Nederlandse strategische autonomie en cybersecurity

Paul Timmers

Freddy Dezeure

Januari 2021

Dit onderzoek is uitgevoerd in opdracht van de Cyber Security Raad (CSR)

1 Executive Summary

Toenemende afhankelijkheid van digitale informatiesystemen betekent dat de impact van cyberincidenten op onze samenleving, economie, democratie en fundamentele vrijheden steeds groter wordt. Er duiken ook nieuwe en niet eerder beoordeelde dreigingen op. Cybersecurity wordt tot nog toe veeleer technisch aangepakt en vrijwel niet vanuit de zorg om strategische autonomie en soevereiniteit. Tot 2017 was strategische autonomie, en zeker in het digitale domein[1], vrijwel onbekend terwijl het vandaag *Chefsache* is. Uitdagingen en bedreigingen voor strategische autonomie in cybersecurity zijn te belangrijk om niet vanuit een breed perspectief te bezien en bij de top te beleggen.

Deze studie analyseert strategische autonomie met betrekking tot cybersecurity, zowel in algemene zin als vanuit specifieke cases. De studie geeft ook een aanzet naar een beter begrip van “controle” in deze context. Vanuit de analyse worden observaties geformuleerd die richting geven aan methodes en aanbevelingen. De studie geeft een concreet toetsingskader om digitale strategische autonomie in relatie tot cybersecurity in Nederland op een strategische en tegelijk praktische manier aan te pakken.

De studie bevat een verscheidenheid aan inzichten die voeding tot reflectie en handelen kunnen geven. De voorgestelde methodes zijn getoetst aan de cases. Ze kunnen zonder veel moeite in gebruik genomen worden in de dagelijkse praktijk.

Er zijn in Nederland heel wat aanknopingspunten, structuren en processen aanwezig die toelaten om cybersecurity en digitale strategische autonomie op een permanente, coherente en geïntegreerde manier aan te pakken. Vele ervan zijn echter nog te beperkt toegepast of onvoldoende bekend. Maar er is een goede basis voor een grotere slagkracht.

Een sterkere samenhang van beleid en expliciete prioritering van digitale strategische autonomie is niet alleen wenselijk maar ook noodzakelijk. Bovendien zou het een grote waarde hebben om het reactief handelen te combineren met proactief monitoren en anticiperen. Dit zou ook inhouden om meerdere beleidsterreinen en belangen hecht met elkaar te verbinden, met sturing vanaf het hoogste niveau (Whole-of-Government).

De verschillende departementen zouden op beleids-operationeel niveau hun samenwerking permanent moeten maken. Het herzien van de organisatie en governance in verband met digitale strategische autonomie is een ambitieuze stap. Niettemin, het langere termijnperspectief is verankering in organisatie en governance van de Nederlandse overheid.

Het is op korte termijn haalbaar, en ook hoogst relevant, om de cases uit de studie uit te werken als startpunt van een interdepartementale samenwerking en om de voorgestelde methodes daarbij in de praktijk te brengen. Vele van deze cases komen voort uit concrete triggers die vandaag of in de nabije toekomst met urgentie aan de orde zijn.

Evenzeer is het op korte termijn haalbaar om een aantal concrete actiepunten uit te werken waarmee Nederland binnen de EU-leiderschap kan tonen en impact kan bereiken die de digitale strategische autonomie met betrekking tot cybersecurity bewerkstelligen en bestendigen.

[1] Zie hieronder over terminologie. In dit document wordt mogelijk digitale strategische autonomie gebruikt i.p.v. digitale soevereiniteit.

2 Breder kader en historisch perspectief

2.1 Inleiding

Sinds het jaar 2000 en versneld sinds 2010 is cybersecurity op de agenda gekomen. Cyber incidenten leken niet te stoppen en - zorgwekkend - kritische infrastructuren te bedreigen. Naast criminelen verschenen toenemend staatsactoren op het toneel. Al in 2007 was er een heuse cyber-aanval op Estland, toegeschreven aan Rusland. In Oekraïne werd in 2015 en 2016 een deel van het elektriciteitsnetwerk platgelegd (ook toegeschreven aan Rusland). De grootschalige diefstal van intellectuele eigendom o.m. door de goed-gedocumenteerde APT1 groep[2] noopte Obama ertoe met Xi Jingping een gedragscode af te spreken, zonder veel resultaat. De Mirai Internet of Things aanval in 2017 legde een deel van het Internet plat.

Table 1. Frequency of use of the notion of "sovereignty" as related to the digital (using ProQuest Central).

	Data sovereignty		Technological sovereignty		Digital sovereignty	
	Academic	Other	Academic	Other	Academic	Other
Before 2011	0	23	12	81	0	6
2011–2014	18	794	6	101	2	49
2015–2018	89	2459	20	131	22	239

[3]

Het besef begon door te dringen dat het functioneren van de staat mogelijks fundamenteel bedreigd werd. Ofwel door het platleggen van kritische voorzieningen, ofwel door systematische weglekken van nationale kennis en voortdurende verstoringen (een situatie van 'unpeace'). De voorlopige conclusie was dat reguliere staten hun soevereiniteit onvoldoende konden verdedigen met hun traditionele militair/defensie aanpak van nationale veiligheid en interstatelijk overleg. Kello noemt dat de 'sovereignty gap'[4].

De situatie verergerde echter nog. De ontwikkelingen in Europa gingen steeds verder afstaan van soevereiniteit. Onvoorwaardelijk omarmden en stimuleerden we digitalisering. Een groot succes, vooral voor Amerikaanse en Chinese leveranciers. De cloud markt in Europa is voor twee derde in handen van Amazon, Microsoft, IBM en Google. Sociale media zijn vrijwel volledig Amerikaans. Europese telecom hardware en softwareleveranciers moesten massaal terrein prijsgeven aan Huawei en ZTE. Autonomie van Europese landen wordt nu niet alleen bedreigd door derde staten maar ook door niet-Europese megabedrijven.

Nog meer indicatoren gingen op rood toen kritische Europese technologie in buitenlandse handen viel: ARM ging naar Softbank en daarna naar het Amerikaanse Nvidia, Kuka robots werd verkocht aan het Chinese Midea.

Het verhaal is niet af: fake news en hacking tijdens de Amerikaanse verkiezingen in 2016 en in meerdere Europese landen toonden aan dat cyberdreigingen zich niet langer tot de economie beperkten. Zelfs de democratie wordt bedreigd.

Europa was al aan het wankelen toen het ook nog speelbal werd in het geopolitieke beleid van de VS en China. Europa werd doelwit in oplopende trans-Atlantische spanningen zoals rond NATO en was 'sitting duck' in de oplopende handelsoorlog tussen de VS en China. China's sluipende infiltratie in Europa met haar "Belt and Road" initiatief leidde tot toenemende

[2] Mandiant, 2017, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
[3] Stéphane Couture, http://globalmedia.mit.edu/2020/08/05/the-diverse-meanings-of-digital-sovereignty/
[4] Lucas Kello, The Virtual Weapon and International Order, Yale University Press, 2017

onrust in Brussel. Merkel verklaarde dat het tijd werd dat Europa haar eigen toekomst in handen nam. Macron verzuchtte dat we de soevereiniteit uit handen gegeven hadden aan (telecom) bedrijven[5].

Een systematische analyse laat zien dat tot 2016 strategische autonomie slechts bekend is in het militair/defensie denken in Frankrijk (frappe de force) en economisch/militair denken van India (onafhankelijkheid van Washington, Moskou, en Peking). Maar in de drukketel van internationale spanningen, diepgaande digitalisering gedreven door buitenlandse megabedrijven, en explosief groeiende cyberdreigingen borrelde het besef dat strategische autonomie een bredere interpretatie moest hebben. De Europese Commissie sprak in de herziening van de Cybersecurity Strategie in 2017 over het vermogen om economie, maatschappij en democratie veilig te stellen[6].

Welke beleidsinstrumenten liggen dan op tafel om het tij te keren? De realiteit is dat een doortastend en samenhangend beleid in verband met digitale strategische autonomie er tot recent nauwelijks was in Europa of in Nederland. Een reden daarvoor is natuurlijk dat de dreigingen pas sinds kort actueel werden. Op Europees niveau is er nog een andere reden: soevereiniteit was tot voor kort een taboe. Toen Juncker in zijn *State of the Union* in 2018 verklaarde dat het uur van Europese soevereiniteit gekomen was viel half Europa over hem heen. Zelfs de Europese Verdragen noemen 'soeverein' alleen om te refereren aan militaire bases van de VK in Cyprus. Europa worstelt met 'soevereiniteit' waar anderen zoals de VS en China zonder aarzeling maatregelen nemen verwijzend naar hun nationale veiligheid, zelfbeschikking, territoriale bescherming en ook soevereiniteit in cyberspace claimen.

Europa en ook Nederland moest dus roeien met de riemen die het had – riemen die geen van allen ontworpen waren vanuit het perspectief om soevereiniteit te beschermen en die bovendien vooral gericht waren op bedreiging van kritische infrastructuren zoals elektriciteit, water en transport en op bestrijding van cyber-criminaliteit. Logisch dan dat zonder bindend principe en breed perspectief op de dreigingen het beleid tot nu toe beperkt en onsamenhangend was.

2.2 Strategische autonomie en soevereiniteit

Soevereiniteit wordt algemeen geassocieerd met territorialiteit, grondgebied, jurisdictie, een bevolking, gezag met interne erkenning (interne legitimiteit) en externe erkenning (externe legitimiteit). Om soevereiniteit te bekomen/behouden moet het begrip operationeel worden gemaakt: wanneer en hoe soevereiniteit te realiseren? Dit wordt veelal *strategische autonomie* genoemd, een begrip dat uit het militaire/defensie denken komt maar tegenwoordig gezien wordt als het vermogen om als natie autonoom te kunnen beslissen en handelen aangaande essentiële aspecten van de langere-termijn toekomst in economie, maatschappij en democratie[7].

Vanaf 2016 begonnen de termen strategische autonomie en (digitale) soevereiniteit op te duiken in politieke speeches en beleidsdocumenten. Europese leiders plaatsen strategische autonomie steeds meer op hun agenda. Het begint een *leitmotif* te worden in Europees beleid

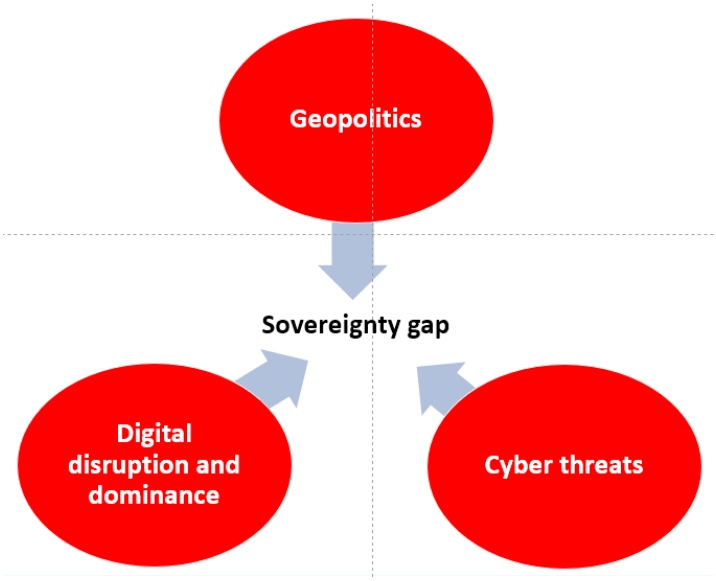
[5] Interview in The Economist, 9 november 2019.
[6] Europese Commissie en Hoge Vertegenwoordiger van de Unie voor Buitenlandse Zaken en Veiligheidsbeleid, 13 september 2017, https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
[7] 'The capabilities and capacities to decide and act upon essential aspects of the longer-term future in the economy, society, and democracy' in Timmers, P., Strategic Autonomy and Cybersecurity, European Institute of Security Studies, mei 2019

voor handel, veiligheid, industrie, buitenlandse investeringen en overnames[8], voor gezondheid (COVID-19) en natuurlijk voor digitaal beleid. In 2020 is het thema naar de top van politieke agenda's gestegen.

Observatie: tot 2017 was de term "strategische autonomie" vrijwel onbekend, terwijl het vandaag de dag *Chefsache* in Europa is. Niettemin is het concrete beleid en de bijbehorende investeringen nog beperkt en drijven we nog op historisch beleid. Weliswaar nam dat cybersecurity wel serieus maar vrijwel niet vanuit zorgen om soevereiniteit. Bovendien is het beleid weinig samenhangend en daardoor minder effectief in het geopolitieke machtsspel.

Observatie: strategische autonomie is een middel om soevereiniteit te realiseren en te behouden. Het bestaat uit het vermogen en de middelen om beslissingen te kunnen nemen en uitvoeren over de langere-termijn toekomst van economie, maatschappij en democratie[9].

Cybersecurity dreigingen kunnen tot een daadwerkelijk risico voor soevereiniteit leiden. Maar cybersecurity dreigingen kunnen zelf ook weer uit voorkomen uit de geopolitieke machtsstrijd of radicale digitale transformatie en digitale marktdominantie (zie diagram). Die krachten kunnen ook op andere wijzen tot risico's voor soevereiniteit leiden en de genoemde 'sovereignty gap' veroorzaken. Deze studie beperk zich echter tot cybersecurity-gerelateerde situaties.



Deze studie analyseert de combinatie van strategische autonomie en cybersecurity. Dat betekent zowel de directe controle over strategische cybersecuritymiddelen en -vermogens alsook strategische autonomie die indirect de cyber-weerbaarheid raakt.

[8] Een aanleiding voor de EU Foreign Direct Investment Regulation was dat Kuka, de Duitse producent van industriële robots in 2017 werd overgenomen door het Chinese bedrijf Midea. Sindsdien heeft Duitsland nationale wetgeving (Kartellamt) nog verder aangescherpt om in te grijpen in geval van dreigende internationale overname van Duitse ondernemingen

[9] 'capabilities and capacities' komt oorspronkelijk uit het militaire begrip van strategische autonomie en omvat zowel *intangibles* zoals kennis, vaardigheden, organisatie processen en procedures, besluitvormingscultuur, politiek, enz. en *tangibles* zoals middelen in de financiële, personele, industriële productie, en anderszins fysieke zin. Voor een defensie-perspectief op strategische autonomie, zie bijv. IFRI, 'France, Germany, and the Quest for European Strategic Autonomy', p.10, https://www.ifri.org/sites/default/files/atoms/files/ndc_141_kempin_kunz_france_germany_european_strategic_autonomy_dec_2017.pdf

2.3 Het digitale veiligheidsrisico

Cybersecuritydreigingen kunnen soevereiniteit ondermijnen. We spreken dan over het hele spectrum van beschikbaarheid, integriteit en confidentialiteit van kritische informatie en diensten met een potentiële impact op essentiële diensten (energie, water, transport, communicatie, gezondheid, het financiële systeem enz.) tot en met het functioneren van de democratische processen, het vertrouwen van de burger in de overheid, de werking van de rechtstaat, de vrijheid van meningsuiting en persvrijheid, betrouwbaarheid van communicatie…

De potentiële dreiging komt hierbij niet enkel meer van vijandige naties maar ook vanuit traditionele partnerlanden en mogelijkerwijze zelfs vanbinnen de eigen staatsstructuur. Recente ontwikkelingen tonen ook aan dat goed georganiseerde criminele bendes (inbegrepen witteboordencriminaliteit en digitale afpersing) een reële en relevante bedreiging zijn geworden.

In toenemende mate is die potentiële ondermijning zodanig dat onze toekomst en die van de samenleving zoals we die kennen daadwerkelijk op het spel kan staan. Dit risico wordt nog versterkt door oplopende geopolitieke spanningen, de toenemende digitale afhankelijkheid en de complexiteit van de digitale infrastructuur.

Vaak wordt ook de term '*digitale soevereiniteit*' gehanteerd. Dit is de digitale dimensie van strategische autonomie.

Onze samenleving, onze economie, ons dagelijks leven en zelfs ons leven zijn steeds meer afhankelijk van informatietechnologie en connectiviteit. Het is positief dat deze digitale transformatie ons ook veel voordelen oplevert. Denk maar aan de grotere economische verstoring door COVID als we niet van thuis uit zouden kunnen werken.

Maar deze toenemende afhankelijkheid brengt ook een verhoogd risico met zich mee. De verbondenheid van steeds complexere systemen stelt ons bloot aan nieuwe kwetsbaarheden. De apparaten waarvan wij afhankelijk zijn worden steeds autonomer en onbeheerd/onhandelbaar. Er ontstaan nieuwe bedreigende actoren, of het nu staten zijn die buiten de traditionele groep van geavanceerde landen vallen of georganiseerde cybermisdaadgroepen. Steeds vaker zijn deze dreigingsgroepen nauw met elkaar verbonden en maken zij gebruik van soortgelijke instrumenten die steeds moeilijker te bestrijden zijn.

Enkele concrete cybersecurity dreigingen voor de soevereiniteit, uitgedrukt in de CIA van information security (Confidentiality, Integrity, Availability) zijn:

Vertrouwelijkheid (Confidentiality)

- Systematisch stelen van intellectuele eigendom van Nederlandse bedrijven[10]
- Misbruik van privégegevens van politici om invloed uit te oefenen op de verkiezingen in de VS in 2016 en in Frankrijk in 2017[11]
- Het bespioneren van Nederland door "bevriende" naties[12]

Integriteit (Integrity)

- Fake news/desinformatie om verkiezingen of stabiliteit in een land te beïnvloeden
- Vervalsing van certificaten, zoals het DigiNotar incident in 2011[13]

[10] Cybersecuritybeeld Nederland CSBN 2019
[11] https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
[12] https://nos.nl/artikel/2356718-vs-bespioneerde-vanuit-denemarken-bondgenoten-waaronder-nederland.html
[13] https://www.onderzoeksraad.nl/nl/page/6749/onderzoek-diginotar-digitale-veiligheid-overheid-moet-sterk-verbeteren

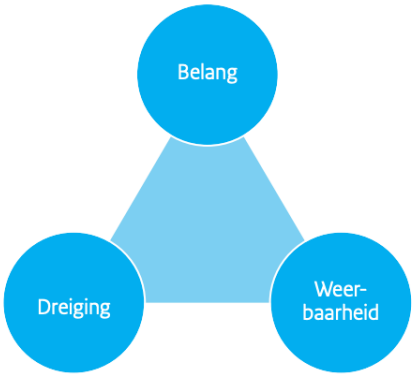
- Het gebruik van “deep fakes” om de identiteit van leidinggevers te vervalsen

Beschikbaarheid (Availability)

- Verstoring van diensten zoals het Oekraïense elektriciteitsnet in 2015-2016[14]
- Verstoring van de media bijv. TV-uitzendingen van TV5Monde in 2015[15]
- Systemische incidenten die het hele financiële stelsel kunnen verstoren, waarvan we een idee hebben gezien de aanvallen tegen de SWIFT-backbone sinds 2017[16]
- Gecoördineerde ransomware-aanvallen die leiden tot grote economische gevolgen zoals gesimuleerd in de Bashe-aanval[17]
- Mogelijke verstoring van het verkiezingssysteem, hetzij elektronisch, hetzij per post

Cyber “insider threats" beginnen ook te verschijnen op het niveau van de staatsleiding. Een voorbeeld is de financiële impact in de 1MDB zaak in Maleisië. Bij informatiemanipulatie kunnen we denken aan het schandaal rond Cambridge Analytica in de politieke manipulatie van opinie van burgers en de beïnvloeding van verkiezingen.

Een moderne aanpak van het cyber veiligheidsrisico houdt ook in dat we alle aspecten van het risico bevatten en benaderen, zoals aangegeven het volgende schema in het Cybersecuritybeeld Nederland.



Figuur 1 Model belang, dreiging en weerbaarheid - bron CSBN rapport

Observatie: onze toenemende afhankelijkheid van informatiesystemen en connectiviteit betekent ook dat de impact van cyberincidenten op onze samenleving, economie, democratie en fundamentele vrijheden steeds groter wordt en dat we in de zorg voor onze bescherming verder moeten kijken dan wat we tot nu toe definiëren als “vitaal” en niet enkel moeten kijken naar de weerbaarheid maar ook de dreiging en de belangen goed moeten inschatten. Dit heeft ook een impact op de vernieuwing van de NIB Richtlijn, de rol van het NCSC en de mogelijke rol van telecomoperatoren in het leveren van een veilig netwerk aan de eindgebruiker. Zie in dit verband ook het CSR Advies inzake het WRR-rapport over cyberweerbaarheid[18] en de CITRIX-evaluatie[19].

[14] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[15] https://www.bbc.com/news/technology-37590375
[16] https://www.swift.com/news-events/news/how-cyber-attackers-cash-out-following-large-scale-heists
[17] Bashe aanval: Wereldwijde infectie door besmettelijke malware, CyRim Report in 2019
[18] https://www.wrr.nl/publicaties/publicaties/2020/06/16/kwetsbaarheid-en-veerkracht
[19] https://www.cybersecurityraad.nl/binaries/CSR_Advies_kabinetsreactie_WRR-rapport_en_Citrix-evaluatie_NED_DEF_tcm107-463191.pdf

2.3.1 Case: Disruptieve ransomware

Het jaar 2019 werd gekenmerkt door het opduiken van grootschalige cyberafpersing incidenten (ransomware). In maart 2019 werd bekend dat het Noorse energie- en aluminiumconcern Hydro besmet was geraakt met ransomware. Hydro, dat ook vestigingen in Nederland heeft, werd door de aanval gedwongen om op verschillende locaties in Europa en de VS de productie stop te zetten en waar mogelijk over te schakelen op handmatige bediening. De Universiteit Maastricht werd op 23 december 2019 ook slachtoffer van een ransomware-aanval. Omdat ook back-up servers geraakt waren, was het herstel complex. De universiteit besloot om losgeld te betalen aan de criminelen om weer toegang te krijgen tot de eigen versleutelde bestanden.

Ransomware aanvallen zijn in 2020 meer en meer in het nieuws. De cyber-criminelen gaan daarbij steeds driester en vernuftiger tewerk. Sommige ransomware varianten zijn specifiek ontwikkeld om industriële controlesystemen aan te vallen. Het wordt steeds moeilijker om de ransomware aanvallen te stoppen en de impact door het versleutelen of lekken van informatie wordt steeds groter. En de criminelen ontzien daarbij geen enkele organisatie, zeker niet de kritische, want daar is de kans op een losgeld nog hoger.

Observatie: de disruptieve en financiële impact van ransomware op onze economie wordt steeds groter en is “landsbreed”. De traditionele werkmethodes van politie en justitie hebben hierop nog steeds weinig of geen vat.

2.3.2 Case: Desinformatie en Fake News

Een veelbeproefde techniek in het strategische machtsspel is het gebruik van desinformatie. Regimewijzigingen werden teweeggebracht en carrières van politici werden gemaakt en gekraakt door zulke manipulaties. Recenter is het gebruik van desinformatie op grote schaal via sociale media. Het probleem werd al uitvoerig gedocumenteerd wat betreft de verkiezingen in de VS in 2016 en Frankrijk in 2017 en ook wat betreft de Brexit. Op Europees vlak is het probleem niet alleen onderkend maar is er een dienst opgericht die desinformatiecampagnes probeert te ontdekken en bestrijden[20]. Ook Nederland wordt het toneel van desinformatiecampagnes, een voorbeeld hiervan is de MH-17 rechtszaak[21]. De database van de EU bevat begin november ’20 bijna 300 gevallen van desinformatie in verband met deze rechtszaak. Ook de COVID-crisis werd gebruikt voor het verspreiden van valse informatie. In de eerste drie maanden na het uitbreken van de crisis heeft Twitter meer dan 3,4 miljoen verdachte accounts gevonden die Coronavirus discussies aangingen. YouTube heeft in diezelfde periode meer dan 100.000 video's met betrekking tot gevaarlijke of misleidende informatie over het coronavirus onderzocht en 15.000 van hen verwijderd.

Er werd op EU-niveau aan een “Code of Practice on Disinformation” vastgelegd[22] die onder andere ondertekend werd door Google, Facebook, Twitter en Mozilla.

Observatie: desinformatie wordt sinds mensenheugenis gebruikt door statelijke actoren om in te grijpen in de stabiliteit van andere landen. Met het gebruik van sociale media als beïnvloedingskanaal werd het een acute uitdaging voor de burgers en respectvolle overheid. Internationale normen en samenwerking met de grote privéspelers zijn een noodzaak.

[20] https://euvsdisinfo.eu/
[21] https://euvsdisinfo.eu/mh17-desinfo-sinds-start-proces/
[22] https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation en gerelateerde initiatieven waar de voorgestelde Digital Services Act op bouwt (zie ook sectie 6.6)

2.3.3 Case: Lawful intercept - surveillance

Er is een lopende discussie over het duaal gebruik van technische middelen voor “lawful interception”. Enerzijds is er het legitieme doel van de veiligheids- en inlichtingendiensten om de samenleving te beschermen tegen criminele en terroristische dreigingen en de technische middelen om inzicht te verwerven in bedoelingen van de tegenstander voordat de schade wordt aangericht, of om de gebeurtenissen achteraf te traceren en toe te schrijven. Het gebruik van deze technische middelen voor legale interceptie is vastgelegd in de wetgeving en wordt bewaakt door toezicht mechanismen die erop gericht zijn het gebruik van deze technologieën te beperken tot wat als "legitiem" wordt beschouwd.

Anderzijds kunnen diezelfde technische middelen ook worden gebruikt voor surveillance in al zijn variaties; om strategisch voordeel te bekomen, om interne oppositie te bewaken, om politieke tegenstanders te lokaliseren en uit te schakelen, om commerciële of concurrentievoordelen te verwerven.

In het standpunt van de Nederlandse regering over sterke encryptie van januari 2016[23] wordt vermeld: “Het kabinet heeft tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie. Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan ten grondslag liggen uitdragen. Ten aanzien van het stimuleren van sterke encryptie zal de Minister van Economische Zaken opvolging geven aan de strekking van het amendement (Kamerstuk 34 300 XIII, nr.10) op de begroting van het Ministerie van Economische Zaken.”

Zonder dieper in te gaan op de verdiensten van de verschillende argumenten, zijn hier enkele aanknopingspunten voor dit dilemma:

- Huawei heeft recent gereageerd op beschuldigingen van ingebouwde achterpoortjes door aan te geven dat zij, net zoals andere leveranciers, legale interceptiefunctionaliteit aanbieden volgens industriestandaards[24]. Het trekt hierbij de aandacht op leveranciers uit andere landen waarbij een gelijkaardige functionaliteit ingebouwd is en waarbij eventueel een gelijkaardige soevereiniteitsdreiging zou kunnen bestaan.
- Vele Corona contact tracing apps beschermen privacy omdat ze gebaseerd zijn op bluetooth nabijheid die binnen de telefoon wordt gehouden. Google en Apple hebben hun besturingssysteem aangepast om dat mogelijk te maken, in samenwerking met de academische wereld. In sommige landen heeft de regering echter gekozen voor een gecentraliseerde aanpak die niet dezelfde bescherming van de privacy biedt.
- De digitale certificaten die in SSL/TLS en code signing worden gebruikt zijn een belangrijke hoeksteen voor cyberveiligheid. Als met een certificaat wordt geknoeid of indien het in de verkeerde handen valt kan dit tot onderschepping van gecodeerd

[23] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015
[24] https://www.huawei.com/en/facts/voices-of-huawei/media-statement-regarding-wsj

verkeer leiden. Sinds 2005 hebben de aanbieders van dergelijke certificaten zich in het CAB Forum[25] georganiseerd. Pogingen om een veilig en transparant register van certificaten te bouwen zijn tot nu toe mislukt omdat sommige landen en leveranciers hiertegen gekant zijn.

- In veel landen worden implementaties van digitale identiteit opgezet en ook door commerciële partijen aangeboden. De meeste systemen zijn gebaseerd op een gecentraliseerd platform die de identiteitseigenaars toelaat om zich te identificeren in toepassingen maar die ook alle identiteitsattributen en de meta-gegevens van de transacties centraliseert (en potentieel blootstelt). Er bestaan ook soevereine, gedecentraliseerde identiteitsimplementaties (zoals IRMA), maar die hebben niet hetzelfde adoptieniveau bereikt.
- Er is veel discussie over offensieve commerciële tools van bedrijven als Hacking Team en FinFisher die beweerden enkel diensten aan rechtshandhavings- en veiligheidsdiensten aan te bieden, maar waarvan is aangetoond dat ze hun producten ook aan repressieve regimes hebben verkocht.
- Ook het gebruik (en het niet openbaar maken) van *zero days* door inlichtingendiensten heeft wereldwijd geleid tot enorme veiligheidsrisico's, zichtbaar in de WannaCry- en NotPetya-incidenten, waarbij werd gebruik gemaakt van de zero day "EternalBlue".

