Universiteit Utrecht

Reflecties over digitale soevereiniteit

Preadvies Staatsrechtconferentie 2020

prof. dr. Lokke Moerel, prof. dr. Paul Timmers[1]

[1] Lokke Moerel is hoogleraar Global ICT Law (Tilburg University) en lid van de Cyber Security Raad. Paul Timmers is research associate aan de Universiteit van Oxford en hoogleraar aan de European University Cyprus.

Samenvatting

De term digitale soevereiniteit komt steeds vaker voor in de media en heeft dan een variëteit aan betekenissen. In dit preadvies nemen de auteurs het begrip digitale soevereiniteit onder de loep. Zij concluderen dat digitale soevereiniteit niet is beperkt tot het hebben van controle van een Staat over het gebruik en inrichting van kritieke digitale systemen en de daarmee gegenereerde en opgeslagen data, maar ook moet worden vertaald naar het bredere staatsbelang van ***economie*** *(controle over essentiële economische ecosystemen) en* ***maatschappij*** *en* ***democratie*** *(vertrouwen in het rechtssysteem en kwaliteit van democratische besluitvorming). De auteurs geven een concreet overzicht met voorbeelden van de oorzaken waarom digitale soevereiniteit van de Nederlandse Staat onder druk staat, waaronder (i) de toenemende afhankelijkheid van overheidsinstanties en aanbieders van vitale infrastructuren van digitale infrastructuur die grotendeels in handen is van een beperkt aantal dominante buitenlandse marktspelers; (ii) de toenemende cyberdreigingen van onze vitale infrastructuur, systematische diefstal van intellectuele eigendom van onze kennisintensieve bedrijven, digitale afpersing, doelgerichte misinformatie en systematische infiltratie van sociale media om verkiezingen en democratische processen te beïnvloeden; en (iii) de toenemende geopolitieke spanningen, die leiden tot extraterritoriale claims van vreemde mogendheden, zoals export control beperkingen op technologie opgelegd door vreemde mogendheden en toegang door vreemde mogendheden tot data van Europese burgers en bedrijven.*

De auteurs analyseren de beleidsmatige en staatsrechtelijke implicaties van de gesignaleerde knelpunten zowel op mondiaal, EU als Nederlands niveau. Drie case studies worden besproken waar Europese regelgeving onvoldoende de Europese (en daarmee Nederlandse) digitale soevereiniteit ondervangt: (i) de Europese voorstellen terzake van een Europese cloud infrastructuur, (ii) de Europese Netwerk- en Informatiebeveiliging Richtlijn; en (iii) de Europese Richtlijn voor erkenning van elektronische authenticatie middelen van burgers (zoals het Nederlandse DigiD). De auteurs dragen oplossingen aan die passen binnen het huidige kader van internationaal, Europees en nationaal recht. Belangrijke constatering is dat het Europese mandaat om de benodigde vorm van soevereiniteit te borgen beperkt is. Digitale soevereiniteit raakt al gauw aan de nationale veiligheid van lidstaten, dat onder de EU Verdragen juist is voorbehouden aan de lidstaten. Waar de lidstaten ieder voor zich hun soevereiniteit niet langer kunnen beschermen, ondermijnt het beperkte ***Europese*** *mandaat om* ***nationale*** *soevereiniteit te bewaken, juist de* ***nationale*** *veiligheid. Voorstellen worden gedaan hoe de Europese wettelijke basis voor EU-soevereiniteit kan worden versterkt. Doordat de soevereiniteitsvraag steeds meer gebieden van economie, maatschappij en democratie raakt, dient aansturing centraal plaats te vinden. De departementen van de ministeries opereren echter vooral in silo's waardoor de benodigde integratie van beleid ontbreekt. Op dit moment bestaat zelfs onvoldoende inzicht in de nieuwe afhankelijkheden om überhaupt in staat te zijn een geïntegreerd en proactief beleid te kunnen voeren op het gebied van onderzoek, valoratie en industrie. Het ligt voor de hand op z'n minst een coördinator digitale zaken aan te stellen onder directe aansturing van de minister-president, met eigen budget en doorzettingsmacht. Zonder centrale aansturing zal ons land terecht komen op een onomkeerbaar pad van geleidelijke erosie van onze nationale technologische en industriële capaciteiten.*

1. Inleiding

1. De term *digitale soevereiniteit* komt steeds vaker voor in de media en heeft dan een variëteit aan betekenissen.[2] Eén interpretatie is het vermogen van nationale staten om zeggenschap te hebben over de digitale infrastructuur op hun grondgebied en de data van hun burgers. We zien echter dat het begrip in steeds bredere context wordt gebruikt. De digitale technologieën zijn inmiddels het slagveld voor de wedijver om mondiaal leiderschap en leiden tot steeds groter wordende geopolitieke spanningen tussen de VS en China (ook wel: de *tech cold war*).[3] De strijd gaat dan vooral over het leiderschap op het gebied van 5G, computer chip technologie, en *Artificial Intelligence* (**AI**). Zowel de VS als China trekken in dat verband regelmatig de *soevereiniteits*-kaart. President Trump vaardigde onlangs een verbod uit op populaire Chinese apps– zoals TikTok en WeChat – omdat deze de "*national security, foreign policy and economy"* van de VS zouden ondermijnen.[4] Dergelijke maatregelen worden *geframed* als noodzakelijke bescherming van Amerikaanse burgers tegen de ongebreidelde verzameling van hun data door de Chinese overheid.[5] De VS staan niet alleen, ook de Indiase overheid kondigde aan grote aantallen Chinese consumenten apps te verbieden, waaronder TikTok, eveneens omdat deze een "*threat to sovereignty and integrity*" zijn en de *nationale veiligheid* ondermijnen.[6]

2. Ander voorbeeld is de Amerikaanse ban van Huawei als leverancier van Amerikaanse telecominfrastructuur. In aanvulling daarop is Huawei nu ook beperkt in de mogelijkheid om computer chips aan te kopen die buiten de VS met Amerikaanse technologie zijn geproduceerd. Niet verassend is dat China represailles treft.[7]

3. In Europa zien we het begrip digitale soevereiniteit in de media momenteel vooral in relatie tot de dominante positie van met name Amerikaanse (en inmiddels ook Chinese) tech bedrijven op het gebied van cloud computing en sociale media. De data van nagenoeg alle Europese burgers en bedrijven bevinden zich inmiddels in de cloud van deze niet-Europese bedrijven en zijn daarmee niet beschikbaar voor Europese innovatie.[8] Wat betreft de *social media*-platforms, is er vooral kritiek op hun gebrek aan maatregelen om misinformatie, *fake news* en politieke beïnvloeding op hun platforms tegen te gaan.[9] Verontrustende voorbeelden van

---

[2] Zie voor mooi overzicht Stephane Couture, The Diverse Meanings of Digital Sovereignty, 5 augustus 2020, http://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/. Zie verder , Eanne Kelly, Decoding Europe's new fascination with 'tech sovereignty', Science-Business, 3 september 2020, https://sciencebusiness.net/news/decoding-europes-new-fascination-tech-sovereignty.

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

[4] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/; https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html.

[5] In een persverklaring van Mike Pompeo, secretary of state, van 5 augustus 2020, kondigt de VS een *Clean Network Program* aan, met 5 maatregelen om het aftappen en misbruik van data van Amerikaanse burgers te voorkomen: "Working to keep Chinese phone carriers (presumably compromised by Beijing) out of U.S. markets, to have privacy-violating Chinese apps kicked off American app stores, to remove U.S. apps from app stores run by Chinese companies, to keep U.S. citizens' data off of Chinese cloud servers "accessible to our foreign adversaries," and to ensure that the undersea cables that ferry internet signals between continents aren't secretly tapped by eavesdropping Chinese intelligence services.", https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/. De verwijten van de Amerikaanse overheid aan het adres van China hebben een hoog *pot verwijt de ketel* gehalte gezien de datapraktijken van de Amerikaanse techbedrijven en het stelselmatig aftappen van de onderzeese kabels door de Amerikaanse intelligence services zelf, zie hierover https://theintercept.com/2020/08/06/the-filthy-hypocrisy-of-americas-clean-china-free-internet/.

[6] https://timesofindia.indiatimes.com/business/india-business/government-bans-118-mobile-apps-including-pubg/articleshow/77890898.cms

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

[8] Digital Services Act package, Inception Impact Assessment, file:///C:/Users/pti/Downloads/090166e5cff964b0.pdf

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

misinformatie zijn het - door Russische infiltratie gestimuleerde - samenzweringsdenken van de anti-vax en anti-5G bewegingen.[10]

4. Specifieke frictie ontstond verder rondom de corona *contact tracing* apps. Kritiek kwam met name van de Franse en Britse overheid dat Google en Apple door de technische inrichting van hun gezamenlijke COVID-19 tracing platform, in feite voor de overheden bepalen hoe zij data van hun burgers kunnen verzamelen in de strijd tegen Covid.[11] Ook in de Amerikaanse pers kwam het verwijt dat Google en Apple hier als een *private government* macht uitoefenen:

> "[They] are exercising sovereign power (…) You have a private government that is making choices over your society instead of democratic governments being able to make those choices".[12]

5. Niet verrassend is dat voornoemde afhankelijkheden van buitenlandse partijen hebben geleid tot een reeks van Europese beleidsvoorstellen.[13] 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,[14] is inmiddels het herstel van de EU's technologische soevereiniteit (naast herstel van de corona-crisis en bestrijding van klimaatverandering) de kern-ambitie van de Europese Commissie voor de komende vijf jaar. Bij haar inaugurele speech als voorzitter van de Commissie zei Ursula Von der Leyen:

> "We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies. (…) [W]e need infrastructure fit for the future, with common standards, gigabit networks, and secure clouds of both current and next generations."[15]

6. Deze strategie wordt ook uitgedragen door de lidstaten. In de woorden van de Franse president Emmanuel Macron:[16]

> "If we don't build our own champions in all areas — digital, artificial intelligence, our choices will be dictated by others."

Ook Angela Merkel kondigde de aanvang van het Duitse voorzitterschap van de EU, aan dat de focus zal liggen op:

---

[10] https://allianceforscience.cornell.edu/blog/2020/04/anti-vaxxers-and-russia-behind-viral-5g-covid-conspiracy-theory/.
[11] Toepasselijke quote van de Franse minister van digitale zaken: "We're asking Apple to lift the technical hurdle to allow us to develop a sovereign European health solution that will be tied our health system," https://www.bloomberg.com/news/articles/2020-04-20/france-says-apple-s-bluetooth-policy-is-blocking-virus-tracker?srnd=progno
[12] Reed Albergotti and Drew Harwell, "Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless." *Washington Post*, May 15, 2020, https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/.
[13] 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.*
[14] "Horizon 2020 is open to the world", https://ec.europa.eu/programmes/horizon2020/en/area/international-cooperation.
[15] https://ec.europa.eu/info/sites/info/files/president-elect-speech-original_en.pdf.
[16] https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/

> "…technological sovereignty, particularly in key areas such as artificial intelligence and quantum computing, also in securing a secure, trustworthy data infrastructure."

7. Wat betreft het laatste is een belangrijk Europees project het zogenaamde *GAIA-X initiatief*.[17] Dit project, dat is geïnitieerd door Duitsland met steun van Frankrijk, heeft tot doel om tot een eigen Europese aanbod van cloud-infrastructuur, diensten en data te komen en is expliciet gebaseerd op basis van beginselen van *sovereignty-by-design,* waarbij de afnemer volledige controle heeft over de opslag en verwerking van de data en de toegang daartoe. De GAIA-X documenten geven zelf overigens aan dat er nog een lange weg te gaan is:

> "Europe's digital infrastructure currently lies in the hands of a small number of major non-European corporations: Europe has no notable operating system developers, no relevant search engines, no global social network and no competitive cloud infrastructure."

8. Het nieuwe Europese soevereiniteits-denken beperkt zich niet tot digitaal beleid, en omvat inmiddels een – bijna caleidoscopisch aandoend – scala aan initiatieven en maatregelen. Er wordt momenteel gewerkt aan *materials autonomy* voor de Europese Green Deal (het veiligstellen van schaarse grondstoffen benodigd voor batterijen voor elektrische auto's -zoals lithium[18] en opslag schone energie - zoals magnesium),[19] *financial sovereignty* getriggerd door de Iranese sancties,[20] en *energy autonomy* ten opzichte van Rusland.[21] De coronacrisis legde verder de Europese afhankelijkheden bloot van wereldwijde *supply chains* van kritische grondstoffen en producten; zo werd ineens pijnlijk duidelijk dat we voor nagenoeg alle chemische componenten die benodigd zijn voor productie van generieke medicijnen afhankelijk zijn van China,[22] hetgeen leidde tot allerlei rapporten inzake '*Health Sovereignty*'.[23] Tot slot wordt gesproken over het uitsluiten van het VK uit de beveiligde zone van het Galileo-satellietsysteem,[24] het tegengaan van *fake news*,[25] en beperkingen voor zogenaamde *Foreign Direct Investment.*[26]

9. Bij deze waaier aan maatregelen, ontkom je niet aan de vraag wat nu precies de samenhang daartussen is en of deze maatregelen voor Nederland en ook de EU als geheel, tot een relevante mate van digitale soevereiniteit kunnen gaan leiden.

