CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'

Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?

CSR

Cyber Security Council

Cyber Security Raad

CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'

Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie

Cyber Security Council Cyber Security Raad

6 mei 2021

CSR Advies 2021, nr. 3

Excellenties,

Hierbij ontvangt u van de Cyber Security Raad (hierna: de raad) het advies 'Nederlandse Digitale Autonomie en Cybersecurity'.

Introductie

Digitale autonomie raakt het hart van onze rechtstaat en daarmee het fundament van onze samenleving. Digitale autonomie is een complex en urgent vraagstuk dat een belangrijk onderdeel is van een integrale aanpak voor cyberweerbaarheid, inclusief de noodzakelijke investeringen conform het eerdere advies hierover van de raad.[1] Het nu voorliggende advies gaat specifiek in op het onderdeel digitale autonomie en cybersecurity. Dit is nodig gezien de enorme urgentie die van de thematiek uitgaat en de noodzaak om het op de juiste niveaus onder de aandacht te krijgen.

De ultieme uitdaging is: *hoe behouden we als Nederland ook in de digitale wereld controle over onze democratie, rechtstaat en economisch innovatiesysteem.* Ons vermogen om autonoom beslissingen te nemen staat vanuit drie kanten onder druk:

- ***Cyberdreigingen nemen verder toe***, waarbij ook kleinere landen en niet-statelijke actoren zich op het mondiale strijdtoneel begeven.[2] Het gaat om directe bedreiging van onze vitale infrastructuur (sabotage), systematische diefstal door statelijke actoren van intellectueel eigendom van onze kennisintensieve bedrijven (*economische spionage*), digitale afpersing (*ransomware*) en doelgerichte misinformatie en systematische infiltratie van sociale media om bijvoorbeeld onze verkiezingen en democratische processen te beïnvloeden.
- ***De geopolitieke spanningen tussen de VS en China nemen steeds verder toe,*** waarbij de digitale technologieën inmiddels het slagveld zijn voor de wedijver om mondiaal leiderschap (ook wel: de *tech cold war*).[3] De strijd gaat dan vooral over het leiderschap op het gebied van 5G/6G, kwantumcomputers, computerchiptechnologie en *artificial intelligence (AI)*. Zowel de VS als China trekken in dat verband regelmatig de *soevereiniteits*-kaart. Voorbeeld is de Amerikaanse ban van Huawei als leverancier van Amerikaanse telecominfrastructuur. In aanvulling daarop is Huawei nu ook beperkt in de mogelijkheid om computerchips aan te kopen die buiten de VS met Amerikaanse technologie zijn geproduceerd. Niet verrassend is dat China represailles treft, zoals exportbeperkingen op technologie.[4]
- ***We worden als samenleving steeds afhankelijker van de digitale infrastructuur die in handen is van een beperkt aantal dominante buitenlandse marktspelers.*** De data van nagenoeg alle Europese bedrijven en burgers bevinden zich inmiddels in de cloud van met name Amerikaanse techbedrijven en zijn daarmee niet beschikbaar voor Europese innovatie.[5] De sociale mediaplatforms bepalen steeds meer de spelregels van onze democratie, door hun gebrek aan maatregelen om misinformatie, *fake news* en politieke beïnvloeding op hun platforms tegen te gaan.[6] De sterke afhankelijkheid van niet Europese bedrijven brengt tevens controle van andere landen mee, die andere spelregels hanteren wat betreft spionage, privacy en afgifte van data.

[1] CSR Advies 'Integrale aanpak voor cyberweerbaarheid', CSR Advies 2021, nr. 2

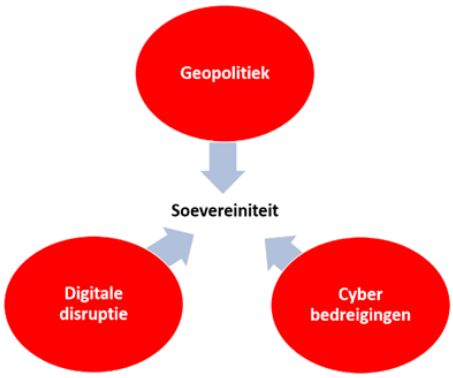
[2] Sanger, D.A. (2018), *The perfect weapon. War sabotage and fear in the cyber age*, New York; Crown. Ook Corien Prins signaleert dat het nieuwe digitale wapentuig de (geopolitieke) orde verandert: "De machtsbalans verschuift, nu ook kleinere landen zich op het mondiale strijdtoneel kunnen begeven. Zonder dat ze daartoe een grootschalige militaire confrontatie aan moeten gaan of feitelijk het grondgebied van een andere staat dienen te betreden. Kortom, op relatief eenvoudige wijze valt grote slagkracht te ontwikkelen", https://www.njb.nl/blogs/consequenties-van-een-nieuw-type-oorlogsvoering/

[3] https://usinnovation.org/news/whos-winning-tech-cold-war-china-vs-us-scoreboard

[4] Zie voor een overzichtsartikel: https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html

[5] Digital Services Act package, Inception Impact Assessment, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services

[6] European Commission, "Tackling online disinformation", https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation



Ook Europa voelt de dreiging van wat wel het *techkolonialisme* van de VS en China wordt genoemd. Waar in 2017 het spreken over Europese soevereiniteit nog *not done* was en Europa voorstander was van de open liberale markteconomie en bijvoorbeeld Europese research programma's *open to the world* moesten zijn,[7] is inmiddels het herstel van de *technologische soevereiniteit* van de EU (naast herstel van de coronacrisis en bestrijding van klimaatverandering) de kernambitie van de Europese Commissie en de Europese Raad voor de komende vijf jaar.[8] Digitale soevereiniteit is inmiddels op Europees niveau en in meerdere lidstaten *Chefsache* geworden. Begin maart 2021 hebben elf EU landen in publieke brieven aan de Europese Commissie een oproep gedaan nog sterker in te zetten op maatregelen om de Europese digitale soevereiniteit te versterken.[9] In Nederland staat het echter nog onvoldoende op de politieke agenda en overwegingen van digitale autonomie worden niet structureel meegenomen bij het opstellen van beleid en wetgeving. De raad constateert dat cybersecurity tot nog toe vooral technisch en reactief wordt aangepakt en vrijwel niet vanuit het bredere perspectief van strategische autonomie. Als gevolg daarvan lopen we meestal achter de feiten aan en moeten we in crisismode reageren op incidenten. Uitdagingen en bedreigingen voor strategische autonomie in cybersecurity zijn echter te belangrijk om deze niet vanuit een breed perspectief te bezien.

De raad heeft onderzoekers Freddy Dezeure en Paul Timmers een studie[10] laten uitvoeren naar 'Nederlandse Strategische Autonomie en Cybersecurity' (hierna: *de studie*). Deze studie geeft een diepgaande analyse van het gehele spectrum van bedreigingen voor onze controle over strategische cybersecuritykennis, technologieën, innovaties en vaardigheden en de impact daarvan op onze strategische autonomie. Het advies van de raad is gebaseerd op de resultaten van dit onderzoek. *De raad beveelt verantwoordelijken en geïnteresseerden aan de inhoud van het advies en het rapport tot zich te nemen.*

Gezien de urgentie en het belang van het onderwerp zal de raad actief inzetten op een brede verspreiding van dit advies en de studie en wordt ook een aantal workshops georganiseerd. Verder zal de raad in samenwerking met de onderzoekers een praktisch toetsingskader ter beschikking stellen voor proactief, coherent en integraal beleid ter versterking van de digitale autonomie.