Observatie: wettelijke onderschepping van informatie opent ook het pad naar onwettige onderschepping en creëert daarmee ook een risico voor de nationale soevereiniteit.

2.4 Strategische autonomie benaderingen

Strategische autonomie betekent niet zelfredzaamheid of zelfvoorziening. Dat is niet weggelegd voor Nederland en veelal ook niet voor Europa. Laat staan dat dit wenselijk zou zijn. Er zijn drie realistische benaderingen voor strategische autonomie, en mogelijk in combinatie:

1. De risicomanagement benadering
2. Strategische samenwerking: op strategische '*like-minded*' partners vertrouwen, eventueel gecombineerd met *strategic interdependency*, d.w.z een sterke en wederzijdse afhankelijkheid ten opzichte van de belangrijke '*not like-minded*' partijen.
3. Mondiaal samenwerken aan oplossingen die soevereiniteit respecteren én het wereldwijd gemeenschappelijk belang waarborgen (*global common goods*).

Idealiter wordt soevereiniteit integraal ondersteund, d.w.z. in een slimme combinatie van de drie benaderingen en niet alleen op de digitale dimensie. Dat besef is aan het groeien in Europa sinds 2019: er wordt momenteel gesproken over *materials autonomy* voor de Europese Green deal, *health sovereignty* i.v.m. COVID, *financial sovereignty* getriggerd door de Iran sancties[26], *energy autonomy* t.o.v. Rusland[27], autonomie in batterijen voor elektrische auto's om niet onze auto-industrie aan China te verliezen[28]. De lijst groeit…

Momenteel populair op Europees niveau is om over 'open strategische autonomie' te spreken. Dit is een selectieve combinatie van strategische partnering en strategische afhankelijkheden, dus de tweede benadering zoals hierboven aangegeven. Buitenlandse

[25] https://cabforum.org/
[26] Het gerelateerde financiële instrument is INSTEX, https://instex-europe.com/about-us
[27] Ursula von der Leyen State of the Union september 2020, https://ec.europa.eu/info/sites/info/files/soteu_2020_en.pdf. Zie ook SWP Paper 2019/RP 04, maart 2019, European Strategic Autonomy, https://www.swp-berlin.org/10.18449/2019RP04/#hd-d14204e721
[28] https://ec.europa.eu/growth/industry/policy/european-battery-alliance

bedrijven zijn en blijven in die benadering welkom in de EU, mits ze aan randvoorwaarden voldoen, dus overtuigend *'like-minded'* zijn.

Observatie: een realistische benadering van strategische autonomie voor de EU en Nederland vereist een combinatie van risicomanagement, strategische samenwerkingsverbanden, en bevorderen van wereldwijde gemeenschappelijke belangen.

2.5 Cases

2.5.1 Case: GPS - Galileo

Het Global Positioning System (GPS) satellietnavigatiesysteem is eigendom van de Verenigde Staten en wordt beheerd door hun strijdkrachten. Het GPS-project is in 1973 door het ministerie van Defensie van de VS van start gegaan en in 1978 zijn de eerste satellieten gelanceerd. Civiele toepassingen zijn toegestaan vanaf de jaren tachtig. GPS beschikt over veiligere en nauwkeurigere functies (PPS) die alleen door de VS kunnen worden gebruikt.

China en Rusland hebben autonome concurrerende systemen, BeiDou (eerste lancering in 2000) en GLONASS (eerste lancering in 1982). Het GLONASS-systeem was vele jaren in verval, maar de Russische regering heeft het in 2001 opnieuw tot een prioriteit gemaakt.

De GPS-kwaliteit kan door de Amerikaanse overheid beperkt worden door gebruik te maken van *Selective Availability* (SA). SA werd tijdens de eerste oorlog in Irak in 1991 gebruikt, maar de VS maakte er vervolgens een eind aan omdat de Amerikaanse strijdkrachten ter plaatse niet over voldoende militaire GPS-ontvangers beschikten. SA werd in 1999 gebruikt tegen het Indiase leger in de oorlog tegen Pakistan in Kargil. Als gevolg daarvan besloot India zijn eigen GPS-systeem[29] (IRNSS) te ontwerpen.

In 2000 hebben de VS besloten SA uit te schakelen als reactie op de dreiging van het Galileo-systeem[30] van de EU. In het tweede Irak oorlog in 2003 werd het GPS-systeem door de VS aangepast om een acht keer hogere precisie te bieden aan zijn satellietgeleide raketten.

Het Europese Galileo-programma is in het midden van de jaren negentig door de EU op gang gebracht. Reeds in juni 1994 heeft de Europese Commissie haar ontevredenheid uitgesproken over haar strategische afhankelijkheid van het mondiale positioneringssysteem van de Verenigde Staten. De Europese Commissie verklaarde dat "als Europa niet snel optreedt, de controle over het gehele systeem vanaf het buitenland zal plaatsvinden door een civiele Amerikaanse aanvulling op het militaire GPS-systeem in te voeren. De normen voor de gebruikerseisen en de certificeringsregelingen voor apparatuur worden vastgesteld door degenen die het systeem bezitten en exploiteren. Het resultaat zou een grote afhankelijkheid van Europa zijn van de levering van een strategisch asset voor de toekomst en een slecht perspectief voor de industrie om de enorme markt voor gebruiksapparatuur in te slaan"[31].

In 1998 heeft de Europese Commissie belangrijke bedenkingen geuit met betrekking tot de voortdurende afhankelijkheid van positionerings- en navigatiesystemen van derde landen[32]:

- Er moest voor worden gezorgd dat Europese gebruikers niet gegijzeld worden door mogelijke toekomstige heffingen of vergoedingen die buitensporig lijken: indien een machtspositie of een virtueel monopolie tot stand zou komen, zou het moeilijk zijn om

[29] https://timesofindia.indiatimes.com/home/science/How-Kargil-spurred-India-to-design-own-GPS/articleshow/33254691.cms
[30] https://media.defense.gov/2017/Nov/22/2001847932/-1/-1/0/WP_0012_CONSTANTINE_GPS_AND_GALILEO.PDF
[31] COM (94) 248 definitief
[32] COM (1998) 29 definitief

zich tegen dergelijke heffingen te verzetten en zou het misschien onmogelijk zijn om snel alternatieven te ontwikkelen.

- Het concurrentievermogen van de EU-industrie op deze lucratieve markt zou ernstig worden beperkt als Europa geen gelijke toegang heeft tot de technologische ontwikkelingen in het systeem zelf. Met name de VS laten zien dat zij het strategische voordeel van hun systeem voor militaire positionering (GPS) zullen aanwenden om een dominante positie op de wereldmarkt voor systemen en diensten in te nemen.
- Er zouden ernstige problemen zijn op het gebied van strategische autonomie en veiligheid als de Europese navigatiesystemen buiten de controle van Europa zouden staan.

De eerste operationele Galileo-satelliet is in 2011 gelanceerd. Het systeem is sinds 2019 volledig operationeel, meer dan tien jaar later dan oorspronkelijk gepland. Galileo was oorspronkelijk bedoeld om te worden opgebouwd door een publiek-privaat partnerschap (PPP in een gemeenschappelijke onderneming Galileo) dat twee-derde van de kosten voor de invoering van het systeem wilde laten dragen door een particuliere concessiehouder die het systeem met winst zou exploiteren. De PPP-inspanningen zijn medio 2006 uiteengevallen, toen de indieners van het programma — de Europese Commissie namens de EU en het Europees Ruimteagentschap (ESA) — besloten het programma om te vormen tot een traditionele openbare aanbesteding.

Tijdens de ontwikkeling van het Galileo-systeem is de EU in een conflict met de VS gekomen over het gebruik van frequentiebanden. Met de oorspronkelijke keuze voor de Galileo-frequentieband zouden de VS hun eigen GPS-systeem hinderen bij het blokkeren van het Galileo-systeem. In 2001 hebben de VS ingegrepen om deze keuze te laten wijzigen. In 2004 werd het geschil beslecht, de EU aanvaardde het gebruik van frequentiebanden die toelaten dat de VS het Galileo-systeem kunnen blokkeren zonder dat dit van invloed is op de militaire frequentiebanden van hun eigen GPS-systeem. Als de VS besluiten het civiele gebruik van hun GPS-systeem te blokkeren zal dat ook voor het signaal[33] van Galileo gebeuren, waardoor een deel van de oorspronkelijke doelstelling van Galileo wordt tenietgedaan.

Onlangs is het VK, als gevolg van de Brexit, uitgesloten van de ontwikkeling van het versleutelde systeem van Galileo, dat in 2026 operationeel moet worden. Het VK heeft daarom besloten zich volledig uit het Galileo-systeem terug te trekken, omdat het niet in het belang van het VK zou zijn om de beveiligde elementen van het systeem te gebruiken als het niet volledig bij de ontwikkeling ervan was betrokken. De ontwikkeling van een autonoom satellietnavigatiesysteem wordt momenteel om strategische redenen uitvoerig besproken in het VK.

Observatie: GPS-Galileo is een mooi voorbeeld van een nieuwe technologie/dienst die ontwikkeld werd voor strategische doeleinden maar ook een breder gebruik beoogde (duale technologie). Europa deed een inhaalslag om strategisch onafhankelijk te worden en is daar ook tot op zekere hoogte in geslaagd, na heel wat vallen en opstaan en met veel vertraging. Galileo is een voorbeeld van strategische autonomie en geïntegreerd beleid voor versterking van Europese soevereiniteit[34] in zowel veiligheid als economie.

[33] https://media.defense.gov/2017/Nov/22/2001847932/-1/-1/0/WP_0012_CONSTANTINE_GPS_AND_GALILEO.PDF

[34] Soevereiniteit als doelstelling wordt expliciet genoemd, zie https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system

2.5.2 Een breder perspectief op Europese succesverhalen

Op een aantal terreinen heeft Europa in het verleden industriële kampioenen en infrastructuren van wereldklasse kunnen bouwen, soms zelfs uitgaande van een situatie van achterstand. Voorbeelden van industriële kampioenen zijn:

- Chiptechnologie, micro-elektronica: ASML, Infineon, NXP, IMEC
- 5G netwerkinfrastructuur: Ericsson/Nokia
- IT voor de automobielindustrie: Bosch, Continental. Magneti Marelli daarentegen werd onlangs door FCA verkocht aan Calsonic (JP), gesteund door KKR (VS)
- Informatietechnologie (Thales, Atos, SAP, F-Secure).

Al deze bedrijven profiteren op regelmatige basis van EU- en nationale financiering voor onderzoek en innovatie. Zij weten de weg naar de overheidsfinanciering te vinden en zij zijn ook zeer actief in het input geven aan de agenda voor de financiering van onderzoek. Dit is in feite zowel een sterke als een zwakke factor bij de toewijzing van deze middelen. De procedures voor de vaststelling van de agenda, de oprichting van consortia en de evaluatie van de voorstellen worden sterk beïnvloed door de gevestigde spelers (industrie, universiteiten en onderzoekscentra). De processen hebben een lange aanlooptijd en een administratieve overhead die weinig kleine organisaties zich kunnen veroorloven.

Veel investeringen in R&D gebeuren op dit moment op een losstaande manier van een strategische perspectief en worden ook niet op een samenhangende en gecoördineerde manier gecombineerd met andere, versterkende, maatregelen. Ze leiden in het algemeen niet tot industriële doorbraken noch tot de creatie van nieuwe wereldspelers in Europa.

En toch heeft Europa in het verleden successen geboekt bij gecoördineerde inspanningen om nieuwe industriële kampioenen op te richten in gebieden zoals de luchtvaart (Airbus) en de ruimte (Ariane). Evenzo heeft Europa succes geboekt bij de bouw van infrastructuur van wereldklasse op het gebied van navigatie (Galileo) en aardobservatie (Copernicus). Ook fundamentele deeltjesonderzoek (CERN) is een illustratie.

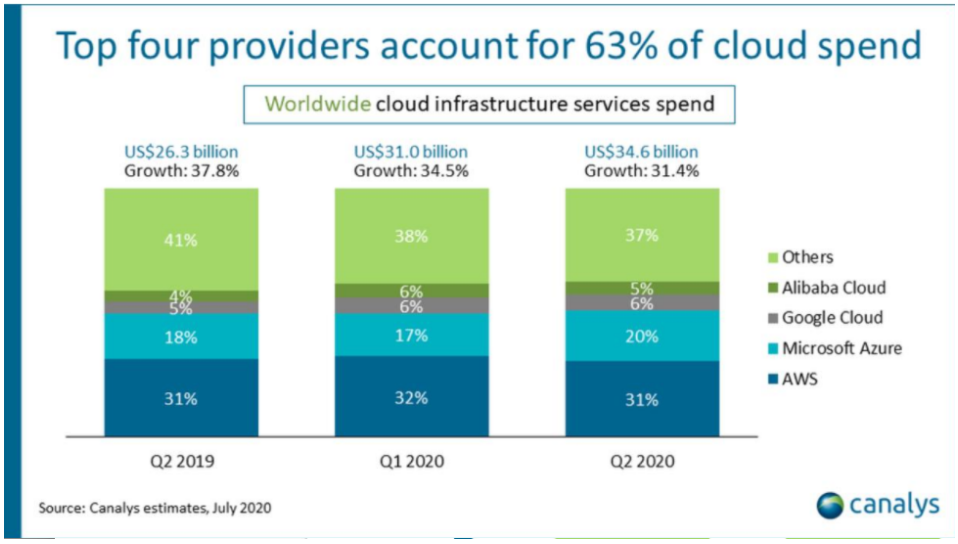
Observatie: Europese succesverhalen uit het verleden (Airbus, Ariane, Galileo, Copernicus) duiden op het belang van strategisch perspectief en een doelgerichte, gecoördineerde en geïntegreerde aanpak wars van subsidiering van middelmaat.

Al deze gevallen hebben een aantal aspecten gemeen. Ze hebben een strategisch perspectief, een duidelijke doelstelling, een volgehouden en aangepast budget, een projectmatige, gefocuste en gecoördineerde aanpak gecombineerd met regelgeving, standaardisatie, overheidsaankopen en een marksituatie die niet zelfregulerend was/is. En ze ondersteunden *excellence* boven middelmaat.

2.5.3 Case: Cloud - Hyperscalers

De huidige markt van cloud aanbieders wordt gedomineerd door vier belangrijke spelers; Amazon, Microsoft, Google en Alibaba. Samen zijn zij goed voor bijna twee derde van de markt, waarbij Amazon en Microsoft samen het leeuwendeel voor hun rekening nemen.

Figuur 2 Wereldwijde marktaandeel cloud aanbieders - bron Canalys



Amazon profiteert nog steeds van het feit dat het als eerste, in 2006, een service van schaalbare infrastructuur voor gedeelde computerverwerking (EC2) en opslag (S3) heeft aangekondigd[35]. De oplossing was het resultaat van een intern project om de ontwikkeling van infrastructuur voor de website van Amazon te harmoniseren en te vergemakkelijken, maar het project was al aan het begin bedoeld als dienst voor derden en werd later AWS.

Microsoft Azure kwam in 2011 op de markt na een proefperiode tussen 2008 en 2011. Microsoft verschoof haar strategie volledig naar cloud services in 2014. Azure en Office 365 profiteren van dezelfde infrastructuur en schaalgrootte.

Het Google Cloud Platform (GCP) groeide uit zijn App Engine, dat in april 2008 werd gelanceerd als een platform als dienst. De App Engine kwam uit trial in 2011 en de naam van GCP wordt gebruikt sinds 2013. GCP draait op dezelfde infrastructuur die Google gebruikt voor zijn eindgebruiker producten zoals Search, Gmail en YouTube.

In de Europese markt volgen lokale spelers op grote afstand (OVHcloud heeft een jaaromzet van 600 miljoen euro)[36].

Figuur 3 Europees marktaandeel cloud aanbieders - bron Synergy Research Group

Cloud Services Leadership – Europe

Rank	Total Europe	UK	Germany	France	Netherlands	Rest of Europe
Leader	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
#3	Google	Google	Google	OVH	Google	Google
#4	IBM	IBM	Deutsche Telekom	Orange	KPN	IBM
#5	Salesforce	Rackspace	IBM	Google	IBM	Salesforce
#6	Deutsche Telekom	Salesforce	Oracle	IBM	Oracle	Swisscom

Based on IaaS, PaaS and hosted private cloud revenues in Q1 2020

Source: Synergy Research Group

[35] https://techtv.mit.edu/videos/16180-opening-keynote-and-keynote-interview-with-jeff-bezos
[36] https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries

Deutsche Telekom en OVHcloud hebben een partnerschap[37] aangekondigd waarbij in het GAIA-X initiatief aangekondigde beginselen worden omgezet in een industrieel productgamma. De aankondiging verwijst naar de naleving van de GDPR-regels, open standaarden, maar ook portabiliteit, privacy van gebruikers en de hoogste beveiligingsnormen. Het valt nog af te wachten of dit initiatief succesvol zal zijn en opkomende technieken als homomorfe encryptie en privacybeschermende gegevensverwerking ook worden opgenomen.

Ondertussen staan de drie koplopers niet stil en zijn begonnen met het aanbieden van oplossingen voor encryptie en privacy-beveiligde berekeningen. Soms bieden ze "hybrid clouds" aan met hun concurrenten[38]. Alle drie hebben nu ook een marktplaats waarin derde partijen hun oplossingen aanbieden. Voor de verkopers blijkt het een efficiënte manier te zijn om nieuwe klanten te bereiken en het platform haalt er voordeel uit zonder inspanning.

Observatie: cloud-hyperscalers is een case waar Europa het initiatief volledig uit handen heeft gegeven en waar de achterstand ten opzichte van de marktleiders niet meer in te halen lijkt. Europa doet pogingen om een cloud *flagship* op te zetten met GAIA-X maar het succes ervan is nog af te wachten.

De sterke punten van GAIA-X lijken te zijn dat een technische architectuur, standaardisatie, wetgeving, economische incentives, investering (10 miljard Euro) en EU-beleid gecombineerd worden. De zwaktes zijn dat het een inhaalactie is die moet opboksen tegen de enorme bestaande investeringen van de hyperscalers met veel nog te verhelderen elementen zoals migratie, hybrid cloud, en deelname van niet-Europese leveranciers. Het laat zien dat een groot infrastructuur initiatief veel consistentie in maatregelen en langere tijd nodig heeft en niet voor een individueel land weggelegd is.

2.6 Beleidsterreinen en -instrumenten tot recent

De meeste EU-beleidsmaatregelen voor cybersecurity die zouden kunnen bijdragen aan digitale strategische autonomie waren tot op heden gedreven vanuit een risicomanagement perspectief en passend binnen het open, globale, liberale markteconomie perspectief. Beide perspectieven worden nu als 'onvoldoende' of als 'naïef' aangemerkt[39]. Strategische autonomie wordt nu toenemend genoemd in beleidsuitspraken en in wetgeving en dit niet alleen in cybersecurity[40].

Observatie: strategische autonomie als drijfveer begint geleidelijk in nieuwe EU-beleidsmaatregelen door te dringen.

[37] https://www.telekom.com/en/media/media-information/archive/t-systems-and-ovhcloud-cooperate-for-gaia-x-607634
[38] https://azure.microsoft.com/en-us/overview/security/
[39] Het meest expliciet waar het de relatie met China betreft, zie Europese Commissie/EEAS, 12 maart 2019, EU-China – A Strategic Outlook, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.
[40] Een voorbeeld is de op 25 november 2020 voorgestelde EU Data Governance Act, een Europese Verordening waarvan de presentatie aangeeft: 'The data governance regulation will ensure access to more data for the EU economy and society and provide for more control for citizens and companies over the data they generate. This will strengthen Europe's digital sovereignty in the area of data.'

3 Actuele situatie

3.1 Actuele cases en thema's

3.1.1 Case: mandaat voor cyber-weerbaarheid van kritische infrastructuren en diensten

De netwerk- en informatiebeveiligingsrichtlijn (NIB Richtlijn, in Nederland omgezet in de WBNI) voor een gemeenschappelijke aanpak van de cyber-weerbaarheid van essentiële infrastructuren diensten is een van de belangrijkste stukken cyberwetgeving in de EU. Het voorstel dateert van 2013, is in 2016 overeengekomen en nu in werking.

Initieel werd deze regelgeving betwist om dat dit zou raken aan nationale veiligheid en dat "nationale veiligheid de exclusieve verantwoordelijkheid van elke lidstaat blijft" (artikel 4 van het Verdrag betreffende de Europese Unie, VEU). De Europese Commissie had de NIB-richtlijn echter voorgesteld op basis van het interne markt artikel 114 van het Verdrag betreffende de Werking van de Europese Unie, VWEU. Op dit gebied heeft de EU een sterk mandaat: lidstaten kunnen niet afwijken van de interne marktbenaderingen, omdat anders het vrije verkeer van mensen, goederen, diensten en kapitaal zou worden belemmerd.

In de huidige NIB-Richtlijn gaat het om cyberbestendigheid, bescherming tegen en herstel van cyberincidenten, en expliciet wordt gesteld dat deze gebaseerd moeten zijn op een risicobeheer aanpak. Het bestrijkt cyberbestendigheid van geselecteerde vitale infrastructuur (zoals elektriciteit, water en vervoer) en digitale infrastructuur/diensten die momenteel slechts drie diensten bestrijkt (cloud, elektronische markten, zoekmachines).

In 2020 is de bezorgdheid over soevereiniteit en strategische autonomie een belangrijke politieke drijfveer geworden. Het is duidelijk dat diverse essentiële digitale infrastructuren en diensten niet worden afgedekt door de van kracht zijnde NIB-Richtlijn en slechts beperkt door andere EU-wetgeving[41]. Voorbeelden zijn:

- sociale media en media in het algemeen, waar de dagelijkse realiteit bestaat in het actief ondermijnen door aanvallen, intrusies, hacken, diefstal en misbruik, bijvoorbeeld door nep-nieuws. De *mainstream* politieke wereld is zeer bezorgd over de voortdurende ondermijning van onze democratie en waarden.
- Industriële en andere fysieke infrastructuur (bijvoorbeeld staalfabrieken waar aanvallen zijn gezien!) die steeds meer gebaseerd is op het internet van de dingen (IoT). IoT-beveiliging is bijna volledig in handen van industriële consortia - waarin veel Chinese deelnemers - maar we worden er wel kritisch van afhankelijk.
- Kritieke intellectuele eigendom (Intellectual Property of IP) voor onze economische toekomst. Cyberdiefstal van IP is een van de grootste dreigingen voor de toekomst van onze landen. Er is echter geen systematische en verplichte bescherming van intellectuele eigendom. Zelfs niet als voorwaarde voor het gebruik van EU O&O-geld.
- De opkomende Europese gegevensruimten, zoals voor industriële, overheidsdiensten, gezondheids- en milieugegevens. Deze gegevensinfrastructuur op Europees niveau is van essentieel belang voor het concurrentievermogen van de Europese industrie of voor de bestrijding van grensoverschrijdende besmettelijke ziekten zoals COVID-19.
- Onderwijs en opleiding, waar digitale platforms in de COVID-tijd onmisbaar zijn geworden terwijl deze grotendeels in handen zijn van niet-EU-aanbieders.

[41] Voor recente voorstellen van de Europese Commissie (eind 2020) zie ook hoofdstuk 6 en i.h.b. sectie 6.6.

Het soevereiniteitsperspectief geeft een heel andere kijk op cyberweerbaarheid. Het wijst erop dat de cyberbescherming van alle cruciale middelen voor onze economie, samenleving en democratie in overweging moet worden genomen.

Op 16 december 2020 stelde de Europese Commissie een herziening van de NIB-richtlijn voor ('NIS2 Directive'), samen met een aanzienlijk aangepaste Cybersecurity Strategie. Alhoewel, de herziene NIB-Richtlijn een breder gebied betreft zijn niet alle bovengenoemde kwetsbaarheden daarin afgedekt. Er zijn dan ook aanzienlijke belemmeringen om dit te doen. Deze zijn gedeeltelijk politiek: is voor deze kwesties het bundelen van de strategische autonomie via een gemeenschappelijk optreden wel de juiste weg? Is marktinterventie door middel van wetgeving noodzakelijk? Heeft de EU wel een mandaat[42] om op te treden, zeker daar waar nationale veiligheid ook een rol speelt[43]?

Wat de juridische belemmeringen betreft: een juridisch anker ('rechtsgrondslag") in de Verdragen is noodzakelijk om Europese wetgeving voor te stellen. Om al deze punten op te nemen moet naast artikel 114 VWEU (de interne markt), een beroep worden gedaan op een hele reeks bijkomende artikelen uit de Verdragen. Voor sommige zaken kost het zelfs grote moeite om een juridisch anker te vinden of is dat er eenvoudigweg niet. Bovendien geeft niet elk artikel een krachtig mandaat voor maatregelen op EU-niveau. De volgende tabel geeft een overzicht.

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

[42] L. Moerel en P.Timmers, 'Reflecties over digitale soevereiniteit Pre-advies Staatsrechtconferentie 2020', 4 december 2020, https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf, en P. Timmers, 'When Sovereignty Leads and Cyber Law Follows', 13 oktober 2020, https://directionsblog.eu/when-sovereignty-leads-and-cyber-law-follows/

[43] Nationale veiligheid is uitgesloten middels artikel 4 van het Verdrag betreffende de Europese Unie

Observatie: vanuit een strategisch autonomie-perspectief moeten alle activa en infrastructuren die cruciaal zijn voor economie, samenleving en democratie cyber-beschermd zijn. Regelgeving op het gebied van cyberbeveiliging is een hulpmiddel om dit te doen. Op EU-niveau bestaat een alomvattende aanpak nog niet, noch op nationaal niveau. Dit vormt een aanzienlijk en urgent strategische autonomie risico.

3.1.2 Case: e-ID, digitale beveiliging, diepe beveiliging

Ondertussen zijn we allemaal gewend aan verschillende vormen van e-ID, van eenvoudige gebruikersnaam en wachtwoord op sociale media tot door de overheid ondersteunde e-ID met een hardware apparaat zoals een smartcard en tweeledige verificatie. Met verschillende e-ID's zijn er ook verschillende elektronische handtekeningen. In de EU-wetgeving (eIDAS-verordening) wordt bepaald dat al deze instrumenten een juridische waarde hebben, zelfs als zijn ze van verschillende sterkte. Een voldoende sterke e-ID die op EU-niveau is aangemeld, kan in de hele EU worden gebruikt voor toegang tot overheidsdiensten. eIDAS heeft ook betrekking op een aantal verwante digitale beveiligings- of "vertrouwde diensten" (tijdstempeling, geregistreerde levering en websiteverificatie).

In de praktijk wordt het gebruik van overheid e-ID's overschaduwd door de e-ID's van de digitale platformreuzen[44]. De acceptatie van overheid e-ID's door de particuliere sector wordt bevorderd maar is niet verplicht door de wetgeving en er is weinig bereikt met deze promotie.

De dominantie van deze oligopolistische particuliere e-ID's vormt een ernstige bedreiging voor de strategische autonomie. E-ID is de sleutel tot deelname aan de digitale samenleving, waar steeds meer mensen leven en werken. Het wordt gekoppeld aan persoonlijke gegevens zoals online gedrag en het persoonlijke en professionele sociale netwerk en kan worden gecombineerd met afgeleide gegevens over voorkeuren, politieke standpunten, geslacht, leeftijd, enz. Er wordt een nauwkeurig beeld van ons opgebouwd, een beeld dat in handen is van een paar bedrijven. Deze profielen worden gebruikt voor commerciële doeleinden. Maar, zoals het schandaal rond Cambridge Analytica aantoont, is het ook de sleutel tot politieke beïnvloeding. Verlies van controle over e-IDs ondermijnt de soevereiniteit.

De identificatie van burgers was vroeger het exclusieve privilege van de overheid. De identificatie van burgers is een staatsbezit en moet zorgvuldig worden beschermd. Nu lopen regeringen echter het risico om door de internetreuzen een zijdelingse rol te spelen in de economie, de maatschappij en zelfs in de democratie. Door de controle over e-ID te verliezen, vrezen burgers en regeringen dat ze de controle over essentiële beslissingen in de economie, de samenleving en de democratie verliezen.

Controle op e-ID is ongetwijfeld een onderdeel van de digitale strategische autonomie. De Europese Commissie overweegt regeringen en burgers bij de herziening van de eIDAS-verordening de mogelijkheid te bieden om de controle over e-ID te behouden en definieert reeds een opstap daarvoor in de recente Digital Markets Act[45]. Dat is misschien niet genoeg. Gebruiksgemak van de e-ID van de overheid of de onafhankelijke e-ID (zoals IRMA) zal onmisbaar zijn. Nederland zou ervoor kunnen zorgen dat een toekomstige eIDAS een grotere kans op succes heeft door actief het gebruiksgemak van soevereine e-ID-oplossingen te bevorderen. In dit verband heeft de CSR ook reeds een Advies verleend[46].

