Defence, Safety & Security
Kampweg 55
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77

TNO-rapport

TNO 2022 R10843

Aanpak voor het vaststellen van interventienoodzaak en handelingsperspectief ten aanzien van strategische autonomie op cybersecurity

Datum	9 mei 2022
Auteur(s)	T.C.C. van Schie MA Y.N. Kamphuis MA M. Rademaker (HCSS) L. Faesen (HCSS) W.C.R. Verdaasdonk Dr. M.P.W. van Berlo
Aantal pagina's	43 (incl. bijlagen)
Aantal bijlagen	3
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	Strategisch autonomie cybersecurity
Projectnummer	060.49275

Managementuittreksel

Titel :	Aanpak voor het vaststellen van interventienoodzaak en handelingsperspectief ten aanzien van strategische autonomie op cybersecurity
Auteur(s) :	T.C.C. van Schie MA, Y.N. Kamphuis MA, M. Rademaker (HCSS), L. Faesen (HCSS), W.C.R. Verdaasdonk, Dr. M.P.W. van Berlo
Datum :	9 mei 2022
Opdrachtnr. :	060.49275
Rapportnr. :	TNO 2022 R10843

Nederland is een van de meest gedigitaliseerde landen wereldwijd. Daarmee is de Nederlandse samenleving ook steeds meer afhankelijk geworden van een goed functionerende digitale infrastructuur. Strategische autonomie wordt door staten en de EU nadrukkelijk verbonden aan de borging van publieke waarden en grondrechten. In Nederland zijn tot op heden op het gebied van strategische autonomie op cybersecurity nog geen nationale doelstellingen en ambities vastgesteld. Een belangrijke reden hiervoor is dat het een uitdaging is om integraal cybersecurity ontwikkelingen te duiden in de context van autonomie. Daarnaast vindt een dergelijk beschouwing op cybersecurity ontwikkelingen nog plaats vanuit verschillende departementen. De uitkomsten van de samenwerking tussen de projectgroep (HCSS en TNO) en verschillende ministeries is een instrumentarium dat concrete ondersteuning biedt bij het bepalen van de noodzaak van strategische autonomie op cybersecurity en van het handelingsperspectief en de instrumenten die hieraan bijdragen.

In het instrumentarium staat het stroomschema ‘Strategische Autonomie Cybersecurity’ centraal. Ondersteunend aan dit instrument zijn opgeleverd een RACI-Matrix, een Scorekaart, een Handleiding voor het instrumentarium, en een informerende video. Het stroomschema bestaat uit twee delen, opgebouwd uit een serie van vragen. Deel 1 dient om te kunnen concluderen of er een noodzaak is om de strategische autonomie op cybersecurity te borgen. Indien dat het geval is kan deel 2 worden gebruikt om keuzes te maken uit instrumenten die hieraan bijdragen. Hiermee ontstaat zicht op het handelingsperspectief. Om het gebruik van het instrumentarium te ondersteunen, is een handleiding ontwikkeld. Aan de hand van deze handleiding wordt de gebruiker in een logische volgorde stap voor stap door het stroomschema geleid en gevraagd om inschattingen, antwoorden, inzichten en verantwoordelijkheden vast te leggen.

Om de toepassing van het instrumentarium gestructureerd en geharmoniseerd in een interdepartementale context mogelijk te maken, is het belangrijk om een systeemverantwoordelijk departement te identificeren. Het is goed om de vragen door verschillende departementen in te laten vullen: sommige vragen passen van nature goed bij de expertise van een specifiek departement, maar bij andere vragen wil je juist verschillende perspectieven van diverse departementen en actoren krijgen. Aan de hand van het stroomschema en de RACI-Matrix kan gezamenlijk

een beleidsnotitie worden opgesteld op basis van de diverse separate notities van de betreffende departementen. Het is een goede werkwijze om tot een goed onderbouwd, gezamenlijk en goed gestructureerd beleidsadvies te komen dat als basis gebruikt kan worden om gecoördineerd de voorgenomen interventies uit te voeren.

Op basis van dit onderzoek worden de volgende **conclusies** getrokken:

1 De noodzaak en meerwaarde van een gezamenlijk interdepartementaal proces om de noodzaak van strategische autonomie (en in het bijzonder op cybersecurity) te bepalen, wordt duidelijk erkend.

2 Het instrumentarium wordt ervaren als een waardevolle toevoeging voor de verdere discussie en een grote vooruitgang ten opzichte van eerder ontwikkelde instrumenten. Het biedt concretere handvatten voor en een helder beeld van een eventueel handelingsperspectief en zal doorontwikkeld moeten worden.

3 De RACI-insteek faciliteert een eenduidige verdeling van rollen en verantwoordelijkheden. Dit instrumentarium helpt bij het toewerken naar een eenduidige *whole of government* benadering.

4 Dit instrumentarium bevordert het bij elkaar brengen van de versnipperde kennis en belangen van de departementen om zo tot een weloverwogen beslissing voor strategische autonomie te komen. Hierdoor kunnen prioriteiten worden gesteld over de noodzaak en haalbaarheid van het zekerstellen of de versterking van de strategische autonomie op cybersecurity.

De volgende **aanbevelingen** worden gedaan:

1 Ontwikkel een *forward looking capacity*, of monitoringsfunctie en richt deze in binnen de Rijksoverheid; gebruik hiervoor ondersteuning van kennisinstellingen. Dit kan bijdragen aan de ontwikkeling van een strategische cultuur, waarbij er niet alleen maar reactief wordt opgetreden maar ook preventief wordt gehandeld op (middel)langere termijn.

2 Hanteer een eenduidig format voor de beleidsnotitie die volgt uit het toepassen van het instrumentarium waardoor de gezamenlijke interpretatie en beoordeling wordt verbeterd en de verantwoording vereenvoudigd.

3 Ontwikkel een digitale versie van het instrumentarium om de toepassing te vergemakkelijken en alle losstaande onderdelen te integreren in één applicatie.

4 Implementeer het instrumentarium en zet het daadwerkelijk in conform het voorgestelde interdepartementale proces.

5 Pas dit instrumentarium regelmatig aan op basis van ervaringen. Maak de inzet en verdere ontwikkeling van dit instrumentarium onderdeel van de nationale cybersecurity strategie.

Inhoudsopgave

1 Achtergrond

1.1 Probleemstelling

Nederland is een van de meest gedigitaliseerde landen wereldwijd. Daarmee is de Nederlandse samenleving ook steeds meer afhankelijk geworden van een goed functionerende digitale infrastructuur. Digitalisering is de afgelopen decennia de drijvende kracht geweest achter economische groei en wereldwijde integratie. Cybersecurity is cruciaal om dit te bewerkstelligen. De toenemende geopolitieke instabiliteit in de wereld, de Russische invasie in Oekraïne, de snelgroeiende macht van China, heeft er toe geleid dat Europa zich ook bewust is geworden van zijn afhankelijkheid van buitenlandse grondstoffen, producten en diensten. Vooral op het terrein van digitale technologieën dreigt de EU achterop te raken. Deze toenemende afhankelijkheid heeft ertoe geleid dat vele Europese initiatieven zijn ontplooid om de strategische autonomie te versterken. In Nederland speelt deze discussie echter nog beperkt en heeft nog niet geleid tot een breed debat over de nationale doelstellingen en ambities op dit terrein.

De ambitie van staten om de strategische autonomie op cybersecurity te waarborgen is voor een groot deel ingegeven door het belang om de nationale veiligheid te waarborgen. Strategische autonomie wordt door staten en de EU ook nadrukkelijk verbonden aan de borging van publieke waarden en grondrechten. De uitdaging is daarbij de balans te vinden tussen enerzijds het optimaal benutten van de kansen die digitalisering en de vrije markt bieden en anderzijds het behouden van controle over en toezicht op de toepassingen van nieuwe technologieën. De overheid moet immers het (economisch) welzijn van de samenleving bevorderen en tegelijkertijd haar veiligheid beschermen. Doel bij het formuleren van overheidsbeleid (zeker in de Nederlandse context) is om de strategische autonomie op cybersecurity dusdanig vorm te geven dat deze effectief en efficiënt is.

De vraag van het Ministerie van Economische Zaken en Klimaat aan TNO en het Den Haag Centrum voor Strategische Studies (HCSS) is om ondersteuning te bieden bij het inzicht krijgen in hoe de strategische autonomie op cybersecurity bewaakt kan worden en welke beleidsmaatregelen in dit kader genomen kunnen worden. Het instrumentarium moet bruikbaar zijn in een interdepartementale context voor verschillende belanghebbenden die een rol hebben bij het bepalen van strategische autonomie op cybersecurity, zoals beleidsverantwoordelijken, dossier-houders, onderzoekers en vertegenwoordigers van bedrijven. De gebruikersgroep binnen de overheid bestaat uit diverse niveaus binnen verschillende departementen, variërend van beleidsmedewerkers tot het directeurenoverleg cybersecurity. Dit vraagt van het instrumentarium dat het kan worden ingezet op deze verschillende (abstractie) niveaus binnen en tussen departementen. Hierbij is het belangrijk te onderkennen dat de inhoudelijke beleidsmedewerkers en dossierhouders het betreffende vraagstuk dermate inzichtelijk maken dat de verantwoordelijke beslissers hierover een besluit kunnen nemen.

1.2 Doelstelling en onderzoeksvragen

De doelstelling van het huidige project is te komen tot een instrumentarium dat concrete ondersteuning biedt bij het bepalen van de noodzaak van strategische autonomie op cybersecurity en van het handelingsperspectief en de instrumenten die hieraan bijdragen.

Dit project geeft een vervolg op het TNO/HCSS project 'Strategische Digitale Autonomie' dat in 2020 is uitgevoerd.[1] Daarin werd een uiteenzetting gegeven van het begrip 'strategische autonomie op cybersecurity', en van wat belangrijke factoren zijn die daar een invloed op hebben. Daarnaast is dit project een vervolg op de studie van de Cyber Security Raad[2] waarin tevens een substantiële voorzet werd gegeven ten aanzien strategische autonomie op cybersecurity. Beide studies hebben geresulteerd in een *flowchart* die bedoeld was als eerste orde stappenplan voor de analyse rondom strategische autonomievraagstukken en eventueel te ondernemen activiteiten (beleidsmatig of meer praktisch, juridisch etc.). Die bieden een goed fundament, maar nog niet voldoende praktisch handelingsperspectief. Ze zijn nog niet voldoende gelinkt met de werkprocessen van betrokkenen, en geven nog te weinig richting voor duiding en besluitvorming.

Strategische autonomie gaat over het creëren van handelingsperspectief op basis van een risicobeoordeling, en perceptie van de weerbaarheid van Nederland. Die perceptie verschilt per stakeholder en per gebeurtenis dan wel risico. Daarnaast zal de perceptie over strategische autonomie veranderen over tijd. Dialogen over strategische autonomie zullen daarom wellicht in de toekomst tot andere uitkomsten leiden dan nu. Een instrumentarium zal er op moeten anticiperen dat de indicatoren en randvoorwaarden voor strategische autonomie snel veranderen, net als de technologie, en helpen om de duiding van verschillende belangen over strategische autonomie op cybersecurity te ondersteunen. Het instrumentarium zal daarmee eerder faciliterend zijn dan normatief. Beschouwing over strategische autonomie op cybersecurity vraagt om een dialoog tussen stakeholders en gezamenlijke besluitvorming rondom voorziene handelingsperspectieven.

Overheden moeten zich bewust zijn van de verschillende knoppen waaraan ze kunnen draaien om strategische autonomie te waarborgen, wat de kosten en baten zijn, en wanneer verschillende maatregelen elkaar versterken of tegenwerken. Daarnaast is de rol van de overheid vooralsnog beperkt. De technologische sector wordt gedomineerd door de private sector, die de software, producten, infrastructuur en diensten beheert. Verder spelen *civil society* actoren ook een belangrijke rol, zoals met name de technische gemeenschap en academici die een belangrijk deel van de discussies en normen van de onderliggende *internet governance* structuren beheren.

Hoewel de overheid beschikt over een breed palet aan instrumenten om de strategische autonomie op cybersecurity te versterken, zijn er ook uitdagingen en dilemma's. In de kern gaat het om het vinden van een balans tussen het versterken van de concurrentiekracht en het borgen van de nationale veiligheid. Een te ver doorgevoerd streven naar digitaal protectionisme (de wens om de eigen markt af te

[1] Veenendaal, van Schie, Rademaker, Faesen (2020), Whitepaper Strategische Autonomie op Cybersecurity (2020), TNO rapport 2020 R11599. TNO: Den Haag.
[2] Timmers, P. & Dezeure, F. (2021), Nederlandse strategische autonomie en cybersecurity.

schermen op grond van veiligheidsoverwegingen) kan bijvoorbeeld de internationale concurrentiepositie van de eigen digitale technologiesector verzwakken.

Op basis van de benoemde onderzoeksdoelstelling zijn de volgende onderzoeksvragen gedefinieerd:

- Uit welke onderdelen bestaat het instrumentarium aan de hand waarvan een interdepartementale gebruikersgroep (incl. deelnemers vanuit bedrijfs- en onderzoekwereld) kan vaststellen of er een noodzaak is voor strategische autonomie op cybersecurity?
- Op welke wijze kan het instrumentarium de gebruikers praktisch ondersteunen in hun besluitvormingsproces, zowel in situaties met een langere termijn als in urgente, korte-termijn situaties?

In hoofdstuk 2 wordt de aanpak beschreven die we hebben gehanteerd. De verschillende onderdelen van het instrumentarium, evenals het proces om dit instrumentarium in een interdepartementale context toe te kunnen passen, worden nader toegelicht in hoofdstuk 3. Hoofdstuk 4 tenslotte bevat de conclusies en aanbevelingen.

2 Aanpak

Het door TNO/HCSS ontwikkelde stroomschema uit 2021 diende als uitgangspunt voor het instrumentarium beschreven in dit rapport.[3] Deze werd aangevuld met de bevindingen van de workshops die TNO en HCSS hebben georganiseerd en het adviesrapport 'Nederlandse strategische autonomie en cybersecurity' dat de Cyber Security Raad in samenwerking met Paul Timmers en Freddy Dezeure[4] heeft opgesteld.

Het was belangrijk voor de ontwikkeling van het instrumentarium om grip te krijgen op de belangrijkste '*use cases'*, oftewel, wat zijn de aanleidingen voor de gebruikersgroep om bij elkaar te komen, onder welke omstandigheden wordt het instrumentarium ingezet, en door wie? Bijvoorbeeld:

- Investeringen van buitenlandse bedrijven in Nederland (en het opzetten van beschermingsconstructies).
- Beschikbaarheid van nieuwe technologische producten.
- Technologische R&D ontwikkelingen.
- Veranderingen in infrastructuren.
- Geopolitieke ontwikkelingen.
- Veranderingen in Europees beleid, standaarden of afspraken tussen (EU-) lidstaten.
- Invloed van buitenlandse mogendheden.
- Verstoring van infrastructuur in binnen- en buitenland door moedwillige disruptie of natuurrampen.
- Geplande lange-termijn plannen en investeringen.