De raad is van mening dat er nu actie moet én kan worden genomen om strategische autonomie met betrekking tot cyberveiligheid te waarborgen.

[7] 'Horizon 2020 is open to the world', https://ec.europa.eu/programmes/horizon2020/en/area/international-cooperation.
[8] Zie ook de inaugurele speech van Ursula Von der Leyen als voorzitter van de Commissie: "We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies, https://ec.europa.eu/info/sites/info/files/president-elect-speech-original_en.pdf.
[9] 'Digital sovereignty letter European Commission from Germany, Denmark, Estonia and Finland', dd. March 1, 2021, https://www.valitsus.ee/en/news/heads-government-germany-denmark-estonia-and-finland-europes-digital-sovereignty-gives-us en 'Letter on digital sovereignty by 8 EU countries', dd. March 8, 2021, https://edri.org/wp-content/uploads/2021/03/POLITICO_Letter-on-digital-sovereignty-by-8-EU-countries.pdf
[10] Nederlandse strategische autonomie en cybersecurity, Paul Timmers en Freddy Dezeure, januari 2021, https://www.cybersecurityraad.nl/documenten/rapporten/2021/02/18/onderzoeksrapport-digitale-autonomie

Soevereiniteit wordt over het algemeen geassocieerd met territorialiteit, jurisdictie, een bevolking, gezag met interne erkenning (*interne legitimiteit*) en externe erkenning (*externe legitimiteit*).
Strategische autonomie is een *middel* om soevereiniteit te verkrijgen en te behouden en bestaat uit het vermogen en de middelen om beslissingen te kunnen nemen en uit te voeren aangaande essentiële aspecten van de langetermijn-toekomst in economie, maatschappij en democratie.
Digitale autonomie is strategische autonomie in het digitale domein.

Wat is digitale autonomie?

Digitale autonomie is niet beperkt tot het hebben van controle van onze staat over het gebruik en de inrichting van kritieke digitale systemen en de daarmee gegenereerde en opgeslagen data. Het moet daarnaast ook worden vertaald naar het bredere staatsbelang van **economie** (controle over essentiële economische ecosystemen), **maatschappij** en **democratie** (vertrouwen in het rechtssysteem en kwaliteit van democratische besluitvorming).[11] Een belangrijke dimensie van digitale autonomie is de *cybersecurity* van onze kritische sectoren, processen, en data. De steeds toenemende cyberdreigingen ondermijnen onze digitale autonomie. We spreken dan over het hele spectrum van een directe bedreiging van onze vitale infrastructuur, systematische diefstal van het intellectueel eigendom van onze kennisintensieve bedrijven die wereldwijd toonaangevend zijn, digitale afpersing, doelgerichte misinformatie en systematische infiltratie van sociale media om verkiezingen en democratische processen te beïnvloeden.[12]

Wanneer onze overheid en kritische sectoren geen controle hebben over belangrijke processen en data raakt dit vooral de *interne legitimiteit* van de staat. Cyberbedreigingen kunnen ook de *externe legitimiteit* van Nederland onder druk zetten. Zo blijkt dat de Nederlandse digitale infrastructuur regelmatig door statelijke actoren wordt misbruikt bij cyberaanvallen op andere landen.[13] Nederland is hiervoor aantrekkelijk doordat de digitale infrastructuur van hoge kwaliteit is en digitale capaciteit relatief simpel kan worden gehuurd. Deze vorm van misbruik kan het internationale imago van Nederland schaden en slecht zijn voor bondgenootschappelijke belangen. Het ondermijnt daarmee onze externe legitimiteit in internationale betrekkingen.[14]

Digitale soevereiniteit kan niet los worden gezien van de drie basisprincipes van informatieveiligheid: *vertrouwelijkheid, integriteit en beschikbaarheid*.[15] In deze drie domeinen dient de autonomie te worden gewaarborgd, niet alleen op het niveau van een *specifiek systeem* in een bepaalde sector (zoals een ICT-systeem in de strafrechtketen), maar ook in het grotere kader van *economie, maatschappij en democratie*.

Verzwakte controle over *economische ecosystemen en kennis* kan soevereiniteit in gevaar brengen – denk aan gebrek aan controle over kritische technologie, zoals AI en cryptografie en andere vormen van informatiebeveiliging. Indien hier niet genoeg innovatie plaatsvindt, ontstaan potentieel nieuwe afhankelijkheden. Zo spelen bijvoorbeeld nieuwe technologieën een steeds crucialere rol voor cyberweerbaarheid.[16]

[11] Voor definities zie: Timmers, P., Strategic Autonomy and Cybersecurity, European Institute of Security Studies, mei 2019.
[12] Zie het Cybersecuritybeeld Nederland 2020 (CSBN 2020), voor een actueel overzicht van alle soorten cyberdreigingen, https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020.
[13] Cybersecuritybeeld Nederland 2020 (CSBN 2020), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), juni 2020
[14] Cybersecuritybeeld Nederland 2020 (CSBN 2020), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), juni 2020, p. 18, onder verwijzing naar het AIVD Jaarverslag 2019, april 2020.
[15] Ook wel genoemd de CIA van cybersecurity: *Confidentiality, Integrity, Availability*.
[16] Kennis- en innovatieagenda Veiligheid, Ministerie van Economische Zaken & Klimaat, 2019; zie verder Van Boheemen, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos (2019). Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie. Den Haag: Rathenau Instituut. Zie ook CSR Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland', CSR Advies 2020, nr. 5, september 2020, p. 3.

AI vergemakkelijkt bijvoorbeeld het uitvoeren van cyberaanvallen, doordat bestaande kwetsbaarheden automatisch op grote schaal kunnen worden ontdekt en uitgebuit.[17] AI zal het echter naar verwachting ook mogelijk maken om zelf automatisch kwetsbaarheden in software op te sporen en te herstellen. Met post-kwantumcryptografie moeten we uiteindelijk dataversleuteling mogelijk maken, die bestand is tegen aanvallen waarbij gebruik wordt gemaakt van de rekenkracht van een kwantumcomputer.[18]

Wat betreft het *maatschappelijke en democratische belang* gaat het vooral over het functioneren van en vertrouwen in de rechtsstaat. In soevereiniteitstermen betreft dit dan vooral de *interne* legitimiteit van de staat. Wanneer de interne legitimiteit ter discussie staat (bijvoorbeeld wanneer de staat geen controle heeft over het verkiezingsproces, omdat dit is geïnfiltreerd en wordt gemanipuleerd door vreemde mogendheden) is het niet uitgesloten dat ook de *externe* legitimiteit in het gedrang komt (Nederland als betrouwbare internationale partner).