[44] Slechts 15 van de 27 lidstaten bieden e-ID aan onder eIDAS.
[45] Zie ook sectie 6.6
[46] https://www.cybersecurityraad.nl/binaries/CSR_Advies_eID_NED_DEF_tcm107-415886.pdf

Deze studie richt zich op het snijpunt van soevereiniteit met cyberveiligheid. Cyberbeveiliging van e-ID moet inderdaad een bron van zorg zijn gezien de toename van online identiteitsdiefstal. Wat sterke e-ID betreft, hebben veel EU-regeringen nog steeds een voordeel. Toch bewegen internetreuzen zich snel in de richting van sterkere private e-ID met twee-factor-authenticatie en biometrie.

Gezien de link naar e-ID moeten we ook aandacht besteden aan digitale beveiligingsdiensten. Voor deze bedrijven bestaat dezelfde bezorgdheid over de controle door de particuliere sector. Misschien zijn ze nog ernstiger omdat dergelijke diensten steeds dieper in het platform worden geïntegreerd. Bijvoorbeeld, is de *security assurance* van apps op de AppStore van Apple exclusief in handen van Apple, zonder enig toezicht. De veiligheid van Nederlandse DigID-apps (die duidelijk betrekking hebben op het gebruik van een staatsactivum) wordt beoordeeld door een buitenlandse commerciële partij die buiten de controle van een EU-regering valt! Geen wonder dat het cloud-beleid van de EU en GAIA-X[47] de ontvlechting ('*unbundling*') van digitale beveiligingsdiensten specificeren.

Unbundling zou het terugnemen van de soevereine controle vergemakkelijken en zou ook een veelbelovende markt voor digitale beveiliging kunnen openen. Gemeenschappelijke certificering in het kader van de EU CyberAct van 2018 zou belemmeringen in de interne markt van de EU voor dergelijke diensten wegnemen. Ze moeten echter voldoen aan steeds hogere veiligheidsnormen en het hoofd bieden aan toenemende cyberdreigingen.

Voor een concurrerende markt in de EU en in Nederland is het noodzakelijk te investeren in technologieën zoals AI voor inspectie van software, strenge beveiliging voor certificaten, en gedistribueerde beveiligingscontroles. Dit zou ook moeten gebeuren door een sterkere betrokkenheid bij normalisatie, ook in internationale consortia die marktstandaardisatie beogen. Bovendien is het noodzakelijk de marktacceptatie te bevorderen door bewustmaking en overheidsopdrachten voor dergelijke oplossingen op het gebied van cyberveiligheid.

Tot slot leidt de opkomst van een strijd tussen de grote internet- en cloud-spelers die steeds meer security en e-ID in hun portefeuille proberen te integreren door acquisities van internetbeveiligingsbedrijven tot marktverdrukking van de resterende spelers. Dit is op zichzelf een verontrustende ontwikkeling die van nabij dient gevolgd te worden.

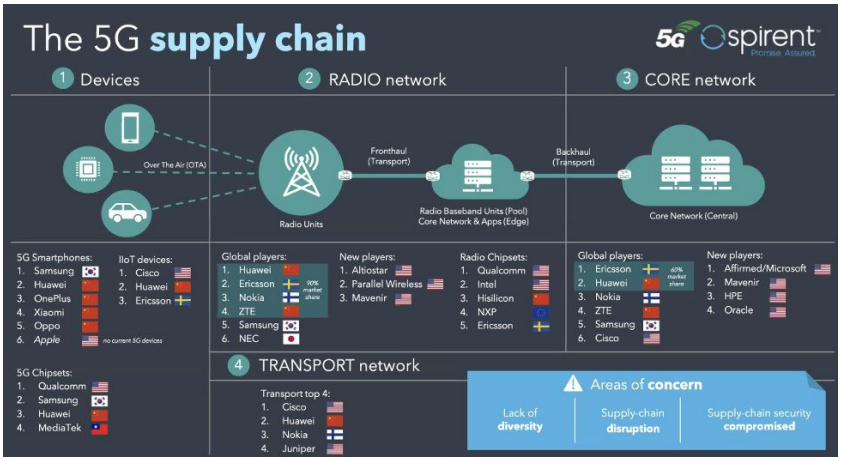
Regeringen die een zekere mate van controle willen herwinnen moeten ook nadenken over *deep security*: geavanceerde digitale beveiligingsservices en -oplossingen, onder meer voor zeer veeleisende toepassingen zoals de kerncommunicatie van de regering, het diplomatieke verkeer, defensie en het leger. Dit zijn nichemarkten, maar ze zijn wel essentieel voor strategische autonomie. *Deep security* kan profiteren van dezelfde triggers die aanzetten tot *unbundling* van vertrouwen- en verzekeringsdiensten. Nederland heeft een historische kracht in *deep security*. Een geïntegreerd beleid hiervoor zou overwogen moeten worden.

Observatie: e-ID en daarmee samenhangende vertrouwensdiensten zijn essentieel voor digitale strategische autonomie, maar glippen steeds meer uit handen van de regeringen. Versterking van de EU-wetgeving kan nuttig zijn, maar volstaat niet. Een slim geïntegreerd beleid kan de regeringen van de EU in staat stellen de controle terug te winnen, veelbelovende markten voor vertrouwensdiensten en, ook voor Nederland, voor '*deep security*' te openen.

[47] GAIA-X is een initiatief uit Duitsland en Frankrijk en is een concretisering van het EU cloud beleid

3.1.3 Case: 5G-beveiliging

In 2017 is de kwestie van de 5G-veiligheid in de telecommunicatiesector wereldwijd snel bovenaan de agenda komen te staan. De aanleiding was een offensief van de regering Trump om bevriende regeringen onder druk te zetten om Huawei uit te sluiten van de nieuwe 5G-contracten. 5G moet de basis digitale infrastructuur van de toekomst worden. De VS voerden aan dat de uitrusting van Huawei niet kon worden vertrouwd omdat de onderneming onder controle zou staan van de Chinese staat. De nationale veiligheid zou worden bedreigd door spionage of een verborgen "*kill switch*". Naast de veiligheid werd bezorgdheid geuit over de afhankelijkheid van China en een mogelijke verstoring van de toeleveringsketen van 5G.



Figuur 4 5G toeleveringsketen - bron Spirent

De Verenigde Staten waren sinds een aantal jaren zeer bezorgd over de diefstal van intellectuele eigendom door China, de voortdurende cyberdreiging van China en de succesvolle economische groei van China zonder dat de communistische dictatuur in sterkte afnam. De VS hadden de beperkingen op de Chinese directe buitenlandse investeringen (FDI) in sleuteltechnologieën zoals halfgeleiders, telecommunicatie, robotica en AI geïntensiveerd. Peter Navarro, directeur van het Witte Huis voor handel en industriebeleid, verklaarde dat de VS anders "geen economische toekomst zouden hebben".

De regeringen van de EU waren gewaarschuwd en bezorgd over de nationale veiligheid, maar waren niet overtuigd door de VS. Zij gaven de voorkeur aan meer objectiviteit, maar dat was moeilijk individueel te bereiken. Ze realiseerden zich dat ze ver verwijderd waren van de 5G-technologieën en -normen en dat 5G uiterst complex is. De Europese Commissie is erin vervolgens in geslaagd alle EU-lidstaten rond de tafel te krijgen om een gezamenlijke aanpak voor risicobeheer te volgen, de 5G Cybersecurity Toolbox[48]. Deze bestaat uit een technische cyberveiligheidsbeoordeling en een politieke beoordeling over de overheid van het land van de leverancier van de apparatuur.

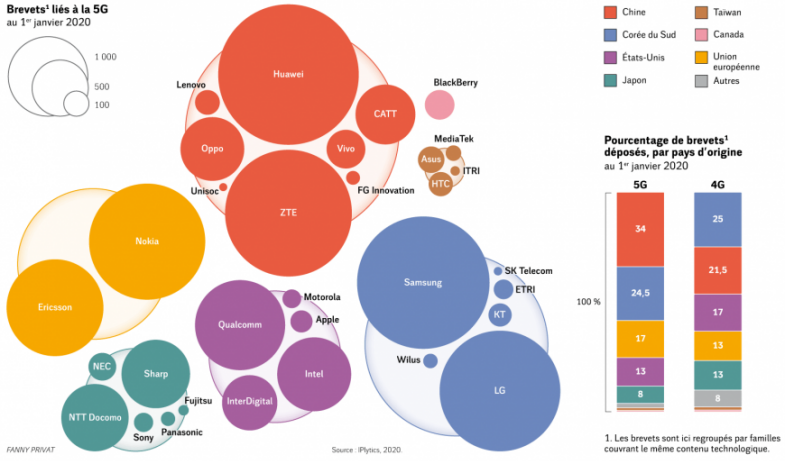
De bezorgdheid over 5G gaat vooral over de nationale veiligheid en raakt het hart van de strategische autonomie en daarmee van soevereiniteit. Echter, nationale veiligheid is expliciet uitgesloten van het mandaat van de EU. Het is dan ook opmerkelijk dat de lidstaten zo'n centrale rol voor de Europese Commissie hebben geaccepteerd om aanbevelingen te formuleren over de veiligheid van de 5G!

[48] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

De 5G-gereedschapskist bood echter nog veel ruimte voor landen om hun eigen routekaart op te stellen, en nog steeds met Huawei in zee te gaan. De Verenigde Staten verminderden dan ook niet de politieke en diplomatieke druk. Als gevolg daarvan besloot een groeiend aantal landen om Huawei uit te sluiten, ook omdat de VS-sancties oplegden aan bedrijven die technologie leveren aan Huawei om onderdelen in 5G te ontwerpen en te produceren en te onderhouden.

Voor de EU speelt het ook dat de twee grootste alternatieve leveranciers, Ericsson en Nokia, marktaandeel aan de Chinese leveranciers Huawei en ZTE aan het verliezen waren. In de jaren 2017-2019 was er veel speculatie over andere maatregelen om alternatieven te versterken en zo de diversiteit van de leveranciers te garanderen zoals een open source 5G met ondersteuning door een '*coalition of the willing*' en de suggestie om Nokia en Ericsson over te nemen met Amerikaanse investeringsfondsen. Recentelijk komt ook een technologisch alternatief in de aandacht: OpenRAN.

Waarom zijn we in deze nogal ongemakkelijke situatie terecht gekomen? Een van de redenen is dat de regeringen in het Westen de 5G-standaardisatie niet in de gaten hebben gehouden. Deze gebeurt vooral in industrie geleide consortia zoals 3GPPP[49]. Hierdoor werd de deur opengezet om de nationale veiligheid niet centraal te stellen in de 5G-architecturen. Er is ook het vermoeden dat de Chinese regering bedrijven als Huawei actief heeft gestuurd en daarmee de veiligheid van de 5G zou kunnen ondermijnen. Veel van de 5G patenten, al zijn die mogelijk niet allemaal erg relevant, zijn inmiddels ook in handen van Chinese bedrijven.



Figuur 5 5G Patenten - bron Le Monde

Een andere reden, die vaak in de VS wordt genoemd, is dat de Amerikaanse regering sinds ongeveer 2000 de sector van de telecommunicatieapparatuur negeerde en daarmee controle kwijtspeelde. In de EU werd de ontwikkeling van de netwerken van de volgende generatie ondersteund door de kaderprogramma's voor O&O van de EU, waarvan het motto destijds was: "Wij staan open voor de wereld". Huawei was een belangrijke deelnemer aan de door de EU geleide 5G O&O-consortia. Over het algemeen wordt de samenwerking met China op het gebied van O&O en het bedrijfsleven al vele jaren als positief beschouwd. Maar tegenwoordig wordt China door velen in de EU beschouwd als een "systemische concurrent". De vrije mondiale marktbenadering uit het verleden wordt als "naïef" aangemerkt.

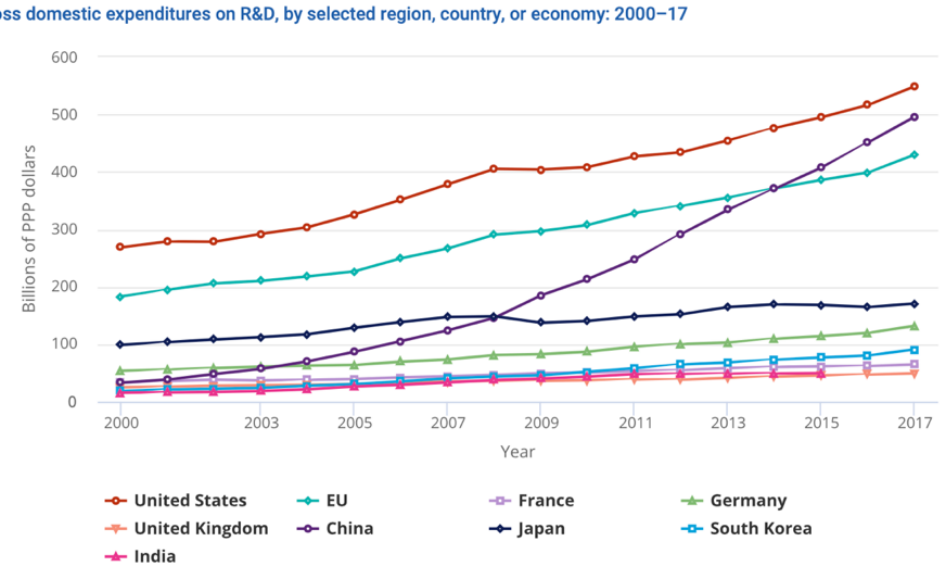
[49] Paul Timmers, Geopolitics of Standardization, 9 april 2020, https://directionsblog.eu/the-geopolitics-of-standardisation/

Observatie: De veiligheid van de 5G is een aanjager van digitale strategische autonomie. De aanleiding was de druk van de VS, maar belangrijke zwakke signalen die ook aanleiding tot bezorgdheid hadden moeten geven (geen belangstelling van de overheid voor een essentiële toekomstige digitale infrastructuur, toenemende teleurstelling over het beleid van China). Het antwoord op de 5G-veiligheidsuitdaging toont aan dat men bereid is verschillende beleidsinstrumenten te mobiliseren (cyberbeveiligingscertificering, O&O, normalisatie, aanbestedingsbeleid), maar ook dat er nog steeds geen sprake is van een volledig coherente en solide strategie op EU- en nationaal niveau. In de tussentijd kan nieuwe technologie het veld verstoren. Het veiligheidsverhaal van de 5G dreigt zichzelf te herhalen voor een andere toekomstige digitale infrastructuur, het internet van de dingen (Internet of Things, IoT).

3.2 Onderzoek en ontwikkeling

3.2.1 Geografisch perspectief

De uitgaven voor O&O zijn de afgelopen jaren gestaag gegroeid, waarbij de EU een vergelijkbare curve volgt als de VS, en China sneller groeit in absolute waarde dan zowel de VS als de EU[50].

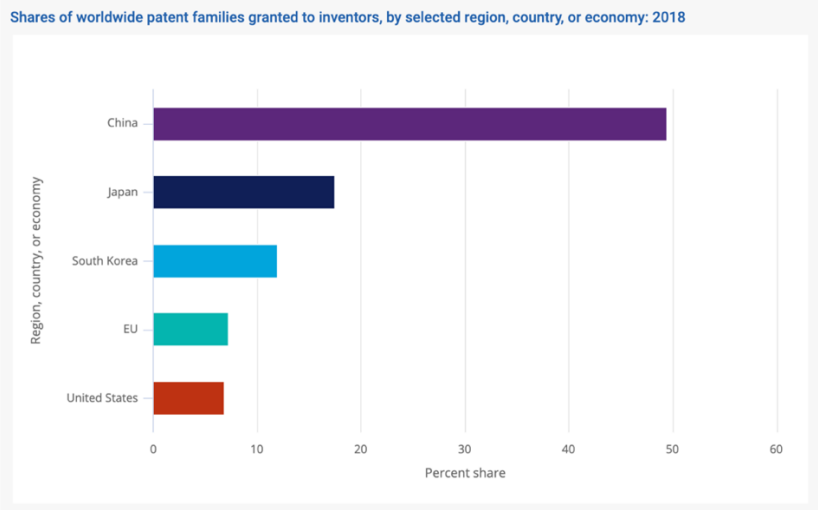


Figuur 6 Uitgaven voor O&O - bron National Science Board

De onderzoeks-financiering vergelijkend met het bbp (onderzoeks-intensiteit), laat zien dat de EU (2% in 2018) achterblijft op de VS (2,8%) maar ongeveer evenveel investeert als China (2.1%). Ook Nederland zit op 2.1%[51]. De koploper is Israël met bijna 5%.

Een heel ander beeld lijkt te worden gegeven bij de statistieken van octrooifamilies per regio. Hier lopen de VS en de EU duidelijk achter op Azië. China is met name verantwoordelijk voor 50% van de octrooifamilies die in 2018 zijn verleend.

[50] https://ncses.nsf.gov/pubs/nsb20201
[51] https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm



Figuur 7 Octrooifamilies per regio - bron National Science Board

Uit gesprekken met academici en ondernemers volgen een aantal aandachtspunten. Er werd aangegeven dat de budgetten voor wetenschappelijk onderzoek op EU en nationaal niveau in voldoende mate aanwezig zijn. Maar er wordt ook gewezen op een aantal verschillen in vergelijking met de VS:

- Programma prioriteiten worden bepaald in meerjarige cycli en zijn niet agile genoeg
- Hoge mate van bureaucratie in de selectie van projecten en de opvolging ervan
- Gebrek aan excellence en te veel compromissen bij de financiering van O&O
- Gebrek aan directe verbinding met productontwikkeling bij de financiering van R&D

De EU is goed in het investeren in fundamenteel onderzoek, veel minder in het ondersteunen van innovatie. Grote industriële bedrijven die aan EU-financiering deelnemen, doen dat niet omdat ze nieuwe producten willen ontwikkelen maar om kosten te dekken en nieuwe werknemers op te leiden. In plaats van deel te nemen aan de modernste onderzoeks- en innovaties, geven de grote Europese industriële bedrijven er de voorkeur aan om technologie aan te kopen of te verwerven via M&A.

EU-financiering wordt te zeer uitgesmeerd/herverdeeld op basis van compromissen en rekening houdende met gevestigde belangen. Er is weinig plaats voor disruptie, de agenda en de verdeling wordt bepaald door gevestigde spelers.

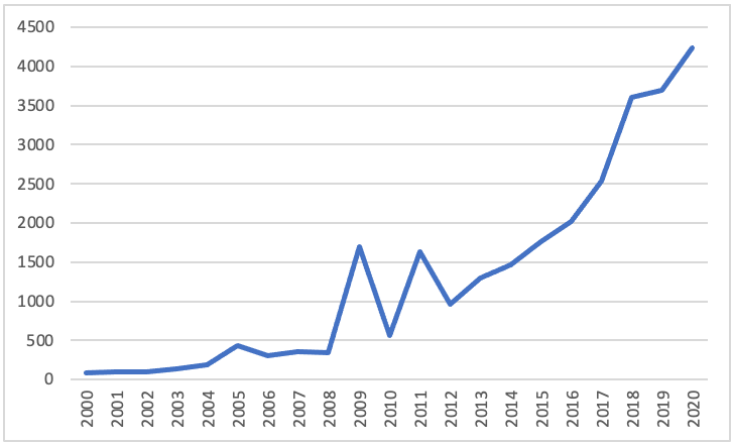
Observatie: qua onderzoeks-intensiteit houden Europa en Nederland gelijke tred met China en lopen wat achter ten opzichte van de VS. De VS en China zijn wel efficiënter in het omzetten van onderzoek naar innovatie.

3.2.2 Case: O&O in homomorfe encryptie en differentiële privacy

In deze case wordt een specifiek domein wat diepgaander geanalyseerd, namelijk homomorfe encryptie en veilige (privacy-bewarende) computerverwerking. Sterke encryptie als middel om de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie te waarborgen is een belangrijke doelstelling van de Nederlandse overheid en deze, weliswaar erg specifieke sleuteltechnologieën, zouden in de toekomst een belangrijke bijdrage kunnen leveren.

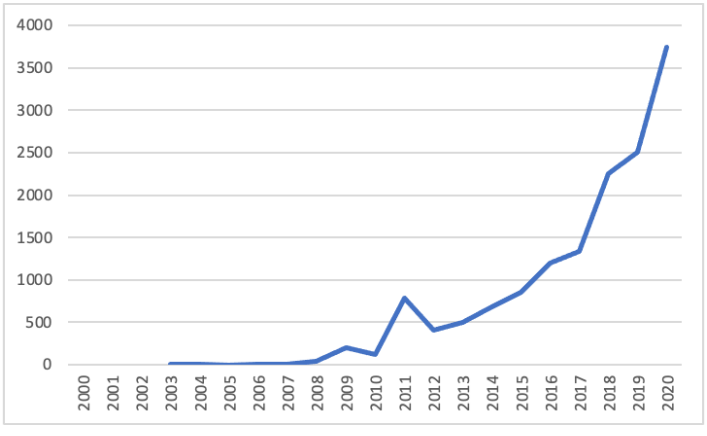
Homomorfe encryptie is een vorm van versleuteling die toestaat om berekeningen op gecodeerde gegevens uit te voeren zonder deze te ontsleutelen. Homomorfe encryptie kan

voor opslag en verwerking worden gebruikt waarbij de privacy wordt gewaarborgd. Hierdoor kunnen gegevens worden gecodeerd en uitbesteed aan commerciële cloud omgevingen voor verwerking, en dat terwijl ze versleuteld blijven. De uitdaging werd in 1978 voor het eerst gesuggereerd. Meer dan 30 jaar was het onduidelijk of er een oplossing gevonden kon worden. De wetenschappelijke basis voor de wiskundige oplossingen voor homomorfe encryptie is in de VS gelegd door Craig Gentry (Stanford, nu IBM), Marten van Dijk (thans bij het CWI in Nederland), Shai Halevi en Vinod Vaikuntanathn. Ook Shafi Goldwasser (tweevoudig winnaar van de Gödel-prijs en ook winnaar van de Turing-prijs) leverde grote bijdragen. Het volgende plaatje toont duidelijk de sprong in de publicaties in 2009 en de gestage toename van het aantal publicaties in de afgelopen jaren.



Figuur 8 Wetenschappelijke publicaties homorfische encryptie - bron Dimensions

Differentiële privacy is een systeem om informatie over een dataset te delen door de patronen van groepen binnen de dataset te beschrijven terwijl de specifieke informatie over individuen in de dataset geheim blijft. In 2006 werden eerste technische oplossingen voorgesteld. Fundamenteel onderzoek over differentiële privacy[52] werd uitgevoerd door Cynthia Dwork (Microsoft), Frank McSherry (Microsoft), Kobbi Nissim (Ben-Gurion Universiteit) en Adam Smith (Weizmann Institute). De groei van publicaties over differentiële privacy volgt een soortgelijke curve als die over homomorfe encryptie.



Figuur 9 Wetenschappelijke publicacties "Differential Privacy" - bron Dimensions

[52] https://link.springer.com/chapter/10.1007%2F11681878_14

DARPA en IARPA hebben al sinds 2011 financieringsprogramma's voor homomorfe encryptie en privacy veilige gegevensverwerking opgezet, PROCEED[53], SPAR[54], BRANDEIS[55] en HECTOR[56]. Het Mission Assurance programma van MITRE financierde ook zulk onderzoek in dezelfde periode, bijvoorbeeld het DataStorm-project. NIST heeft ook onderzoek op dit gebied gefinancierd (PEC-project) en ook de NSF financierde onderzoek.

De eerste door de EU gefinancierde projecten in verband met homomorfe encryptie en differentiële privacy zijn in 2014 (programma Horizon 2020), van start gegaan. Sinds 2015 is meer dan 100 miljoen euro EU-geld geïnvesteerd in projecten voor homomorfe encryptie en ongeveer 20 miljoen euro in projecten die verband houden met differentiële privacy.

Deze substantiële EU O&O-financiering heeft (nog) niet geleid tot een sterke startups op dit gebied in Europa. Bijna alle onderzoeksgelden zijn gevloeid naar universiteiten, publieke onderzoeksinstellingen (TNO, CWI, CNRS, INRIA) en grote industriële groepen (Thales, NXP, IBM, Atos, Orange, Philips).

Er zijn in Nederland een aantal academische expertisecentra die op het gebied van encryptie kunnen meepraten op wereldniveau (CWI, Radboud Universiteit, TU Delft, TU Eindhoven). Op industrieel vlak is de situatie minder rooskleurig. Expertise werd afgebouwd (Philips, NXP) en nieuwe veelbelovende startups zijn er in dit specifieke domein in Nederland niet opgestart.

Uit deze gevallen kan worden opgemaakt dat de VS twee jaar na de publicatie van de haalbaarheid van de technische concepten in 2009 in staat was onderzoeksgelden naar homomorfe encryptie te sluizen. De EU volgde pas drie jaar later in 2014-2015 maar zonder veel omzetting in industriële producten en groei.

Observatie: Europa is niet goed in staat om snel in te spelen op nieuwe wetenschappelijke domeinen en om onderzoeks-investeringen om te zetten in innovatie.

3.2.3 Academische expertise ter validatie van sleuteltechnologieën

Nederland (en zelfs de EU) kan onmogelijk de industriële capaciteit opbouwen in alle sleutel technologieën die van belang zijn voor cyber veiligheid. We moeten ervan uit gaan dat we ook in de toekomst technologische oplossingen en diensten zullen betrekken van bedrijven uit derde landen. Controle en autonomie in de strikte zin is in dat geval moeilijk te verwezenlijken.

Om de doelstellingen van risico mitigatie te bereiken zal het daarom noodzakelijk zijn om in sommige gevallen op een onafhankelijke en competente manier de geclaimde functionaliteit van technische oplossingen te valideren en te certifiëren. De nieuwe rol van ENISA[57] kan hierin ook ondersteunend werken.

Om een voorbeeld te geven in het domein van encryptie en privacy, indien een cloud-provider aangeeft dat ze de gegevens bewaren op een manier die totale privacy garandeert en dat zelf de aanbieder de sleutels tot de gegevens niet heeft dan zou dat in situaties van strategisch belang (maar waarschijnlijk ook in een bredere context) moeten kunnen gevalideerd worden.

[53] https://www.darpa.mil/program/programming-computation-on-encrypted-data
[54] https://www.forbes.com/sites/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/#23eb92287613
[55] https://www.darpa.mil/news-events/2015-03-11
[56] https://www.iarpa.gov/index.php/research-programs/hector
[57] Europese cybersecurity agentschap, met vernieuwd mandaat: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

Een diepgaand inzicht in sleuteltechnologie is noodzakelijk om de doeltreffendheid ervan onafhankelijk te kunnen valideren en om cryptografische achterdeuren te voorkomen, zoals in het verleden gebeurd is bij de "elliptic curve random generators"[58] die in veel beveiligingsproducten zijn geïntegreerd.

Observatie: Indien de academische expertise aanwezig is kan die ingeroepen worden om de "controle op de controleurs" van sleuteltechnologieën te verwezenlijken. Op voorwaarde dat daarvoor de processen bestaan, de budgetten beschikbaar zijn en de onafhankelijkheid kan gegarandeerd worden.

3.2.4 Private sponsoring van academisch onderzoek

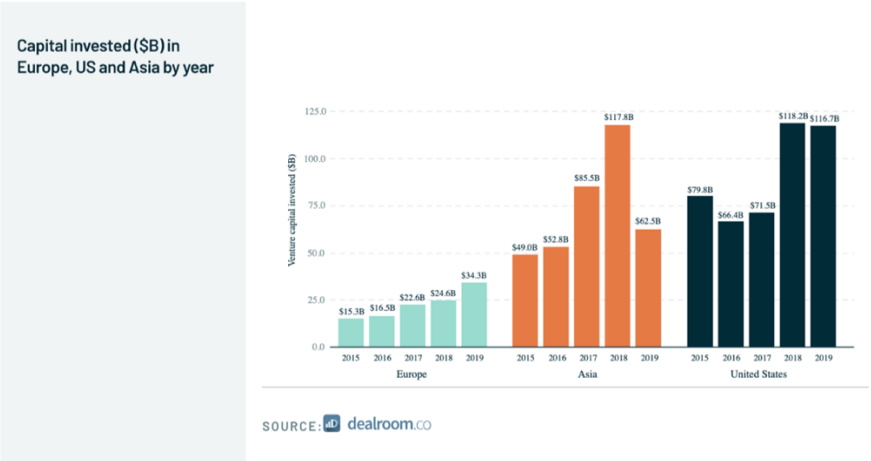
De uitgaven voor onderzoek in de EU gebeuren voor 66% in de privésector, voor 22% in de academische onderzoeksinstellingen en voor 11% binnen de overheid. In Nederland ligt het aandeel van bedrijven wat lager en van universiteiten wat hoger (gegevens van 2017)[59]. Van de onderzoeksgelden binnen de Nederlandse universiteiten komt €300 miljoen van het bedrijfsleven op een totaal van €1770 miljoen, dus 17%[60].