---

[17] Project GAIA-X, A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem, German Federal Ministry for Economic Affairs, oktober 2019, https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/project-gaia-x.pdf?__blob=publicationFile&v=5; zie verder Franco-German Position on GAIA-X, 18 februari 2020, p. 1 – 2.
[18] Onder de vlag van de European Battery Alliance, eveneens een IPCEI project, https://ec.europa.eu/growth/industry/policy/european-battery-alliance.
[19] Onder de vlag van de European Raw Materials Alliance, zie voor persbericht inzake het Europese Action Plan on Critical Raw Materials, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1542. Zie voor overzicht van de kritische grondstoffen, Critical Raw Materials for Strategic Technologies and Sectors in the EU, A Foresight Study, 2020, file:///C:/Users/lxm16/Downloads/Critical%20Raw%20Materials%20in%20Technologies%20and%20Sectors_foresight.pdf.
[20] Het gerelateerde financiële instrument is INSTEX, https://instex-europe.com/about-us.
[21] Ursula von der Leyen State of the Union september 2020, https://ec.europa.eu/info/sites/info/files/soteu_2020_en.pdf; zie ook SWP Paper 2019/RP 04, maart 2019, European Strategic Autonomy, https://www.swp-berlin.org/10.18449/2019RP04/#hd-d14204e721.
[22] https://www.politico.eu/article/europe-braces-for-coronavirus-induced-drug-shortages/;
[23] Zie bijvoorbeeld: https://www.ecfr.eu/publications/summary/health_sovereignty_how_to_build_a_resilient_european_response_to_pandemics
[24] Financial Times, 13 juni 2018, "Brussels spurns UK demand for unrestricted access to Galileo satellite" https://www.ft.com/content/332e1a94-6f00-11e8-92d3-6c13e5c92914
[25] Zie eerder genoemde referentie, "Tackling online disinformation"
[26] EU Foreign Direct Investment Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452 t

10. Kortom, alle aanleiding om het begrip *digitale soevereiniteit* nader onder de loep te nemen en de beleidsmatige en staatsrechtelijke implicaties daarvan te analyseren.[27] In deze bijdrage zullen we een overzicht geven van wat we onder digitale soevereiniteit verstaan, hoe de digitale soevereiniteit van de Nederlandse staat op dit moment onder druk staat en welke maatregelen – op welk niveau – kunnen worden overwogen om hierin verbetering te brengen. Daarbij stellen we voorop dat voor ons digitale soevereiniteit niet inhoudt volledige zelfredzaamheid of zelfvoorziening. Dat is in het algemeen niet weggelegd voor Nederland en veelal ook niet voor Europa en is ook niet nodig.

2. Wat is digitale soevereiniteit

A. Soevereiniteit en strategische autonomie

11. *Soevereiniteit* is een politiek begrip waarvoor niet een eenduidige algemeen geaccepteerde definitie bestaat. Soevereiniteit wordt algemeen geassocieerd met territorialiteit, grondgebied (inclusief natuurlijke hulpbronnen), jurisdictie, een bevolking en gezag met zowel interne als externe erkenning (legitimiteit). *Interne legitimiteit* betreft de effectiviteit van de staat als uitvoerder van overheidstaken (bijvoorbeeld het *in control* zijn van het verkiezingsproces en de strafrechtketen) en ook de erkenning door burgers van de staat (het hebben van vertrouwen in de rechtstaat). *Externe legitimiteit* betreft in eerste instantie vooral de erkenning door buitenlandse staten en de handelingsautonomie van een staat jegens vreemde staten.

12. Als soevereiniteit het *doel* is, is strategische autonomie het *middel*. Soevereiniteit moet operationeel worden gemaakt: wat zijn de middelen om soevereiniteit te realiseren? Dit wordt *strategische autonomie* genoemd, een begrip dat oorspronkelijk uit het militaire/defensie denken komt maar tegenwoordig wordt gezien als "het vermogen om autonoom te kunnen beslissen en handelen aangaande essentiële aspecten van de langere-termijn toekomst in economie, maatschappij en democratie."[28]

13. In de huidige informatiesamenleving wordt vaak ook de term *digitale soevereiniteit* gehanteerd. Vrijwel altijd heeft men het dan over de digitale dimensie van strategische autonomie, namelijk het vermogen om autonoom te kunnen beslissen en handelen aangaande de essentiële digitale aspecten van onze langere-termijn toekomst in economie, maatschappij en democratie. Dit betreft dus het gebruik en inrichting van digitale systemen en de daarmee gegenereerde en opgeslagen data en gerelateerde werkprocessen.[29] Een betere term dan digitale soevereiniteit is dan ook digitale strategische autonomie. In dit artikel zullen we echter

[27] Over dit perspectief op dit onderwerp is nog niet veel academische literatuur. Zie voor een Essay Collection van de Europese Denktank *European Council on Foreign Relations*, Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-Chana Rivalry, July 2020, https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf; zie verder EOS Position Paper, EU Digital Autonomy: Challenges & Recommendations for the Future of European Digital Transformation, november 2019, http://www.eos-eu.com/Files/EOSEUDigitalAutonomyPositionPaper.pdf. Zie voor een bredere ontwikkeling in dit verband – namelijk een expliciete link met economisch denken in geo-politiek - de column van Haroon Sheikh: https://www.nrc.nl/nieuws/2020/08/07/leer-geo-economisch-denken-ook-in-de-eu-a4008101.

[28] "The capabilities and capacities to decide and act upon essential aspects of the longer-term future in the economy, society, and democracy", Timmers, P., Strategic Autonomy and Cybersecurity, European Institute of Security Studies, mei 2019).

[29] Een vergelijkbare definitie is 'digital sovereignty is the possibility of independent self-determination by the state and by organisations with regard to the use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result', Digital Summit Focus Group, gerefereerd in aangehaalde GAIA-X document, oktober 2019.

de term digitale soevereiniteit blijven gebruiken aangezien dit momenteel gangbare terminologie is.

14. Binnen digitale soevereiniteit wordt ook *data soevereiniteit* gebezigd. Dit is dan het hebben van zeggenschap over de opslag en verwerking van gegevens en het hebben van controle over wie daar toegang toe heeft.[30] Europese data soevereiniteit wordt gepromoot door eerder genoemd GAIA-X cloud-initiatief en het recente *European Cloud Federation Initiative*, waar standaarden worden gezet voor interoperabiliteit tussen providers en portabiliteit van gegevens[31] en waar van cloudproviders zal worden verwacht dat deze keuze bieden waar (persoons-)gegevens worden opgeslagen en verwerkt, zonder overigens opslag in Europe te verplichten.

> ***Portabiliteit*** is het vermogen van software en data om – met een redelijke inspanning - van de ene IT omgeving naar een andere te worden overgezet (het traject van overzetten, noemen we *migratie*)
>
> ***Interoperabiliteit*** is het vermogen van IT-systemen om samen te werken met ander IT-systemen, waardoor data kan worden uitgewisseld en in de ontvangende systemen verder kan worden verwerkt.

15. Zelfs is er een discussie of bepaalde categorieën data (bijv. patiëntengegevens en industriële data) op zichzelf al als soeverein bezit dienen te worden aangemerkt, vergelijkbaar met natuurlijke hulpbronnen als gas of olie onder ons grondgebied. Op grond van een dergelijke zienswijze kunnen dan territoriale rechten worden geclaimd op Europese data, zoals dat ook met natuurlijke hulpbronnen het geval is. Zo zou Eurocommissaris Thierry Breton recent hebben gezegd dat "European data should be stored and processed in Europe because they belong in Europe".[32]

16. Het zal weinig toelichting behoeve dat waar overheden en aanbieders van kritische infrastructuur steeds verdergaand hun ICT-systemen en dataopslag en -verwerking uitbesteden aan leveranciers, nieuwe afhankelijkheden ontstaan, in het bijzonder als die leveranciers dominante marktspelers zijn (zie hierna sub 33 e.v.). Het begrip digitale soevereiniteit strekt zich dan tevens uit tot de autonomie van onze overheid en aanbieders van kritische infrastructuur *jegens deze commerciële partijen*, en waar dit buitenlandse partijen zijn, *tot hun respectievelijke overheden*.

17. Kortom, de ontwikkelingen van de digitale wereld dwingen ons indringend vragen te stellen omtrent soevereiniteit en autonomie. De overgang naar de digitale en technologische geconstrueerde maatschappij[33] hebben direct gevolgen voor de geopolitieke verhoudingen.

18. Als *food for thought* van hoe ver de vragen reiken: landen beschouwen het DNA van inheemse flora en fauna als behorend tot hun natuurlijke hulpbronnen, het valt onder hun soevereiniteit. Ze leggen uitvoer aan banden, of eisen op z'n minst *Fair and Equitable Sharing of Benefits*, als ondertekenaars van het Nagoya Protocol.[34] Maar met digitalisering en *gene-sequencing* wordt DNA een reeks digitale data. Die data zijn gemakkelijk het land uit te brengen en kunnen vervolgens met genetische technologieën van digitale sequentie weer in fysiek DNA worden omgezet. Is dan ook de digitale weergave van DNA, deel van soevereiniteit?

---

[30] 'complete control over stored and processed data and also the independent decision on who is permitted to have access to it', Project GAIA-X, BMWI, oktober 2019.
[31] Portabiliteit is het vermogen van software en data om – met redelijke inspanning - van de ene IT omgeving naar een andere te worden overgezet, https://www.techopedia.com/definition/8921/portability.
[32] Volgens een POLITICO interview op 1 september 2020, https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/.
[33] Over de relatie tussen technologie en maatschappij zie bijv. Jean Baudrillard, Simulacra et Simulation, 1981, en Paul Timmers, 'Challenged by "Digital Sovereignty"' in Journal of Internet Law, December 2019.
[34] Nagoya Protocol over biodiversiteit, https://www.iucn.org/theme/global-policy/our-work/convention-biological-diversity-cbd/nagoya-protocol.

B. *De facetten van digitale soevereiniteit*

1. *Cyberweerbaarheid van kritische systemen, processen en data*

19. Een belangrijke dimensie van digitale soevereiniteit is de *cyberweerbaarheid* van onze kritische sectoren, processen, en data. De steeds toenemende cybersecurity bedreigingen, ondermijnen soevereiniteit. We spreken dan over het hele spectrum van directe bedreiging van onze vitale infrastructuur, systematische diefstal van intellectuele 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.[35] Wanneer onze overheid en kritische sectoren niet *in control* zijn van 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.[36] 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, en ondermijnt daarmee onze externe legitimiteit in internationale betrekkingen.[37]

20. Wat betreft cyberbedreigingen kan digitale soevereiniteit niet los worden gezien van de drie basisprincipes van informatieveiligheid: vertrouwelijkheid, integriteit en beschikbaarheid, ook wel genoemd de CIA van cybersecurity: *Confidentiality, Integrity, Availability*. In deze drie domeinen dient de autonomie te worden gewaarborgd, dit 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*.

21. Via een specifiek ICT-systeem van de overheid kan soevereiniteit worden ondermijnd – denk aan het stelen van informatie van overheidsfunctionarissen voor spionage doeleinden[38] (*vertrouwelijkheid*) en aan cyberaanvallen op zogenaamde *Industrial Automation & Control Systems (IACS)*[39] in onze kritische infrastructuur (*beschikbaarheid)*.[40] Deze systemen zijn doelwit van vooral statelijke actoren om in de

> ***IACS*** zijn de meet- en regelsystemen die onze sluizen en bruggen aansturen, zorgen dat energie en gas worden gedistribueerd, drinkwater wordt gereinigd en nucleair materiaal wordt verwerkt.

[35] 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
[36] CSBN 2020
[37] CSBN 2020, p. 18, onder verwijzing naar het AIVD Jaarverslag 2019, AIVD, april 2020.
[38] De AIVD meldt dat onder andere ministeries, inlichtingen- en veiligheidsdiensten, politieke partijen en cultureel-maatschappelijke organisaties doelwit waren van politieke spionage, CSBN 2020, p.19. Bijvoorbeeld worden inlichtingen verzameld om landen tegen elkaar uit te spelen om de eenheid en de internationale samenwerking binnen de Noord-Atlantische Verdragsorganisatie en Europese Unie te ondermijnen, CSBN 2020,p. 15. Zie voor recent voorbeeld: Bloomberg, Chinese Hackers Targeted European Officials in Phishing Campaign, 2 september 2020, https://news.bloomberglaw.com/privacy-and-data-security/chinese-hackers-targeted-european-officials-in-phishing-campaign.
[39] Ook wel SCADA systemen genoemd, Supervisory Control and Data Acquisition. Sommige cyber-aanvallen staan bekend als SCADA-attacks, zoals Stuxnet die Iraanse nucleaire centrifuges onklaar maakte in 2010.
[40] Zie voor een overzicht van kwetsbaarheden in IACS, CSBN 2020, p. 16 en 19. Zie voor vijandelijke cyberaanvallen op attacks op IACS in kritische infrastructuren: Gartner, Een rapport voor het Ministerie van Justitie en Veiligheid, Onderzoek Cybersecurity voor Industrial Automation en Control Systems, 21augustus 2019, https://www.cybersecurityraad.nl/binaries/CSR_Advies_IACS_Onderzoeksrapport_Gartner_DEF_tcm107-442489.pdf, en het advies terzake van de Cyber Security Raad, "Advies inzake de digitale veiligheid van Industrial Automation & Control Systems (IACS) in de vitale infrastructuur van Nederland, 24 april 2020 (**CSR Advies Cyberweerbaarheid IACS**), https://www.cybersecurityraad.nl/binaries/CSR_Advies_IACS_NED_DEF_tcm107-444304.pdf.

toekomst sabotage mogelijk te maken als drukmiddel om geopolitieke doestellingen te bereiken.[41]

22. In deze gevallen kunnen we digitale soevereiniteit vertalen in *directe eisen* aan ICT-systemen. Het betreft dan eisen aangaande beveiliging, detectie van dreigingen, continuïteit (back-up, disaster recovery), *vendor lock-in* (voorkomen van afhankelijkheid van een specifieke leverancier), en toegang tot data voor buitenlandse mogendheden (zie hierna sub 35 e.v. voor een overzicht van specifieke afhankelijkheden bij cloudcomputing). Digitale soevereiniteit moet zoals gezegd echter ook worden vertaald naar het bredere staatsbelang van *economie, maatschappij en democratie*. Dan gaat het bijvoorbeeld over de mate van controle over essentiële economische ecosystemen, kennis en data, vertrouwen in het rechtssysteem, en kwaliteit van democratische besluitvorming.[42] We geven hierna een aantal voorbeelden.

> ***Vendor lock-in*** ontstaat doordat de leverancier eigen beschermde standaarden hanteert, waardoor software en applicaties alleen op het eigen platform werken, hetgeen een overstap van een klant naar een andere leverancier kostbaar of zelfs onmogelijk maakt.