Cybersecurity benaderen vanuit soevereiniteitsperspectief

Door de veelzijdigheid van de oorzaken van de druk op onze digitale soevereiniteit en de snelle geopolitieke ontwikkelingen, is er geen *one-size-fits-all* oplossing voorhanden. Onze soevereiniteit zal moeten worden ondersteund door een ‘slimme’ combinatie van maatregelen. Een ‘slimme’ aanpak betekent ook het maken van een kosten-baten- afweging. Digitale autonomie betekent niet zelfredzaamheid of zelfvoorziening. Dat is niet weggelegd voor Nederland en veelal ook niet voor Europa. Laat staan dat dit wenselijk zou zijn. Globalisering heeft enorme voordelen gebracht, zeker ook voor Nederland. Balkanisering van technologie en protectionisme kan wereldwijde handel belemmeren en daarmee ook welvaart en banen kosten in Nederland. Nederland doet er derhalve goed aan zijn afhankelijkheden te inventariseren en eenzijdige afhankelijkheden te verkleinen, dit ook buiten de bekende samenwerkingsverbanden van EU en NAVO.[19]

1. Sterk in eigen huis, sterk in Europa, sterk in de wereld

Nederland en de EU hebben alleen dan een stem op het internationale digitale speelveld, en dus in de geopolitiek, als we sterk zijn in eigen huis. Dat betekent, meer zeggenschap over eigen data, meer grip op kritische digitale processen, en meer innovatie en kennis onder eigen controle. Dit moet samengaan met onze traditionele kracht, de interne markt en de Europese waarden.
De kernambitie van de Europese Commissie om in te zetten op technologische soevereiniteit, heeft inmiddels geleid tot een reeks van Europese beleidsvoorstellen.[20] Nederland kan in het EU-beleid een aanjagersrol spelen door ervoor te zorgen in het Nederlandse beleid haar eigen visie van digitale autonomie expliciet te maken en deze visie en aanpak als bijdrage in het EU-beleid in te brengen. Nederland zou daarmee - net als voorlopers Duitsland en Frankrijk - helderheid creëren en zich versterken als gesprekspartner.

[17] Cybersecuritybeeld Nederland 2020 (CSBN 2020), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), juni 2020, p. 15 – 26.
[18] CSR Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland’, CSR Advies 2020, nr. 5, september 2020, p. 4.
[19] De WRR noemt specifiek als voorbeelden landen als Zuid-Korea, Chili, Canada en Nieuw-Zeeland, Hollands Spoor, debatten strategieberaad Rijksbreed & WRR, Verslag Toekomst multilaterale orde, p. 3. De EU zet ook in op actieve cyber-dialogen in deze zin onder meer met Japan en Zuid-Korea.
[20] Een van de eerste beleidsdocumenten was van de Europese Commissie/Hoge Vertegenwoordiger voor Buitenlandse Zaken en Veiligheidsbeleid, ‘Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU’, 13 september 2017. Zie verder: Europese Commissie, ‘Een Europese datastrategie’, COM(2020)66, 19 februari 2020; Europese Commissie, White Paper ‘On Artificial Intelligence - A European approach to excellence and trust’, 19 februari 2020; ‘A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem’, het door Duitse en Franse regering geïnitieerde GAIA-X project, oktober 2019, dat gebaseerd is op basis van beginselen van *sovereignty-by-design.*

Dit is actueel, gezien de aanzienlijke hoeveelheid EU-beleidsvoorstellen die een relatie met digitale autonomie hebben.[21] Dit geeft Nederland tevens een betere uitgangspositie om sturing te geven aan de honderden miljarden die de EU heeft gealloceerd voor digitale investeringen, zoals het Europese financieringsprogramma's voor onderzoek & ontwikkeling (*Horizon*), digitale innovatie (*Digital Europe*), uitrol van Europese digitale infrastructuur (*Connecting Europe Facility*), kern projecten waarbij zonder schending van het mededingingsrecht kan worden samengewerkt (*Important Projects of Common European Interest (IPCEI)*, en herstel van de crisis (*Resilience and Recovery Fund*).[22] Dit brengt Nederland eveneens in een betere uitgangspositie om de eigen agenda met Europese cofinanciering te verwezenlijken.

De ambitie om in Europa een voortrekkersrol te spelen en gesprekspartner te kunnen zijn, vergt dat op nationaal niveau een aantal fundamentele stappen moeten worden gezet.

2. Aanpak cybersecurity onvoldoende vanuit perspectief van strategische autonomie

De raad constateert dat cybersecurity tot nog toe vooral technisch en reactief wordt aangepakt en vrijwel niet vanuit het bredere perspectief van strategische autonomie. In Nederland staat digitale autonomie nog onvoldoende op de politieke agenda en overwegingen van digitale autonomie worden niet structureel meegenomen bij het opstellen van beleid en wetgeving. Regelgeving wordt nu vooral ingezet om verlies aan digitale autonomie te compenseren in plaats van verlies aan digitale autonomie te voorkomen. Een voorbeeld van het laatste is het recente voorstel van de Europese Commissie voor een Digital Markets Act,[23] die een voorzet doet om de digitale platformen die als poortwachter functioneren van de digitale wereld aan banden te leggen.

In een eerder advies constateerde de raad dat we als Nederland op dit moment onvoldoende inzicht hebben in onze nieuwe afhankelijkheden[24] en daardoor niet in staat zijn om voldoende proactief gecoördineerd technologiebeleid te kunnen voeren op het gebied van onderzoek, valorisatie en industriële capaciteiten.[25] Daarvoor is ook nodig dat bedrijven in Nederland in een florerend ecosysteem acteren; een ecosysteem waarin zij de mogelijkheid hebben om te groeien door voldoende toegang tot onder andere talent, data en financiering. Doordat de soevereiniteitsvraag steeds meer gebieden van economie, maatschappij en democratie raakt, dient aansturing centraal plaats te vinden. Hiervoor ontbreekt het volgens de raad aan de benodigde integratie van beleid en bijbehorende verantwoording. Het reactief handelen dient te worden gecombineerd met proactief monitoren en anticiperen, mede op basis van structurele rapportages aan de Tweede Kamer. Dit vergt dat verschillende beleidsterreinen en belangen hecht met elkaar worden verbonden, met sturing vanaf *het hoogste niveau* (‘*Whole-of-Government*’).

Landen zoals de VS, het Verenigd Koninkrijk en China koppelen hun strategische autonomie aan hun streven om op militair vlak autonoom en dominant te blijven. Ze hebben daartoe processen en middelen gecreëerd die continu de doelstellingen verbinden met de noodzakelijke middelen om ze te bereiken op een

[21] Relevant in dit verband is de in 2020 voorgestelde herziening van de Network & Information Security richtlijn (‘NIS2’) die cyberweerbaarheid betreft; alsook de in 2020 voorgestelde Digital Markets Act en Digital Services Act die regulering van grote digitale platformen betreffen en de voorgestelde Data Governance Act betreffende toegang tot en delen van Europese data. Relevante wetgeving die in 2021 verwacht wordt is de herziening van de EU-verordening aangaande elektronische identiteit/elektronische handtekening en andere ‘trust services’ (‘eIDAS2’) en nieuwe wetgeving aangaande hoog-risico toepassingen van artificiële intelligentie, alsook wetgeving over specifieke EU-data ruimtes (‘data spaces’) zoals voor gezondheidsdata.