De bruikbaarheid van het instrumentarium hangt samen met het draagvlak dat bestaat onder de beoogde gebruikers, en de mate waarin het instrumentarium departementen en andere stakeholders in staat stelt hun analyse en besluitvorming te ondersteunen. Om de perspectieven van de diverse departementen goed te kunnen verwerken en te waarborgen dat het instrumentarium leidt tot concrete handelingsperspectieven, is er gekozen voor een co-creatie traject. Het instrumentarium is ontwikkeld en getest aan de hand van vier workshops: deze co-creatie heeft geleid tot een betere toepasbaarheid van, en draagvlak voor het instrumentarium.

2.1 Opzet van de workshops

De deelnemers aan de workshops komen van diverse departementen zoals EZK, BZK, JenV/NCTV, Defensie, IenW en de Nationale Politie. Per workshop nemen ongeveer 15 personen deel, begeleid door het projectteam. De deelnemers hebben ervaring met eerdere cases, zodat hun ervaringen (knelpunten, oplossingen, dilemma's) mee kunnen worden genomen. De meeste deelnemers waren in staat om aan alle workshops deel te nemen dan wel te reflecteren op de resultaten wat heeft bijgedragen aan de continuïteit van de discussies.

[3] https://hcss.nl/report/strategische-autonomie-op-cybersecurity/
[4] Timmers, P. & Dezeure, F. (2021), Nederlandse strategische autonomie en cybersecurity.

In samenwerking met de deelnemers is bepaald wat de scope is van strategische autonomie op cybersecurity aan de hand van geselecteerde *use cases*. We hebben een iteratief proces gevolgd waarbij het projectteam een versie van het instrumentarium ontwikkelde dat vervolgens tijdens de workshops werd getest, en vervolgens werd bijgesteld. Tijdens een serie van vier workshops zijn diverse scenario's doorlopen gebaseerd op de geselecteerde use-cases om inhoud, vormgeving en toepasbaarheid van het instrumentarium verder te ontwikkelen en te evalueren. Tussen de derde en vierde workshops hebben de meeste deelnemers het instrumentarium besproken met andere collega's en/of de leidinggevende om aanvullende feedback te verzamelen en draagvlak te creëren. Deze feedback evenals de resultaten van de vierde workshop zijn gebruikt om de finale versie van het instrumentarium te ontwikkelen.

Tijdens de eerste, derde en vierde workshops zijn de volgende fictieve *use-cases* gebruikt:

- Foreign Direct Investment:
  - Korte termijn gebeurtenis: Onverwachte bedrijfsovername van Compumatica door grote investeerder uit Bangalore (India).
  - Lange termijn gebeurtenis: Bedrijfsovername ASML door buitenlands overheidsfonds United Arabic Emirates.
- Kennisinfrastructuur – Brain-computer interfacing en cybersecurity:
  - Een braindrain staat te gebeuren, wat zijn de mogelijke consequenties?
  - De ambitie is uitgesproken dat Europa/Nederland een sterkere positie wil bereiken.
- Cryptografie in cybersecurity:
  - De bestaande kleine groep Nederlandse bedrijven kan moeilijk rondkomen van alleen deze markt in Nederland. Voor *high assurance* toepassingen is tevens de eis dat deze oplossingen in Nederlandse handen zijn.
  - Om de kennis in stand te houden voor Nederland is het voor deze bedrijven lastig mensen vast te houden en de kennisontwikkeling in stand te houden en op gezonde schaal te ontwikkelen.
  - Er is vertrouwelijk kenbaar gemaakt dat twee Nederlandse bedrijven (60% van de markt) een buitenlands (Europees) overnamebod hebben gehad. Zij hebben dit laten weten aan het ministerie van Economische Zaken.

Tijdens de tweede workshop hebben we aan de hand van ratings met behulp van Mentimeter discussies gevoerd over de effectiviteit en appreciatie van clusters van instrumenten. Deze ratings zijn op geen enkele wijze bedoeld als kwantificering, maar alleen als trigger voor het voeren van goede kwalitatieve inhoudelijke discussies.

De volgende criteria werden hierbij gehanteerd:

- Is er een **juridische** basis?
- Wie is de **uitvoerende partij**?
- Welk **effect** moet bereikt worden door het instrumentarium om het **gewenste doel** te behalen? Hoe versterkt het de strategische autonomie?
- Heeft het een effect op de **korte of lange termijn**?
- Veroorzaakt het instrument **ongewenste neveneffecten**?
- Is er een **monitoringssysteem** om de effectiviteit van de ingezette instrumenten in het behalen van het gewenste doel te **evalueren**?
- Wordt de **strategische autonomie voldoende gewaarborgd**?

De volgende clusters van instrumenten zijn besproken.
Controle behouden:

1 Versterking van de binnenlandse markt.
2 Voorwaarden opleggen in verband met verandering van zeggenschap.
3 Talent behouden.

Controle verwerven:

4 Kennisopbouw.
5 Productie.
6 Investeringen.
7 Regelgeving.

Algemeen:

8 Monitoren van instrumentarium en doelstelling.

2.2 Resultaten van de workshops

Tijdens de workshops zijn diverse reflecties gegeven op de inhoud van het instrumentarium, de vormgeving en het proces om dit instrumentarium. Deze zijn zo veel als mogelijk verwerkt in de nieuwere versies van het instrumentarium. Enkele voorbeelden ter illustratie zijn:

- De focus ligt vooral op wat we in Nederland hebben en willen; zorg ervoor dat er ook voldoende oog is voor strategische autonomie in internationaal verband.
- Kijk naast economisch en veiligheidsbelang ook naar maatschappelijk belang.
- Het gebruiken van een scorekaart kan als ongewenst bijeffect hebben dat je de discussie plat slaat terwijl het stroomschema nu juist moet dienen als vehikel om de discussie te starten.
- Sommige vragen zijn nogal ruim geformuleerd, waardoor ze lastig zijn te beantwoorden.
- In het stroomschema wordt alleen gesproken over ‘impact’. Beter is om te spreken over ‘risico’ (kans x impact). Dit is vergelijkbaar bij de statelijke actor: het gaat er hier niet zozeer om of een statelijke actor het kan, maar wat het risico (kans x impact) hierop is.

Daarnaast hebben we waar nodig een nadere toelichting op enkele onderdelen van het stroomschema gegeven, en de natuurlijke flow in het stroomschema geoptimaliseerd. De relatie tussen het stroomschema en de RACI-Matrix is expliciet aangegeven en de inhoud is volledig met elkaar geharmoniseerd. De instrumenten die in het stroomschema als mogelijke interventies zijn aangegeven hebben we geordend naar de tijdstermijn waarop mogelijkerwijs effecten van de inzet van instrumenten verwacht kunnen worden: per blokje met instrumenten is een indicatieve volgorde aangebracht van korte termijn naar meer langere termijn.

Uiteindelijk zijn de volgende resultaten ontwikkeld:

- Stroomschema ‘Strategische Autonomie Cybersecurity’ inclusief een overzicht van mogelijke interventies.
- RACI-Matrix waarin per stap in het stroomschema kan worden aangegeven wie welke vragen moet beantwoorden.
- Scorekaart ter ondersteuning van de inschatting van de noodzaak tot interveniëren.
- Handleiding voor dit instrumentarium.
- Informerende video.

Deze resultaten worden in het volgende hoofdstuk toegelicht.

3 Het ontwikkelde instrumentarium

In dit hoofdstuk wordt het ontwikkelde instrumentarium ter ondersteuning van het omgaan met strategische autonomie op cybersecurity beschreven.

Het instrumentarium biedt concrete ondersteuning bij het vraagstuk of in voorkomend geval de overheid interventie zou moeten en kunnen plegen om de strategische autonomie op cybersecurity te garanderen of herstellen. Voorbeelden van deze overwegingen zijn: een buitenlands bedrijf wil een belangrijk cybersecurity bedrijf overnemen, of Nederland ziet zich genoodzaakt de kennispositie op een bepaald deelterrein te garanderen of versterken.

Het instrumentarium beoogt daarbij op systematische wijze handvatten te bieden bij vragen die opkomen met betrekking tot:

- Welk departement of directie is waarvoor verantwoordelijk?
- Welke perspectieven dienen er (op korte en lange termijn) tegen elkaar worden afgewogen?
- Welke overwegingen moeten een rol spelen?
- Waar liggen de grensvlakken en relaties tussen verschillende domeinen?
- Welke handelingsperspectieven zijn er om te interveniëren?
- En wat zijn daarbij de voor- en nadelen?

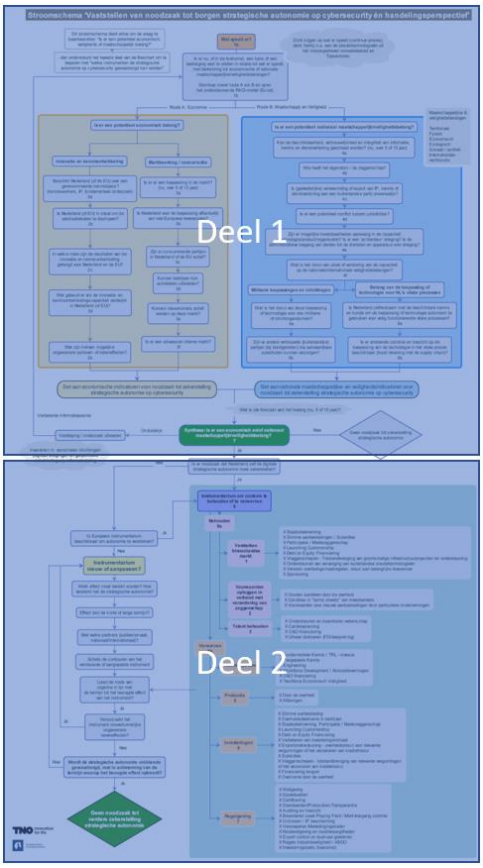
Onderdeel van het instrumentarium zijn het Stroomschema ‘Strategische Autonomie Cybersecurity’, de RACI-Matrix, een Scorekaart, een Handleiding voor het instrumentarium, en een informerende video.

Het stroomschema en bijbehorend Excel-bestand kunnen worden gebruikt om de noodzaak tot het borgen van de strategische autonomie op cybersecurity vast te stellen, evenals het identificeren van de ondersteunende instrumenten die hieraan kunnen bijdragen. Hierbij is rekening gehouden met de samenhang tussen cyber-security enerzijds en economische, maatschappelijke en nationale veiligheids-belangen anderzijds.

De verschillende onderdelen van het instrumentarium worden in dit hoofdstuk nader toegelicht, evenals het proces om dit instrumentarium in een interdepartementale context toe te kunnen passen.

3.1 Stroomschema ‘Strategische Autonomie Cybersecurity’

Het stroomschema ‘Strategische Autonomie Cybersecurity’ bestaat uit twee delen (zie Figuur 1). Deel 1 dient om te kunnen concluderen of er een noodzaak is om de strategische autonomie op cybersecurity te borgen. Indien dat het geval is kan deel 2 worden gebruikt om keuzes te maken uit instrumenten die hieraan bijdragen. Hiermee ontstaat zicht op het handelingsperspectief.



Figuur 1: Schematisch overzicht stroomschema.

Elk deel van het stroomschema is opgebouwd uit een serie van vragen. In veel gevallen zal het antwoord op een vraag in het stroomschema niet direct kunnen worden gegeven omdat de desbetreffende informatie niet op voorhand beschikbaar is. Het stroomschema kan dus ook aanleiding geven tot het uitvoeren van een nadere analyse of onderzoek. Nadat het stroomschema is doorlopen kan worden bepaald of er de noodzaak is tot het versterken van de strategische autonomie op cybersecurity en met behulp van welke instrumenten dat kan worden gedaan.

Voor de beantwoording van de vragen in het stroomschema is veelal achtergrondinformatie nodig die niet in het stroomschema zelf past; die wordt in de handleiding gegeven. De handleiding volgt de volgorde en nummering van het stroomschema en wordt verder toegelicht in paragraaf 3.4.

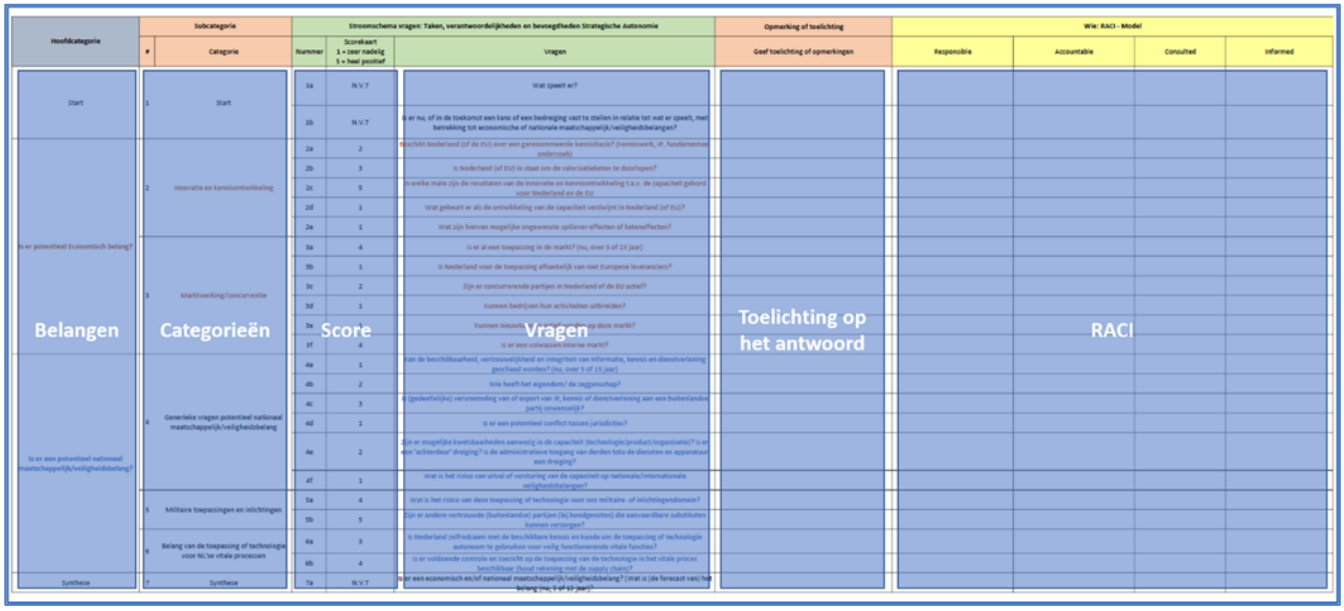
Het stroomschema hoeft niet altijd volledig doorlopen te worden. Sommige aspecten zullen voor een bepaald thema niet of minder relevant zijn en kunnen in dat geval worden overgeslagen. Gebruikers kunnen hierin zelf beargumenteerde beslissingen maken. Vele onderdelen uit het stroomschema zijn belangrijk en relevant, maar vormen niet noodzakelijkerwijs een vast onderdeel van de analyse en de besluitvorming. Mochten er vragen lastig of gecompliceerd zijn om te beantwoorden, dan is het goed om te rade te gaan waarom dit zo is, in plaats van deze zondermeer over te slaan.