Private sponsoring van academisch onderzoek lijkt dus relatief weinig belangrijk. Niettemin geeft dit geen zicht op de invloed van het bedrijfsleven, laat staan van buitenlandse bedrijven, op strategische autonomie via dit soort sponsoring en ook geen zicht op de mogelijke invloed van vreemde mogendheden. Waar het sleuteltechnologieën betreft is een beter inzicht wenselijk[61].

3.3 R&D en opstartfinanciering (Business Angels, Seed, VC, Private Equity)

3.3.1 Geografisch perspectief

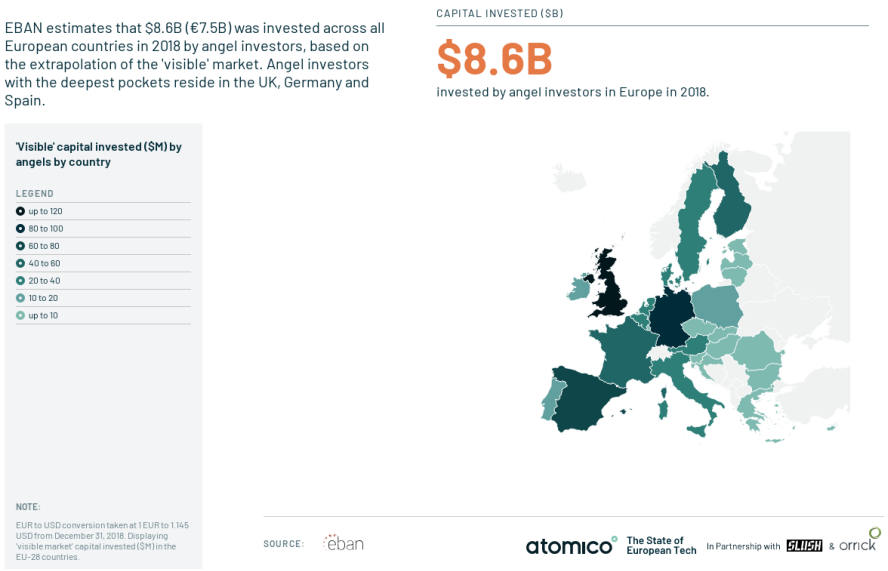
In 2019 is het volume van particuliere risico investeringen in startende Europese bedrijven met 40% gestegen tot meer dan 34 miljard USD. In dezelfde periode bleven de investeringen in de VS stabiel, op ongeveer 118 miljard USD[62], meer dan drie keer zo hoog als in de EU. De investeringen in Azië zijn in 2019 aanzienlijk gedaald.



Figuur 10 Risico investeringen in startups - bron Dealroom

[58] https://en.wikipedia.org/wiki/Dual_EC_DRBG
[59] Eurostat, https://ec.europa.eu/eurostat/documents/2995521/9483597/9-10012019-AP-EN.pdf/856ce1d3-b8a8-4fa6-bf00-a8ded6dd1cc1
[60] Rathenau instituut, https://www.rathenau.nl/nl/vitale-kennisecosystemen/financiering-van-onderzoek-aan-universiteiten
[61] We denken aan sleuteltechnologieën zoals quantum-computing of in het algemeen de aanwezigheid van China in Nederlands academisch onderzoek (via bedrijven als Huawei, of via samenwerkingsverbanden met Chinese universiteiten)
[62] https://2019.stateofeuropeantech.com/chapter/key-findings/

Opvallend is dat in 2018 in Europa 8,6 miljard USD door Angel-investeerders werd geïnvesteerd.



Figuur 11 Investeringen door Business Angels in 2018 - bron EBAN

De top Business Angel beleggers (met uitzondering van 3) in de EU zijn oprichters die eerder een exit realiseerden. Enkele voorbeelden:

- Xavier Niel (Free Mobile en Worldnet), met 54 investeringen in 2015-2018
- Pierre Kosciusko-Morizet (PriceMinister), met 23 investeringen
- Taavet Hinrikus (TransferWise), met 22 investeringen

Dit maakt deel uit van een meer algemene trend waarbij voormalige oprichters met een succesvolle uitstap belangrijke investeerders in een vroeg stadium worden. Bijkomende voorbeelden zijn:

- Daniel Ek (Spotify) die 1 miljard EUR wil investeren in beginnende[63] deeptech-bedrijven;
- Niklas Zennström (Skype), die in 2011 Atomico (https://www.atomico.com/) heeft gecreëerd en oa heeft geïnvesteerd in Rovio (Angry Birds), dat in 2018 IPO realiseerde,
- Jaan Tallin (Skype), die Ambient Sound Investments (https://asi.ee/) heeft gestart,
- Illka Paananen die na de verkoop van Supercell aan Tencent Holdings de Illusian Group Oy als investeringsvehikel oprichtte en onlangs in n8n en Hopin investeerde,
- Oliver Samwer (Rocket Internet), heeft met Global Founders Capital reeds in meer dan 400 startups geïnvesteerd.

Hoewel deze ontwikkelingen in de EU een positieve trend laten zien, zijn er nog steeds belangrijke verschillen tussen de EU en de VS. Investeringen bij het opstarten zijn in de VS gemakkelijker, vooral als de onderneming geen of weinig aantoonbare inkomsten heeft. Het is niet ongebruikelijk dat een startende onderneming in Europa met 100 durfkapitalisten moet praten om financiering in een vroeg stadium te vinden, indien ze nog geen substantiële en voorspelbare ARR hebben en ook omdat ze bang zijn om het eigen vermogen van hun stichters te verwateren. Het investeringsklimaat in de VS is in ieder geval veel meer gericht op groei dan op winst.

[63] https://techcrunch.com/2020/09/24/spotify-ceo-daniel-ek-pledges-1bn-of-his-wealth-to-back-deeptech-startups-from-europe/

In de volgende tabellen kan men ook zien dat de transactieomvang in de VS gemiddeld met een factor 2 groter is dan in de EU en dat de waardering vóór het geld van bedrijven aanzienlijk hoger is en tijdens de levensduur van de bedrijven toeneemt.

	VS	EU
Angel/Seed	0,6-2 miljoen USD	0,9 miljoen Euro
Vroege VC	6 miljoen USD	2,5 miljoen Euro
Late VC	9 miljoen USD	5,1 miljoen Euro

Figuur 12 Transactieomvang - bron Pitchbook

	VS	EU
Angel/Seed	6,5-7,5 miljoen USD	4 miljoen Euro
Vroege VC	30 miljoen USD	8,5 miljoen Euro
Late VC	110 miljoen USD	14,4 miljoen Euro

Figuur 13 Mediane waardering - bron Pitchbook

Als het gaat om latere fase VC-investeringen (D, E-ronde) of private equity investeringen in cyberveiligheid, dan zijn de bedrijven in Europa op weinig bekend terrein. De meeste Europese starters moeten kijken naar de VS, JP (SoftBank) of CN (Tencent), als ze meer dan 100 miljoen euro willen ophalen, om niet over meer dan 1 miljard euro te spreken. In 2019 haalde slechts één EU-onderneming (Northvolt) 1 miljard USD op, en dit gebeurde in een combinatie van een ondernemingsronde (Goldman Sachs, Volkswagen) en schuldfinanciering (Europese Investeringsbank EIB).

De reden lijkt niet het gebrek aan beschikbaar particulier geld in Europa, maar eerder een verschil in risicoacceptatie en misschien een gebrek aan kennis van technologie in de grote private equity fondsen in de EU. De namen van VS private equity fondsen die investeren in cyberbeveiligingsbedrijven zijn KKR, Advent, Insight, Blackstone en Thoma Bravo. In Europa hebben we enkel EQT.

Observatie: In de VS wordt aanzienlijk (drie keer) meer risicokapitaal geïnvesteerd in de technologiesector dan in de EU. Investeringen in startups zijn er makkelijker, vooral als de onderneming geen of weinig aantoonbare inkomsten heeft, de groei is ook sneller. Individuele investeringen hebben een transactieomvang die twee tot drie keer groter is in de VS en ook de waardering (valuation) is twee tot drie keer hoger.

Uit de gesprekken met entrepreneurs volgende als notities:

- dat ze heel wat problemen hebben bij de verkoop van hun producten aan grote ondernemingen en overheden in Europa. Er zijn te veel hindernissen van formele aard (leeftijd van het bedrijf, certificaties, solvabiliteit etc.);
- dat ze geconfronteerd worden met grote uitdagingen in verband met regelgeving. In Europa moet bedrijven (en hun klanten) zich houden aan individuele nationale regelgevingseisen, zelfs op gebieden die in de EU gemeenschappelijk zijn (gegevensbescherming, gezondheid, financiën). Dit leidt tot veel overheadkosten en vertragingen. Het is niet mogelijk om interne kennis te hebben met betrekking tot al deze nationale regelgevingsbeperkingen. De EU-brede erkenning van regelgevende vergunningen zou moeten worden bevorderd. In de VS zijn er veel minder problemen

van deze aard, wat een duidelijk voordeel biedt aan starters op de Amerikaanse markt. De Amerikaanse markt is veel meer een ééngemaakte markt dan de EU;
- er is een groot verschil in investeringscultuur en ecosysteem tussen de VS en Europa. Het bestaan van een "starter ecosysteem" in de VS wordt ervaren als bijzonder aantrekkelijk;
- Zwitserland blijkt een erg actieve startup scene te hebben. Het heeft een zeer gunstige regeling voor oprichters. Er is een gunstige regeling voor stock opties (geen vermogenswinstbelasting) en het aanwerven/ontslaan van werknemers levert ook geen problemen op. Er is wel een probleem in de immigratiewetgeving, waardoor het werven van talent buiten de EEA wordt belemmerd.

Uit de gesprekken met investeerders volgt:
- Risicokapitaal is in grote hoeveelheid beschikbaar, ook in Europa. De COVID-situatie heeft de financieringsbronnen niet opgedroogd, integendeel, investeerders zoeken actief naar een betere opbrengst voor hun beschikbaar kapitaal;
- Er zijn voor de fondsbeheerders geen noemenswaardige wettelijke of regulerende beperkingen die als hinderlijk worden ervaren;
- Er zijn in Europa ondersteunende mechanismen voor risico-investeerders opgezet (Europese Investeringsbank, Europees Investeringsfonds). Die dreigen echter een nadelige impact te krijgen van de Brexit. Aangezien een groot percentage van de investeringsmogelijkheden in cybersecurity in het VK liggen, is dit een reëel probleem voor fondsbeheerders. Aanvaarden van de Europese Investeringsfonds-voorwaarden sluit het fonds uit van investeren in startups in het VK;
- Toegang tot mensen/netwerken is belangrijk als differentiator ten opzichte van de VS. Oprichters met een goede zichtbaarheid en goede connecties zijn zeer succesvol in het aantrekken van middelen en het opstarten/uitbreiden van hun bedrijf, zelfs in Europa. Oprichters zonder een netwerk/zichtbaarheid hebben moeite om geld bijeen te brengen;
- Iedereen vermeldde het belang van het ecosysteem. Maar het grootste nadeel voor oprichters in Europa ten opzichte van de VS is het verschil in het menselijk ecosysteem. In de Amerikaanse hotspots (NYC, Boston, Seattle, SFO) is er een veel hogere concentratie van technologie/technologen en oprichters en een veel grotere bereidheid tot interactie en hulp, zelfs tussen concurrerende starters. In de VS is er een ecosysteem dat uitmuntendheid en concurrentie bevordert, dat zeer gezond is en dat stichters van energie voorziet. Elke Europese stichter zou zes maanden in de VS moet doorbrengen. Er is meer energie, een opener en intensievere netwerking. Dit verschil is een beslissende factor, ook voor investeerders. Het kan de verschillen in de grootte van de tickets en de waardering deels verklaren (naast het verschil in risicocultuur);
- De beschikbaarheid van een aantrekkelijk wettelijk kader voor aandelenopties is heel erg belangrijk. Werknemers moeten op heden investeren om aandelen te verkrijgen in hun bedrijf en vermogenswinst wordt onderworpen aan een zeer complex belastingstelsel in de meeste landen in Europa (ook in Nederland). Daardoor is het moeilijk om talent uit de VS aan te trekken. Relocatie van de bedrijven naar de VS of oprichting van dochterondernemingen om hieraan een oplossing te geven is hiervan een gevolg;

- Gunstige herinvesteringsvoorwaarden voor oprichters die een exit realiseren zou ook de activiteit van Angels in de sector kunnen stimuleren;
- Wetgeving die het flexibel aanwerven/ontslaan van werknemers mogelijk maakt zou erg helpen voor starters;
- Het grootste probleem voor starters is de beschikbaarheid van voldoende kapitaal in een vroeg stadium, wanneer het bedrijf geen ononderbroken en voorspelbare opbrengststroom produceert. Durfinvesteerders in Europa zijn meer risico-avers;
- Intrigerend was de feedback dat risico investeerders in Europa te zacht omgaan met de oprichters na de investering. Ze bieden te veel speelruimte voor (niet-succesvolle) oprichters en wachten te lang voordat ze de schroeven vastdraaien of de stekker uittrekken. De durfinvesteerders in de VS zijn veel minder tolerant voor bedrijven die hun overeengekomen mijlpalen missen;
- Een ander probleem waarmee Europa wordt geconfronteerd, is de moeilijkheid om in een vroeg stadium te slagen in de verkoop aan grote ondernemingen en overheden. Deze zijn zeer terughoudend om te kopen bij ondernemingen die minder dan drie jaar bestaan en geen grote klantenportefeuille kunnen aantonen. Het risico kan gedeeltelijk worden gecompenseerd door gefaciliteerde/bevoorrechte overheidsopdrachten, subsidies of door overheidsinvesteringen in het eigen vermogen van ondernemingen die van strategische waarde worden geacht;
- Europese durfinvesteerders zien een (minderheid)deelname van een in de VS gevestigde durfkapitaalonderneming niet als een probleem voor de autonomie. Minderheidsaandeelhouders hebben geen toegang tot de technologie van de onderneming waarin zij investeren. Bepaalde voorzorgsmaatregelen kunnen worden genomen (of zelfs worden verruimd) in de term sheets voor de deelnames. Dit kan in het geval van sleuteltechnologie bedrijven ook een mogelijke bescherming vormen die door de overheid opgelegd kan worden (40-50% van de waardering);
- Verschillende fondsbeheerders gaven aan de ze een sterke reputatie willen opbouwen/behouden, ook op maatschappelijk vlak, maar de belangrijkste drijfveer blijft het opbouwen van waarde voor de investeerders. Het is geen probleem om een bedrijf aan de VS te verkopen. Als de EU/NL het bedrijf onder controle wil houden, moet de staat bereid zijn om het verschil compenseren.

Observatie: er is geen gebrek aan risicokapitaal in Europa. Maar er is een groot verschil met de VS wat betreft het starters ecosysteem, de risico inschatting van investeerders, een echte ééngemaakte markt (ook wat betreft regulering) en het wettelijk kader wat betreft stock options. Het is in dit verband ook interessant om het voorbeeld van Zwitserland als succesvol startup land te bestuderen.

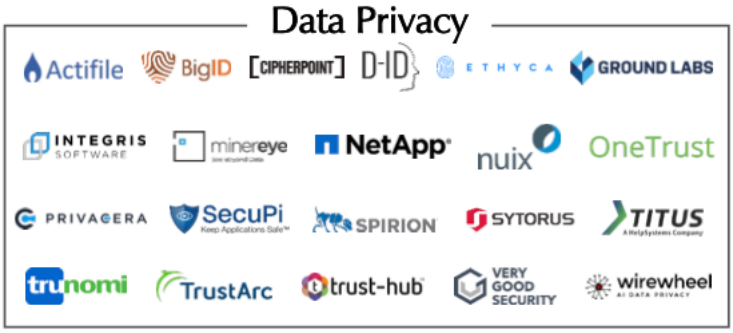
3.3.2 Case: Startups in privacybeschermende technologieën

Om een beter inzicht te krijgen in de opstartdynamiek op specifieke sleutel technologieën neemt deze studie als uitgangspunt technologieën die een belangrijk onderdeel kunnen vormen van de praktische implementatie van de GDPR en van privacy-beveiligde gegevensverwerking o.a. in de cloud.

Behulpzaam in de analyse is de Momentum Cyber[64] CYBERscape inventaris, met name de bedrijven die vermeld staan onder de categorieën "Encryptie" en "Data Privacy".

[64] https://momentumcyber.com/docs/CYBERscape.pdf

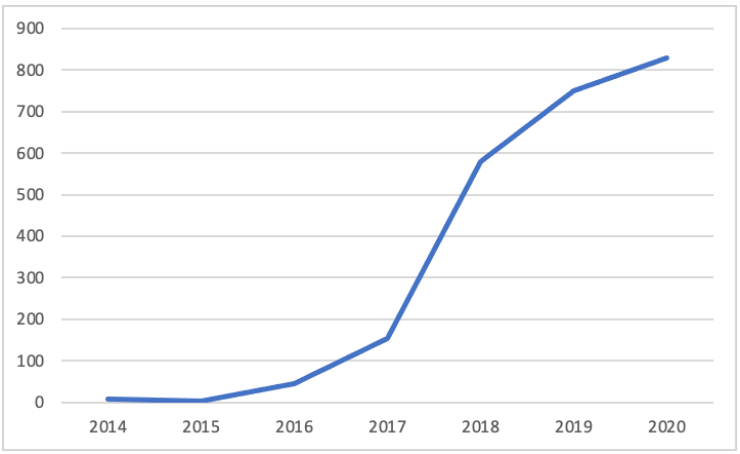
Figuur 14 Startups in encryptie - bron Momentum Cyber



Figuur 15 Startups in Data Privacy - bron Momentum Cyber

Het is natuurlijk zo dat Momentum Cyber een onvolledig en enigszins Amerikaans-centrisch perspectief heeft, maar een analyse van de geselecteerde bedrijven geeft een aantal interessante inzichten. Van de 33 ondernemingen die in het segment “Encryption” van Momentum zijn opgenomen, zijn er slechts 5 in de EU gevestigd, en geen van hen is sinds 2015 opgericht. In de VS zijn sinds 2015 vier nieuwe bedrijven opgericht, die al 75 miljoen dollar hebben opgebracht.

In het geval van “Data Privacy” is slechts 1 van de 21 ondernemingen in de EU gevestigd (in 2013 is opgericht). In de VS werden sinds 2015 7 nieuwe bedrijven opgericht, die 2,6 miljard USD (!) hebben opgehaald. Al deze onlangs gelanceerde Amerikaanse bedrijven verwijzen naar de GDPR in hun positionering. Pro Memory, de GDPR is op 14 april 2016 aangenomen en in mei 2018 van kracht geworden. Het volgende plaatje toont de groei van wetenschappelijke publicaties met "GDPR" in de titel of het abstract.



Figuur 16 GDPR in titel of abstract - bron Dimensions

In twee opeenvolgende jaren (2017 en 2018) kwam de winnaar van de RSA Innovation Sandbox uit deze twee segmenten in de CYBERscape. In 2018 en 2019 was er bijkomend ook nog een "runner-up":

- Homomorfe encryptie: **Enveil** (winnaar in 2017), opgericht door een voormalig medewerker van de NSA en DARPA. Aanvankelijk gefinancierd door Datatribe (VS), gevolgd door een ronde waarin ook In-Q-Tel investeerde. De A-ronde in 2020 werd geleid door een in het Verenigd Koninkrijk gevestigd fonds (C5). Reeds 15 miljoen USD opgehaald.
- Data privacy: **BigID** (winnaar in 2018) heeft al 146 miljoen USD opgehaald. Het opmerkelijke is de investering door SAP in de opeenvolgende rondes. **Fortanix** (runner-up in 2018) heeft al 30 miljoen USD opgehaald, onder andere van Intel.

Niet opgenomen in het Momentum-overzicht zijn **Duality Technologies (VS en IL)**. Deze onderneming is in 2016 opgericht en heeft Shafi Goldwasser als mede-oprichter. Het is gespecialiseerd in homomorfe encryptie en veilige gegevensverwerking. In 2019 was het een runner up in de RSA Innovation Sandbox. Het heeft al 20 miljoen USD opgehaald in Israël (Team8) en de VS (Intel). Ze hebben ook steun van DARPA[65] ontvangen.

Aan de Europese zijde zijn de volgende bedrijven (niet opgenomen door Momentum):

- **Cosmian**, opgericht in 2018 in Parijs. 1,4 miljoen USD opgehaald van oa Angels, Elaia (FR), Blacailloux (FR) en Acecap (VS). Lid van het Confidential Computing Consortium.
- **Decentriq**, opgericht in 2019 in Zürich. Seed ronde van 3,8 miljoen Euro van BToV (DE), Palladin (US) en Atlantic Labs (DE). Lid van het Confidential Computing Consortium.
- **CYSEC** (voorheen ArcaTrust), opgericht in 2019 Lausanne. Haalde 1,5 mlnCHF op in seed in 2020 (investeerder niet openbaar). Lid van het Confidential Computing Consortium. In 2019 ontving de Commissie een subsidie van 50.000 euro uit het EU-mkb-instrument. Ook ondersteund door Innosuisse, Eureka, FIT en ESA.
- **iEXEC**, opgericht in 2017. Haalde 12 miljoen euro op via een ICO.
- **Zama**, opgericht in Parijs in 2019. Initiële financiering door de stichter van Snips (Rand Hindi). A-ronde door Plug and Play (VS). De CTO komt van CryptoExperts, dat 1,85 miljoen Euro aan EU-onderzoeksfinanciering voor homomorfe encryptie heeft ontvangen.
- **Statice**, in 2017 in Berlijn opgericht, heeft seed financiering van Capnamic (DE) en WestTech (VK). Het bedrijf werd gehost door DataPitch (https://datapitch.eu/), een door de EU gefinancierde accelerator.
- **Madana,** in 2017 in Berlijn opgericht, heeft nog geen risicokapitaal opgehaald.
- **Collibra** heeft ook kunnen profiteren van de GDPR-nalevingsvereisten, ook al was de onderneming veel eerder opgericht, in 2009. Heeft in totaal 347 miljoen USD opgehaald. Alle middelen die latere rondes werden aangetrokken waren afkomstig uit de VS. Hun oplossingen zitten niet rechtstreeks in het domein van encryptie of differentiële privacy maar eerder in het buurdomein van gegevensclassificatie.
- **Privatar**, in 2014 in Londen opgericht, al 150 miljoen USD opgehaald van 19 investeerders in EU en VS. Biedt privacybeschermende gegevensoplossingen aan. Privatar en Collibra hebben onlangs een samenwerking aangekondigd. Privatar werkt samen met BigID.

[65] https://www.prnewswire.com/il/news-releases/darpa-contracts-with-duality-technologies-to-develop-privacy-preserving-machine-learning-for-covid-19-research-301096126.html

Observatie: Hoewel er in 2014-2020 aanzienlijk is geïnvesteerd in EU-financiering voor onderzoek op deze twee gebieden en er substantiële wetgeving is aangenomen (GDPR, *privacy shield*), heeft dit niet geleid tot de creatie van recente (na 2015 gecreëerde) wereldspelers in Europa. Ook de gevestigde Europese industriële groepen hebben technisch niet kunnen kapitaliseren op de privacy regulering waarin de EU het voortouw neemt. De twee Europese uitschieters (Collibra en Privatar) zijn al wat langer aan de weg aan het timmeren en zijn succesvol geworden zonder EU-financiering.

In de VS daarentegen zijn er sinds 2015 al minstens 14 ondernemingen op deze twee gebieden opgericht, die reeds aanzienlijke hoeveelheden particuliere investeringen hebben ontvangen. Sommigen komen voort uit onderzoek dat deels door DARPA gefinancierd werd.

3.4 Standaardisatie en marktstandaardisatie

Onlangs berichtte de Financial Times[66] over de Chinese overheersing bij het vaststellen van normen voor gezichtsherkenning en surveillance bij de International Telecommunications Union, een orgaan van de VN. Soortgelijke observaties zijn gedaan over de 5G-standaarden en gerelateerde 5G-beveiliging. ICT-standaardisatie wordt een volgend geopolitiek slagveld.

Standaardisatie zorgt voor breed overeengekomen normen, regels, richtlijnen of specificaties. Deze bieden schaalvoordelen wat leidt tot lagere productiekosten, lagere prijzen en meer keuze voor de consument. Ze kunnen zorgen voor een betere bescherming van fundamentele waarden zoals privacy en gemeenschappelijke goederen zoals het milieu. Standaarden maken verbonden infrastructuren mogelijk die de hele wereld overspannen. Optimale digitale standaardisatie is mondiaal omdat de meeste digitale diensten wereldwijd relevant zijn en functioneren dankzij op standaarden gebaseerde interoperabiliteit.

Regeringen beseffen nu echter dat ze de controle over bepaalde elementen van kritieke digitale infrastructuur te veel aan de industrie hebben overgelaten. Dit zou geen probleem zijn als de private sector zou leveren wat de regeringen willen op het gebied van veiligheid. Maar dit is niet het geval. Standaardisatie zou dus als een kwestie van strategische autonomie moeten worden geherwaardeerd. Maar dan wel zo dat de voordelen van mondiale standaardisering niet verloren gaan[67]. Hoe dan deze uitdaging aan te gaan?[68]

Ten eerste zouden bedrijven en technologie-experts, die vandaag de dag grotendeels nog de standaardisatieprocessen uitvoeren, proactief met regeringen moeten samenwerken en hun zorgen wegnemen. De tijd dat ingenieurs/techneuten en beleidsmakers in de gescheiden werelden leefden is voorgoed voorbij. Beleidsmakers moeten ook meer tijd en middelen investeren in standaardisatie.

Ten tweede zou cybersecurity standaardisatie moeten worden besproken bij de Verenigde Naties (waar Nederland heel actief is). Maatregelen voor het opbouwen van cybervertrouwen worden effectief indien ondersteund door standaarden, zoals gestandaardiseerde informatie-uitwisseling over kwetsbaarheden en beveiligingscertificering van kritieke infrastructuren.

Ten derde zou een rol moeten worden toebedeeld aan belanghebbenden die cyberveiligheidsnormalisatie niet als geopolitiek betwistbaar beschouwen, maar eerder als een zaak van wereldwijde samenwerking. Zij zoeken een goede werking en continuïteit van

[66] https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385
[67] Bildt Rapport, Standardization for EU Competitiveness in the Digital Era, oktober 2019, https://www.etsi.org/images/files/Calling-The-Shots-Standardization-For-The-Digital-Era.pdf
[68] Paul Timmers, Geopolitics of Standardization, 9 april 2020, https://directionsblog.eu/the-geopolitics-of-standardization/

hun kernactiviteiten, zoals gezondheid, productie of zelfs van het wereldwijde internet zelf. Dit mag volgens hen geen harde nationale veiligheid betreffen. Ze kunnen inzetten op open source, open standaarden, gestandaardiseerde cyberbeveiligingsvaardigheden en wereldwijd erkende beveiligingsstandaarden zoals ISO 27000 promoten.

Dergelijke acties zullen Nederlandse en Europese actoren in staat stellen het voortouw te nemen bij een herzien normalisatiebeleid dat zowel geschikt is voor wereldwijde samenwerking als soevereiniteit respecteert[69].

Observatie: overheden in de EU hebben standaardisering lange tijd overgelaten aan de industrie en technologie consortia. Een deel van die industrie wordt mogelijk aangestuurd door hun Chinese overheid. Een ander deel van de industrie, onder meer uit de VS, zet door standaardisatie de commerciële regels naar haar hand. Internationale digitale standaardisering heeft daarmee de facto zeggenschap deels uit handen gegeven over nationale veiligheid en cybersecurity van EU-landen. De oorzaak ligt voor een deel in het liberale markteconomie denken ('de markt is beter in staat beslissingen te nemen dan de overheid') en voor een deel in beperkte capaciteit en vaardigheden bij de overheid (dus gebrek aan strategische autonomie bij de overheid).

