



Soevereiniteit en Digitale Autonomie

Auteurs: Louk Faesen (HCSS), Tom van Schie (TNO), Michel Rademaker (HCSS), Paul Timmers (European University Cyprus/iivii) en Matthijs Veenendaal (TNO)

Februari 2021

Introductie

De reeds lang gesignaleerde afhankelijkheid van buitenlandse technologie, heeft binnen Europa¹ geleid tot een discussie over soevereiniteit en digitale autonomie om zo meer zeggenschap en handelingsperspectief te creëren. Deze ambitie is al van verschillende hoeken benaderd, vanuit rechtsbescherming (mensenrechten, privacy, of mededingingsrecht), vanuit veiligheid (cybersecurity, nationale en internationale veiligheid), vanuit onderwijs (kennisopbouw) tot en met de economie (innovatie, concurrentiekracht). Dit laat zien hoe breed de ambitie wordt gedeeld en dat er tegelijkertijd geen eenduidige oplossing is.

De discussie over strategische autonomie en soevereiniteit is al een tijdje aan de gang in Brussel, maar binnen Nederland lijkt dat debat nog te ontbreken. Daarom hebben TNO en het *Den Haag* Centrum voor Strategische Studies (HCSS), samen met Prof dr. Paul Timmers verschillende experts² uit het bedrijfsleven, academische sector, en overheid bij elkaar gebracht in een workshop eind januari 2021 om op basis van recent onderzoek het Nederlandse debat en inzet op verbetering van de strategische autonomie verder te brengen.^{3,4} Deze notitie beschrijft de bevindingen en aanbevelingen die tijdens deze workshop ter sprake kwamen. Allereerst wordt de noodzaak voor strategische autonomie beschreven en wat het betekent binnen de digitale context. Vervolgens worden de uitdagingen in het investeringsbeleid en het instrumentarium uitgelegd. Tot slot, zijn er een aantal suggesties voor verdere acties die bijdragen aan het versterken van digitale strategische autonomie.

De noodzaak

Digitalisering is de afgelopen decennia de drijvende kracht geweest achter economische groei en wereldwijde integratie. Nederland bezit en ontwikkelt sleuteltechnologieën voor het digitale tijdperk, heeft een sterke digitale economie, hoge internetpenetratie, relatief veel ICT-specialisten en experts, beschikt over sterke internetinfrastructuur, is de grootste exporteur van bandbreedte, en heeft een sterke reputatie in het versterken van de internationale rechtsorde in cyberspace. Tegelijkertijd zijn Europa en Nederland vooral een afnemer van elders geproduceerde digitale

¹ <https://www.consilium.europa.eu/nl/press/press-releases/2020/09/08/recovery-plan-powering-europe-s-strategic-autonomy-speech-by-president-charles-michel-at-the-brussels-economic-forum/>

² De on-line discussie vond plaats onder Chatham House Rules waardoor de vele deelnemers niet genoemd kunnen worden.

³ Whitepaper Strategische Autonomie op Cybersecurity, Matthijs Veenendaal, Tom van Schie, Michel Rademaker en Louk Faesen, TNO & HCSS, 2020;

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

Reflecties over digitale soevereiniteit, Lokke Moerel, Paul Timmers (Staatsrechtconferentie), 2020.

⁴ In opdracht van de Cybersecurity Raad deden Paul Timmers en Freddy Dezeure verdiepend onderzoek naar en stelden een toetsingskader op voor Nederlandse strategische autonomie en cybersecurity, , , https://www.cybersecurityraad.nl/010_Actueel/een-proactieve-en-integrale-aanpak-is-noodzakelijk-voor-behoud-digitale-autonomie.aspx, februari 2021.

technologieën (met name uit de VS en China).⁵ De Cloud markt in Europa is voor tweederde in handen van Amazon, Microsoft, IBM en Google. Sociale media zijn vrijwel volledig Amerikaans. Europese telecom hardware en softwareleveranciers moesten massaal terrein prijsgeven aan Huawei en ZTE. Europese technologiebedrijven vallen ook steeds vaker in buitenlandse handen: ARM ging naar Softbank en daarna naar het Amerikaanse Nvidia, Kuka robots werd verkocht aan het Chinese Midea.