Een leesbare versie van het stroomschema staat in Bijlage A.

3.2 RACI-Matrix

Bij het stroomschema hoort de RACI-Matrix (zie figuur 2). Aangezien strategische autonomie op cybersecurity een breed vraagstuk betreft, is het niet altijd eenvoudig om vast te stellen wie waarover gaat, dan wel wie het beste in staat is om antwoorden op vragen te formuleren. Daarom is de RACI-Matrix, in de vorm van een Excel-document, toegevoegd, waarin per vraag kan worden aangeven wie voor een bepaalde casus operationeel verantwoordelijk (*Responsible*) is, wie als

systeemverantwoordelijke de eindverantwoordelijkheid heeft (*Accountable*), wie geconsulteerd dient te worden (*Consulted*) en wie geïnformeerd (*Informed*). De RACI-Matrix wordt gebruikt bij het beantwoorden van de vragen in het stroomschema (in deel 1) en bij het kiezen van handelingsperspectief (deel 2).



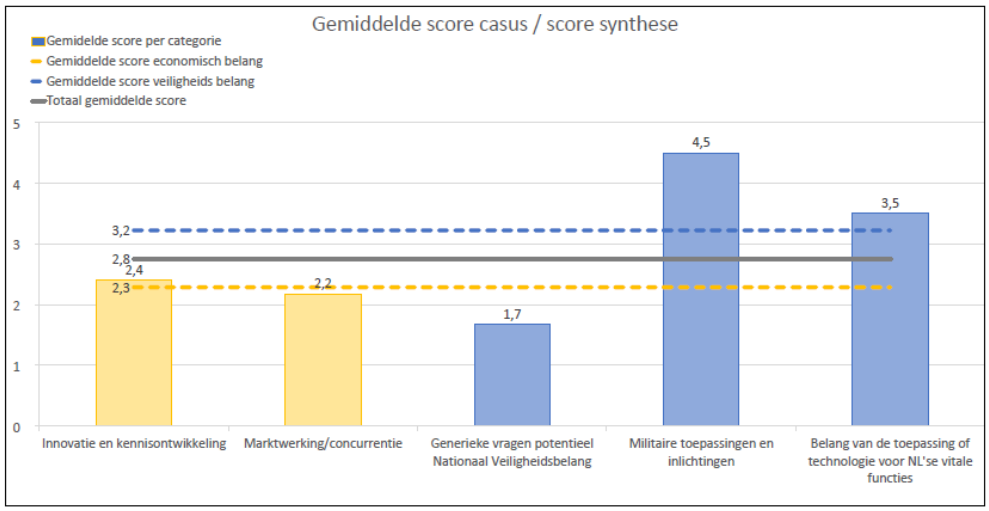
Figuur 2: Overzicht RACI-Matrix.

Een leesbare versie van de RACI-Matrix staat in Bijlage B.

3.3 Scorekaart

In de RACI-Matrix is een scorekaart opgenomen. Deze geeft de mogelijkheid om kwalitatieve scores te geven per vraag. Het toewijzen van een score op een schaal van 1 t/m 5 is bedoeld om het belang van een vraag te objectiveren. Een score van 1 is zeer nadelig ten aanzien van de strategische autonomie op cybersecurity, en een score van 5 is heel positief waarbij over het algemeen geldt: hoe lager de score, hoe hoger de noodzaak om interventie te plegen. De scores zijn een voorzichtige kwantificering van veelal subjectieve antwoorden op de vragen en zijn in eerste instantie primair bedoeld om het gesprek te starten tussen de betrokken partijen om tot een goede onderlinge afweging van de argumenten en keuzen te komen.

De scores worden onder de vragen opgeteld in de categorieën “Economisch belang” en “Veiligheidsbelang” (zie ook Figuur 3). Bij veelvuldig gebruik van het stroomschema en het monitoren van de effecten van interventies bij meerdere cases, is het mogelijk een stevige basis voor deze scores op te bouwen.



Figuur 3 : Illustratie van de scorekaart.

Met klem benadrukken wij dat de uitleg van de score op dit moment belangrijker is dan de feitelijke score die gegeven wordt.

3.4 Handleiding

Om het gebruik van het instrumentarium te ondersteunen, is een handleiding ontwikkeld. Aan de hand van deze handleiding wordt de gebruiker in een logische volgorde stap voor stap door het stroomschema geleid en gevraagd om inschattingen, antwoorden, inzichten en verantwoordelijkheden vast te leggen.

De volledige handleiding staat in Bijlage C.

3.5 Toepassing van het instrumentarium in een interdepartementale context

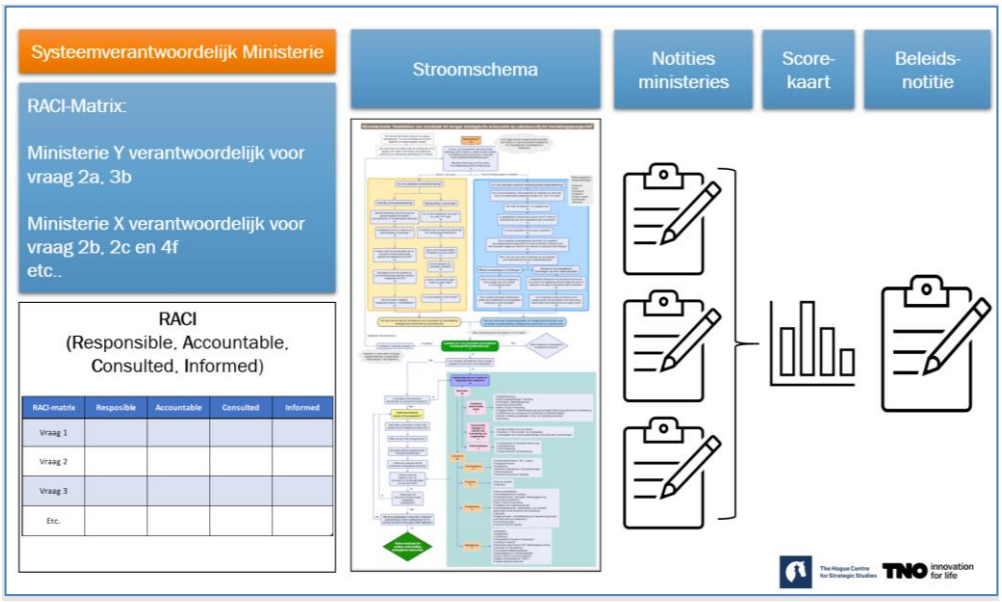
Wie is voor een bepaald vraagstuk de systeemverantwoordelijke? Is dat altijd EZK, of moet dat per casus vastgesteld worden? Dit is expliciet als beslismoment in het stroomschema opgenomen. Deze systeemverantwoordelijke is verantwoordelijk om andere departementen te vragen bepaalde onderdelen van de RACI-Matrix in te vullen, en de diverse notities samen te voegen tot één beleidsnotitie. Een mogelijke *rule of thumb* om te bepalen wie bij welke trigger de systeemverantwoordelijke zou kunnen zijn is:

- Incident: NCTV.
- Langere termijn cryptostrategie: BZK.
- FDI/overname, kennisborging, markt falen: EZK.

Uiteraard zal de waarheid altijd wel ergens in het midden liggen. Maar het is wel belangrijk deze systeemverantwoordelijke te identificeren om te waarborgen dat het hele proces gestructureerd en geharmoniseerd wordt uitgevoerd.

Het is goed om de vragen door verschillende departementen (of andere actoren zoals een toezichthouder, of een regionale ontwikkelingsmaatschappij) in te laten vullen: sommige vragen passen van nature goed bij de expertise van een specifiek departement, maar bij andere vragen wil je juist verschillende perspectieven van diverse departementen en actoren krijgen. Op deze manier kan je ook beter de bevindingen uit de economische pijler en de veiligheidspijler van de flowchart met

elkaar integreren. Het wordt aanbevolen om aan de hand van het stroomschema en RACI-Matrix gezamenlijk een beleidsnotitie op te stellen op basis van diverse separate notities die door de betreffende departementen worden opgesteld (zie Figuur 4 voor een schematische weergave van dit proces). De nummeringen uit het stroomschema kunnen worden gebruikt om de beleidsnotitie te structureren. Het is een goede werkwijze om tot een goed onderbouwd, gezamenlijk en goed gestructureerd beleidsadvies te komen. En dat dus ook als basis gebruikt kan worden om gecoördineerd de voorgenomen interventies uit te voeren.



Figuur 4: Procesweergave van het gebruik van het instrumentarium 'Strategische Autonomie Cybersecurity'.

De beantwoording van de vragen moet goed beargumenteerd worden. Scores kunnen hierbij helpen om dit meer te objectiveren. En die weging is ook van invloed op wie welke effort moet gaan steken om welke interventie uit te gaan voeren. Per vraag dient een kwalitatieve beschrijving van de situatie te worden gegeven, de noodzaak om al dan niet te interveniëren, en de rationale daarachter. Bij een advies om te interveniëren moet worden aangegeven welk instrumentarium in te zetten en waarom deze keuze is gemaakt. Vervolgens dient een kwalitatieve bepaling te worden gegeven van het restrisico na inzet van het instrumentarium, of dit een acceptabel restrisico is en zo nee, wat er nog extra nodig is (bijvoorbeeld ontwikkeling van nieuw instrument). De algemene waardering en conclusie (en de beleidsaanbeveling) is dan het sluitstuk van de uiteindelijke beleidsnotitie.

Bij de keuze van de interventies/instrumenten moet ook de urgentie worden meegenomen. Bij een hele hoge urgentie vallen automatisch al diverse instrumenten af. Daarnaast is de urgentie een belangrijke trigger voor de financiële consequenties. Bijvoorbeeld moeten we budgetten van departementen samen brengen (als het enkele budget van een enkel departement ontoereikend blijkt te zijn), passen budgetten niet bij de voorziene looptijd van een interventie, hoe kunnen we aanspraak maken op ander/meer budget. Voor al deze vragen dient het Ministerie van Financiën betrokken te worden.

Sommige instrumenten vallen primair onder de verantwoordelijkheid van departementen. Echter, het inzetten van die instrumenten moet niet te stevig/exclusief aan een departement worden gekoppeld. Dat moet aan een sterke opdracht gekoppeld worden om de samenwerking met andere departementen te stimuleren. Zoals tijdens de laatste workshop werd opgemerkt: “Op nationaal niveau meer autonomie door op individueel niveau wat autonomie in te leveren.” De echte impact zit uiteindelijk immers in de gezamenlijke uitvoering van de plannen c.q. toepassing van de instrumenten. Dat valt strikt genomen buiten het stroomschema, maar wellicht kan er wel worden afgesloten met een tijdpad met maatregelen en handelingsperspectief. Hieronder valt dus ook het monitoren van de effecten van de inzet van maatregelen. Dat geeft wat meer sturing aan het daadwerkelijk implementeren van alle acties met betrekking tot het nastreven van de strategische autonomie (incl. dus het eventueel ontwikkelen van nieuwe instrumenten).

3.6 Informerende video

Tenslotte is er een korte informerende video gemaakt. Deze video is een visuele managementsamenvatting van de handleiding. In deze Nederlandstalige video wordt beknopt geïllustreerd waar het instrumentarium voor dient, hoe het te gebruiken is, en wat de resultaten zijn.

4 Conclusies en aanbevelingen

In dit hoofdstuk treft u vier conclusies en vijf aanbevelingen aan.

4.1 Conclusies

1 Er is dringend behoefte aan inzicht in de stand van de Nederlandse digitale strategische autonomie en afhankelijkheden. Tot dusver zijn de analyses vaak te oppervlakkig geweest en de aanpak te versnipperd. Er zijn talloze strategieën, kennisagenda's of vergelijkebare departementale documenten die onvoldoende op elkaar aansluiten. Op basis van de workshops is de noodzaak en meerwaarde benadrukt van een gezamenlijk interdepartementaal proces om de versnipperde kennis en belangen van de departementen bij elkaar te brengen om zo tot een weloverwogen beslissing voor strategische autonomie te komen.

2 Het instrumentarium wordt ervaren als een waardevolle toevoeging voor de verdere discussie en een grote vooruitgang ten opzichte van eerder ontwikkelde instrumenten. Het biedt concretere handvatten voor en een helder beeld van een eventueel handelingsperspectief en zal doorontwikkeld moeten worden.

3 De RACI-insteek faciliteert een eenduidige verdeling van rollen en verantwoordelijkheden. Binnen de Rijksoverheid is dit vaak nog te onduidelijk, met name als het gaat om het goed aangeven van wie (primair) verantwoordelijk is bij een bepaalde casus, en wie bij aansprakelijk, geconsulteerd en geïnformeerd moeten worden aangegeven. Het in dit project ontwikkelde instrumentarium helpt bij het toewerken naar een eenduidige *whole of government* benadering. Dit wil niet zeggen dat de overheid dit proces alleen moet doorlopen of alleen in staat is strategische autonomie te behalen. Het is van groot belang om ook de Nederlandse en Europese kennisinstellingen en het bedrijfsleven te betrekken.

4 Dit instrumentarium bevordert het bij elkaar brengen van de versnipperde kennis en belangen van de departementen om zo tot een weloverwogen beslissing voor strategische autonomie te komen. Hierdoor kunnen prioriteiten worden gesteld over de noodzaak en haalbaarheid van het zekerstellen of de versterking van de strategische autonomie op cybersecurity. Nederland of Europa kan immers niet op alle technologiegebieden strategisch autonoom zijn.