3.4.1 Case: Privacybeschermende gegevensverwerking

Deze sleuteltechnologieën voor privacybeschermende gegevensverwerking zijn zeer veelbelovend, maar het blijft een uitdaging indien het bedrijf dat de diensten aanbiedt toegang heeft tot de encryptiesleutels en dus de privacy niet volledig bewaart. Er wordt veel marktstandaardisatie ondernomen door de grote cloud- en netwerkspelers uit de VS en China. Deze prijzen hun oplossing als betrouwbaar aan en proberen hun eigen oplossingen als standaarden te positioneren. Ze gebruiken daartoe verschillende methodes:

- Het ter beschikking stellen in open source van hun algoritmes en softwarebibliotheken
    - Microsoft heeft een homomorfe bibliotheek (Microsoft SEAL[70]) en het Confidential Computing Framework [71] als open bron vrijgegeven.
    - IBM heeft een homomorfe bibliotheek in open source vrijgegeven[72]
    - Google heeft "Private-join-and-compute" in open source[73] vrijgegeven en heeft vertrouwelijke computerverwerking als product vrijgegeven[74].
- Consortia om interoperabiliteit en industriestandaarden vast te leggen:
    - Het Confidential Computing Consortium[75] is opgericht onder de paraplu van de Linux Foundation. De leden zijn onder meer Google, Facebook, Intel, Microsoft, Huawei, ARM/nVidia en ByteDance (TikTok). Aan de Europese kant vinden we Cosmian (FR), Decentriq (CH), Cysec (CH), iExec (FR) en Swisscom (CH). Geen van de grote Europese industriële spelers op dit moment aanwezig;
    - Het Homomorphic Encryption Standardization consortium[76], met deelnemers als Microsoft, Intel, IBM, Google en Alibaba. Langs Europese kant vinden we

[69] De herziene EU Cybersecurity Strategie (16 december 2020) roept de EU op om haar 'betrokkenheid bij en leiderschap op het gebied van internationale normalisatieprocessen te versterken en haar vertegenwoordiging in internationale en Europese normalisatie-instellingen en andere standaardontwikkelingsorganisaties te versterken'.
[70] https://www.microsoft.com/en-us/research/blog/the-microsoft-simple-encrypted-arithmetic-library-goes-open-source/
[71] https://github.com/Microsoft/CCF
[72] https://github.com/homenc/HElib/releases/tag/v1.1.0-beta.0
[73] https://github.com/Google/private-join-and-compute
[74] https://cloud.google.com/confidential-computing
[75] https://confidentialcomputing.io/members/
[76] https://homomorphicencryption.org/

SAP, Mercedes Benz en Crypto Experts. Publieke organisaties en academia nemen deel maar ook hier is de Europese deelname erg beperkt;

Intel speelt een belangrijke rol in dit domein met hun Software Guard Extensions (SGX) die in alle moderne Intel processoren sinds 2015 ingebouwd is. SGX laat toe om beveiligde "enclaves" te creëren. Gegevens zijn altijd versleuteld, zelfs in het geheugen. De encryptie gebeurt door de SGX-hardware en is veel efficiënter dan software alternatieven (Trusted Execution Environment of TEE genaamd). Intel SGX is op dit moment, geruisloos, de facto standaard aan het worden voor confidential computing doordat grote industriële spelers hun aanbiedingen op SGX baseren.

Intel SGX vormt een uitdaging voor de digitale strategische autonomie door de afhankelijkheid van Intel, het gebrek aan controleerbaarheid en het risico dat de controle voor alle versleutelingen ingebakken zit in de hardware en beschikbaar zou kunnen zijn aan Intel. Bovendien zijn er al proof-of-concepts van succesvolle en extreem moeilijk te detecteren malware aanvallen tegen SGX gedocumenteerd[77].

De traditionele technische- en marktvoorsprong van Europese bedrijven op het gebied van versleuteling door *hardware security modules* (HSMs) wordt hierdoor geërodeerd. De situatie werd nog in de hand gewerkt door de conditie die de Europese concurrentie toezichthouder aan Thales stelde bij de overname van Gemalto. Er werd geoordeeld dat door die overname Thales een dominante machtpositie zou verwerven in HSMs. Als conditie voor de overname werd een verkoop van de HSM-dochteronderneming nCipher opgelegd.

Observatie: De grote Amerikaanse ondernemingen hebben reeds aanzienlijk geïnvesteerd in onderzoek en technologie op dit het gebied van "*confidential computing*" en zij organiseren zich om de normen te bepalen door ze via hun "cloud product"-voetafdruk op te leggen, door een aantal van hun instrumenten actief te promoten in open source of via industriële consortia zoals het "Confidential Computing Consortium". Ook de Chinese wereldspelers bepalen mee het speelvlak. Europese industriële partners zouden aan de tafel moeten aanschuiven om het resultaat te beïnvloeden en dit is op het moment niet het geval.

Observatie: Met het op grote schaal uitrollen van Intel's SGX-systeem voor het versleutelen van informatie in de cloud tekent zich opnieuw een dominante situatie af waarin Europese industriële spelers buitenspel gezet worden. Dit is des te pijnlijker omdat Europa de technologie- en marktleider was in HSMs. De situatie werd in de hand gewerkt door een strikte toepassing van het Europese mededingingsbeleid.

Observatie: Er is in Nederland nog nauwelijks industriële capaciteit en expertise aanwezig om aan de behoefte aan *high assurance* oplossingen van de Nederlandse overheid te voldoen. De commerciële markt voor dat soort technologie is onvoldoende om zelf bedruipende economische activiteit te ontplooien. Oplossingen van de grote spelers in de VS hebben inherent beperkingen. Alternatieve oplossingen zijn te verkrijgen vanuit Europese landen (FR, DE, CH). Hoogwaardige en betrouwbare kennis in Nederland om die oplossingen te valideren voor de Nederlandse strategische autonomie dient niettemin aanwezig te zijn in Nederland.

[77] https://arxiv.org/abs/1902.03256

3.5 Aankoopbeleid (publiek en privaat)

Eén van de instrumenten om strategische autonomie te versterken ligt in het aankoopbeleid van de overheid. Een aantal aspecten is mooi uitgewerkt in hoofdstuk 4 van de Beleidsnota Defensie Industrie Strategie van 2018[78]. Deze zijn over te zetten of uit te breiden naar het bredere domein van cyberveiligheid, waarbij de groep van relevante departementen ook wordt uitgebreid van Defensie, EZK en BZ naar JenV en BZK:

- De concepten “open innovatie” en “fieldlabs” en missie-gedreven innovatiebeleid;
- Het intensiveren van de samenwerking tussen Rijksoverheid, bedrijfsleven en kennisinstellingen over de hele levensduur van kritische onderdelen;
- Alternatieve contractvormen;
- Gerichte verwervingsstrategie en correcte afweging van uitzonderingsclausules in de Aanbestedingswet 2012[79] en Aanbestedingswet op defensie en veiligheidsgebied[80]. De definitie van “gevoelig materiaal” en “gerubriceerde gegevens” is hier van belang voor de *high assurance* oplossingen. Deze afweging dient rekening te houden met de interpretatie van het Europese Hof van Justitie in relevante gevallen zoals C-187/16[81] en C-615/10[82];
- “smart buyer”, “smart specifier”, “smart developer” en “launching customer”;
- Industriële participatie verbonden aan aankoopsopdrachten in defensie en veiligheid.

Het vergt ook aanbeveling om meer zichtbaarheid te geven aan de mogelijkheden van de Commissie Defensie Materieel Ontwikkeling (CODEMO) regeling[83] en deze op een bredere manier te gebruiken als ondersteuning van strategische autonomie in het digitale domein.

Aankopen van cybersecurity relevante infrastructuur onderdelen door private operatoren vallen niet onder de openbare aanbestedingswetten. Toch heeft de overheid de mogelijkheid om aankopen van cruciale onderdelen door private partijen in kritische infrastructuur de beïnvloeden. Dit kan bijvoorbeeld door:

- De toepassing van de Algemene Beveiligingseisen Defensieopdrachten 2019[84] in bredere zin. Een uitgebreidere toepassing kan een bredere impact hebben op de cyberveiligheid in Nederland en op de strategische autonomie;
- Aankoop door de overheid van sleutelcomponenten en het verplicht gebruik ervan door operatoren van kritische infrastructuur, zoals in het Nationale Detectie Netwerk;
- Het opleggen van technische randvoorwaarden aan private operatoren als conditie voor een exploitatievergunning.

De Algemene Beveiligingseisen Defensie Opdrachten (ABDO) bevat bovendien een plicht om voorgenomen veranderingen in zeggenschap en bedrijfsstructuur te melden. Sinds 2014 is er ook een kabinetsinzet om per vitale sector te kijken of er aanvullende maatregelen nodig zijn om de nationale veiligheid voldoende te borgen bij een overname of investering. Voor elk vitaal proces, wordt een ex-ante analyse uitgevoerd om te kijken of er beschermende maatregelen tegen ongewenste overnames en investeringen moeten worden genomen.

[78] https://www.defensie.nl/downloads/beleidsnota-s/2018/11/15/defensie-industrie-strategie
[79] https://wetten.overheid.nl/BWBR0032203/2019-04-18
[80] https://wetten.overheid.nl/BWBR0032898/2019-04-18
[81] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A62016CJ0187
[82] https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:62010CA0615
[83] https://www.rijksoverheid.nl/ministeries/ministerie-van-defensie/contact/zakendoen-met-defensie/codemo
[84] https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019

Observatie: er zijn in Nederland, in het Defensie en Veiligheidsdomein, al heel wat wettelijke aanknopingspunten en processen aanwezig die toelaten om cyberveiligheid en digitale strategische autonomie op een meer structurele en strategische manier te ondersteunen. Vele ervan zijn echter nog wat embryonaal, te beperkt toegepast of onvoldoende bekend. Maar er is alvast een goede basis gelegd voor een grotere slagkracht.

Een aantal innovatieve ideeën om de slagkracht van Defensie te vrijwaren zouden kunnen toegepast worden in het bredere domein van (cyber)veiligheid.

De Defensie Industrie Strategie zou een bredere en drijvende rol kunnen spelen in het behouden en versterken van digitale strategische autonomie.

3.6 Bedrijfsovernames (M&A)

Het besef dat bedrijfsovernames de strategische autonomie kunnen beïnvloeden begint te groeien en in Europa beginnen we te beseffen dat we hier lange tijd te naïef en te marktgericht mee omgegaan hebben. Bekende recente gevallen zijn te vinden in Duitsland met Kuka (verkocht aan een Chinees bedrijf) en ARM (via een tussenstap verkocht aan nVidia in de VS). Duitsland heeft zijn wetgeving in verband met overnames van high tech bedrijven aangepast naar aanleiding van de Kuka overname[85]. Dit was ook een aanleiding om de EU Foreign Direct Investment Screening Regulation voor te stellen[86].

Door overheidsinterventie (regulering, *golden share*, onderzoeksfinanciering) werden in Duitsland overnames verhinderd van onder andere Curevac en IMST[87]. In Nederland is een recent voorbeeld Smart Photonics.

Het is aan de orde hier met aandrang te wijzen op wijdverbreide (actieve) marktverdrukking van cybersecurity startups door de grote, gevestigde, spelers. Dominantie als economisch streefdoel wordt daarbij op een speelveld zonder veel spelregels gebruikt om nieuwe spelers de toegang te verhinderen, uit de markt te prijzen of te absorberen.

De economische wetmatigheden voor de risico investeerders in de startups spelen hierin natuurlijk ook een rol. En voor de ondernemer is er de keuze tussen de optie om snel rijk te worden of economisch versmacht te worden. Beschouwingen met betrekking tot strategische autonomie moeten hierbij vanuit de overheid komen. Dit vergt een proactieve en realistische benadering, ook wat betreft de bescherming van de startups en economische compensatie. Innovatieve en geïntegreerde ondersteuning van de kroonjuwelen van de high tech industrie in het kader van de strategische autonomie in cybersecurity.

Observatie: bedrijfsovernames worden door de gevestigde spelers in de markt gebruikt om hun dominantie te versterken en nieuwe, innovatieve, bedrijven te absorberen. Deze evoluties dienen van nabij (actief) gevolgd te worden wat betreft strategische autonomie. Nieuwe werktuigen met een combinatie van regulering, participaties en condities in term sheets, slim aankoopbeleid, innovatieondersteuning kunnen hierbij selectief en in combinatie tot een optimaal resultaat leiden.

Het zou nuttig zijn om de Nederlandse aanpak te vergelijken met de ervaring in andere Europese landen (UK, FR, DE, CH, FI).

[85] https://www.dw.com/de/altmaier-will-%C3%BCbernahmen-deutscher-hightech-firmen-erschweren/a-51447649
[86] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2019:079I:FULL
[87] https://uk.reuters.com/article/uk-germany-china-m-a/germany-blocks-chinese-takeover-of-satellite-firm-on-security-concerns-document-idUKKBN28I1U0

3.7 Vergelijking van beleidsaanpak

3.7.1 De Amerikaanse aanpak

In vergelijking met de EU hanteren de VS een meer strategische, toekomstgerichte en gecoördineerde benadering van wetenschappelijke en technische ontwikkelingen, sterk verankerd in de drang om de sterkste natie te blijven in termen van militaire macht.

De Amerikaanse aanpak combineert de selectie van thema's met onderzoek financiering, overheidsopdrachten, door de overheid gefinancierde investeringen in een vroeg stadium, uitvoerbeperkingen en interventie bij fusies en overnames. In het centrum staat hun begrip van "fundamentele en opkomende technologieën". De selectie van strategische onderwerpen wordt toegepast om wetenschappelijke en technische gebieden te definiëren die het verdienen te worden gereserveerd voor financiering door overheidsinstanties zoals DARPA, IARPA, NIST, MITRE, NSF, enz. Het is ook de drijvende kracht achter het (niet-openbare) interne onderzoek en de ontwikkelingen binnen de NSA.

Het Bureau voor Industrie en Veiligheid (BIS) houdt twee lijsten bij van gebieden van strategisch belang in het kader van de Export Control Reform Act (ECRA), een lijst van fundamentele technologieën en een lijst van opkomende technologieën[88]. Onlangs is om bijdragen aan deze lijsten verzocht. De lijst die voor raadpleging is gepubliceerd, biedt een interessant perspectief. Ze omvat onderwerpen zoals computerzicht, expertsystemen, spraak- en audioverwerking, AI, cloud technologie, kwantumcomputing, kwantumencryptie...

De publiekelijke informatie over de "fundamentele en opkomende technologieën" in de VS kan worden gezien als een nuttige inbreng in het besluitvormingsproces bij de selectie van onderwerpen voor EU- en/of nationale onderzoek financiering.

Het ook is interessant om de recente investeringen door In-Q-Tel, het financieringsinstrument van de CIA, te analyseren.

	Lead	Country		Created
Truwave		US	Machine vision	2017
Morpheus Space		DE	Space, propulsion technologies	2018
Snorkel AI		US	AI	2019
Sayari Labs		US	Fraud and threat detection	2018
Ocient		US	Big data analysis	2016
Lilt		US	AI	2015
Toposens	Yes	DE	Machine vision, autonomous driving	2015
Coder		US	Software quality, Kubernetes	2015
AI.Reverie		US	Synthetic data, training AI	2017
Q-Ctrl	Yes	AU	Quantum computing	2017

Figuur 17 Recente investeringen in startups door In-Q-Tel - bron Crunchbase

Verrassend genoeg zijn twee van de tien investeringen gedaan in Duitse startende ondernemingen. In één geval was In-Q-Tel zelfs de hoofdinvesteerder. Het geval van Morpheus Space is bijzonder intrigerend omdat het bedrijf is opgericht op basis van een zeven jaar durende onderzoeksinspanning aan de Universiteit van Dresden in 2018. Het bedrijf heeft een aandrijfsysteem ontwikkeld voor kleine satellieten.

[88] https://www.federalregister.gov/documents/2020/08/27/2020-18910/identification-and-review-of-controls-for-certain-foundational-technologies

In 2018 kreeg Morpheus Space steun voor technologieoverdracht van Dresden-Exist, maar toen ging het bedrijf naar de VS voor groei. In 2019 startte het bedrijf in de Techstars Starbust Space Accelerator in Los Angeles. De VC A-ronde werd geleid door Vsquared (DE) en omvatte ook Airbus, Lavrock (US), Techstars (US) en Pallas (US).

Er zijn geen aanwijzingen dat de EU of ESA-middelen (onderzoek, innovatie of aanbesteding) aan Morpheus Space hebben verstrekt. Gezien het tijdpad (oprichting in 2018 en financiering met durfkapitaal in 2019) zou het moeilijk zijn om onderzoek financiering te verkrijgen in het licht van het bestaande proces.

De zaak-Morpheus Space toont de flexibiliteit en doeltreffendheid van de VS in een strategisch gebied en in een praktisch geval waarin de mogelijkheid werd gecreëerd op basis van onderzoek en deskundigheid van de EU.

Meer in het algemeen blijkt uit de vorige hoofdstukken over wetenschap en financiering dat de VS met vergelijkbare niveaus van investeringen in wetenschap en technologie twee tot drie jaar voor de EU liggen, waar het gaat om het concentreren van de inspanningen op gebieden van strategisch belang en ook veel efficiënter is om het opstarten en de groei van bedrijven op deze gebieden te stimuleren.

Sommige instrumenten die de VS in hun strategische aanpak gebruiken, verdienen te worden beoordeeld op hun verdienste voor de EU:

- In-Q-Tel als door de overheid gefinancierd investeringsinstrument bij startup financiering
- De snelle financiering van onderzoek in wetenschap en starters door DARPA en IARPA
- Uitzonderingen voor overheidsopdrachten

Er wordt vaak verwezen naar de manier hoe in de VS de publieke departementen DARPA/IARPA het academische O&O en industriële R&D aanjagen. Erg strategisch gericht op basis van een selectie van technologie die relevant is. Laagdrempelig voor goede projecten, snelle beslissingen. Maar competitief, ook kort op de bal in de opvolging en corrigerend indien de milestones niet gerespecteerd worden. Sommige Europese academici en bedrijven hebben de weg naar DARPA ook al gevonden en verkiezen deze financiering boven de EU-financiering.

DARPA werkt met een beperkt aantal projectmanagers die competitief betaald worden en die een hoge mate van autonomie hebben. Ze genieten een hoge mate van respect en zeer begeerd in de industrie wanneer ze DARPA verlaten. DARPA beheerd een jaarlijks budget van 3,4 miljard USD.

In oktober 2020 heeft het White House aangegeven[89] welke strategische autonomie benadering ingezet wordt voor elk van 'Critical and Emerging Technologies': namelijk risicomanagement, strategisch partnership, of exclusief onder eigen beheer (die optie is voor de EU of NL niet weggelegd). Opvallend is dat de optie van 'global common good' (wereldwijd gemeenschappelijk belang) niet onderkend wordt. Dit is mogelijk een reflectie van de scepsis over multilaterale samenwerking.

Observatie: DARPA/IARPA zijn in het verleden reeds als voorbeeld bekeken voor initiatieven in Europa. In het VK wordt er op dit moment overwogen om een gelijkaardige organisatie op te richten. In-Q-Tel begint vanuit strategisch perspectief ook in Europese startups te investeren.

[89] https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf

3.7.2 Het Britse voorbeeld

Het Verenigd Koningrijk spiegelt zich erg aan de VS wat betreft strategische autonomie. En ook in het VK spelen de inlichtingendiensten en defensie een belangrijke rol in het bepalen van de agenda en het verwerven en behouden van control over sleutel technologieën. Offensieve macht wordt hierin als een even belangrijk argument gebruikt als de defensieve.

Recent werd de S&T-strategie van de defensie gepubliceerd[90]. Het geeft aan hoe O&O en R&D-investeringen zullen aangewend worden om de belangrijkste operationele noden van het leger te kunnen ondersteunen. Een citaat uit het voorwoord; " by excelling in S&T we can secure our future strategic advantage". Prospectief onderzoek en coördinatie zijn belangrijke bouwstenen van de strategie. Er worden vijf "capability challenges" aangepunt:

- Pervasive, full spectrum, multi domain Intelligence, Surveillance and Reconnaissance
- Multi-domain Command & Control, Communications and Computers (C4)
- Secure and sustain advantage in the subthreshold
- Asymmetric hard power
- Freedom of Access and Manoeuvre

Inspanningen worden gepland ter ondersteuning van deze vijf domeinen. Een interessant concept in dit document is "Generation after next", verder kijken dan de horizon wat betreft de *capabilities* maar ook de technologie die zulke toekomstige *capabilities* kunnen ondersteunen.

De inlichtingendienst GCHQ heeft een eigen cyber accelerator en innovatieprogramma[91] en investeert in O&O en R&D van relevante technologie. Ook het Ministerie van Defensie heeft haar eigen DASA-accelerator en financieringsprogramma[92]. Er zijn op dit moment op het hoogste niveau opnieuw plannen om een DARPA-achtige organisatie op te zetten in het VK.

Het nationale cyberveiligheidscentrum van het VK, NCSC-UK, maakt deel uit van de inlichtingendienst GCHQ. Informatie verzameld door de inlichtingendienst wordt daarbij ook actief ingezet om de veiligheid van het netwerk van overheid en gezondheidsdiensten te beveiligen in het Protective DNS systeem[93]. Dit is een onderdeel van het Active Cyber Defence programma waarin GCHQ een leidende rol speelt.

3.7.3 China

Volgens Tai Meung Chang[94] wordt de ontwikkeling van 'strategische sectoren' in China top-down gedreven door het 'national security apparatus – which includes the military, internal security, law and order, intelligence and information control apparatuses – [and which] occupies a powerful presence in China's cyber affairs. Moreover, the development of the cybersecurity industry and associated information technology domain is significantly driven by the development of technological capabilities.

China combineert protectionisme met nationale kampioenen, technologie transfer van buitenland naar Chinese bedrijven en de promotie van Chinese technologie standaarden zowel in eigen land als internationaal. China heeft ook 'cyber sovereignty' als sinds meerdere jaren als primair uitgangspunt. Jonathan Holslag beargumenteert in detail dat China dit

[90] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/927708/20201019-MOD_ST_Strategy_2020_v1-23.pdf
[91] https://techcrunch.com/2015/11/18/uk-gov-to-invest-in-security-startups/?guccounter=1
[92] https://www.gov.uk/government/organisations/defence-and-security-accelerator
[93] https://www.ncsc.gov.uk/information/pdns
[94] Tai Ming Cheung (2018) The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities, Journal of Cyber Policy, 3:3, 306-326, DOI: 10.1080/23738871.2018.1556720.

combineert met handelsbeleid en buitenlandse investeringen (Belt & Road Initiative, M&A) om strategische buitenlandse invloed te krijgen[95]. De EU ziet China als een 'systemic rival' en stelt een vernieuwde trans-Atlantische alliantie voor om de opmars van China naar wereld-dominantie in technologie te keren[96].

De meningen mogen verschillen over de uiteindelijke intenties van het Chinese leiderschap. Duidelijk is echter dat China een hele reeks beleidsinstrumenten combineert, top-down, met een lange adem. En tot nu toe grotendeels met succes.

3.7.4 De situatie in Nederland

In Nederland bestaat, in vergelijking met de VS en het VK (en Frankrijk), niet zo'n sterke koppeling tussen defensie- en innovatiebeleid. Laat staan dat Nederland een geïntegreerde aanpak van beleid heeft zoals die in China bestaat. Meer algemeen concludeert een recente SWOT-analyse van de Nederlandse cybersecurity waardeketen het volgende: "Nederland kent nauwelijks een 'maakindustrie' in cybersecurity. Hardware en software komen voornamelijk uit het buitenland. Nederland is vooral betrokken bij de dienstverlening. Het landschap is versnipperd; zowel in het bedrijfsleven als binnen de overheid. Geopolitieke overwegingen kunnen leiden tot de wens meer onafhankelijk te zijn. Goed gekwalificeerde mensen zijn soms onvoldoende beschikbaar in Nederland"[97].

Niettemin, is er een aantal concrete sterktes waar Nederland op kan bouwen om haar beleid te versterken, onder meer en zonder uitputtend te zijn:

- de strategische oriëntatie en brede samenstelling van de CSR
- het gezag van de WRR
- de operationele effectiviteit van de NCSC
- de dreigingsinformatie van AIVD
- de publiek-private sterkte van de Defensie Industrie Strategie
- de EZ voorstellen voor een nieuwe kennisimpuls
- de innovatieve aanpak van brede bewustwording en kennis van EPC.NL
- academische reputatie in een groot aantal terreinen van quantum-technologie tot privacy tot open source initiatieven
- de sterke stem van Nederland in de EU
- het internationale gezag van Nederlandse cyber-diplomatie.

Observatie: de VS, het VK en China koppelen hun strategische autonomie rechtstreeks aan hun streven om op militair vlak autonoom en dominant te worden en te blijven (en voor de VS en China ook in het digitale domein). Ze hebben daartoe processen en middelen gecreëerd die continue de doelstellingen verbinden met alle noodzakelijke middelen om ze te bereiken op een gecoördineerde manier. Een essentieel onderdeel hierbij vormt een lijst van sleutel technologieën.

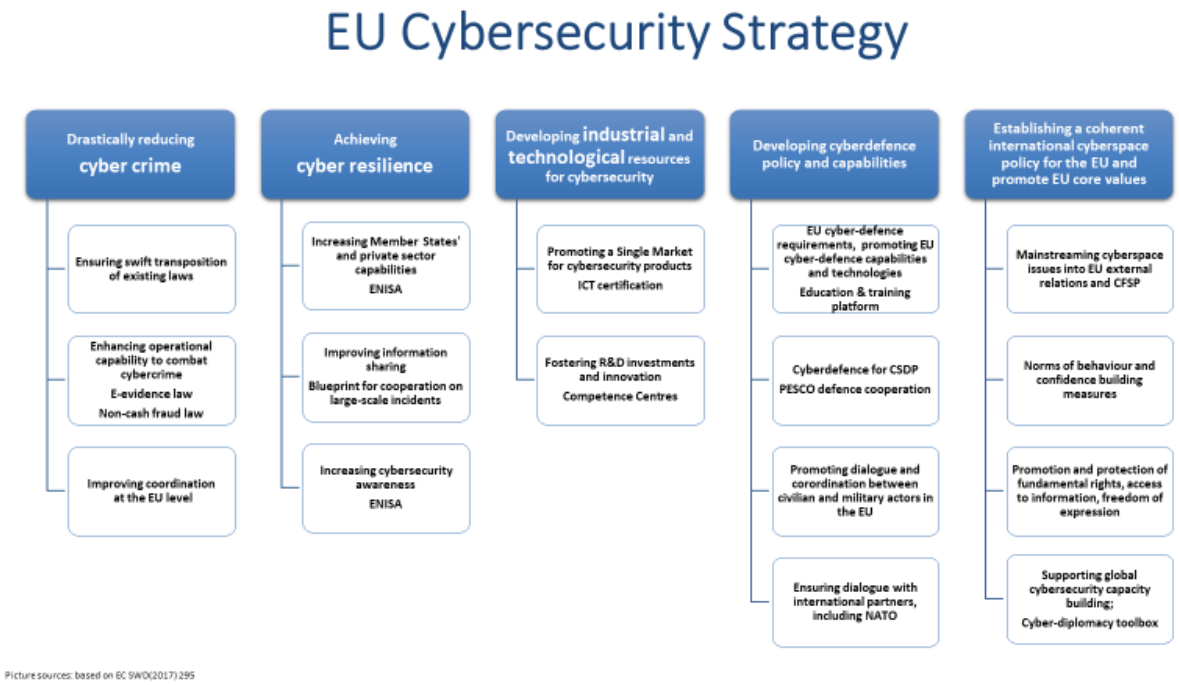
Er is ook een veel grotere synergie tussen de defensie/inlichtingendiensten en de actieve cyber-beveiliging van de betreffende landen.

[95] Jonathan Holslag, The Silk Road Trap: How China's Trade Ambitions Challenge Europe, Polity Press
[96] EC en EEAS, 2 dec 2020, A new EU-US agenda for global change, https://ec.europa.eu/info/files/joint-communication-new-eu-us-agenda-global-change_en
[97] KPMG, okt 2020, SWOT Analyse Strategische Waardeketens in opdracht van EZK

4 Beleidsinstrumenten

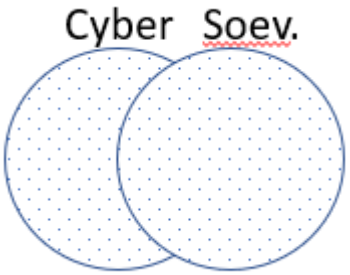
Er is hier al eerder verwezen naar beleidsinstrumenten. Bovendien is er een gerelateerde beschrijving van instrumenten in een recent TNO-rapport[98].

De EU-cybersecuritymaatregelen zijn in onderstaand diagram van de Europese Commissie samengevat. Het omvattende kader is de EU Cybersecurity Strategie van 2013. Die werd uitgebreid in 2017. Een verdere herziening is aangekondigd voor 2021.