[22] Omvang van digitale investeringen zoals specifiek vastgelegd betreffen tenminste €134.5 miljard in het Resilience & Recovery Fund, €7.5 miljard in het Digital Europe programma, ongeveer €3 miljard in Connecting Europe Facility en een aanzienlijk deel van de €83.9 miljard in Horizon Europe (in het verleden in de orde van 15%)

[23] The Digital Services Act package: https://ec.europa.eu/digital-single-market/en/digital-services-act-package

[24] Inmiddels is er geleidelijk wel meer aandacht voor dit onderwerp bij diverse departementen en loopt er een initiatief om de (geopolitieke) economische afhankelijkheden in kaart te brengen die ons land kwetsbaar maken. Momenteel wordt er door het kabinet gewerkt aan een methode om geopolitieke kwetsbare afhankelijkheden systematisch in beeld te brengen: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/02/10/tk-nationale-veiligheid-strategische-afhankelijkheden-en-planbureau/tk-nationale-veiligheid-strategische-afhankelijkheden-en-planbureau.pdf

[25] Reflecties over digitale soevereiniteit, Moerel en Timmers, 2020

gecoördineerde manier. Daarnaast gebruiken deze landen, maar ook Frankrijk, een strategische aanpak voor het stimuleren van hun technologische voorsprong en bestendigen die met financiële, regulerende en aankoopinstrumenten. Zo werkt de VS met een lijst van 'fundamentele en opkomende technologieën'. In een eerder advies[26] heeft de raad op de noodzaak voor het opstellen van een dergelijke lijst met sleuteltechnologieën aangedrongen.

3. Er is een belangrijk verschil in innovatieklimaat tussen Europa en de VS

Nederland had een historisch sterke positie in belangrijke deelgebieden van cybersecurity zoals cryptografie. Qua kennis is Nederland nog steeds sterk, ook in opkomende gebieden zoals kwantumtechnologie en AI. Maar de omzetting van die kennis in producten en diensten gebeurt veelal elders, terwijl die wel essentieel zijn voor de Nederlandse digitale autonomie in cybersecurity. Met name de VS en China zijn efficiënter in het omzetten van wetenschap naar markt en uiteindelijk dominantie. Ze schuwen daarbij ook niet om internationale standaarden in hun voordeel te beïnvloeden.[27]

Factoren die een gezonde Nederlandse (en Europese) bedrijvigheid in cybersecurity belemmeren is de geringe investeringsbereidheid in vergelijking met de VS en China, de kolonisatie van het innovatie-ecosysteem door de grote digitale platformen en het gebrek aan proactieve analyse vanuit het strategisch autonomie perspectief. De VS hebben bijvoorbeeld een gunstiger ecosysteem voor startups, dat zich uit in het netwerk van ondernemers en risico-investeerders en ook in het investeringsklimaat. Startups starten makkelijker en groeien sneller. Het is als startup in Europa moeilijk om risicokapitaal aan te trekken op het moment dat er nog geen jaarlijkse inkomsten in de boeken staan. En als een Europese startup succesvol is en verdere financiering nodig heeft, komt deze meestal uit de VS. Reden hiervoor is dat investeringstickets van meer dan EUR 100 mio zeer zeldzaam zijn in Europa.

Het risico voor overnames van succesvolle Europese high techbedrijven door partijen buiten Europa is dan ook erg groot. Amerikaanse bedrijven monitoren voortdurend nieuwe innovaties en startups, die zij vervolgens in een vroeg stadium overnemen en in het eigen aanbod integreren.[28] Hierdoor is er geen sprake meer van een *level playing field*, maar van ernstige marktverstoring. Als onderdeel van een geïntegreerde aanpak kunnen mitigerende maatregelen ook hier op een proactieve manier worden genomen, bijvoorbeeld door aanscherping van export- en overnamerestricties, gecombineerd met actieve overheidsdeelname in sleutelbedrijven, inclusief het selectief gebruik van middelen uit het nationale groeifonds.

De raad verwijst verder naar voorbeelden van mechanismen en processen die leiden tot een beter innovatieklimaat, zoals het VK (*Defence S&T Strategy, Govern Smarter*), Finland (*Business Finland*), Zwitserland (*Innovation climate*) en Italië (*National Cybersecurity Perimeter*).

4. Drie basisvoorzieningen

De raad adviseert de volgende drie basisvoorzieningen met voorrang op te pakken om onze positie zowel in eigen land als in Europa te versterken. Deze basisvoorzieningen dienen te worden ingebed in of op zijn minst bij te dragen aan het Europese beleid. Realisatie van deze basisvoorzieningen vergt nauwe samenwerking en afstemming tussen de overheid en de technologische industrie. Belangrijke factor voor succes van dit beleid zal zijn transparantie en voorspelbaarheid waarin de overheid wil investeren en innoveren, alsmede een duidelijk kader voor hoe partijen binnen de mededingingsregels kunnen samenwerken.

[26] CSR Advies 'Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland', CSR Advies 2020, nr. 5, september 2020

[27] Paul Timmers, Geopolitics of Standardisation, 9 april 2020, https://directionsblog.eu/the-geopolitics-of-standardisation/

[28] De strategie van de grote techbedrijven om competitie in de kiem te smoren door stelselmatig innovatieve startups op te kopen, wordt inmiddels onderzocht door de Amerikaanse FTC.

Dit vergt tevens dat de overheid vanuit overwegingen van digitale soevereiniteit haar inkoopkracht actief inzet en vol gebruikmaakt van de mogelijkheden om te sturen op andere factoren dan laagste kosten.

- **Soevereiniteit respecterende cloud:**
  De cloud wordt de centrale infrastructuur voor bedrijven en publieke diensten. Dit geldt ook voor onze gevoelige toepassingen, variërend van de COVID-19 aanpak, opsporing van criminelen tot het beheer van de Rotterdams haven. Om op grote schaal gebruik te kunnen maken van data-analyse door middel van AI is enorme rekenkracht vereist. De cloud-infrastructuur die hiervoor is benodigd, wordt snel het fundament voor de Nederlandse en Europese innovatie- en kennisinfrastructuur. Daarover zeggenschap houden, is een wezenlijk deel van de Nederlandse strategische autonomie.[29] De huidige marktdynamiek kenmerkt zich door enkele dominante buitenlandse techbedrijven. De afhankelijkheid van niet-Europese aanbieders brengt controle van andere landen mee, die andere spelregels hanteren wat betreft bijvoorbeeld spionage, privacy en afgifte van data. De overheid dient te komen tot een visie op een geïntegreerd en bindend cloud-kader voor uitbesteding en haar inkoopkracht actief inzetten om nationale cloud-initiatieven te stimuleren die aan de Europese cloud-initiatieven bijdragen, waarvan al een aantal loopt.[30]