4.2 Aanbevelingen

1 Ontwikkel een *forward looking capacity*, of monitoringsfunctie en richt deze in binnen de Rijksoverheid met ondersteuning van kennisinstellingen. Dit kan bijdragen aan de ontwikkeling van een strategische cultuur, waarbij er niet alleen maar reactief wordt opgetreden maar ook preventief wordt gehandeld op (middel)langere termijn. Dit vergt een heldere prioritering en periodieke evaluaties aangezien technologieën en risico's over de tijd veranderen. Het is daarom aan te raden om ook expliciet aan te geven wat de mogelijke impact van een situatie kan zijn in de (nabije) toekomst.

Op die manier is het wellicht ook mogelijk om een gerichtere afbakening te maken van het type technologieën die met name gemonitord dienen te worden: anders wordt het in potentie te breed. Het belang van een technologiegebied kan pas goed worden bepaald wanneer toepassingen voor zijn. Dan wordt duidelijk of het een belang voor strategische autonomie vertegenwoordigt. Welke producten, diensten, processen maken gebruik van deze technologie en wat is hiervan de impact bij verstoring, uitval of vermindering van beschikbaarheid?

Het duiden van de toekomstige impact is ook van belang om ontwikkelingen die nu gebeuren te extrapoleren. Zal de technologie op korte en lange termijn in belang toenemen, waardoor vervreemding aan een buitenlandse partij de Nederlandse belangen mogelijk schaadt? Het uitvoeren van een technologische forecast is belangrijk om inzicht te krijgen in de toegevoegde waarde van de technologie voor andere innovaties. 5G wordt bijvoorbeeld gezien als een sleuteltechnologie die andere technologische innovatie mogelijk maakt, zoals autonome voertuigen, *smart electric grids*, en het *internet of things*. Door te analyseren welke potentiële toepassingen mogelijk worden, kan een inschatting worden gemaakt van de impact en van het belang om als staat vrij te kunnen beslissen en handelen.

2 Hanteer een eenduidig format voor de beleidsnotitie die volgt uit het toepassen van het instrumentarium, bestaande uit de volgende onderdelen: beschrijving van de situatie, de noodzaak om al dan niet te interveniëren en de rationale daarachter, welk instrumentarium dient te worden ingezet en de rationale daarachter, het eventuele restrisico na inzet van het instrumentarium (incl. of dit acceptabel is en zo niet, wat nog extra nodig is), en de overall waardering en conclusie.

3 Ontwikkel een digitale versie van het instrumentarium om de toepassing te vergemakkelijken en alle losstaande onderdelen te integreren in één applicatie. Bijvoorbeeld, de gebruikers kunnen op een vraag in het stroomschema klikken, waarna ze de betreffende toelichting kunnen lezen en vervolgens de RACI-rollen kunnen invullen. Departementen kunnen vervolgens de hun toegewezen vragen direct beantwoorden, waarna automatisch een notitie wordt gegenereerd. Het departement dat systeemverantwoordelijke is kan vervolgens de diverse afzonderlijke notities automatisch samenvoegen tot één beleidsnotitie met conclusies en aanbevelingen.

4 In navolging van de deelnemers aan de workshop bevelen we aan dat dit instrumentarium daadwerkelijk wordt geïmplementeerd en ingezet conform het proces dat in paragraaf 3.5 is beschreven. Bij voorkeur niet direct op een actuele casus, maar op een casus die mogelijk over drie jaren relevant is. Op deze wijze kan men ervaren hoe dit proces werkt, en of er dan meer inzicht wordt verkregen in hoeverre de Rijksoverheid in staat is de goede instrumenten/interventies in te zetten, dan wel inzicht krijgt in waar aanvullende instrumenten nodig zijn (of om instrumenten die momenteel worden ontwikkeld, zoals met betrekking tot *Foreign Direct Investment*) hierin te integreren. Een andere optie is het uitvoeren van een *reverse engineering* exercitie op reeds genomen investeringsbeslissingen.

5 Pas dit instrumentarium regelmatig aan. De huidige versie is een eerste iteratie en het is essentieel voor de kwaliteit van het instrumentarium om het de komende periode toe te passen en te blijven verbeteren. Goed monitoren van effecten en timing van interventies is belangrijk om een goede kennisbasis hierover op te bouwen. Feitelijk zou de inzet en verdere ontwikkeling van dit instrumentarium onderdeel moeten worden van de nationale cybersecurity strategie.

5 Referenties

Analistennetwerk Nationale Veiligheid*:* publicaties te downloaden via https://www.rivm.nl/onderwerpen/nationale-veiligheid.

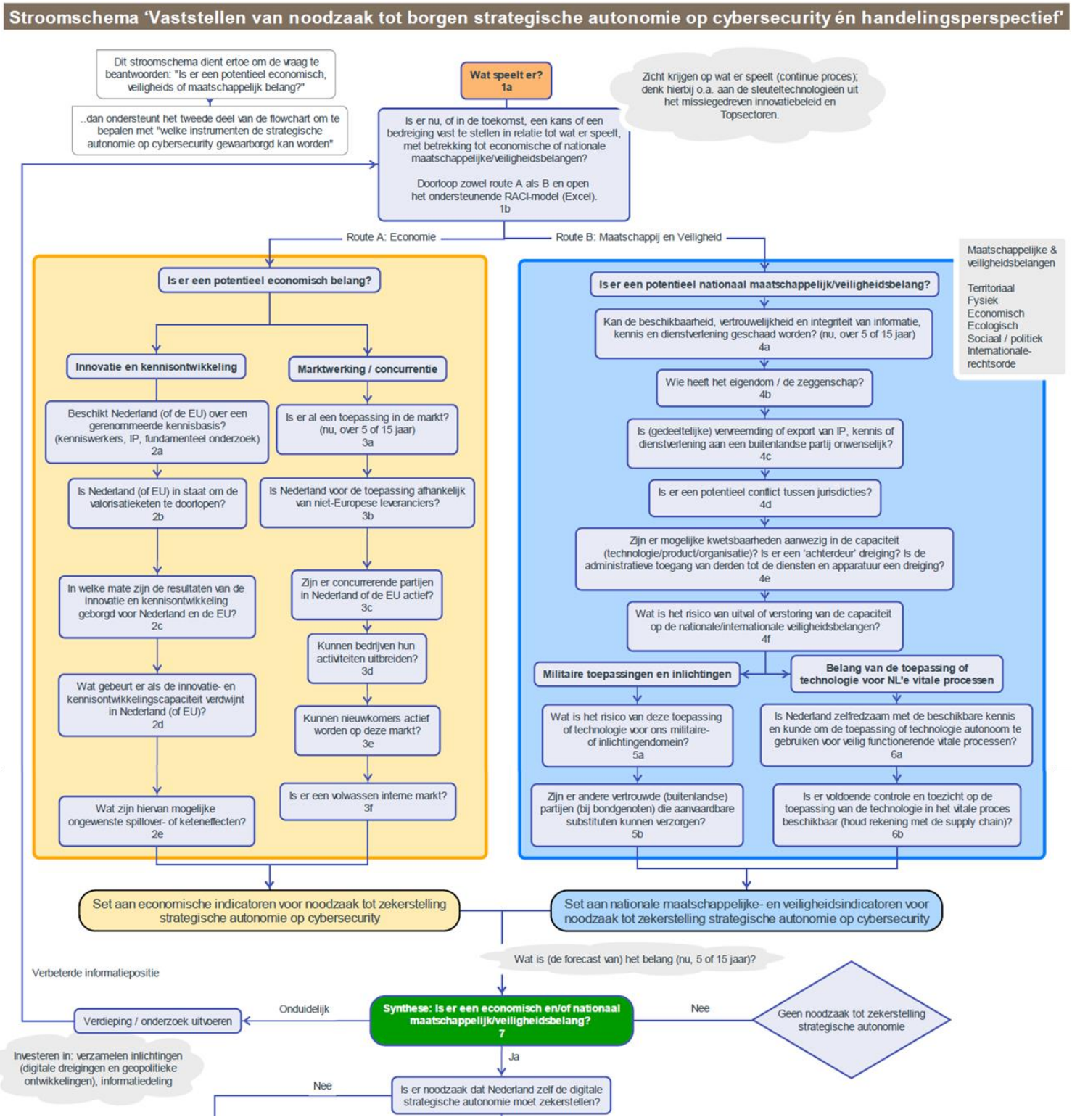
KIA Veiligheid (2019), online: https://www.nwo.nl/sites/nwo/files/assets/KIA%20Veiligheid%20-%2020191015%20definitief_0.pdf.

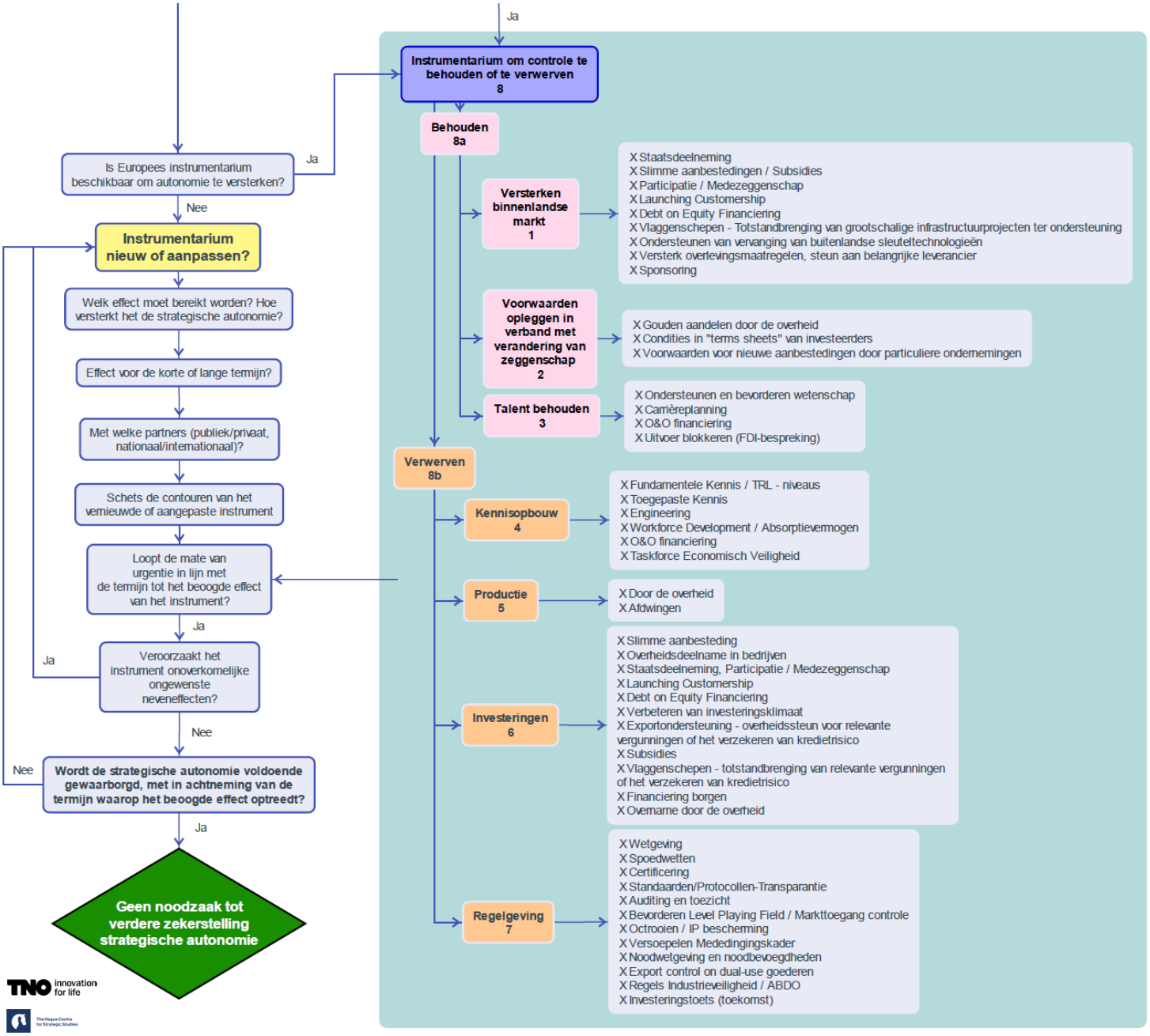
Timmers, P. & Dezeure, F. (2021), *Nederlandse strategische autonomie en cybersecurity*. Rapport ten behoeve van de Cyber Security Raad.

Veenendaal, M.A., Schie, T.C.C. van, Rademaker, M., & Faesen, L. (2020), *Whitepaper Strategische Autonomie op Cybersecurity,* TNO rapport 2020 R11599. TNO: Den Haag.

Veenendaal, M.A., Schie, T.C.C. van, Rademaker, M., & Faesen, L. (2021), *Soevereiniteit en Digitale Autonomie, online:* https://hcss.nl/report/soevereiniteit-en-digitale-autonomie/.

A Stroomschema ‘Strategische Autonomie Cybersecurity’




Is Europees instrumentarium beschikbaar om autonomie te versterken?
Ja
Nee
Instrumentarium nieuw of aanpassen?
Welk effect moet bereikt worden? Hoe versterkt het de strategische autonomie?
Effect voor de korte of lange termijn?
Met welke partners (publiek/privaat, nationaal/internationaal)?
Schets de contouren van het vernieuwde of aangepaste instrument
Loopt de mate van urgentie in lijn met de termijn tot het beoogde effect van het instrument?
Ja
Veroorzaakt het instrument onoverkomelijke ongewenste neveneffecten?
Ja
Nee
Nee
Wordt de strategische autonomie voldoende gewaarborgd, met in achtneming van de termijn waarop het beoogde effect optreedt?
Ja
Geen noodzaak tot verdere zekerstelling strategische autonomie
Ja
Instrumentarium om controle te behouden of te verwerven 8
Behouden 8a
Versterken binnenlandse markt 1
X Staatsdeelneming
X Slimme aanbestedingen / Subsidies
X Participatie / Medezeggenschap
X Launching Customership
X Debt on Equity Financiering
X Vlaggenschepen - Totstandbrenging van grootschalige infrastructuurprojecten ter ondersteuning
X Ondersteunen van vervanging van buitenlandse sleuteltechnologieën
X Versterk overlevingsmaatregelen, steun aan belangrijke leverancier
X Sponsoring
Voorwaarden opleggen in verband met verandering van zeggenschap 2
X Gouden aandelen door de overheid
X Condities in "terms sheets" van investeerders
X Voorwaarden voor nieuwe aanbestedingen door particuliere ondernemingen
Talent behouden 3
X Ondersteunen en bevorderen wetenschap
X Carrièreplanning
X O&O financiering
X Uitvoer blokkeren (FDI-bespreking)
Verwerven 8b
Kennisopbouw 4
X Fundamentele Kennis / TRL - niveaus
X Toegepaste Kennis
X Engineering
X Workforce Development / Absorptievermogen
X O&O financiering
X Taskforce Economisch Veiligheid
Productie 5
X Door de overheid
X Afdwingen
Investeringen 6
X Slimme aanbesteding
X Overheidsdeelname in bedrijven
X Staatsdeelneming, Participatie / Medezeggenschap
X Launching Customership
X Debt on Equity Financiering
X Verbeteren van investeringsklimaat
X Exportondersteuning - overheidssteun voor relevante vergunningen of het verzekeren van kredietrisico
X Subsidies
X Vlaggenschepen - totstandbrenging van relevante vergunningen of het verzekeren van kredietrisico
X Financiering borgen
X Overname door de overheid
Regelgeving 7
X Wetgeving
X Spoedwetten
X Certificering
X Standaarden/Protocollen-Transparantie
X Auditing en toezicht
X Bevorderen Level Playing Field / Markttoegang controle
X Octrooien / IP bescherming
X Versoepelen Mededingingskader
X Noodwetgeving en noodbevoegdheden
X Export control on dual-use goederen
X Regels Industrieveiligheid / ABDO
X Investeringstoets (toekomst)

B RACI-Matrix

Zie volgende pagina.