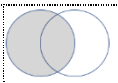
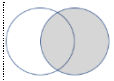
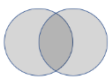


Picture sources: based on EC SWD(2017) 295

Hieronder worden al die beleidsinstrumenten samengevat, met een aanduiding van hun relevantie voor cybersecurity en voor soevereiniteit. Ook wordt aangegeven wat de huidige status en motivatie is en wat er – indien van toepassing – in de toekomst te verwachten is.



Deze studie houdt de focus op maatregelen die zowel cybersecurity als soevereiniteit betreffen dus enige overlap tonen tussen die twee domeinen. Symbolisch aangegeven met:

Cybersecurity-gemotiveerde maatregelen met relevantie voor soevereiniteit:	
Soevereiniteit -gemotiveerde maatregelen met relevantie voor cybersecurity:	
De maatregelen die het sterkst samenhangen met zowel het *bredere* cybersecuritybeleid én het *bredere* soevereiniteitsbeleid:	

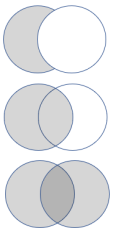
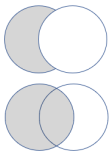
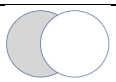
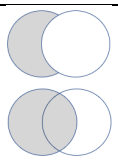
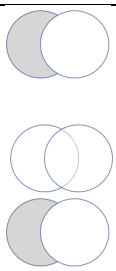
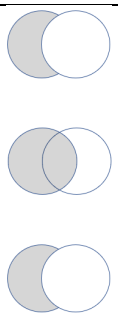
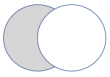
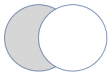
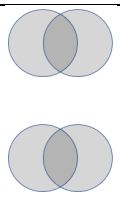
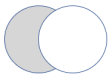
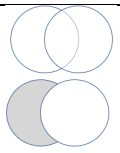
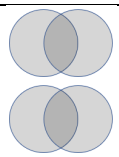
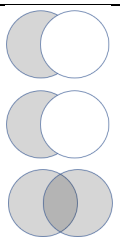
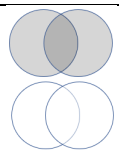
[98] TNO 2020 R11599 "Strategische Autonomie op Cybersecurity".

Voor het meest coherente en krachtige beleid is het aan te raden cybersecuritymaatregelen die strategische autonomie aangaan in het bredere kader van strategische autonomie beleid te plaatsen[99]. Omgekeerd, daar waar maatregelen voor strategische autonomie worden genomen is het sterk aan te raden ook hun eventuele relatie met cybersecurity in rekening te brengen[100].

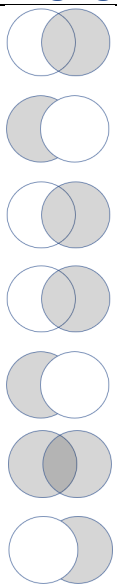
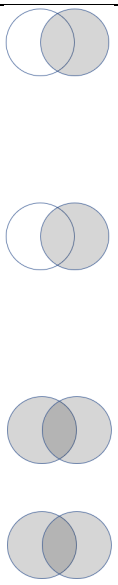
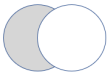
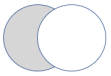
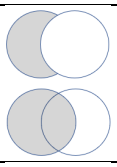
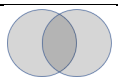
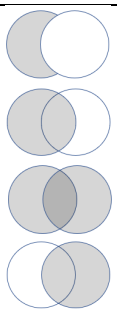
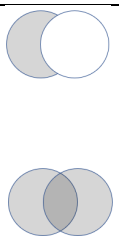
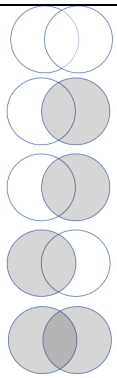
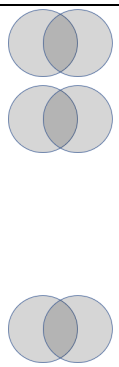
Enkele observaties over het uitvoerige (maar niet exhaustieve) overzicht dat in de hierna volgende tabellen wordt gegeven:

- Slechts een deel van deze maatregelen betreft zowel cybersecurity als soevereiniteit. Het overzicht suggereert terreinen waarop in de toekomst een sterkere focus op de combinatie van cybersecurity en soevereiniteit nodig of wenselijk is
- Beleidsmakers kunnen met dit overzicht analyseren of soevereiniteit en/of cybersecurity mogelijk een rol zou moeten spelen in hun beleid in het algemeen[101].
- Er zijn nog verdere beleidsinstrumenten denkbaar zoals:
    - Leverancier-uitzonderingen voor overheidsopdrachten voor cyberveiligheid
    - Belastingbeleid/vermogenswinstbelasting
    - Open-sourcebeleid
    - Mededingingsbeleid
    - Overheidsdeelname aan risicokapitaal (cf. In-Q-Tel in de VS)
    - Investeringssteun.
- De sterkte van maatregelen kan niet uit het overzicht worden afgelezen. Bijvoorbeeld EU-industriebeleid is intentioneel en ontbeert wetgevende kracht of financiering.
- Niet direct uit de tabellen af te leiden maar volgend uit de case analyses is dat er weinig synergie tussen maatregelen is. Niettemin, geïntegreerd beleid is een noodzaak gezien de dreigingen én een kans om effectiever met maatregelen te zijn.
- Schuinschrift in de tabellen geven toekomstig beleid aan (aangekondigd of in deze studie gesuggereerd).
- Sectie 6.6 gaat dieper in op recent en aangekondigd EU-beleid en wetgeving.

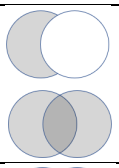
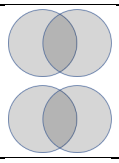
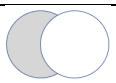
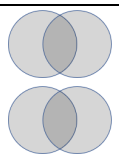
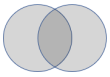
[99] Een opening daarvoor wordt op Europees niveau geboden door een nauwe koppeling van wetgeving voor cyber en non-cyber bescherming van kritische entiteiten (i.c. de NIS2 Directive en de CER Directive, zie hoofdstuk 4 en sectie 6.6).
[100] Een voorbeeld is de digitale euro, die financiële autonomie kan versterken maar ook cyber-veilig moet zijn.
[101] De analysemethode is dus ook toepasbaar op situaties die soevereiniteit maar niet cybersecurity betreffen, zoals de gevolgen voor soevereiniteit van het Europees/NL telecombeleid, waarbij prijzen gedrukt worden en concurrentie toeneemt maar ook binnenlandse innovatie en zelfstandigheid het risico lopen om te eroderen.

Faciliterend				
	EU maatregel	**Cybersecurity en/of Soevereiniteit**	**NL maatregel**	**Cybersecurity en/of Soevereiniteit**
Strategie en agendering	CS strategie 2013 - 2020 CS strategie 2020 - EU-US Agenda 2020		CSR tot recent *CSR toekomst?*	
Monitoring	ENISA dreigingsbeeld		NL dreigingsbeeld; *Strategische autonomie-monitor?*	
Kennis	EU R&D AI beleid Quantum R&D flagship		O&O cyber heden *O&O cyber toekomst?* NCSC	
Cybervaardigheden	Cyber Month (ENISA)		ECP-NL Cyber	
Infrastructuur ondersteuning	Connecting Europe Facility Cloud beleid, GAIA-X		NL Cloud beleid	
Marktstimulerend	Resilience & Recovery Fund R&D inkoop		*Overheid als launching customer?* *Overheid cyber-R&D inkoop?*	
Ecosysteem (industrieel, innovatie, kennis, beleid)	Cyber competence centres ; ENISA ; Industrie, 2020[102]		EZK Platform[103] StartupDelta	

[102] COM(2020) 102 final, 3 maart 2020.
[103] Samenwerkingsplatform Cybersecurity en Innovatie

Regelgevend				
Markt-voorschrijvend of markt-controlerend	GDPR CyberAct certificering FDI Regulation EU export controls Wassenaar *AI liability* Digital Services Act, Digital Markets Act		AVG M&A/FDI controle bureau *Voor specifieke bedrijven :* - *poison pill* - *golden share* - *overheids-participatie* - *financieringssteun* - *clausules in term sheets* *Wet Toetsing Investeringen*	
Operationele cyber-resilience	CERT-EU		NCSC	
Cyber-crime	Non-cash fraud E-Evidence		*Rechtsketen cloud?*	
Kritische infrastructuren en diensten	NIS-Directive 2016 NIS2-Directive 2020 5G Security Recommendation CER Directive[104]		NIB Richtlijn WOTZ[105]	
Kritische assets (staatsgeheimen, industriële kennis/IP, data spaces, identificatie burgers en bedrijven)	IP Action Plan 2020 .eu Regulation 2003 *EU Data Spaces '21* eIDAS 2014 *eIDAS 2021*		Staatsgeheimen *Kennisveiligheid initiatief EZK* *Deep security?*	

[104] Critical Entities Directive, 16 december 2020 (opvolger van Directive 2008/114/EC — identification and designation of European critical infrastructures)
[105] Wet Ongewenste Zeggenschap Telecom

Internationaal				
Internationale standaardisatie	ETSI, CEN/CENELEC CS Strategie 2020			
Rechten en waarden	UN OEWG, GGE CS Strategie 2020			
Internationale verdragen	Budapest Convention on cyber-crime			
Defensie	CSDP NATO		Defensie industrie strategie	

5 Toetsingskader

De observaties in deze studie leiden tot een rijke set aan inzichten en triggers voor overheidsinterventie. De inzichten en de triggers zijn het startpunt van een analyse om te beoordelen of de staat moet interveniëren om strategische autonomie te versterken of evenwicht te herstellen en hoe ze dat moet doen. Alle elementen worden verzameld in een "case" die op een geïntegreerde manier beoordeeld wordt en al dan niet aanleiding geeft tot interventie.

Een case wordt uitgedrukt in een aantal relevante domeinen waarin geageerd wordt of kan worden. In deze domeinen is ook op een actieve en continue manier informatie te verzamelen om ontwikkelingen te identificeren die de strategisch autonomie uit evenwicht brengen.

Die domeinen vormen één dimensie van het toetsingskader. De tweede dimensie van het toetsingskader zijn de relevante beleidsterreinen.

Dit hoofdstuk geeft de presentatie en uitleg van het toetsingskader. Het volgende hoofdstuk past het kader toe op concrete cases.

5.1 Focus

De cases in de vorige hoofdstukken leveren heel wat materiaal om de concepten de beschrijven die toelaten om strategische autonomie een op een strategische maar ook praktische manier aan te pakken.

Deze studie en het toetsingskader beperken zich tot die factoren die zowel cyberveiligheid betreffen alsook strategische autonomie beïnvloeden. Met andere woorden, de digitale aspecten van strategische autonomie en met name betreffende de cyberveiligheid. Een dergelijke focus correspondeert met de opdracht en (beperkte) omvang van deze studie.

Eén criterium om die focus in de praktijk om te zetten is te verifiëren of het over "sleuteltechnologieën" gaat. Een andere vorm van focus kan zijn om deze mogelijke beleidsinstrumenten te beperken. Dit zou echter niet terecht zijn. Een algemene observatie is namelijk dat:

Algemene observatie:

1. Coherent en geïntegreerd beleid is noodzaak, dit doen anderen ook in het geopolitieke veld, maar is in Nederland en de EU nog weinig te zien.
2. Strategische autonomie en daarmee soevereiniteit worden nauwelijks als uitgangspunt voor beleid genomen. Dit houdt een groot risico in.
3. Proactieve monitoring van triggers voor strategische autonomie en cybersecurity heeft een grote waarde om tijdig en coherent te reageren.

5.2 Sleuteltechnologieën

Ter ondersteuning van de focus is een lijst van "sleuteltechnologieën" waarmee de cyberveiligheid kan bewaakt worden of die toelaten om cyberveiligheidsrisico's te mitigeren.

Observatie: een lijst van sleuteltechnologieën dient opgesteld en onderhouden te worden als essentieel hulpmiddel om relevante veranderingen in onze omgeving te identificeren, te beoordelen en te beïnvloeden.

Landen zoals de VS en het VK gebruiken ook lijsten van sleuteltechnologieën om hun interventies in verband met strategische autonomie te sturen. In hun geval worden deze

lijsten niet alleen economisch en maatschappelijk bezien maar ook gekoppeld aan militaire strategische doelstellingen.

Ook in Nederland heeft het concept van sleuteltechnologieën reeds ingang gevonden. In dit verband is het recente advies van de CSR "*Naar structurele inzet van innovatieve toepassingen van nieuwe technologieën voor de cyberweerbaarheid van Nederland*[106]*"* pertinent. Het CSR-advies bevat vier aanbevelingen:

1. De overheid ontwikkelt integraal beleid rondom nieuwe technologieën met impact op cyberweerbaarheid.
2. De overheid werkt aan het jaarlijks in kaart brengen van de technische ontwikkelingen die relevant zijn voor het benutten en creëren van kansen, het borgen van cyberweerbaarheid en de bredere digitale autonomie van Nederland.
3. De overheid voert een actief industriebeleid voor cybersecurity.
4. De overheid stimuleert (inter)nationale samenwerking bij relevante technologieën voor cybersecurity.

Bijkomende bestaande aanknopingspunten in Nederland zijn de lijst van sleuteltechnologieën opgesteld door de High Level Group voor sleuteltechnologieën in 2017[107] en het advies van de AWTI van januari 2020, "Krachtiger kiezen voor sleuteltechnologieën"[108].

Ook de Beleidsnota Defensie Industrie Strategie van 2018 verwijst naar (opkomende) technologie gebieden die in de toekomst belangrijk kunnen zijn. Er wordt in deze Beleidsnota ook een afweging gemaakt over de noodzaak van overheidsinterventie en het gewenste betrokkenheidsniveau van de overheid (Defensie in dit geval).

Op internationaal niveau is er een lijst van goederen en technologieën[109] voor duaal gebruik van het Wassenaar Arrangement. Het Wassenaar Arrangement[110] wordt gesteund door 41 landen, waaronder de VS en de EU. Bijzonder relevant in de lijst[111] zijn categorie 5, "Telecommunicatie" en "Informatiebeveiliging". De lijst van Wassenaar zou ook een bijdrage kunnen leveren aan de gebieden die van belang kunnen worden geacht voor de digitale strategische autonomie.

Ten aanzien van sleuteltechnologieën zijn er nog verschillende vragen te stellen:

- Is de technologie van cruciaal belang in de enge (specifieke) betekenis of in de brede (fundamentele) zin en derhalve van essentieel belang?
- Is de technologie uniek (geen alternatieven) op dit moment of in de toekomst?
- Is de technologie eigendom van een organisatie waarover vanuit het strategisch perspectief onvoldoende controle bestaat?
- Kan het risico worden beperkt door andere technologische componenten of door regelgeving of condities voor markttoegang?

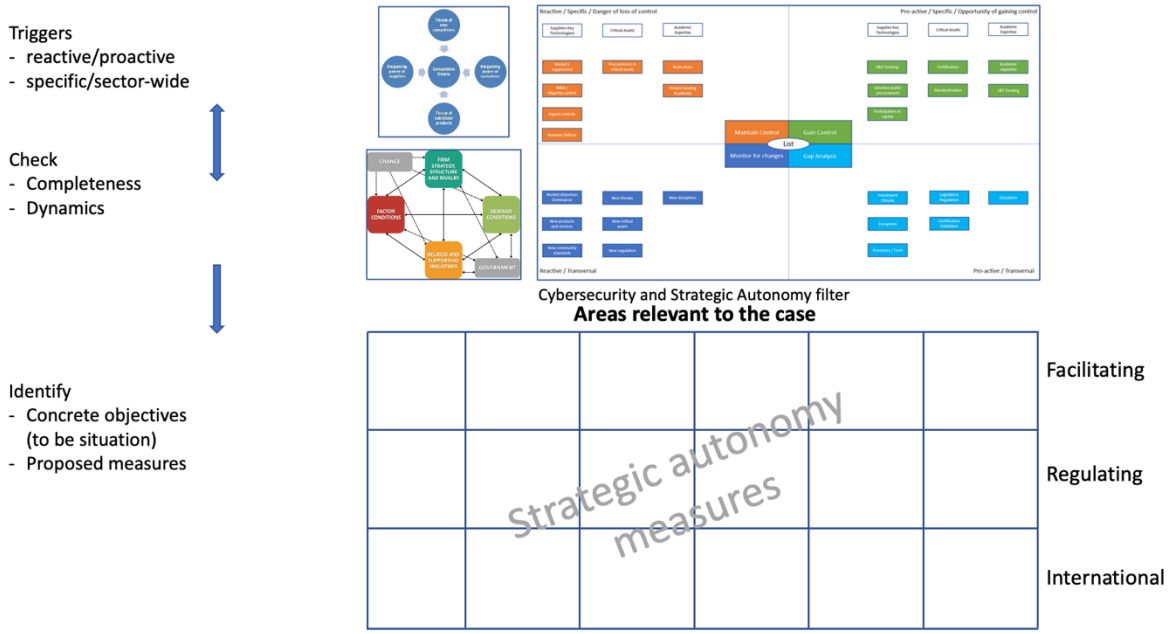
[106] 18 september 2020 CSR-advies 2020, nr. 5
[107] https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/kwantitatieve-analyse-van-onderzoek-en-innovatie-in-sleuteltechnologieen-in-nederland
[108] https://www.awti.nl/actueel/nieuws/2020/01/30/advies-krachtiger-kiezen-voor-sleuteltechnologieen
[109] https://www.federalregister.gov/documents/2019/05/23/2019-10778/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2018
[110] https://www.wassenaar.org/
[111] https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf

5.3 Overzicht van toetsingskader

De voorgestelde toetsingslogica is als volgt:

1. **Trigger(s) identificeren**, die reactief of proactief gevonden kunnen worden, en specifiek of sectorbreed kunnen zijn
2. **Analyseren** van de markt-, regelgeving- en technologiedynamiek die met de geactiveerde trigger(s) samenhangen, bijvoorbeeld met modellen van Porter
3. **Case beschrijving**, een 'narrative' in termen van de **domeinen** of factoren (uit de modellen) die relevant zijn op basis van de voorgaande analyse van dynamiek en triggers; dit beschrijft ook de **controle** in de zin van strategische autonomie[112]
4. **Focus** op factoren die cyberveiligheid en strategische autonomie beïnvloeden
5. **Doelstelling:** gewenste resultaat in versterking van de strategische autonomie definiëren
6. Breng een samenhangend geheel van voorgestelde acties of **maatregelen** (interventions) in kaart om controle op te bouwen of te herstellen.

De totale aanpak wordt hieronder aangegeven en vervolgens uitgelegd.



Figuur 18 Toetsingskader

Dit schema geeft, van bovenaf startend, een 'trigger diagram' waarvan de functie is om aanleidingen voor interventie te identificeren en twee Porter modellen om de dynamiek van kennis, industrie, markt en overheid te analyseren. Porter modellen en trigger diagram dienen om tot een complete case beschrijving te komen, die dan vervolgens op strategische autonomie in cybersecurity toegespitst wordt (stappen 1, 2, 3 en 4). Op basis van de

[112] Controle over vermogen en middelen om te kunnen beslissen over de eigen toekomst in economie, maatschappij en democratie.

verzamelde gegevens worden doelstellingen voor controle verbonden aan interventies die zowel mogelijk als gewenst zijn (stappen 5 en 6).

Eén praktische aanpak is om op het trigger-niveau te beginnen. Vervolgens moet de volledige situatie in kaart worden gebracht in een Case (de 'as is' situatie) teneinde de dynamiek te begrijpen. Dan moet het gewenste resultaat worden gedefinieerd, dus het doel in termen van strategische autonomie, de "to be"-situatie. De volgende stap is de relevante instrumenten voor interventie te definiëren en ten slotte de samenhang van deze instrumenten te verifiëren. Zo nodig kan ook worden vastgesteld welke monitoring nodig is van de interventies.

Er worden twee Portermodellen gebruikt voor de analyse. Het Five Forces model gaat over de krachten die inwerken op een *specifiek bedrijf* en correspondeert daarmee met de bovenste helft van het trigger diagram. Het Diamond Model beschrijft krachten in een *sector als geheel* ofwel sector-wijd en correspondeert daarmee met de onderste helft van het trigger diagram.

Enerzijds dienen de twee Porter-modellen om de oorsprong van "triggers" te groeperen en zo te voorkomen dat bepaalde triggers gemist worden en dat er willekeur is bij de keuze van triggers om op te concentreren. Bovendien helpen de modellen om verwante factoren te zien, en daarmee samenhangende beleidsinstrumenten. Ze helpen de dynamiek te begrijpen zoals de wisselwerking tussen regulering en marktontwikkeling. Dit kan als de **top-down** benadering worden beschouwd.

Anderzijds volgt uit de **bottom-up** analyse een reeks triggers, die gegroepeerd worden in het 2x2 overzicht beschreven in sectie 5.4, Trigger . De twee dimensies van de groepering zijn het identificatieproces, dat reactief of proactief is, en het niveau van de trigger, dat specifiek of sector-breed is.

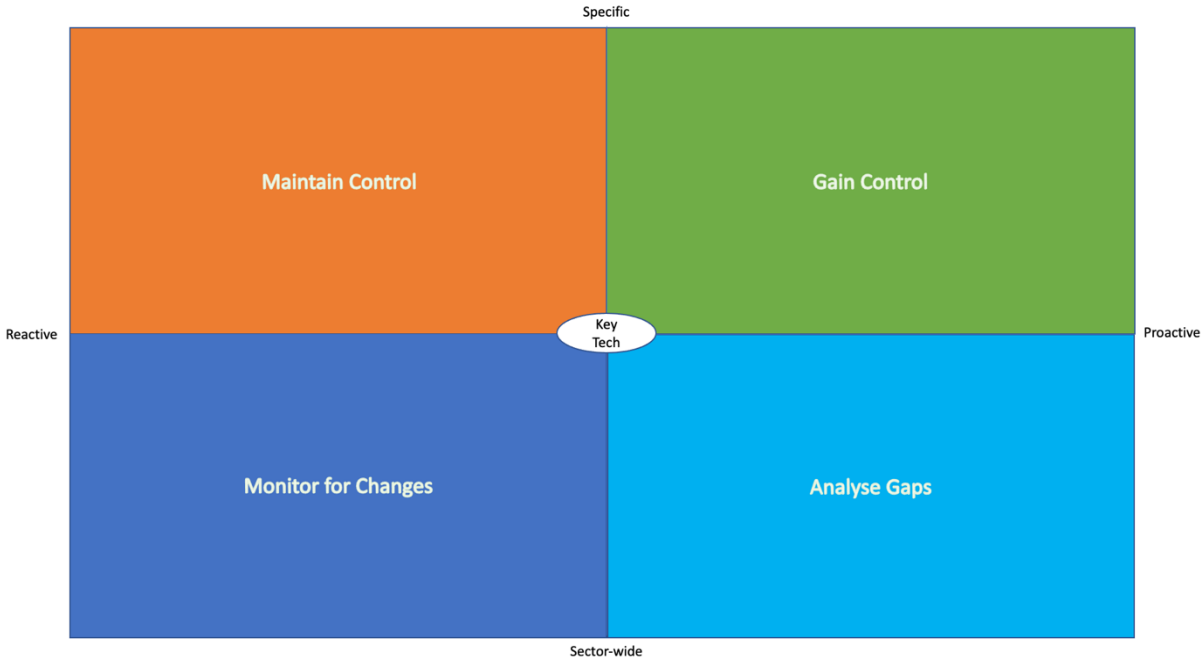
Een voorbehoud is dat dit een rijke maar geen volledige analyse zal opleveren: de interacties zullen complexer zijn dan in deze modellen is vastgelegd. Bovendien hebben de gekozen modellen overwegend hun oriëntatie op concurrentievermogen eerder dan - bijvoorbeeld - op het regeringsbeleid, laat staan dat ze een geïntegreerd beeld geven van wisselwerking tussen overheid en marktdynamiek (die recente inzichten in *governmentalism* gebruiken[113]). De ontwikkeling van meer geïntegreerde modellen valt buiten het kader van deze studie.

Tenslotte, het toetsingskader is modulair, in de zin dat indien gewenst de Porter modellen en het Trigger Diagram afzonderlijk gebruikt kunnen worden of vervangen kunnen worden door alternatieve analyse-tools, bijv. *agent-based modelling, system dynamics*, en *multi-modelling*. De essentie is om te komen tot een complete en samenhangende case beschrijving die moet toelaten het effect te beredeneren van een of meerdere interventies gebaseerd op de genoemde beleidsinstrumenten.

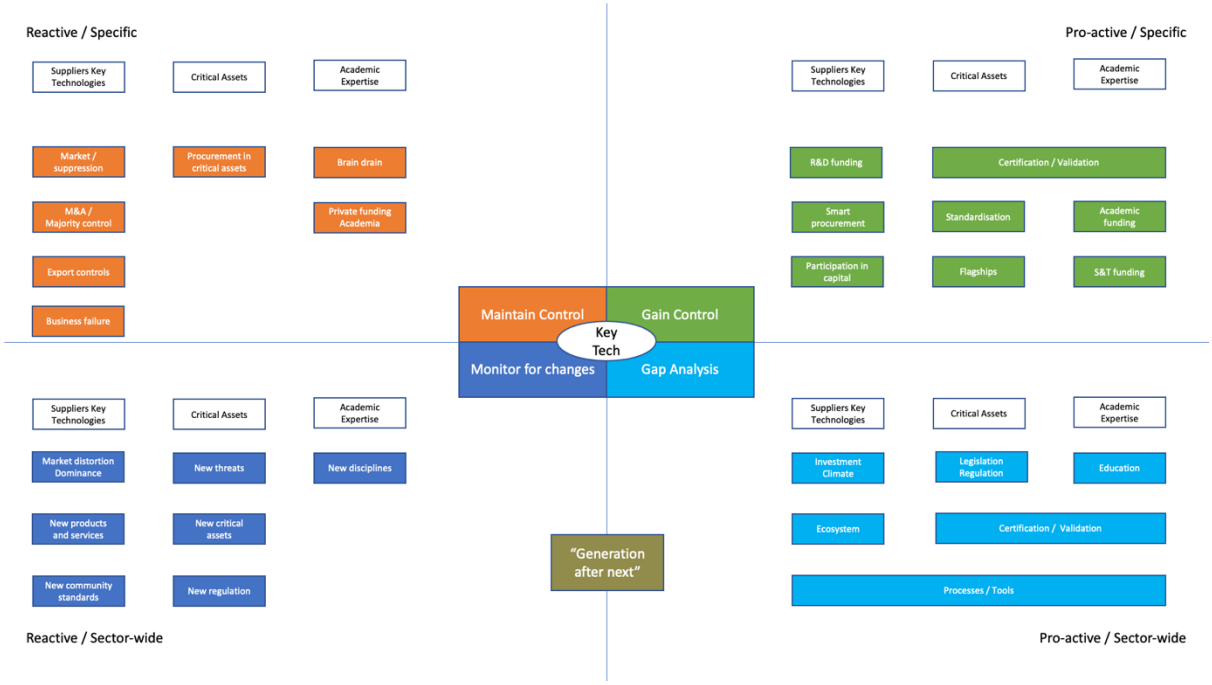
5.4 Trigger Diagram

De geanalyseerde cases in onze studie leiden tot een overzichtsschema van relevante domeinen waaruit triggers kunnen verzameld worden en waar impact mogelijk is. Het Trigger Diagram bevat twee dimensies: reactief of proactief en specifiek of sector-breed. Hierdoor ontstaan vier kwadranten: "Behoud controle", "Verwerf controle", "Observeer wijzigingen" en "Analyseer en dicht hiaten".

[113] Julie Cohen, 2019, "Between Truth and Power".



