*. 199–208. https://doi.org/10.1007/978-3-319-56154-7_19

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 edition). New York: PublicAffairs.

Bijlage 1: Begrippenlijst

In dit rapport wordt gesproken over de volgende nieuwe technologieën.

Technologie	Toelichting
2-factor-authenticatie	Methode waarbij een gebruiker twee stappen moet doorlopen om te bewijzen dat deze is wie hij beweert te zijn.
5G-netwerken	De vijfde generatie draadloze of mobiele systemen. Deze kunnen bijvoorbeeld gegevens in grotere hoeveelheden en met minder vertraging transporteren. Dit kan de functionaliteit van veel digitale toepassingen verbeteren.
automatische responssystemen	Systemen die zelfstandig reageren op incidenten.
behaviourial analytics	Analysemethode die het gedrag van gebruikers in digitale systemen in kaart brengt, bijvoorbeeld om afwijkend gedrag te kunnen signaleren.
biometrische identificatie	Een vorm van identificatie die vaak wordt toegepast in toegangscontrole, gebaseerd op biologische kenmerken van een persoon, zoals een vingerafdruk of iris.
botnet	Een netwerk dat bestaat uit een groot aantal digitale apparaten die door één actor simultaan kunnen worden aangestuurd, meestal met als doel schade aan te richten zonder dat de eigenaren van de apparatuur daar weet van hebben.
cloudtechnologie	Dienstverlening van softwarebedrijven waarbij gebruikers gebruik maken van systemen van de aanbieder.
deep fakes	Beeldmateriaal dat door *machine learning*-software dusdanig is gemanipuleerd dat het nauwelijks van echt is te onderscheiden.
deep learning	Vorm van *machine learning* die is gebaseerd op neurale netwerken – geïnspireerd op de biologie van ons brein – en die verschillende lagen informatie met elkaar combineert.
desktop-as-a-service	Een dienst die nagenoeg de volledige gebruikerservaring van een traditionele desktopcomputer simuleert en aanbiedt in de vorm van een clouddienst.
encryptie; homoforme encryptie	Digitale versleuteling; bij homomorfe encryptie kunnen gebruikers versleutelde gegevens verwerken zonder ze te moeten ontsleutelen.

gedistribueerde systemen	Een samenhangend netwerk van zelfstandige computersystemen die functies voor de gebruiker als een coherent systeem uitvoeren, zonder centraal aanstuurpunt.
harvest and decrypt-strategie	Een ontsleutelingsstrategie die er van uitgaat dat in de (nabije) toekomst nu gangbare encryptiemethoden kunnen worden doorbroken. Versleutelde data worden daartoe nu alvast verzameld.
IMSI-*catching*	Een methode waarbij een aanvaller op een mobiel telefonie/communicatienetwerk verbindingen onderschept.
interferentie	De samen- of tegenwerking van verscheidene golven op dezelfde tijd en plaats.
Internet of Things (IoT)	Het geheel aan apparaten die op het internet zijn aangesloten.
IP-protocol	Een netwerkprotocol waarmee computers in een netwerk met elkaar kunnen communiceren.
lawful interception	Wettelijke mogelijkheid om telecommunicatie af te tappen.
LiFi	Dataoverdrachtstechnologie gebaseerd op snel knipperend LED-licht.
kwantumcomputer	Computer die zijn rekenkracht ontleent aan kwantumfysische eigenschappen.
kwantumcommunicatie	Dataoverdrachtstechnologie gebaseerd op kwantumfysica.
kwantumcomputing	Het gebruik maken van de rekenkracht van een kwantumcomputer.
machine learning	Algoritmen met een zekere mate van lerend vermogen. Doorgaans gebaseerd op het vergelijken van data met een dataset van aangeleerde patronen. De technologie leunt sterk op statistiek.
multifactor-authenticatie	Authenticatiemethode die meerdere methoden combineert om authenticiteit vast te stellen.
Named Data Networking (NDN)	Netwerkprotocol dat de beveiliging van data als uitgangspunt neemt.
network slicing	De mogelijkheid die 5G biedt om datastromen te scheiden.
NIST-prijsvraag	In dit rapport refereert dit begrip aan een prijsvraag met als doel het ontwikkelen, evalueren en standaardiseren van één of meer kwantumbestendige cryptografische algoritmes.
post-kwantumcryptografie	Een dusdanig sterke versleutelingsmethode die bestand is tegen de rekenkracht van een kwantumcomputer.