Hoofdcategorie	Subcategorie		Stroomschema vragen: Taken, verantwoordelijkheden en bevoegdheden Strategische Autonomie			Opmerking of toelichting	Wie: RACI - Model			
	#	Categorie	Nummer	Scorekaart 1 = zeer nadelig 5 = heel positief	Vragen	Geef toelichting of opmerkingen	Responsible	Accountable	Consulted	Informed
Start	1	Start	1a	N.V.T	Wat speelt er?					
			1b	N.V.T	Is er nu, of in de toekomst een kans of een bedreiging vast te stellen in relatie tot wat er speelt, met betrekking tot economische of nationale maatschappelijk/veiligheidsbelangen?					
Is er potentieel Economisch belang?	2	Innovatie en kennisontwikkeling	2a	2	Beschikt Nederland (of de EU) over een gerenommeerde kennisbasis? (Kenniswerk, IP, fundamenteel onderzoek)					
			2b	3	Is Nederland (of EU) in staat om de valorisatieketen te doorlopen?					
			2c	5	In welke mate zijn de resultaten van de innovatie en kennisontwikkeling t.a.v. de capaciteit gebord voor Nederland en de EU					
			2d	1	Wat gebeurt er als de ontwikkeling van de capaciteit verdwijnt in Nederland (of EU)?					
			2e	1	Wat zijn hiervan mogelijke ongewenste spillover-effecten of keteneffecten?					
	3	Marktwerking/concurrentie	3a	4	Is er al een toepassing in de markt? (nu, over 5 of 15 jaar)					
			3b	1	Is Nederland voor de toepassing afhankelijk van niet Europese leveranciers?					
			3c	2	Zijn er concurrerende partijen in Nederland of de EU actief?					
			3d	1	Kunnen bedrijven hun activiteiten uitbreiden?					
			3e	1	Kunnen nieuwkomers actief worden op deze markt?					
			3f	4	Is er een volwassen interne markt?					
Is er een potentieel nationaal maatschappelijk/veiligheidsbelang?	4	Generieke vragen potentieel nationaal maatschappelijk/veiligheidsbelang	4a	1	Kan de beschikbaarheid, vertrouwelijkheid en integriteit van informatie, kennis en dienstverlening geschaad worden? (nu, over 5 of 15 jaar)					
			4b	2	Wie heeft het eigendom/ de zeggenschap?					
			4c	3	Is (gedeeltelijke) vervreemding van of export van IP, kennis of dienstverlening aan een buitenlandse partij onwenselijk?					
			4d	1	Is er een potentieel conflict tussen jurisdicties?					
			4e	2	Zijn er mogelijke kwetsbaarheden aanwezig in de capaciteit (technologie/product/organisatie)? Is er een 'achterdeur' dreiging? Is de administratieve toegang van derden toto de diensten en apparatuur een dreiging?					
			4f	1	Wat is het risico van uitval of verstoring van de capaciteit op nationale/internationale veiligheidsbelangen?					
	5	Militaire toepassingen en inlichtingen	5a	4	Wat is het risico van deze toepassing of technologie voor ons militaire- of inlichtingendomein?					
			5b	5	Zijn er andere vertrouwde (buitenlandse) partijen (bij bondgenoten) die aanvaardbare substituten kunnen verzorgen?					
	6	Belang van de toepassing of technologie voor NL'se vitale processen	6a	3	Is Nederland zelfredzaam met de beschikbare kennis en kunde om de toepassing of technologie autonoom te gebruiken voor veilig functionerende vitale functies?					
			6b	4	Is er voldoende controle en toezicht op de toepassing van de technologie in het vitale proces beschikbaar (houd rekening met de supply chain)?					
Synthese	7	Synthese	7a	N.V.T	Is er een economisch en/of nationaal maatschappelijk/veiligheidsbelang? (Wat is (de forecast van) het belang (nu, 5 of 15 jaar)?					

Belangen | Categorieën | Score | Vragen | Toelichting op het antwoord | RACI

C Handleiding vaststelling interventienoodzaak en handelingsperspectief Strategische Autonomie Cybersecurity

1. Inleiding

Voor u ligt een handleiding die onderdeel vormt van een instrument voor beleidsanalyse en besluitvorming. Het biedt concrete ondersteuning bij het vraagstuk of in voorkomend geval de overheid interventie zou moeten en kunnen plegen om de strategische autonomie op cybersecurity te garanderen of herstellen. Voorbeelden van deze overwegingen zijn: een buitenlands bedrijf wil een belangrijk cybersecurity bedrijf overnemen, of Nederland ziet zich genoodzaakt de kennispositie op een bepaald deelterrein te garanderen of versterken.

Het instrumentarium beoogt daarbij op systematische wijze handvatten te bieden bij vragen die opkomen met betrekking tot:

- Welk departement of directie is waar voor verantwoordelijk?
- Welke perspectieven dienen er (op korte en lange termijn) tegen elkaar worden afgewogen?
- Welke overwegingen moeten een rol spelen?
- Waar liggen de grensvlakken en relaties tussen verschillende domeinen?
- Welke handelingsperspectieven zijn er om te interveniëren?
- En wat zijn daarbij de voor- en nadelen?

Onderdeel van het instrumentarium zijn deze handleiding, het bijbehorende Stroomschema ‘Strategische Autonomie Cybersecurity’ en een Excel-bestand RACI-Matrix.

Het stroomschema en bijbehorend Excel-bestand kunnen worden gebruikt om de noodzaak tot het borgen van de strategische autonomie op cybersecurity vast te stellen, evenals het identificeren van de ondersteunende instrumenten die hieraan kunnen bijdragen. Hierbij is rekening gehouden met de samenhang tussen cybersecurity enerzijds en economische, maatschappelijke en nationale veiligheidsbelangen anderzijds.

Aan de hand van deze handleiding wordt u in een logische volgorde stap voor stap door het stroomschema geleid en gevraagd om inschattingen, antwoorden, inzichten en verantwoordelijkheden vast te leggen. Daarbij wordt eerst de opbouw van het stroomschema op hoofdlijnen besproken; daarna worden alle individuele stappen toegelicht.

Allereerst wordt een korte toelichting gegeven van het proces om dit instrumentarium in een interdepartementale context toe te kunnen passen.

2. Toepassing van het instrumentarium in een interdepartementale context

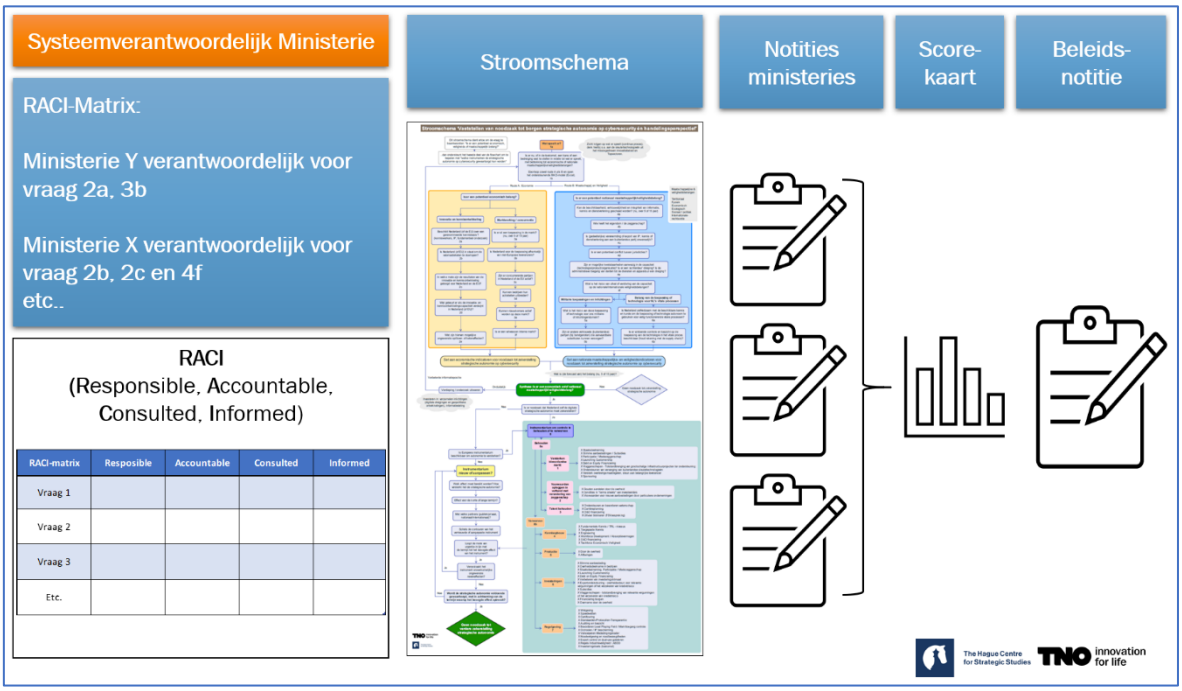
Zoals verderop in de handleiding wordt toegelicht is het belangrijk om te bepalen wie voor een bepaald vraagstuk de systeemverantwoordelijke is, en die de regie neemt op het doorlopen van het stroomschema. Dit is als een expliciet beslismoment in het stroomschema opgenomen. Deze systeemverantwoordelijke is verantwoordelijk om andere departementen te vragen bepaalde onderdelen van de RACI-Matrix in te vullen, en alle antwoorden samen te voegen tot één beleidsnotitie.

Een mogelijke *rule of thumb* om te bepalen wie bij welke trigger de systeemverantwoordelijke zou kunnen zijn is:

- Incident: NCTV
- Langere termijn cryptostrategie: BZK
- FDI/overname, Kennisborging, markt falen: EZK

Uiteraard zal de waarheid altijd wel ergens in het midden liggen. Maar het is wel belangrijk deze systeemverantwoordelijke te identificeren om te waarborgen dat het hele proces gestructureerd en geharmoniseerd wordt uitgevoerd.

Het is goed om de vragen door verschillende departementen (of andere actoren zoals een toezichthouder, of een regionale ontwikkelingsmaatschappij) in te laten vullen: sommige vragen passen van nature goed bij de expertise van een specifiek departement, maar bij andere vragen wil je juist verschillende perspectieven van diverse departementen en actoren krijgen. Op deze manier kan je ook beter de bevindingen uit de economische pijler en de veiligheidspijler van de flowchart met elkaar integreren. Het wordt aanbevolen om aan de hand van het stroomschema en RACI-Matrix gezamenlijk een beleidsnotitie op te stellen op basis van diverse separate notities die door de betreffende departementen worden opgesteld (zie Figuur 1 voor een schematische weergave van dit proces). De nummeringen uit het stroomschema kunnen worden gebruikt om de beleidsnotitie te structureren. Het is een goede werkwijze om tot een goed onderbouwd, gezamenlijk en goed gestructureerd beleidsadvies te komen. En dat dus ook als basis gebruikt kan worden om gecoördineerd de voorgenomen interventies uit te voeren.



Figuur 1: Procesweergave van het gebruik van het instrumentarium 'Strategische Autonomie Cybersecurity'

De beantwoording van de vragen moet goed beargumenteerd worden. Scores kunnen hierbij helpen om dit meer te objectiveren. En die weging is ook van invloed op wie welke effort moet gaan steken om welke interventie uit te gaan voeren. Per vraag dient een kwalitatieve beschrijving van de situatie te worden gegeven, de noodzaak om al dan niet te interveniëren, en de rationale daarachter. Bij een advies om te interveniëren moet worden aangegeven welk instrumentarium in te zetten en waarom deze keuze is gemaakt. Vervolgens dient een kwalitatieve bepaling te worden gegeven van het restrisico na inzet van het instrumentarium, of dit een acceptabel restrisico is en zo nee, wat er nog extra nodig is (bijv. ontwikkeling van nieuw instrument). De algemene waardering en conclusie (en de beleidsaanbeveling) is dan het sluitstuk van de uiteindelijke beleidsnotitie.

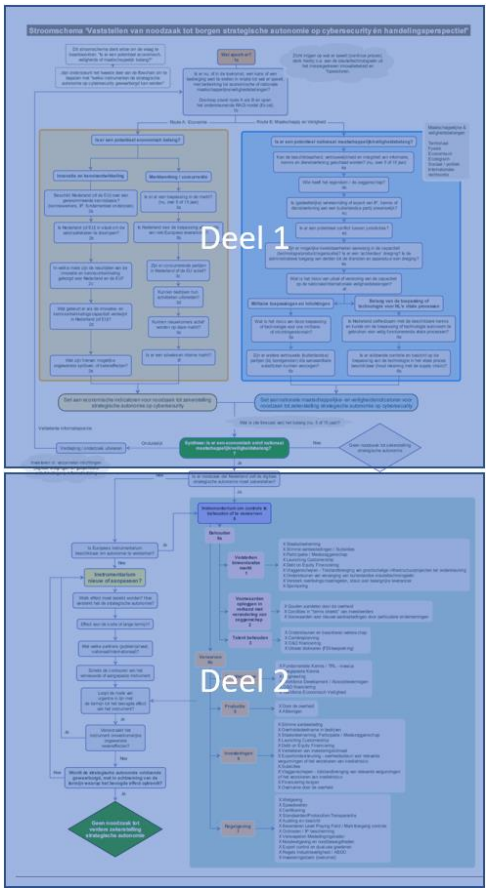
Bij de keuze van de interventies/instrumenten moet ook de urgentie worden meegenomen. Bij een hele hoge urgentie vallen automatisch al diverse instrumenten af. Daarnaast is de urgentie een belangrijke trigger voor de financiële consequenties. Bijv. moeten we budgetten van departementen samen brengen (als het enkele budget van een enkel departement ontoereikend blijkt te zijn), passen budgetten niet bij de voorziene looptijd van een interventie, hoe kunnen we aanspraak maken op ander/meer budget. Voor al deze vragen dient het Ministerie van Financiën betrokken te worden.