2. Controle over economische ecosystemen

23. Voor het *economische belang* moet worden gekeken naar de mate waarin we als Nederland controle hebben over het economische ecosysteem, economische waarde-creatie en kennis. Hiervoor is er inmiddels een nationaal digitaal beleid,[43] niet alleen voor de overheid als gebruiker van ICT maar ook voor Nederlandse bedrijven als leverancier en als kennisland.[44] Verzwakte controle over *economische ecosystemen en kennis* kan soevereiniteit in gevaar brengen – denk aan gebrek aan controle over kritische technologie, zoals AI en encryptie. Indien hier niet genoeg innovatie plaatsvindt, ontstaan potentieel nieuwe afhankelijkheden. Bijvoorbeeld spelen bij cyberweerbaarheid nieuwe technologieën een steeds crucialere rol.[45] Zo vergemakkelijkt AI het uitvoeren van cyberaanvallen, doordat bestaande kwetsbaarheden automatisch en op grote schaal kunnen worden ontdekt en uitgebuit.[46] AI zal het echter naar verwachting ook mogelijk maken om zelf automatisch kwetsbaarheden in software op te sporen en te herstellen. Met post-quantum cryptografie moeten we uiteindelijk dataversleuteling mogelijk maken, die bestand is tegen aanvallen waarbij gebruik wordt gemaakt van de rekenkracht van een kwantumcomputer. Hoewel de kwantumcomputer de komende jaren onvoldoende ver zal zijn ontwikkeld om in de praktijk te kunnen worden gebruikt, zullen we toch nu al moeten inzetten op innovatie om IT-systemen te beschermen tegen het risico van een aanval met een kwantumcomputer. Immers, zodra de kwantumcomputer het mogelijk maakt om bestaande vormen van encryptie te breken, is post-

[41] CSBN 2020, p. 8 en 16.
[42] Voor een aantal van deze aspecten zie ook het Ongevraagd Advies van de Raad van State, 31 augustus 2018, https://www.raadvanstate.nl/@112661/w04-18-0230/
[43] 'ICT en economie' https://www.rijksoverheid.nl/onderwerpen/ict/ict-en-economie.
[44] Met specifieke aandacht voor de cybersecurity sector, https://www.rijksoverheid.nl/onderwerpen/ict/veilige-infrastructuur, http://www.seo.nl/uploads/media/2016-56_Economische_kansen_Nederlandse_Cybersecurity_sector.pdf.
[45] 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, 18 september 2020, https://www.cybersecurityraad.nl/binaries/CSR_Advies_NT_NED_DEF_tcm107-466703.pdf (**CSR Advies Nieuwe Technologieën**), p. 3.
[46] CSBN 2020, p. 15 – 26.

kwantumcryptografie een noodzakelijke voorwaarde om de veiligheid van data van bedrijven en burgers te borgen.[47]

24. Waar buitenlandse bedrijven vooroplopen wat betreft de (verdere) ontwikkeling en implementatie van genoemde nieuwe technologieën, zoals AI, quantum computing, maar ook satelliet- en 5G-netwerken, ontstaan potentieel nieuwe afhankelijkheden. Deze afhankelijkheden gaan verder dan de specifieke technologische toepassingen zelf. Om op grote schaal gebruik te kunnen maken van data-analyse door middel van AI, is enorme rekenkracht vereist. De verwachting is dat de cloud-infrastructuur die hiervoor is benodigd het fundament wordt voor de Nederlandse en Europese innovatie- en kennisinfrastructuur. Daarover zeggenschap houden, is een wezenlijk deel van de Nederlandse strategische autonomie.[48]

3. Vertrouwen in rechtssysteem en democratische processen

25. 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. Niet is uitgesloten dat als de interne legitimiteit ter discussie staat (bijv. wanneer de staat geen controle heeft over het verkiezingsproces, omdat dit is geïnfiltreerd en wordt gemanipuleerd door vreemde mogendheden), ook de *externe* legitimiteit in het gedrang komt (Nederland als betrouwbare internationale partner).

26. Daarbij moet worden bedacht dat elke digitalisering van overheidsprocessen nieuwe kwetsbaarheden schept in het maatschappelijk verkeer, in dit geval nieuwe mogelijkheden van potentiële beïnvloeding en verstoring van een vitale functie van onze rechtstaat. Dit heeft ook een impact op de burgers, omdat het ongemak en de nadelen van het gebruik van nieuwe technieken door de overheid, vaak bij hen terechtkomen. Dit raakt de rechtsstatelijke verhouding van burgers tot de overheid, waarbij hun positie en bescherming in het geding zijn. In een ongevraagd advies uit 2018 omschrijft de Raad van State de problematiek treffend:[49]

> "Bij digitalisering van de besluitvorming dreigt de burger in toenemende mate te worden geconfronteerd met besluiten die volautomatisch zijn genomen, zonder menselijke tussenkomst. Die burger kan niet meer nagaan welke regels zijn toegepast en het is niet meer vast te stellen of de regels ook werkelijk doen waarvoor ze bedoeld zijn. Ook dreigt de burger slachtoffer te worden van een robotachtige gelijkheid, waarbij geen oog meer bestaat voor de eigenheid van zijn situatie. Daarnaast dreigt hij geconfronteerd te worden met besluiten die berusten op profilering en statistische verbanden. Er is dan niet aangetoond dat de burger verwijtbaar heeft gehandeld; er is alleen een vermoeden op basis van algemene kenmerken. Er ontstaat een statistische werkelijkheid die afwijkt van de concrete feiten. Tenslotte dreigt de burger te worden geconfronteerd met besluiten die genomen zijn op basis van gegevens die van verschillende andere bestuursorganen zijn verkregen. Het valt dan niet meer na te gaan

[47] CSR Advies Nieuwe Technologieën, p. 4.[48] Paul Timmers, There will be no global 6G unless we resolve sovereignty concerns in 5G governance. Nature Electronics 3, 10–12 (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.

[48] Paul Timmers, There will be no global 6G unless we resolve sovereignty concerns in 5G governance. Nature Electronics 3, 10–12 (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.

[49] Zie het Ongevraagd Advies van de Raad van State, 31 augustus 2018, para. 1, https://www.raadvanstate.nl/@112661/w04-18-0230/. Zie over de impact van de digitalisering op brugers: L. Moerel & C. Prins, *Privacy voor de Homo Digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things*, Preadviezen 2016 Nederlandse Juristen-Vereniging, Deventer: Kluwer juridisch 2016, p. 9-124.

of de besluiten op basis van correcte gegevens zijn genomen. Bovendien zal de burger zelf aannemelijk moeten maken dat er een fout is gemaakt; in geval van fouten in het systeem moet hij zijn eigen "onschuld bewijzen".

27. Ook bij infiltratie van een vitaal overheidsproces kan tot ondermijning van het vertrouwen in de rechtstaat leiden. Illustratief is een recent incident in Duitsland. In januari 2020 rapporteerde *Der Spiegel* dat het Hooggerechtshof in Berlijn (o.m. verantwoordelijk voor terrorismezaken), systematisch was geïnfiltreerd door een Russische hacker-groep die waarschijnlijk wordt gesponsord door de Russische overheid, geïdentificeerd als APT 28 (*Advanced Persistent Threat*). Deze hackersgroep was eerder verantwoordelijk gehouden voor de infiltratie van de Duitse Bundestag. De attack was gericht op data exfiltratie, waarbij toegang was verkregen tot de gehele database met identiteiten van verdachten, slachtoffers, getuigen en undercoveragenten en informanten.[50]

28. Een ander voorbeeld van ondermijning van het vertrouwen in de rechtstaat is de maatschappelijke ophef die in Duitsland ontstond doordat de federale politie in maart 2019 de *bodycam* opnamen van politieagenten onderbracht in de public cloud van Amazon.[51] Dit leidde tot vernietigende kritiek van de Duitse federale privacy toezichthouder, dat deze praktijk in strijd is met de privacy wet en dat de opnamen moeten worden ondergebracht in een private Duitse cloud. Belangrijkste bezwaar van de toezichthouder was dat Amazon een Amerikaans bedrijf is waarop de U.S. CLOUD Act van toepassing is, waardoor de Amerikaanse autoriteiten potentieel toegang hebben tot deze data.[52]

29. De publieke ophef in Duitsland is niet zo verassend als je bedenkt, dat de bodycam opnamen potentieel gevoelig materiaal betreffen voor burgers: het betreft beeld- en geluidsopnamen die potentieel bewijs van strafrechtelijk handelen kunnen inhouden, maar ook niet-betrokken omstanders kunnen in beeld zijn. Voor doorzoeking van grote hoeveelheden bodycam-opnamen en *blurring* van gezichten van niet-betrokken personen, wordt AI-gestuurde gezichtsherkenning ingezet. Hoe goed zal die AI zijn, herkent die *fake* en manipuleerd materiaal, en wie ziet daarop toe? Wat indien fake materiaal wordt gemist en in de strafrechtketen terecht komt? In deze gevallen ligt de bewijslast de facto bij de burger in plaats van bij de strafrechtketen, hetgeen het functioneren van, en vertrouwen in, de rechtstaat ondermijnt. Dit raakt daarmee de *interne legitimiteit* van de staat.[53]

30. Gezien de mogelijke impact op het vertrouwen in de rechtsstaat (dus opnieuw: soevereiniteit), overweegt de Europese Commissie regulering van AI-gestuurde gezichtsherkenning en heeft zij hierover een debat gelanceerd.[54]

31. Een laatste voorbeeld betreft de eerder gesignaleerde verwachting dat AI het mogelijk zal maken om zelf automatisch kwetsbaarheden in software op te sporen en te herstellen. Waar AI autonoom beslissingen kan nemen, is dat vooral kritiek waar dit staatsverantwoordelijkheden betreft. De huidige wetgeving voor cyberweerbaarheid is niet op dergelijke autonome AI voorbereid. Die wetgeving gaat ervan uit dat overleg plaatsvindt hoe met dreigingen om te gaan. Voordat echter het vereiste overleg heeft kunnen plaats vinden, heeft een cyber-virus

[50] https://www.tagesspiegel.de/berlin/cyberangriff-auf-berliner-kammergericht-russische-hacker-koennten-justizdaten-gestohlen-haben/25477570.html
[51] https://www.noz.de/deutschland-welt/politik/artikel/1685384/bundespolizei-geraet-wegen-speicherung-von-bodycam-aufnahmen-unter-druck
[52] De Minister van Binnenlandse zaken antwoordde hierop dat de oplossing tijdelijk zou zijn, totdat er een federale rijkscloud is opgezet. Teven zijn hierover vragen in het parlement gesteld (inclusief over het risico van de U.S. Cloud Act), waarna een officieel onderzoek is ingesteld, waarop de Duitse federale overheid heeft geantwoord. Hieruit bleek dat op dat moment migratie naar een alternatieve oplossing nog niet mogelijk was.
[53] Dit is een fundamentele zorg van de Raad van State, zie para 2 'Groeiende zorg-burger in de knel.
[54] https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-european-approach-excellence-and-trust

zich allang verspreid en bovendien nog aangepast. We moeten dus kunnen reageren met de snelheid van virusverspreiding, en dat kan alleen met AI. Maar wat als die AI in feite beslissingen over leven en dood gaat nemen, bijvoorbeeld door een deel van het elektriciteitsnetwerk af te schakelen om een cyber-virus af te remmen? Indien we AI toelaten in het hart van onze cyberverdediging en in het hart van onze staat, zullen we de bevoegdheden én verantwoordelijkheden duidelijk moeten bepalen. Ook dit raakt weer de inrichting van de staat en is vooralsnog vrijwel niet verkend gebied.

3. Waarom staat digitale soevereiniteit onder druk?

32. De druk op (digitale) soevereiniteit komt van drie kanten, die we hierna verder zullen toelichten:

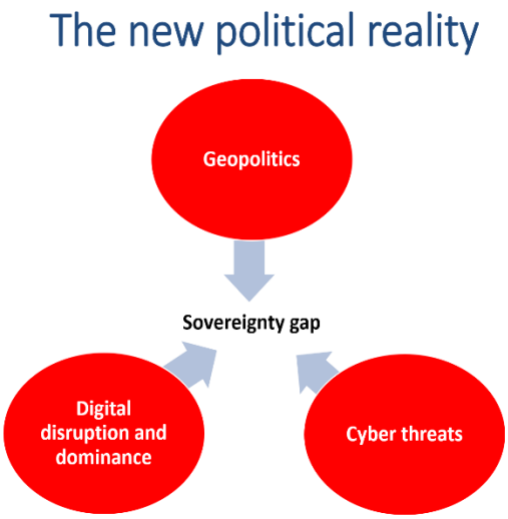
- De toenemende afhankelijkheid van digitale technologie die bovendien grotendeels in handen is van een beperkt aantal buitenlandse spelers;[55]

- De toenemende cyber-dreigingen – waarbij ook kleinere landen en niet-statelijke actoren zich op het mondiale strijdtoneel kunnen begeven[56] - die van dien aard zijn dat ze nationale soevereiniteit en de internationale orde serieus ondermijnen en daarmee een *sovereignty gap*[57] creëren;

- De toenemende geopolitieke spanningen, in het bijzonder in de relatie VS - China, EU-Rusland, en trans-Atlantisch, die leiden tot extraterritoriale claims.

Het diagram geeft deze nieuwe politieke realiteit weer.

[55] De Wetenschappelijke Raad voor het Regeringsbeleid geeft in het advies "Voorbereiden op digitale ontwrichting", 2019, hoofdstuk 3, een goed overzicht van de vergaande digitalisering van de samenleving, de sterke verwevenheid van het digitale domein en het fysieke domein, en de nieuwe kwetsbaarheden die daardoor voor maatschappelijke kernprocessen ontstaan, WRR Advies Digitale Ontwrichting , https://www.wrr.nl/adviesprojecten/digitale-ontwrichting/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting .
[56] 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/.
[57] Lucas Kello, The Virtual Weapon and International Order, Yale University Press, 2017;



A. AFHANKELIJKHEDEN VAN BEPERKT AANTAL BUITENLANDSE LEVERANCIERS

33. Hiervoor is al een aantal voorbeelden gegeven waarom digitale soevereiniteit onder druk staat. Hierna gaan we dieper in op de specifieke afhankelijkheden die ontstaan doordat organisaties leveranciers inzetten om hun digitale infrastructuur te leveren.

34. Duidelijk is dat indien een organisatie zelf de hardware, software en data in beheer heeft die benodigd zijn voor haar werkprocessen, de afhankelijkheden van derden beperkt zijn. De afhankelijkheden worden groter al naar gelang de levering en het beheer van de diverse componenten wordt uitbesteed aan een leverancier. Het hebben van eigen controle over de digitale infrastructuur wordt dan voor onderdelen vervangen door het maken van contractuele afspraken. Steeds vaker kunnen bepaalde afhankelijkheden ook worden ondervangen door bijvoorbeeld toegang tot data en systemen technisch af te schermen of door data zelf te beveiligen door middel van encryptie.