Opendatastandaarden en -software	Openbare standaarden voor databestanden en software met openbare broncode, die afhankelijk van de mate van openheid door iedereen gebruikt, bewerkt en verspreid mogen worden.
Privacy Enhancing Technologies (PETs)	Technologieën die de privacy van de gebruiker ten goede komen, bijvoorbeeld door het toepassen van een sterke vorm van versleuteling en de minimalisatie van datavergaring.
secure multi-party computation	Rekenmethode die meerdere partijen in staat kan stellen om gezamenlijk informatie te delen, zonder dat de gegevens te herleiden zijn tot één bepaalde partij.
Single Point of Failure	Het risico dat ontstaat wanneer enkele of meerdere cruciale functies van een proces zijn ondergebracht bij één partij, waardoor verstoring bij deze partij leidt tot een onderbreking van het gehele proces.
superpositie	Het kwantummechanische verschijnsel dat een systeem tegelijkertijd in twee verschillende posities kan verkeren.
vendor lock-in	Een situatie waarin een gebruiker dermate afhankelijk is geworden van één leverancier, dat de kosten van een overstap naar een andere leverancier te hoog zijn geworden.
wearables	Mobiele digitale gadgets die op het lichaam worden gedragen.

Bijlage 2: Deelnemers interviews

Jaya Baloo, KPN
Maarten Bodlaender, Philips
Hans Bos, Rijkswaterstaat
Jeremy Butcher, Fox-IT
René van Buuren, Thales
Frank Fransen, TNO
Wil van Gemert, Europol
Koen Gijsbers
Frank Groenewegen, Fox-IT
Allard Kernkamp, TNO
Raymond Kleijmeer, De Nederlandsche Bank
Cees de Laat, Universiteit van Amsterdam
Erwin Mededorp, Onderzoeksraad voor Veiligheid
Jasper Nagtegaal, Agentschap Telecom
Bert Jan te Paske, TNO
Roeland Reijers, Universiteit van Amsterdam
Hessel Schut, Team High Tech Crime
Dimitri Tokmetzis, De Correspondent
Jos Weyers, Tennet
Paul Wijninga, Agentschap Telecom
Rejo Zenger, Bits of Freedom
Annemarie Zielstra, TNO
Lodewijk van Zwieten, Openbaar Ministerie
AIVD

Bijlage 3: Deelnemers workshops

Maarten Bodlaender, Philips
Pieter van Boheemen, Rathenau Instituut
Mark Crooijmans, Gemeente Amsterdam
Gijs Diercks, Rathenau Instituut
Sander van Dorst, Ministerie van Defensie
Jeroen Gaiser, Rijkswaterstaat
Jurriën Hamer, Rathenau Instituut
Elly van den Heuvel, Cyber Security Raad
Andreas Hülsing, Universiteit Eindhoven
Bart Jacobs, Radboud Universiteit Nijmegen
Linda Kool, Rathenau Instituut
Michiel Leenaars, Internet Society
Geert Munnichs, Rathenau Instituut
Luisella ten Pierik, Stedin
Remco Poortinga, SURF
Inge Quest, NCTV
Melanie Rieback, Radically Open Security
John Sinteur, Radically Open Security
Harold Vermanen, Microsoft
Anouk Vos, RevNext/Radically Open Security
René Vroom, Agentschap Telecom
Sandra van der Weide, Ministerie van Economische Zaken en Klimaat
Jos Weyers, Tennet
Paul Wijninga, Agentschap Telecom
Ministerie van Justitie en Veiligheid

Open Access
Het Rathenau Instituut heeft een Open Access beleid. Rapporten, achtergrondstudies, wetenschappelijke artikelen, software worden vrij beschikbaar gepubliceerd. Onderzoeksgegevens komen beschikbaar met inachtneming van wettelijke bepalingen en ethische normen voor onderzoek over rechten van derden, privacy, en auteursrecht.

Contactgegevens
Rathenau Instituut
Anna van Saksenlaan 51
Postbus 95366
2509 CJ Den Haag
070-342 15 42
info@rathenau.nl
www.rathenau.nl

Het Rathenau Instituut stimuleert de publieke en politieke meningsvorming over de maatschappelijke aspecten van wetenschap en technologie. We doen onderzoek en organiseren het debat over wetenschap, innovatie en nieuwe technologieën.

Rathenau Instituut