- **Veilige digitale communicatienetwerken voor heel Nederland**:
  We zijn in toenemende mate afhankelijk van digitale communicatie voor het welzijn van burgers en voor een sterke economie. Denk aan video-vergaderen, en *smart homes*, maar ook aan nieuwe veiligheids-kritische diensten zoals *smart energy grids*, intelligente mobiliteitssystemen en op afstand bedienbare zorgrobots. De ontwikkeling en het beheer van de onderliggende technische systemen en -netwerken (zoals routers, switches, DNS-servers) worden steeds vaker gedomineerd door buitenlandse partijen. Hierdoor hebben organisaties en individuen slechts een beperkt inzicht in hun afhankelijkheden van deze partijen en hun systemen, laat staan dat ze daar controle over hebben. Dit beperkt onze mogelijkheden om autonoom te beslissen en te handelen over hoe we onze digitale infrastructuur inrichten en aan welke partijen we het transport van onze data toe willen vertrouwen. In een aantal landen gaat *quantum key distribution* ingezet worden voor essentiële communicatie van overheid, defensie en financiële wereld. Nederland moet daarin deelnemen en ambiëren een van de leiders te worden. Nederland moet ook op wereldniveau inzetten op en bijdragen aan een *responsible internet*. Hiervoor dient een actieplan te worden opgesteld om gebruikers inzicht te geven in de netwerkinfrastructuur die hun data en communicatie transporteren (zoals machtsconcentraties en *single-points-of failure*). Ook moet dit actieplan hen extra security-gerelateerde handelingsmogelijkheden bieden waaronder authenticatie en digitale ondertekening. Daarmee krijgen zij meer grip op hun afhankelijkheden van het internet om zo hun vertrouwen in en controle over internetcommunicatie te verhogen.[31]

- **Post-kwantumcryptografie**:
  Zonder cryptografie is er geen bescherming van de meest gevoelige overheidsinformatie, industriële geheimen van bedrijven en persoonlijke informatie van burger. De encryptie zoals we die kennen, wordt inmiddels gehackt door statelijke actoren, gecontroleerd door dominante marktspelers van buiten de EU en zal binnen enkele jaren te kraken zijn met kwantumcomputing.

[29] Reflecties over digitale soevereiniteit, Moerel en Timmers, 2020. Zie ook de Duitse 'Industrial Strategy 2030. Guidelines for a German and European industrial policy', waarin men erkent dat onvoldoende grip op nieuwe technologieën een direct risico betekent voor het behoud van de technologische soevereiniteit van de Duitse economie.

[30] Inmiddels hebben Nederlandse cloud, hosting en infrastructuur bedrijven een coalitie gesloten om aan GAIA-X te kunnen bijdragen: http://www.tno.nl/nl/over-tno/nieuws/2020/11/nederlandse-cloud-infrastructuur-coalitie-cic-eerste-stap-naar-slagvaardig-digitaal-nederland

[31] Zie voor een eerste aanzet: A Responsible Internet to Increase Trust in the Digital World, https://www.sidnlabs.nl/downloads/2v6sEqlLniFGTWbbKqTvhx/ee9f96134c0607c67efe40940039cd76/Hesselman_et_al-2020-Journal_of_Network_and_Systems_Management.pdf

De overheid dient te investeren in post-kwantumcryptografie, waarmee we bedoelen digitale beveiligingsdiensten en -oplossingen die langdurige bescherming van gevoelige informatie kunnen garanderen, ook als nieuwe technologieën, en toepassingen opkomen en cyberaanvallen evolueren.

Bovenstaande basisvoorzieningen zijn een *conditio sine qua non* voor het borgen van onze digitale soevereiniteit. De investeringen in deze basisvoorzieningen en de daarbij behorende kennis zijn tegelijkertijd ook een enorme kans voor de Nederlandse ICT- en internetindustrie, die traditioneel sterk is op dit gebied. Nederland heeft een toppositie in kwantumtechnologie. Verder is AMS-IX een van de grootste internet-knooppunten ter wereld, is .nl een van de grootste en veiligste landen top-level domeinen ter wereld en hebben we een grote hostingsector. Met de basis op orde en onze internationaal erkende kwaliteiten in bestuur, democratie, en diplomatie is het een reële ambitie dat Nederland de beste digitale toegangshaven tot Europa biedt; het land met de beste digitale bescherming van kennis en gevoelige informatie en dat ook het grootste vertrouwen heeft van burgers en bedrijven om deel te nemen aan de digitale maatschappij. De voorzieningen dragen alleen bij aan onze soevereiniteit als we de maatregelen combineren. De genoemde studie en het toetsingskader laten zien hoe dit aan te pakken.

ADVIEZEN

Digitale autonomie raakt het hart van onze samenleving. We moeten daarom weerbaar zijn en proactief en gecoördineerd kunnen anticiperen op onze (digitale) toekomst. De raad adviseert om *vooruitlopend* op de uitwerking en implementatie van zijn eerdere adviezen, zonder uitstel een aantal concrete zaken in gang te zetten, omdat deze naar oordeel van de raad niet op uitwerking van vorenbedoeld beleid kunnen wachten. De volgende acties zijn op korte termijn noodzakelijk om onze positie te versterken:

1. **Implementeer een toetsingskader digitale autonomie cybersecurity.**
2. **Borg drie basisvoorzieningen voortuitlopend op nationale strategie- en beleidsvorming.**
3. **Verhoog bewustwording van het belang van strategische autonomie in cybersecurity.**
4. **Verbeter het valorisatie- en innovatieklimaat in Nederland.**
5. **Zet actief in op aansluiting bij EU-beleid en EU-financiering.**

Ad 1. Implementeer een toetsingskader digitale autonomie cybersecurity.

De raad zal een voorstel voor een '*Handreiking toepassing toetsingskader digitale autonomie en cybersecurity*' beschikbaar maken. Ter ondersteuning zal een aantal raadsleden interdepartementale workshops organiseren. Deze handreiking met het toetsingskader zou voor de beleidsontwikkeling en wetsvoorbereiding urgent beschikbaar moeten worden gemaakt. Alleen zo kan worden voorkomen dat soevereiniteit een *after-thought* blijft. De raad adviseert gebruik te maken van dit toetsingskader en gaandeweg het gebruik van de methodes en doelstellingen uit te breiden. Een dergelijk kader kan een grote bijdrage leveren aan het (op voorhand) inschatten van mogelijke risico´s voor digitale soevereiniteit en schept de mogelijkheid hier tijdig en in samenhang op te anticiperen.

Ad 2. Borg drie basisvoorzieningen vooruitlopend op nationale strategie- en beleidsvorming.

De volgende drie onderwerpen dienen met voorrang te worden aangepakt om strategische autonomie in de basisinfrastructuur voor economie, maatschappij en democratie te realiseren:

- Soevereiniteit-respecterende cloud voor veilige dataopslag en data-analyse
- Veilige digitale communicatienetwerken
- Post-kwantumcryptografie

In de bijlagen van dit advies heeft de raad hiervoor een aanzet gedaan.

Ad 3. Verhoog bewustwording van het belang van strategische autonomie in cybersecurity.

Het belang van strategische autonomie in cybersecurity is tot nog toe onvoldoende onderkend op alle relevante niveaus van de Nederlandse overheid, politiek, bedrijfsleven en wetenschap, maar ook bij onze belangrijkste partners in de EU. Digitale autonomie begint met kennis en begrip zodat alle partijen acties kunnen ondernemen om de digitale gevaren te elimineren of te minimaliseren. We moet ons bewust zijn van de ontwikkelingen, uitdagingen en behoeften rond digitale autonomie. Gezien de urgentie en het belang van het onderwerp zal de raad actief inzetten op verspreiding van dit advies en de studie en een aantal workshops organiseren.

Ad 4. Verbeter het valorisatie- en innovatieklimaat in Nederland.

Ons valorisatie- en innovatieklimaat dient sterk te worden verbeterd. Dit vraagt een andere organisatie en aansturing. Hierbij kunnen voorbeelden van mechanismen en processen uit andere landen inspirerend werken, zoals in landen als de VS (*Darpa, In-Q-Tel*), het VK (*Defence S&T Strategy, Govern Smarter*), Finland (*Business Finland*), Zwitserland (*Innovation climate*) en Italië (*National Cybersecurity Perimeter*).