35. De mate van 'controle' die de opdrachtgever heeft en de grip op de beveiligingsmaatregelen over infrastructuur en data, verschilt per soort uitbesteding. We zien dat in het bijzonder bij clouddiensten. De meest vergaande vorm van uitbesteding is wanneer gebruik wordt gemaakt van zogenaamde SaaS-diensten (*Software as a Service*). Bij SaaS wordt zowel de infrastructuur als de software door de leverancier als dienst aan de klant geleverd (deze heeft geen eigen hardware en software licenties), waardoor de data van de afnemer zich dus niet meer in de eigen omgeving van de afnemer bevindt. Bij SaaS is meestal sprake van een *public cloud,* waarbij infrastructuur en software worden gedeeld met andere klanten om zo beoogde kosten en schaalvoordelen te benutten. Waar we hierna over SaaS spreken bedoelen we een *public cloud* oplossing.[58]

36. De internationale cloudaanbieders concurreren op beveiliging en zijn *best in class*. De inzet van cloudoplossingen biedt verder inmiddels zoveel voordelen wat betreft functionaliteit (bijvoorbeeld ingebouwde data-analyse tools), hogere implementatiesnelheid, innovatie, de mogelijkheid van samenwerken en veelal lagere kosten, dat het gebruik van clouddiensten

[58] Een uitleg van cloud en de veel gebruikte begrippen IaaS, PaaS, SaaS is te vinden in https://www.nist.gov/publications/nist-definition-cloud-computing.

inmiddels ook wordt gezien als 'noodzakelijk voor een goed werkende overheid', waardoor het overheidsbeleid inmiddels *cloud first* is, zowel in Nederland als Europa.

37. In de markt is er een zeer beperkte keuze aan zogenaamde *hyperscalers* (cloudaanbieders met grote capaciteit). De Amerikaanse en Chinese hyperscalers hebben wereldwijd 75% marktaandeel (65% al voor Amazon, Google, Microsoft en IBM); en in de EU komen Europese leveranciers nauwelijks in het plaatje voor.[59] De dominantie in markposities leidt tot een disbalans tussen leverancier en klant, met monopolistische gedrag in contracten, prijs, dienstverlening, en afhankelijkheden voor de toekomst (niet alleen wegens afhankelijkheden bij contractbeëindiging (exit en transitie), maar ook omdat het aanbrengen van wijzigingen in standaardoplossingen lastig is).[60]

Exit en Transitie: bij contractbeëindiging ontstaan voor de klant vaak afhankelijkheden, omdat de klant de medewerking van de leverancier nodig heeft voor transitie van data naar een opvolgend leverancier (die weer eigen standaarden toepast). Hiervoor worden al bij contractsluiting specifieke protocollen voor 'exit en transitie' overeengekomen.

38. De grote marktspelers bieden beperkte interoperabiliteit en portabiliteit van data en applicaties. Door hun schaal zijn zij in staat eigen – vaak door intellectuele eigendomsrechten beschermde – standaarden te hanteren en zelfs een private internet infrastructuur aan te leggen (tot eigen onderzeekabels aan toe),[61] waardoor hun zowel fysiek als juridisch nagenoeg autonoom zijn en elke interconnectie zowel wat betreft infrastructuur als uitwisseling van data wordt bemoeilijkt.[62] Om vendor lock-in te voorkomen hebben opdrachtgevers (en ook de Nederlandse en Europese overheid)[63] meestal een zogenaamde *multi-vendor* strategie. Dit is echter bij de huidige marktomstandigheden, lastig te bereiken.

39. De huidige verwachting is dat – zonder overheidsingrijpen - de dominante posities van deze marktspelers alleen nog maar zullen toenemen. Deze marktspelers breiden hun ecosysteem systematisch uit door nieuwe functionaliteiten in hun dienstverlening te integreren (zoals cybersecurity en data-analyse tooling), waardoor de *vendor lock-in* alleen maar toeneemt.[64] Zij zijn verder in staat het beste talent wereldwijd aan zich te binden en hebben bijna onuitputtelijk toegang tot kapitaal. Hiermee monitoren ze voortdurend nieuwe innovaties en start-ups, die zij vervolgens in een vroeg stadium overnemen en in het eigen aanbod integreren. De strategie van de grote tech bedrijven om competitie in de kiem te smoren door

[59] Synergy Research Group, 29 oktober 2019.
[60] Europese Commissie, Mededeling: Een Europese datastrategie, https://eur-lex.europa.eu/legal-content/NL/TXT/?qid=1593073685620&uri=CELEX:52020DC0066, 19 februari 2020.
[61] Waarbij zelfs eigen onderzeekabels worden aangelegd, zie voor Google, http://www.datacenterknowledge.com/google-alphabet/three-new-submarine-cableslink-google-cloud-data-centers; en voor Microsoft en Facebook, https://thenextweb.com/facebook/2017/09/22/microsoft-and-facebook-just-laid-a-160tbpsundersea-cable-17000-feet-deep/.
[62] Zie afscheidsrede Jan Smits, https://pure.tue.nl/ws/portalfiles/portal/99880344/Rede_Jan_Smits_LR_15_06_2018.pdf.
[63] Zie bijv. Cloud uitgangspunten JenV, p.2, en Europese Commissie/DIGIT (Bijlage 3 – EU Cloud beleid)
[64] Dit probleem wordt ook door de Europese Commissie gesignaleerd, zie Europese Datastrategie, p.7 (zie ook volgende paragraaf inzake het Europees cloudbeleid). Ook de financiële wereld (banken, toezichthouders etc) analyseert de strategische aspecten van het eigen cloudbeleid. De European Securities and Markets Authority (ESMA) heeft op 3 juni een consultatie over haar richtlijnen voor cloud outsourcing geopend. Steven Maijoor, EMA voorzitter lichtte toe "Financial markets participants should be careful that they do not become overly reliant on their cloud services providers. They need to closely monitor the performance and the security measures of their cloud service provider and make sure that they are able to exit the cloud outsourcing arrangement as and when necessary.", https://www.esma.europa.eu/press-news/esma-news/esma-consults-cloud-outsourcing-guidelines

stelselmatig innovatieve start-ups op te kopen, wordt inmiddels onderzocht door de Amerikaanse FTC.[65]

40. De afhankelijkheid van buitenlandse aanbieders brengt controle van andere landen mee, die andere spelregels hanteren wat betreft spionage, privacy en afgifte van data. We gaan op deze specifieke afhankelijkheden hierna in detail in (zie sub 43 e.v.).

B. CYBER-SECURITY DREIGINGSBEELD NEDERLAND

41. De Nationaal Coördinator Terrorismebestrijding en Veiligheid publiceert jaarlijks een *Cybersecuritybeeld Nederland,* dat inzicht geeft in de digitale dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het Cybersecuritybeeld Nederland 2019[66] (**CSBN 2019**), geeft als belangrijkste bevindingen dat in Nederland sprake is van een "permanente digitale dreiging", dat de grootste (en steeds groeiende) dreiging daarbij komt vanuit statelijke actoren, dat landen als China, Iran en Rusland offensieve cyberprogramma's hebben die specifiek zijn gericht tegen Nederland, zowel om geopolitieke als economische doelstellingen te bereiken ten koste van Nederlandse belangen, en waarbij verstoring en sabotage van onze vitale infrastructuur de meeste impact hebben vanwege de potentieel maatschappij-ontwrichtende effecten.[67] Dit beeld wordt in het CSBN 2020 bestendigd.[68] Specifiek wordt gerapporteerd dat meer Nederlandse topsectoren doelwit zijn (geweest) van digitale spionage. Het gaat daarbij vooral om hightech, energie, maritiem en life sciences & health.

42. Het CSBN 2019 constateert verder dat de digitale leverancierskeketen (en met name *Managed Service Providers*) de kwetsbaarheid verhogen, dat cyberaanvallen daarop in de rapportage periode "zeer succesvol waren" en dat deze naar verwachting in de toekomst "verder zullen toenemen."[69] Het CSBN 2020 bestendigt dit beeld en constateert dat vooral de leverancierskeketen wordt misbruikt omdat actoren op zoek gaan naar de zwakke schakel in ketens waar het beoogde doelwit van afhankelijk is.[70] Ook de Amerikaanse National Security Agency waarschuwt expliciet voor de risico's die het gebruik van clouddiensten met zich meebrengt.[71] Juist doordat de clouaanbieders wereldwijd zoveel afnemers bedienen, zijn hun diensten een voortdurend doelwit van APT's (*Advanced Persistent Threats*), niet alleen van cybercriminelen maar vooral ook van statelijke actoren.[72]

43. Het CSBN 2019 constateert verder dat de afhankelijkheid van de kleine groep internationale leveranciers risico's meebrengt voor de nationale veiligheid en de soevereiniteit en autonomie

[65] https://www.ftc.gov/news-events/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies.
[66] Cybersecuritybeeld Nederland 2019, https://www.nctv.nl/documenten/publicaties/2019/6/12/cybersecuritybeeld-nederland-2019
[67] CSBN 2019, p. 7.
[68] CSBN 2020, p. 19. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
[69] CSBN 2019, p.18; zie tevens AIVD-jaarverslag 2018, p. 8, https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018.
[70] CSBN 2020, p. 19. Gerapporteerd wordt dat ook IBM een toename ziet van het gebruik van legitieme hulpmiddelen in plaats van het gebruik van malware: bij meer dan de helft van de cyberaanvallen (57 procent) werd gebruik gemaakt van algemene beheertoepassingen.
[71] 'NSA waarschuwt voor beveiligingsrisico's clouddiensten', Security.nl, 28-1-2020, https://www.security.nl/posting/641329/NSA+waarschuwt+voor+beveiligingsrisico%27s+clouddiensten
[72] Zie bijv. Reuters 2019, Cloud Hopper attack: Eight of the world's biggest technology service providers were hacked by Chinese cyber spies in an elaborate and years-long invasion, Reuters found. The invasion exploited weaknesses in those companies, their customers, and the Western system of technological defense. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/
Zie verder: Crowdstrike, 2020, About 2019 trends: An alarming trend in targeted ransomware operations is the compromise of managed service providers (MSPs). Subsequent use of remote management software can enable the spread of ransomware to many companies from a single point of entry. WIZARD SPIDER also targeted this sector and impacted cloud service providers. Ransomware is BitPaymer, REvil, Ryuk.

van de Nederlandse Staat en de Europese Unie.[73] Afhankelijkheden ontstaan doordat een beperkt aantal leveranciers *de facto* de standaarden bepaalt waardoor het mogelijk is hun positie ten opzichte van andere aanbieders te versterken, en doordat de maatschappelijke impact van een storing of een digitale aanval groot kan zijn omdat veel verschillende processen of diensten afhankelijk zijn van een beperkt aantal aanbieders. Met de afhankelijkheid van dit beperkt aantal aanbieders ontstaat verder ook een afhankelijkheid van een beperkt aantal landen. Deze hanteren andere spelregels wat betreft privacy en afgifte van data, en kunnen de aanbieders ook dwingen mee te werken aan (economische) spionageactiviteiten en het aanbrengen van *backdoors.*[74]

44. Tot slot: nu de cyberdreigingen groot zijn en de clouddiensten inherent kwetsbaar, is belangrijk als opdrachtgever in staat te zijn (i) de cloudinfrastructuur te kunnen monitoren op incidenten, (ii) in geval van incidenten digitale forensische analyse te kunnen doen; en (iii) mitigerende maatregelen te kunnen treffen. Ook hier ontstaan specifieke afhankelijkheden.[75] Inmiddels heeft zowel het Rijk als het Ministerie van Justitie en Veiligheid (en daarbinnen ook weer de Nationale Politie)[76] voor het beoordelen van cloudprojecten zogenaamde cloudkaders opgesteld, waar de specifieke risico's en afhankelijkheden worden geïnventariseerd en geadresseerd. Het Cloudkader dat is opgesteld door het Ministerie van Justitie en Veiligheid geeft een goed overzicht van de *specifieke* afhankelijkheden wat betreft detectie van dreigingen en incident response.[77] Bij bestudering van de Cloudkaders valt op dat deze vooral zien op de directe eisen die aan een specifiek cloudproject dienen te worden gesteld en dat deze geen bredere overwegingen van digitale soevereiniteit meenemen. Wij komen hier later op terug.

C. *EXTRATERRITORIALE CLAIMS*

1. *Toegang data door vreemde mogendheden*

45. Indien data in een SaaS cloud worden gezet, bestaat de mogelijkheid dat deze toegankelijk zijn voor vreemde staten. Hoewel in dit kader altijd het voorbeeld wordt genoemd van de Amerikaanse CLOUD Act (CLOUD = *Clarifying lawful overseas use of data*),[78] betreft dit nog een met *waarborgen omgeven* mogelijkheid voor Amerikaanse *opsporingsautoriteiten* om bij Amerikaanse cloudaanbieders gegevens op te vorderen die op hun servers in een ander land zijn opgeslagen, zoals de inhoud van e-mails, documenten, foto's en video's, etc. Voor deze vordering is een verstrekkingsbevel vereist van een Amerikaanse rechter (*warrant*) gebaseerd

---

[73] CSBN 2019, p. 7, 11 en 22.
[74] CSBN 2019, p. 22. Een *backdoor* is een geheim poortje in software of een computersysteem dat hackers en inlichtingendiensten de mogelijkheid geeft om illegaal toegang te krijgen, https://en.wikipedia.org/wiki/Backdoor_(computing).
[75] Zie voor een specifiek overzicht hiervan ENISA paper "Exploring Cloud Incidents", juni 2016, waarin de technische, organisatorische en juridische knelpunten worden besproken voor zowel Iaas, PaaS en SaaS.
[76] De Notitie *Verkenning Cloudbeleid voor de Nederlandse Rijksdienst*, 29 november 2019; de gezamenlijke documentatie voor beoordeling van clouddiensten JenV: Uitgangspunten Cloud JenV van 27 september 2019; Cloud afwegingskader JenV van 12 december 2019; Cloud PIA Model [ongedateerd]; Quickscan Informatiebeveiliging JenV van 2 januari 2019; en Cloud specifieke BIO-maatregelen JenV van 27 september 2019. Het cloudkader van de nationale politie is wel opgesteld, maar nog niet gepubliceerd.
[77] Zie bijvoorbeeld Cloud *specifieke BIO maatregelen* JenV, para. 4.1 – 4.3:

- **Incident response**. Cloudproviders zijn huiverig met het delen van allerlei logbestanden en data, zeker wanneer deze gegevens bevatten van andere klanten. Het is daarnaast niet vanzelfsprekend dat wanneer zich een incident voordoet in de cloudomgeving van de cloudprovider dit incident (of een melding ervan) ook de weg zal vinden naar het Ministerie van Justitie en Veiligheid.
- **Forensics**: Onvoorwaardelijke toegang tot logbestanden en overige gegevens is doorgaans een voorwaarde voor het efficiënt en effectief kunnen afhandelen van incidenten. Cloudproviders zullen echter niet alle logbestanden en data kunnen delen, zeker wanneer deze gegevens bevatten van andere klanten.
- **Logging en monitoring**: Met de transitie van on-premisse naar cloudomgevingen verandert de wijze waarop logging en monitoring vormt krijgt. De migratie van applicaties en diens data naar de systemen van de cloudprovider leidt veelal tot (een gevoel van) verlies van controle en zicht op logdata.

