Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2020 R11599

Whitepaper Strategische Autonomie op Cybersecurity

Datum	oktober 2020
Auteur(s)	M.A. Veenendaal (TNO) T.C.C. van Schie (TNO) M. Rademaker (HCSS) L. Faesen (HCSS)
Aantal pagina's	42 (incl. bijlagen)
Aantal bijlagen	2
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	Whitepaper Strategische Autonomie op Cybersecurity
Projectnummer	060.44146

Managementsamenvatting

Digitalisering is de afgelopen decennia de drijvende kracht geweest achter economische groei en wereldwijde integratie. De toenemende geopolitieke instabiliteit in de wereld, de snelgroeiende macht van China en de afnemende bereidheid tot samenwerking vanuit de VS, hebben er toe geleid dat Europa zich ook bewust is geworden van zijn afhankelijkheid van buitenlandse grondstoffen, producten en diensten. Vooral op het terrein van digitale technologieën dreigt de EU achterop te raken. Deze toenemende afhankelijkheid heeft ertoe geleid dat, vooral vanuit de EU, vele initiatieven zijn ontplooid om de strategische autonomie te versterken. In Nederland speelt deze discussie echter nog beperkt en heeft nog niet geleid tot een breed debat over de nationale doelstellingen en ambities op dit terrein.

“Strategische autonomie” of “digitale soevereiniteit” zijn abstracte en beperkt uitgewerkte begrippen en hebben soms een dubbelzinnige betekenis. In beleidsdocumenten wordt vooralsnog ook niet duidelijk gemaakt wat er onder wordt verstaan, hoe die autonomie er nu voorstaat of wat nodig is om deze te waarborgen. Dit *whitepaper* is opgesteld om hier meer duidelijkheid over te scheppen, met name vanuit het perspectief van digitale weerbaarheid. Hiertoe is een begrippen- en analysekader voor strategische autonomie op het gebied van cybersecurity uitgewerkt om de discussie over dit onderwerp te structureren.

In dit *whitepaper* definiëren wij strategische autonomie als ‘het vermogen van een staat om haar eigen koers te varen, oftewel haar eigen regels en doelstellingen te bepalen en zelfstandig te beslissen en daarnaar te handelen’. Strategische autonomie kan door staten ook nadrukkelijk in multilateraal verband, zoals de EU, worden nagestreefd. De ambitie van staten om de strategische autonomie op cybersecurity te waarborgen is daarmee in ieder geval voor een belangrijk deel ingegeven door het belang om de nationale veiligheid te waarborgen. Strategische autonomie wordt door staten en de EU ook nadrukkelijk verbonden aan de borging van publieke waarden en grondrechten.

De uitdaging is daarbij 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 en toezicht op 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 overheid beschikt over een breed scala aan instrumenten die kunnen bijdragen aan het versterken van de strategische autonomie. Door te investeren in het versterken van de informatiepositie, door kennisopbouw, technologieontwikkeling en innovatie, en door het ontwikkelen van normen, standaarden en wet- en regelgeving. Nederland kan zelf echter onvoldoende handelingsperspectief creëren

om alle uitdagingen het hoofd te bieden. Samenwerking met vertrouwde publieke en private partners, met de EU, binnen de EU en daarbuiten, is noodzakelijk om de strategische autonomie in het digitale domein structureel en duurzaam te kunnen borgen.

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 waarden en normen en voldoet aan wet- en regelgeving.

Achterblijvende investeringen bedreigen echter de strategische positie van Nederland en de EU doordat de toekomst van het digitale domein voor een groot deel wordt vormgeven en beheerd door niet EU-partijen. Dit 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 ontwikkelen van standaarden voor nieuwe technologiegebieden. Hoe groter de technologische achterstand, hoe kwetsbaarder het digitale domein zal worden. Zo kan de afhankelijkheid van buitenlandse partijen ook de cybersecurity response capaciteiten nadelig beïnvloeden. Cybersecurity moet dan ook niet in isolement worden bezien maar is afhankelijk van en verbonden aan de kennisbouw en innovatie voor digitale technologieën.

Digitale weerbaarheid is echter geen *zero-sum game* waarbij alles wat niet in eigen hand 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 zullen ook tot vergeldingen leiden. Dit beperkt de concurrentiekracht van de Nederlandse en Europese cybersecurity sector op de lange termijn en kan ons als samenleving afhankelijker van derden maken.

Samenwerking met specifieke landen aan banden leggen heeft ook gevolgen voor de innovatiekracht in Nederland. Door intensief 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. Gezien de verregaande globalisering van de digitale sector is het ook maar de vraag in hoeverre een streven naar meer autonomie een beperking van technologische vooruitgang en verschraling van het aanbod tot gevolg zal hebben.

Om de strategische autonomie voor de lange termijn te kunnen blijven waarborgen moet Nederland fors investeren in de eigen innovatie- en concurrentiekracht. Dit moet zoveel mogelijk in EU-verband worden uitgewerkt. Alleen zo kan voldoende massa worden gecreëerd om wereldwijd relevant te blijven ten aanzien van de hoogtechnologische ontwikkelingen die noodzakelijk zijn om de digitale weerbaarheid te waarborgen.

Inhoudsopgave

1 Inleiding

De toenemende digitalisering van onze samenleving heeft tot gevolg dat het belang van zeggenschap over en invloed op de ontwikkeling en toepassing van de daarvoor benodigde technologieën navenant toeneemt. Tevens zorgen de veranderende geopolitieke verhoudingen en spanningen tussen en met de VS en China voor een toenemende ongerustheid over de afhankelijkheid van technologieën uit deze landen. Daarnaast maakt de COVID-19-crisis versneld duidelijk dat een te grote afhankelijkheid van buitenlandse leveranciers onwenselijk is en dat internationale toeleveringsketens (*supply chains*) kwetsbaar zijn.

Deze crisis onderstreept daarmee de noodzaak zeker te stellen dat landen autonoom kunnen blijven functioneren, zelfstandig en in multilateraal verband. Dit streven wordt steeds vaker onder de noemer strategische autonomie gevat. Dit is ook het geval in de Europese Unie (EU) en Nederland. Dit streven is op zich niet nieuw: staten wegen voortdurend af welke kennis en andere capaciteiten benodigd zijn om de nationale veiligheid en de stabiliteit van de samenleving te kunnen waarborgen. Economische en technologische ontwikkelingen geven echter een nieuw gevoel van urgentie aan dit streven.

De mogelijkheid voor Nederland om haar belangen te beschermen en te bevorderen (al dan niet in EU-verband) hangt in belangrijke mate af van de (innovatie)kracht van de technologiesector en de digitale weerbaarheid van de samenleving. De vergevorderde digitalisering van Nederland biedt kansen, maar maakt de samenleving ook kwetsbaar. Daardoor rijst de vraag: hoe is het gesteld met de strategische autonomie van Nederland op het gebied van digitale weerbaarheid of cybersecurity? Deze uitdaging werd bijvoorbeeld al in 2013 zichtbaar toen KPN overgenomen dreigde te worden door América Móvil. Ook bracht de overname van Fox-IT door het Britse NCC Group in 2015 een discussie op gang over de vraag of een bedrijf dat staatsgeheimen beveiligt wel overgenomen kan worden.[1]

Een belangrijke, recente impuls voor het denken over strategische autonomie in het digitale domein wordt geleverd door de Europese Commissie en EU-lidstaten.[2] In Nederland wordt echter nog geen brede discussie gevoerd over de nationale doelstellingen en ambities voor strategische digitale autonomie. De vraag naar een dergelijke discussie is er echter wel. Zo stelt de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in haar rapport *'Voorbereiden op Digitale Ontwrichting'* dat "de kwetsbaarheid van kernprocessen in de samenleving steeds meer door digitalisering [wordt] bepaald. Daarom is een discussie nodig over welke mate van 'strategische autonomie' wenselijk en haalbaar is voor Nederland."[3] In een eerder WRR-rapport wordt eenzelfde nadruk gelegd op de kwetsbaarheden die

---

1 NRC, *Wakker geschrokken na Britse overname Fox-IT*, 24 januari 2017. Online: https://www.nrc.nl/nieuws/2017/01/24/wakker-geschrokken-na-britse-overname-6381515-a1542736

2 De European Centre for International Political Economy (ECIPE) heeft een overzicht van speeches opgesteld die gegeven zijn door EU-commissarissen, beleidsmakers en regeringsleiders over technologische soevereiniteit. Online: https://ecipe.org/publications/europes-technology-sovereignty/

3 WRR, *Voorbereiden op digitale ontwrichting,* 2019, p.211. Online: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

afhankelijkheden in het digitale domein met zich meebrengen (WRR 2014, p88).[4] Ook in het rapport '*Brede Maatschappelijke Heroverwegingen: Speelbal of spelverdeler?'* wordt aanbevolen "onderzoek te doen naar strategische afhankelijkheden, met daarbij in het bijzonder aandacht voor de (potentiële) impact op de nationale veiligheid (bijvoorbeeld diensten, producten, gevoelige technologieën, grondstoffen of transportroutes)."[5]

In hoofdstuk 3 wordt een aanzet gegeven voor een begrippenkader rondom het thema strategische autonomie. Hoofdstuk 4 vormt het analysekader om de discussie over het thema strategische autonomie op cybersecurity te structureren. Deze analyse vindt plaats vanuit drie invalshoeken: de drijfveren achter de ambitie om de strategische autonomie te versterken, het handelingsperspectief (instrumentarium) waarover de overheid beschikt en de uitdagingen en dilemma's Nederland (en/of Europa) die voortkomen uit het streven naar voldoende autonomie op cybersecurity. In de bijlagen is een aanzet voor een toetsingskader opgenomen in de vorm van een *flowchart*. De *flowchart* stelt gebruikers in staat op een gestructureerde manier na te denken over de noodzaak tot versterken of zekerstelling van de strategische autonomie op cybersecurity.

[4] WRR, *De publieke kern van het internet. Naar een buitenlands internetbeleid,* 2015, p.88. Online: https://www.wrr.nl/publicaties/rapporten/2015/03/31/de-publieke-kern-van-het-internet

[5] Beleidsoptie 38 in Rijksoverheid, *Brede Maatschappelijke Heroverwegingen Speelbal of spelverdeler? Concurrentiekracht en nationale veiligheid in een open economie,* 2020. Online: https://www.rijksfinancien.nl/bmh/bmh-16-speelbal-of-spelverdeler.pdf

2 Doelstelling

“Strategische autonomie” of “digitale soevereiniteit” zijn abstracte en beperkt uitgewerkte begrippen en hebben soms een dubbelzinnige betekenis. In beleidsdocumenten wordt vooralsnog niet duidelijk gemaakt wat er onder wordt verstaan, hoe die autonomie er nu voor staat en dus ook niet wat nodig is deze te waarborgen. Verder kan soevereiniteit zowel op het niveau van een natiestaat of in multilateraal verband (vooral EU, maar bijvoorbeeld ook de Benelux) worden belicht. Wil de Nederlandse overheid handelingsperspectieven en daarmee gestructureerd beleidsdiscussies kunnen voeren op nationaal en internationaal vlak (b.v. in EU-verband), dan is een scherpere positionering van het begrip nodig.

Dit *whitepaper* is opgesteld om hier meer duidelijkheid over te bieden, op basis van de opdracht:

“Ontwikkel ten behoeve van politieke en ambtelijke beleidsmakers een conceptueel begrippen- en analysekader voor strategische autonomie op het gebied van cybersecurity om de discussie over dit onderwerp te kunnen structureren. Geef daarbij specifieke aandacht aan digitale weerbaarheid en concurrentiekracht, en schets realistische handelingsperspectieven hoe deze autonomie in Nederland te beschermen dan wel te herstellen en te bevorderen valt. Hanteer hierbij de kennis- en valorisatieketen aanpak en overweeg om de Nederlandse kritische infrastructuren als startpunt te hanteren.”

Dit *whitepaper* beschrijft een begrippen- en analysekader voor strategische autonomie op cybersecurity en doet een voorzet voor een toetsingskader aan de hand van een *flowchart*. De *flowchart* stelt gebruikers in staat op een gestructureerde manier na te denken over de noodzaak tot versterken of zekerstelling van de strategische autonomie op cybersecurity. Hierbij wordt rekening gehouden met de bredere samenhang tussen cybersecurity en economische, maatschappelijke en nationale veiligheidsbelangen.

Het doel van het *whitepaper* is om Nederlandse beleidsbepalers ondersteuning te bieden bij het ontwikkelen van handelingsperspectieven om strategische autonomie op het gebied van cybersecurity zeker te stellen of te versterken.

Dit *whitepaper* is in samenwerking tussen TNO en The Hague Centre for Strategic Studies (HCSS) tot stand gekomen.

3 Begrippenkader strategische autonomie

Strategische autonomie betreft het vermogen van een staat om haar eigen koers te varen, oftewel haar eigen regels en doelstellingen te bepalen en zelfstandig beslissingen te nemen en daarnaar te handelen.

De tegenhanger van strategische autonomie is het noodgedwongen en onvrijwillig volgen van andermans regels of doelstellingen. Het streven naar strategische autonomie uit zich in praktijk in het zoeken naar een balans tussen enerzijds volledige zelfvoorzienigheid en onafhankelijkheid (*autarkie*) en anderzijds volledige afhankelijkheid van andere staten of bedrijven.[6] In de naoorlogse periode is deze balans voor een belangrijk deel gezocht in multilaterale samenwerking.

De soevereiniteit van de overheid omvat nadrukkelijk ook het vermogen om de veiligheid en het welzijn en de veiligheid van haar burgers te waarborgen. Ten aanzien van het digitale domein is een belangrijke uitdaging zeker te stellen dat burgers voldoende toegang tot digitale informatie en diensten en dat de overheid voldoende waarborgen aanbrengt ten aanzien van de verzameling, opslag en het gebruik van data van burgers.

Soevereiniteit is echter niet ondeelbaar. Zo kunnen juridische bevoegdheden worden overgedragen aan multilaterale instanties. Voor Nederland gebeurd dit voor een belangrijk deel in EU-verband. Hoewel de EU de EU allereerst een unie van staten is, heeft er wel een overdracht van bevoegdheden plaatsgevonden. Hiermee wordt onderkent dat bepaalde, nationale doelstellingen alleen kunnen worden verwezenlijkt door binnen het kader van de EU samen op te treden.

Autonomie is een belangrijk aspect van de soevereiniteit van staten. Hoewel er geen eenduidige definitie van soevereiniteit bestaat, betreft het in ieder geval het zelfbeschikkingsrecht van staten. Een staat is soeverein wanneer zij binnen haar grondgebied het hoogste gezag voert; en autonomie behelst de capaciteit om hier invulling aan te geven en daar naar te handelen (handelingsperspectief). Autonomie betreft dus de mogelijkheid voor een staat haar eigen belangen zeker te stellen of te bevorderen, in het bijzonder bij uitzonderingssituaties.[7] De staat acteert hierin niet alleen, maar in samenwerking met andere nationale actoren zoals het bedrijfsleven, kennisinstellingen en *civil society*. Digitale autonomie betreft dan het vermogen van een staat om het digitale domein te beheren en te reguleren als soevereine entiteit. Nederland kan er voor kiezen de noodzakelijk geachte strategische autonomie in EU-verband vorm te geven of via andere multilaterale verdragen.