Daarnaast neemt de geopolitieke instabiliteit toe en dat uit zich onder andere in de tech-race en de toename van cyberincidenten, waardoor onze cybersecurity, samenleving, economie, democratie en fundamentele vrijheden onder nog meer druk komen te staan. Denk aan de handelsoorlog tussen de VS en China, het verschil van aanpak tussen de VS en Europa wat betreft privacy, de race voor 5G, of de Chinese zijderoute. Dit zijn allemaal voorbeelden met een sterke digitale component waarin politieke, economische en nationale veiligheidsdiscussies samenkomen. Op Europees niveau is de discussie over strategische autonomie of soevereiniteit inmiddels een topprioriteit. Europa erkent haar afhankelijkheid van buitenlandse technologie en de impact die dit heeft op haar eigen economie, concurrentievermogen, veiligheid en cybersecurity, en slaat een koers in van digitale zelfbescherming gericht op verbetering van de strategische autonomie en soevereiniteit om zo meer handelingsvermogen te creëren. Dit gaat samen met de terugkeer van industriepolitiek en de versterking van het Europees buitenlandsbeleid. In Nederland speelt de discussie echter nog beperkt en heeft nog niet geleid tot een breed debat over de nationale doelstellingen en ambities op dit terrein. Dit blijkt onder meer uit de onderlinge verschillen in bijvoorbeeld het Cloud beleid van Nederlandse ministeries.

Wat betekent strategische autonomie en soevereiniteit?

Strategische autonomie is geen einddoel op zich, maar een manier om meer handelingsperspectief te creëren ter bevordering van de eigen positie. Strategische autonomie en soevereiniteit wordt door velen verschillend geïnterpreteerd, de praktische invulling daarvan verschilt afhankelijk van de positie die men daarin kan innemen en de consequenties zijn nog zeker niet helemaal te overzien. Soevereiniteit wordt in het algemeen geassocieerd met territorialiteit, grondgebied, jurisdictie, een bevolking, gezag met interne erkenning (interne legitimiteit) en externe erkenning (externe legitimiteit). Om soevereiniteit te verkrijgen of te behouden moet het begrip operationeel worden gemaakt: wanneer en hoe soevereiniteit te realiseren? Dit wordt veelal strategische autonomie genoemd, een begrip dat uit het militaire/ defensie denken komt maar tegenwoordig toch vooral gezien wordt als het vermogen om als natie autonoom te kunnen beslissen en handelen aangaande essentiële aspecten van de langere-termijn toekomst in economie, maatschappij en democratie. Met de kanttekening dat in Europa al veel autonomie danwel soevereiniteitsaspecten door de lidstaten aan de EU zijn overgedragen op die terreinen waar de meerwaarde van het

⁵ Hoewel er nog steeds sprake is van grote wederzijdse afhankelijkheden, hebben grote buitenlandse technologieplatformen verregaande schaalvoordelen verkregen door een integratie van diensten en door strategische overnames. Daarmee hebben ze een vrijwel onoverbrugbaar concurrentievoordeel behaald op kleinere, gespecialiseerde dienstverleners. Het merendeel van deze grote partijen komt niet uit Europa, maar is wel dominant op de Europese markt, of heeft er grote invloed op.

collectief groter is dan van de individuele lidstaten.⁶ Beter zou gesproken kunnen worden van Europese autonomie. Maar deze discussie is waarschijnlijk meer politiek en mogelijk semantisch. In de praktijk zijn de meeste landen en haar bewoners het wel eens dat de EU als eenheid in de internationale arena meer effect heeft dan de *einselgang* van lidstaten.