Aanbeveling is verder om structurele ondersteuning te geven aan het borgen van de academische expertise die is vereist om claims van leveranciers van sleuteltechnologieën onafhankelijk te kunnen valideren (*trust validators*). Ook ondersteunende maatregelen voor nieuwe ondernemingen via 'slimme' aankoopprocedures, overheid als *launching customer* en gerichte innovatieondersteuning zijn middelen om valorisatiekansen te verbeteren. Verder kan gedacht worden aan invoering van beschermende maatregelen, zoals aanscherping interne marktcondities en export- en overnamerestricties gecombineerd met actieve overheidsdeelname in sleutelbedrijven, inclusief het selectief gebruik van middelen uit het nationale groeifonds.

Ad 5. Zet actief in op aansluiting bij EU-beleid en EU-financiering.

Nederland kan in het EU-beleid een aanjagersrol spelen door ervoor te zorgen in het Nederlandse beleid haar eigen visie van digitale autonomie expliciet te maken en deze visie en aanpak als bijdrage in het EU-beleid in te brengen. Nederland zou daarmee - net als voorlopers Duitsland en Frankrijk - helderheid creëren en zich versterken als gesprekspartner. Dit is actueel, gezien de aanzienlijke hoeveelheid EU-beleidsvoorstellen die een relatie met digitale autonomie hebben.[32] Dit geeft Nederland tevens een betere uitgangspositie om sturing te geven aan de honderden miljarden die de EU heeft gealloceerd voor digitale investeringen, zoals de Europese financieringsprogramma's voor onderzoek & ontwikkeling (*Horizon*), digitale innovatie (*Digital Europe*), uitrol van Europese digitale infrastructuur (*Connecting Europe Facility*). Denk daarbij ook aan de kernprojecten waarbij zonder schending van het mededingingsrecht kan worden samengewerkt (*Important Projects of Common European Interest (IPCEI),* en herstel van de crisis (*Resilience and Recovery Fund*).[33] Dit brengt Nederland eveneens in een betere uitgangspositie om de eigen agenda met Europese cofinanciering te verwezenlijken.

[32] Relevant in dit verband is de in 2020 voorgestelde herziening van de Network & Information Security richtlijn ('NIS2') die cyberweerbaarheid betreft; alsook de in 2020 voorgestelde Digital Markets Act en Digital Services Act die regulering van grote digitale platformen betreffen en de voorgestelde Data Governance Act betreffende toegang tot en delen van Europese data. Relevante wetgeving die in 2021 verwacht wordt is de herziening van de EU-verordening aangaande elektronische identiteit/elektronische handtekening en andere 'trust services' ('eIDAS2'), de nieuwe wetgeving aangaande hoog-risico-toepassingen van artificiële intelligentie, alsook wetgeving over specifieke EU-data ruimtes ('dataspaces') zoals voor gezondheidsdata.

[33] Omvang van digitale investeringen zoals specifiek vastgelegd betreffen tenminste €134.5 miljard in het Resilience & Recovery Fund, €7.5 miljard in het Digital Europe programma, ongeveer €3 miljard in Connecting Europe Facility en een aanzienlijk deel van de €83.9 miljard in Horizon Europe (in het verleden in de orde van 15%).

GERICHTE ADVIEZEN

De adviezen van de raad zijn gericht op de overheid en via de overheid ook op het bedrijfsleven. Alleen als er beter wordt samengewerkt tussen de publieke sector, de private sector en kennisinstellingen kan de digitale autonomie met betrekking tot cyberweerbaarheid ook in de toekomst worden gegarandeerd en kan de Nederlandse samenleving ook in de toekomst vertrouwen op de veiligheid en continuïteit van onze digitale maatschappij.

Advies van de raad aan de demissionair minister-president:

1. Beleg nog dit jaar de verantwoordelijkheid voor onze digitale autonomie op het hoogst mogelijke niveau[34] en neem aandacht voor digitale autonomie structureel mee in de voorbereiding op de vergadering van de ministerraad.
2. Organiseer strategische autonomie in cyberveiligheid als een continue, proactieve, en geïntegreerde activiteit op politiek en beleidsuitvoerend niveau.
3. Draag de adviezen over aan het komende kabinet zodat de continuïteit van de gerichte adviezen wordt geborgd.
4. Voer in 2022 een jaarlijkse overzichtsrapportage digitale autonomie in, bij voorkeur als onderdeel van een bestaande rapportage.

De raad adviseert de demissionair minister van Justitie en Veiligheid, de demissionair staatssecretaris van Economische Zaken en Klimaat en de demissionair staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties gezamenlijk om in samenwerking met de belangrijkste stakeholders (publiek, privaat en wetenschap)[35] de volgende acties in gang te zetten:

5. Implementeer voor eind 2021 het ‘Toetsingskader digitale autonomie en cybersecurity’ ten behoeve van beleid en wetgeving en ondersteun de implementatie met workshops.
6. Inventariseer in 2021 de (digitale) afhankelijkheden en definieer concrete doelstellingen voor de strategische controle in cyberveiligheid. Gebruik hierbij het voorgestelde toetsingskader.
7. Neem een vooraanstaande positie in binnen de EU op basis van de eigen visie over digitale autonomie waardoor tevens een gericht beroep kan worden gedaan op Europese cofinanciering.
8. Zet direct actief in op de verhoging van het bewustzijn van nut en noodzaak van digitale autonomie bij zowel publieke als private partijen.
9. Coördineer de verwezenlijking van de drie genoemde basisvoorzieningen, zie voor een aanzet bijlage 1 van dit rapport.

[34] CSR Adviesrapport ‘Integrale aanpak voor cyberweerbaarheid’, CSR Advies 2021, nr. 2
[35] Zoals ook benoemd in de brief van staatssecretaris Keijzer van het ministerie van Economische Zaken en Klimaat, gericht aan de voorzitter van de Tweede Kamer der Staten-Generaal inzake 'Resultaten verkenningen en vervolgaanpak cybersecurity kennisontwikkeling en innovatie', dd. 9 april 2020.

10. Stimuleer de verdere ontwikkeling van kennis en innovatie op het gebied van digitale autonomie en sluit daarbij aan bij de Europese ontwikkelingen. Zet deze acties in 2021 in gang op basis van een integrale aanpak.
11. Zet daarbij actief in op valorisatie en de creatie van een gunstig innovatieklimaat met focus op digitale autonomie en cybersecurity.

De raad adviseert de demissionair minister van Onderwijs, Cultuur en Wetenschap om in samenwerking met de belangrijkste stakeholders de volgende actie in gang te zetten:

12. Zet nog dit jaar actief in op kennisontwikkeling en kennisbehoud met betrekking tot het cyberdomein. Stimuleer hoogwaardig onderwijs en onderzoek zodat ons land over een stevige kennispositie en voldoende gekwalificeerd personeel kan beschikken.

De raad adviseert de demissionair staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties om in samenwerking met de belangrijkste stakeholders de volgende acties in gang te zetten:

13. Stem het Rijksinkoopbeleid af op de behoeften die voortvloeien uit de noodzaak tot digitale autonomie.
14. Stimuleer een dergelijke aanpak ook voor de decentrale overheden.