De ambitie van staten om de strategische autonomie te waarborgen is voor een belangrijk deel ingegeven door het belang om de nationale veiligheid van de staat

---

[6] Paul Timmers, *Strategic Autonomy and cybersecurity*, EU Cyber Direct 2019. P.2. Online: https://eucyberdirect.eu/content_research/strategic-autonomy-and-cybersecurity

[7] Thierry Piette-Coudol, *State digital sovereignty and open public data,* 2019.

en haar burgers te waarborgen.[8] De uitdaging voor strategische autonomie op cybersecurity ligt er daarbij de balans te vinden tussen:

- *Enerzijds het optimaal benutten van de kansen die digitalisering en de vrije markt bieden voor het welzijn en welvaart van de samenleving;*
- *Anderzijds het behouden van controle over en toezicht op de toepassingen van nieuwe technologieën (en de negatieve impactvolle neveneffecten daarvan op de samenleving).*

Het gaat er dus om de balans te vinden op het grensvlak tussen het beschermen van de nationale veiligheid en het versterken van (onder meer) de concurrentiekracht. Deze twee ambities zijn in de kern niet tegenstrijdig maar bij het bepalen van de gewenste beleidskeuzes kunnen afwegingen wel botsen. Buitenlandse directe investeringen leveren een belangrijke bijdrage aan de Nederlandse economische veiligheid in de vorm van groei, welvaart en banen terwijl overnames van bedrijven uit de vitale sectoren ook schadelijk kunnen zijn voor de nationale veiligheidsbelangen. Ten aanzien van economische veiligheid gaat het dus zowel om het belang van het tegengaan van ongewenste onderbrekingen van het vrije economische verkeer als de noodzaak tot het beschermen van strategische economische sectoren en vitale infrastructuur.[9]

Het eerder genoemde handelingsperspectief wordt vooral op de proef gesteld in uitzonderingssituaties, bijvoorbeeld in tijden van schaarste, rampen en bij escalerende politieke, of maatschappelijke spanningen. In een dergelijke uitzonderingssituatie functioneren bestaande afspraken, procedures en processen soms onvoldoende (of worden deze zelfstandig, of door andere landen en bedrijven gewijzigd). De overheid moet terug kunnen vallen op andere maatregelen en middelen, al dan niet gedefinieerd in crisismanagementprocessen die voorbereid zijn op een dergelijk scenario. Zo bleek bij de uitbraak van de COVID-19 pandemie al snel dat bestaande overeenkomsten en procedures voor de productie, distributie en levering van mondkapjes en ventilatiemachines niet afdoende functioneerden. Staten zochten naar alternatieve manieren om in de behoefte te voorzien. Daarom is het belangrijk vast te kunnen stellen of er voldoende handelingsperspectief aanwezig is in het geval van een potentiële grote verstoring, uitval of manipulatie van vitale onderdelen van de samenleving (de zogenaamde uitzonderingssituaties). Hierbij is het wenselijk te bezien of de overheid (in samenwerking met andere nationale en internationale actoren zoals het bedrijfsleven, kennisinstellingen en *civil society*) zelfstandig in staat is om te ageren op de geïdentificeerde handelingsperspectieven, of dat af te dwingen.

Tevens kan een beperking van de strategische autonomie het democratische systeem aantasten, bijvoorbeeld door verkiezingen te manipuleren, het publieke debat te verstoren of publieke instituties en vitale infrastructuur gericht aan te

---

[8] In de Strategie Nationale Veiligheid van de NCTV (2019) worden zes nationale veiligheidsbelangen onderscheiden. Te weten: Territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en internationale rechtsorde. Online: https://www.nctv.nl/onderwerpen/nationale-veiligheid-strategie/documenten/publicaties/2019/6/07/nationale-veiligheid-strategie-2019

[9] Wetenschappelijke Raad voor het Regeringsbeleid (hierna 'WRR'), *Veiligheid in een wereld van verbindingen,* 2017. P. 67. Online: https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen.

vallen.[10] Strategische autonomie kan dan ook niet los worden gezien van de vertrouwensrelatie tussen overheid en burger. Het streven naar autonomie is in veel gevallen gelijk aan het waarborgen en versterken van het vertrouwen van burgers in nationale en internationale instituties.[11]

Een belangrijke doelstelling bij het bevorderen van strategische autonomie is het waarborgen van de digitale weerbaarheid van de samenleving. Digitale weerbaarheid is voor de staat, burgers en bedrijven in toenemende mate een randvoorwaarde voor een functionerende samenleving. Begrip van het fenomeen cybersecurity en het toepassen van effectieve maatregelen om deze zeker te stellen, maakt dat onze samenleving veilig, betrouwbaar en succesvol digitaliseert.

In een samenleving waarin vrijwel alles van software afhankelijk is, die veelal ontwikkelt, geëxploiteerd of beheerd wordt door buitenlandse private partijen, komt de digitale weerbaarheid onder druk te staan. Software die constant in verbinding staat met het internet en kan worden gemodificeerd en geüpdatet is ook kwetsbaar voor misbruik. Zeker wanneer software als dienst wordt afgenomen (software-as-a-service) en het beheer, en dus ook de beveiliging, aan de dienstverlener wordt uitbesteed. De organisaties die deze diensten afnemen verliezen controle over het beheer en daarmee uiteindelijk ook het functioneren van het product. Als Nederland en Europa te afhankelijk worden van diensten die primair door organisaties buiten de EU worden geleverd, komt ook de strategische autonomie op cybersecurity onder druk te staan. Te meer als er gegronde redenen zijn om te veronderstellen dat statelijke actoren ongewenste invloed op de dienst of de dienstverlener uit kunnen oefenen.

Het volgende hoofdstuk introduceert een analysekader waarmee het begrip strategische autonomie op cybersecurity in dit *whitepaper* uiteengezet wordt.

[10] Paul Timmers in EU Cyber Direct Policy Focus, S*trategic autonomy and cybersecurity*, 2019, p. 3.

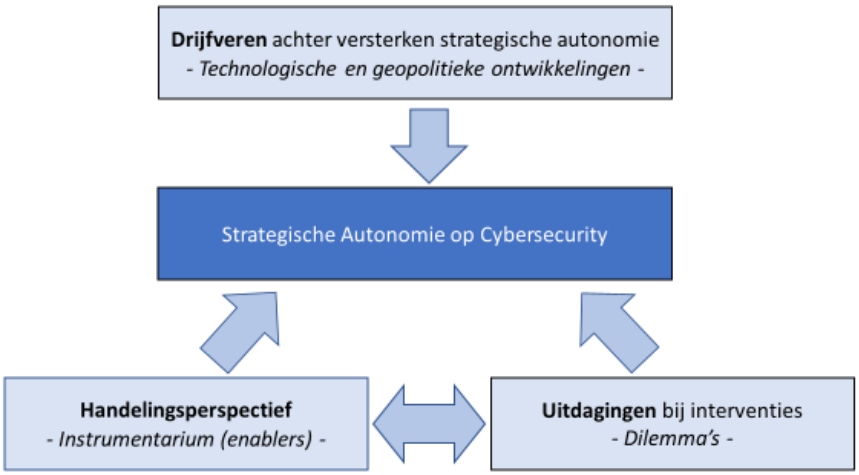
[11] Interview met Prof. Dr. M.J.G. (Michel) van Eeten in augustus 2020.

4 Analysekader strategische autonomie op cybersecurity

Voor een gestructureerde blik op het belang van en handelingsperspectief voor het versterken en borgen van strategische autonomie op cybersecurity, gebruiken we drie invalshoeken. De invalshoeken bevatten ieder een dikgedrukt kernwoord en als begeleiding een deelvraag. De invalshoeken tezamen vormen het analysekader:

1 **Drijfveren** achter versterken strategische autonomie: welke ontwikkelingen (*drivers*) vergroten het belang van strategische autonomie op cybersecurity voor Nederland en/of Europa?
2 **Handelingsperspectief:** over welk instrumentarium (of *enablers*) beschikt de overheid om de eigen strategische autonomie te versterken?
3 **Uitdagingen bij interventies**: tegen welke uitdagingen en dilemma's loopt Nederland (en/of Europa) aan bij het streven naar voldoende zelfbeschikking?

De drie invalshoeken vormen de paragrafen van dit hoofdstuk.



Figuur 1 Analysekader strategische autonomie cybersecurity.

De in dit hoofdstuk beschreven invalshoeken vormen tezamen ook de kern van een *flowchart* die is opgenomen in bijlage 1. Deze flowchart en de bijbehorende handleiding (bijlage 2) stellen haar gebruikers in staat op een gestructureerde manier te analyseren wat de noodzaak tot versterken of zekerstelling van de strategische autonomie is. Tevens helpt het inzichtelijk te maken wat de bredere samenhang is tussen cybersecurity en economische, maatschappelijke en nationale veiligheidsbelangen.

4.1 Drijfveren achter strategische autonomie op cybersecurity

Deze paragraaf beschrijft drie drijfveren die ten grondslag liggen aan het toenemende belang dat wordt gehecht aan strategische autonomie voor Nederland en Europa.
Het toenemende belang van het zekerstellen van de strategische digitale autonomie wordt door drie aspecten aangejaagd: 1) geopolitiek: toenemende

internationale spanningen, 2) de digitale transformatie en 3) onderkende digitale dreigingen.

Figuur 2 Driehoeksverhouding van drijfveren (naar Paul Timmers).[12]

Aspect 1. De digitale transformatie heeft ertoe geleid dat onze samenleving en economie sterk afhankelijk zijn van digitale infrastructuren en diensten, waarbij Europa en Nederland vooral consument zijn van elders geproduceerde digitale technologieën. Staten en bedrijven die de belangrijkste digitale technologieën[13] ontwikkelen en in hoge mate controleren, zijn in toenemende mate in staat hun belangen en waarden op economisch, sociaal en politiek, cultureel, fysiek, ecologisch en rechtstatelijk vlak te sturen en te bevorderen. Hiervoor geldt ook dat private partijen zowel de centrale architectuur van het digitale domein ontwikkelen en beheren als de daaruit voortvloeiende wereldwijde datastromen beheren.

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.

Centraal bij de beleidsontwikkeling door de EU op het terrein van cybersecurity staat dan ook het terugdringen van de afhankelijkheid van buitenlandse leveranciers ten aanzien van de vitale digitale infrastructuur.[14] Terwijl de VS tot nu toe heeft gekozen voor een vrijemarkt benadering van "*permissionless innovation*"

---

[12] Paul Timmers in EU Cyber Direct Policy Focus, S*trategic autonomy and cybersecurity*, 2019, p.2.

[13] Voor het analyseren van de technologie gebieden waar de uitdaging voor het waarborgen van digitale autonomie het grootst is, kan uit worden gegaan van de sleuteltechnologieën zoals vastgelegd in de methodische bijlage 'inzet op sleuteltechnologieën' van het Nederlandse "missiegedreven innovatiebeleid". De benoemde sleuteltechnologieën zijn**:** *Artificial intelligence* (incl. *machine* en *deep learning*), *Big data and data analytics***,** *encryption technologies / digital security***,** *Blockchain***,** *High Performance Computing, Grid Computing and Cloud Technologies/ Computing*, en quantum technologies (Quantum computing**,** communication, sensors and metrology). Online: https://www.bedrijvenbeleidinbeeld.nl/bouwstenen-bedrijvenbeleid/missiegedreven-innovatiebeleid/sleuteltechnologieen.

[14] EPRS, Ideas Paper for the European Parliament, *Digital Sovereignty for Europe*, 2020. P.3. Online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf,

en China voor een door de staat gestuurd model, kiest Europa voor de middenweg, een '*human centric approach*', gebaseerd op Europese waarden en meer gericht op het uitoefenen van toezicht op digitale technologieën om de veiligheid, privacy en het vertrouwen van haar burgers te waarborgen en te zorgen voor een competitieve, duurzame digitale economie.[15]

Aspect 2. Digitale dreigingen nemen toe zodra het digitale raakoppervlak toeneemt. Met andere woorden: hoe afhankelijker we zijn van digitale technologieën, hoe kwetsbaarheden we zijn voor cyberaanvallen. De aard van deze dreiging is veelzijdig: het varieert van cybercriminelen die handelen vanuit een financieel gewin, tot staten die de cybersecurity van andere staten ondermijnen..

Niet alle dreigingen zijn echter gelijk. Het strategische belang van een technologie(gebied) volgt uit de toepassing waarvoor en de context waarbinnen deze wordt gebruikt. Neem bijvoorbeeld nieuwe versleutelingsstandaarden. De implementatie van een nieuwe versleutelingsstandaard kan hackers buiten de deur van DigiD houden. Deze toepassing vertegenwoordigt een grotere maatschappelijke waarde dan wanneer het gaat om het versleutelen van chatberichten in datingapps.

De Europese Commissie en de Europese Raad zijn zich ervan bewust dat de afhankelijkheid van buitenlandse bedrijven leidt tot minder zeggenschap over hoe deze producten en diensten kunnen voldoen aan de eigen waarden en veiligheidsstandaarden. Een te grote afhankelijkheid van buitenlandse producten en diensten die geen *information assurance* kunnen geven en technologische *black boxes* aanleveren, maakt het steeds moeilijker om te bepalen of er onaanvaardbare risico's zijn.[16]

Tot slot kan de afhankelijkheid van buitenlandse partijen ook de cybersecurity responscapaciteiten nadelig beïnvloeden. Zo is er een risico dat bij oplopende internationale spanningen software updates om kwetsbaarheden te verhelpen niet meer beschikbaar (of selectief beschikbaar) worden gesteld door een producent, of dat de patches niet meer vertrouwd kunnen worden. Om tot een afgewogen oordeel te komen over het al dan niet toelaten van een bepaalde technologie of dienst op de Nederlandse markt op basis van cybersecurity, is het dan ook noodzakelijk eigenstandig over de hiervoor noodzakelijke kennis te beschikken om dit adequaat te kunnen beoordelen en eventueel mitigerende maatregelen te kunnen nemen.

---

[15] Ministerie van Economische Zaken en Klimaat, *Nederlandse Digitaliseringsstrategie 2020*. P. 6. Online: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/25/nederlandse-digitaliseringsstrategie-2020

[16] De term *Black Box* is een verzamelbegrip voor apparaten of softwareproducten waarvan de kennis over de interne werking niet beschikbaar is ,of slechts beperkt beschikbaar wordt gemaakt.

Aspect 3. Internationale spanningen nemen toe en manifesteren zich ook in het digitale domein. Digitale dreigingen spelen een steeds belangrijkere rol in statelijke conflicten en competitie. Steeds vaker wordt het risico van een cyberincident tussen natiestaten gezien als de grootste of een van de belangrijkste dreigingen tegen de nationale veiligheid.[17] Digitale producten en diensten worden in deze context gezien als een potentiële dreiging tegen de nationale veiligheid die handelingsbekwaamheid van de overheid kunnen ondermijnen via achterdeurtjes.

Terwijl digitale dreigingen of *governance* vraagstukken voorheen vooral technisch van aard waren, worden ze nu steeds meer vanuit economisch, geopolitiek of nationale veiligheid perspectief benaderd. De EU en de VS behandelen een Chinees of Russisch bedrijf niet meer als een apolitieke marktspeler, maar als een potentieel Trojaans paard. Het boycotten van producten kan ertoe leiden dat bedrijven een groot deel van hun markt moeten afstoten, omdat ze een keuze maken voor het ene machtsblok of het andere. De toenemende spanningen blijven niet beperkt tot de relatie tussen het Westen en China: de trans-Atlantische gemeenschap van gedeelde waarden en belangen komt onder druk te staan wanneer de achterliggende gedachte van een vrije (digitale) interne markt botst met de noodzaak voor de EU om persoonsgegevens, de digitale zelfbeschikking en eerlijke concurrentie (*level playing field*) te beschermen.