[78] Zie Rijks Cloudkader, paragraaf 3 en brief in volgende noot.

op de gerechtvaardigde verwachting dat de gegevens bewijs opleveren voor het onderzoek naar het strafbare feit (*probable cause*).[79]

46. Ook de Nederlandse opsporingsautoriteiten hebben in bepaalde gevallen bevoegdheden tot vordering van bewijs en inmiddels is Europese wetgeving in een vergevorderd stadium, die erop is gericht de grensoverschrijdende toegang tot *e-evidence* tussen lidstaten te verbeteren voor Europese opsporingsautoriteiten.[80] Daartoe wordt een Europees verstrekkingsbevel en een bewaringsbevel in het leven geroepen die kunnen worden verstuurd aan internetdienstverleners die diensten aanbieden in de EU. De Europese Commissie is verder inmiddels in onderhandeling met de VS om een bilaterale overeenkomst met de VS mogelijk te maken voor grensoverschrijdende verzoeken tot elektronisch bewijs.[81]

47. Wat betreft controle over Europese data, is vanuit soevereiniteitsperspectief zorgwekkender dat de Amerikaanse *inlichtingendiensten* voor spionage doeleinden en terrorisme bestrijding bepaalde bevoegdheden hebben om op trans-Atlantische kabels buitenlandse data *in transit* naar de VS af te tappen, en verder bevoegdheden hebben data op te vorderen bij de Amerikaanse cloudaanbieders indien deze op servers in de VS worden gehost.[82] Twee specifieke aftapbevoegdheden[83] zijn recent aanleiding geweest voor het Hof van Justitie in het bekende *Schrems II-arrest*,[84] om te bepalen dat het recht van de VS geen gelijkwaardig niveau van bescherming biedt aan persoonsgegevens van Europese burgers die naar de VS worden doorgegeven. Daarmee is niet voldaan aan de vereisten van de Algemene Verordening Persoonsgegevens (**AVG**) en het Handvest van de grondrechten van de Europese Unie. Het arrest heeft verstrekkende gevolgen, omdat in landen zoals China, Rusland en India de autoriteiten vergelijkbare aftap bevoegdheden hebben. Ook hier staan de data doorgiftes als gevolg ter discussie.

---

[79] Brief Ministerie van Justitie en Veiligheid aan de Tweede Kamer inzake CLOUD Act, d.d. 5 oktober 2018. In deze brief wordt erop gewezen dat de cloud aanbieders de mogelijkheid hebben een dergelijk bevel aan te vechten door in het geval van conflicterende rechtsregels een beroep doen op de Amerikaanse rechter volgens de *comity procedure* in de zin van de CLOUD Act. Onze informatie is dat de kans van slagen van een dergelijk beroep bijzonder klein is. De Amerikaanse rechter heeft verder de mogelijkheid om de cloudaanbieder een zogenaamde *gagging order* op te leggen, hetgeen betekent dat de cloudaanbieder de opdrachtgever niet mag informeren dat deze een dergelijk bevel heeft gekregen.

[80] Regulation on European Production and Preservation Orders for electronic evidence in criminal matters COM(2018) 225 final https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN en Directive laying down harmonised rules on the appointment of legal representatives for the purposes of gathering evidence in criminal proceedings, COM(2018) 226 final.

[81] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890.

[82] Zie voor een (nog steeds up-to-date) overzicht van de mogelijkheden van aftappen door de Amerikaanse inlichtingendiensten van gegevens van niet-Amerikanen, Summary of U.S. Foreign Intelligence Surveillance Law, Practice, Remedies and Oversight, Ashley Gorski, American Civil Liberties Union Foundation, 30 augustus 2018, https://www.aclu.org/sites/default/files/field_document/cjeu_schrems_report_final_august_30_2018.pdf. Dit rapport dateert uit 2018,

[83] Dit betreft de bevoegdheden van de Amerikaanse inlichtingendiensten op grond van Section 702 van de Foreign Intelligence Surveillance Act ("FISA") en Executive Order ("EO") 12333.

[84] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, ECLI:EU:C:2020:559 (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=10382780.

48. Het Hof laat de mogelijkheid open dat organisaties aanvullende mitigerende maatregelen treffen die in specifieke gevallen de tekortkomingen adresseren waardoor doorgiftes toch kunnen plaatsvinden.[85] Omdat de Amerikaanse inlichtingendiensten niet gebonden zijn aan contractuele maatregelen tussen de data exporteur en importeur, ligt voor de hand de aanvullende bescherming te zoeken in encryptie van de data. De data kan dan nog steeds worden afgetapt, maar de vreemde staten kunnen hier dan weinig mee. In dit verband wordt vaak over het hoofd gezien dat encryptie vooralsnog alleen mogelijk is bij *data at rest* en bij *data in transit*. Encryptie is tot nu praktisch niet mogelijk wanneer data worden bewerkt (*data in use*). Ook hier zien we technische innovaties, waarbij ook data *in use* kan worden ge-encrypt (zogenaamde *homomorphic encryption*).[86] De Amerikaanse cloudproviders komen hier als eerste met toepassingen.[87] Met deze vorm van encryptie wordt zeker gesteld dat de Amerikaanse inlichtingendiensten geen toegang hebben tot identificeerbare data, ook niet als deze worden bewerkt. Tegelijkertijd wordt zeker gesteld dat de providers zelf de data wel kunnen analyseren om zo inzichten te kunnen genereren. Deze innovatie zal daarmee de dominante positie van deze aanbieders alleen nog maar versterken.

> Data kan zich in drie stadia bevinden:
> ***Data at rest***: de data is inactief en is opgeslagen, bijvoorbeeld in een database.
> ***Data in transit***: de data wordt getransporteerd over een netwerk.
> ***Data in use***: de data wordt verwerkt in een applicatie.

> ***Homomorphic encryption*** is een vorm van encryptie die toelaat dat er bewerkingen op de data worden gedaan, zonder dat deze eerst moet worden ontsleuteld.

2. Exportbeperkingen opgelegd door vreemde mogendheden

49. In toenemende mate worden Nederland en de EU geraakt door exportbeperkingen ten gevolge van de oplopende handels- en ideologische spanningen tussen de VS en China. Recente voorbeelden zijn de in de inleiding genoemde Amerikaanse ban van Huawei als leverancier van Amerikaanse telecominfrastructuur, en de beperking voor Huawei om computer chips aan te kopen die buiten de VS met Amerikaanse technologie zijn geproduceerd.[88]

50. Europa-breed speelt dit in de leverancierskeuze voor 5G apparatuur, waar Huawei een belangrijke potentiële gegadigde voor is. Indien deze spanningen aanhouden moet er rekening mee worden gehouden dat beperkingen zich gaan uitstrekken naar andere apparatuur, zoals de Huawei servers die cloud ondersteunen, de aanwezigheid van Chinese leveranciers in het Internet of Things, camera's, airport scanners, en andere bewakingsapparatuur en drones van Chinese oorsprong. Het toegeven van lidstaten aan Amerikaanse druk zal mogelijk leiden tot verdere Chinese druk op Europese regeringen, met bijvoorbeeld dreigingen van Chinese importbeperkingen voor Europese apparatuur en producten.

51. Deze voorbeelden laten zien dat Nederland en de EU in hun soevereiniteit worden beperkt door geopolitiek-gemotiveerde maatregelen van derde landen, in het bijzonder van de VS en China. Gevolg hiervan is dat 5G, een kritische digitale infrastructuur, hoogstwaarschijnlijk kostbaarder wordt nu de *multi-vendor choice* afneemt. Dit raakt uiteindelijk onze digitale soevereiniteit en maakt indringender dat we ook een eigen aanbod ontwikkelen waardoor we minder afhankelijk zijn van een multi-vendor strategie.

---

[85] Zie rov. 133
[86] Zie hierover: Fact and Fiction of Homomorphic Encryption, https://www.darkreading.com/attacks-breaches/the-fact-and-fiction-of-homomorphic-encryption/a/d-id/1333691
[87] Zie voor aanbod Microsoft: https://azure.microsoft.com/en-us/blog/dcsv2series-vm-now-generally-available-from-azure-confidential-computing/; IBM: https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/ en Google: https://eprint.iacr.org/2019/723.pdf.
[88] https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html.

4. Benaderingen realiseren digitale soevereiniteit

52. In de praktijk zien we drie benaderingen voor strategische autonomie, dus om` digitale soevereiniteit te realiseren. De eerste is een *risicomanagement benadering*, gebaseerd op *state of the art* en *best effort*. Voorbeelden zijn de NIB Richtlijn en de Europese Algemene Verordening Gegevensbescherming (AVG). De cybersecurity verplichtingen onder deze regelgeving zijn *risk based*, waarbij de te treffen beveiligingsmaatregelen passend moeten zijn in het licht van de stand van de techniek, de uitvoeringskosten, en de context (hoe kritisch is het systeem en hoe gevoelig de toepassing en de gegevens).

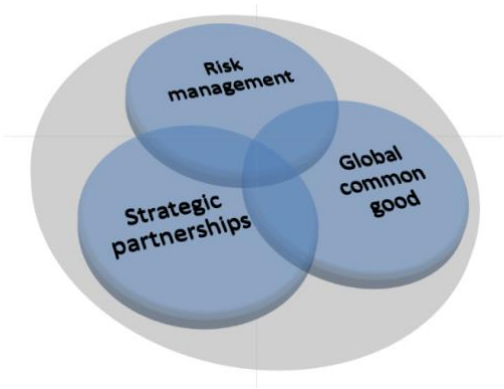
53. De tweede benadering is gebaseerd op het vertrouwen op strategische partners die *like-minded* zijn, dus het aangaan van strategische partnerschappen. Like-minded partners kunnen andere staten zijn en ook bedrijven, of beiden, in een publiek-private samenwerking. De primaire intentie is om afhankelijkheden van derde partijen die niet like-minded zijn uit te sluiten of tot uitzonderingen te beperken (een dergelijke intentie bestaat niet in de risico management benadering). Een voorbeeld is het eerder vermelde *European Cloud Federation Initiatief* (een publiek-privaat initiatief). Met wetgeving kunnen er strikte verplichtingen tussen de like-minded partijen zijn. Een voorbeeld is de *EU Foreign Direct Investment Regulation*, die regels oplegt voor gezamenlijke beoordeling van buitenlandse investeringen (zoals bedrijfsovernames) daar waar *essentiële belangen* van lidstaten en EU in het gedrang kunnen komen. Voorbeelden van nog beperktere, interstatelijke, strategische partnerschappen zijn de *Five Eyes Alliance* op het gebied van intelligence (VS, VK, Canada, Australië, Nieuw-Zeeland) en de *SOG-IS* samenwerking voor security certificatie door 13 Europese landen.[89] Strategische partnerschappen kunnen ook worden gecombineerd met *strategic interdependency*, waarbij tussen *not- like-minded* partijen op geselecteerde onderwerpen wederzijdse afhankelijkheden gelden (in EU beleid heet dit *open strategic autonomy).* Ook dit concept heeft wortels in de militaire wereld, zoals in wapenbeheersingsverdragen.[90]

54. De derde benadering is het op *mondiaal niveau* samenwerken aan oplossingen in het gemeenschappelijk belang (*global common goods*). Deze overstijgen het nationale belang, of althans conflicteren daar niet mee. Een voorbeeld is het Internet zoals de pioniers dit oorspronkelijk voor ogen hadden. Voor sommigen was die visie gemotiveerd door ideologie over soevereiniteit[91] of door techno-idealisme. Dit ideaal is niet houdbaar gebleken en inmiddels is het Internet meer en meer een splinternet aan het worden.[92] Niettemin heeft het internet nog steeds *global common goods,* zoals het internet domein naam systeem[93] dat grotendeels door de mondiale organisatie ICANN wordt beheerd. De *global common goods* benadering is ook bekend op andere terreinen. Een van de grote successen is de erkenning en de bescherming van de ozonlaag als een bezit en belang van de mensheid als geheel, dankzij het Protocol van Montreal uit 1987.

55. De drie benaderingen sluiten elkaar niet volledig uit, maar waar ze overlappen spreken we over de uitzonderingen op de regel. Van belang is dus het *primaire* uitgangspunt van de benadering: risicobeheersing, strategische samenwerking van like-minded partijen of het wereldwijde gezamenlijke belang. Het diagram geeft de drie benaderingen weer.

---

[89] https://www.sogis.eu/.
[90] Paul Timmers, Strategic Autonomy and Cybersecurity, https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf, mei 2019.
[91] Bekend is de Declaration of the Independence of Cyberspace van John Perry Barlow, een van de Internet pioneers: "Governments […] You are not welcome among us. You have no sovereignty where we gather".
[92] Kieran O'Hara en Wendy Hall, https://www.wired.co.uk/article/internet-fragmentation, 24 december 2019.
[93] Het domain naam systeem of DNS vertaalt internet adressen zoals 145.58.22.3 naar meer begrijpelijke namen zoals NPO.nl.



Figuur 1 Drie benaderingen van strategische autonomie

56. Het belang van het onderscheiden van de drie benaderingen in het kader van dit artikel is dat de keuze van primaire benadering de verhoudingen tussen staten beïnvloedt, met staatsrechtelijke consequenties. In een *global common good* benadering denken we aan internationale afspraken waar alle landen aan kunnen deelnemen, zoals binnen de Verenigde Naties. Voor *strategic partnerships* denken we aan afspraken met een exclusiviteit van deelnemers zoals wetgeving die een exclusieve groep van staten bindt (voor Nederland primair de EU) of contractuele privaat-publieke partnerschappen. Voor de risicomanagement benadering is het hele spectrum mogelijk van zachte en harde afspraken, op nationaal, EU, bi-/multilateraal, of mondiaal niveau. Overigens zien we bij de risicobenadering dat vaker de private sector de leiding heeft dan de overheid, zelfs zodanig dat President Macron verzuchtte dat we onze soevereiniteit in de handen van de telecom industrie hebben gegeven.[94] Hier gaan we straks nader op in.