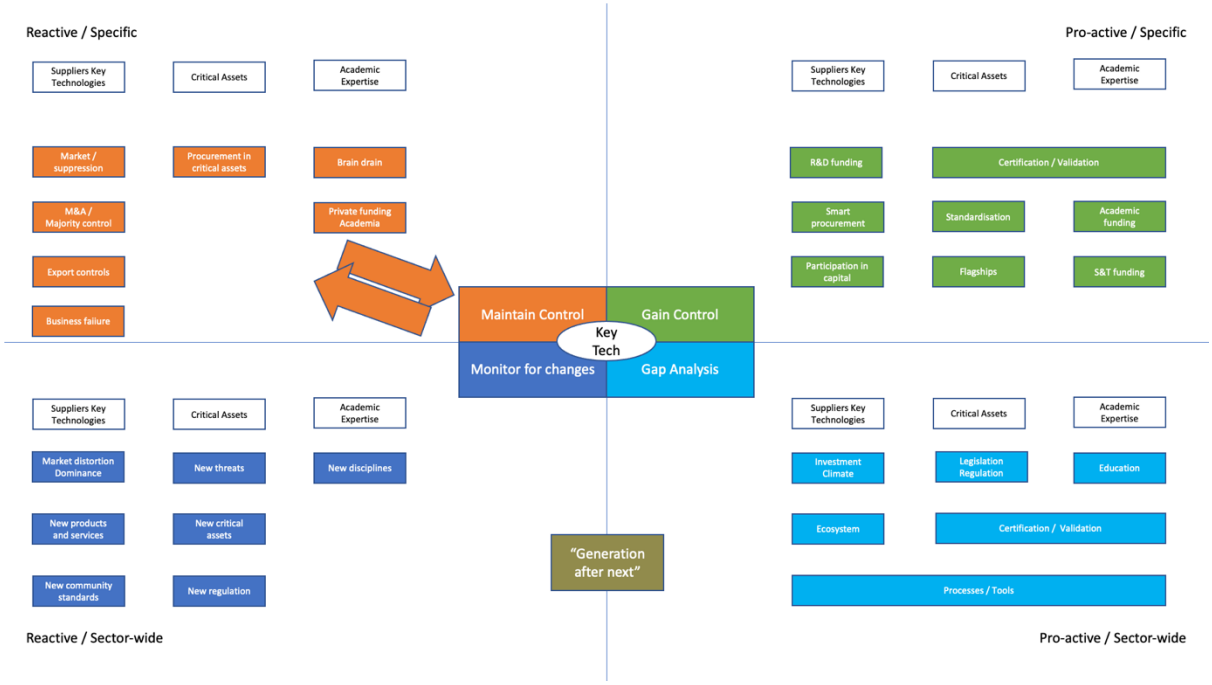
Elk kwadrant maakt ook nog een onderscheid tussen de domeinen van de leveranciers van sleuteltechnologie, de kritische assets die sleuteltechnologie gebruiken en de wetenschappelijke wereld die de fundamentele basis legt voor de sleuteltechnologieën. Een verklarende legende van de verschillende domeinen en de link naar de cases is opgenomen in Annex 2.



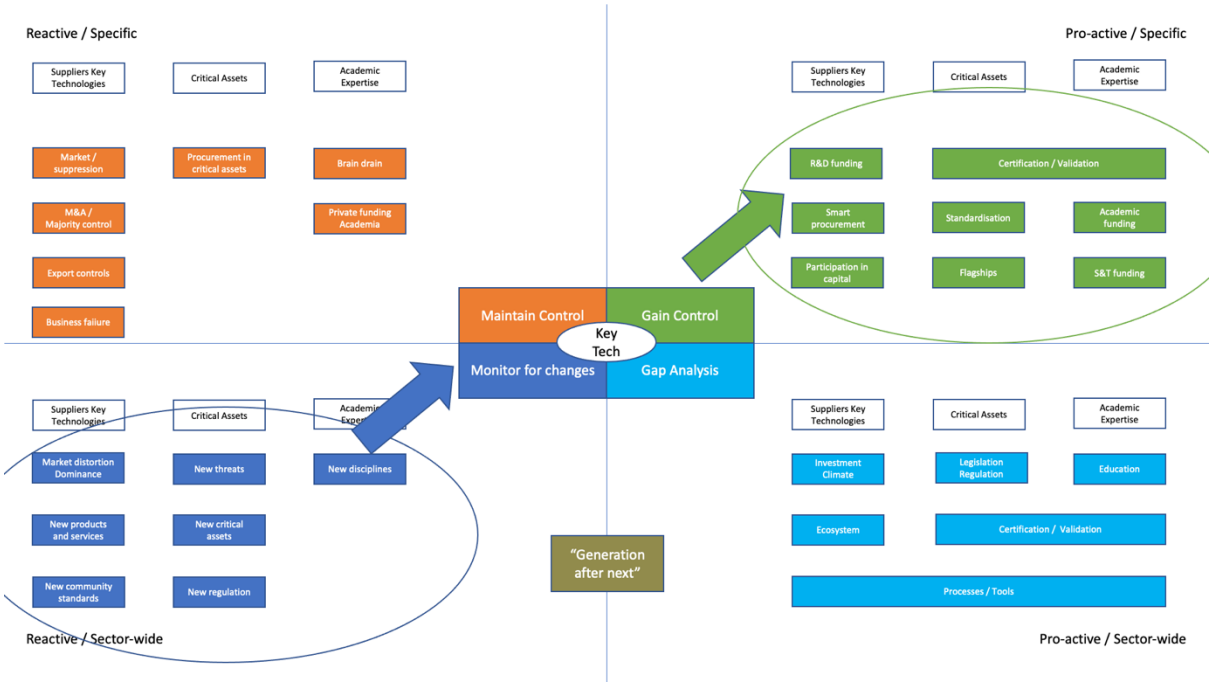
Centraal in het Trigger Diagram is een permanente (interdepartementale) activiteit om relevante ontwikkelingen in de diverse domeinen die verband houden met de sleuteltechnologieën te onderkennen en te beoordelen.

Observatie: relevante ontwikkelingen in de domeinen dienen op een continue en proactieve manier geobserveerd, geanalyseerd en beoordeeld te worden. Deze activiteit is binnen de overheid **interdepartementaal en betreft in het algemeen meerdere stakeholders**.

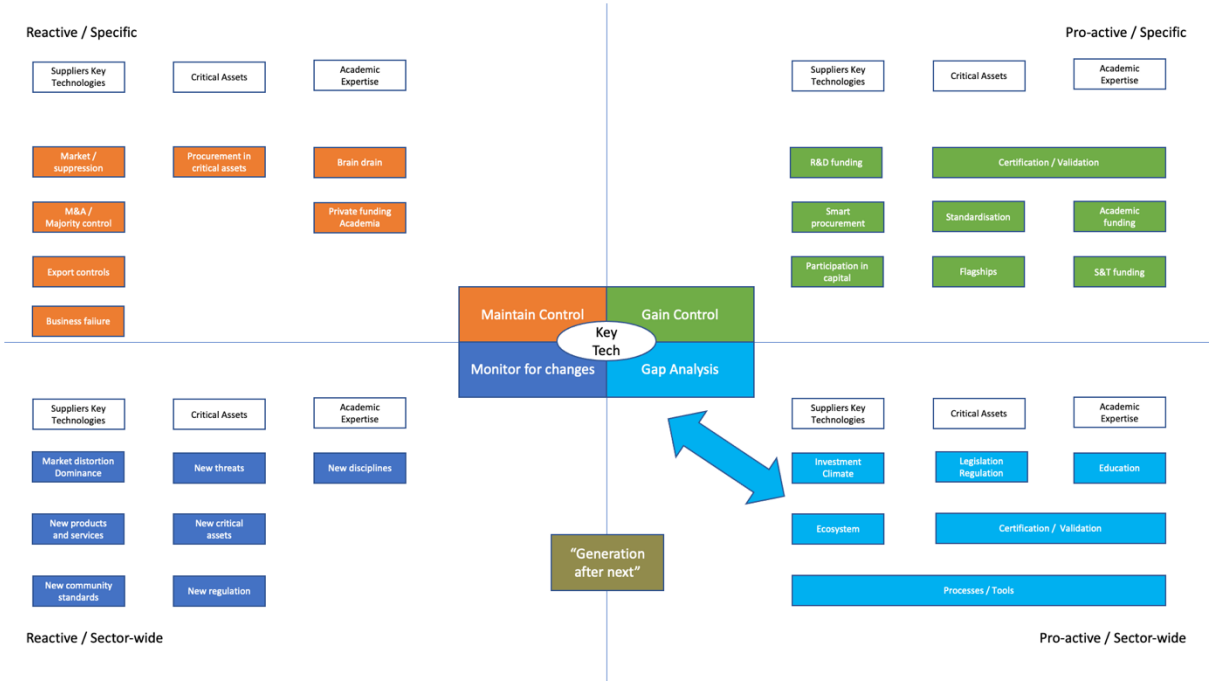
De werking van het Trigger diagram kan worden toegelicht met enkele voorbeelden. Een trigger in het kwadrant links bovenaan is een specifieke situatie waarin een bestaande controle in het gevaar dreigt te komen. Een voorbeeld hiervan is een aangekondigde overname van een unieke leverancier van sleuteltechnologie. Dit observerend, kan er actie ondernomen worden om de controle te behouden.



Een trigger in het kwadrant links beneden kan komen uit een sector-brede relevant evolutie die een nieuwe cyberveiligheidsdreiging (of opportuniteit) kan teweegbrengen. Een voorbeeld hiervan is de ontwikkeling van nieuwe sleuteltechnologieën zoals privacybeschermende gegevensverwerking. Als dit waargenomen wordt, kan proactief actie worden ondernomen door de ontwikkeling en gebruik van deze nieuwe technologie te ondersteunen in de domeinen beschreven in het kwadrant rechts bovenaan. Dit kan eventueel gecombineerd worden met wetgeving en regelgeving (in het kwadrant rechts onderaan). Een voorbeeld is de GDPR.

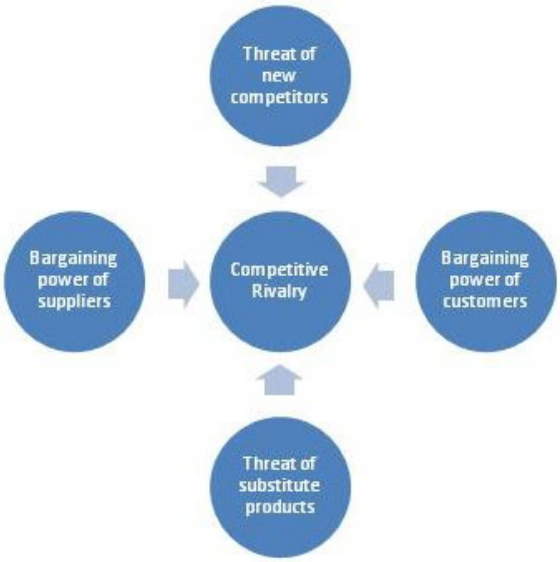


Een laatste voorbeeld is de vergelijkende analyse van werktuigen en wetgeving in andere landen met betrekking tot digitale strategische autonomie. Welke landen doen het anders en beter dan Nederland? Wat doen ze anders en is dat over te zetten naar de Nederlandse situatie en wat moet daar dan voor gebeuren?



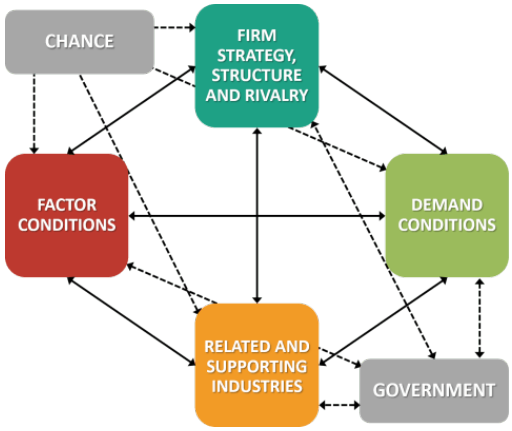
5.5 Porter modellen

Het Five Forces model van Porter verklaart de krachten die inwerken op concurrentie op ondernemingsniveau. Kort gezegd, op bedrijfsniveau legt het uit dat de concurrentie-dynamiek beïnvloed wordt door de macht van leveranciers en klanten, de dreiging van nieuwkomers (die *barriers to entry* moeten overwinnen) en de dreiging van substitutie. Dit model is heel bekend als het gaat over de analyse van strategische concurrentie, dus business strategie.



Figuur 19 Porter Five Forces model (bron: zie bijlage)

Het Porter Diamond-model bevindt zich op een hoger, geaggregeerd, niveau en betreft het concurrentievermogen van een land of industriesector als geheel. Aangezien het op staatsniveau werkt, staat dit model het dichtst bij strategische autonomie. In dit model worden de relaties uitgelegd tussen factor condities (zoals kapitaal en kennis), sleutelkenmerken van het industriële ecosysteem zoals de mate van concurrentie, de vraagzijde op macroniveau, en het grotere ecosysteem van toeleverende industrieën. In dit model past ook de invloed van de overheid. Dit model is toegepast, onder meer door de OESO, voor strategische analyse van industriebeleid in Finland, Mexico en Taiwan.



Figuur 20 Porter Diamond Model (bron: zie bijlage)

De Porter-modellen weerspiegelen echter geen trends op macroniveau zoals in geopolitiek (bijvoorbeeld de rivaliteit tussen de VS en China), maatschappelijke verandering (bijvoorbeeld populisme), leefomgeving (zoals het klimaat). Dit zijn allemaal trends die soevereiniteit aangaan en doorwerken in het Diamond-model, en dan vervolgens leiden tot veranderingen in het model van de Five Forces. Omgekeerd kunnen veranderingen die direct bedrijven of organisaties betreffen (en dus in de Five Forces geanalyseerd worden), zich uitbreiden tot staatskwesties, d.w.z. doorwerken in het Diamond Model en daardoor uiteindelijk strategische autonomie en daarmee soevereiniteit kunnen aangaan. Bijlage 8.3 geeft een korte toelichting van de twee modellen.

5.6 Relevante domeinen, controle en strategische autonomie test

De casebeschrijving zoals ontwikkeld in de trigger- en modellen-analyse leidt tot een aantal domeinen die relevant zijn, zoals technologie-leveranciers, factor condities zoals academische kennis en kritische middelen, en aard van overheidsinkopen. Dit zijn de domeinen om te beschouwen voor mogelijke overheidsinterventie.

Een volgend element in de analyse is 'controle'. De analyse moet een beschrijving opleveren van de verandering - verlies of toename - van controle over vermogen en middelen om de eigen toekomst te kunnen bepalen in de zin van strategische autonomie. Door met betrekking tot controle voldoende specifiek zijn volgen daarmee ook direct concrete doelstellingen voor herstel of versterking van strategische autonomie en cybersecurity.

Waar heeft controle betrekking op waarover en welke soort controle? Categorieën van de middelen en vermogens van strategische autonomie kunnen dit illustreren (zie voetnoot 9):

Intangibles:

- Kennis: braindrain, verplaatsing van O&O naar buitenland (cf: encryptie, AI)
- Vaardigheden: weinig overheidservaring met technologie en beleid combinatie (cf: cloud)
- Organisatie processen/procedures: onmogelijkheid om controleur te controleren (cf: 5G)
- Besluitvormingscultuur: erosie van samenwerking bedrijfsleven – overheid (cf: voormalige taboe op industriepolitiek)
- Randvoorwaarden: voor het deelnemen van buitenlandse bedrijven in de Europese of Nederlandse markt (cf: 5G, EU cloud beleid)
- Politiek: reflectie van prioriteit voor strategische autonomie in de verkiezingsprogramma's van politieke partijen (momenteel: beperkt en impliciet[114]).

Tangibles:

- Financieel: verschuiving van lange-termijn continuïteit naar kortetermijnwinst (case: M&A)
- Personeel: geen aantrekkingskracht voor nieuwe ondernemers door vertrek groot bedrijf (cf: ARM)
- Onderzoeksfaciliteiten: nodige schaalvergroting onmogelijk door M&A wetgeving (cf: klachten van cybersecurityindustrie[115])
- Industriële faciliteiten: outsourcing van industrieketens die kritisch zijn in crisissituatie (cf: computerchips voor onderhoud apparatuur).

Een mogelijk toekomstige stap in deze methodes zou een systematische strategische autonomie test kunnen zijn in het kader van nieuwe wetgeving in de zin van de EU regulatory impact assessment of de Nederlandse Memorie van Toelichting[116].

[114] Bernold Nieuwesteeg, Cybersecurity in de verkiezingsprogramma's TK 2021 (v. 0.3).
[115] Rapport ECIL, European Cybersecurity Industry Leader, https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders
[116] L. Moerel en P. Timmers, ibid.

6 Toepassing en validatie van toetsingskader

Dit hoofdstuk geeft de toepassing van het toetsingskader op enkele specifieke gevallen teneinde te begrijpen waar de aanzet tot overheidsoptreden op het gebied van strategische autonomie en cyberveiligheid vandaan komt.

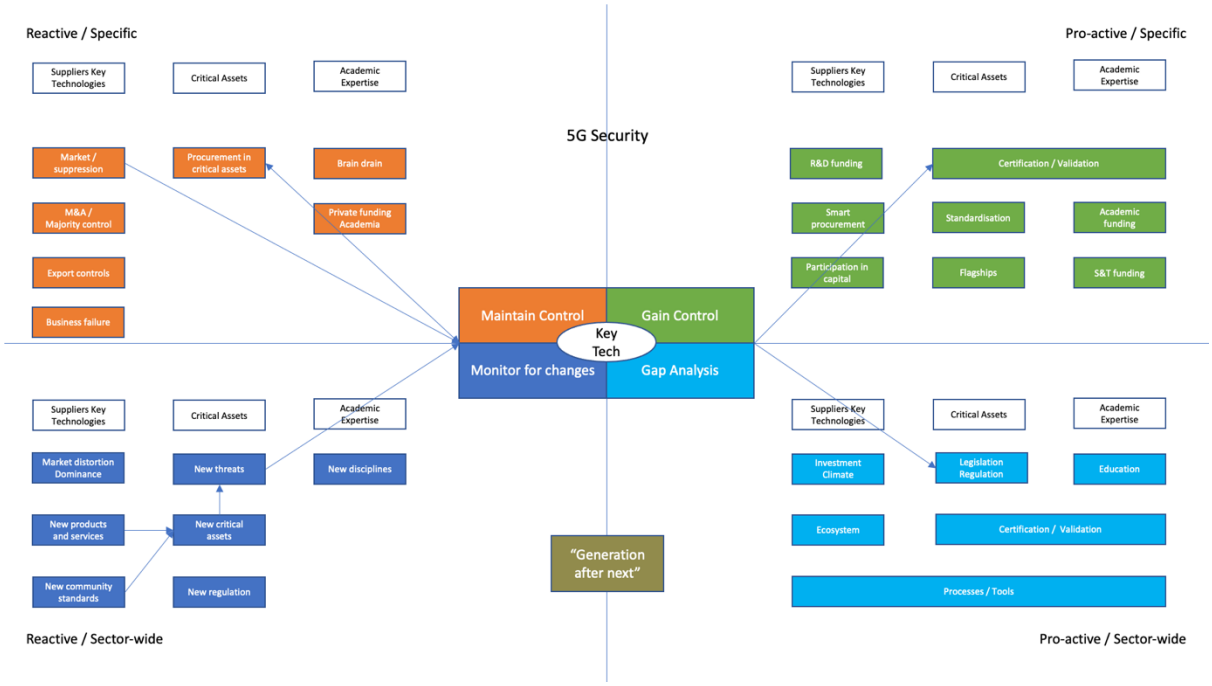
6.1 5G beveiliging

Een belangrijke trigger is in dit geval de druk van de VS om weg te gaan van Huawei als leverancier van telecom appratuur. In het Five Forces diagram verandert dit de aanbodzijde voor de telecom operatoren, het verandert de concurrentiestrijd tussen telecombedrijven, maar maakt ook deel uit van het bredere overheidsbeeld van het industriële ecosysteem voor telecomapparatuur. Een andere aanleiding kan gevonden worden in de eerdergenoemde verklaring van President Macron: "Wij hebben onze soevereiniteit aan de telecomindustrie overgelaten". Ook die past in de relatie tussen overheid en industrie in het industriële het ecosysteem in Porter's Diamond-diagram. Tenslotte zijn triggers die zich meer geleidelijk manifesteren de opkomst van 5G als een nieuwe (sleutel-) technologie.

Indien we deze laatste aanleiding in het trigger diagram bekijken dan starten we links onderaan, bij het ontstaan van nieuwe producten en diensten (5G technologie ontwikkeld door de netwerkproduct fabrikanten) en de ontwikkeling van industriestandaards door de leveranciers. Deze producten en diensten worden opgenomen in nieuwe kritische assets die essentieel zijn voor landsbelang (5G netwerken vervangen bestaande interne bedrijfsnetwerken, internet wordt het bedrijfsnetwerk) en geven daarmee ook aanleiding tot nieuwe cyberveiligheidsrisico's (kwadrant links onderaan).

Terug naar het Trigger Diagram is de observatie dat Europese leveranciers (Nokia en Ericsson) uit de markt geprezen worden naar aangenomen wordt met Chinese overheidssteun (voor Huawei) en dat de kritische telecom infrastructuur operatoren onder andere voor die reden opteren voor de Chinese leverancier. Dat versterkt dan weer de buitenlandse invloed en daarmee verlies van strategische autonomie ofwel controle met betrekking tot die kritische assets.

Als reactie werd er door nationale overheden druk uitgeoefend op telecomoperatoren en werd er een EU 5G Cybersecurity toolbox uitgewerkt die een combinatie inhoudt van wetgeving (kwadrant rechts onderaan) en certificatie/standaardisatie (kwadrant rechts bovenaan) die door de operatoren dient geïmplementeerd te worden.



Een aantal domeinen in het schema werden tot nu toe in dit verband nog niet op een gecoördineerde en geïntegreerde manier toegepast in deze specifieke case. In het bijzonder zijn er (nog) geen maatregelen voor de versterking van de telecomapparatuur industrie in de EU en Nederland via:

- Selectief gebruik van (EU) R&D financiering
- Selectieve aankoop door de overheid
- Flagships als stimulans aan de vraagzijde (vanuit industrie, overheid, defensie)
- Overheids-deelname in het kapitaal van de leveranciers
- Trans-Atlantische samenwerking.

Verder lijkt het raadzaam in de Case van 5G beveiliging om ook meteen "strategisch" verder te kijken dan de huidige horizon en de "Generation after next" op een betere manier aan te pakken. Een samenvatting van het resultaat van de toepassing van het toetsingskader op 5G Security is te vinden in Bijlage 4.

6.2 NIB-richtlijn

De aanleiding (trigger) in dit geval is de herziening van de NIB richtlijn. In het Diamond Model komt die trigger uit het blok overheid ('government' zie Figuur 20). Uit de eerdere analyse is al gebleken dat de van kracht zijnde richtlijn tekortkomingen vertoont. De belangrijkste interventie is een herziening van de wetgeving.

De herziene NIB-Richtlijn is door de Europese Commissie voorgesteld op 16 december 2020 en is nog steeds gebaseerd zijn op risicobeheer in plaats van strategische partnerschapsopbouw voor exclusieve competenties of het nastreven van cyberweerbaarheid als algemeen goed. Ze is slechts in beperkte mate en indirect door strategische autonomie aangestuurd.

De analyse van de marktdynamiek suggereert naar aanverwante bedrijfstakken te kijken om met deze herziening de cyberweerbaarheid als sector te versterken. Dit betreft bijvoorbeeld cyberincident analyse, cyberdefensie/offensive en cyberverzekeringen. In sommige van deze heeft Nederland al een positie, maar in andere moet het ook overwegen soevereine controle te krijgen. Bovendien is de realiteit dat een aantal van de sectoren die onder de (herziene) NIB-richtlijn vallen in hoge mate afhankelijk zijn van buitenlandse leveranciers. Interventie aan de EU overlaten is misschien niet voldoende. Verder is er een kans en ook behoefte aan het versterken van cybervaardigheden, zowel als factor conditie (input) als vraagzijde conditie.

Coherente ondersteunende maatregelen zouden dan kunnen zijn:

1. bevordering van de industriële activiteiten op het gebied van cyber-analyse door middel van co-investeringen, overheidsopdrachten, partnerschappen tussen de industrie en de academische wereld en de overheid, eventueel ook exportbevordering
2. versterking van de vaardigheden op de nieuwe gebieden die onder de NIB herziening vallen (bijv. het opzetten van ISAC's voor de industrie in farmaceutische producten en medische apparatuur en bij de overheid)
3. Het internationaal bevorderen van de risicobeheerbenadering van de herziene NIB-richtlijn, met name voor vertrouwen-bouwende maatregelen ter uitvoering van de VN-normen en waarden in cyberspace.

6.3 e-ID

Het bewustzijn is sterk gegroeid van de risico's van een dominante positie van de internetplatforms ook op het gebied van identificatie – bijv. via Facebook en Google ID. In het Trigger Diagram is deze evolutie zichtbaar in het kwadrant links onderaan. In het Five Forces diagram is dit een trigger die komt uit de aanbodzijde. Die dominantie betekent een aanzienlijk verlies van strategische autonomie. Een andere, zwakkere, trigger is het opkomen van een zelfsoevereine identiteit, hetgeen een substituut product is.

Een derde trigger is de aangekondigde herziening van eIDAS. Dit is, in het Porter Diamond Model, een door de overheid geïnitieerde trigger. Dit biedt een kans om de toetredingsdrempels te verlagen. Dit is van groot belang omdat de overheid als aanbieder van e-ID een laatkomer is, die wordt geconfronteerd met aanzienlijke toegangsbelemmeringen (*barriers to entry)*. Die kans ligt er ook voor *self-sovereign identity* initiatieven.

Om de eIDAS-herziening doeltreffend te maken als een spel-verandering, zal er meer nodig zijn dan een nieuwe eIDAS-wet. Het triggerdiagram suggereert mogelijke andere interventies, maar alvorens daarop in te gaan is de vraag, in het kader van deze studie, of e-ID voldoende

betrekking heeft op cyberveiligheid. Dit is niet in sterke mate het geval voor e-ID op zich, maar duidelijker voor de veiligheidsverzekeringsdiensten (authenticatie van websites, mogelijk attribuut *assurance*) die verwante industrieën en academische vaardigheden hebben die tot op zekere hoogte in Nederland aanwezig zijn. Security assurance diensten zijn echter veel breder dan wat onder eIDAS valt. Voor e-ID is er dus een duidelijke behoefte aan en mogelijkheid om de (digitale) strategische autonomie te versterken, maar interventie moet deel uitmaken van een breder plan dat niet alleen over cyberveiligheid gaat. Binnen dat bredere beleid past ook de recent voorgestelde Digital Markets Act, zelfs al beperkt die zich in deze context tot e-identificatie (zie ook Tabel 1 Recente en verwachte EU-wetgeving hieronder).

6.4 Homomorfe encryptie

Dit is een technologie-trigger. Deze leiden gewoonlijk tot vervangende producten, in dit geval met gevolgen voor de veilige gegevensanalyse door cloudbedrijven. Een korte analyse voor de follow-up van deze trigger is als volgt:

Als we willen dat het nationale concurrentievermogen in de cloud verandert (dat wil zeggen we willen een strategische autonomie kwestie aanpakken), dan moeten we activiteiten in deze vorm van encryptie beschouwen in het Diamond Model. Het is dan relevant om te denken over factor-condities (kennisbasis, investeringen in homomorfe encryptie), een vraagvoorwaarde (bv. overheidsopdrachten), invloed door de overheid (bv. verplichte veilige gegevensanalyse), en inzicht in het gewenste concurrerende industriële ecosysteem (bv. industriële allianties, landschap van fusies en overnames).

6.5 M&A van een strategische autonomie-essentieel bedrijf

Dit zou een hypothetische overname kunnen zijn, bv. een kritische infrastructuur operator, of een overname uit het verleden zoals FOX-IT door NCC. Dit is een typische aanleiding voor de toetreding van nieuwe concurrenten. Zo'n bedrijf kan bijvoorbeeld een fundamentele technologie in handen hebben of een essentiële infrastructuur. Er zijn andere triggers die kunnen komen uit een van de Five Forces. Een eerder voorbeeld is dat Huawei op de markt zou zijn gekomen door prijs-onderbieding.

6.6 EU-beleid en wetgeving

Relevant EU-beleid ontwikkelt zich snel. Hoofdstuk 4 geeft een overzicht waar in dit beleid cybersecurity én strategische autonomie het meest van belang is. In de tabel hieronder wordt beknopt aangegeven welke aandachtspunten nodig zijn, volgens de analyses in deze studie, voor recent beleid uit 2020 of voor beleid dat verwacht wordt voor de eerste helft van 2021[117].

[117] Zie werkprogramma Europese Commissie voor 2020 (update van mei 2020) en voor 2021 (oktober 2020).