Uitdagingen en bedreigingen die bij het verbeteren van de autonomie komen kijken zijn belangrijk om vanuit een breed perspectief te bezien en bij de top te beleggen. Uiteindelijk gaat het om de vraag welke waarden en belangen Nederland en de EU moeten zekerstellen om handelingsvermogen te behouden of creëren. Denk daarbij aan de waarden zoals die in de nationale veiligheidsstrategie zijn verwoord: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en internationale rechtsorde. Deze komen sterk overeen, danwel overlappen met wat de EU daarover stelt: Vrede bewaren, Internationale veiligheid versterken, Internationale samenwerking bevorderen, Ontwikkelen en versterken van democratie en de rechtsstaat en respect voor mensenrechten en fundamentele vrijheden beschermen. Tegelijkertijd moet soevereiniteit en strategische autonomie geen excuus zijn voor verregaande digitale staatscontrole, zoals in het Chinese cybersoevereiniteitsmodel. De rol van de Nederlandse overheid is beperkt - slagkracht vergt nauwe samenwerking tussen de industrie, kennisinstituten, overheid en de technische sector.

Investeren in innovatie

De uitdaging is de balans te vinden tussen enerzijds het optimaal benutten van de kansen die digitalisering en de vrije markt bieden en anderzijds het behouden van controle over de toepassingen van nieuwe technologieën. De overheid moet immers het (economisch) welzijn van de samenleving bevorderen en tegelijkertijd haar veiligheid beschermen. Deze twee ambities zijn in de kern niet tegenstrijdig, maar bij het bepalen van de gewenste beleidskeuzes kunnen afwegingen botsen. Het vinden van een balans tussen het versterken van de concurrentiekracht (waar ook het streven naar een *level playing field* onder valt) en het borgen van de nationale veiligheid vereist een brede maatschappelijke discussie door belanghebbenden uit de politiek, overheid, industrie en *civil society*.

De mogelijkheid voor Nederland om haar economische en veiligheidsbelangen te beschermen en te bevorderen hangt in belangrijke mate af van de (innovatie)kracht van de technologiesector en de digitale weerbaarheid van de samenleving. Het kunnen beschikken over, en vooroplopen bij, de ontwikkeling en het gebruik van geavanceerde digitale technologieën stelt staten en andere actoren in staat economische, politieke en sociale ontwikkelingen te beïnvloeden en zeker te stellen dat het gebruik aansluit op nationale en Europese waarden en normen en voldoet aan wet- en regelgeving.

Achterblijvende investeringen blijven de strategische positie van Nederland en de EU bedreigen doordat de toekomst van het digitale domein voor een groot deel wordt vormgegeven en beheerd door partijen buiten de EU. Het beperkt de invloed op - en controle over - de ontwikkeling en het toepassen van sleuteltechnologieën. Dit heeft ook impact op de mate van invloed van de EU op het

⁶ https://www.europa-nu.nl/id/vg9piqcfmzzz/buitenlands_beleid_gbv

ontwikkelen van standaarden voor nieuwe technologiegebieden. Hoe groter de technologische achterstand, hoe kwetsbaarder de Europese positie in het digitale domein zal worden. Zo kan de afhankelijkheid van buitenlandse partijen ook de cybersecurity responsecapaciteiten nadelig beïnvloeden. Cybersecurity moet dan ook niet in isolement worden gezien maar is afhankelijk van en verbonden aan de kennisbouw en innovatie voor digitale technologieën.