57. Door de veelzijdigheid van de oorzaken waarom onze digitale soevereiniteit onder druk staat en de snelle geopolitieke ontwikkelingen, is er geen *one-size-fits-all* oplossing voorhanden. Het meest voor de hand ligt om onze soevereiniteit integraal te ondersteunen door een 'slimme' combinatie van de drie benaderingen.

58. Een 'slimme' aanpak betekent ook het maken van een kosten/baten afweging. Eerder is gezegd dat het niet reëel en ook niet wenselijk is voor de EU, laat staan voor Nederland, om allerlei technologieën volledig onder eigen beheer te willen ontwikkelen. Globalisering heeft enorme voordelen gebracht, zeker ook voor Nederland. Balkanisering van technologie en protectionisme kan wereldwijde handel belemmeren en daarmee welvaart en banen kosten in Nederland. Nederland doet er derhalve goed aan zijn afhankelijkheden te inventariseren en eenzijdige afhankelijkheden te verkleinen. Dit niet alleen binnen de bekende samenwerkingsverbanden van EU en NAVO, maar we zullen actief op zoek moeten gaan naar landen in andere delen van de wereld die karakteristieken met ons delen, zoals democratische politiek, een open economie en een beleid van vreedzame conflictresolutie.[95]

59. Kosten/baten afwegingen moeten ook worden gemaakt waar soevereiniteit de bescherming van waarden en cultuur betreft. Dit is een discussie die ook in de politiek dient te worden gevoerd. Hoeveel zijn we bereid te investeren in eigen e-identity oplossingen om te voorkomen dat iedereen inlogt op digitale diensten met een Google of Facebook- account? Hoeveel risico zijn we bereid te lopen het vertrouwen in onze rechtspraak te verliezen door op

[94] The Economist, 9 november 2019.
[95] 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.

buitenlandse cloudproviders te vertrouwen? Vinden we het acceptabel dat de grote tech bedrijven in feite bepalen wat wel en niet beschikbaar is op sociale media?

5. Wat doen we eraan en waarom is dit lastig?

60. In dit hoofdstuk analyseren we een aantal acties die worden ondernomen om digitale soevereiniteit te versterken, op internationaal, Europees en nationaal niveau. Opnieuw zullen we de staatsrechtelijke relevantie benoemen. Vervolgens geven we drie illustratieve voorbeelden, de cloud strategie, cyberweerbaarheid in de NIB Richtlijn en e-identiteit. We concluderen met een aantal belemmeringen en uitdagingen, als opstap naar het laatste hoofdstuk, dat een perspectief voor de toekomst schetst.

1. Internationaal

61. Het is bijzonder lastig om op nationaal niveau op te treden tegen cybercrime omdat ICT systemen op afstand worden binnengedrongen. Het is ook bijzonder moeilijk om hierop internationaal actie te ondernemen – bijvoorbeeld door sancties op te leggen – omdat de daders vrijwel geen spoor achterlaten of zich kunnen voordoen als een andere partij (dit is het attributie probleem in cybersecurity). Waar cyberaanvallen worden uitgevoerd door vreemde staten of waar cybercriminelen worden gesteund door vreemde staten, zullen rechtshulpverzoeken aan deze staten geen gehoor vinden.

62. Nederland zet daarom sterk in op het maken van internationale afspraken over normen voor verantwoord gedrag van overheden in cyberspace, vooral in de Verenigde Naties. De EU-lidstaten proberen verder hun externe legitimiteit te versterken door gezamenlijk als EU op te treden in cyber-conflicten. Hiertoe is een *cyber-diplomacy toolbox* ontwikkeld die in escalatie-procedures voorziet. De nuchterheid gebiedt te erkennen dat deze middelen en ook het VN-proces vooralsnog weinig effectief zijn. Ondermijning van democratische processen, het gebruik van cyber-wapens in internationale conflicten, en cyber-spionage gaan onverminderd voort.

63. Nederland is ook partner in internationale initiatieven voor vrede en stabiliteit in *cyberspace* waarin met het internationale bedrijfsleven wordt opgetrokken, zoals de *Paris Call for Trust and Security in Cyberspace*[96] en het *Geneva Cyberspace Accord*.[97] Deze initiatieven creëren geen internationaal recht maar kunnen daarvoor wel wegbereiders zijn. We zien hier wel een zekere mate van wantrouwen wanneer grote bedrijven de penvoerder of zelfs leider zijn van dit soort initiatieven en zich dan acties en status aanmeten die voorheen het exclusieve terrein van regeringen waren. Een voorbeeld is het genoemde Geneva Cyberspace Accord, een initiatief van Microsoft.

64. Sluipend soevereiniteitsverlies treedt ook op waar de industrie door middel van internationale standaardisering *de facto* de normen stelt en overheden de tweede viool spelen. Een voorbeeld is 5G – een kritische digitale infrastructuur – waar de telecomindustrie veel van de security standaarden bepaalt.[98] In dit soort fora is er een sterke aanwezigheid van Chinese bedrijven. Sommigen verdenken de Chinese overheid ervan hier de sturende kracht op de achtergrond te

[96] https://pariscall.international/en/
[97] https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.
[98] Paul Timmers, Geopolitics of Standardisation, 9 april 2020, https://directionsblog.eu/the-geopolitics-of-standardisation/.

zijn.[99] 5G is een voorbeeld waar de interne legitimiteit van de staat op het spel staat omdat de staat zich extern niet sterk genoeg kan opstellen, dus waar haar externe legitimiteit te zwak is.

65. Digitale soevereiniteit betreft dus ook het vermogen om *de jure* en *de facto* internationale regelgeving mee te kunnen bepalen, zowel als individuele staat en in toenemende mate met gelijkgezinde partners. Deze partners zouden in het bijzonder in de EU moeten worden gezocht, maar Nederland heeft historisch ook nauwe banden op het gebied van veiligheid met het VK en de VS. Ondanks de recente geopolitieke spanningen met deze landen blijven deze banden een kans om de Nederlandse digitale soevereiniteit te versterken. Het gezamenlijk optreden met het VK tegen de digitale spionage van Rusland jegens de OPCW in Den Haag is hier een voorbeeld van.[100]

2. Europese samenwerking

66. Om tal van redenen ligt voor de hand om in EU-verband op te trekken. In EU verband kunnen we in alle drie de benaderingen onze soevereiniteit versterken (risicomanagement, strategische partnerschappen, wereldwijde gedeeld belang).

67. In het kader van risicomanagement kunnen we bijvoorbeeld cyber risico's verdergaand mitigeren in de komende revisie van de Europese Netwerk- en Informatiebeveiliging Richtlijn[101] (**NIB Richtlijn**). Hieronder in de *case study* analyseren we wat een revisie vanuit soevereiniteitsperspectief op die Richtlijn zou betekenen.

68. Binnen de EU kunnen we ook interstatelijk optrekken met gelijkgestemde partijen in technologie-initiatieven waarin alleen EU-lidstaten mogen deelnemen zoals quantum-encryptie – dus in de vorm van een strategisch partnerschap. We kunnen ook denken aan aanscherping van exclusieve EU-regelgeving zoals de *Foreign Direct Investment* Verordening.

69. Tenslotte kunnen we in EU verband ook sterker inzetten op open source ontwikkeling en bijbehorende standaardisering voor het mondiale goed, zoals voor de cybersecurity van wereldwijde logistieke systemen. Daarin als EU de agenda zetten geeft ook meer slag- en onderhandelingskracht om op mondiaal niveau afspraken te maken.

70. Hoewel de EU op een groot aantal vlakken initiatieven neemt en kan nemen om 'digitale soevereiniteit' te versterken, zijn hier wel een aantal obstakels. In de kern is het probleem dat digitale soevereiniteit al gauw raakt aan de nationale veiligheid, die onder de EU Verdragen juist is voorbehouden aan de lidstaten en waar de Europese Unie een zeer beperkt mandaat heeft.[102] Artikel 4(2) van het Verdrag betreffende de Europese Unie bepaalt:

> "De Unie […] eerbiedigt de essentiële staatsfuncties, met name de verdediging van de territoriale integriteit van de staat, de handhaving van de openbare orde en de bescherming van de nationale veiligheid. Met name de nationale veiligheid blijft uitsluitend de verantwoordelijkheid van elke lidstaat."

71. Het is duidelijk dat dit Artikel 4(2) over *nationale* soevereiniteit gaat zonder het met zoveel woorden te noemen. Het Verdrag biedt geen referenties, laat staan grondslagen, voor *Europese* soevereiniteit (het woord *soevereiniteit* komt in de Europese verdragen in het geheel

[99] Zie referenties in Paul Timmers, Geopolitics of Standardisation, https://directionsblog.eu/the-geopolitics-of-standardisation/, 9 april 2020.
[100] https://www.dvhn.nl/binnenland/Defensie-Russische-actie-tegen-OPCW-verijdeld-23618009.html.
[101] European Commission, Annexes to Adjusted Workprogramme 2020, https://eur-lex.europa.eu/resource.html?uri=cellar%3Af1ebd6bf-a0d3-11ea-9d2d-01aa75ed71a1.0006.02/DOC_2&format=PDF
[102] Zie over het Europese veiligheids- en defensiebeleid, Adviesraad Internationale Vraagstukken, *Europese Veiligheid: tijd voor nieuwe stappen*, juni 2020.

niet voor).[103] Dit betekent ook dat bijvoorbeeld de *Regulatory Impact Assessment,* een analyse die bij nieuwe Europese regelgeving de voorstellen dient te motiveren en verantwoorden, momenteel geen kader biedt om de mogelijke impact op soevereiniteit van de lidstaten en de EU als geheel te analyseren en af te wegen.

72. De beperking van het *Europese* mandaat om *nationale* soevereiniteit te bewaken, heeft in het huidige tijdsgewricht een tegenovergesteld effect. Waar door de digitale en technologische ontwikkelingen de lidstaten ieder voor zich hun soevereiniteit niet langer kunnen beschermen, ondermijnt het beperkte Europese mandaat juist de nationale veiligheid. We illustreren dit hieronder met de case study inzake de NIB Richtlijn.

73. Dat het beperkte Europese mandaat hier onnodig knelt, zien we terug in de recent toegenomen bereidheid van lidstaten om in het digitale domein toch Europees samen te werken en soevereiniteit te *poolen* of te delen. Een sprekend voorbeeld is 5G security. De lidstaten hebben aan de Europese Commissie gevraagd een gezamenlijke richting voor 5G security op te stellen, zelfs al betreffen de zorgen daarover bovenal nationale veiligheid. Dat was nog niet zo lang geleden nog ondenkbaar.

3. Nationaal

74. Op dit moment zijn bijzonder weinig acties te vermelden die op nationaal niveau worden getroffen om onze digitale soevereiniteit te beschermen.[104] Onze constatering is zelfs dat we als Nederland op dit moment onvoldoende inzicht hebben in onze nieuwe afhankelijkheden en daardoor niet in staat zijn om voldoende proactief gecoördineerd beleid te kunnen voeren. De nieuwe technologieën zijn dermate onderling verweven, dat bij een eenzijdige focus op cyberweerbaarheid, de grotere implicaties voor de digitale soevereiniteit van Nederland worden gemist. Illustratief hier is de brief van de Minister van Buitenlandse Zaken namens het kabinet aan de Tweede Kamer van 17 april 2020 inzake de nationale veiligheidsstrategie.[105] Hoewel daar het onderwerp *economische veiligheid* wordt aangestipt, is dit getriggerd door (en beperkt tot) de discussie over de introductie van het 5G netwerk, de zorgen over de export van kritische technologieën naar niet-bondgenoten, en de economische spionage door China. De rol van technologie in de samenleving wordt vervolgens vooral getypeerd als een *asset* in de verschuiving van geopolitieke machtsverhoudingen, waardoor er een dreiging is van technologische afhankelijkheden. Het kabinet acht vervolgens geen verdere specifieke maatregelen nodig omdat voor een open en innovatief Nederland technologische samenwerking en wederzijdse afhankelijkheden juist voordelig zijn.

> "Technologie is, **naast** de grote economische en maatschappelijke waarde, een onmisbare *asset* in de verschuiving van geopolitieke machtsverhoudingen. Er kunnen daarom reële dreigingen kleven aan technologische afhankelijkheden waarover Nederland en de EU een zelfstandige afweging moet maken. Het kabinet sluit de ogen niet voor deze veiligheidsrisico's, maar erkent tegelijkertijd dat wederzijdse afhankelijkheid en vervlechting ook kunnen bijdragen aan stabiliteit en veiligheid. Voor een open en innovatief land als Nederland schuilen belangrijke risico's in de politisering van de toepassing en samenwerking op gebied van technologische vooruitgang."[106] (vetdruk toegevoegd)

[103] Afgezien van een zeer beperkte referentie naar enkele territoriale kwesties onder VK soevereiniteit.
[104] We zitten nog in de verkennende fase, waar de Cyber Security Raad heeft aangekondigd een advies inzake digitale soevereiniteit uit te zullen brengen en ook het Ministerie van Economische Zaken een onderzoeksopdracht heeft uitgezet.
[105] https://zoek.officielebekendmakingen.nl/kst-33694-57.html
[106] De Kamerbrief refereert overigens wel naar beschermingsmaatregelen zoals de Wet Ongewenste Zeggenschap Telecommunicatie.

75. In onze ogen mist deze analyse een meer uitgewerkte en gebalanceerde afweging wat betreft digitale technologieën. Namelijk een beschouwing over zowel hun *waarde* voor economie en maatschappij als hun *bedreiging* van onze essentiële economische ecosystemen en vertrouwen in de rechtstaat en democratie. Als die verdieping wordt gemaakt kan er ook een meer gebalanceerd menu van maatregelen worden ontwikkeld.

76. Sprekend voorbeeld van het ontbreken van bredere soevereiniteitsoverwegingen is het cloudbeleid van onze overheid. Eerder zagen we dat binnen Nederland verschillende Cloudkaders zijn opgesteld, die niet bindend zijn en verder op belangrijke onderdelen verschillende beleidskeuzes maken.