Sommige instrumenten vallen primair onder de verantwoordelijkheid van departementen. Echter, het inzetten van die instrumenten moet niet te stevig/exclusief aan een departement worden gekoppeld. Dat moet aan een sterke opdracht gekoppeld worden om de samenwerking met andere departementen te stimuleren. Zoals tijdens de laatste workshop werd opgemerkt: “Op nationaal niveau meer autonomie door op individueel niveau wat autonomie in te leveren.” De echte impact zit uiteindelijk immers in de gezamenlijke uitvoering van de plannen

c.q. toepassing van de instrumenten. Dat valt strikt genomen buiten het stroomschema, maar wellicht kan er wel worden afgesloten met een tijdpad met maatregelen en handelingsperspectief. Hieronder valt dus ook het monitoren van de effecten van de inzet van maatregelen. Dat geeft wat meer sturing aan het daadwerkelijk implementeren van alle acties met betrekking tot het nastreven van de strategische autonomie (incl. dus het eventueel ontwikkelen van nieuwe instrumenten).

3. Het stroomschema en RACI-Matrix

Het stroomschema ‘Strategische Autonomie Cybersecurity’ bestaat uit twee delen (zie Figuur 2). Deel 1 dient om te kunnen concluderen of er een noodzaak is om de strategische autonomie op cybersecurity te borgen. Indien dat het geval is kan deel 2 worden gebruikt om keuzes te maken uit instrumenten die hieraan bijdragen. Hiermee ontstaat zicht op het handelingsperspectief.

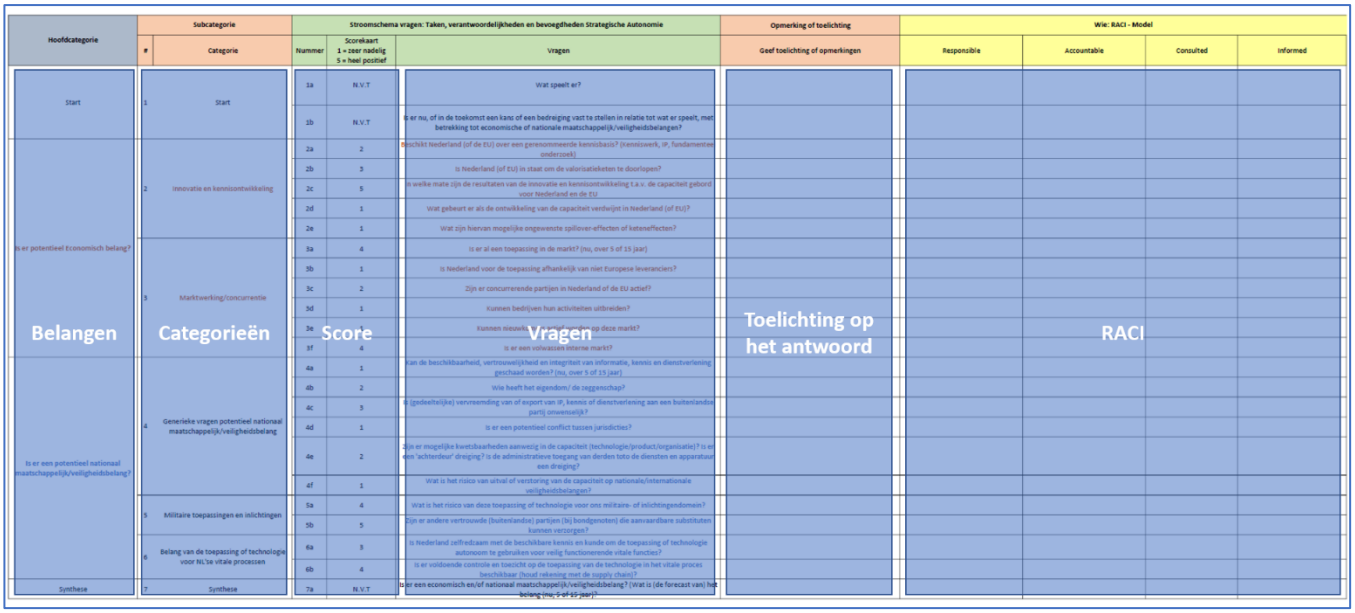


Figuur 2: Schematisch overzicht stroomschema

Elk deel van het stroomschema is opgebouwd uit een serie van vragen. In veel gevallen zal het antwoord op een vraag in het stroomschema niet direct kunnen worden gegeven omdat de desbetreffende informatie niet op voorhand beschikbaar is. Het stroomschema kan dus ook aanleiding geven tot het uitvoeren van een nadere analyse of onderzoek. Nadat het stroomschema is doorlopen kan worden bepaald of er de noodzaak is tot het versterken van de strategische autonomie op cybersecurity en met behulp van welke instrumenten dat kan worden gedaan.

Voor de beantwoording van de vragen in het stroomschema is veelal achtergrondinformatie nodig die niet in het stroomschema zelf past; die wordt in deze handleiding gegeven. De handleiding volgt de volgorde en nummering van het stroomschema.

U maakt tevens gebruik van het Excel-bestand RACI-Matrix dat bij het stroomschema hoort (zie Figuur 3). Aangezien strategische autonomie op cybersecurity een breed vraagstuk betreft, is het niet altijd eenvoudig om vast te stellen wie waarover gaat, dan wel wie het beste in staat is om antwoorden op vragen te formuleren. Daarom is de RACI-Matrix toegevoegd, waarin u per vraag kan aangeven wie voor een bepaalde casus verantwoordelijk (Responsible) is, wie aansprakelijk (Accountable), wie geconsulteerd dient te worden (Consulted) en wie geïnformeerd (Informed).

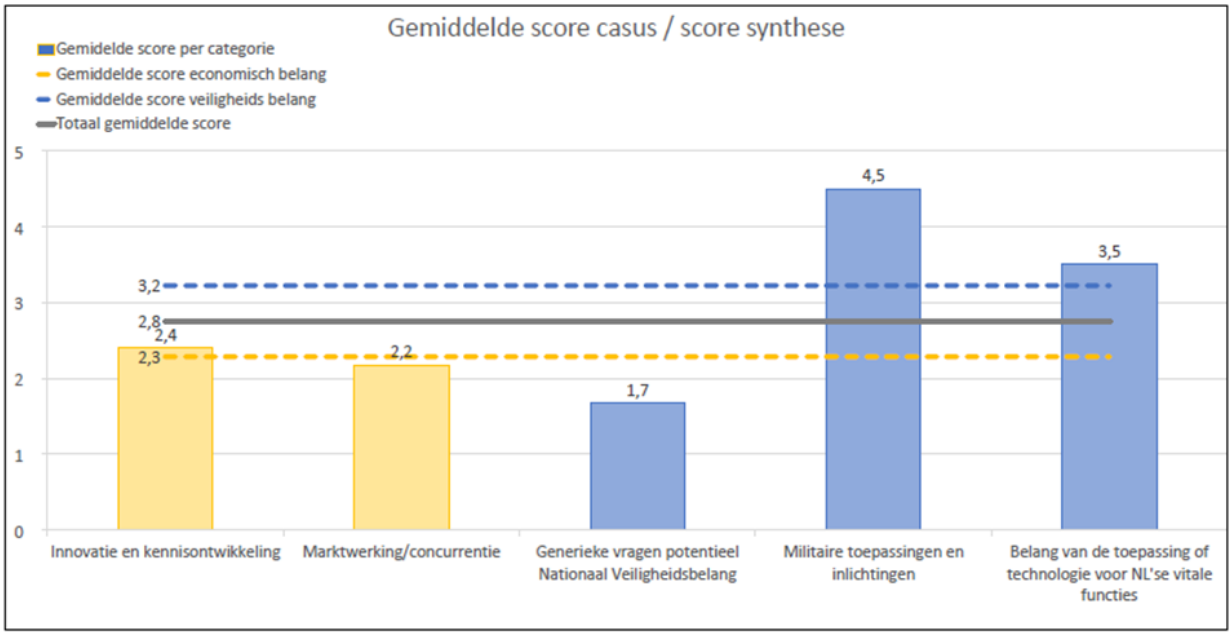


Figuur 1 Overzicht RACI-Matrix

Als in deze handleiding wordt verwezen naar een specifieke cel uit de RACI-Matrix, wordt deze verwijzing onderstreept. De RACI-Matrix wordt gebruikt bij het beantwoorden van de vragen (in deel 1) en bij het kiezen van handelingsperspectief (deel 2). Dezelfde tweedeling is ook terug te vinden in de naam van de twee tabbladen van de matrix:

In de RACI-Matrix is Kolom F (scorekaart) opgenomen. In deze kolom is er de mogelijkheid om kwalitatieve scores te geven per vraag. Het toewijzen van een score op een schaal van 1 t/m 5 is bedoeld om het belang van een vraag te objectiveren. Een score van 1 is zeer nadelig ten aanzien van de strategische autonomie op cybersecurity, en een score van 5 is heel positief waarbij over het algemeen geldt: hoe lager de score, hoe hoger de noodzaak om interventie te plegen. De scores zijn een voorzichtige kwantificering van veelal subjectieve antwoorden op de vragen en zijn in eerste instantie primair bedoeld om het gesprek te starten tussen de betrokken partijen om tot een goede onderlinge afweging van de argumenten en keuzen te komen.

De scores worden onder de vragen opgeteld in de categorieën “Economisch belang” en “Veiligheidsbelang” (zie ook Figuur 4). Bij veelvuldig gebruik van het stroomschema en het monitoren van de effecten van interventies bij meerdere cases, is het mogelijk een stevige basis voor deze scores op te bouwen.



Figuur 4 Gemiddelde score casus / score synthese

Met klem benadrukken wij dat de uitleg van de score op dit moment belangrijker is dan de feitelijke score die gegeven wordt.

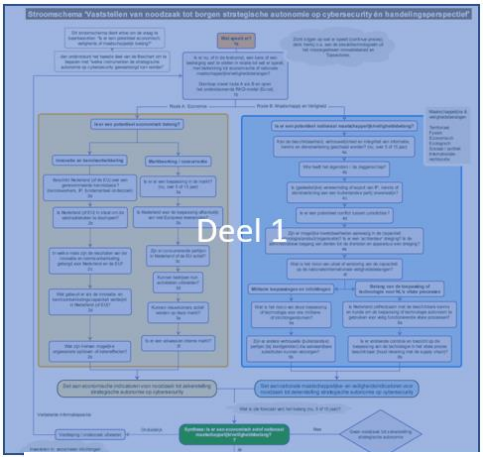
Ten slotte is het nog van belang om te beseffen dat het stroomschema niet altijd volledig doorlopen hoeft te worden. Sommige aspecten zullen voor een bepaald thema niet of minder relevant zijn en kunnen in dat geval worden overgeslagen. Gebruikers kunnen hierin zelf beargumenteerde beslissingen maken. Vele onderdelen uit het stroomschema zijn belangrijk en relevant, maar vormen niet noodzakelijkerwijs een vast onderdeel van de analyse en de besluitvorming. Mochten er vragen lastig of gecompliceerd zijn om te beantwoorden, dan is het goed om te rade te gaan waarom dit zo is, in plaats van deze zondermeer over te slaan.

4. Beschrijving van en toelichting op de vragen uit het stroomschema

Aan de hand van de informatie in dit hoofdstuk wordt u in staat gesteld om het stroomschema te gebruiken. In chronologische volgorde treft u hier toelichtingen aan voor de vragen in het stroomschema.

Deel 1: Is er een noodzaak tot borgen van de strategische autonomie op cybersecurity?

Context: Wat speelt er en wie wordt betrokken?



Figuur 5 Stroomschema deel 1

1. Vraag 1a: Wat speelt er?
De eerste stap is de beschrijving van de casus en het kaderen van het technologiegebied. In sommige gevallen is dit betrekkelijk eenvoudig of eenduidig – bijvoorbeeld voor 5G – terwijl in andere gevallen de kadering eerst dient te worden vastgesteld. Wat vaststaat is dat er iets speelt op het gebied van cybersecurityonderzoek, -innovatie, -toepassing, of -gebruik wat de aandacht trekt en de vraag oproept of dit de strategische autonomie op cybersecurity raakt.
Om te bepalen of het een passende cybersecurity casus is, kan gebruik worden gemaakt van technologiegebieden uit de publicaties van het Analistennetwerk Nationale Veiligheid (ANV)[5], of bijvoorbeeld de Kennis en Innovatie Agenda (KIA) Veiligheid[6]. In de KIA zijn zogenoemde sleuteltechnologieën opgenomen waarvan het belang reeds is onderkend. Dit zijn *Artificial intelligence* (incl. *machine and deep learning*), *Big data* en *data analytics*, *Encryption technologies*, D*igital security*, *Blockchain*, *High Performance Computing*, *Grid Computing* en *Cloud Technologies Computing*. Ook kan een technologische impactbeoordeling uitgevoerd worden om te bepalen of het een sleuteltechnologie is die aan de basis ligt van andere technologische innovaties.

2. Vraag 1b: Is er nu, of in de toekomst, een kans of een bedreiging vast te stellen in relatie tot wat er speelt, met betrekking tot economische of nationale maatschappelijke/ veiligheidsbelangen?

In dit gedeelte van het stroomschema draait het om de vraag of er een aanleiding is voor interventie ter bescherming of bevordering van ***strategische autonomie* cybersecurity**. Om tot de beantwoording van deze vraag te komen worden twee routes in het stroomschema doorlopen.

[5] Zie het Analistennetwerk Nationale Veiligheid, publicaties te downloaden via https://www.rivm.nl/onderwerpen/nationale-veiligheid
[6] KIA Veiligheid (2019), online: https://www.nwo.nl/sites/nwo/files/assets/KIA%20Veiligheid%20-%2020191015%20definitief_0.pdf

De gele **Route A: Economie** helpt inzicht te ontwikkelen op de vraag of er een potentieel economisch belang is door aan de ene kant de impact op innovatie en kennisontwikkeling te analyseren, en aan de andere kant de marktwerking en concurrentie te beoordelen. De blauwe **Route B: Maatschappij en Veiligheid**, richt zich op de nationale maatschappelijke- en veiligheidsbelangen van Nederland, zoals beschreven in de Nationale Veiligheidsstrategie.[7]

In deze stap moet worden vastgesteld wie de **systeemverantwoordelijke** is voor de betreffende casus. De systeemverantwoordelijke is het verantwoordelijke ministerie voor een onderwerp, gebeurtenis of belang waarvoor strategische autonomie mogelijk geborgd moet worden. Zij is penvoerder van het proces in het stroomschema en draagt zorg voor het bundelen van informatie die geleverd wordt door derden (andere ministeries, of andere organisaties zoals bijvoorbeeld een toezichthouder, een industrie, of een externe expert).