Instrumentarium

Overheden beschikken over een breed scala aan instrumenten die kunnen bijdragen aan het versterken van de strategische autonomie. Investeren in het versterken van de informatiepositie, kennisopbouw, technologieontwikkeling en innovatie, en het ontwikkelen (en agenderen) van normen, certificeringen, standaarden en wet- en regelgeving zoals voor het harmoniseren van de Europese interne markt en het uitvaardigen van sancties en export-controles. Nederland kan niet zelfstandig voldoende handelingsperspectief creëren om alle uitdagingen het hoofd te bieden. Proactieve samenwerking met vertrouwde publieke en private partners, binnen en buiten de EU, is noodzakelijk om de strategische autonomie in het digitale domein structureel en duurzaam te borgen.

Digitale weerbaarheid is echter geen zero-sum game waarbij alles wat niet in eigen land of door de meest vertrouwde partners is ontwikkeld of kan worden gecontroleerd, onveilig is. Samenwerking op het terrein van cybersecurity is voor de meeste partijen, zowel publiek als privaat, een vanzelfsprekendheid. Alleen door informatie, methodes en technieken te delen kan gelijke pas worden gehouden met de dreiging. Het afschermen van de eigen markt om onbetrouwbare partijen buiten te houden en de eigen markt te ondersteunen kan noodzakelijk zijn. Maar protectionistische maatregelen kunnen ook tot vergeldingen leiden, ook op andere terreinen. Dit kan dan weer de concurrentiekracht van de Nederlandse en Europese economie op de lange termijn beperken.

Het aan banden leggen van de samenwerking met specifieke landen heeft ook gevolgen voor de innovatiekracht in Nederland. Door intensieve samenwerking binnen Europa te bevorderen kan dit deels worden opgevangen. Echter, wanneer samenwerking met kennisinstellingen en private partijen van buiten Europa wordt beperkt, zal dit er ook toe leiden dat onze capaciteit om te profiteren van innovatie van buiten de EU vermindert.

De EU heeft ook sterktes, en de grote interne markt is daarvan een van de belangrijkste, waardoor - met alle beperkingen - samenwerking met 'ongelijk gestemde' landen mogelijk zal zijn. De partijen accepteren dan een wederzijdse strategische afhankelijkheid.

Mogelijke acties:

Economische openheid is een groot goed maar niet de heilige graal voor al ons handelen. Bovendien zijn er ook andere dan economische belangen te verdedigen, zoals de rechtstaat, nationale veiligheid en democratische vrijheid. Om de strategische autonomie voor de lange termijn te kunnen blijven waarborgen moet Nederland meer zicht krijgen op de stand van haar strategische

afhankelijkheid en autonomie in het digitale domein en op basis hiervan investeren in de eigen innovatie- en concurrentiekracht.

Er is geen eenduidige oplossing die leidt naar strategische autonomie. De sleutel zal met name liggen in het creëren van de juiste randvoorwaarden of basisvoorzieningen. De Nederlandse aanpak vraagt om een interdepartementaal (en met bedrijven en kennisinstellingen) afgestemde *whole-of-Nation* en zelfs *whole-of-Union* strategie. Niet alleen het defensiedomein, dat van nature al denkt in strategisch autonome handelingscapaciteit maar ook het economisch en technologisch domein moeten hierbij worden betrokken. Nederland kan enkel in EU-verband een betekenisvolle bijdrage leveren.

Alleen dan is er voldoende massa om wereldwijd relevant te blijven ten aanzien van de hoogtechnologische ontwikkelingen die noodzakelijk zijn om de digitale weerbaarheid te waarborgen. Hiervoor is een verdere politieke en economische integratie op EU-niveau nodig en de EU moet durven de macht die dat met zich meebrengt ook actief in te zetten. De capaciteit en politieke wil maken dat Nederland alleen in de combinatie met de EU haar autonomie kan verbeteren. Het vraagt een eigenstandige mening en positie van Nederland om zinvol en proactief betrokken te zijn bij politiek strategische ontwikkelingen in de EU. Nederland moet niet teruggevallen op het adagium dat de EU hierin het voortouw heeft.

Tijdens de genoemde workshop zijn een aantal acties gesuggereerd om strategische autonomie te agenderen en mogelijk te versterken.