77. De Cloudkaders adresseren verder vooral de directe eisen die aan een specifiek cloudproject dienen te worden gesteld en nemen geen bredere overwegingen van digitale soevereiniteit mee. Gevolg hiervan is dat door overheidsinstanties telkens per project een afweging wordt gemaakt tussen de voordelen van public cloud (betere beveiliging, betere functionaliteiten) en de specifieke afhankelijkheden in het betreffende project. Niet worden meegenomen de steeds verdergaande afhankelijkheden en verlies van soevereiniteit. Dit leidt ertoe dat voor elk project de beslissing te rechtvaardigen is, maar dat uiteindelijk deze beslissingen gezamenlijk onze soevereiniteit wel degelijk bedreigen (een voorbeeld van *The Tragedy of the Commons*).[107] De eerste *case study* bespreekt in hoeverre Europees beleid en initiatieven hier verandering kunnen brengen.

B. CASE STUDIES

1. Cloud / GAIA-X

78. De afhankelijkheden van buitenlandse partijen en de impact daarvan op de digitale autonomie en concurrentiepositie van de EU hebben geleid tot een reeks van EU-beleidsvoorstellen.[108] Het belangrijkste doel van deze voorstellen is te komen tot een gezamenlijke Europese digitale innovatiestrategie en agenda, niet alleen voor cloud, maar ook op het gebied van AI, en het creëren van zogenoemde *European data spaces*. Deze voorstellen zijn ingegeven door de zorg dat deze voorzieningen en de gerelateerde data en kennis onder buitenlandse controle dreigen te komen.

79. **Data spaces**. Belangrijk onderdeel van de beleidsinitiatieven is om uiteindelijk de waarde van Europese data voor Europa zelf te kunnen ontsluiten. Opdrachtgevers zetten nu ieder voor zich hun data in de cloud van de hyperscalers, waardoor silo's ontstaan en iedere gebruiker voor zich niet genoeg data beschikbaar heeft voor AI-gerelateerde innovatie. Het streven is om voor bepaalde clusters met gemeenschappelijke belangen (bijv. een bepaalde industrie, ziekenhuizen, maar ook overheden), gemeenschappelijke *data spaces* te creëren, zodat de voor innovatie voor deze groep vereiste schaal aan data kan worden wordt bereikt.

80. **Opschaling door interoperabiliteit**. Doel van de voorstellen is verder te komen tot de vereiste *schaalbaarheid* van de cloudinfrastructuur die benodigd is voor AI-gerelateerde

[107] De Tragedy of the Commons is in feiten een conflict tussen individuele en collectieve belangen, waarbij juist taak is van de overheid is om de collectieve belangen te behartigen.
[108] Zie met name: 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.*

innovatie, niet door het creëren van eigen verticale Europese hyperscalers, maar door het huidige Europese aanbod van cloud-infrastructuur te vernetwerken (interoperabel te maken), waardoor opdrachtgevers binnen dat netwerk kunnen opschalen. Dit wordt bereikt door het stellen van gemeenschappelijke technische standaarden en juridische kaders voor de digitale infrastructuur en standaardisering van contractvoorwaarden. Deze vorm van interoperabiliteit gaat dus verder dan portabiliteit van data en applicaties van de ene naar de andere leverancier ter voorkoming van vendor lock-in; het betreft echt het creëren van open API's, interoperabiliteit van sleutel beheer bij encryptie, eenduidig identity & access management, etc.

81. Het GAIA-X project is niet zo alomvattend als het Europese beleid, maar is wel een concrete realisatie van de voor het Europese beleid benodigde open interfaces, standaarden, en interconnectie. Vanuit digitale soevereiniteit is het GAIA-X project een logisch en veelbelovend initiatief.[109] Hetzelfde geldt voor de andere beleidsvoorstellen. Als we echter het geheel van beleidsvoorstellen overzien, is onze conclusie vooral dat de voorstellen vooralsnog niet-verplichtend zijn. Op dit moment is er een grote mate van vrijblijvendheid waardoor ook de vereiste coördinatie ontbreekt.

82. Als gevolg zijn cloud-keuzes van de overheden van de lidstaten op dit moment op zijn best onderworpen aan de specifieke eisen die in de nationale cloudkaders aan zulke uitbestedingen worden gesteld. Het gebrek aan bindend Europees en Nederlandse cloudbeleid illustreert een meer algemeen patroon van het ontbreken van overwegingen inzake soevereiniteit dat we ook op andere gebieden terugzien.

2. NIB Richtlijn

83. De NIB Richtlijn betreft de cyberweerbaarheid (*cyber-resilience*) van geselecteerde *essentiële diensten* zoals de voorzieningen voor water, energie, en transport. De Richtlijn reguleert ook een drietal 'digitale diensten', namelijk elektronische markplaatsen, zoekmachines en clouddiensten. De NIB Richtlijn heeft risicomanagement als uitgangspunt en legt cyber security verplichtingen op, en ook een meldplicht van cyber security incidenten. De lidstaten dienen verder zogenaamde *Computer Security Incident Response Teams* op te zetten en verder met de andere lidstaten samen te werken, zowel voor strategische planning als om incidenten af te handelen. Die samenwerking is vereist omdat incidenten in kritische voorzieningen serieuze grensoverschrijdende effecten kunnen hebben[110] en daarmee het functioneren van de EU interne markt als geheel kunnen ondermijnen.

84. Toen de NIB Richtlijn in 2013 door de Europese Commissie werd voorgesteld was digitale soevereiniteit nog niet eens bekend als begrip. De focus was op het verhogen van de cyberweerbaarheid van Europa. De voorstellen leidden al snel tot spanning met nationale veiligheid, hetgeen is voorbehouden aan de lidstaten. Dit zorgde ervoor dat de NIB-richtlijn in de onderhandelingen uiteindelijk werd beperkt tot het harmoniseren van cyber-risicomanagement voor onze vitale sectoren, die een territoriale aanwezigheid vereisen en slechts enkele digitale infrastructuren.

85. De NIB Richtlijn diende op 9 mei 2018 in de nationale wetgeving van de lidstaten te zijn omgezet. De ontwikkelingen gaan echter zo snel dat nu al blijkt dat belangrijke cyber-

[109] In Nederland draagt een coalitie van TNO en aantal brancheverenigingen actief bij aan het GAIA-X project, https://www.agconnect.nl/artikel/nieuwe-infrastructuurcoalitie-wil-nederlandse-gaia-x-behoeften-representeren

[110] CSR Advies Cyberweerbaarheid IACS, p. 11 adviseert daarom om binnen de vitale infrastructuur regelmatig bij cyberoefeningen de internationale afhankelijkheden meet te nemen.

kwetsbaarheden niet worden ondervangen terwijl die wel een risico vormen voor onze soevereiniteit:

- Actief misbruik van sociale media en media in het algemeen (zoals *fake news*), wat inmiddels aan de orde van de dag is en onze democratie en waarden ondermijnt.

- Kwetsbaarheden in IACS (of SCADA) systemen van de industrie in vitale sectoren zoals productie en levering van medicijnen.

- Het stelen van intellectuele eigendom die essentieel is voor onze economische toekomst. Volgens het CSBN wordt dergelijke intellectuele eigendom op grote schaal door buitenlandse mogendheden gestolen – in het bijzonder door China - en is dat een van de grootste bedreigingen voor de economische toekomst van Nederland.

86. Er zijn ook nieuwe essentiële infrastructuren die volledig Europees zijn en niet onder de NIB Richtlijn vallen. Deze overstijgen dus nationale soevereiniteit, behoren niet toe aan een enkel land, en zijn *de facto* nu al deel van EU-soevereiniteit. Ze kunnen alleen worden beschermd in Europees verband. Voorbeelden zijn:

- Het Europese .eu domeinnaamregistratiesysteem. Er zijn aanhoudende aanvallen op de Internet domeinnaam systemen, een grote zorg voor ICANN, de internationale organisatie voor domeinnaambeheer. De DYN-aanval (2016) leidde bijvoorbeeld tot het uitvallen van Internet in een deel van de VS.[111]

- De aangekondigde *European Data Spaces*, zoals voor gezondheidsdata. Deze Europees-brede data infrastructuren moeten een essentiële rol gaan vervullen bijvoorbeeld in de grensoverschrijdende strijd tegen besmettelijke ziektes zoals COVID-19. De bescherming van deze data spaces moet nog worden geregeld[112].

87. De NIB Richtlijn wordt eind 2020 door de Europese Commissie herzien. Dit lijkt dus hét moment om althans een aantal van de voornoemde zwakke plekken wettelijk te ondervangen. Het beperkte mandaat van de EU waar cyber-weerbaarheid raakt aan nationale veiligheid blijft echter een obstakel, dus dit is makkelijker gezegd dan gedaan.

88. Een tweede obstakel is dat de NIB richtlijn is gebaseerd op het *Interne Markt* artikel 114 van het Verdrag betreffende de Werking van de Europese Unie. De Interne Markt betreft het vrij verkeer van goederen, diensten, kapitaal en personen in de EU. Het is niet bepaald evident dat cyber-weerbaarheid van sociale media of bescherming van intellectuele eigendom onder deze grondslag kan vallen, aangezien er geen duidelijke dimensie is van vrij verkeer. Het alternatief om bescherming van sociale media of intellectuele eigendom dan maar over te laten aan het nationale niveau is weinig aantrekkelijk. Aanvallen kennen geen grenzen en zijn zo gesofisticeerd dat kleinere landen de strijd riskeren te verliezen. Deze zullen in groter verband dienen te worden beveiligd. Het gaat echter nog een hele discussie worden om een grondslag voor de bescherming van sociale media te vinden.

89. Tot slot zijn er essentiële gebieden zoals volksgezondheid waar het EU-mandaat nog beperkter is dan dat van de Interne Markt. De tabel hieronder[113] geeft een overzicht van de

[111] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack.
[112] In heel beperkte mate wordt cybersecurity vermeld in de Data Governance Act, een verordening over het EU-breed delen van data (op 27 november 2020 door de Europese Commissie voorgesteld).
[113] Paul Timmers, When Sovereignty Leads and Cyber Law Follows, 13 oktober 2020, https://directionsblog.eu/when-sovereignty-leads-and-cyber-law-follows/.

voorzieningen waarvoor kan worden beargumenteerd dat die verplicht cyberbescherming zouden moeten hebben, althans als we soevereiniteit serieus nemen.

Cyberbestendigheid van	Rechtsgrondslag in de Verdragen	EU-mandaat
Geselecteerde fysieke en digitale infrastructuur	Artikel 114 VWEU Interne markt	Sterk
Telecommunicatie	Artikel 114 VWEU Interne markt	Sterk
Sociale media en media	Artikel 6, lid 1 VEU, grondrechten	Zwak
Industriële infrastructuur	Artikel 114 Artikel 173 VWEU (Industrie)	Sterk Zwak
Intellectuele eigendom	Artikel 114 VWEU Interne markt Artikel 173 VWEU (Industrie) Artikel 182, 183 Onderzoek	Zwak Zwak Gemiddeld
Internetdomein .eu	Artikel 170 Trans-Europese netwerken	Sterk
Europese gegevensruimten	Afhankelijk van het gebied, bijv. - Artikel 168 Volksgezondheid - Artikel 114 Interne markt?	 Zwak Sterk
Onderwijs	Geen werkelijke wettelijke basis	Afwezig

90. Uit voorgaande tabel volgt, dat zelfs als we zoveel mogelijk genoemde voorzieningen in een herziene NIB Richtlijn zouden proberen te ondervangen, het resultaat een wirwar van grondslagen zou zijn: Interne Markt (Artikel 114); Volksgezondheid (Artikel 168); Trans-Europese netwerken (Artikel 172, de grondslag van .eu); Industrie (Artikel 173), enz. Op zich is mogelijk om een herziene NIB Richtlijn op meer dan één wettelijke basis te laten rusten[114]. De vraag is echter of de EU wel is gebaat bij dergelijke ingewikkelde wetgeving, terwijl de werkelijke gemeenschappelijke noemer is de bescherming van soevereiniteit. In het afsluitende hoofdstuk gaan we in op deze vraag.

3. E-identiteit

91. Een vergelijkbare reflectie is nodig voor de lopende herziening van de eIDAS Verordening, die wederzijdse erkenning in de EU reguleert van aangemelde nationale elektronische identiteiten voor burgers (**eID's**). Deze Verordening moedigt de lidstaten aan om hun elektronische identificatie van burgers voor inloggen op digitale overheidsdiensten (in Nederland: DigiD) ook beschikbaar te stellen voor gebruik door het bedrijfsleven voor online e-commerce transacties.[115]

92. Voor een florerende e-commerce dienen belangrijke randvoorwaarden goed te worden geborgd: veiligheid, vertrouwen en betrouwbaarheid van de digitale infrastructuur. eID's vormen daarvoor een noodzakelijke pijler. In de fysieke wereld kunnen we ons nauwelijks economische transacties voorstellen zonder zekerheden over de identiteit van een wederpartij, over eigenaarschap van onroerende goederen, en of iemand is gemachtigd om wat te doen.

[114] Dit artikel is gedateerd vóór het voorstel tot herziening van de NIB Richtlijn (voorzien voor eind 2020).
[115] Zie overweging 17 van eIDAS.

Daarvoor heeft de overheid in de fysieke wereld een heel stelsel van middelen en organisaties ontwikkeld, zoals paspoorten en identiteitskaarten, het kadaster voor zekerheid omtrent eigendom van onroerend goed, de kamer van koophandel voor zekerheid over bevoegdheden van vertegenwoordigers van bedrijven, notarissen en gemeentebalies. Voor deze structuren bestaan wettelijke kaders en garanties.

93. De overheid heeft DigiD ontwikkeld voor toegang tot digitale overheidsdiensten, maar authenticatie van vertegenwoordigers van bedrijven en authenticatie van burgers in het private domein zijn vooralsnog aan de markt overgelaten. Daardoor beschikken burgers vooralsnog niet over een veilig en privacy-vriendelijk eID dat vrijelijk voor e-commerce kan worden gebruikt.