De lang geobserveerde, maar doch stilletjes geaccepteerde, dominantie van Amerikaanse internetbedrijven heeft Europa ertoe gedwongen een koers van digitale zelfbescherming in te slaan - van gegevensbescherming en mededingingsrecht tot belastingheffing.[18]

---

[17] Er is een sterke toename in het aantal nationale veiligheidsevaluaties waarin cybersecurity als de belangrijkste of een van de grootste bedreigingen voor de nationale veiligheid wordt beschreven. Dit wordt niet alleen erkend in de Nederlandse Nationale Veiligheid Strategie 2019 (https://www.rijksoverheid.nl/documenten/rapporten/2019/06/07/tk-bijlage-nationale-strategie-2019), maar ook door in die van de VS (https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf), de EU (https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf), en vele andere landen (https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace).

[18] Voorbeelden zijn: Regulering (GDPR, discussies rondom de EU-US *Privacy Shield*), Mededinging (opknippen van *big tech* en het onderzoeken van recente overnames door grote internetbedrijven, onderzoeken door de US *Federal Trade Commission* en het Duitse *Bundeskartellamt*), Toezichthouders (*Brief* door drie Europese toezichthouders, zie: https://www.acm.nl/sites/default/files/documents/2019-10/benelux-memorandum-over-toezicht-mededinging-in-digitale-economie.pdf).

Drijfveer achter strategische autonomie: 5G

De introductie van 5G speelt in op de wereldwijde vraag naar meer data en connectiviteit en zou digitalisering op grote schaal moeten gaan ondersteunen.[19] Het zou de sleuteltechnologie moeten zijn die andere technologische innovatie en toepassingen mogelijk maken, zoals autonome voertuigen, *smart electric grids*, en het *internet of things*. Wat betreft de digitale dreigingen, spraken sommige Europese lidstaten zich initieel niet uit over de mogelijke risicotoename die 5G introduceert, terwijl de VS redelijk snel waarnam dat 5G een uniek veiligheidsrisico met zich meebrengt.[20] Deze zorg werd daarna onderstreept door de Europese Commissie en ENISA : "*5G networks is [sic] the future backbone of our increasingly digitized economies and societies […] ensuring the security and resilience of 5G networks is therefore essential."*[21] Daarnaast wordt er ook aandacht besteed aan het risicoprofiel van de aanbieder. Het meest genoemde technische risico van vele westerse overheden is dat Huawei een te lage '*information assurance*' kan geven van hun 5G-diensten.[22]

De gemaakte risicoanalyse is niet alleen van technische aard. Het gaat ook om (geo)politieke en handelsbelangen. Huawei wordt namelijk gezien als een proxyagent van de Chinese overheid, die door westerse overheden wordt beticht van oneerlijke handelspraktijken[23], geopolitieke armdraaiingen[24] en heimelijke operaties zoals het stelen van intellectueel eigendom en beïnvloedingscampagnes.[25] De Europese Commissie roept daarbij haar lidstaten op om zo min mogelijk gebruik te maken van leveranciers met een hoog risico voor de aanbesteding van cruciale of gevoelige elementen van hun 5G-netwerken, zoals internet-*backbone* of kernnetwerken die het dataverkeer beheren.[26]

De escalerende handelsoorlog tussen de VS en China zorgde ervoor dat Washington op verschillende manieren duidelijk maakt dat het Chinese technologie niet vertrouwt en dat niemand dat zou moeten doen. Dit doet de VS bijvoorbeeld

[19] Wat betreft de digitale transformatie biedt 5G vele voordelen ten opzichte van eerdere generaties, waaronder snellere gegevensoverdrachtssnelheden.

[20] Zo zou 5G bijvoorbeeld volgens sommigen "de zesde generatie gevechtsvliegtuigen in gevaar brengen" terwijl anderen het een veiliger alternatief vinden dan 4G als het "correct" wordt uitgevoerd. Tussen deze twee uitersten bevindt zich een grijs gebied, maar er is geen twijfel over mogelijk dat het grotere raakoppervlak zorgt voor meer kwetsbaarheden.

[21] NIS Cooperation Group, *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks,* 2019.

[22] United Kingdom Cabinet Office, *Huawei cyber security evaluation centre oversight board: annual report 2019.*

[23] Oneerlijke handelspraktijken zoals het weigeren van markttoegang voor buitenlandse bedrijven, het geven van overheidssteun aan eigen bedrijven en het negeren van WHO-regels.

[24] Geopolitieke armdraaiingen zoals het Chinese infrastructuurproject *Belt and Road Initiative*

[25] Heimelijke Chinese operaties zijn een groeiende zorg voor Westerse landen, waarbij twee ontwikkelingen specifiek opvallen. Ten eerste, de ongebreidelde "overdracht" van intellectueel eigendom waarin de nadruk is verlegd van onverhulde cyberdiefstallen naar een combinatie van onbetrouwbare joint ventures en "ongecontroleerde" technologieoverdrachten binnen legitieme zakelijke relaties. Ten tweede, een sterk toegenomen heimelijke beïnvloedingscampagne, met name gericht op Europa, die poogt "gunst te kopen" binnen de media, de academische wereld en onderzoeksinstellingen, maar ook rechtstreeks gericht is op politieke opinievormers. Deze laatste ontwikkeling is vooral zichtbaar in de gevallen van Italiaanse, Griekse en Servische politieke verklaringen, die vanwege hun plotseling toegenomen relatie met China een minder kritische toon hebben aangenomen.

[26] Frances g. Burwell and Kenneth Propp in Atlantic Council, *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?*, 22 juni 2020.

door het "*Clean Network*" programma[27] en het exportverbod van computerchips aan Huawei die nodig zijn voor de 5G productie op grond van zorgen over de nationale veiligheid en cybersecurity.[28] Deze maatregelen leiden tot Chinese reputatieschade en een vertraagde 5G-productie – geen enkele aanbieder kan namelijk alle benodigde onderdelen zelf ontwikkelen en produceren, ook Huawei niet. De Chinese overheid realiseert zich dat de toegang tot geavanceerde microchips of andere hoogwaardige technologieën of diensten haar ieder moment kan worden ontzegd. Het *Made in China 2025*-beleid – dat van oorsprong gericht was op het vergroten van de competitiviteit van de Chinese hightechindustrie – wordt nu dus belangrijker voor de Chinese strategische autonomie om zelfvoorzienend te worden op het gebied van dit soort sleuteltechnologieën.

Figuur 2 laat zien dat strategische autonomie sterk beïnvloed wordt door de wisselwerking van verschillende aspecten. Het kan niet los worden gezien van de vertrouwensrelatie tussen overheid, burger en het bedrijfsleven, tussen staten onderling, en het vertrouwen in ICT. Vertrouwen ligt aan de grondslag van digitale technologieën, cybersecurity, de rechtstaat en internationale betrekkingen. Een sterke toename van de digitale dreigingen en internationale spanningen leidt tot een vertrouwenscrisis. Toenemende internationale competitie en conflicten zorgen voor meer wantrouwen tussen westerse democratieën en autocratische landen, terwijl de gedeelde waarden tussen de VS en Europa ook onder druk komen te staan. Westerse staten wantrouwen technologieën van buitenlandse bedrijven die vanuit andere waardesystemen opereren.[29] De private sector ervaart dit in meer of mindere mate ook en neemt in sommige gevallen het heft in eigen handen in reactie op verzande of langdurende multilaterale discussies. Tegelijkertijd zetten overheden steeds vaker digitale middelen in als wapen om verwarring te zaaien, schade te berokkenen, intellectueel eigendom te stelen of om de eigen burgers te bespioneren.[30] Tevens heeft de burger steeds minder vertrouwen in de internetveiligheid en twijfelt men of bedrijven en overheden voldoende doen om de online veiligheid en privacy waarborgen.[31]

Kortom, het streven naar strategische autonomie is een *coping*-mechanisme geworden voor Europese staten om met het toenemende wantrouwen in buitenlandse bedrijven en staten om te gaan. Maar dat mechanisme moet het vertrouwen elders niet schaden. Strategische autonomie moet bijvoorbeeld geen

---

[27] United States Department of State, *Announcing the Expansion of the Clean Network to Safeguard America's Assets*, 5 augustus 2020.

[28] The Washington Post, *U.S. tries to block foreign-made semiconductors from reaching Huawei,* 15 mei 2020.

[29] Interview met Prof. Dr. M.J.G. (Michel) van Eeten in Augustus 2020.

[30] Sinds 2015 is er weinig vooruitgang in multilaterale gremia zoals de VN over het vaststellen van internationale regels over verantwoordelijk statelijk gedrag in cyberspace. Zonde zinvolle diplomatieke vooruitgang hebben andere – niet-statelijke- stakeholders de touwtjes in eigen handen genomen in het ontwikkelen van gedragsregels, zoals het Siemens *Charter of Trust*, Microsoft *Cybersecurity Tech Accord* en de *Global Commission on the Stability of Cyberspace*. Tegelijkertijd nemen bedrijven steeds vaker op eigen houtje toevlucht tot offensieve maatregelen tegen de dader, ook bekend als de hack-back. Zie ook HCSS, *Conflict in Cyberspace; Parsing the threats and the state of international order in cyberspace.* Online: https://www.hcss.nl/report/conflict-cyberspace-parsing-threats-and-state-international-order-cyberspace

[31] CIGI-Ipsos, *Global Survey on Internet Security and Trust*, 2019. Online: https://www.cigionline.org/internet-survey-2019.

excuus zijn voor meer digitale staatscontrole. Een Europese aanpak moet geloofwaardig, competitief, transparant, interoperabel en veilig zijn.

De rol van de Nederlandse overheid in het leveren van zo'n alternatief is beperkt. Het internet en veel van de digitale technologieën waarvan we afhankelijk zijn, worden ontwikkeld en bestuurd door een complex systeem van publieke en private *stakeholders* met eigen regels, normen, standaarden en processen. Een nauwe samenwerking tussen overheid, industrie, kennisinstituten en de technische sector is onmisbaar om voldoende slagkracht te ontwikkelen. De overheid kan hier het voortouw nemen door te identificeren welke technologieën digitale autonomie vergen en in samenwerking met wie en wanneer.

Het besluit om te acteren kan leiden tot leiden tot stimuleren, benadrukken, of inzetten van beleidsinstrumenten. De volgende paragraaf zet een breed scala van beleidsinstrumenten uiteen en geeft invulling aan het tweede gedeelte van het analysekader.

4.2 Instrumentarium voor bevorderen strategische autonomie

De overheid beschikt over een breed scala aan instrumenten die kunnen bijdragen aan het versterken van de strategische autonomie op cybersecurity. Daar waar Nederland zelf geen of onvoldoende handelingsperspectief heeft of kan ontwikkelen, moet worden bezien hoe deze op Europees of internationaal niveau zeker kan worden gesteld. De volgende instrumenten (dikgedrukt) bieden de overheid handelingsperspectief om de strategische autonomie in het digitale domein te versterken.

Versterken informatiepositie: Zicht op dreigingen is een belangrijke randvoorwaarde voor strategische autonomie. Dit wordt met name gefaciliteerd door het verzamelen van inlichtingen en deze ook te delen met partners (Europese partners of industrie). Het betreft hier niet alleen inlichtingen over digitale dreigingen maar ook over (geo)politieke, economische en technologische ontwikkelingen. Hier zijn minstens drie redenen voor. Ten eerste, Nederland en haar partners moeten het vermogen hebben om buitenlandse sleuteltechnologieën op regelmatige basis te kunnen beoordelen en controleren. Ten tweede, Nederland moet een sterke inlichtingenpositie hebben van de mogelijke cybersecuritydreigingen die voortvloeien of meekomen met het gebruik van deze technologieën. Alleen dan kan er daadkrachtig gereageerd worden op nieuwe dreigingen. Ten derde moet het inzichtelijk worden waar enerzijds Nederland relatief goed in staat is zelfstandig kennis te ontwikkelen en te investeren in innovatie en anderzijds waar Nederland afhankelijk is van partijen van buiten de EU en of deze afhankelijkheid acceptabel is.

Kennisopbouw: het opbouwen van kennis is een eerste stap in het versterken van de strategische autonomie. Het gaat hier niet alleen om het verbeteren van de kwaliteit van specifieke cybersecurityopleidingen. Het is ook noodzakelijk zeker te stellen dat voldoende experts voor bepaalde technologiegebieden worden opgeleid. Hiervoor moet voldoende talent beschikbaar zijn en sterke academische instituties aanwezig zijn. Het onderzoek naar de cybersecurityvalorisatieketen uit 2019 (TNO) heeft de toenemende behoefte aan gekwalificeerde cybersecurity experts en beperkte uitstroom uit het onderwijs of bijscholings-mogelijkheden nogmaals

benadrukt. Wanneer de arbeidsperspectieven in Nederland achterblijven kan er een uitstroom van experts naar het buitenland ontstaan waardoor de krapte op de arbeidsmarkt alleen maar toeneemt.[32]

Investeren in innovatie: Het investeren in innovatie is nodig om te zorgen voor een betere Nederlands of Europees concurrentievermogen en minder afhankelijkheid van buitenlandse partijen. Europese digitale diensten en infrastructuur zouden een hoge mate van interoperabiliteit moeten bieden om op te schalen met nieuwe technologieën en toepassingen (zogenaamde *open innovation*). Terwijl Europa een sterke R&D-capaciteit heeft, is het niet in staat om Europese digitale koplopers te creëren die kunnen concurreren met Amerikaanse of zelfs Chinese bedrijven. Overgereguleerde markten verminderen risico's, maar kunnen tegelijkertijd innovatief en risicovol ondernemerschap ondermijnen. Dit leidt tot een tekort aan durfkapitaal en investeringen. Hoewel Nederland en de EU-innovatiesubsidies en budgetten vrijmaken, zijn deze vaak te versplinterd. Zonder een structurele financiering en brede politieke en industriële ondersteuning kan GAIA-X hetzelfde lot ondergaan als Quaero – een zoekmachine die het Europese alternatief voor Google moest worden.[33] Het instrumentarium zal goed toegerust moeten zijn om in te kunnen spelen op de steeds kortere productiecycli van cloud- en dataminingindustrie.[34] Een te grote nadruk op het in eigen beheer of met eigen kennis en middelen waarborgen van de digitale veiligheid kan tot gevolg hebben dat het concurrentievermogen en de innovatiekracht van de samenleving wordt beperkt. Investeren in innovatie in een open omgeving kan op termijn de digitale weerbaarheid ook vergroten.

Opstellen wetgeving en normen: de EU en haar lidstaten breiden hun strategisch digitaal beleid uit om aan de ene kant een sterke interne digitale economie te bouwen die internationaal competitief is, maar ook regie te houden op de veiligheid en privacy van haar burgers en bedrijven. Tegelijkertijd kan het Nederlandse beleid voortbouwen op het vaststellen van gedragsnormen – niet juridisch bindende overeenkomsten - voor het digitale tijdperk binnen diplomatieke fora om zo meer indirecte controle en medezeggenschap over technologische ontwikkelingen te krijgen. De reikwijdte en invloed van de GDPR voor andere continenten toont bewijs dat de EU en haar lidstaten wereldwijde effecten teweeg kunnen brengen met EU *Regulations*. Een voorbeeld van Europese wetgeving om betere bescherming te bieden tegen digitale dreigingen is de Network and Information Security (NIS) richtlijn (in Nederland geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen van 2018). De EU is op dit moment bezig met een inhoudelijke update van deze richtlijn, wat het belang ervan onderstreept.