’s-Gravenhage,
Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR

BIJLAGEN

In deze bijlagen wordt een aanzet gegeven tot het verwezenlijken van de drie basisvoorzieningen. Verdere (beleids)ontwikkeling vraagt om nadere detaillering en validatie.

BIJLAGE 1: OVERZICHT CYBERWEERBAARHEID STAKEHOLDERVELD

Doelstelling 1: Soevereiniteit-respecterende cloud

Met soevereiniteit-respecterende cloud bedoelen we een cloud-infrastructuur en -dienstverlening die de gegevens en processen in de cloud beschermt tegen toegang door ongeoorloofde derden en die de toekomstige toegevoegde waarde uit data-analyse (AI) en vertrouwensdiensten in eigen handen houdt.

Huidige triggers in verband met strategische autonomie en cybersecurity:

- Toenemende dominantie en *lock-in*-ambities van de grote *hyperscalers*.
- Dreiging van ongeoorloofde gegevenstoegang door derden in cloud-projecten met impact op het functioneren van en vertrouwen in de staat.
- Wettelijke ontwikkelingen (Cloud Act en cloud-leveranciers meldplicht VS, Schrems II) en cloud-beleidsontwikkelingen in EU (GAIA-X, data spaces, AI).
- Technische ontwikkelingen in privacybeschermende gegevensverwerking.

Cloud wordt de centrale infrastructuur voor de meeste bedrijven en publieke diensten. De huidige marktdynamiek is gekenmerkt door enkele partijen (Microsoft, Amazon, Google, Alibaba), die ook een grote greep op het kennis-ecosysteem hebben. Bovendien wordt data erkend als een ‘grondstof’ en van essentieel belang voor toekomstige welvaart en welzijn van een land. Ook hier zien we een strijdtoneel ontstaan waar de grote spelers (Google, Apple, Facebook en de Chinese partijen, zoals Alibaba en ByteDance) het onder elkaar uitvechten. Tegenspel kan komen van overheid, klant en regelgever en opkomende gerelateerde industrie (AI, eID, edge computing, nieuwe vormen van encryptie).

Data en processen in de cloud zouden ingebouwd beschermd moeten zijn tegen ongeoorloofde of ongemerkte toegang door derde partijen, zoals de leverancier van de infrastructuur, de overheid, markteers of criminelen. Wetgeving, zoals *General Data Protection Regulation (GDPR)*, geeft al een zekere bescherming maar die berust op respectvolle implementatie en handhaving. Het zou beter zijn om de bescherming op een betrouwbare en valideerbare manier in te bedden in de technologie die de data en processen herbergt.

Doelstelling:
Voldoende controle te krijgen ten opzichte van de cloud-aanbieders en hun controlerende overheden als het gaat over de toegevoegde waarde in diensten en data en de komende cloud-generatie, zoals industriële cloud, en dit te realiseren tegen 2025. Het is in dit stadium niet de inzet en zelfs een illusie om de controle over de grote cloud-platforms terug te winnen.

Voorbeelden van mogelijke maatregelen, mede in EU-verband:

Politiek, beleid en organisatie:

- Een eenduidig en coherent en verplichtend cloud-beleid van de overheid dat ook doorgetrokken wordt naar (gecoördineerd) aankoopbeleid, eventueel exploitatie randvoorwaarden, ten laatste in 2022.
- Deelname aan voor ons land veelbelovende Europese cloud-projecten, vanaf eind 2021.
- Actieve bijdrage aan EU-beleid en EU-wetgeving (NIS2, eIDAS2, DMA, DSA, AI, cloud, data spaces), inclusief strategische autonomie perspectief, per direct.
- Overheid als *launching customer* van nieuwe privacybeschermende cloud-oplossingen in gebieden zoals justitie/politie en gezondheid.[36]

Kennis, R&D, Industrie:

- Prioritering en samenhang van Nederlandse ondersteuning van onderzoek en innovatie in relevante domeinen, vast te leggen in 2022. Nederland brengt deze prioriteit in de Europese programma's Horizon Europe, Digital Europe, CEF en EU4Health.
- Actieve en doelgerichte ondersteuning van innovatie, monitoring van groei-investeringen in de relevante startups, interactie met gebruikers in industriële sectoren, zoals logistiek, defensie en gezondheid om bewustwording en vrijmaking van middelen te bevorderen.
- Financiële ondersteuning met lange termijnperspectief van academische expertise die trust van cloud-technologie kan valideren en verzekeren. Promotie van het gebruik van privacybeschermende cloud-oplossingen in het bedrijfsleven in gebieden als logistiek.

[36] Waar geen opleverdatum genoemd wordt, is de maatregel bedoeld vanaf 2022 (of z.s.m.).

Doelstelling 2: Veilige landelijke communicatie

Met veilige landelijke communicatie bedoelen we het aanbieden van internetconnectiviteit en dienstverlening met ingebouwde cybersecurity over het hele land.

Huidige triggers in verband met strategische autonomie en cybersecurity:

- Verbreding van de digitale dreiging over het hele land, naar organisaties die minder cyberweerbaar zijn maar daarom niet minder belangrijk (bv. gezondheidssector).
- Invoering van nieuwe technologie (5G en IoT) technologie vergroten de 'attack surface'.
- Voor essentiële data is landelijke veilige communicatie *conditio sine qua non*.
- Prijsconcurrentie van netwerkoperatoren, die aankoop van minder betrouwbare netwerkapparatuur en inkorten op de veiligheid in de hand werkt.
- Mogelijke buitenlandse overnames van kritische netwerkinfrastructuur.
- Opkomst van nieuwe technologieën (OpenRAN, quantum key distribution).

Cyberdreigingen via de digitale communicatienetwerken raken nu vrijwel alle economische en maatschappelijke partijen. COVID-19 laat zien dat we nieuwe kritische data en toepassingen moeten beschermen en wel over het hele land. De digitale communicatie-infrastructuur is fundamenteel aan het veranderen met 5G en Internet of Things en wordt meer gedistribueerd, dynamischer en flexibeler. EU-wetgeving voorziet al een aanzienlijke uitbreiding van wettelijke cybersecurityverplichtingen, maar dit is niet voldoende om het gebrek aan maturiteit en weerbaarheid van de meeste bedrijven en organisaties te compenseren. Meer veiligheid inbouwen in het netwerk waar die bedrijven en organisaties mee communiceren met de buitenwereld kan daar voor een deel het cyberrisico verminderen. De EU zet ook aanzienlijk in op kwantum-communicatie en de volgende generaties (6G).

De noodzaak voor cybersecurity, algemene markt-wetgeving en het gericht samenwerken van de overheid met de aanbieders van veilige communicatie kan betekenen dat de overheid sterker in de markt ingrijpt. Indien dit concurrentieverstorend zou zijn, moet het duidelijk in het landsbelang zijn.

Doelstelling:
Voorzie uiterlijk in 2025 een landelijke, ingebouwd veilige en stabiele *end-to-end* digitale communicatie als ruggengraat van economie, maatschappij en democratie. Begeleid dit met gerichte sensibilisering en ondersteuning van de brede bevolking en alle geledingen van de economie.