94. Op dit moment moeten burgers derhalve voor bijna iedere commerciële dienst nog steeds inloggen met het kwetsbare systeem van gebruikersnaam gecombineerd met wachtwoord en daarbij handmatig (steeds dezelfde) persoonsgegevens invoeren en prijsgeven. Om inloggen te versimpelen bieden veel websites burgers de optie om zich te authentiseren via hun account bij een van de grote buitenlandse platformen, zoals Facebook, Apple, Amazon, Google, Alibaba of Tencent. Hierdoor ontstaan bij deze platformen grote concentraties van zowel Nederlandse bedrijfs- als persoonsgegevens, hetgeen direct gevolgen heeft voor onze privacy en digitale soevereiniteit.

95. De vraag is of we in Nederland voldoende aankoersen op het neerzetten van een solide digitale infrastructuur, die burgers en bedrijven beschermt in het digitale tijdperk en de economische groei faciliteert in de volgende fase van de digitale interne Europese markt.[116]

96. Wat betreft de eIDAS Verordening kondigde Ursula Von Leyen in haar eerste *State of the Union* (september 2020) aan dat er een Europese e-identiteit komt, dit tegen de achtergrond van het verlies aan controle over de data van Europese burgers. Dat is een goede stap, mits dit ook wordt gekoppeld aan een verplichting van bedrijven (en met name voornoemde platforms) om de EU-brede eIDAS, en ook de daarmee compatible DigID,[117] als inlogmiddel *te accepteren*. Het soevereiniteitsperspectief zet dus aan tot een Europese e-identiteit én een toegangsverplichting in een herziene eIDAS.

6. Waarheen vanaf hier

97. De ontwikkelingen staan niet stil en we zien dat soevereiniteit inmiddels op Europees niveau en in meerdere lidstaten *Chefsache* is geworden. De consequentie van soevereiniteits-denken zijn echter nog niet echt doorgedrongen in beleid en wetgeving. De stap die we nu moeten zetten is daadwerkelijke inbedding van soevereiniteits-denken: in Nederland, als Nederland in de EU, en als Nederland in internationaal verband.

98. In dit licht, geven we hierna een aantal perspectieven voor de toekomst, die staatsrechtelijke relevant zijn. We gaan hier wederom van het internationale, naar het Europeses, naar het Nederlandse niveau.

A. INTERNATIONALE INBEDDING

99. De stevige inbedding van Nederland in de EU en internationale organisaties (en de gebondenheid aan Europese wetgeving en internationale verdragen) is zowel een beperking als

[116] De CSR vindt van niet, zie CSR Advies Naar een veilig eID-stelsel, 7 november 2019, https://www.cybersecurityraad.nl/binaries/CSR_Advies_eID_NED_DEF_tcm107-415886.pdf.
[117] https://www.eherkenning.nl/vraag-antwoord/eidas.

een kans. Het is een beperking omdat bestaande kaders zoals Interne Markt en GATTS-afspraken de speelruimte voor Nederland beperken bijvoorbeeld wat betreft restricties op markttoelating. Nederland kan vaak niet autonoom opereren. Maar zoals betoogd, gezamenlijk optreden in EU-verband biedt ook een kans voor Nederland om haar stem sterker te doen gelden in internationaal verband.

100. Dit is des te meer het geval indien bescherming van nationale of Europese soevereiniteit spoort met een *globaal belang* (en *vice-versa)*. Goede voorbeelden hiervan zijn het beheren van kritische internetvoorzieningen zoals het internet domeinnaam systeem, het bestrijden van cybercriminaliteit in de gezondheidssector, en standaarden voor het *Internet of Things*. De implicatie hier is dat voor digitale soevereiniteit ons buitenlands beleid evenzeer van belang is als ons binnenlands beleid. Alleen door samenhangend beleid is het mogelijk om zowel de interne als de externe dimensie van soevereiniteit te versterken. Om internationaal mee te kunnen spelen is echter ook nodig om als Europa op te kunnen treden. Zoals we hebben gezien heeft de EU hier echter een beperkt mandaat. Wat hieraan kan worden gedaan staat in de volgende paragraaf.

B. Europese inbedding en de ontoereikendheid van de EU Verdragen

101. Gezien de eerder gesignaleerde beperkingen in het Europese mandaat inzake digitale soevereiniteit, is het wat ons betreft tijd om na te denken over het versterken van de Europese wettelijke basis voor EU-soevereiniteit, mits goed omkaderd. Zoals aangegeven: in termen van versterking, uitbreiding, en vereenvoudiging van de Verdragen. Het Verdrag biedt openingen voor een beperkte Verdragswijziging onder Artikel 48 TEU. Het nadeel hiervan is dat dit nog steeds lapwerk zou blijven, verspreid over meer *internal policies,* zoals interne markt, trans-Europese netwerken, en R&D. Wat ons betreft moeten we dus toch het meer fundamentele debat aangaan, bijvoorbeeld in het kader van de lopende Conferentie over de Toekomst van de Europese Unie en Artikel 48(2) VEU.

102. Wij realiseren ons dat sommigen hiervoor terug zullen schrikken omdat dit de doos van Pandora opent voor allerlei andere Verdragsdiscussies. Anderen zullen tegenwerpen dat verdere versterking van Europese soevereiniteit te ver gaat, het populistische argument rond Brexit voor ogen hebbend.

103. De belangrijkste argumenten[118] voor versterking van Europese soevereiniteit zijn:

- Europees krachtenbundeling versterkt de nationale soevereiniteit. Vrijwel elke Lidstaat staat anders te zwak in het gevecht tegen grensoverschrijdende cyber-bedreigingen.

- Een sterk Europees mandaat draagt bij aan het geloofwaardig digitaal beschermen – en creëren - van Europese soevereine voorzieningen. Het domeinnaamsysteem .eu en Europese *data spaces* zijn sprekende voorbeelden.

- Het bezitten van eigen sterke digitale voorzieningen versterkt de geloofwaardigheid van de EU in de wereld (*externe legitimiteit*) wanneer het gaat over het maken van internationale afspraken en de positie van Europa tegenover de internet giganten.

104. Timmers[119] suggereerde eerder dat soevereiniteit, zoals hierboven geïnterpreteerd, kan worden versterkt door Artikel 3 VEU als volgt aan te vullen:

[118] Paul Timmers, When Sovereignty Leads and Cyber Law Follows.
[119] Paul Timmers, When Sovereignty Leads and Cyber Law Follows.

> "de Unie zal soevereiniteit in de Europese Unie versterken in zoverre dit de soevereiniteit van de Lidstaten respecteert of versterkt, en bijdraagt aan gemeenschappelijke interesses en middelen van de Unie of de positie van de Unie in de wereld versterkt".

105. In dit licht zou een debat in Nederland over soevereiniteit in het kader van de mogelijke herziening van de Verdragen op z'n minst wenselijk zijn. Dit zou geen revolutionaire stap zijn maar eenvoudigweg in lijn met de *Zeitgeist*. Overigens zijn die drie argumenten niet nieuw, maar al sinds ca. 75 jaar deel van het denken over Europese samenwerking. In feite spreken we dus over een aanpassing van de Verdragen aan de 21e eeuw.

106. In afwachting van de uitkomst van een meer fundamenteel debat, bevelen we aan dat Nederland zich in Europees verband vooral sterk maakt voor binnen de huidige Verdragen haalbare ingrepen die een hefboomwerking kunnen hebben voor soevereiniteit. De focus moet zijn op *where sovereignty matters most.* Een voorbeeld bij uitstek is het initiatief om een Europese e-identiteit te realiseren. Het verzorgen van betrouwbare middelen ter identificatie van burgers en bedrijven ter facilitering van handel is een kerntaak van de overheid. Gezien de gemeenschappelijke belangen van de lidstaten inzake cybersecurity, is verder denkbaar dat de lidstaten op specifieke onderwerpen (zoals 5G) ook zonder fundamenteel debat, toch *soevereiniteit poolen* en tot Europese coördinatie komen.

107. Om dezelfde reden is het mogelijk om vaker te onderzoeken of Nederland met een groep lidstaten tot bepaalde afspraken kan komen, in een *coalition of the willing.*[120] Voor de levensvatbaarheid van een project is vaak niet nodig dat alle lidstaten zich verbinden, maar wel een initiële kritische massa. Dit kan dan later worden opgeschaald met aansluiting van andere lidstaten. Op deze manier wordt sneller resultaat bereikt dan via de kwetsbare route van aanpassing van de EU verdragen.

108. Buiten de scope van dit pre-advies vallen de mogelijke stappen die kunnen worden ondernomen tegen dominante marktpartijen wegens marktmisbruik en schending van consumentenrecht en privacywetgeving om data van Europese burgers te verzamelen. In de dataeconomie gaan die vaak hand in hand en bijzonder voor de hand ligt om net als voor mededinging, ook wat betreft handhaving van privacywetgeving een centrale Europese toezichthouder op te zetten. Verder dient op Europees niveau de handhaving door de mededingings-, consumenten- en privacyautoriteiten verplicht te worden gecoördineerd.[121]

C. NEDERLANDS PERSPECTIEF

109. Ook op nationaal niveau heeft Nederland nu al mogelijkheden – ook in staatsrechtelijke zin – om haar digitale soevereiniteit op nationaal niveau te versterken. De eerste stappen zijn zeker geen revolutionair ingrijpen maar veeleer een kwestie van 'gezond verstand'. We geven hieronder aantal suggesties.

110. **Van nationale veiligheid naar digitale soevereiniteit**. Eerder constateerden we dat onze nationale veiligheidsstrategie weliswaar economische veiligheid aanstipt, maar onvoldoende onderkent dat de digitale technologieën niet alleen *waarde* hebben voor economie en maatschappij, maar ook een *bedreiging* zijn van onze essentiële economische ecosystemen en

[120] Dit is ook de eerste aanbeveling van het rapport van de Adviesraad Internationale Vraagstukken, *Europese Veiligheid: tijd voor nieuwe stappen*, juni 2020: Nederland doet er goed aan zoveel mogelijk aansluiting te zoeken bij Frans-Duitse initiatieven voor Europese veiligheid, file:///C:/Users/lxm16/Downloads/Europese_veiligheid_tijd_voor_nieuwe_stappen-AIV-advies-112_202006.pdf.

[121] Caleidoscopische handhaving tegen het datagebruik van ondernemingen, Svetlana Yakovleva, Wessel Geurtesen en Axel Arnbak, Pre-advies van de Vereeninging Handelsrecht 2019, p. 77.

vertrouwen in de rechtstaat en democratie. Verder constateerden we dat we als Nederland op dit moment onvoldoende inzicht hebben in onze nieuwe afhankelijkheden en daardoor niet in staat zijn om voldoende proactief gecoördineerd technologiebeleid te kunnen voeren op het gebied van onderzoek, valoratie en industriële capaciteiten. 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. Daartoe dient bewust te worden geïnventariseerd welke start-ups, technologie, kennis en infrastructuur van strategisch belang zijn, waardoor inzichtelijk wordt gemaakt wanneer verkoop aan of vertrek naar het buitenland nadelig kan zijn voor de Nederlandse strategische positie. We dienen vervolgens een proactieve strategie op te stellen, waarvan ook strategische inzet van de *gebundelde* inkoopkracht van de overheid deel uitmaakt.[122] Zonder een dergelijk omvattend plan zal ons land terecht komen op een onomkeerbaar pad van geleidelijke erosie van onze nationale technologische en industriële capaciteiten.

111. **Cloudbeleid.** Specifiek wat betreft cloudbeleid is onze aanbeveling te komen tot een geïntegreerd en bindend cloudkader en te onderzoeken hoe Nederland maximaal kan aansluiten bij de concrete ontwikkeling van GAIA-X vanuit overwegingen van digitale soevereiniteit en zelfs om zich tezamen met een groep lidstaten daaraan te committeren. Inmiddels hebben Nederlandse cloud, hosting en infrastructuur bedrijven een coalitie gesloten om aan GAIA-X te kunnen bijdragen.[123] Voor een goede aansluiting is vereist dat ook de inkoopkracht van de Nederlandse overheid wordt ingezet voor onze kennis en concurrentiepositie op de langere termijn.

112. **Samenhangende governance.** Doordat de soevereiniteitsvraag steeds meer gebieden van economie, maatschappij en democratie raakt, dient aansturing centraal plaats te vinden. In het bedrijfsleven is men daar eerder van doordrongen. ICT is nu een strategische factor voor concurrentiekracht, en is onderwerp van de bestuurstafel ('*C-level*').[124] De overheid wordt in dezelfde richting gedreven, maar we zien dat de verschillende departementen vooral in silo's opereren en de benodigde integratie van beleid ontbreekt. Alhoewel reeds vaker voorgesteld, blijft het voor de hand liggen om op z'n minst een coördinator digitale zaken aan te stellen die direct rapporteert aan de minister-president, met eigen budget en doorzettingsmacht.[125]

113. **Memorie van toelichting**. Onze wetsvoorstellen moeten worden gemotiveerd en verantwoord in een memorie van toelichting (in Europese beleidsontwikkeling is dit de *regulatory impact assessment*). Er is momenteel geen kader om mogelijke impact op soevereiniteit te analyseren en af te wegen. Zo'n kader zou voor de wetsvoorbereiding urgent beschikbaar moeten worden gemaakt, om te voorkomen dat soevereiniteit een *afterthought* blijft.

[122] Een Nederlands voorbeeld van een proactieve strategie is de Defensie Industrie Strategie. Hierin is vanuit nationaal veiligheidsbelang (hetgeen ook cyberdreigingen omvat) beoordeeld welke kennis, technologie en industriële capaciteiten Nederland zelf in huis dient te hebben om onze nationale veiligheid te borgen, en hoe dit met actief Nederlands innovatie- en industrieel participatiebeleid kan worden geborgd, waarbij Defensie vaker optreedt als launching customer.

[123] http://www.tno.nl/nl/over-tno/nieuws/2020/11/nederlandse-cloud-infrastructuur-coalitie-cic-eerste-stap-naar-slagvaardig-digitaal-nederland/.

[124] C-level refereert aan de 'C' in de titels van bestuurders van ondernemingen, zoals CEO (Chief Executive Officer), CFO (Chief Financial Officer).

[125] Hoewel rijkelijk laat, is een stap in de goede richhting dat de Tweede Kamer inmiddels tot de vaststelling gekomen dat er een afzonderlijke vaste commissie voor digitalisering moet komen, https://www.digitaleoverheid.nl/nieuws/tweede-kamer-krijgt-vaste-commissie-voor-digitale-zaken/ Zie ook https://www.tweedekamer.nl/nieuws/persberichten/eindrapport-tijdelijke-commissie-digitale-toekomst-%E2%80%9Cupdate-vereist%E2%80%9D.

***