I. Strategische afhankelijkheid en autonomie inzichtelijk maken.

Er is dringend behoefte aan inzicht in de stand van de Nederlandse digitale strategische autonomie en afhankelijkheden. Tot dusver is deze analyse vaak te oppervlakkig geweest: er wordt bijvoorbeeld gerefereerd aan het veiligstellen van sleuteltechnologieën – een *catch-all term* die technologieën niet op hetzelfde niveau definieert – zonder de noodzaak en haalbaarheid van strategische autonomie te toetsen. Voor iedere sleuteltechnologie in de Kennis en Innovatie agenda (KIA) Veiligheid (2019) zou per technologie inzichtelijk moeten worden gemaakt hoe afhankelijk of strategisch autonoom Nederland momenteel is en zou moeten zijn.⁷ Bij dit proces is het van groot belang om ook de kennisinstellingen en het bedrijfsleven te betrekken. Bovendien biedt ook de gelegenheid om proactief inzicht op te bouwen van opkomende technologieën en te signaleren of sprake is van verlies van strategische autonomie zoals sluipend groeiende marktdominantie, overnames van kritische kennis, erosie van vertrouwen door desinformatie of verkeerd gebruik van technologie, of haperende doorgroei van startups. Het proactief gebruiken van het Cybersecuritybeeld Nederland en inlichtingeninformatie is een *conditio sine qua non*.

⁷ KIA Veiligheid van EZK: *Artificial intelligence* (incl. machine and deep learning), *Big data* en *data analytics*, *Encryption technologies / digital security*, *Blockchain*, *High Performance Computing*, *Grid Computing* en *Cloud Technologies Computing*. <https://www.bedrijvenbeleidinbeeld.nl/bouwstenen-bedrijvenbeleid/missiegedreven-innovatiebeleid/sleuteltechnologieen>

2. Realistische doelstelling: welke afhankelijkheid is onacceptabel en welke mate van autonomie is haalbaar?⁸

Op basis van het overzicht uit punt 1 kan worden beslist welke afhankelijkheden (on)acceptabel zijn. Vervolgens moet een realistisch doel worden gesteld voor de verbetering van de strategische autonomie. Nederland kan dit niet op eigen houtje. Hierbij moet een onderscheid worden gemaakt tussen: (a) de Nederlandse kroonjuwelen en kernbelangen (Defensie en nationale veiligheid) die nationale strategische autonomie vergen, (b) de toepassingsgebieden van sleuteltechnologieën waarbij het noodzakelijk en realistisch wordt geacht dat Nederland in Europees verband of met andere *like-minded* partners in een *coalition of the willing* strategisch autonoom kan worden of blijven, (c) toepassingsgebieden waarop Nederland en de EU juist wereldwijde samenwerking moeten zoeken zodat deze als een *global public good* gezien en bevorderd worden en (d) de overblijvende technologieën waarvoor strategische autonomie wellicht wenselijk maar onhaalbaar wordt geacht en er alleen een benadering van best-effort risicobeheersing resteert. Er moet dus prioritering plaatsvinden op basis van de noodzakelijk en haalbaarheid. Zodra de Europese route wordt gekozen, wordt er gekeken hoe de Nederlandse bijdrage aan strategische autonomie zich verhoudt tot die van de andere lidstaten. Het lijkt voor de hand liggend om in te zetten op die technologieën en niches waar Nederland een goede uitgangspositie heeft of waar autonomie voor de bescherming van het hart van de staat nodig is (zoals encryptie).