Bevorderen certificering en standaarden: de ontwikkeling en implementatie van certificaten draagt bij aan de cybersecurity van een sector en aan het behouden

---

[32] TNO, *Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity, 2019*. P. 21. Online: https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/10/onderzoek-naar-het-versterken-van-de-innovatieketen-op-het-terrein-van-cybersecurity

[33] Het Gaia-X iniaitief is later in het document toegelicht. Informatie over Quaero op Webwereld.nl, Online: https://webwereld.nl/nieuws/business/frans-duitse-samenwerking-aan-quaero-ten-einde-3736334/

[34] Center for Strategic and International Studies, *Has Europe Lost Both the Battle and War over Its Digital Future?,* 2020. Online: https://www.csis.org/analysis/has-europe-lost-both-battle-and-war-over-its-digital-future

van indirecte controle over en toezicht op de toepassing van nieuwe technologieën binnen Nederland en Europa. Deze standaarden worden door de industrie zelf, en/of niet-gouvernementele organisaties (ISO), en/of diplomatieke fora (ITU of de EU) ontwikkelt. Het zetten van standaarden binnen deze gremia is bijvoorbeeld een belangrijk onderdeel van Chinees beleid *Made in China* 2025 dat wordt uitgebreid in de *China Standards 2035 Plan* dat eind 2020 uitgebracht wordt.[35] De ontwikkeling en implementatie van EU-cybersecurity certificaten binnen deze velden – nu mogelijk binnen de context van de EU Cybersecurity Act – vergt agendering op de Europese politieke agenda.

Uitvaardigen sancties en export-controles: Nederland kan haar buitenlandbeleid intensifiëren om op EU-niveau gezamenlijk beslissingen te kunnen maken, bilaterale en multilaterale niveau vertrouwenwekkende maatregelen te treffen en politieke druk en sancties uit te voeren om haar strategische autonomie te waarborgen.

Versterken interne markt: De interne markt functioneert nog verre van optimaal. Vooral ten aanzien van de dienstensector bestaan er nog hardnekkige belemmeringen. Hierbij gaat het met name om aspecten als de hoeveelheid en complexiteit van de verschillende nationale regels van EU-lidstaten, beperkte administratieve capaciteit; slechte en complexe omzetting van Europese regels en onvoldoende handhaving van deze regels.[36] De belemmeringen staan de groei van Europese tech bedrijven in de weg doordat de individuele lidstaten simpel weg te klein zijn om voldoende marktvolume te creëren. Dit is een van de redenen waarom er geen Europese tegenhangers zijn. Een sterke interne markt vergroot de thuismarkt en kan grote industriespelers in staat stellen om de valorisatieketen van fundamenteel onderzoek naar eindproducten vorm te geven.

Nederland kan het instrumentarium uit bovenstaand overzicht op verschillende niveaus oppakken en/of uitvoeren. Voor het vormgeven van de innovatie uitdagingen op de lange termijn kan ook een gerichte **industriepolitiek** worden gevoerd. Tot voor kort was de consensus dat de overheid niet te veel in de markt moest ingrijpen om ‘winnaars’ aan te wijzen. De markt zou veel beter in staat zijn vorm te geven aan innovatie dan de overheid. Dit neemt echter niet weg dat in de afgelopen decennia veel van de belangrijkste bouwstenen voor de digitale economie in opdracht van de overheid zijn ontwikkeld. Zo zijn veel van de technologieën die de smartphone mogelijk hebben gemaakt ontwikkelt in opdracht van het Amerikaanse ministerie van Defensie.

De overheid kan er dan ook voor kiezen specifieke innovatiedoelen op te stellen en gericht te investeren in technologieontwikkeling. Industriepolitiek wordt

---

[35] De Chinese overheid stimuleert deelname van Chinese bedrijven in deze gremia en is daardoor sterk toegenomen, met name binnen de context van nieuwe technologieën zoals 5G, IoT en AI. Veel standaarden die binnen de ITU worden gezet met betrekking tot *surveillance* technologie en *facial recognition* komen momenteel van Chinese bedrijven. John Seaman, *China and the New Geopolitics of Technical Standardization*, *Notes D’Ifri*, January 2020. Online: https://www.ui.se/butiken/uis-publikationer/ui-brief/2019/chinas-standard-power-and-its-geopolitical-implications-for-europe/ 34; en Financial Times, https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96.

[36] Europese Commissie, Identifying and addressing barriers to the single market. 2020. https://ec.europa.eu/info/sites/info/files/communication-eu-single-market-barriers-march-2020_en.pdf

tegenwoordig niet alleen maar gebruikt in relatie tot wat een overheid in uiterste noodzaak kan en wil doen om een zelfstandige nationale industrie te bewerkstelligen. Het wordt ook genoemd voor transnationale samenwerkingen ter bevordering van strategische autonomie op cybersecurity.

Het missie-gedreven innovatiebeleid van de regering is een eerste stap. In maart 2020 heeft de Europese Commissie haar nieuwe industriestrategie gelanceerd. Centraal daarin staat "het vermogen van de Europese industrie om de leiding te nemen bij de [digitale en klimaat]transitie […] en ons concurrentievermogen te bevorderen. Zij kan het zich niet veroorloven zich enkel aan te passen – zij moet zelf zorgen voor verandering en innovatie aandrijven."[37] De rol die de EU voor zichzelf ziet is hierbij vooral die "van katalysator en regelgever".[38]

Overheidsinterventie: GAIA-X

Een speerpunt van de EU is het terugdringen van de technologische afhankelijkheid van buitenlandse – met name Amerikaanse – *cloud*-infrastructuur en -diensten.[39] Duitsland en Frankrijk zijn daarom in oktober 2019 begonnen met de ontwikkeling van de eerste Europese clouddienst genaamd GAIA-X.[40] GAIA-X voorziet in een data-infrastructuur met gemeenschappelijke regels, normen en technologieën voor *cloud* en *edge* diensten van Europese aanbieders om de afhankelijkheid van veelal Amerikaanse aanbieders te verkleinen. De grote *cloud providers* vallen uiteindelijk ook onder de wetgeving van hun moederland waardoor Europese organisaties er niet zeker van zijn dat de datasoevereiniteit is geborgd. Zo eist de Amerikaanse CLOUD-act bijvoorbeeld dat data bij een Amerikaans bedrijf op servers in het buitenland voor inlichtingendiensten inzichtelijk moet kunnen zijn.

GAIA-X is een concrete invulling van één van de ambities van het Duits voorzitterschap. Een van de Nederlandse initiatieven om deel te (gaan) nemen is een strategische samenwerking tussen TNO, DINL, ISPConnect, the Dutch Data Center Association en de Dutch Hosting Providers Association. Nederland is geen hoofdparticipant in GAIA-X, maar het initiatief is mogelijk een invulling voor systeeminteroperabiliteit en openheid van *cloud*-platformen die fundamentele principes voor Europese digitale diensten en infrastructuur waarborgen. Of het initiatief slaagt met in acht neming van de voorgespiegelde doelstellingen is nog ongewis.

Tot slot; overheden moeten zich bewust zijn van de verschillende knoppen waaraan ze kunnen draaien om strategische autonomie te waarborgen, wat de kosten en baten zijn, en wanneer verschillende maatregelen elkaar versterken of

---

[37] Europese Commissie, Een nieuwe industriestrategie voor Europa. 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0102

[38] Ibidem.

[39] Ook de strategie van de European Data Protection Supervisor (2020-2024) juicht intiatieven die bijdragen aan 'digitale soevereiniteit' toe: "*We do not support the creation of artificial geographical borders, but we do have a preference for data being processed by entities sharing European values, including privacy and data protection*." European Data Protection Supervisor, *Shaping A Safer Digital Future – The EDPS Strategy 2020-2024*. Online: https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en

[40] Alex Alley, *Legal Entity for Gaia-X Established*, European Cloud Platform Now Official," *Data Centre Dynamics,* 2020. Online: https://www.datacenterdynamics.com/en/news/legal-entity-gaia-x-established-european-cloud-platform-now-official

tegenwerken. Daarnaast is de rol van de overheid vooralsnog beperkt. De technologische sector wordt gedomineerd door de private sector, die de software, producten, infrastructuur en diensten beheert. Verder spelen *civil society* actoren ook een belangrijke rol, zoals met name de technische gemeenschap en academici die een belangrijk deel van de discussies en normen van de onderliggende internet *governance* structuren beheren (zoals het zetten van standaarden, *best practices* in internet *governance* en cybersecurity documenteren en ad-hoc coalities oprichten in bijvoorbeeld het Internet Governance Forum (IGF)).

Ter illustratie zijn twee kaders opgenomen waarin Duitse en Franse ontwikkelingen en voorbeelden van instrumentarium beschreven zijn.

Voor **Duitsland** is strategische autonomie een van de speerpunten van haar voorzitterschap van de Raad van de Europese Unie in 2020.[41]

Duitsland beschrijft haar ambities en *roadmaps* voor strategische autonomie op het gebied van cybersecurity onder de noemers Industrie 4.0 en de *Industrial Policy 2030.*

De discussie in Duitsland is mede vormgegeven door een studie uit 2019 over de toenemende afhankelijkheid van de publieke sector van softwareproducten die ontwikkeld worden door buitenlandse bedrijven. Deze afhankelijkheid, met name op Microsoftproducten, werd gepositioneerd als een afname in de digitale soevereiniteit van de staat. De afhankelijkheid had een nadelig effect op informatiebeveiliging (kwetsbaarheden, GDPR, telemetriedata), prijs en flexibiliteit.

Opvallend is dat autonomie een van de drie pijlers is van de Duitse Industrie 4.0 visie voor 2030.[42] Autonomie is onderverdeeld onder infrastructuur, *safety and (data) security*, en technologisch onderzoek en innovatie. De overige twee pijlers zijn interoperabiliteit en duurzaamheid. De beleidsdoelstellingen en doelgroep van het platform liggen nadrukkelijk op de (innovatie)kansen en het belang van het MKB. In de studie *Industrie 4.0 in a Global Context* wordt data security als het grootste economisch risico genoemd.[43] Daarnaast vreest men ook dat de kennis om gedigitaliseerde systemen te produceren en te ontwikkelen bij verschillende partijen komt te liggen, waardoor het product en de werking ervan niet ten volle begrepen kan worden. Interessant genoeg zijn data beveiliging en het gebrek aan kennis geen barrières voor de geïnterviewde partijen om te blijven ontwikkelen en produceren.

De *Industrial Policy 2030* van Duitsland is gebouwd op drie pilaren: 1) *Improving the overall conditions for entrepreneurial activities,* 2*) Strengthening new technologies –*

[41] Een van de hoofdthema's van het Duitse voorzitterschapsprogramma luidt "Een sterker en innovatiever Europa" met onder andere als prioriteit het "Uitbreiden van de digitale soevereiniteit van de EU". Federal Foreign Office, *Together for Europe's Recovery: The Programme for Germany's Presidency of the Council of the European Union,* Berlin: Federal Foreign Office, 2020. P. 8. Online: https://www.bundesgesundheitsministerium.de/eu2020/en/german-eu-presidency.html

[42] Platform i40, *2030 Vision for Industrie 4.0.* Online: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Vision-2030-for-Industrie-4.0.html

[43] Zie figuur 3 op pagina 22: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/industrie-40-in-a-global-context.html

mobilising private capital en 3*) Maintaining technological sovereignty*.[44] De aandachtspunten onder pilaar 1 zijn gericht op beleidsraamwerken die nationale beleidsmakers moeten vormgeven. Pilaar 2 benadrukt het belang van investeringen door de overheid en bedrijven in nieuwe technologieën. Enerzijds om koploper te blijven, maar ook om technologieën te ontwikkelen en daarvoor standaarden te definiëren. Pilaar 3 is onorthodox en geeft aan dat de technologische soevereiniteit beschermd moet worden door een betere cybersecurity en het verstevigen van maatregelen om technologie te beschermen (privatiseren of door wet en regelgeving).

Frankrijk adresseerde strategische autonomie op cybersecurity in twee documenten. De *Strategic Review of Defence and National Security* uit 2017 gaf aan dat er weinig toe- en inzicht is waar cyberaanvallen vandaan komen en wat ze teweeg kunnen brengen. Het concludeert dat digitale soevereiniteit een prioriteit is. De Franse cybersecuritystrategie is opgebouwd uit vijf pijlers die bijdragen aan de digitale transitie van Frankrijk en daarmee de uitdagingen van digitale technologieën het hoofd moeten bieden. Een van de vijf pijlers van deze *nationale cybersecuritystrategie* is het garanderen van nationale soevereiniteit.

Frankrijk trekt in veel initiatieven samen op met Duitsland. Bijvoorbeeld door investeringen in AI aan te moedigen door publiek geld te investeren in datacenters. Bij de lancering van dit fonds wordt samenwerking niet uitgesloten, maar wel gepresenteerd als een activiteit die ten minste door de Frans-Duitse as geïnitieerd moet zijn.[45] Doelstelling is om de data die gegenereerd en opgeslagen wordt in Europa te houden.

Vergelijkbaar met Duitsland heeft Frankrijk ook wettelijke bevoegdheden om buitenlandse overnames of investeringen te blokkeren. In Décret No. 2058-1057 van 29 November 2018 is te lezen dat de sectoren en producten uitgebreid zijn en tegelijkertijd specifiek benoemd. Er wordt expliciet beschreven dat het wetsartikel van toepassing is op bijvoorbeeld technologie die communicatie kan onderscheppen, AI, robotisering, 3D printing, IT-security producten, systemen en diensten en datahosting.[46]

Ten slotte heeft Frankrijk sinds 2015 een Frans Cybersecurity Label, opgericht en bestuurd door de overheid en industrie. Het label geeft kopers (bedrijven en overheidspartijen) aan dat de hardware, software, producten en diensten in kwestie aan de Franse cybersecurity eisen voldoen. Het label kan ook verworven worden door cybersecurity professionals.[47]

---

[44] Federal Ministry For Economic Affairs and Energy, *Industrial Strategy 2030 - Guidelines for a German and European industrial policy*, 2019. Online: https://www.bmwi.de/Redaktion/EN/Publikationen/Industry/industrial-strategy-2030.html

[45] European Council on Foreign Relations, *Machine politics: Europe and the AI revolution,* 2019. P.11. Online: https://ecfr.eu/publication/machine_politics_europe_and_the_ai_revolution/

[46] Squire Patton Boggs, *France's new investment control in the cybersecurity and technology sectors, 2019.* Online https://www.lexology.com/library/detail.aspx?g=008d9f8a-0d42-4a5b-8b34-041d2642803f

[47] *France Cybersecurity Label.* Online*:* https://www.francecybersecurity.fr/en/the-label/

4.3 Uitdagingen en dilemma's bij strategische autonomie op cybersecurity

Hoewel de overheid beschikt over een breed palet aan instrumenten om de strategische autonomie op cybersecurity te versterken, zijn er wel uitdagingen en dilemma's bij het borgen van strategische ambities.

Het mag duidelijk zijn dat de overheid voldoende geëquipeerd moet zijn om te waarborgen dat essentiële gedigitaliseerde of door digitale systemen ondersteunde functies (betalingsverkeer, transport, energie, gezondheidszorg etc.) niet in te grote mate afhankelijk zijn van of beheerst worden door buitenlandse private of publiek-private partijen. De mogelijkheden een eigen weg in te slaan in een geglobaliseerde en gedigitaliseerde samenleving zijn echter beperkt en komen niet zonder dilemma's. Bij het bepalen van de ambities voor het versterken van de strategische autonomie moet dan ook in ogenschouw worden genomen dat een streven naar meer controle en impact ook nadelige effecten kan hebben op de economie en de samenleving als het economische groei en innovatie belemmert. Tevens heeft de beperkte omvang van de technologiesector tot gevolg dat Nederland in veel gevallen eenvoudigweg niet zelfstandig de gewenste maatregelen kan nemen.