Tabel 1 Recente en verwachte EU-wetgeving

Data Governance Act	27 nov 2020	Beperkt relevant voor de combinatie van cybersecurity en strategische autonomie. Vaardigheden bij toeziende overheid. Kans voor ondersteunende industrie (in NL security assurance en EU cloud).
NIB2-Richtlijn	16 dec 2020	zie meer gedetailleerde analyse in sectie 6.1.
Cybersecurity Strategie	16 dec 2020	samenhang van maatregelen voor industrieel ecosysteem, R&D/sleutel-technologieën, cyber-certificering, cyber-weerbaarheid, standaardisatie, cyber & defensie, internationale normen en waarden.
EU-US trans-Atlantische Agenda	2 dec 2020	Consistentie EU-US partnership en Cybersecurity Strategie, White House strategie, middelen multilaterale instrumenten zoals internationale standaardisatie, WTO, samenwerking in sleuteltechnologieën, gezamenlijke agendering van 'global common goods'[118].
eIDAS	Q1 2021	zie meer gedetailleerde analyse in sectie 6.3
AI-aansprakelijkheid in high-risk toepassingen	Q1 2021	Impact van AI voor cyber-incident analyse en response op soevereiniteit, bijv. crisis-verantwoordelijkheid; coherentie met NIB2 Richtlijn; AI-vaardigheden. Kansen én noodzaak voor Nederlandse kennis en industrie.
Horizon Europe, Digital Europe en Connecting Europe Facility	Q1 2020	Werkprogramma's voor 10-20 miljard in EU R&D, toepassingen, samenwerking, en infrastructuur; voor strategische autonomie moeten keuzes consistent zijn met investeringen in startups, opschaling en overheids-aankopen in Nederland en Europa. Zie bijv. homomorfe encryptie, sectie 6.4 en 5G security in sectie 6.1.
Digital Services Act	15 dec 2020	Grote online gatekeeper platforms moeten een risk assessment doen van 'inauthentic' gebruik (bijv., fake nieuws en deep fakes) maar hebben geen eis voor betrouwbare authenticatie zoals wel bepleit[119].
Digital Markets Act	15 dec 2020	Terugnemen van e-ID controle van gatekeeper platforms. Houdt niet in dat nationale of Europese e-ID aangeboden moet worden (wellicht in komende eIDAS herziening?). Ook geen ontkoppeling van trust & assurance services, dus strategische autonomie verbetert slechts deels.

Nog lopend zijn onderhandelingen over EU e-evidence wetgeving die de samenwerking met dienstverleners (bijv cloud providers) moet stroomlijnen om autoriteiten snelle instrumenten bieden om elektronisch bewijs te verkrijgen. Het valt nog te bezien of er een trans-Atlantische overeenkomst komt die de brug slaat tussen de VS Cloud Act en de EU E-Evidence wetgeving.

[118] Als de Biden administratie consistent meer openheid voor multilateralisme toont zal er ruimte komen om wereldwijd gemeenschappelijk belang in cybersecurity te promoten, hetgeen voor Nederland van bijzonder relevant is.
[119] Bart Jacobs, iBestuur online, 9 dec 2019, https://ibestuur.nl/weblog/teken-tegen-nepnieuws en 24 dec 2020, https://ibestuur.nl/podium/ontwakende-europese-digitale-soevereiniteit

6.7 Andere 'trigger' cases

Andere voorbeelden van triggers zijn:

- Een fundamentele technologie wordt overgenomen door één unieke gebruiker (Europees of niet-Europees). Dit beïnvloedt de factor omstandigheden in het Diamond Model. Een voorbeeld zou quantum-encryptie kunnen zijn.
- Overname van een 'kritisch' bedrijf.
- Onthulling over spionage of surveillance, zoals de Snowden of Cambridge Analytica cases.
- Ransomware in ziekenhuizen die op grote schaal op een kritisch moment de continuïteit van gezondheidszorg in gevaar brengen (bijv. tijdens de COVID-19 crisis).
- Het steeds oplaaiende debat over de risico's van achterdeuren voor legale interceptie.
- Kritische momenten voor keuzes in fundamentele/kritische wetenschap en technologie. Zie hierboven voor de nakende politieke besluitvorming over de besteding van de miljarden van het EU R&D Horizon Europe programma. Daarnaast het recente White House Critical & Emerging Technologies[120] en President Xi Jinping's 2025 plannen.

De analysemethode is ook toe te passen op grotere uitdagingen. Hier drie voorbeelden.

6.7.1 Bescherming van gevoelige overheidsinformatie.

Dit is van direct belang voor de overheid van justitie tot defensie, maar ook bijvoorbeeld voor de privacy van individuele burgers en vertrouwen in de rechtsstaat. Dit relateert aan de eerdergenoemde analyses van cloud, (homomorfe) encryptie, deep security, en ook aan AI; gezien de infrastructurele aspecten van informatie- en data-beheer is hier ook de Galileo ervaring van belang, en daarmee ook het industriële ecosysteem. Dit is een case waar internationaal het 'Brussels effect'[121] van toepassing kan zijn, de hefboomwerking van EU-wetgeving, en ook het omgaan met extraterritoriale claims van vreemde mogendheden (cf Cloud Act, Schrems II).

6.7.2 Spionage en stelen van intellectuele eigendom.

Dit is van eminent direct belang, zie de eerdergenoemde dreigingsanalyse en de waarschuwingen van de Cybersecurity Coördinator en het CSBN. Dit relateert aan de herziening van de NIS Richtlijn, 5G security, EU-regels omtrent het gebruik van Europese O&O-financiering, Foreign Direct Investment Regulation en M&A triggers en ook aan de economische kansen om een security assurance industrie te stimuleren. Ook dit heeft een sterke internationale dimensie (norms and values of state behaviour).

6.7.3 Online desinformatie en fake news

Dit is van groot belang voor het functioneren van de democratie maar ook voor de effectiviteit van de staat, publieke sector en het bedrijfsleven in het uitvoeren van beleid (bijv. gezien anti-5G en anti-vax campagnes).

[120] Ibid.
[121] Anu Bradford, https://www.law.columbia.edu/faculty/anu-bradford

7 Aanbevelingen

7.1 Strategische autonomie is cruciaal in cyberveiligheid

Strategische autonomie is in toenemende mate essentieel in cybersecurity en vereist een **voortdurende aandacht en betrokkenheid tot op het hoogste niveau**. Dit is op het moment onvoldoende het geval, met een sluipende erosie van soevereiniteit tot gevolg. Steeds grotere digitale afhankelijkheid, nieuwe technologieën en marktspelers, nieuwe dreigingen zijn ons aan het inhalen. Indien we reageren is het vaak te laat. Dit door laten gaan is niet verantwoord.

Er moet én kan **nu** actie genomen worden om politiek, beleid en uitvoering bewust te maken, instrumenten aan te reiken, en praktisch te handelen. Nederland dient daarbij op te trekken met partners in de EU en internationaal.

7.2 Proactieve en integrale aanpak

Een ongecoördineerde en gefragmenteerde aanpak zet weinig zoden aan de dijk. Samenhang van beleid en expliciete prioritering zijn een noodzaak. Dit is al meermaals geconstateerd, maar waar deze studie van eerdere adviezen verschilt is dat deze strategische autonomie als een noodzaak en prioriteit voor cyberveiligheid positioneert en een praktisch toetsings- en handelingskader geeft. Bovendien geeft de studie een groot aantal relevante en actuele onderwerpen om nú aan de slag te gaan.

Onze eerste aanbeveling betreft strategische governance:

1. Organiseer het cybersecurity-beleid als een **continue, proactieve, en geïntegreerde activiteit;**
2. Gebruik hierbij de voorgestelde gemeenschappelijke methodes en het **toetsingskader;**
3. Maak een **prioriteit** van strategische autonomie in cybersecurity,
4. Definieer **doelstellingen** voor de **strategische controle** in cybersecurity, zowel in het algemeen en per specifieke case. Het is in ieder geval prioriteit om de strategische controle in cybersecurity te versterken ten aanzien van:
   - Cloud: privacybeschermend, veilig voor bedrijfsinformatie en afgeschermd van overheidsinterventie van derde landen, rekening houdend met GAIA-X en EU-beleid
   - Veilige communicatie: lands-brede, robuuste en veilige netwerken voor staat, bedrijven en burgers (waaronder security van 5G en de volgende generatie, en IoT)
   - Deep security (geavanceerde digitale beveiligingsservices en -oplossingen): langdurige (ook, post-quantum) bescherming van gevoelige informatie.

Verder is voor het bepalen van doelstellingen een lijst van **sleuteltechnologieën** een belangrijke hulp.

7.3 Uitbouwen van bestaande sterktes

Er zijn in Nederland al heel wat sterktes aanwezig om cyberveiligheid in relatie tot strategische autonomie op een goede manier aan te pakken. Deze zijn onder meer de strategische insteek van de CSR, de operationele effectiviteit van de NCSC, de dreigings-inzichten van AIVD, de publiek-private sterkte van de Defensie Industrie Strategie, de EZK voorstellen voor een nieuwe innovatie- en kennisimpuls, de academische reputatie, en het internationale gezag van Nederlandse cyber-diplomatie.

Onze tweede aanbeveling is dat bouwend op bestaande sterktes, meerdere departementen, instanties en stakeholders gaan **samenwerken op strategisch en beleids-operationeel niveau**, mogelijk met verdere versterking, en met sturing vanaf het hoogste niveau.

De identificatie van die relevante partijen, hun precieze rol, en organisatorische gaten om op termijn op te vullen was geen onderdeel van deze studie. Onze analyse geeft wel als derde aanbeveling **belangrijke aandachtpunten** aan per beleidsterrein:

- Economisch beleid en uitvoering: in het bijzonder investeringen, FDI- en M&A voorwaarden, innovatie-ecosysteem, industrieel/logistieke flagships, concurrentiebeleid, markttoegang, standaardisering en industriële samenwerking, participaties en bescherming van “kroonjuwelen” tegen overnames
- Kennisbeleid en uitvoering, in het bijzonder ondersteuning van sleuteltechnologieën, interactie met een versterkt ecosysteem van innovatie en markt, pre-standaardisatie
- Defensiebeleid en uitvoering, in het bijzonder samenhang van defensie industriebeleid met economisch, kennis, en intelligence beleid, uitbreiding van de slimme aankoopmethodes naar de andere veiligheidsdomeinen
- Intelligence over dreigingen, in het bijzonder inzichten in de dreiging van erosie van waarden en normen, van verlies van intellectuele eigendom en gevoelige overheidsinformatie en van mogelijke "black swan" events
- Operationele cyberweerbaarheid en respons, in het bijzonder uitbreiding naar een landsbrede aanpak, nauwere samenwerking met de telecomoperatoren en strategische interactie met de andere functies
- Beleid en uitvoering betreffende criminaliteit en publieke veiligheid, in het bijzonder waar deep security in cloud, AI en het functioneren van en vertrouwen in de rechtsstaat raakt
- Beleid en uitrol van digitale overheidsdiensten en overheidsaankopen in het bijzonder waar het cybersecurity én strategische autonomie betreft (bijv. e-ID)
- EU en internationaal, in het bijzonder samenhang Nederland-EU, bijdrage aan huidige en nabije EU-beleid, en gebalanceerde aanpak van strategische autonomie voor een Nederland dat ‘open naar de wereld’ is en blijft.
- Strategisch advies, agendering, prospectieve analyse, onafhankelijke “controle op de controleurs”, en bredere implicaties voor economie, maatschappij en democratie.

Andere beleidsterreinen zullen vanzelfsprekend ook een rol spelen bijv. belastingbeleid om Nederland als aantrekkelijk startup land te positioneren zoals door risico investeringen op een competitieve manier te belasten (stock options, angel investment).

Tenslotte kan een lijst van sleutel-technologieën als rode draad gebruikt worden voor de ondersteunende en coördinerende activiteiten van de gewenste samenwerking.

7.4 Een praktische aanzet

Een concreet resultaat van deze studie is het **toetsings- en handelingskader**. De aanbeveling is met dit kader **praktisch en zonder uitstel aan het werk te gaan**. Drie voorbeeldthema’s om met het toetsingskader en actuele ‘triggers’ de case analyse uit te voeren en samenhang van beleid te illustreren zijn:

5G security: er is een concreet beleidskader, namelijk de Europese 5G Security Aanbeveling en de Nederlandse telecom wet. Echter, de case analyse laat zien dat het 5G-security innovatie-ecosysteem verder te versterken is. Dit kan o.m. door investeringsstimulans om

kennis in innovatie om te zetten, versterking van de samenwerking tussen vraag en aanbod met flagships in Nederland (bijv. logistiek, gezondheid, industrie). Er is ook meer actieve deelname vereist in internationale 5G/6G standaardisatie initiatieven en een duidelijker EU/Nederlands beleid t.o.v. oneerlijke overheidssteun in China. Naast de case analyse in sectie 6.1 geeft bijlage 8.4 een matrix van maatregelen.

Defensie – civiel: de Defensie Industrie Strategie met daarbij de aanzet tot sleutel-technologieën identificeert concrete instrumenten. Dit zijn o.m. innovatie ondersteuning, slimme aankoopmethodes, het gebruik van de CODEMO-regeling, en industriële participaties. Landen als Frankrijk, het VK en VS gebruiken defensiestrategie als aanjager voor zowel cybersecurity als strategische autonomie. Zoals aangeven, is concretisering gerelateerd aan kennisbeleid (bijv. deep security, AI), economische beleid (bijv. aankoop van innovatie in security assurance), en aan intelligence. Sommige instrumenten en processen van de Defensie Industrie Strategie kunnen veralgemeend worden naar het bredere domein van veiligheid en cyberveiligheid en dragen daarmee bij aan verder inzicht over overheidsdeelname in de cybersecurity market in termen van risicokapitaal, overheid als launching customer, overheidsaankoop van R&D, en een sectorale strategie als drijver.

EU – Nederland: het Europese beleid in cybersecurity en strategische autonomie is in stroomversnelling. Nederland zal een actieve of zelfs proactieve rol moeten en kunnen spelen. Voor cybersecurity en strategische autonomie zijn de top-aandachtspunten vanaf begin 2021: de NIB2 Richtlijn waarbij Nederland op een landsbrede benadering in moet zetten, de komende herziening van de eIDAS Richtlijn inclusief de relatie met de recente Digital Markets Act, het cloud beleid, en het komende AI-beleid voor high-risk toepassingen. In al deze gevallen, zoals in meer detail geïllustreerd in de case analyses van de NIB Richtlijn en de eIDAS Verordening, is het nodig verdere samenhangende actie te ondernemen. Onder meer is dit bewustzijn vergroten, trust/assurance services stimuleren en deels in eigen hand te houden, en inzicht ontwikkelen in de impact van AI in cybersecurity op democratische controle over rechtsstaat en economie. Er is ook duidelijk behoefte aan een beter investeringsklimaat om door te kunnen groeien, en aan aanpassing van concurrentiewetgeving aan de geopolitiek.

Deze drie voorbeelden zullen een impuls geven om andere situaties te analyseren (zie bijv. sectie 6.7). In het bijzonder kan dit helpen om **technologiebeleid** te formuleren dat vanuit strategische autonomie en cybersecurity perspectief van groot belang en ook hoognodig is.

Deze werkwijze kan ook verdere strategische analyse en samenhang in Nederland voeden teneinde **grote uitdagingen voor de cyber-bescherming van maatschappij, economie, en democratie** aan te pakken. Dit zijn uitdagingen zoals de bescherming van gevoelige overheidsinformatie, industriële cyber-spionage, en online disinformatie en ondermijning van democratie.

Tenslotte, de studie bevat een verscheidenheid aan inzichten (relevante dreigingen, nieuwe evoluties in fundamentele technologieën, gap analysis met andere landen) die voeding tot reflectie en handelen kunnen geven. Het advies is dan ook om de **studie ruim te verspreiden** onder de relevante departementen van de ministeries en relevante stakeholders.

8 Bijlages

8.1 Bijlage 1: cybersecurity startups: successen en mislukkingen

Succesverhalen (eenhoorns) met weinig of geen EU-financiering voor onderzoek en ontwikkeling:
Collibra, opgericht in 2008 in Brussel, heeft in totaal 347 miljoen USD opgehaald. Alle middelen die latere rondes werden aangetrokken waren afkomstig uit de VS. 700 werknemers.
Elastic, opgericht in 2012 in Amsterdam, IPO in 2018. Heeft Endgame overgenomen in 2019, een Amerikaans EDR-bedrijf. Alle middelen kwamen van de VS. 2000 werknemers.
Avast, opgericht in 1988 in Praag, IPO in 2018. 2000 werknemers.
F-Secure, opgericht in 1988 in Helsinki, IPO in 2002. 1700 werknemers.
Darktrace, in 2013 in Cambridge opgericht, heeft in totaal 230 miljoen USD opgehaald uit Britse en Amerikaanse middelen. 1300 werknemers.
Privatar, in 2014 in Londen opericht, heeft 150 miljoen USD opgehaald in het VK en de VS, maar ook van industriële partijen (ABN/AMRO, SalesForce, HSBC, CITI)

Gevallen met aanzienlijke EU-financiering voor onderzoek en ontwikkeling:
Guardtime, opgericht in 2007 in Tallin, heeft in 2019 corporate funding opgehaald (CH). Meer dan 5 miljoen euro aan EU-onderzoeksfinanciering. Actief in cryptografische authentificatie en integriteit. Gecertificeerde leverancier van Amerikaanse DOD-leveranciers (Lockheed). Nog geen VC- of PE-middelen. 150 werknemers.
Gemalto, opgericht in 1979, werd in 2019 overgenomen door Thales. Bijna 6 miljoen Euro aan EU-onderzoeksfinanciering. Sterke technologieportefeuille in digitale identiteit en veiligheid (beveiliging van betalingen, mldmetrische gegevens, grensbeheer, IOT, mobiel, eSIM, betrouwbare ID). 15.000 werknemers.

Kleine ondernemingen met fundamentele technologie en beperkte durfkapitaalfinanciering of EU-financiering voor onderzoek:
Utimaco, opgericht in 1983 in Duitsland. VC-ronden in 2005 (DE) en 2013 (DE, LU). Overgenomen door EQT in 2017. Produceert HSM-modules, “root of trust” infrastructuur en apparatuur voor legale interceptie. Werkt aan quantum-veilige HSM in samenwerking met ISARA (VS) en Microsoft[122]. Utimaco verwierf in 2018 de sleutelbeheerfirma Geobridge (VS). 170 werknemers.

Een paar opmerkelijke tekortkomingen op het gebied van "controle" door de EU:
Deepmind, In 2010 in Londen gecreëerd en in 2014 door Google geabsorbeerd
ARM, opgericht in 1990 in Cambridge, IPO in 1998, werd in 2016 uit de markt genomen en opgekocht door private equity (Softbank) en werd in 2020 geabsorbeerd door nVidia.
Skype, opgericht in 2003 in Estland, geabsorbeerd door Microsoft in 2011.
Virustotal, opgericht in 2004 in Spanje, geabsorbeerd door Google in 2012.
Sophos, opgericht in 1985 in het Verenigd Koninkrijk, overgenomen door Thoma Bravo (VS)
IDEMIA (Sagem, Morpho, Safran), opgericht in 1982 in Frankrijk, overgenomen door Advent (VS) in 2017. Produceert gezichtsherkenning, biometrische identificatie voor financiële diensten, grenscontrole en toegangscontrole. VN-project voor identiteit aan iedereen in 2030. Bezorgdheid over biometrische gegevens en het gebruik van de apparatuur in digitale surveillance[123].

[122] https://hsm.utimaco.com/solutions/applications/post-quantum-crypto-agility/
[123] https://www.amnesty.org/download/Documents/EUR0125562020ENGLISH.PDF

8.2 Bijlage 2: Legende van de domeinen in het Trigger Diagram

Eerste kwadrant – maintain control: sleuteltechnologie waar controle dreigt verloren te gaan

Market/suppression: een kritische leverancier van sleuteltechnologie die uit de markt gedreven dreigt te worden door concurrentie waar geen controle over bestaat. Case: Europese cloud leveranciers, 5G.

Business failure: een kritische leverancier van sleuteltechnologie die dreigt failliet te gaan.

M&A/majority control: een kritische leverancier van sleuteltechnologie waar de controle verloren dreigt te gaan door een overname. Case: ARM

Export control: kritische technologie die dreigt uitgevoerd te worden naar landen of bedrijven waar dat niet wenselijk is vanuit strategisch perspectief.

Procurement in critical assets: aankoop van belangrijke componenten in een kritische infrastructuur waar overwogen wordt om die "extern" aan te schaffen. Case: aankoop 5G apparatuur.

Brain drain: verlies aan sleutel talent in academia die noodzakelijk zijn om een onafhankelijk advies te leveren over de goede werking van specifieke sleuteltechnologie.

Private funding academia: mogelijk verlies van controle door vreemde investering of sponsoring van academia, die noodzakelijk zijn om een onafhankelijk advies te leveren over de goede werking van specifieke sleuteltechnologie. Case: Huawei en de UvA, VU Amsterdam.

Tweede kwadrant – gain control: sleuteltechnologie waar controle over kan bekomen worden in nieuwe domeinen of wanneer zich een opportuniteit voordoet

R&D funding: financiering van ontwikkeling van nieuwe sleutel technologie door bedrijven waar controle over bestaat

Smart procurement: geprivilegieerde aankoop van sleuteltechnologie van bedrijven waar controle over bestaat (uitzonderingen op openbare aanbestedingen, exploitatie voorwaarden, "smart buyer", "smart specifier", "smart developer" en "launching customer").

Participation in capital: overheidsdeelname in het kapitaal van bedrijven die sleuteltechnologie produceren (golden share, controling stake, controling term sheets). Case Kuka.

Certification: uitbouw en financiering van certificatie schema's die het voor kritische infrastructuur operatoren mogelijk maakt of betrouwbare oplossingen aan te schaffen. Case encryptie, Intel SGX.

Standardisation: actieve deelname in de standardisatie en inter-operabiliteit van sleuteltechnologieën

Academic expertise: uitbouw en bestendiging van de capaciteit een onafhankelijk advies te leveren over de goede werking van specifieke sleuteltechnologie. Case encryptie.

Flagships: het opzetten van grootschalige infrastructuur die kritische diensten levert. Case Galileo.

Derde kwadrant - gap analysis: generieke ondersteunende maatregelen ontwikkelen uitgaande van een analyse van hoe het elders succesvol gebeurt

Investment climate: het creëren van en wettelijk kader dat risico investeringen en ondernemerschap bevordert (bv stock options, hire/fire). Case Zwitserland.

Ecosystem: het faciliteren van een ecosystem dat starters helpt en stimuleert (inventory of funds, Angels, network of entrepreneurs). Case Verenigde Staten

Processes/Tools: Het definiëren en implementeren van processen en hulpmiddelen die digitale autonomie ondersteunen. Case VS en UK, In-Q-Tel, Darpa, Defensie strategie, selectief aankoopbeleid, exploitatievoorwaarden, lijst van sleuteltechnologieën.

Legislation / Regulation: aanpassingen maken in de wetgeving om strategische autonomie te bevorderen. Bv. uitzonderingen voor overheidsopdrachten, concurrentie politiek (Duitsland Kuka)

Certification / Validation: infrastructuur en processen om certificatie te bevorderen. Case ENISA

Education: opleiding en begeleiding van ondernemerschap / stages

Vierde kwadrant – monitor for changes: prospectief onderzoek naar belangrijke wijzigingen in de sector (technologie, assets) en dreigingen

Market distortion / Dominance: evoluties in de markt die aanleiding zouden kunnen geven tot ongecontroleerde dominantie. Case hyperscalers, Intel SGX.

New products and services: nieuwe producten/ diensten met een cybersecurity impact. Case GPS.

New community standards: industriestandaarden in een relevant domein. Case Confidential computing.

New threats: nieuwe types van cyberdreiging waar onvoldoende bescherming voor bestaat. Case ransomware, disinformation.

New critical assets: het gebruik van nieuwe infrastructuur in kritische domeinen. Case: cloud, 5G.

New regulation: nieuwe wetgeving die een cybersecuritycomponent bevat. Case GDPR, eIDAS.

New disciplines: nieuwe wetenschappelijke disciplines die mogelijks een cybsecurity toepassing hebben. Case homomorfe encryptie, differentiële privacy, multi-party computation.

8.3 Bijlage 3: Porter modellen

Michael Porter ontwikkelde in de jaren '80-'90 twee veelgebruikte modellen[124]. Het eerste, het Five Forces model is bedoeld om concurrentiekrachten analyseren om bedrijfsstrategie te kunnen ontwikkelen. Een uitstekende uitleg is in de 2008 Harvard Business Review[125].

Een korte beschrijving van de hoofdelementen, uit de genoemde referentie is:

Dreiging van nieuwkomers: nieuwkomers brengen nieuwe capaciteit, zetten prijzen en investeringen onder druk

Machtige leveranciers houden meer waarde voor zichzelf door prijzen op te drijven, beperken kwaliteit, of hevelen kosten over naar de afnemers.

Machtige kopers houden meer waarde voor zichzelf door prijzen te drukken, eisen meer kwaliteit of meer service, en spelen leveranciers tegen elkaar uit.

Dreiging van substituten: deze kunnen het product vervangen door dezelfde functie op een andere wijze te realiseren.

Rivaliteit tussen de bestaande concurrenten: kan allerlei vormen aannemen, zoals kortingen, advertising, nieuwe producten, en verbetering van dienstverlening.

Het tweede model is bedoeld om op landsniveau de nationale concurrentiekracht te analyseren. Een uitleg is in de 1990 Harvard Business Review[126]. Een korte beschrijving van de elementen is, uit de gegeven referentie is:

Factorcondities. De positie van het land wat betreft productiefactoren, zoals geschoolde arbeidskrachten of infrastructuur, die nodig zijn om te concurreren in een bepaalde bedrijfstak.

Vraagvoorwaarden. De aard van de vraag op de thuismarkt naar het product of de dienst van de branche.

Gerelateerde en ondersteunende industrieën. De aan- of afwezigheid in het land van toeleveringsbedrijven en andere aanverwante bedrijfstakken die internationaal concurrerend zijn.

Bedrijfsstrategie, structuur en rivaliteit. De omstandigheden in de natie die bepalen hoe bedrijven worden opgericht, georganiseerd en beheerd, evenals de aard van binnenlandse rivaliteit.

De modellen laten allereerst toe om fenomenen te benoemen en te classificeren zoals de macht van leveranciers (voor individuele bedrijven) of de factoren die input zijn voor een internationaal concurrerende industriesector (nationale analyse). Ze laten ook toe om de dynamiek van krachten en factoren te beschrijven, in een 'narrative'. Het zijn geen wiskundige modellen.

[124] https://www.isc.hbs.edu/competitiveness-economic-development/frameworks-and-key-concepts/Pages/default.aspx
[125] https://www.isc.hbs.edu/strategy/business-strategy/Pages/the-five-forces.aspx
[126] https://hbr.org/1990/03/the-competitive-advantage-of-nations

8.4 Bijlage 4: Voorbeeld van maatregelen vs domeinen (5G-Security)

De toepassing van het toetsingskader op 5G-security zoals beschreven in sectie 6.1 leidt tot een matrix van maatregelen en domeinen:

Domein / Strategische Autonomie	Trigger / Maatregel	Factor condities			Vraagzijde conditions	Industrie strategie, structuur, rivaliteit	Overheid
		Technologie verandering	*R&D investering*	*Standaardisatie processen*	*Voorwaarden voor kopers*	*Overheidssteun China*	*Druk door VS; Nationale veiligheid; Markt toegang*
Randvoorwaarden	***Security eisen***				EU 5G Toolbox NL Telecom Wet		EU 5G Toolbox
	Markt toegang			ENISA specificaties			ICT security certificatie (Cyber Act)
	Overheids-aankopen				EU 5G sectoral flagships? 5G in Defensie?		
Financieel	***Kapitalisatie door 'like-minded'***					Overheids-deelname?	
Kennis / R&D faciliteiten	***EU R&D***	Meer EU innovatie naast EU R&D?	Horizon Europe funding: 1) exclusieve deelname? 2) patent-protected?				
Industriële faciliteiten	***Standaardisatie***			Standaardisatie als prioriteit?			
Politiek, Beleid, Organisatie	***Strategie***						EU-US strategie t.o.v. CN? ENISA / NCSC dreigingslandschap

8.5 Bijlage 5: auteurs

Prof Dr Paul Timmers

Paul Timmers is Adjunct Professor at European University Cyprus, visiting professor at Rijeka University, senior advisor to EPC Brussels, board member of Digital Enlightenment Forum and of the Estonian eGovernance Academy supervisory board. Previously he was research associate at Oxford University for cybersecurity and digital transformation and Director at the European Commission dealing with EU legislation and funding for cybersecurity, digital health, smart cities, e-government. He was cabinet member of European Commissioner Liikanen, manager in a large ICT company, and co-founded an ICT start-up. Physics PhD from Nijmegen University, MBA from Warwick University, EU fellowship at UNC Chapel Hill, and cybersecurity qualification at Harvard. Contact: paul.timmers@iivii.eu.

Freddy Dezeure, MSc

Freddy Dezeure graduated from the KUL in Belgium, with a master of science in engineering in 1982. He was CIO of a private company from 1982 until 1987. He joined the European Commission in 1987 where he held a variety of management positions. He founded the EU Computer Emergency and Response Team (CERT-EU) in 2011 and managed it until May 2017. He is an Independent Strategic Advisor in cybersecurity and cyber-risk management and a Board Member and Advisor in several high-tech companies. He is also leading the EU ATT&CK Community.

Contact: contact@freddydezeure.eu.