3. Gerichte inzet van het instrumentarium: aanjagers en remmers.

Innovatieve kennisopbouw moet op een meer langjarige en integrale manier worden aangejaagd. De basis hiervoor is een actueel overzicht naar de staat van de Nederlandse afhankelijkheid en strategische autonomie. Tegelijkertijd, kan er ook gericht door de overheid geremd worden door het weren van onwenselijke actoren of het opleggen van wetgeving of standaarden. Zonder een sterke visie op dit dossier, zijn investeringen ongericht, ontbreekt bijvoorbeeld een spin-off verplichting, is er onvoldoende aandacht voor scale-ups en is de resultaatgarantie laag. Er is daarmee behoefte aan beleid dat zowel strategischer en selectiever investeert en de bereidheid industriepolitiek te voeren dat binnen de Europese kaders eisen oplegt aan buitenlandse aanbieders ten gunste van de Nederlandse/ Europese digitale strategische autonomie. Er is behoefte aan het inzichtelijk maken van het instrumentarium dat het effectiefst kan bijdragen aan strategische autonomie. Dit bevat de beleidsmogelijkheden van de overheid op nationaal en Europees niveau, maar ook de mechanismes van de private sector. Aanbevelingen 1, 2 en 3 vragen een iteratief proces, waarbij men regelmatig de staat van de Nederlandse digitale autonomie en afhankelijkheid van specifieke technologieën bijwerkt en bijstuurt. Een Europese variant van de Amerikaanse Foreign Ownership, Control or Influence (FOCI) kan hierbij helpen.

⁸ Zie hiervoor ook de flowchart op pagina 33 in: [Whitepaper Strategische Autonomie op Cybersecurity](#), Matthijs Veenendaal, Tom van Schie, Michel Rademaker en Louk Faesen, TNO & HCSS, 2020;

4. Strategic Autonomy Impact Assessment.

Integrale analyses van toepassingsgebieden voor digitale technologieën helpen een breder bewustzijn en inzicht bij beleidsmakers en directieleden te bevorderen. Een dergelijk assessment moet ervoor zorgen dat er op een holistische en gebalanceerde manier informatie samenkomt, ter vergelijking zoals impact- of milieuanalyses opgesteld worden. Dergelijke analyses kunnen voor de gehele keten van een toepassingsgebied de mate van afhankelijkheid inzichtelijk maken én inventariseren welke instrumenten ingezet kunnen worden om afhankelijkheid te beperken.

5. Strategische Autonomie/ Soevereiniteit Tafels.

Om brede betrokkenheid van de samenleving te faciliteren zou naar analogie van de Klimaattafels, een vergelijkbaar proces kunnen worden ingericht voor strategische autonomie. Met gedeeld eigenaarschap en verantwoordelijkheid om zo de inzichten en beleidsvorming te stimuleren tussen overheid, bedrijfsleven en maatschappelijk middenveld. Uiteindelijk zou dit kunnen leiden tot een Plan van Aanpak.

6. Europese integratie creëert nationaal handelingsvermogen.

Enkel door gezamenlijk op te trekken onder regie van de EU, kan er meer Europees handelingsperspectief worden gecreëerd vis-a-vis andere grootmachten, wat ten gunste komt van de Nederlandse nationale veiligheid en strategische autonomie. Dit vergt een proactieve rol van Nederland binnen de EU en versterkt ook nationaal de boodschap. Enkel door de marktkracht en normatieve macht van de EU te benutten, kan men geloofwaardig met andere grootmachten concurreren. EU-landen vullen momenteel de *EU-Directives* en beleidsinitiatieven veelal lokaal in, waardoor in sommige gevallen meer barrières worden opgeworpen voor Europese bedrijven dan voor de niet-Europese Big Tech bedrijven. Bescherming en ondersteuning van de *digital single market* moet samengaan met maatregelen om juist Europese bedrijven betere kansen te geven.

Auteurs: Louk Faesen (HCSS), Tom van Schie (TNO), Michel Rademaker (HCSS), Paul Timmers (European University Cyprus/iivii), Matthijs Veenendaal (TNO)

Deze paper wordt onderschreven door:

Berry Vetjes, TNO, Director Market TNO ICT
John Weyne, Photonis, Vice President Business Strategy & Development