In de kern gaat het om het vinden van een balans tussen het versterken van de concurrentiekracht en het borgen van de nationale veiligheid. Een te ver doorgevoerd streven naar digitaal protectionisme (de wens om de eigen markt af te schermen op grond van veiligheidsoverwegingen) kan de internationale concurrentiepositie van de eigen digitale technologiesector verzwakken. Het belang van deze balans wordt veelvuldig benadrukt, ook weer in de conclusies van de Europese Raad van 2 oktober 2020. De EU-ambitie is dan ook "[s]trategische autonomie bereiken met behoud van de open economie." Daar waar op de korte termijn beschermende maatregelen de weerbaarheid van de samenleving misschien versterken, zal de impact op de lange termijn mogelijk negatief zijn. Niet alleen doordat de markt niet optimaal wordt benut maar ook door beperkingen aan de samenwerking tussen bedrijven waardoor het algehele niveau van digitale weerbaarheid kan afnemen.

4.3.1 Veiligheid versus marktwerking

Een belangrijke drijfveer voor beleidsontwikkeling door de EU op het terrein van cybersecurity is de, veronderstelde, te grote afhankelijkheid ten aanzien van de vitale digitale infrastructuur van leveranciers van buiten de EU.[48]

Om deze afhankelijkheid terug te dringen richt de EU zich tot nu toe vooral op innovatie in de ontwikkeling van cruciale digitale technologieën, met als doel een sterk industrieel en technologisch ecosysteem dat door een gemeenschappelijke technologie-strategie en gebundelde middelen wordt verenigd. Door het bevorderen van een competitieve interne markt wil de EU wereldwijd een relevante speler blijven op het terrein van digitale technologie. Ook op economisch, militair en cybersecurity gebied, met name waar het vitale infrastructuur en diensten betreft.[49] De EU tracht de sterke positie van veel Amerikaanse en Chinese technologische

[48] EPRS, Ideas Paper for the European Parliament, *Digital Sovereignty for Europe*, p.3. Online: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651992

[49] Atlantic Council, *European strategic autonomy and its future trade policy,* 2020, p.2. Online: https://www.atlanticcouncil.org/blogs/new-atlanticist/european-strategic-autonomy-and-its-future-trade-policy/

bedrijven op de Europese markt terug te dringen door het ontwikkelen van regels en standaarden die van toepassing zijn op de ontwikkeling, het gebruik en het beheer van digitale technologieën. Dit wil ze onder andere bewerkstelligen door het sluiten van betrouwbare en toekomstgerichte partnerschappen omtrent digitale strategische kwesties.[50]

Een voorbeeld hiervan is de oproep van de Europese Commissie om zo min mogelijk gebruik te maken van leveranciers met een hoog risico voor de aanbesteding van cruciale of gevoelige elementen van hun 5G-netwerken, zoals internet-*backbone* of kernnetwerken die het dataverkeer beheren.[51] De invloed van de Chinese overheid op technologiebedrijven, zorgt ervoor dat de veiligheid van de producten en diensten van, bijvoorbeeld, Huawei onvoldoende kan worden gewaarborgd. Huawei heeft daarbij een voorsprong op Europese bedrijven bij de ontwikkeling en implementatie van 5G producten en diensten waardoor een ongewenste economische afhankelijkheid dreigt te ontstaan.

Het verbieden of beperken van de toegang van Huawei tot Europese 5G-netwerken heeft echter ook een negatieve impact. Zo beperkt het de vrije marktwerking. Vanuit het oogpunt van innovatie en economische groei is het onwenselijk, en tot op zekere hoogte ook onhaalbaar, te streven naar een economisch model waarbij kritische componenten en diensten volledig geproduceerd en beheerd worden in één land of alleen door bevriende en vertrouwde staten. Het instellen van een algemeen verbod op het gebruik van technologie uit bepaalde landen of van specifieke leveranciers zal in veel gevallen een grote impact hebben op de eigen innovatie- en concurrentiekracht en die van bevriende staten.

Een verbod of verregaande beperking zal niet alleen leiden tot extra kosten voor de uitrol van 5G-technologie binnen Europa, maar ook de toegevoegde waarde van deze netwerken negatief kunnen beïnvloeden. Alternatieve leveranciers lopen mogelijk achter bij de ontwikkeling, implementatie en beheer van relevante of aanpalende technologieën. Daarnaast zal China naar verwachting tegenmaatregelen nemen, wat de concurrentiekracht van de Nederlandse en Europese IT-sector kan beperken. Door de grote afhankelijkheid van Nederland, en de EU in het algemeen, van buitenlandse hoogtechnologische en relatief goedkope producten, kan de impact van dergelijke maatregelen hoog zijn.

Ook op het gebied van hoogwaardige securityproducten en -diensten kunnen de behoeften van de overheid aan specifieke beveiligingsproducten de marktwerking verstoren. De uitgangspositie van de EU is op dit terrein niet optimaal. Het aantal Europese bedrijven dat actief is op de markt van hoogwaardige (*assurance*) securityproducten en -diensten is zeer beperkt. Europese en Nederlandse spelers zijn veelal niet in staat om te concurreren met de marktleiders.[52] Voor Nederland geldt daarnaast dat de laatste jaren verschillende cybersecurity-bedrijven zijn overgenomen door buitenlandse partijen. De sector zelf stelt echter dat het minder afhankelijk wil zijn van het buitenland en er meer innovatie in Nederland moet

---

[50] De EU heeft in partnerschappen met Japan, de VS en in NAVO-verband inspanningen gedaan om regelgeving over gegevensbeheer en ethisch gebruik van Artificiële Intelligentie (AI) op te stellen. EPSC, 2020. P. 2-3, 7, 17. Online: https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-118064052

[51] *Ibid*. p. 7.

[52] Interview met Prof. Dr. M.J.G. (Michel) van Eeten in Augustus 2020.

blijven. Het is de vraag of de beperkte omvang van Nederlandse kennis en expertise toereikend zal zijn om de noodzakelijke kwaliteit van hoogwaardige cybersecurityproducten te kunnen waarborgen.

De veiligheidsdiensten hechten groot belang aan de aanwezigheid van Nederlandse bedrijven die specifieke, hoogwaardige producten en diensten produceren. Een begrijpelijke wens, maar dit kan ertoe leiden dat deze bedrijven minder afzet in het buitenland genereren en minder intensief met internationale partners kunnen samenwerken. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) stelt "[m]et de huidige ontwikkelingen op het wereldtoneel en cybersecurity is het essentieel dat er producten zijn die bijzondere informatie kunnen beschermen tot het hoogste niveau. De Nederlandse crypto-industrie met haar producten geeft hier zodanig invulling aan dat de overheid veilig kan werken."[53] In de praktijk blijkt dat de overheid argwanend kijkt naar buitenlandse invloed op de sector. Zoals eerder vernoemd leidde de overname van Fox-IT door de Britse NCC Group ertoe dat overheidsinstellingen diverse contracten *on hold* werden gezet, ondanks de juridische afbakening van het crypto-bedrijfsonderdeel.[54] Hierdoor liep Fox-IT waarschijnlijk niet alleen opdrachten mis, maar vormde het ook een belemmering bij het vinden van opdrachtgevers in het buitenland.

4.3.2 Investeren in open Innovatie

Wil de EU de strategisch autonomie kunnen waarborgen dan zal het toonaangevend moeten zijn op het terrein van technologische innovatie. Openheid, transparantie en samenwerking zijn over het algemeen voorwaarden voor innovatie.[55] Het beperken van internationale samenwerking en toegang tot financiering kan een negatieve impact op de digitale weerbaarheid kunnen hebben doordat innovatie kan worden beperkt en landen en organisaties niet meer kunnen beschikken over *state of the art* technologieën. Een streven naar een grote mate van zelfredzaamheid is dan ook niet realistisch noch wenselijk. Duitsland heeft dit in haar Industrial Policy 2030 als volgt verwoord:

"it is necessary to avoid losses of expertise, and to retain self-determination in key fields of technology. Viewed in this way, technological autonomy is in line with the principles of open world markets."[56]

De investeringen van de EU-lidstaten in belangrijke nieuwe technologiegebieden als *5G*, *Artificial Intelligence* en *Quantum Computing* blijven echter achter bij de VS en China.[57] Onderzoek naar de wereldwijde registratie van patenten op het terrein van 5G toont aan dat de technologieën en specialisaties die noodzakelijk zijn voor

---

[53] EMERCE, *Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van de AIVD bestempelt beveiligingswaarde Fox Crypto DataDiode als 'ZEER GEHEIM', 2019.* Online: https://www.emerce.nl/wire/nationaal-bureau-verbindingsbeveiliging-onderdeel-aivd-bestempelt-beveiligingswaarde-fox-crypto-datadiode-zeer-geheim

[54] Het Financieel Dagblad, *De verloren jaren van Fox-IT,* 07-09-2019, pagina 20.

[55] Amerikaanse klimaatwetenschappers merkten dat door het beleid en de opvattingen van President Trump deze randvoorwaarden in het geding kwamen. Het aanbod van President Macron om klimaatonderzoek in Frankrijk voort te zetten is een voorbeeld vanuit een ander domein, met een eenzelfde impact op innovatiekracht en capaciteit binnen de Verenigde Staten.

[56] Federal Ministry For Economic Affairs and Energy, *Industrial Strategy 2030 - Guidelines for a German and European industrial policy*, p. 27.

[57] European Political Strategy Centre , *Rethinking Strategic Autonomy in the Digital Age* (Brussels: European Political Strategy Centre, 2019), 5.

de ontwikkeling van 5G-producten en diensten in toenemende mate geconcentreerd zijn in een beperkt aantal landen. Dit fenomeen vergroot de kloof tussen leiders en volgers. De koplopers zijn duidelijk de VS, China, Japan en Zuid-Korea terwijl Europese landen achteropraken.[58] Echter, als regio's op geaggregeerd(er) niveau worden bekeken, blijkt dat Europa haar positie merkbaar kan versterken indien er intensiever wordt samengewerkt. Een EU die in staat is het gezamenlijke innovatie potentieel te benutten door effectieve coördinatie kan het zich ontwikkelen tot een meer invloedrijke speler.[59]

Automated Security

Automated security is een onderzoeksgebied waar de afgelopen jaren veel in wordt geïnvesteerd, met name door de VS en China. Het gaat om het automatisch opsporen en verhelpen van kwetsbaarheden in software door gebruik te maken van *machine learning* en AI-technologie. De toenemende complexiteit van software in combinatie met de diversiteit aan hardware waarop de software draait zorgt ervoor dat de veiligheid van hardware, software en diensten op termijn alleen kan worden gewaarborgd indien de ontwikkeling ervan (testen van prototypes) en gebruik (monitoring- en detectieprocessen) voor een groot deel geautomatiseerd worden. Aanhoudende schaarste aan gekwalificeerd personeel blijft in deze context ook een grote uitdaging, alhoewel bedrijven die hardware-en softwaretesten uitvoeren reeds veelvuldig gebruik maken van de internationale arbeidsmarkt. Desondanks is het geautomatiseerd kunnen verdedigen van groot belang omdat ook de aanvallers in toenemende mate gebruikmaken van *automated exploitation* technieken. Hierdoor zal de diversiteit en kracht van de aanvallen exponentieel toenemen.

Aangezien het kunnen beschikken over voldoende data ten grondslag ligt aan iedere succesvolle *machine learning* toepassing, ligt samenwerking bij het delen van data voor de hand. In de VS en China is echter zichtbaar dat de ontwikkeling van *automated security*onderzoek en -ontwikkeling steeds meer wordt afgeschermd.[60] De relevante kennis en kunde worden op gronden van nationale veiligheid vaak gerubriceerd.

Door de beperkte omvang van de Nederlandse cybersecurity sector op het terrein van *automated security* wordt het moeilijk om voldoende kennis op te bouwen om de eigen belangen voldoende te beschermen. Tevens is de in Nederland beschikbare data beperkt van omvang en daarmee een belemmering voor de ontwikkeling van producten en diensten op dit terrein. Door in Europees verband nauw samen te werken kunnen deze beperkingen (deels) overkomen worden. Een voorbeeld van samenwerking binnen Nederland is het Consortium Automated Security Operations waar publieke en private partijen aan deelnemen.[61]

---

[58] Pier Luigi Parcu, et. al., *Ubiquitous technologies and 5G development. Who owns the rarest technologies?* Online*:* https://cadmus.eui.eu/bitstream/handle/1814/68117/RSCAS%202020_56.pdf?sequence=1&isAllowed=y

[59] *Ibid*, p. 14.

[60] Merics, *Chinese hackers are expected to put their country first*. Online: https://merics.org/en/analysis/chinese-hackers-are-expected-put-their-country-first en CyberScoop, *Mayhem, the tech behind the DARPA Grand Challenge winner, now used by the Pentagon*. Online: https://www.cyberscoop.com/mayhem-darpa-cyber-grand-challenge-dod-voltron/

[61] TNO, *Consortium Automated Security Operations van start voor een weerbaar digitaal Zuid-Holland,* 2019. *O*nline: www.tno.nl/nl/over-tno/nieuws/2019/10/consortium-automated-security-van-start/

Daarnaast coördineert en participeert TNO in een H2020-project dat tot doel heeft een '*security automation and decision support platform*' te ontwikkelen en implementeren.[62]

De achterblijvende overheidsinvesteringen in sleuteltechnologieën bedreigen de strategische positie van Nederland en de EU. Hoe kleiner de bijdrage vanuit de EU aan het ontwikkelen van nieuwe digitale technologieën, hoe beperkter de strategische autonomie, doordat de toekomst van het digitale domein dan voor een groot deel wordt vormgeven en beheerd door niet EU-partijen. Hierdoor is er afnemende invloed en controle op sleuteltechnologieën en de leveranciers die producten en diensten leveren voor bijvoorbeeld onze vitale infrastructuur. Dit kan resulteren in een vermindering van controle en daardoor grip op beschikbaarheid, continuïteit, integriteit en vertrouwelijkheid van data, producten, IT-systemen, netwerken en processen. Daarnaast heeft het ook impact op de mate van invloed van de EU op het ontwikkelen van standaarden voor nieuwe technologie gebieden.[63]

4.3.3 Beperkte investeringen private sector

Bij innovatie is niet alleen de overheid aan zet maar is het ook noodzakelijk dat private partijen investeren. Voor de sleuteltechnologieën blijven Europese bedrijven hier ook vaak achter bij concurrenten uit China de VS. Dit geldt bijvoorbeeld bij de ontwikkeling van de kwantumcomputer. Door de verwachte impact wordt er, onder andere, door China, de EU en de VS fors geïnvesteerd in de ontwikkeling van deze technologie. De ontwikkeling van de kwantumcomputer in Nederland vindt voor een belangrijk deel plaats bij QuTech en is een publiek-private samenwerking tussen nationale en internationale partijen. Deze intensieve samenwerking zorgt ervoor dat Nederland nog een koplopers rol kan vervullen op dit terrein.

In 2019 opende Microsoft één van haar vier Quantum Labs in Delft. De investering van Microsoft is een belangrijke impuls voor onderzoek in Nederland waarbij ook intensief wordt samengewerkt met QuTech. De betrokkenheid van het Nederlandse en Europese bedrijfsleven is vooralsnog echter beperkt. Dit kan tot gevolg hebben dat wanneer het onderzoek een hoger TRL-niveau bereikt er geen Europese bedrijven zijn die daar een rol in kunnen spelen. Dit kan de kennispositie en concurrentiekracht van Nederland op de lange termijn benadelen. Ook als het onderzoek voor iedereen toegankelijk is, kan een beperkte betrokkenheid van bedrijven uit Nederland en de EU tot gevolg hebben dat de economische voordelen bij partijen van buiten de EU komen te liggen. Een sterke kennisbasis kan dan alsnog tot gevolg hebben dat de EU afhankelijk wordt van buitenlandse bedrijven.