Voorbeelden van mogelijke maatregelen:

Politiek, beleid en organisatie:

- Integraal plan voor landelijke, veilige en stabiele *end-to-end* digitale communicatie, in 2022.
- Uitbreiding van de functionaliteit en de dekking van het Nationale Detectie Netwerk (volledig in 2025).
- Nationale bewustwordingscampagnes.
- Selectief dreigingsinformatie delen met de telecom-operatoren.
- Leg op nationaal niveau veiligheidseisen op aan telecom, gebaseerd op EU-wetgeving (NIB, telecom wet, certificatie als in EU Cyber Act), uitgebreid met ingebouwde veiligheidseisen.
- Implementeer veilige *end-to-end*-netwerken in alle overheidsactiviteiten, met *backbone*-bescherming gebaseerd op Quantum Key Distribution 2025.
- Zie actief toe op M&A/FDI bij telecomleveranciers.
- Maak investeren in cybersecurity aantrekkelijk voor bedrijven en burgers, bijvoorbeeld fiscaal.

Kennis, R&D, Industrie:

- Prioritering van Nederlandse ondersteuning van onderzoek en innovatie in relevante domeinen (netwerkbeveiliging, optische en kwantumcommunicatie, *Quantum Key Distribution*, 6G) in 2022.
- Actieve en doelgerichte ondersteuning van innovatie, monitoring van groei-investeringen in relevante startups, interactie met gebruikers in telecomoperatoren om bewustwording en vrijmaking van middelen te bevorderen.
- Opzetten van 5G-flagships in Nederland (bijv. logistiek, gezondheid, industrie).
- Actieve participatie in standaardisatie van 5G/6G.

Doelstelling 3: Post-kwantumcryptografie

Met *'post-kwantumcryptografie'* bedoelen we digitale beveiligingsdiensten en -oplossingen die langdurige bescherming van gevoelige informatie kunnen garanderen, ook als nieuwe technologieën, en toepassingen opkomen en cyberaanvallen evolueren. De doelgroep van post-kwantumencryptie is de overheid en de high techindustrie (bescherming van intellectuele eigendom).

Huidige triggers in verband met strategische autonomie en cybersecurity:

- Nieuwe technologieën die de huidige encryptie onveilig maken (kwantumcomputing).
- Groeiende dreiging van spionage door staten (overigens, van vijand en vriend).
- Het verdwijnen van relevante maakindustrie in Nederland.
- Nieuwe technieken (homomorf, post-kwantum) die langer, of zelfs onbeperkte zekerheid geven.

Post-kwantumencryptie-oplossingen zijn sterk verbonden met strategische autonomie. Nederland heeft stelselmatig de controle verloren door het verdwijnen van maakindustrie en een marktgerichte aanpak. Het terugwinnen van volledige controle is onrealistisch. Samenwerking met enkele *like-minded* partnerlanden zal noodzakelijk zijn. Samenwerking in EU of mondiaal verband is in dit dossier enkel zinvol wat betreft het beïnvloeden van betrouwbare standaards en bijbehorende certificering. Het is niet haalbaar om in deze materie op een brede geografische basis voldoende vertrouwen te hebben in de maak- en leveranciersketen.

Doelstelling:
Maak een selectie van operationele en gevalideerde post-kwantumoplossingen (producten, diensten en expertise) beschikbaar voor de Nederlandse overheid en geselecteerde private partijen (hightechindustrie en -wetenschap), vanaf 2022.

Voorbeelden van mogelijke maatregelen:

<u>Politiek, beleid en organisatie</u>:

- Een eenduidig, coherent en langdurig overheidsencryptiebeleid, doorgetrokken naar (gecoördineerd) aankoopbeleid en uitzonderingsclausules voor veiligheidsredenen overheidsaanbestedingen (art. 346 TFEU) om een stabiele markt voor maakindustrie te bevorderen, per 2023.
- Overheid als *launching customer* van nieuwe encryptie-oplossingen.
- Actief toezien op M&A/FDI bij encryptie-leveranciers.
- Sterke en betrouwbare partnerships met partnerlanden, zoals Frankrijk, Duitsland en Zwitserland, die wel nog een relevante maakindustrie hebben, vanaf 2023.

<u>Kennis, R&D, Industrie</u>:

- Langdurige financiële ondersteuning van academische expertise voor trust validatie. Opzetten en implementeren van een programma van testing/validatie van oplossingen, per 2023.
- Stimuleer expertise en ondernemersappetijt voor nieuwe maakindustrie indien er voldoende markt aanwezig zou zijn, gecombineerd met processen en werktuigen die ingezet kunnen worden om autonomie te versterken (defensie-industrie strategie, Nationaal Groeifonds).
- Gerichte financiële ondersteuning van O&O met als bewust objectief om ook innovatie en maakindustrie op te bouwen in Nederland, desgevallend in enkele goed gekozen domeinen.
- Actieve participatie of ten minste van nabij volgen van standaardisatie van post-kwantumencryptie-algoritmes (NIST etc.).

BIJLAGE 2: VOORBEELD UITWERKING VAN VERANTWOORDELIJKHEDEN

Het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' geeft aan de verantwoordelijkheden te beleggen bij de ministeriele commissie onder voorzitterschap van het ministerie van Algemene Zaken (AZ) voor de integratie van digitale autonomie voor cybersecurity op basis van een centrale nationale cyberweerbaarheidsstrategie. Voor verantwoordelijkheden voor specifieke taken ligt het voor de hand te bouwen op bestaande sterktes en taken. Voorbeelden van dergelijke taken, bouwend op de drie prioriteiten en maatregelen in de voorgaande bijlage, betreffen in brede zin de ontwikkeling van industriebeleid op deelterreinen. Treedt daarnaast zoveel mogelijk op als *launching customer*.

Een algemene taak is het financieren van grote interventies, bijvoorbeeld vanuit het Nationaal Groeifonds.

Meer specifiek taken:

- Nieuwe privacybeschermende cloud-oplossingen in gebieden zoals justitie/politie en gezondheid.
- Integraal plan voor landelijke, veilige en stabiele *end-to-end* digitale communicatie, in 2022.
- Uitbreiding van de functionaliteit en de dekking van het Nationale Detectie Netwerk, volledig in 2025.
- Verdere ontwikkeling van selectief dreigingsinformatie delen met de telecomoperatoren.

Tevens:

- Een eenduidig en coherent en verplichtend cloud-beleid van de overheid dat ook doorgetrokken wordt naar (gecoördineerd) aankoopbeleid, eventueel exploitatie randvoorwaarden, ten laatste in 2022.
- Implementatie veilige *end-to-end*-netwerken in alle overheidsactiviteiten, met *backbone*-bescherming gebaseerd op Quantum Key Distribution 2025.
- Een eenduidig, coherent en langdurig overheidsencryptiebeleid, doorgetrokken naar (gecoördineerd) aankoopbeleid en uitzonderingsclausules voor veiligheidsredenen bij overheidsaanbestedingen (art. 346 TFEU) om een stabiele markt voor maakindustrie te bevorderen, per 2023.

Voorbeeldtaken binnen het EU- en internationale kader zijn:

- Deelname aan GAIA-X, vanaf eind 2021;
- Sterke en betrouwbare partnerships met partnerlanden zoals Frankrijk, Duitsland en Zwitserland die wel nog een relevante maakindustrie hebben, vanaf 2023.