> De laatste Europese producent van een belangrijk cryptocomponent meldt zich aan voor niet Europese investeerdersrondes
>
> Bepaal (gezamenlijk) welk departement de systeemverantwoordelijke is (EZK) en duid de rollen van de andere departementen of derden in de casus (Defensie, JenV, etc.). Bereid ze voor om informatie toe te laten sturen en betrek ze in het proces om een standpunt te vormen.

Het systeemverantwoordelijke ministerie(of onderdeel van een ministerie) wordt opgeschreven in cel 3K. De systeemverantwoordelijke nodigt andere partijen (ministeries, organisaties, experts) uit om antwoorden te leveren die nodig zijn bij de vragen in het stroomschema. Elke partij levert de antwoorden in een separate notitie aan die vervolgens door de systeemverantwoordelijke worden geïntegreerd in 1 beleidsnotitie met aanbevelingen.

Om te bepalen wie de verantwoordelijke en relevante partijen zijn, kan de RACI-matrix gebruikt worden. Deze matrix vraagt de rollen en verantwoordelijkheden inzichtelijk te maken middels een onderscheid in vier rollen: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed.

[7] Deze omvatten: (1) territoriale veiligheid; (2) fysieke veiligheid; (3) economische veiligheid; (4) ecologische veiligheid; (5) sociale en politieke stabiliteit, en (6) de internationale rechtsorde. Bron: RIVM https://www.rivm.nl/onderwerpen/nationale-veiligheid

Responsible (operationele verantwoordelijkheid)	dit gaat over de persoon of organisatie die de taak uitvoert. Hij of zij legt verantwoording af aan de eindverantwoordelijke (Accountable);
Accountable (Systeemverantwoordelijke)	deze persoon/organisatie is eindverantwoordelijk voor het voltooien van een of meerdere projecttaken. Aan de eindverantwoordelijke wordt dus verantwoording afgelegd en hij of zij keurt een taak goed of af;
Consulted (Geconsulteerd)	aan deze persoon/organisatie wordt vooraf advies gevraagd. Hij of zij moet goedkeuring of input leveren bij een bepaalde taak in het project;
Informed (Geïnformeerd)	deze persoon/organisatie wordt geïnformeerd over de beslissingen in de voortgang van het proces of project. Hij of zij kan het resultaat van de taak natuurlijk niet beïnvloeden.[8]

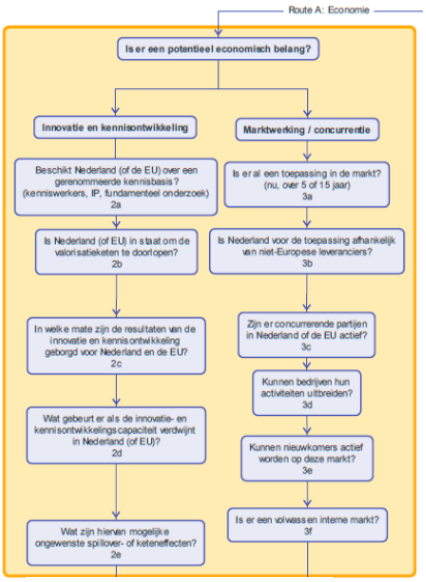
Het is binnen de Rijksoverheid niet altijd eenduidig wie waarover gaat als er een casus speelt, en wie welke RACI-rol vervult. In het belang van het stroomschema en het verkrijgen van eerste inzichten is het wel van belang dat iemand de rol van systeemverantwoordelijke opneemt. Mocht later in het proces blijken dat een andere partij de rol van systeemverantwoordelijke beter op zich kan nemen, dan kan dit alsnog worden aangepast. Met deze aanpak stelt de Rijksoverheid zich in staat om in ieder geval een proceseigenaar aan te stellen die zorg draagt voor het verkrijgen van informatie gegeven de casus.

Zodra de benodigde partijen en hun respectievelijke rol(len) zijn vastgesteld, worden **route A** en **route B** uit het stroomschema doorlopen om de vragen te beantwoorden. Per vraag of set van vragen kan de systeemverantwoordelijke dus aan andere partijen informatie vragen. U gebruikt vanaf hier tegelijkertijd het stroomschema en de RACI-Matrix.

[8] Uitleg RACI-rollen overgenomen van: https://www.getapp.nl/blog/2116/wat-is-raci-model-een-uitleg-excel-voorbeeld.

Route A: Economie: is er een potentieel economisch belang? Hoe ziet de innovatie en kennisontwikkeling eruit, en het speelveld van marktwerking en concurrentie?

Onderdeel Innovatie en kennisontwikkeling



Figuur 6: Route A - Economie

3. Vraag 2a: Beschikt Nederland (of de EU) over een gerenommeerde kennisbasis? (kenniswerkers, intellectueel eigendom (IP), fundamenteel onderzoek)

Voor het ontwikkelen van een vooruitstrevende en concurrerende economische bijdrage op nieuwe technologiegebieden is een sterke kennisbasis, intellectueel eigendom (Engels: IP) en innovatiekracht noodzakelijk. Bij het inventariseren van de kennisbasis moet niet alleen naar Nederland worden gekeken maar ook naar de EU. Nederland is soms te klein om op alle relevante kennisgebieden voorop te lopen en internationale samenwerking bij fundamenteel onderzoek is onvermijdelijk en vaak ook noodzakelijk.

Bedenk hierbij of Nederland over kwalitatief hoogstaande onderzoeksinstellingen, onderzoekers en (nationale en internationale) samenwerkingsverbanden beschikt en of deze (internationaal) ook in hoog aanzien staan. Daarbij kunt u bijvoorbeeld kijken naar het aantal gepubliceerde artikelen door Nederlandse onderzoekers of onderzoeksinstellingen. Ook wanneer de kennisbasis smal is, kan Nederland een relevante bijdrage aan de ontwikkeling van een technologiegebied leveren.
Mogelijke andere relevante indicatoren bij deze vraag zijn: is er een gebrek aan academische financiering en is daarmee de basis te beperkt dan wel ondergraaft dit belangrijke academische mogelijkheden? Hier kan de vergelijking met andere landen worden gemaakt. Zijn er aanwijzingen dat een braindrain plaatsvindt? Is er een risico dat belangrijk academisch talent verloren gaat waardoor kennis verdwijnt of onafhankelijk advies dreigt verloren te gaan?

4. Vraag 2b: Is Nederland (of EU) in staat om de valorisatieketen te doorlopen?

De toegevoegde waarde van fundamenteel onderzoek wordt voor een belangrijk deel geleverd door de mate waarin deze kennis kan worden doorontwikkeld tot concrete producten en diensten. Er moet dus ook worden gekeken naar het functioneren van de gehele valorisatieketen, waarbij ook de vraagzijde mee kan worden genomen.

Denk bijvoorbeeld aan de vraag of er voldoende partijen zijn die specifieke behoeften kunnen identificeren en bereid zijn om te investeren of om (publieke of private) investeringen aan te trekken. Ook kan het zijn dat er binnen de EU nog geen publieke en/of private partijen zijn die bereid zijn te investeren in kennisontwikkeling terwijl dit buiten de EU wel gedaan wordt .

5. Vraag 2c: In welke mate zijn de resultaten van de innovatie en kennisontwikkeling geborgd voor Nederland en de EU?

Voorbeelden van mogelijke indicatoren zijn: bescherming van Intellectueel Eigendom; programma's om innovaties door eindgebruikers te laten inzetten (door hun absorptievermogen te ondersteunen/verhogen); consortia met meer dan 50% aan Nederlandse of Europese onderzoekers of ontwikkelaars; innovatie en kennisontwikkeling dat onderdeel is van meerjarige routekaarten van de overheid.

6. Vraag 2d: Wat gebeurt er als de ontwikkeling van de capaciteit verdwijnt in Nederland (of EU)?

Is de overheid bekend met de rol die zij speelt in de ontwikkeling van capaciteiten op het gebied van het, voor de betreffende casus, relevante cybersecurityonderzoek en -innovatie, en de toepassing ervan? Zo ja, hoe groot is die rol en hoe overtuigd is Nederland of de EU van het gegeven dat de ontwikkeling blijft lopen zoals tot nu toe ? Zo nee, is de overheid op de hoogte van effecten (risico's) die mogelijk ontstaan wanneer de ontwikkeling uit Nederland of de EU verdwijnt? De status van de ontwikkelingen en de effecten van geografische verplaatsing van activiteiten kan bepaald worden door een impactassessment op de betreffende innovatie en kennisontwikkeling.

7. Vraag 2e: Wat zijn mogelijke ongewenste spillover-effecten?

Een laatste belangrijk aspect rondom innovatie en kennisontwikkeling is het inzichtelijk maken welke mogelijke spillover-effecten kunnen optreden. Indien financiering van onderzoek door partijen van buiten de EU wordt vergroot bestaat het risico dat de *marketization* daarvan ook vooral door die partijen zal worden gerealiseerd. Ook als de kennisopbouw (onderzoek) voor iedereen toegankelijk is, kan een (te) beperkte betrokkenheid van bedrijven uit Nederland en de EU tot gevolg hebben dat de economische voordelen voornamelijk bij partijen buiten de EU komen te liggen. Een sterke kennisbasis kan dan alsnog tot gevolg hebben dat de EU afhankelijk wordt van belangrijke delen van de valorisatieketen die in handen zijn van deze buitenlandse bedrijven.

Onderdeel Marktwerking / concurrentie

8. Vraag 3a: Is er al een toepassing in de markt? (nu of over 5 of 15 jaar)

Deze vraag bepaalt of er nu of op een termijn van 5 of 15 jaar, een toepassing op de markt bestaat of gaat ontstaan. Indien de toepassing er al is kan dit meer urgentie geven in het bepalen van de noodzaak tot het borgen van strategische autonomie dan wanneer dit in de toekomst speelt. Dit gegeven heeft ook direct invloed op de keuzes die gemaakt worden in deel 2 van het stroomschema. Sommige instrumenten / interventies leveren pas later effect dan menig ander instrument.

9. Vraag 3b: Is Nederland voor de toepassing afhankelijk van niet-Europese leveranciers?

Een te grote afhankelijkheid van één (niet-EU) aanbieder, zowel van diensten als de onderliggende soft- en hardware, evenals een gebrek aan competitie brengt naast cybersecurityrisico's ook economische risico's met zich mee. Bijvoorbeeld het ontstaan van marktmonopolies en prijsstijgingen, die vervolgens kunnen bijdragen aan een groeiende Nederlandse en Europese innovatieachterstand en potentieel

marktfalen. Hoe afhankelijker Nederland of de EU is van één partij, hoe groter de economische impact is van mogelijke verstoringen in de levering van een bepaalde dienst. Voldoende en eerlijke concurrentie zorgt voor een goede marktwerking waarin deze afhankelijkheid wordt geminimaliseerd en waar bestaande bedrijven hun activiteiten kunnen uitbreiden terwijl nieuwe bedrijven nog kunnen toetreden.

10. Vraag 3c: Zijn er concurrerende partijen in Nederland of de EU actief?

Open concurrentie is een belangrijke voorwaarde voor een vrije Europese handel en de totstandbrenging en het goed laten functioneren van de Europese interne markt. Is er (de facto) sprake van een monopolie, of is er genoeg keuze voor wat betreft producten en aanbieders zodat er substitutie mogelijk is?

11. Vraag 3d: Kunnen bedrijven hun activiteiten uitbreiden?

Een volgende vraag is of bedrijven in staat zijn om bestaande activiteiten uit te breiden of toe te treden tot het onderhavige marktsegment? Of is er sprake van markonderdrukking, met andere woorden, dreigen de marktkrachten een belangrijke leverancier van de desbetreffende (sleutel)technologie uit de markt te drukken? Of is zelfs sprake van een bedreiging voor een sleutelonderneming door een faillissement (bijvoorbeeld als gevolg van een gebrek aan financiering, of een gebrek aan een binnenlandse markt)? Dreigt een leverancier van een kritische sleuteltechnologie, -dienst of -infrastructuur te verdwijnen?

12. Vraag 3e: Kunnen nieuwkomers actief worden op deze markt?

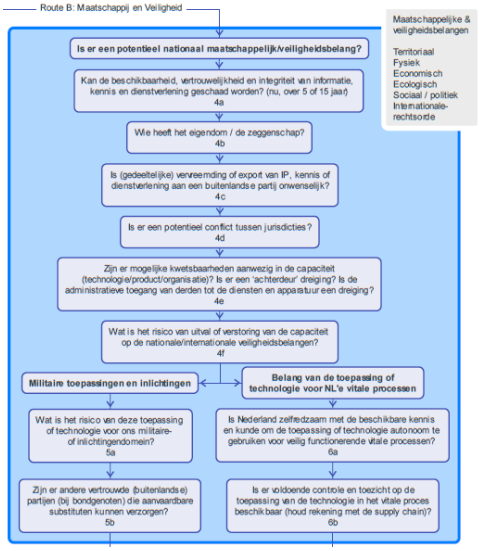
Daarnaast is het van belang om zicht te krijgen op de mate waarin nieuwe bedrijven in staat zijn toegang tot het marktsegment te krijgen. Voorbeelden van mogelijke indicatoren zijn: zijn er grote barrières die toetreding bemoeilijken, zoals bijv. infrastructurele benodigdheden; (zeer) grote (voor)investeringseisen; wet- en regelgeving of certificeringseisen die toetreding bemoeilijken?

13. Vraag 3f: Is er een volwassen interne markt?

In hoeverre is sprake van een volwassen en een goed functionerende interne markt? Groeit de markt snel? Of is er juist consolidatie (benodigd)? Zijn er andere factoren die de groei van Europese bedrijven in de weg staan?

Route B: Maatschappij en Veiligheid: Is er een potentieel nationaal maatschappelijk/veiligheidsbelang?

Voor het beantwoorden van de vragen 4 tot en met 6 is het van belang de zes maatschappelijke en veiligheidsbelangen in het achterhoofd te houden: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit, en bescherming van de internationale rechtsorde.