Ook voor het Nederlandse cybersecurity-innovatielandschap geldt dat de betrokkenheid van de private sector beperkt is. Nederland behoort tot de Europese koplopers, de sector is divers en bestaat uit een grote verscheidenheid aan actoren en omvat relatief veel bedrijven, samenwerkingsverbanden en initiatieven die direct

---

[62] SOCCRATES - Automation of Response to Attack & Threats Project. Online: https://www.soccrates.eu/

[63] Ter illustratie: de werkgroep voor standaarden voor AI-toepassingen van het ISO/IEC wordt bijvoorbeeld voorgezeten door een Huawei-medewerker uit de VS, het secretariaat wordt beheerd door de VS en de eerste bijeenkomst was in China. Zie United Nations University Centre for Policy Research, *AI & Global Governance: Using International Standards as an Agile Tool for Governance,* 2019.

of indirect een bijdrage leveren aan cybersecurity-innovatie.[64] Zo behoort Nederland op het terrein van cybersecurity binnen de EU tot de koplopers wat betreft het aantal wetenschappelijke publicaties.[65]

Het stokt echter vaak bij het doorontwikkelen van deze kennis tot een hoger TRL-niveau waarbij een gebrek aan financieringsopties wordt ervaren.[66] De meeste cybersecurity bedrijven zijn in het algemeen relatief klein in omvang en vaak gericht op de veiligheid van een specifiek product of dienst. Tevens is er nog weinig sprake van een geïntegreerde Europese cybersecuritymarkt – het gebrek aan integratie van Nederlandse en buitenlandse cybersecurity producten en diensten worden als te gefragmenteerd ervaren. Deze fragmentatie vermindert de algehele cybersecurity.[67]

4.3.4 Autonomie in een geglobaliseerde economie

De meeste uitdagingen ten aanzien van cybersecurity blijven niet tot Nederland of de EU beperkt. Landen, organisaties en individuen staan voor het grootste deel voor dezelfde uitdagingen en hebben allen baat bij een afdoende digitale veiligheid. De veiligheid van IoT-applicaties is voor iedere leverancier en gebruiker van belang en dus geen uitdaging die alleen voor bepaalde landen geldt. Vele fabrikanten van IoT-apparaten zetten zich in om veilige producten te maken voor de economische levensduur van het product of dienst en laten prototypes testen bij onafhankelijke bedrijven van over de hele wereld.[68] Er is dus een inherent gedeeld belang bij het waarborgen van de cybersecurity van gedigitaliseerde producten en diensten. Het belang van intensieve, multilaterale en publiek/private, samenwerking is daardoor evident.

Digitale producten en diensten en de onderliggende technologie die gebruikt worden in productieprocessen en ketens bestaan tevens uit componenten die wereldwijd ontwikkeld en geproduceerd worden. Voor vrijwel alle belangrijke *supply chains* geldt dat deze internationaal vorm worden gegeven en gekenmerkt worden door verregaande (wederzijdse) afhankelijkheden. Het volledig inrichten van digitale ketens binnen Nederland of de EU is dan ook vrijwel onmogelijk en ook onwenselijk. De uitdaging is dus niet zozeer het enkel pogen risico's of kwetsbaarheden in *supply chains* te voorkomen of weg te nemen, maar eerder het effectief beperken en beheersen daarvan.[69]

---

[64] Dit betreft zogenaamde '*pure players*' - bedrijven die alleen cybersecurity gerelateerde activiteiten uitvoeren - als ook '*partial players*' - actoren voor wie cybersecurity niet tot de kern van hun activiteiten behoort, zoals bijvoorbeeld banken. Zie TNO, *Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity, 2019*, p.3.

[65] *Ibid.*

[66] *Ibid*, p 42.

[67] Beredeneert vanuit de innovatie en valorisatiebehoefte die geïdentificeerd is door het consortium Automated Security.

[68] Samsung, voluntary secure by design UK/Samsung en Agentschap Telecom. Online: https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices, en https://www.agentschaptelecom.nl/actueel/nieuws/2020/08/26/acht-simpele-eisen-kunnen-de-cyberveiligheid-van-%E2%80%98slimme-apparatuur%E2%80%99-sterk-verbeteren

[69] Luukas Ilves and Anna-Maria Osula in European Cybersecurity Journal, *The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out*, 2019, p.27. Online: https://m.guardtime.com/files/Ilves_Osula.pdf.

Een internationale waardeketen; de F-35

Het belangrijkste luchtverdedigingswapensysteem van Nederland is de F-35. Dit is een Amerikaans toestel, maar bij het gehele ontwikkelings-, productieproces en bij het onderhoud zijn vele internationale partijen betrokken. Veel essentiële onderdelen zijn (mede) in derde landen ontwikkeld, worden daar geproduceerd en mogelijk (deels) ook onderhouden. Dit voorbeeld gaat niet zo zeer om een typische cybersecurity-casus. De 35 casus is opgenomen omdat het een sprekend voorbeeld is van een uitermate complexe internationale waardeketen, wat ook geldt voor cybersecurity producten en diensten.

Voor de F35 zijn zes leveranciers vermeld voor *'safety & security systems'*, zeven voor *'Communications* (*airborne*)', zes voor *'Flight & Data management'*, dertien voor *'Indicators & Instruments'* en zestien voor *'Weapons systems'*. De door derden geproduceerde componenten bevatten ook een veelheid aan ICT-toepassingen, waarvan de individuele onderdelen ook weer door anderen (kunnen) worden geleverd.[70] De informatie over de uitdagingen die hier gegeven zijn over de F-35 zijn veelal ook van toepassing op producten en diensten die in Nederland gebruikt worden ter bescherming van bijvoorbeeld de vitale processen.

Hoewel er bij de ontwikkelingen en het testen van de F-35 nadrukkelijk aandacht is besteed aan de digitale veiligheid van componenten en systemen[71] is de uitdaging voor de lange termijn hierdoor niet weggenomen. Het zekerstellen dat alle ICT-componenten naar behoren (blijven) functioneren, op een correcte manier zijn gecertificeerd en beschikken over voldoende bescherming tegen manipulatie blijft een zeer complexe uitdaging. Hoewel Nederland een partner is bij de ontwikkeling en productie van onderdelen van de F-35, heeft het geen controle over of toezicht op de gehele productie- en leveringsketen.

Defensie heeft een verantwoordelijkheid voor het testen, toetsen en beoordelen van digitale systemen in de F-35, zelfstandig of in samenwerking met (inter)nationale partners en private partijen. Daarmee kan echter nog niet worden zeker gesteld dat Defensie in staat is om ook in uitzonderingssituaties (tijdens een gewapend conflict) zelfstandig zeker te stellen dat de F-35 naar behoren blijft functioneren. Indien partners in de waardeketen in staat blijken te zijn en besluiten om de functionaliteit van het wapensysteem te beperken of bewust kwetsbaar te maken, dan moet de krijgsmacht in staat zijn hiervoor mitigerende maatregelen te nemen. Dit geldt natuurlijk ook voor alle andere wapensystemen en alle andere netwerken en systemen. Er moet dus afdoende kennis, kunde en middelen beschikbaar zijn om voor alle relevante wapensystemen te allen tijde maatregelen te kunnen treffen om de inzetbaarheid van wapensystemen te garanderen. De hiervoor noodzakelijke Nederlandse kennisbasis op het terrein van cybersecurity is als gevolg daarvan zowel breed als specifiek.[72] Gezien de omvang van de uitdaging is het ook aan te bevelen om de samenwerking met specifieke bondgenoten te versterken om

[70] Airframer, Lockheed Martin F-35 Lightning II - *program supplier guide.* Online: https://www.airframer.com/aircraft_detail.html?model=F-35_JSF

[71] Cyber Security Intelligence, *F-35 Is The Most Thoroughly Tested Cyber Weapon.* Online*:* https://www.cybersecurityintelligence.com/blog/f-35-is-the-most-thoroughly-tested-cyber-weapon-3442.html

[72] In een voor Defensie uitgevoerde analyse door Price Watershouse Coopers werd in 2015 nog geconcludeerd dat in relatie tot de F-35 innovatie op het terrein van cybersecurity “minder interessant of niet gerelateerd aan de instandhouding” was. Online: https://zoek.officielebekendmakingen.nl/blg-532420.pdf

gebruik te maken van elkaars sterke punten en op grond daarvan keuzes te maken over wie het voortouw neemt bij het ontwikkelen van specifieke capaciteiten.[73]

Het is nog maar de vraag of een geïntegreerde en dynamische *supply chain* nog wel eenzijdig te beïnvloeden is zonder hieraan afbreuk te doen. De behoefte aan meer zeggenschap over, meer controle op en meer vertrouwen in digitale diensten en de werking van digitale systemen komt onherroepelijk met beperkingen en levert als resultaat wellicht een schijn van autonomie op. Als het bijvoorbeeld om 5G-diensten (apparatuur en software) gaat, kan (vooralsnog) geen enkele leverancier alle benodigde onderdelen zelf ontwikkelen en produceren. Daarom hebben de bedrijven in deze markt een patent/octrooipool gecreëerd waarmee ze de technologie van de competitie kunnen gebruiken.

Om binnen geïntegreerde en dynamische *supply chains* de veiligheid van digitale componenten te kunnen waarborgen is het noodzakelijk om over voldoende capaciteit te beschikken om dit zelfstandig of in combinatie met vertrouwde partners te kunnen beoordelen.

[73] De huidige strategische partners van Defensie voor structurele bilaterale samenwerking zijn: België, Luxemburg, Duitsland, Frankrijk, Noorwegen, het Verenigd Koninkrijk en de Verenigde Staten. Op het terrein van cyber defence wordt samenwerking met Duitsland en het VK specifiek genoemd. Online: https://zoek.officielebekendmakingen.nl/kst-33279-29.html

5 Conclusie

Strategische autonomie op cybersecurity is belangrijk voor de veiligheid en de stabiliteit van Nederland. Het vermogen om zelf te bepalen hoe de samenleving er in een gedigitaliseerde wereld uit komt te zien staat in Nederland en Europa onder toenemende druk. De economische afhankelijkheid van, vooral, digitale diensten uit de VS en digitale hardware uit China neemt snel toe, evenals de daaraan verbonden digitale dreigingen. Ook loopt de EU achter bij het investeren in innovatie op digitale sleuteltechnologieën. Nederland en de EU dreigen hierdoor kwetsbaar te worden. Het onderzoek voor dit *whitepaper* toont aan dat Nederland op de lange termijn de digitale weerbaarheid niet kan waarborgen als de huidige trends zich doorzetten. Een te groot deel van de digitale infrastructuur en diensten, niet alleen vitale onderdelen, wordt te afhankelijk van leveranciers van buiten de EU. Daarnaast is de kennisbasis van Nederland te smal om zelfstandig weerbaar te blijven tegen toekomstige digitale dreigingen.

Het handelingsperspectief van overheden in uitzonderingssituaties komt hierdoor onder druk te staan. Hoe betrouwbaar en beschikbaar zijn vitale capaciteiten en beheersmaatregelen in tijden van schaarste, rampen en politieke, of maatschappelijke spanningen? Daarom is het belangrijk vast te kunnen stellen of er voldoende handelingsperspectief aanwezig is in het geval van een potentiële grote verstoring, uitval of manipulatie van vitale onderdelen van de samenleving (de zogenaamde uitzonderingssituaties). Hierbij is het wenselijk te bezien of de overheid (in samenwerking met andere nationale actoren zoals het bedrijfsleven, kennisinstellingen en *civil society*) zelfstandig in staat is te handelen of dat af te dwingen. In een dergelijke uitzonderingssituatie kan het functioneren van bestaande afspraken, procedures en processen onder druk komen te staan (of worden deze zelfstandig, of door andere landen en bedrijven gewijzigd) en moet de Nederlandse overheid terug kunnen vallen op andere maatregelen en middelen, al dan niet gedefinieerd in crisismanagementprocessen die inspelen op een dergelijk scenario. Hoe kunnen Nederlandse essentiële diensten nog functioneren wanneer internetconnectiviteit uitvalt, of wanneer bestaande internetbeveiligingsstandaarden onbetrouwbaar blijken doordat Nederland niet beschikt over de kennis en kunde om nieuwe encryptie-protocollen of software-updates van buitenlandse leveranciers voor kritieke systemen te kunnen controleren of voldoende mitigerende maatregelen te treffen bij verstoring?

De overheid beschikt over een breed instrumentarium om de positie van Nederland te versterken, door, onder andere, het bevorderen van kennis en innovatie, het ontwikkelen van wet- en regelgeving en het versterken van de concurrentiekracht. Digitale weerbaarheid is echter geen *zero-sum game* waarbij alles wat niet in eigen hand of door de belangrijkste partners is ontwikkeld of kan worden gecontroleerd onveilig is. Samenwerking op het terrein van cybersecurity is voor de meeste partijen, publiek en privaat, een vanzelfsprekendheid. Alleen door informatie, methodes en technieken te delen kan gelijke pas worden gehouden met de dreiging. Kennisdeling en samen innoveren moet dus een gemeenschappelijk vetrekpunt zijn en blijven. Het afschermen van de eigen markt om niet vertrouwde partijen te weren en de eigen markt te ondersteunen kan noodzakelijk zijn. Echter, protectionistische maatregelen zullen ook tot vergeldingen leiden. Dit beperkt de

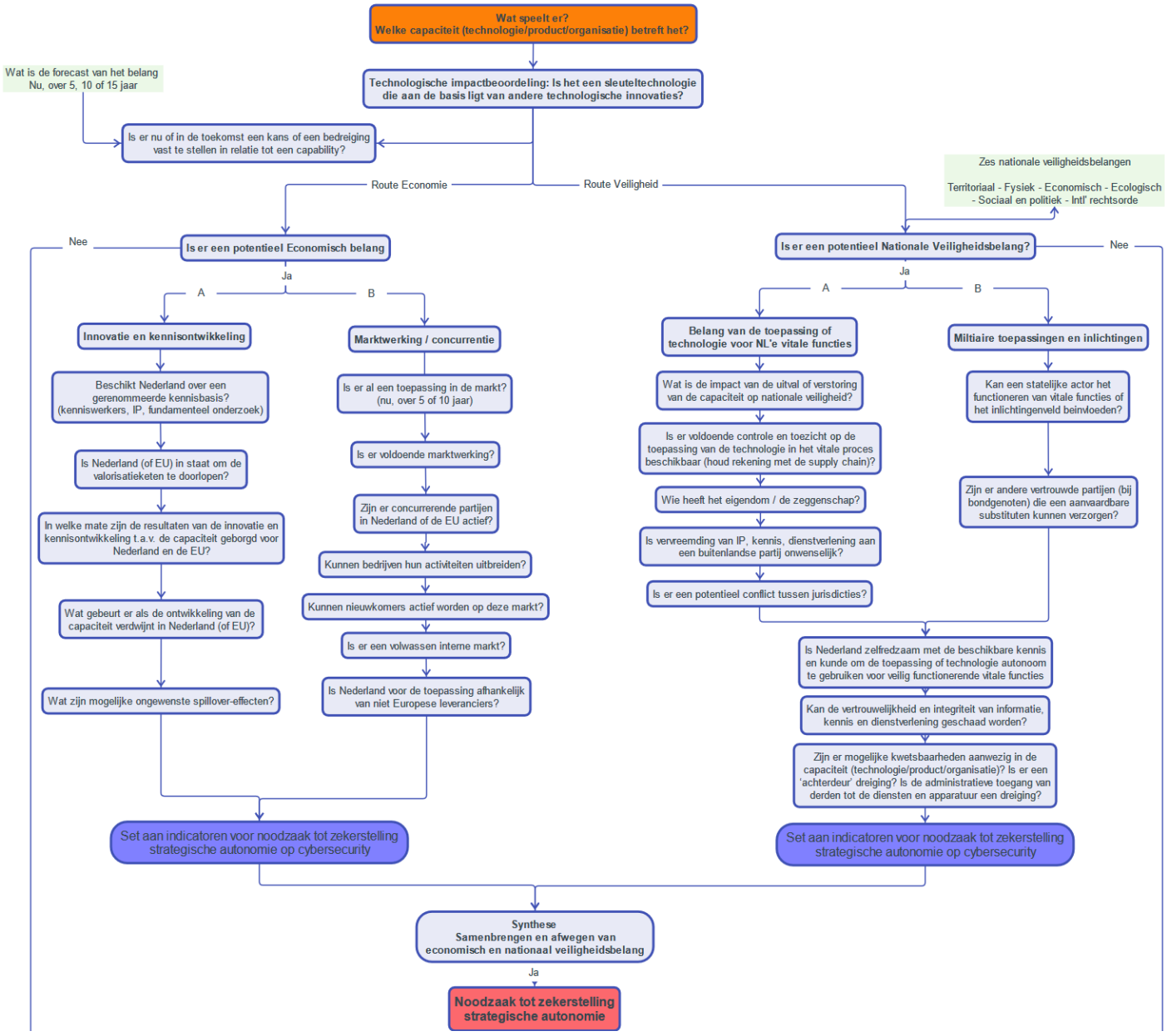
concurrentiekracht van de Nederlandse en Europese cybersecurity sector op de lange termijn en kan ons als samenleving kwetsbaarder en afhankelijk maken.

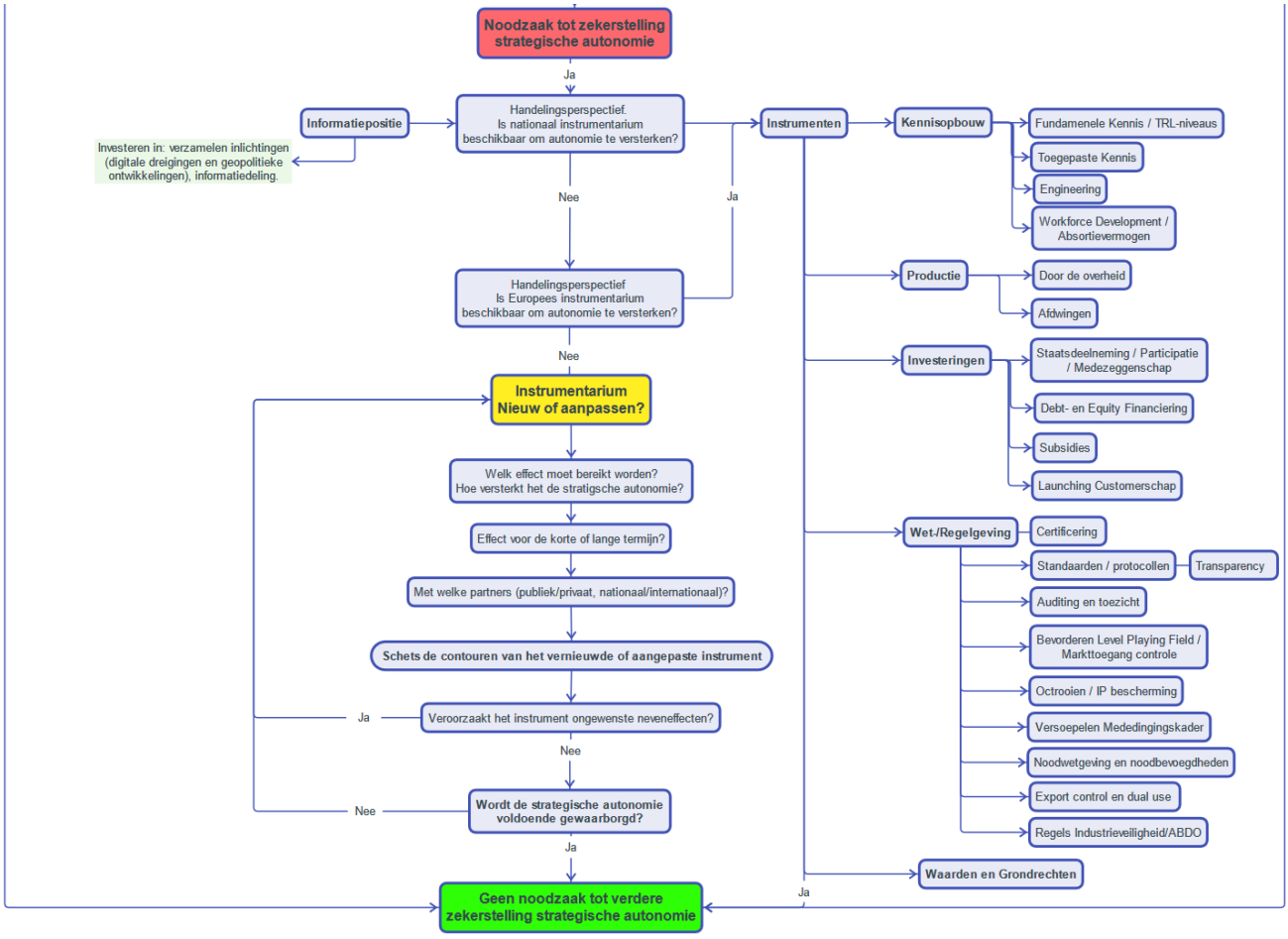
Het aan banden leggen van samenwerking heeft ook gevolgen voor de innovatiekracht in Nederland. Door intensief samenwerking binnen Europa te bevorderen kan dit deels worden opgevangen. Maar wanneer samenwerking met kennisinstellingen en private partijen van buiten Europa wordt beperkt kan dit er ook toe leiden dat onze capaciteit om te profiteren van innovatie van buiten de EU afneemt. Gezien de verregaande globalisering van, met name, de digitale sector is het ook maar de vraag in hoeverre een streven naar meer autonomie een beperking van technologische vooruitgang en verschraling van het aanbod tot gevolg zal hebben.

Om de strategische autonomie voor de lange termijn te kunnen blijven waarborgen moet Nederland fors investeren in de eigen innovatie en concurrentiekracht.

Dit moet zoveel mogelijk in EU-verband worden uitgewerkt. Alleen zo kan voldoende massa worden gecreëerd om wereldwijd relevant te blijven op de hoogtechnologische ontwikkelingen die noodzakelijk zijn om de digitale weerbaarheid te waarborgen.

A Flowchart ‘Vaststellen van noodzaak tot borgen strategische autonomie op cybersecurity’




Noodzaak tot zekerstelling strategische autonomie
Ja
Informatiepositie
Handelingsperspectief
Is nationaal instrumentarium beschikbaar om autonomie te versterken?
Investeren in: verzamelen inlichtingen (digitale dreigingen en geopolitieke ontwikkelingen), informatiedeling.
Nee
Ja
Handelingsperspectief
Is Europees instrumentarium beschikbaar om autonomie te versterken?
Nee
Instrumentarium Nieuw of aanpassen?
Welk effect moet bereikt worden?
Hoe versterkt het de stratigsche autonomie?
Effect voor de korte of lange termijn?
Met welke partners (publiek/privaat, nationaal/internationaal)?
Schets de contouren van het vernieuwde of aangepaste instrument
Ja
Veroorzaakt het instrument ongewenste neveneffecten?
Nee
Nee
Wordt de strategische autonomie voldoende gewaarborgd?
Ja
Geen noodzaak tot verdere zekerstelling strategische autonomie
Instrumenten
Kennisopbouw
Fundamenele Kennis / TRL-niveaus
Toegepaste Kennis
Engineering
Workforce Development / Absortievermogen
Productie
Door de overheid
Afdwingen
Investeringen
Staatsdeelneming / Participatie / Medezeggenschap
Debt- en Equity Financiering
Subsidies
Launching Customerschap
Wet-/Regelgeving
Certificering
Standaarden / protocollen
Transparency
Auditing en toezicht
Bevorderen Level Playing Field / Markttoegang controle
Octrooien / IP bescherming
Versoepelen Mededingingskader
Noodwetgeving en noodbevoegdheden
Export control en dual use
Regels Industrieveiligheid/ABDO
Waarden en Grondrechten
Ja

B Beschrijving Flowchart ‘Vaststellen van noodzaak tot borgen strategische autonomie op cybersecurity’

In dit hoofdstuk wordt het in de *flowchart* gehanteerde analysekader uitgelegd en toegelicht. De *flowchart* stelt gebruikers in staat op een gestructureerde manier na te denken over de noodzaak tot versterken of zekerstelling van de strategische autonomie op cybersecurity. Hierbij wordt rekening gehouden met de bredere samenhang tussen cybersecurity en economische, maatschappelijke en nationale veiligheidsbelangen. De *flowchart* is opgebouwd rondom een specifiek thema en is bedoeld om te bepalen of de strategische autonomie op cybersecurity moet worden beschermd of bevorderd. De meeste vragen worden met ‘ja’ of ‘nee’ beantwoord. Veelal is het noodzakelijk om een gedegen analyse van de context te maken en de benodigde achtergrondinformatie te achterhalen om de vraag te kunnen beantwoorden.

De *flowchart* hoeft niet volledig doorlopen te worden. Sommige aspecten zullen voor een bepaald thema niet of minder relevant zijn en kunnen dus worden overgeslagen. Hierin kan de lezer zelf beslissingen maken. De *flowchart* bestaat uit twee delen. Het gedeelte voor het concluderen dat er een noodzaak is tot zekerstelling van de strategische autonomie en na het gedeelte na de vaststelling van die noodzaak. Dit moment is eenvoudig terug te vinden in de *flowchart* in het enige rode blok.

In veel gevallen zal het antwoord op een vraag in de flowchart ook nog niet kunnen worden gegeven omdat de daarvoor noodzakelijk kennis of informatie (nog) niet beschikbaar is. De *flowchart* kan dus ook aanleiding geven tot nader onderzoek voordat vastgesteld kan worden of er een noodzaak is tot het versterken van de strategische autonomie.

Beschrijving flowchart

Deze paragraaf geeft meer achtergrondinformatie per tekstblok uit de *flowchart*. De tekstblokken in de *flowchart* bieden zijn te weinig ruimte voor de benodigde achtergrondinformatie. De beschrijvingen dienen als hulpmiddel tijdens het doorlopen van de *flowchart*.

1 Scope: Wat speelt er?

De eerste stap is het bepalen van het thema. Dit kan een technologiegebied zijn. In sommige gevallen is dit eenvoudig – bijvoorbeeld voor 5G – terwijl in andere gevallen deze eerst dient te worden afgebakend. Het belang van een technologiegebied is echter afhankelijk van de toepassingen die het mogelijk maakt. Uiteindelijk gaat het om het vermogen van de samenleving om autonoom te handelen en de capaciteiten die daarvoor van wezenlijk belang zijn.

2 Selectie technologiegebied

Het technologiegebied kan aan de basis liggen voor andere technologische innovaties. Voor relevante technologiegebieden voor cybersecurity kan naar de in

de Kennis en Innovatie Agenda (KIA) Veiligheid genoemde sleuteltechnologieën worden gekeken: *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*.

3 Technologische Impactbeoordeling: Is het een sleuteltechnologie die aan de basis ligt van andere technologische innovaties?

Pas bij toepassing van een technologie wordt duidelijk of het een belang voor strategische autonomie vertegenwoordigd. Welke producten, diensten, processen maken gebruik van deze technologie en wat is hiervan de impact? Zal de technologie op korte en lange termijn in belang toenemen waardoor vervreemding aan een buitenlandse partij de Nederlandse belangen mogelijk schaadt? Het uitvoeren van een technologische forecast is belangrijk om inzicht te krijgen in de toegevoegde waarde van de technologie voor andere innovaties. 5G wordt bijvoorbeeld gezien als een sleuteltechnologie die andere technologische innovatie mogelijk maakt, zoals autonome voertuigen, *smart electric grids*, en het *internet of things*. Door te analyseren welke potentiële toepassingen mogelijk worden, kan een inschatting worden gemaakt van de impact en van het belang om als staat vrij te kunnen beslissen en handelen.

4 Beoordeling Economisch en Nationaal Veiligheidsbelang: Brengt de technologie (en aanbieder) risico's met zich mee op het gebied van handel, economie, en nationale veiligheid?

Naast de cybersecurity belangen, is de volgende stap in de *flowchart* het duiden van de (mogelijke) impact van de technologie op de bredere nationale economische en veiligheidsbelangen.[74] Indien dit niet het geval is wordt het proces om de *flowchart* met de desbetreffende specifieke technologie beëindigd; er is geen noodzaak tot verdere zekerstelling van de digitale autonomie. Indien het antwoord nog niet kan worden gegeven is de volgende stap om de belangen in de twee paden te doorlopen.

4.1 Economisch Belang: is er sprake van marktwerking of economische afhankelijkheid en hoe ziet het kennis en innovatie speelveld eruit?

<u>Route A. innovatie en kennisontwikkeling</u>

*S*trategische autonomie kan zorgen voor een betere marktwerking en open concurrentie die de (Europese) industrie innovatiever en competitiever maakt. Dit geldt niet alleen voor de desbetreffende technologie maar ook voor de gerelateerde diensten of markten die eraan verbonden zijn (die de technologie ondersteunen of waarbij de technologie een ondersteunende functie vervult). Allereerst is het van belang vast te stellen wat de kennisbasis in Nederland en de EU is. Voor het ontwikkelen van een vooruitstrevende en concurrerende economische bijdrage op nieuwe technologiegebieden is een sterke kennisbasis en innovatiekracht noodzakelijk. Of het economisch potentieel benut kan worden moet dus bekeken worden of Nederland beschikt over een relevante kennisbasis.

[74] De zes nationale veiligheidsbelangen van Nederland omvat: (1) territoriale veiligheid; (2) fysieke veiligheid; (3) economische veiligheid; (4) ecologische veiligheid; (5) sociale en politieke stabiliteit, en (6) de internationale rechtsorde.

Bij het inventariseren van de kennisbasis moet niet alleen naar Nederland worden gekeken maar ook naar de EU. Nederland is te klein om op alle relevante kennisgebieden voorop te lopen en internationale samenwerking bij fundamenteel onderzoek is noodzakelijk.

Of de kennisbasis voldoende is, is moeilijk te kwantificeren. Het is echter wel mogelijk vast te stellen of Nederland over kwalitatief hoogstaande onderzoekers beschikt en of deze internationaal ook in hoog aanzien staan. Ook wanneer de kennisbasis smal is, kan Nederland een relevante bijdrage aan de ontwikkeling van een technologiegebied leveren.

De toegevoegde waarde van fundamenteel onderzoek wordt voor een belangrijk deel geleverd door de mate waarin deze kennis kan worden doorontwikkeld tot concrete producten en diensten. Er moet dus ook worden gekeken naar het functioneren van de valorisatieketen. In de valorisatieketen is het ook van belang om de vraagzijde mee te nemen. Zijn er partijen die specifieke behoefte kunnen identificeren en bereid zijn daarin te investeren? Het kan bijvoorbeeld zo zijn dat er binnen de EU nog geen partijen zijn die bereid zijn te investeren in kennisontwikkeling terwijl dit buiten de EU wel gedaan wordt door publieke en private partijen.

Een belangrijk aspect in opvolging van alle bovenstaande vragen rondom innovatie en marktontwikkeling is het inzichtelijk maken welke mogelijke spillovereffecten kunnen optreden. Indien financiering van onderzoek door partijen van buiten de EU wordt vergroot bestaat het risico dat de *marketiziation* daarvan ook vooral door die partijen zal worden gerealiseerd. Ook als het onderzoek voor iedereen toegankelijk is, kan een beperkte betrokkenheid van bedrijven uit Nederland en de EU tot gevolg hebben dat de economische voordelen bij partijen van buiten de EU komen te liggen. Een sterke kennisbasis kan dan alsnog tot gevolg hebben dat de EU afhankelijk wordt van buitenlandse bedrijven.

<u>Route B. Marktwerking / concurrentie</u>

Open concurrentie (mededinging) is een belangrijke voorwaarde voor een vrije Europese handel en de totstandbrenging en het goed laten functioneren van de Europese interne markt.

De eerste vraag is dus of er sprake is van een gezonde mate van marktwerking met diverse aanbieders uit verschillende regio's. Hierbij moet specifiek worden gekeken naar de positie van Nederlandse en EU-bedrijven in dit segment.

Een aanvullende vraag hierbij is of bedrijven in staat zijn om bestaande activiteiten uit te breiden of toe te treden tot het onderhavige marktsegment. Dit geldt ook voor de mate waarin nieuwe bedrijven in staat zijn toegang tot het marktsegment te krijgen.

Hierop moet ook worden bezien in hoeverre er sprake is van een volwassen en functionerende interne markt. De interne markt voor diensten functioneert in

veel gevallen nog niet optimaal en staat de groei van Europese bedrijven in de weg doordat ze binnen Europa onvoldoende schaalvoordelen kunnen behalen.

De laatste vraag in route is of Nederland niet te afhankelijk is van niet EU-leveranciers voor de toepassing. Een te grote afhankelijkheid van één (non-EU) aanbieder, zowel van diensten als de onderliggende soft- en hardware, en een gebrek aan competitie brengt naast cybersecurityrisico's ook economische risico's met zich mee. Bijvoorbeeld het ontstaan van marktmonopolies en prijsstijgingen, die vervolgens kunnen bijdragen aan een groeiende Nederlandse en Europese innovatieachterstand en potentieel marktfalen. Hoe afhankelijker men is van één partij, hoe groter de economische impact is van mogelijke verstoringen in de levering van een bepaalde dienst. Voldoende en eerlijke concurrentie zorgt voor een goede marktwerking waarin deze afhankelijkheid wordt geminimaliseerd en waar bestaande bedrijven hun activiteiten kunnen uitbreiden terwijl nieuwe bedrijven nog kunnen toetreden.

4.2 Nationaal veiligheidsbelang: Is Nederland afhankelijk van de technologie om haar nationale veiligheid te waarborgen?

<u>Route A en B</u>

Nieuwe technologieën kunnen ook de nationale veiligheidsbelangen van Nederland aantasten. Dit kan het geval zijn wanneer vitale functies afhankelijk zijn van de desbetreffende technologie, of wanneer deze wordt gebruikt voor militaire, inlichtingen of andere staatsgeheime doeleinden. Het is dus belangrijk om te weten welke rol de technologie speelt in vitale infrastructuur of essentiële diensten en hoe afhankelijk deze zijn voor het functioneren ervan. Welke impact heeft uitval of verstoring op de nationale veiligheid en is er een alternatief beschikbaar binnen afzienbare tijd?

Dit vergt voldoende kennis en ruimte voor toezicht en controle op de functionaliteit en veiligheid. In hoeverre is bezit Nederland het vermogen om zelfstandig het functioneren van een toepassing te waarborgen?

Voor vitale functies en militaire of inlichtingencapaciteiten is het belangrijk te weten of Nederland (al dan niet met vertrouwde partners) zelfredzaam kan zijn. Deze vragen zijn ook relevant voor aanbieder van de technologie. Is deze gevestigd in een ander jurisdictie waarvan de desbetreffende wetgeving mogelijke veiligheidsrisico's introduceert? Een verschil in waarden en wetgeving in het vestigingsland kunnen potentiële belangenverstrengelingen met zich meebrengen, en kan de mate van controle en toezicht verzwakken. Het auditen en testen op een statisch moment in tijd kan niet garanderen dat in de loop van de tijd de functionaliteit en veiligheid gewaarborgd blijven.

De veiligheidsdiensten, het ministerie van Defensie, Justitie en Veiligheid, de NCTV, en andere relevante publieke instellingen zullen een risico- en impactanalyse moeten doen van de desbetreffende technologie en de aanbieder op de Nederlandse nationale veiligheidsbelangen. Deze zal bepalen of strategische autonomie al dan niet wenselijk is vanuit een nationaal veiligheidsoogpunt.

4.2.1 Cybersecurity risico's: Brengt de technologie (en aanbieder) unieke veranderingen teweeg aan de cybersecurity risico's voor zowel de overheid als de samenleving?

Bij toepassingen van nieuwe technologieën moet ook worden beoordeeld wat de impact kan zijn op de digitale veiligheid. Dit vergt een cybersecurity risicoanalyse om na te gaan of het vertrouwen in en de controle op de technologie afdoende is. Indien dit het geval is wordt deze iteratie van het doorlopen van de *flowchart* beëindigd; er is geen noodzaak tot verdere zekerstelling van de digitale autonomie. Deze vraag is vooral van belang wanneer het gaat om technologieën die gebruikt worden binnen de vitale infrastructuur of vitale processen[75] of wanneer het gaat om "cybersecurity sleuteltechnologieën" zoals *Artificial Intelligence*, *Big data* en *data analytics*, encryptie, *blockchain*, of kwantumtechnologie.[76]

Daarnaast wordt er bij de beantwoording van deze vraag ook specifiek gekeken naar de aanbieder van de technologie. Met andere woorden: kan de aanbieder een cybersecurity *base-level* aanbieden of introduceert het onacceptabele cybersecurity risico's in vergelijking met andere aanbieders? Heeft de aanbieder tevens een dominante marktpositie en brengt deze positie onacceptabele cybersecurity risico's met zich mee? De vier sub-vragen die vervolgens worden beantwoord aan de hand van 5G en de aanbieder Huawei en dienen ter illustratie.

Voor vele westerse landen ontstond er geleidelijk aan de consensus dat afhankelijkheid van risicovolle "*third-party equipment*" voor 5G een potentiële dreiging kan vormen waarbij vitale infrastructuur en vitale processen op afstand kunnen worden beïnvloed of beëindigd. Op basis van de beoordeling van het *National Cyber Security Centre* van het Verenigd Koninkrijk identificeren we vier vragen die van dienst kunnen zijn bij het bepalen van de 5G risico's voor de telecom waardeketen:

a. Zijn we te afhankelijk van één aanbieder?

Zodra die aanbieder failliet gaat, onder politieke druk komt te staan, zelf getroffen wordt door een groot cybersecurity incident, of doelwit wordt van economische sancties, zal dit gevolgen hebben voor hun (aanbod van) diensten. Hoe afhankelijker je bent van één partij, hoe groter de impact is van mogelijke verstoringen in de levering van een bepaalde dienst. Daarnaast kan een te grote afhankelijkheid van een (buitenlandse) aanbieder ook de kennispositie van Nederland op de lange termijn verslechteren wanneer ook de kennisontwikkeling en innovatie door deze aanbieder wordt vormgegeven. Nationale afhankelijkheid van één partij is vooral risicovol wanneer de dienst wordt

[75] Nederland benoemt bijna 30 vitale processen in verschillende sectoren, zoals energie, ICT, Transport, Drinkwater, etc. Het maakt een onderscheid tussen twee categorieën: c Categorie A vitale processen hebben grotere gevolgen bij uitval dan categorie B vitale processen: categorie A vitale processen hebben grotere gevolgen bij uitval dan categorie B vitale processen. https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

[76] Zie Kennis en Innovatieagenda Veiligheid (2019). Online: https://www.bedrijvenbeleidinbeeld.nl/bouwstenen-bedrijvenbeleid/missiegedreven-innovatiebeleid/sleuteltechnologieen

gebruikt binnen de vitale infrastructuur. Daarnaast ondermijnt afhankelijkheid van één aanbieder de mate van weerbaarheid, omdat de lage verkopersdiversiteit het risico en de impact van storingen of vijandige exploitaties voor de aanbiedende partij zelf vergroot.

b. Zijn er te veel mogelijke kwetsbaarheden aanwezig in de dienst van de aanbieder?

Onvoldoende productiekwaliteit, softwareontwikkeling of kwetsbaarheidsmanagement kan leiden tot systematisch falen of kwetsbaarheden die geëxploiteerd kunnen worden door externe actoren. Zo heeft in 2018 en 2019 het Britse Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board geconcludeerd dat Huawei een te lage '*information assurance'* kan geven voor hun diensten.[77] In vergelijking met andere aanbieders zou Huawei's aanwezigheid in de vitale infrastructuur van het VK een onacceptabel risico kunnen opleveren. Het is in ieder geval essentieel dat een land over de kennis en capaciteiten beschikt om dit onafhankelijk vast te kunnen stellen. Zicht hebben en houden op een (mogelijke) dreiging is net zo belangrijk als te kunnen handelen in reactie op een daadwerkelijk incident.

c. Is er een 'achterdeur' dreiging?

Een 'achterdeur' dreiging wordt opzettelijk in de apparatuur gebouwd door de aanbieder ofwel doorgevoerd door een vijandige actor die toegang heeft tot de hardware of software van de dienst. In vergelijking met andere aanvalsvectoren is het VK van mening dat een achterdeur niet de makkelijkste, meest effectieve of minst risicovol route is om telecom in het VK aan te vallen.[78] De grootste zorg zit met name in de link tussen de aanbieder en een statelijke actor – in dit geval China – en diens intenties jegens Nederland en de EU en haar bondgenoten. Chinese wetgeving, zoals de Chinese National Intelligence Law of Cybersecurity Law, zorgt bij vele landen voor ophef aangezien Beijing direct controle kan uitoefenen op bedrijven zoals Huawei.

d. Is de administratieve toegang van derden tot de diensten en apparatuur een dreiging?

Administratieve toegang tot de netwerken van een dienst kan een significant cyberrisico met zich meebrengen. Deze potentieel ongeoorloofde toegang is vaak een onderdeel van een onderhoudsovereenkomst of apparatuur ondersteuning. Binnen de 5G-context geeft administratieve toegang bijvoorbeeld toegang tot onderdelen van nationale kritieke telecominfrastructuur die tot mogelijke risico's kunnen leiden in de vorm van het grootschalig verstoren of

[77] GOV.UK, 2019, Huawei cyber security evaluation centre oversight board: annual report 2019. Online: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

[78] United Kingdom Department for Digital, Culture, Media & Sport, 2019, UK Telecoms Supply Chain Review Report. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

extraheren van data. Het VK schatte dit risico voor haar eigen netwerken hoog in.[79] Toegang van derden moet nauwlettend gemonitord worden ongeacht de aanbieder.
Uiteindelijk zal een volledige risicoanalyse toegespitst moeten worden op de desbetreffende technologie. Zo kan worden bepaald of zekerstelling van strategische autonomie al dan niet wenselijk is vanuit cybersecurity oogpunt.

5 Noodzaak tot zekerstelling strategische autonomie

U bent aangekomen bij het einde van het eerste gedeelte. Het tweede gedeelte van de *flowchart* kan doorlopen worden als er een noodzaak tot zekerstelling digitale autonomie is vastgesteld. Het antwoord hierop komt voort uit een politiek besluit op grond van de voorgenoemde vraagstukken die in het eerste gedeelte aan bod zijn gekomen:

1 ***Technologische impactbeoordeling****: Is het een sleuteltechnologie die aan de basis ligt van andere technologische innovaties?*
2 ***Economisch belang****: is er open en eerlijke concurrentie en is er een bredere economische afhankelijkheid?*
3 ***Nationaal veiligheidsbelang****: Is Nederland afhankelijk van de technologie om haar nationale veiligheid te waarborgen?*
4 ***Cybersecurity risico****: Brengt de technologie (en aanbieder) unieke veranderingen teweeg aan de cybersecurity risico's voor zowel de overheid als de bredere samenleving?*

Na het vaststellen van de noodzaak komt u in het tweede gedeelte van de *flowchart* terecht. Hierin wordt u geïnformeerd en uitgedaagd om na te denken over bestaande of nieuwe instrumentaria die strategische autonomie kunnen waarborgen. De *flowchart* is beëindigd als er geen noodzaak is vastgesteld.

6 Instrumentarium voor bevorderen strategische autonomie

Na het vaststellen dat er een noodzaak is om de strategische autonomie zeker te stellen, zijn er twee paden te doorlopen: de Nederlandse staat heeft wel of niet de beschikking over instrumentarium (handelingsperspectieven), nationaal dan wel in EU-verband (of samenwerking in met andere vertrouwde partners). De vraag is dan of dit instrumentarium voldoende is om de autonomie waarborgen voor de desbetreffende technologie?

Op grond van het eerste analysedeel is vastgesteld dat er een noodzaak is de strategische autonomie op cybersecurity zeker te stellen. De vraag is dan of dit met het bestaande instrumentarium voldoende kan worden geadresseerd of dat er aanvullende maatregelen moeten worden.

In hoofdstuk 4.2. worden enkele beleidsinstrumenten benoemd die handelingsperspectief bieden om de strategische autonomie in het digitale domein te versterken:

- Informatiepositie,
- Kennisopbouw,
- Investeren in innovatie,

[79] Ibid.

- Opstellen wetgeving en normen,
- Bevorderen certificering en standaarden,
- Uitvaardigen sancties en export-controles,
- Industriepolitiek.

Hierbij moet worden opgemerkt dat het versterken van de informatiepositie een voorwaarden scheppend instrument is. Door te investeren in het opbouwen van een diepgaande en brede informatiepositie over alle relevante aspecten die voortkomen uit de digitale transformatie kan worden bepaald welke maatregelen het gewenste resultaat op kunnen leveren.

De diversiteit van deze instrumenten weerspiegelt de vele manieren om strategische autonomie voor cybersecurity zeker te stellen. Het vereist nauwe samenwerking en een afweging van belangen, capaciteiten en doelstellingen van een scala aan publieke en private partijen.

7 Aanpassen bestaand of ontwikkelen nieuw instrumentatrium

Wanneer bestaande nationale en Europese/internationale handelingsperspectieven ontoereikend zijn, zal er geïnvesteerd moeten worden in het versterken of aanpassen van het beschikbare instrumentarium of nieuwe instrumenten worden ontwikkeld. Het ontwikkelen van een nieuw instrument of het aanpassen van het bestaande instrumentarium volgt uit een afweging tussen de baten (waarborgen van strategische autonomie met een geïdentificeerd instrument en de lasten (ongewenste neveneffecten)).

Een vernieuwd instrumentarium kan consequenties hebben voor de status quo (op macroniveau de staat, economie en samenleving als geheel en op microniveau de prijs, kwaliteit en precedentschepping). Hiertoe worden een aantal controlevragen gesteld:

- Welk effect moet worden bereikt?
- Wordt er een effect op korte of lange termijn nagestreefd?
- Met welke partners (publiek – privaat, nationaal – internationaal)?
- Veroorzaakt het instrument ongewenste neveneffecten?
  - Zou de betreffende dienst, hardware of software, wanneer de buitenlandse partijen worden uitgesloten, duurder worden of op termijn minder goed worden?
  - Belemmert de uitsluiting op de middellange termijn het economisch vermogen van Nederland?
  - Wat betekent de uitsluiting voor de positie van Nederland. Wordt Nederland elders ook van iets uitgesloten?
  - Wat zijn de gevolgen indien Nederland zou ingrijpen (alleen of in EU-verband), voor de diensten van derde landen dan wel hun economische en/ of politieke zaken? Zijn deze consequenties aanvaardbaar?

8 Geen noodzaak tot verdere zekerstelling strategische autonomie

U heeft het tweede gedeelte van de *flowchart* doorlopen en bent op het einde gekomen. Het einde is bereikt omdat u bestaande of nieuwe instrumenten heeft kunnen inzetten om handelingsperspectief te verkrijgen en daarmee de strategische autonomie heeft versterkt.