Figuur 7: Route B - Maatschappij en Veiligheid

14. Vraag 4a: Kan de beschikbaarheid, vertrouwelijkheid en integriteit van informatie, kennis en dienstverlening geschaad worden? (nu, over 5 of 15 jaar)

Deze vraag bepaalt of er nu of op een termijn van 5 of 15 jaar, schade voor Nederland kan ontstaan. Bij cybersecurity draait alles om de beschikbaarheid, vertrouwelijkheid en integriteit van zowel systemen als ook informatie, kennis en dienstverlening. Vaak wordt allereerst gedacht aan de systemen en de data, maar het wegvallen van de systemen en data heeft ook effecten op kennis en dienstverlening.

Voorbeelden van mogelijke indicatoren zijn: inzetmogelijkheden (beschikbaarheid) van de (nood)diensten; verlies van vertrouwen in systemen van banken; bescherming van de data die de overheid gebruikt voor haar digitale dienstverlening, onzekerheid over de betrouwbaarheid van data uit autonome systemen en sensoren zoals GPS-signalen, weerdata waarmee automatisch genavigeerd wordt en waarmee sluizen en bruggen beslissingen nemen. Andere voorbeelden zijn de integriteit van data waarop (onderzoeks)rapporten voor de overheid zijn gebaseerd, zoals van het IPCC, stikstof, cybersecurity monitoring- en detectiealgoritmen.

15. Vraag 4b: Wie heeft het eigendom / de zeggenschap?

Wie is of wie zijn de partij(en) die juridisch gezien beslissingen kunnen nemen, en wie is de formele eigenaar van een product, dienst, software of bedrijf? Dit geeft aan welke afhankelijkheden er bestaan. Als meerdere partijen zeggenschap hebben, hoe is dan de verhouding? Wat zijn de sleutelposities, en wie zitten op die posities? Een ander voorbeeld van een mogelijke indicator is wat hun belangen zijn. Kan controle worden verloren/gewijzigd door nieuwe aandeelhouders (fondsenwerving, fusies en overnames)? Of is er een risico dat buitenlandse financiering in een bedrijf leidt tot mogelijk verlies van controle over de vaardigheden die nodig zijn om onafhankelijk advies te geven over de goede werking van sleuteltechnologieën?

16. Vraag 4c: Is (gedeeltelijke) vervreemding of export van intellectueel eigendom, kennis en/of dienstverlening aan een buitenlandse partij onwenselijk?

In sommige gevallen kan het voordelen opleveren als een buitenlandse partij een belang heeft in/bij een Nederlandse organisatie; in andere gevallen is dat ongewenst vanuit strategische autonomie oogpunt. Dit heeft te maken met afhankelijkheid van die buitenlandse partij van het intellectueel eigendom (IP) en de kennis en/of dienstverlening waar ze zich willen inkopen. Maar het heeft ook te maken met het risico dat Nederland loopt door (gedeeltelijke) vervreemding of export van het intellectueel eigendom, kennis en/of dienstverlening.

17. Vraag 4d: Is er een potentieel conflict tussen jurisdicties?

Is de aanbieder van de technologie gevestigd in een andere jurisdictie waarvan de desbetreffende wetgeving mogelijke veiligheidsrisico's introduceert? Een verschil in waarden en wetgeving in het vestigingsland kunnen potentiële belangenverstrengelingen met zich meebrengen, en kan de mate van controle en toezicht verzwakken. Het auditen en testen op een statisch moment in de tijd kan niet garanderen dat in de loop van de tijd de functionaliteit en veiligheid gewaarborgd blijven. Daarom zal dit met zekere regelmaat standaard moeten worden onderzocht, dan wel geïnitieerd worden als bepaalde voorwaarden of omstandigheden aanleiding geven om een dergelijke audit of test uit te voeren.

18. Vraag 4e: Zijn er mogelijke kwetsbaarheden aanwezig in de capaciteit (technologie/product/organisatie)? Is er een 'achterdeur'-dreiging? Is de administratieve toegang van derden tot de diensten en apparatuur een dreiging?

Bij toepassingen van nieuwe technologieën moet ook worden beoordeeld wat de impact kan zijn op de digitale veiligheid. Dit vergt een cybersecurity risicoanalyse om na te gaan of het vertrouwen in, en de controle op de technologie afdoende is. Daarnaast moet er bij de beantwoording van deze vraag ook specifiek worden gekeken naar de aanbieder van de technologie. Met andere woorden: kan de aanbieder een cybersecurity basisniveau aan veiligheid bieden, of introduceert die een onacceptabel cybersecurityrisico in vergelijking met andere aanbieders? Heeft de aanbieder tevens een dominante marktpositie en brengt deze positie onacceptabele cybersecurityrisico's met zich mee? Hiervoor zijn de volgende sub-vragen relevant:

Zijn we te afhankelijk van één aanbieder?

Zodra een dergelijke aanbieder failliet gaat, onder politieke druk komt te staan, zelf getroffen wordt door een groot cybersecurity incident, of doelwit wordt van economische sancties, zal dit gevolgen hebben voor hun (aanbod van) diensten. Hoe afhankelijker je bent van één partij, hoe groter de impact is van mogelijke verstoringen in de levering van een bepaalde dienst. Daarnaast kan een te grote afhankelijkheid van een (buitenlandse) aanbieder ook de kennispositie van Nederland op de lange termijn verslechteren wanneer ook de kennisontwikkeling en innovatie door deze aanbieder wordt vormgegeven. Nationale afhankelijkheid van één partij is vooral risicovol wanneer de dienst wordt gebruikt binnen een vitale infrastructuur. Daarnaast ondermijnt afhankelijkheid van één aanbieder de mate van weerbaarheid, omdat de lage verkopersdiversiteit het risico en de impact van storingen of vijandige exploitaties voor de aanbiedende partij zelf vergroot.

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

Onvoldoende productiekwaliteit, softwareontwikkeling of kwetsbaarheidsmanagement kan leiden tot systematisch falen of kwetsbaarheden die geëxploiteerd kunnen worden door externe actoren. Het is in ieder geval essentieel dat een land zelf over de kennis en capaciteiten beschikt om dit onafhankelijk vast te kunnen stellen. Zicht hebben en houden op een (mogelijke) dreiging is net zo belangrijk als te kunnen handelen in reactie op een daadwerkelijk incident.

Is er een ‘achterdeur’ dreiging?

Een ‘achterdeur’ dreiging wordt opzettelijk in de apparatuur gebouwd door de aanbieder ofwel doorgevoerd door een vijandige actor die toegang heeft tot de hardware of software van de dienst. De grootste zorg zit met name in de link tussen de aanbieder en een statelijke actor en diens intenties jegens Nederland en de EU en haar bondgenoten.

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

Administratieve toegang tot de netwerken van een dienst kan een significant cyberrisico met zich meebrengen. Deze potentieel ongeoorloofde toegang kan een heimelijk onderdeel van een onderhoudsovereenkomst of apparatuur ondersteuning vormen. Bijvoorbeeld, binnen de 5G-context geeft administratieve toegang van derden deze partijen toegang tot onderdelen van nationale kritieke telecominfrastructuur die tot mogelijke risico’s kunnen leiden in de vorm van het grootschalig verstoren of extraheren van data. Uiteindelijk zal een volledige risicoanalyse toegespitst moeten worden op de dienst of apparatuur. Zo kan worden bepaald of zekerstelling van strategische autonomie al dan niet wenselijk is vanuit cybersecurity oogpunt.

19. Vraag 4f: Ondermijnt uitval of verstoring van de capaciteit de nationale/internationale veiligheidsbelangen?

Wat kan er gebeuren wanneer de strategische autonomie niet wordt geborgd? Hoe groot is de kans daarop? En wat is de mogelijke impact op de maatschappelijke en veiligheidsbelangen?

20. Vraag 5a: Wat is het risico van deze toepassing of technologie voor ons militaire- en inlichtingendomein?

In welke mate is het risico aanwezig dat vijandige (statelijke) actoren het functioneren van vitale functies van het militaire- of inlichtingendomein kunnen beïnvloeden? Met andere woorden, wat is de veiligheidsdreiging voor (het functioneren van) onze krijgsmacht en/of inlichtingendiensten ?

21. Vraag 5b: Zijn er andere vertrouwde (buitenlandse) partijen (bij bondgenoten) die aanvaardbare substituten kunnen verzorgen?

Wanneer andere partijen (Europese, NAVO of andere bondgenoten) aanvaardbare substituten kunnen leveren, verkleint dit de afhankelijkheid van de te beschouwen situatie of technologie. In welke mate is daar hier sprake van?

22. Vraag 6a: Is Nederland zelfredzaam met de beschikbare kennis en kunde om de toepassing of technologie autonoom te gebruiken voor veilig functionerende vitale functies?

Nieuwe technologieën kunnen de nationale veiligheidsbelangen van Nederland aantasten. Dit kan het geval zijn wanneer vitale functies afhankelijk zijn van de desbetreffende technologie, of wanneer deze wordt gebruikt voor militaire, inlichtingen of andere staatsgeheime doeleinden. Het is dus belangrijk om te weten welke rol de technologie speelt in vitale infrastructuren of essentiële diensten en hoe afhankelijk deze zijn voor het functioneren ervan. Voor vitale functies en militaire of inlichtingencapaciteiten is het belangrijk te weten of Nederland (al dan niet met vertrouwde partners) zelfredzaam kan zijn.

23. Vraag 6b: Is er voldoende controle en toezicht op de toepassing van de technologie in het vitale proces beschikbaar (houd rekening met de supply chain)?

Welke afhankelijkheden bestaan er op de toepassing van de technologie? Specifiek geldt dit voor de vitale infrastructuur en vitale processen; als echter genoeg niet-vitale partijen geraakt worden kan er toch sprake zijn van maatschappelijke ontwrichting. Wie controleert op deze toepassing? Wie houdt het toezicht, en zijn hun bevoegdheden voldoende om zo nodig in te grijpen? Bovendien is soms niet inzichtelijk welke partijen afhankelijk zijn van welke technologie. Daardoor kan de verstoring van ogenschijnlijk iets kleins toch grote gevolgen hebben. In welke mate bestaat inzicht in de supply chain, zodat het (systeem)risico goed kan worden ingeschat?

24. Vraag 7: Synthese: Is er een economisch en/of nationaal maatschappelijk/veiligheidsbelang?

U bent aangekomen bij het einde van het eerste gedeelte van de flowchart die bepaalt of er een noodzaak is om strategische autonomie zeker te stellen. De vragen uit **Route A** hebben geleid tot een **set antwoorden die duiden wat de economische gevolgen zijn**. **Route B** heeft geleid tot een **set antwoorden die duiden wat de gevolgen voor de maatschappelijke en nationale veiligheid zijn**.

De toebedeelde scores 1 tot 5 in Kolom F in de RACI-Matrix zijn ingevuld en worden samengevoegd en per onderdeel weergegeven in het figuur vanaf cel B35. Deze scores zijn bedoeld om een casus verder te verdiepen en te bespreken, en is tevens een objectiveringsmethode. Het systeemverantwoordelijke ministerie brengt samen met de betrokken partijen een advies uit op grond van de notities die door elk van de andere departementen / stakeholders zijn opgesteld tijdens de beantwoording van de aan hen toegewezen vragen . De uiteindelijke beslissing tot interventie en het traject daartoe is aan het systeemverantwoordelijke ministerie. Zowel de huidige situatie als de komende 5 tot 15 jaar kunnen hier in overweging

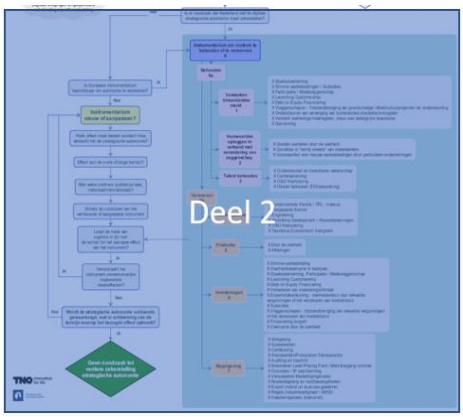
mee worden genomen. Beantwoord de vraag: **"Is er een economisch of nationaal maatschappelijk/veiligheidsbelang?"**

- Indien Nee: dan is er geen noodzaak tot zekerstelling van strategische autonomie op cybersecurity en stopt het stroomschema.
- Indien Ja: ga dan verder naar het tweede deel over het instrumentarium (***Onderdeel 8: keuzepalet instrumentarium***)
- Indien Onduidelijk: dan is een nadere verdiepingsslag of onderzoek nodig naar de onduidelijkheden om zo een sterkere informatiepositie te verkrijgen om de synthesevraag te beantwoorden; doorloop daarna weer het stroomschema vanaf vraag 1b.

Deel 2: Bepalen van het handelingsperspectief

Onderdeel 8: Keuzepalet instrumentarium

Nadat de noodzaak tot het beschermen of bevorderen van de strategische autonomie op cybersecurity is vastgesteld, zijn twee paden te doorlopen: de Nederlandse staat heeft **wel of niet** de beschikking over instrumentarium (handelingsperspectieven), nationaal dan wel in EU-verband of in samenwerking met andere vertrouwde partners. De vraag is dan of dit bestaande instrumentarium voldoende is om de autonomie te waarborgen voor de desbetreffende technologie.



Figuur 8: Stroomschema deel 2

Voor het bestaande instrumentarium wordt een onderscheid gemaakt tussen instrumenten die zijn bedoeld om controle te **behouden** of om controle te **verwerven**. De lijst kan in de loop van de tijd aangevuld worden en overlap van instrumenten is in de praktijk mogelijk. Het dient dus voornamelijk als een handreiking richting de vele instrumenten die kunnen bijdragen aan strategische autonomie op cybersecurity; nu en in de toekomst.

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

- Welk effect moet worden bereikt? Hoe versterkt het instrument de strategische autonomie op cybersecurity?
- Wordt er een effect op korte of lange termijn nagestreefd?
- Met welke partners (publiek – privaat, nationaal – internationaal) moet dit effect worden bereikt?
- Wat zijn de contouren van het vernieuwde of aangepaste instrument?
- Loopt de mate van urgentie in lijn met de termijn waarop het beoogde effect van het instrument wordt verwacht?
- Veroorzaakt het instrument ongewenste neveneffecten? En zo ja, welke?

Na het beantwoorden van deze vragen kan worden gesteld of het instrumentarium het beoogde doel van strategische autonomie op cybersecurity voldoende zal waarborgen, met in achtneming van de termijn waarop het beoogde effect optreedt en de mogelijke neveneffecten. Deze laatste stap vergt niet alleen een evaluatie van het instrumentarium voordat het wordt ingezet, maar ook in een later stadium om te evalueren of het de beoogde effecten heeft behaald. Indien de strategische autonomie voldoende wordt gewaarborgd is het einde van het stroomschema bereikt en is er geen noodzaak meer tot verdere zekerstelling van strategische autonomie op cybersecurity: