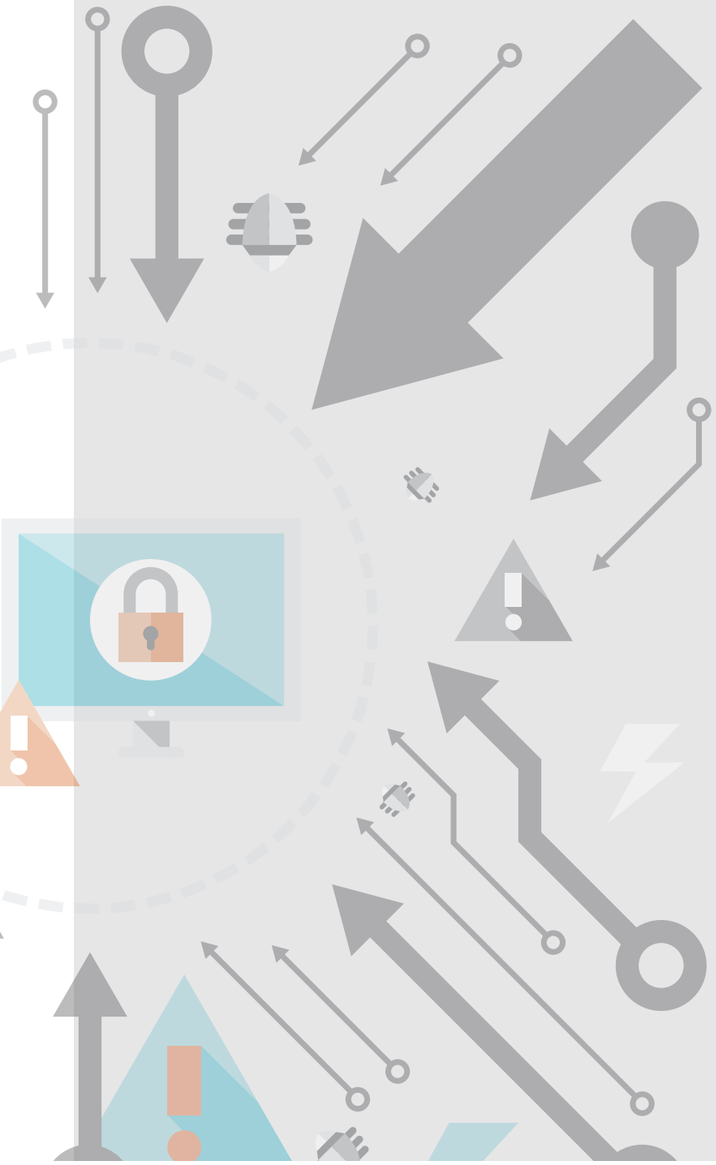
CSR Cyber Security Raad

HANDREIKING ‘TOETSINGSKADER DIGITALE AUTONOMIE EN CYBERSECURITY’



INHOUDSOPGAVE

INLEIDING

Digitale autonomie bestaat uit het vermogen en de middelen om in het digitale domein beslissingen te nemen en uit te voeren betreffende de toekomst van economie, maatschappij en democratie. De Cyber Security Raad (hierna de raad) heeft in het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'[1] geadviseerd dat digitale autonomie op het hoogste politieke en ambtelijke niveau moet worden belegd, vanuit een integrale visie op cyberweerbaarheid. Er moet gericht geïnnoveerd worden en cyberweerbaarheid moet door de overheid en het bedrijfsleven vanuit het soevereiniteitsperpectief worden aangepakt. Uitgangspunt daarbij dient te zijn: sterk in eigen huis, sterk in Europa, sterk in de rest van de wereld. Dit advies is gebaseerd op de studie 'Nederlandse Strategische Autonomie en Cybersecurity'[2] die onderzoekers Freddy Dezeure en Paul Timmers in opdracht van de raad hebben uitgevoerd. Het rapport geeft heldere inzichten in de complexe vraagstukken, illustreert dat met aansprekende actuele voorbeelden en beschrijft een toetsingskader. In opdracht van de raad hebben onderzoekers Dezeure en Timmers dit vertaald naar de Handreiking 'Toetsingskader digitale autonomie en cybersecurity'.

Doelgroep en doel van deze handreiking

De Handreiking 'Toetsingskader digitale autonomie en cybersecurity' is primair geschreven voor beleidsverantwoordelijken binnen de overheid, maar ook private organisaties kunnen gebruikmaken van de handreiking. Zowel de overheid als het bedrijfsleven moeten bewuste keuzes maken als het gaat om de afhankelijkheid van ICT-producten en diensten. De handreiking ondersteunt het nemen van passende maatregelen om digitale autonomie in cybersecurity te borgen. Het doorlopen van het toetsingskader is bij voorkeur een structurele en interdisciplinaire activiteit waarin (interdepartementale) samenwerking en kennisdeling centraal staan.

1 CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity' - CSR-advies 2021, nr. 3, mei 2021
2 Nederlandse strategische autonomie en cybersecurity, Paul Timmers en Freddy Dezeure, januari 2021

Leeswijzer en voorbereiding

Het toetsingskader is een grafische methode die het identificeren en beoordelen van belangrijke ontwikkelingen stimuleert en ondersteunt. Het biedt de gebruiker de mogelijkheid om aan de hand van het Triggerdiagram en Porter-modellen (zie Figuur 1) complexe vraagstukken over digitale autonomie op een overzichtelijke wijze te ordenen en concrete maatregelen te definiëren en te toetsen.

- Hoofdstuk 1 beschrijft de logica van het centrale element van het toetsingskader, het Triggerdiagram en illustreert het gebruik ervan. Het bevat een concrete beschrijving over hoe het Triggerdiagram te gebruiken om specifieke ontwikkelingen te onderkennen en beoordelen. De diverse quadranten worden toegelicht en er worden enkele voorbeelden van de toepassingsmogelijkheden gegeven.

- Hoofdstuk 2 geeft een beschrijving van het managementproces voor de opvolging van deze beleidsontwikkeling en hoe dit op een strategische en continue wijze te dragen en te borgen.

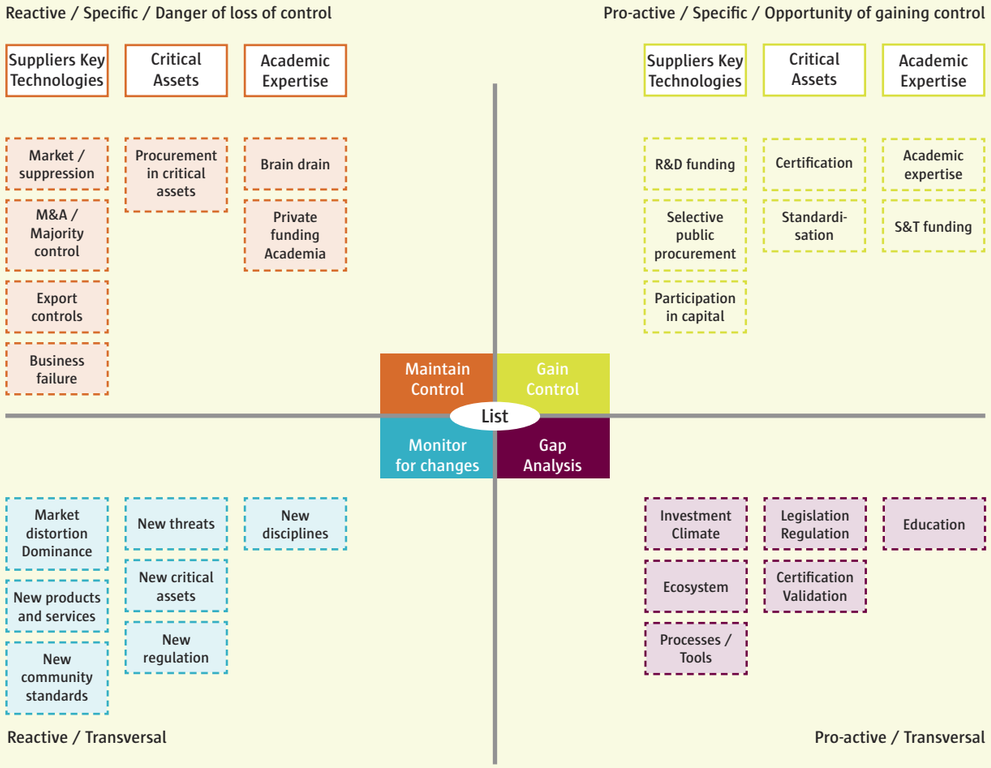
- Hoofdstuk 3 geeft een stapsgewijze beschrijving voor de beleidsontwikkelaar, om individuele ontwikkelingen te analyseren. De beleidsmedewerker kan hiermee de analyse van problemen en passende maatregelen systematisch en volledig uitvoeren.

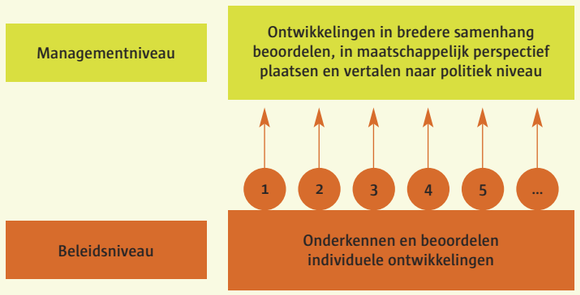
- Hoofstuk 4 biedt tezamen met de bijlagen ondersteuning bij de voorbereiding en uitvoering van de analyse. In de bijlage zijn voor het uitvoeren van de analyse en het identificeren van maatregelen een praktisch stappenplan en een illustratieve vragenlijst opgenomen.

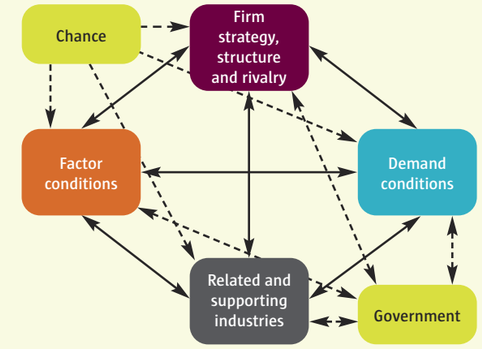
- Een centraal element als het gaat over vermogen en middelen van digitale autonomie is het beschikken over voldoende controle over sleuteltechnologieën en de daarmee samenhangende assets om cybersecurity te kunnen garanderen.

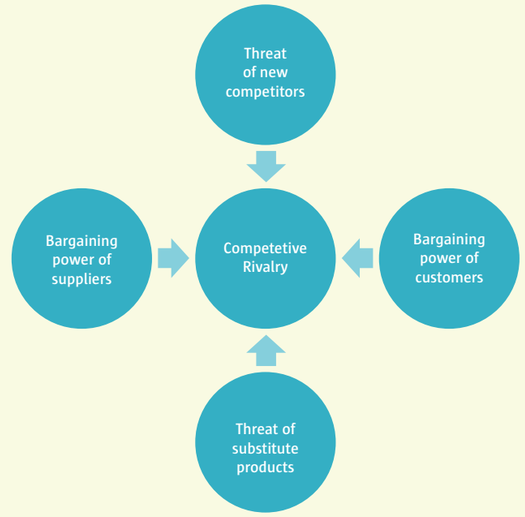
- Voor een optimaal resultaat is het raadzaam om de analyse uit te voeren met behulp van een interdisciplinaire werkgroep waar (externe) specialisten met kennis over bijvoorbeeld het technische- en inkoopdomein deel van uitmaken. Indien gewenst kan deze werkgroep gefaciliteerd worden door een expert die ervaring heeft met het toepassen van de methode.

Figuur 1: **Triggerdiagram en Porter modellen**







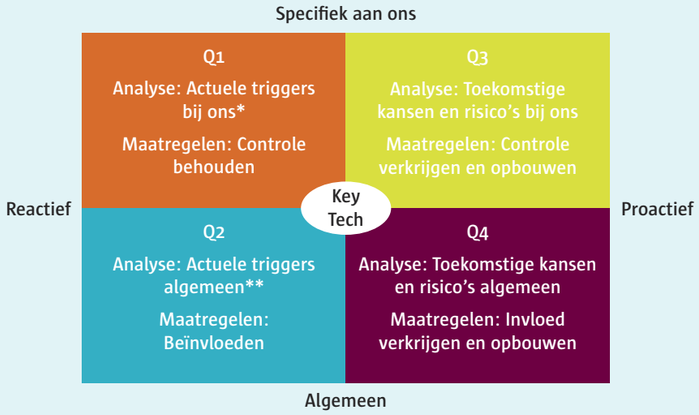


1. PROCES VOOR BELEIDS-ONTWIKKELAARS IN TEAMVERBAND: GEBRUIK TRIGGERDIAGRAM

Waar te starten?

De centrale component in het toetsingskader is het Triggerdiagram (zie Figuur 2), een innovatieve mindmap om risico's, opportuniteiten en maatregelen in kaart te brengen. Het Triggerdiagram bevat vier kwadranten, verdeeld door twee assen: reactief/proactief en specifiek/algemeen. Hiermee kunnen de risico's (reactief) en kansen (proactief) worden weergegeven per organisatie/bedrijf (specifiek) of voor de sector/markt (algemeen). Dit diagram wordt gebruikt zowel voor de probleemanalyse als voor het weergeven van de voorgestelde maatregelen die volgen uit de analyse.

Figuur 2: **Triggerdiagram**



* bij onze bedrijven, onze overheid
** bij anderen of ergens anders in de wereld

Welke kennis is nodig voor het maken van de analyse?

- In de eerste plaats is het van belang dat er kennis aanwezig is over cybersecurity én van de concrete case.
- Daarnaast is er een initieel overzicht nodig van de middelen (leveranciers, klanten, kennis, overheid) die een rol kunnen gaan spelen. Alleen op deze wijze wordt zicht gehouden op de volledigheid en logische samenhang van de analyse. Marktdynamiek-modellen, bijvoorbeeld van Porter, kunnen daarbij een goed hulpmiddel zijn. In bijlage 3[3] van deze handreiking is een toelichting opgenomen over het Porter's model voor nationale concurrentiekracht (Diamond-model). Dit model is bedoeld om op landsniveau de nationale concurrentiekracht, innovatie- en marktdynamiek te analyseren. Concreet gaat het over leveranciers, kopers, factor-condities (kennis, kapitaal, etc) en de overheid die in haar rol regels oplegt en beleid bepaalt. Het kan ook nuttig zijn de krachten die inwerken op een individueel bedrijf beter te begrijpen met Porter's Five Forces-model[4].

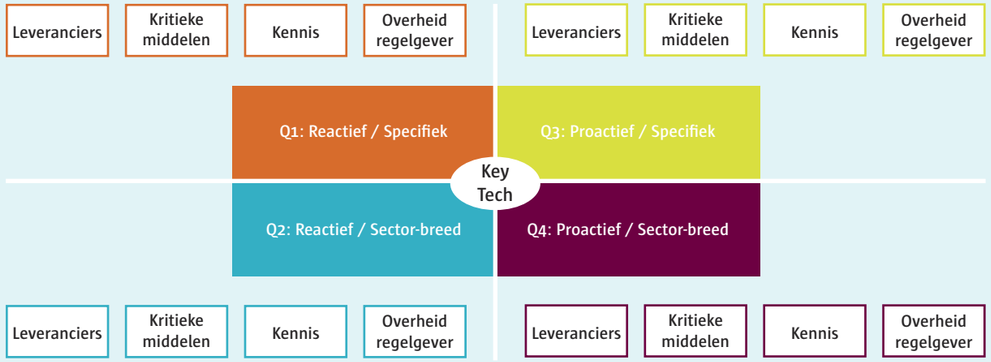
Zowel het Diamond-model als het Five Forces-model helpen om:

1. Te verifiëren dat alle relevante elementen meegenomen zijn in de analyse en maatregelen. Als deze verificatie leidt tot nieuwe elementen dan kunnen deze alsnog worden meegenomen.
2. De impact van maatregelen te begrijpen. Een specifieke maatregel kan andere factoren beïnvloeden zowel op bedrijfsniveau (marktverstoring) als op nationaal niveau (toepassing van wettelijke randvoorwaarden, budget, internationale relaties, etc.).

Wat analyseren we in elk kwadrant?

In elk kwadrant bevindt zich een aantal concrete domeinen om de kansen en risico's te analyseren. Daarin kunnen ook mogelijke maatregelen worden weergegeven die invloed kunnen hebben op deze domeinen. Deze domeinen zijn weergegeven in Figuur 3 en meer specifiek in Figuur 4.

Figuur 3: **Domeinen in het triggerdiagram**



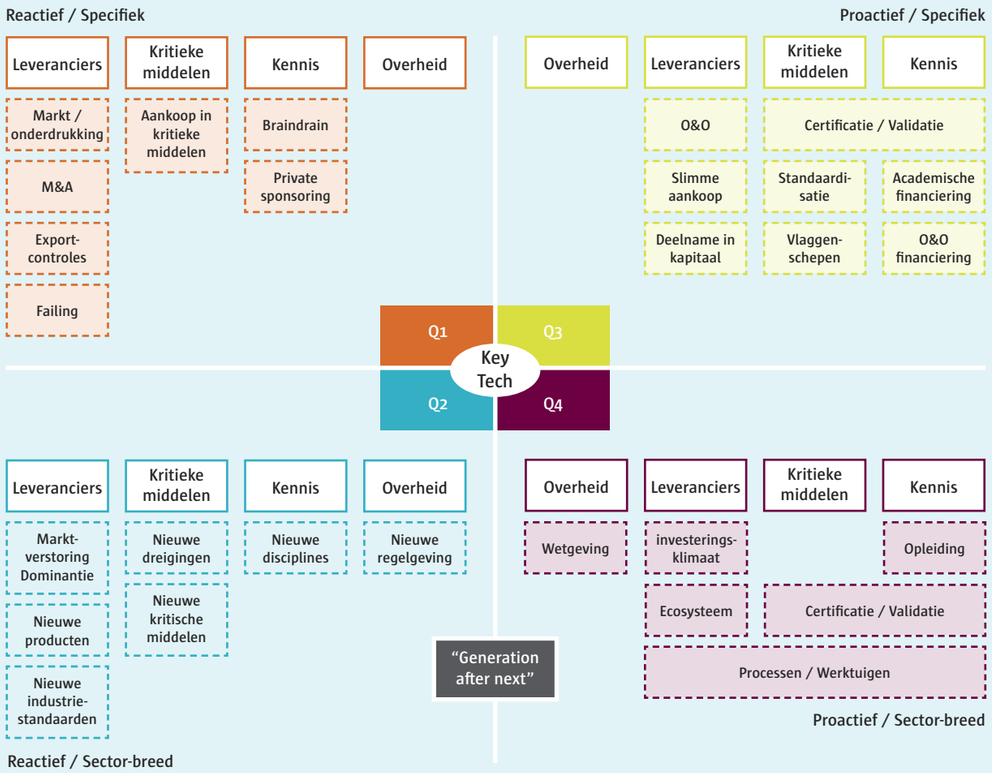
3 Bijlage 3: Porter-modellen, toelichting Diamond-model. Het staat de gebruiker evenwel vrij om een ander model voor de marktdynamiek te nemen indien dat toelaat om de compleetheid en dynamiek van triggers en maatregelen te verifiëren.
4 Bijlage 3: Porter-modellen, toelichting van het Five Forces-model. Het staat de gebruiker evenwel vrij om een ander model voor de marktdynamiek te nemen indien dat toelaat om de compleetheid en dynamiek van triggers en maatregelen te verifiëren.

Welke vragen moeten we beantwoorden?

- In het eerste kwadrant (Q1: ‘reactief en specifiek’) identificeren we dreigingen naar specifieke middelen waar we voldoende controle over hebben. Denk bijvoorbeeld aan een dreigende overname van een belangrijke (lokale) leverancier.
- In het tweede kwadrant (Q2: ‘reactief/sector-breed’) worden relevante nieuwe ontwikkelingen in kaart gebracht, bijvoorbeeld een nieuwe dreiging, een nieuw product of nieuwe wetenschappelijke inzichten. Rechts van de middenlijn worden de kansen en de anticipaties van bedreigingen weergegeven.
- Het derde kwadrant (Q3: ‘proactief/specifiek’) bevat een analyse van de eigen toekomstige kansen en risico's en welke maatregelen genomen moeten worden om hierover controle te krijgen en te behouden. Een voorbeeld hiervan is hoe meer controle te realiseren door ondersteuning van een startup in sleuteltechnologie.
- Tot slot wordt in het vierde kwadrant (Q4: ‘proactief/sector-breed’) een analyse gemaakt van de kansen uit de vergelijking met andere landen, bijvoorbeeld processen voor slimme overheidsaankopen, investeringsklimaat en overheidsprocessen of middelen om strategische autonomie te borgen. Ook worden hier de toekomstige risico’s in kaart gebracht, zoals in de geopolitiek of technologie. Zie ook Figuur 5 en 6 voor een grafische weergave op deze toelichting.

Voor het uitvoeren van de analyse en het identificeren van maatregelen is in deze handreiking een praktisch stappenplan[5] en een illustratieve vragenlijst[6] opgesteld.

Figuur 4: **Triggerdiagram met domeinen en specifieke vragen**



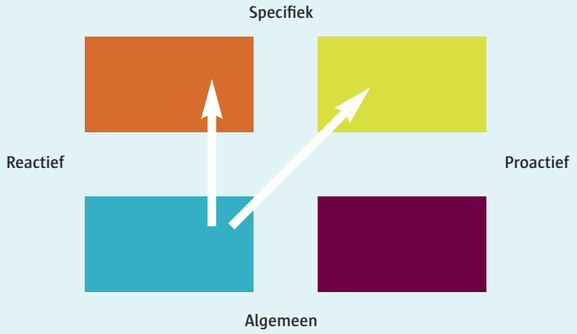
5 Bijlage 1: Stappenplan voor de identificatie van triggers en maatregelen
6 Bijlage 2: Illustratieve vragenlijst ter ondersteuning van identificatie triggers en maatregelen

Enkele voorbeelden van gebruik van het Triggerdiagram

Het Triggerdiagram kan vanuit verschillende invalshoeken doorlopen worden. Concrete cases worden in de diepte toegelicht in het onderzoeksrapport van Paul Timmers en Freddy Dezeure[7] dat zij in opdracht van de raad hebben gemaakt. We geven hier enkele voorbeelden:

1. Trigger van nieuwe en belangrijke wetenschappelijke ontwikkelingen
Een belangrijke technologische/wetenschappelijke ontwikkeling wordt geïdentificeerd (Q2). Van daaruit wordt er bekeken welke sleutelbedrijven (Q1) deze ontwikkeling kunnen omzetten in producten die de cyberveiligheid verbeteren en of we voldoende controle hebben op die bedrijven. Daarnaast kan onderzocht worden of er nieuwe startups in de steigers staan die deze ontwikkelingen kunnen valoriseren en waarover controle gewenst is (Q3). Eventueel worden bijkomende maatregelen, zoals inkoopcondities, overwogen op grond van marktdynamiek (Q3). In het onderzoeksrapport is de case ‘O&O’ in homomorfe encryptie en differentiële privacy te vinden op pagina 25, de daaruit volgende startups en de verschillende benaderingen in andere landen op pagina 32, de rol van standaardisatie en open source-initiatieven in de controle op pagina 36 en het aankoopbeleid (publiek en privaat) op pagina 38. Dit specifieke voorbeeld wordt ook toegelicht op pagina 61 van het onderzoeksrapport.

Figuur 5: **Nieuwe wetenschappelijke ontwikkeling brengt het belang van sleutelbedrijven onder de aandacht**

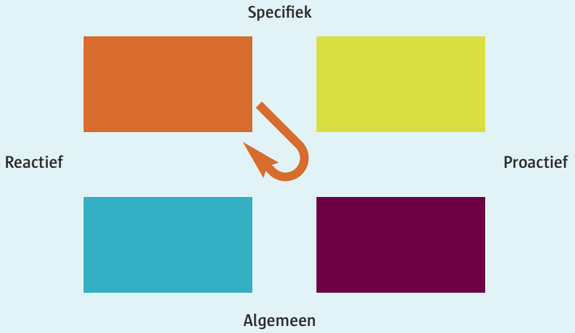


2. Dreigende overname van een sleutelbedrijf
Een dreigende overname van een sleutelbedrijf waar we controle over hebben wordt geïdentificeerd (Q1). Op basis daarvan kunnen gepaste maatregelen worden genomen om controle te behouden. De krachtenanalyse geeft inzicht om bijvoorbeeld strategische samenwerkingen en deelnames te overwegen.

In het onderzoeksrapport is meer informatie over bedrijfsovernames (M&A) en mogelijke overheidsinterventies te vinden op pagina 39.

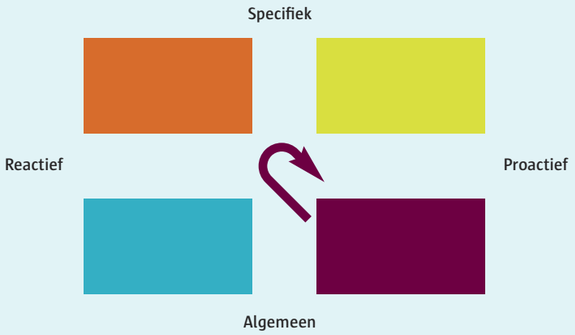
7 Nederlandse strategische autonomie en cybersecurity, Paul Timmers en Freddy Dezeure, januari 2021,

Figuur 6: **Dreigende overname van sleutelbedrijf afwenden**



3. Aanpak van andere landen bekijken en goede praktijken overnemen
Proactief wordt hier gekeken naar de vergelijking van de eigen beleidsaanpak met de aanpak van andere toonaangevende landen met een hoge internethygiëne (Q4). Wat kunnen we van deze aanpak leren en welke maatregelen moeten we nemen om de eigen aanpak te verbeteren? Zie hiervoor ook Figuur 7. Het is van belang om de rol van de overheid in deze landen te begrijpen voor het grotere ‘plaatje’ van de marktdynamiek. In het onderzoeksrapport van Timmers en Dezeure is hierover meer informatie te vinden op pagina 40, 54 en 55.

Figuur 7: **Aanpak bestuderen van landen met een 'zuiverder' internet**



4. Andere voorbeelden in het onderzoeksrapport

- Geopolitieke druk als trigger:
  5G beveiliging, met maatregelen zoals de EU 5G Security Toolbox en mogelijke rol overheid als aanjager (pagina 58).
- Wetgeving verandering als trigger:
  Herziening van de EU NIB Richtlijn en mogelijke ondersteunende maatregelen (pagina 60).

Volledigheid en coherentie

Tenslotte is het van belang om de volledigheid en de samenhang van de analyse en de te nemen maatregelen te verifiëren. Opnieuw is het dus gewenst terug te grijpen op het overzicht van marktactoren en hun relaties. Onder tijdsdruk is het gemakkelijk een belangrijke factor te vergeten (Bijvoorbeeld: Hoeveel kost het? Is de ‘oplossing’ een pleister op het probleem of is er een langdurige beleidsmaatregel gewenst die de oplossing verankert, zoals privaat-publieke samenwerking of wetgeving?).

Daarin is het van belang de samenhang te bewaken, in zowel de analyse als de te nemen maatregelen in relatie tot concrete technologie en structurele zaken rondom de organisatie/het proces. Zie hierna twee opmerkingen als toelichting hierop.

Opmerking 1:
De analyse levert waarschijnlijk een aantal digitale sleuteltechnologieën op waarop Nederland onvoldoende greep heeft. Het kan zijn dat er onderliggende sleutelproblemen zijn, die zelfs nog fundamenteler de strategische autonomie kwetsbaar maken, bijvoorbeeld omdat er onvoldoende capaciteit is voor strategische planning bij de overheid of omdat er onvoldoende kennis aanwezig is om opkomende technologieën te identificeren en er een risicodragend aandeel in te nemen. Het risico is dan dat problemen zich blijven herhalen, met als gevolg een sluipende erosie van soevereiniteit.

Opmerking 2:
De analyse moet uiteindelijk leiden tot concrete beleidsmaatregelen die de strategische (digitale) autonomie in cybersecurity versterken. Cybersecurity draait om concrete technologieën en producten en hun maakindustrie. Als de analyse alleen leidt tot procesmatige maatregelen (zelfs als die concreet zijn) zonder dat er concrete sleuteltechnologieën en bedrijven geïdentificeerd zijn, is het risico reëel dat er geen antwoord is op de actuele problemen van strategische autonomie in cybersecurity.

2. PROCES OP MANAGEMENTNIVEAU

Het proces op managementniveau veronderstelt dat het toetsingskader voor verschillende ontwikkelingen doorlopen wordt vanuit een whole-of-government benadering. Het ‘managementniveau’ is waar de resultaten van de analyse en de beleidsvoorstellen op tafel komen voor besluitvorming, proactieve sturing en/of advies aan het politieke niveau. Het management kan periodiek de verschillende analyses beoordelen en in breed perspectief plaatsen.

Het proces op managementniveau beoogt dit door middel van zes verschillende stappen die worden doorlopen. Deze zijn weergegeven in Figuur 8. Het doel van dit proces is:

- Het verkrijgen van goed overzicht van de analyses op het gebied van digitale autonomie;
- Deze in bredere samenhang te kunnen bezien en
- De prioriteiten vervolgens te vertalen naar politiek niveau.

Figuur 8: Te nemen stappen binnen het proces op managementniveau

Hieronder volgt een toelichting op elke stap binnen dit proces.

1. Kwantiteit analyse
De eerste stap betreft het beoordelen van de hoeveelheid en selectie van de beoordeelde ontwikkelingen die zijn geanalyseerd. De volgende vragen kunnen daarbij behulpzaam zijn: Voor hoeveel ontwikkelingen is het toetsingskader digitale autonomie doorlopen in relatie tot de hoeveelheid potentieel belangrijke ontwikkelingen, zoals de toenemende cyberaanvallen, marktontwikkelingen, Europese en internationale beleidsvoorstellen? Welke ontwikkelingen ontbreken in de analyse die wellicht wel moeten worden meegenomen en om welke reden zijn deze weggelaten? Hoe vaak ontvangt het management signalering over belangrijke ontwikkelingen? Hoe vergelijkt zich dit met voorgaande rapportages?

2. Kwaltiteit analyse
In stap twee van het proces wordt de kwaliteit bepaald van de aangebrachte beoordeelde ontwikkelingen in termen van breedte, diepgang en samenhang van de ontwikkelingen. De volgende vragen kunnen daarbij behulpzaam zijn: Wat is de mate van inzicht in de dynamiek in de markt en tussen markt en overheid? Is er inzicht in mogelijk diepere oorzaken voor de ontwikkelingen, zoals indirecte staatsbemoeienis bij buitenlandse leveranciers, samenwerking ten aanzien van cyberweerbaarheid of het kennisniveau? Met betrekking tot de doelstellingen: Is de gewenste controle voor digitale autonomie en cybersecurity geformuleerd?[8]

3. Kwantiteit maatregelen
Bij deze derde stap wordt vervolgens gekeken naar de hoeveelheid maatregelen en hoe deze eventueel al te rubriceren. Is er een prioritering aan te brengen in kern- en ondersteunende maatregelen? Ook wordt een totaaloverzicht van kosten en opbrengsten in kaart gebracht.

4. Kwaliteit maatregelen
Tijdens de vierde stap van dit proces wordt gekeken naar de kwaliteit van de maatregelen. De volgende vragen kunnen daarbij behulpzaam zijn: Wat is de kwaliteit van de voorgestelde maatregelen? Is er vooraf onderzoek gedaan naar de mogelijke impact van de maatregelen? Is de samenhang tussen de maatregelen beredeneerd? Is er inzicht in bij-effecten en is er nagedacht over unintended consequences, zoals een sluipende toename van de (digitale) afhankelijkheid (bijvoorbeeld door gebrek aan coördinatie bij het inkoopproces)?

5. Maatschappelijke, economische en democratische impact van maatregelen
Bij de vijfde stap moet gekeken worden naar hoe het pakket aan voorgestelde maatregelen in maatschappelijk, economisch en democratisch perspectief geplaatst kan worden. De volgende vragen kunnen daarbij behulpzaam zijn: Zijn er ex-post impact-indicatoren geformuleerd in termen van strategische autonomie (controle, capaciteiten, middelen)? Zijn deze direct gerelateerd aan de doelstellingen?

6. Politieke impact maatregelen
In deze laatste en zesde stap van het proces gaat het management de maatregelen prioriteren, waarbij ook de politieke dimensie meegenomen wordt. De volgende vragen kunnen daarbij behulpzaam zijn: Is er een analyse van politieke haalbaarheid van de maatregelen die moeten leiden tot meer controle? Zijn de politieke alternatieven helder geformuleerd? Wat moet er gerapporteerd worden naar de Kamer?

8 Bijvoorbeeld: controle op of zeggenschap in een technologie, kennis, standaarden, bedrijvigheid, investeringen, EU-fondsen, EU-wetgeving/beleid of andere ontwikkelingen die van belang zijn voor Nederland.

3. PROCES VOOR HET DOOR-LOPEN VAN INDIVIDUELE ONTWIKKELINGEN ALS BELEIDSONTWIKKELAAR

Het proces voor het doorlopen van individuele ontwikkelingen op beleidsniveau, dus als beleidsontwikkelaar, bestaat uit zes stappen. Het resultaat van de analyse zal normaliter aan het management worden voorgelegd (hoofdstuk 2). De stappen vooor de beleidsmedewerker zijn weergegeven in Figuur 9. Tijdens dit proces wordt een probleemanalyse opgesteld, doelstellingen geformuleerd en maatregelen gedefiniëerd. De volgorde van deze stappen kan eventueel gewijzigd worden afhankelijk van de use case.

Het doel van dit proces is om de beleidsontwikkelaar te helpen om:

- De analyse compleet uit te voeren;
- De doelstellingen voor strategische autonomie te formuleren en voor ogen te houden;
- Concrete maatregelen te formuleren voor sterkere strategische autonomie in cybersecurity.

Figuur 9: **Te nemen stappen binnen het proces voor doorlopen individuele ontwikkelingen op beleidsniveau**

1. Identificeren triggers

De triggers die zijn uitgezet in het Triggerdiagram vormen het startpunt voor en de eerste stap van dit proces (zie hiervoor ook hoofdstuk 1 van deze handreiking). Daarbij valt te denken aan een nieuw type dreiging, oplopende geopolitieke spanning, druk om EU-wetgeving te herzien, een kritische bedrijfsovername, een nieuwe wetenschappelijke ontwikkeling, maar ook bestaand beleid kan beschouwd worden door de bril van dit model. Ook een toekomstscenario kan als startpunt dienen om vanuit hier een analyse te starten.

2. Analyse van dynamiek

In de tweede stap van het proces wordt een beschrijving gemaakt van de markt-, regelgeving- en technologiedynamiek die met de geactiveerde triggers samenhangen, bijvoorbeeld met behulp van de Porter-modellen[9]. De bedoeling is om inzicht te krijgen in de context van de triggers, bijvoorbeeld de relaties tussen leveranciers en gebruikers (in verband met *supply chain security*), of wettelijke verplichtingen voor cyberweerbaarheid van kritische infrastructuren.

3. Casebeschrijving

De casebeschrijving vormt de derde stap van het proces. Alle elementen (triggers en dynamiek) uit de analyse worden beschreven. Het doel hiervan is om inzicht te krijgen in hoe een individuele ontwikking, dus een trigger, meer kan zijn dan een losstaande gebeurtenis of incident om vervolgens hierop ook zinvol te kunnen reageren (dus niet bijvoorbeeld ‘dweilen met de kraan open’).

4. Aanbrengen focus

In de vierde stap van het proces wordt focus aangebracht op die factoren die cybersecurity en digitale autonomie beïnvloeden. De bedoeling hiervan is om binnen het mandaat te blijven van de toepassing van het toetsingskader, waar de focus is op de doorsnijding van strategische autonomie met cybersecurity. Het is goed mogelijk dat er bredere verbanden gedetecteerd worden, bijvoorbeeld niet gerelateerd aan cybersecurity. Dit is echter geen onderdeel van de hier beoogde toepassing van het toetsingskader.

5. Doelstellingen formuleren

In de vijfde stap worden de doelstellingen geformuleerd. Daarbij wordt het gewenste resultaat in termen van strategische autonomie gedefinieerd. De argumenten moeten hier duidelijk maken waarom het hier daadwerkelijk strategische autonomie betreft, namelijk dat het gaat over het vermogen en de middelen om beslissingen te kunnen nemen en uit te voeren over de langere-termijntoekomst van economie, maatschappij en democratie (zie hiervoor ook het onderzoeksrapport van Timmers en Dezeure).

6. Maatregelen

Tot slot worden in de laatste stap van het proces aan de hand van de geformuleerde doelstellingen een samenhangend geheel van voorgestelde maatregelen gedefinieerd samen met de te verwachte effectiviteit. Hier is het van belang helder te maken waarom de maatregelen effectief zullen zijn als antwoord op de ontwikkelingen en coherent met de marktdynamiek. Tevens is van belang aan te geven – omdat dit het landsbelang aangaat – welke strategische benadering wordt voorgesteld (namelijk, strategische samenwerking met gelijkgezinde partners, aanpak als wereldwijd gedeeld belang, best-effort risicomanagement of een combinatie hiervan).

9 Zie ook Bijlage 3: Porter-modellen

4. ONDERSTEUNING

Er zijn twee manieren om het toetsingskader te gebruiken:

1. De vragenlijst wordt handmatig in een zelfgekozen volgorde doorlopen.
2. De vragenlijst wordt met behulp van een online tool[10] doorlopen.

Voor het toepassen van de eerste methode is in deze handreiking een praktisch stappenplan opgenomen voor de identificatie van triggers en maatregelen.[11] Dit is geïllustreerd aan de hand van een voorbeeld waarin er vertrokken wordt van triggers in Q1 en Q2 en maatregelen in Q1, Q3 en Q4. De tweede methode geeft meer flexibiliteit dan de lineaire volgorde van de vragenlijst, hetgeen beter bij de realiteit past. Bovendien kan een grafische weergave verrijkend werken voor analyse en inzicht. Verder kan alle informatie, inclusief antwoorden op vragen, geregistreerd en met een team gedeeld worden met digitale ondersteuning.

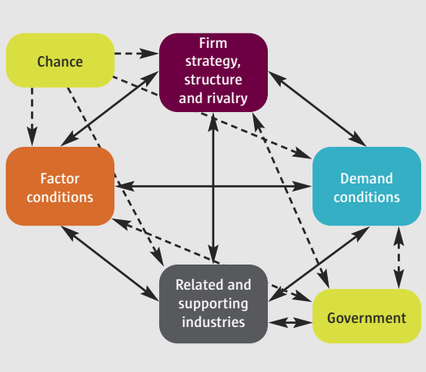
Meer weten?
Om meer te weten te komen over strategische autonomie en cybersecurity is het raadzaam het onderzoeksrapport ‘Nederlandse strategische autonomie en cybersecurity’[12] in zijn geheel te lezen. Hierin zijn verschillende voorbeelden opgenomen die wellicht inspiratie bieden en bovenal kan hier het toetskader worden uitgeprobeerd en toegepast.

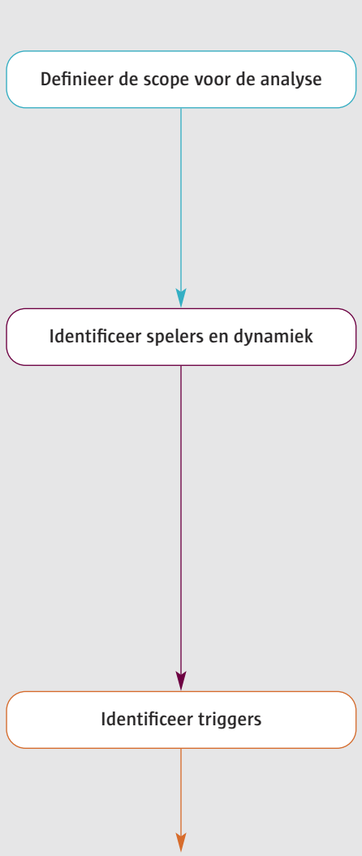
10 Bijvoorbeeld met een digitaal whiteboard.
11 Bijlage 1: Stappenplan voor de indentificatie van triggers en maatregelen
12 Nederlandse strategische autonomie en cybersecurity, Paul Timmers en Freddy Dezeure, januari 2021

BIJLAGEN

BIJLAGE 1:
STAPPENPLAN VOOR DE IDENTIFICATIE VAN TRIGGERS EN MAATREGELEN

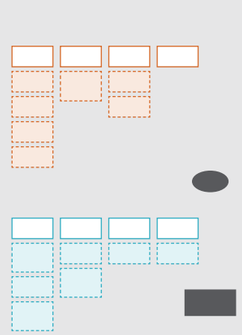
Figuur 10: **Stappenplan te gebruiken met illustratieve vragenlijst als ondersteuning (voor handmatig gebruik)**





Actuele triggers bij ons

Actuele triggers algemeen

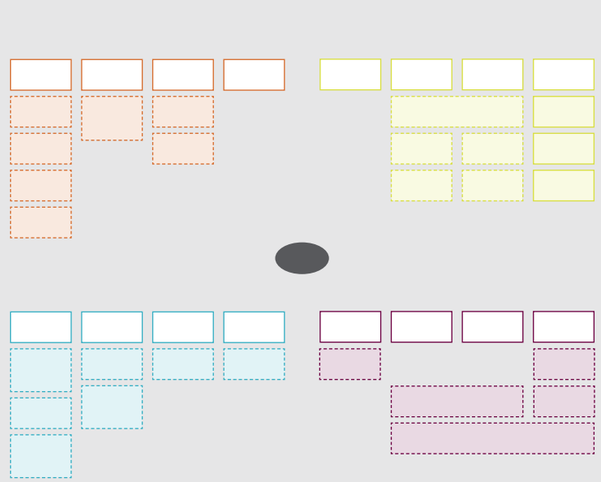


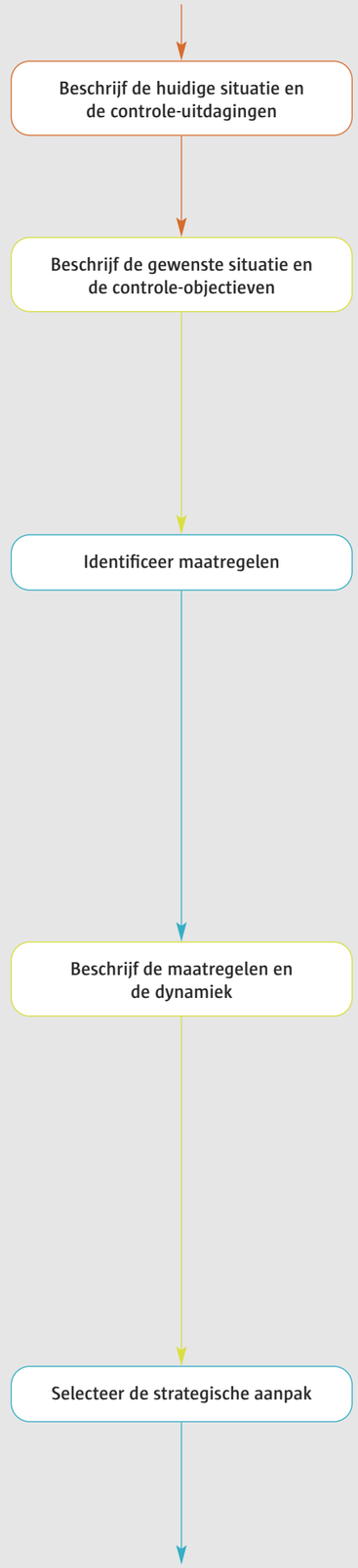
Controle behouden

Controle verkrijgen en opbouwen

Beïnvloeden

Invloed verkrijgen en opbouwen

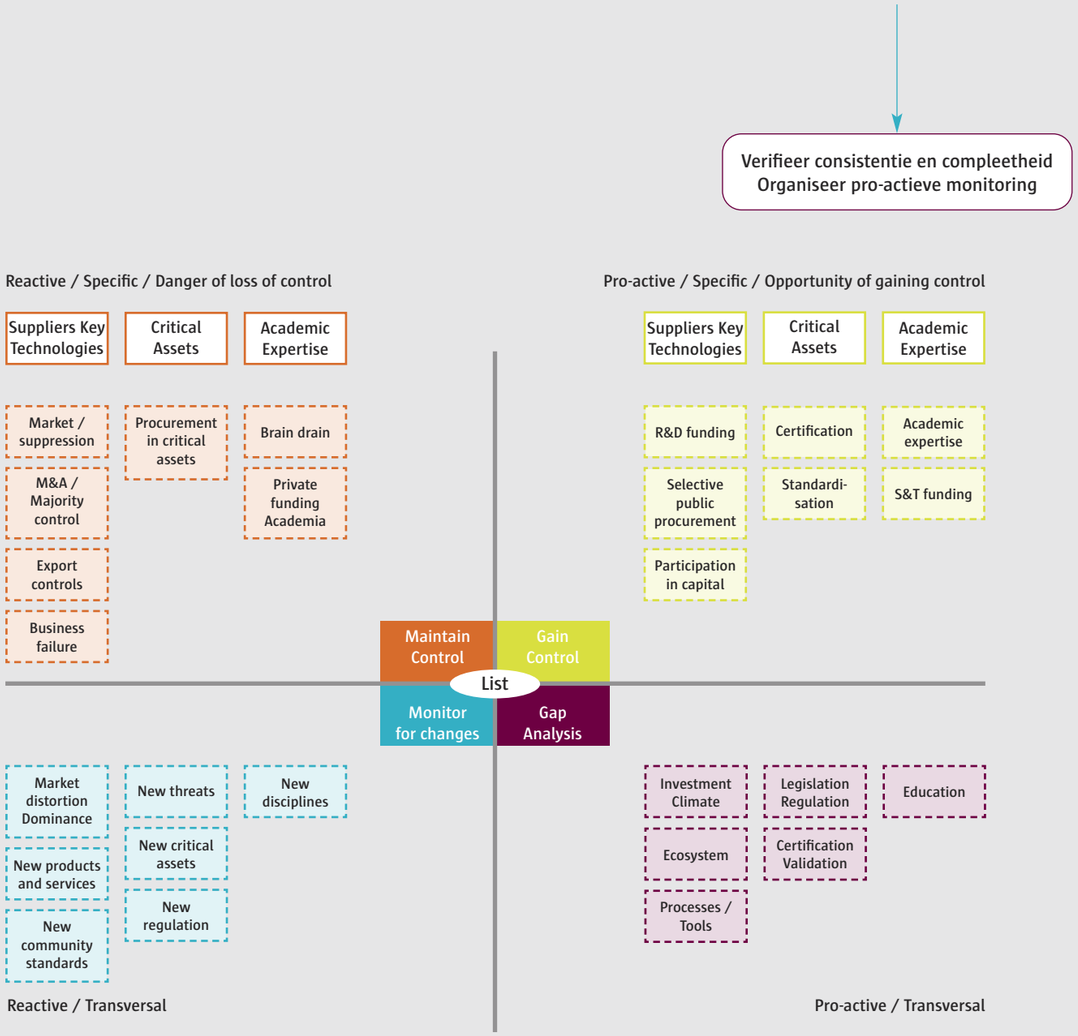




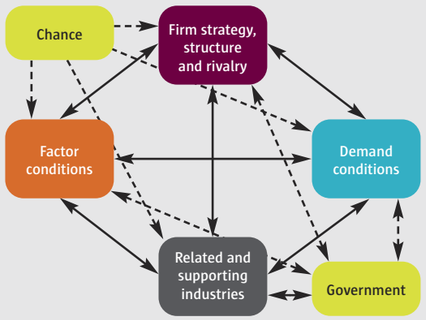
Risicobeheer

Strategisch partnerschap

Algemeen belang


Verifieer consistentie en compleetheid
Organiseer pro-actieve monitoring
Reactive / Specific / Danger of loss of control
Pro-active / Specific / Opportunity of gaining control
Suppliers Key Technologies
Critical Assets
Academic Expertise
Market / suppression
M&A / Majority control
Export controls
Business failure
Procurement in critical assets
Brain drain
Private funding Academia
R&D funding
Selective public procurement
Participation in capital
Certification
Standardi-sation
Academic expertise
S&T funding
Maintain Control
Gain Control
List
Monitor for changes
Gap Analysis
Market distortion Dominance
New products and services
New community standards
New threats
New critical assets
New regulation
New disciplines
Investment Climate
Ecosystem
Processes / Tools
Legislation Regulation
Certification Validation
Education
Reactive / Transversal
Pro-active / Transversal


Threat of new competitors
Bargaining power of suppliers
Competetive Rivalry
Bargaining power of customers
Threat of substitute products


Chance
Firm strategy, structure and rivalry
Factor conditions
Demand conditions
Related and supporting industries
Government

BIJLAGE 2:
ILLUSTRATIEVE VRAGENLIJST TER ONDERSTEUNING VAN IDENTIFICATIE TRIGGERS EN MAATREGELEN

Deze vragenlijst kan uitgebreid worden met nieuwe vragen, onder de aangegeven categorieën.

Identificeer lokale spelers/middelen en dynamiek (Porter: diamond-model)

Factoren

Sleuteltechnologieën
Welke relevante sleuteltechnologieën voor cyberveiligheid zijn er beschikbaar en in welke mate zijn deze 'onder controle'? Er kunnen ook nieuwe technologieën ontstaan als gevolg van de aanvoer, bedreigingen, regelgeving, activa en wetenschappelijke ontwikkelingen. Deze kunnen in verschillende stadia van de toeleveringsketen relevant zijn.

Kennis in de academische wereld, onderzoeksinstellingen, industrie
Welke spelers zijn het meest relevant op dit gebied? Denk bijvoorbaald aan lokale academici en particuliere, wetenschappelijke en technische spelers. In welke mate worden zij gecontroleerd?

Risicokapitaal
Hoe ziet de lokale markt voor risicokapitaal (particulier, openbaar) eruit en wie heeft zeggenschap over de belangrijkste relevante spelers hierin?

Leveranciers

Wie zijn de belangrijkste lokale leveranciers van de sleuteltechnologieën? Wat is hun respectieve marktaandeel? Welke wetgeving passen zij toe? Wie controleert deze leveranciers?

Kopers

Wie zijn de belangrijkste afnemers op de markt (soort, land)? Wat is het aandeel van particuliere – en overheidskopers? Hebben de respectieve regeringen invloed op de besluiten van de particuliere sector in de kritieke infrastructuur in hun land? In hoeverre verstoren overheidskopers deze markt en maken zij het mogelijk dat bepaalde leveranciers hun prijzen dumpen?

Wie zijn de belangrijkste lokale overheidskopers? In hoeverre wordt de aanbesteding gecoördineerd (centrale aanbesteding, gemeenschappelijke technische normen, certificering, validering)?

Verbonden en ondersteunende industrieën

Alternatieve producten
Zijn er alternatieve producten beschikbaar die voldoen aan dezelfde behoefte? Zijn er vereiste sleutelproducten in de toeleveringsketen? Welke lokale leveranciers hebben zij? Wat is hun respectieve marktaandeel? Hoe goed doen ze het in termen van groei, financiële situatie, kapitaal? Wat is het niveau van controle dat we op hen hebben?

Opensource-ecosysteem
Zijn er belangrijke opensourceproducten in dit domein?

Overheid als regelgever

Wetgeving/regelgeving
Welke regels zijn van toepassing in deze sector (wereldwijd) en op welke wijze beïnvloeden zij de markt van sleuteltechnologieën? Welk vermogen heeft Nederland of de EU om op te treden? Welke aanpak hanteren andere landen met betrekking tot strategische autonomie? Hoe zien andere landen toe op de toeleveringsketen van cruciale technologieën in kritieke bedrijfsmiddelen? Is er een mogelijk bevoegdheidsconflict? Welk niveau van bescherming van intellectuele-eigendomsrechten is er en in welke mate is deze afdwingbaar? Hoe belangrijk is het maatschappelijke en politieke bewustzijn en de risicobereidheid van de overheid voor risico's op het vlak van cybersecurity? Is er nationale of Europese wetgeving beschikbaar om noodmaatregelen of herstelmaatregelen te treffen?

Internationale betrekkingen
Zijn er geopolitieke spanningen/gevoeligheden die in overweging moeten worden genomen? Wat is het niveau van overheidssteun voor internationale normalisatie of technologische samenwerking?

Innovatieondersteuning
Zijn er instrumenten en mechanismen beschikbaar voor ondersteuning/toezicht om innovatie van de publieke steun voor O&O te bevorderen en te stimuleren? Is dit voldoende en levert dit een aantoonbaar resultaat op? Wat is het inzicht van de overheid in de innovatievraagstukken en het belang van een ondernemersvriendelijk ecosysteem?

Inzicht in strategische autonomie
Wat is het niveau van bewustzijn en begrip van de strategische autonomie van de belangrijkste belanghebbenden en besluitvormers? Hoe volwassen is de vaardigheid en training van beleidsmakers en uitvoerders?

Kritieke normen en controles
Zijn er relevante Europese en internationale kritische normen en controles op dit gebied?

Identificeer Triggers – Q1 en Q2 (Triggerdiagram)

Q1: Actuele triggers bij ons

Marktonderdrukking
Is er een existentiële bedreiging voor een belangrijke onderneming (die we onder controle hebben) door marktkrachten die de onderneming uit de markt drukken?

Wijziging controle - Mergers and Acquisitions (M&A)
Is er een bestaande sleutelleverancier die het risico loopt dat de controle wordt gewijzigd door nieuwe aandeelhouders (fondsenwerving, fusies en overnames). Kan dit gevolg(en) hebben voor de strategische (digitale) autonomie?

Bedrijfsfalen
Is er een bedreiging voor een sleutelonderneming (die onder controle is) door een faillissement (gebrek aan financiering, gebrek aan binnenlandse markt, etc.)? Is er sprake van een kritische leverancier van sleuteltechnologie, -diensten of -infrastructuur die dreigt te verdwijnen?

Exportcontrolerisico
Is er een kritische technologie die mogelijk wordt geëxporteerd naar landen of bedrijven waar dit vanuit strategisch oogpunt niet wenselijk is?

Nieuwe aanbestedingen door de overheid
Zijn er belangrijke projecten voor de aanschaf van infrastructuur in de overheid die mogelijk van invloed zijn op de cyberveiligheid van essentiële middelen?

Nieuwe aanbestedingen door de particuliere sector
Zijn er belangrijke projecten voor de aanschaf van infrastructuur in de particuliere sector die mogelijk van invloed zijn op de cyberveiligheid van essentiële middelen? Wordt er een externe aankoop van belangrijke componenten in een kritieke infrastructuur overwogen?

Gebrek aan academische financiering
Komen belangrijke academische troeven, die van cruciaal belang zijn voor de huidige technologie, zoals het valideren van vertrouwen of het ontwikkelen van nieuwe technologieën, in het gedrang door het ontbreken aan financiering?

Braindrain
Is er een risico van verlies van het belangrijkste talent in de academische wereld nodig om onafhankelijk advies te geven over de goede werking van een specifieke sleuteltechnologie? Zijn er aanwijzingen dat toonaangevende talenten op relevante gebieden uit het land wegtrekken vanwege betere kansen elders?

Academische sponsoring
Is er een risico voor belangrijke kennisactiva als gevolg van buitenlandse (particuliere) financiering? Denk bijvoorbeeld aan het mogelijk verlies van controle over de vaardigheden die nodig zijn om onafhankelijk advies te geven over de goede werking van sleuteltechnologieën of het mogelijke verlies van controle over wetenschappelijke expertise die als basis kan dienen voor *generation after next*.

Q2: Actuele triggers in het algemeen (sector, markt, wereld)

Marktdominantie
Is de markt voldoende efficiënt? Is de interne markt in de EU op dit gebied volwassen? Zijn er ontwikkelingen op de markt die aanleiding kunnen geven tot een ongecontroleerde dominantie? Is er sprake van marktverstoring? Is er een beperkt aantal leveranciers die een quasi-monopolie hebben opgebouwd door hun marktaandeel of door marktverstorende benaderingen?

Nieuwe producten
Zijn er nieuwe product- of dienstencategorieën met gevolgen voor de cyberveiligheid?

Nieuwe normen
Zijn er nieuwe normen op dit gebied (officieel of sectoraal)?

Nieuwe bedreigingen
Zijn er nieuwe (potentiële) types van cyberdreigingen waarvoor onvoldoende bescherming is of worden bestaande bedreigingen frequenter en groter?

Nieuwe kritieke middelen
Zijn er middelen die een verhoogd risico lopen (denk aan de kritieke infrastructuur, economie, democratie, vrijheid van meningsuiting, essentiële waarden)? Welke relevante bedreigingen zijn dit en wat is de mogelijke impact op deze middelen?

Nieuwe verordening
Is er EU-wetgeving in voorbereiding die een cyberveiligheidscomponent bevat? Is er buitenlandse wetgeving in voorbereiding die nieuwe bedreigingen kan veroorzaken of invloed kan hebben op de levering van sleuteltechnologieën?

Nieuwe disciplines
Zijn er nieuwe of opkomende wetenschappelijke disciplines die een cyberbeveiligingstoepassing kunnen hebben in termen van bedreigingen of mitigaties?

Geopolitieke druk
Is er een nieuwe geopolitieke druk met gevolgen voor leveranciers, gebruikers of wetenschappelijke ontwikkelingen op het gebied van cyberveiligheid?

Generation after next
Welke relevante vervangingstechnologie tekent zich af in een horizon van vijf jaar? Op welke nieuwe wetenschappelijke en technische inzichten is deze nieuwe technologie gebaseerd? Welke spelers hebben op dit moment het leiderschap in kennis en innovatie op dat vlak?

Identificeer maatregelen – Q1, Q2, Q3, Q4 (Triggerdiagram)

Q1: Controle behouden bij ons

Verbetering van de binnenlandse markt
Het creëren of verbeteren van de binnenlandse marktvoorwaarden voor sleuteltechnologieën op nichemarkten. Opties voor overheidsinterventies zijn slimme aanbestedingen, het verbeteren van de bestaande (digitale) infrastructuur, het ondersteunen van vervanging van buitenlandse sleuteltechnologieën.

Voorwaarden opleggen in verband met verandering van zeggenschap
Te overwegen opties zijn gouden aandelen voor de overheid, condities in de overeenkomsten van investeerders (term sheets) en facilitering van deelneming van regionale investeerders in kapitaal. Ook moet de EU-wetgeving worden geactiveerd voor het openstellen van de toegang tot platforms en ontvlechting (DMA, CER-verordening).

Verstrek overlevingsmaatregelen
Steun aan een belangrijke leverancier die door faillissement dreigt te verdwijnen met behulp van juridische en financiële beschermingsmaatregelen.

Uitvoer blokkeren
De uitvoer van sleuteltechnologieën weigeren naar landen die de strategische autonomie in gevaar zouden kunnen brengen. Het totstandbrengen van beperkingen voor de Foreign Direct Investment (FDI).

Voorwaarden voor overheidsopdrachten door de overheid
Stel selectiecriteria, exploitatievoorwaarden of certificeringen op.

Voorwaarden voor nieuwe aanbestedingen door particuliere ondernemingen
Leg exploitatievoorwaarden of certificeringen op.

Selectieve financiering
Het verstrekken van financiering voor belangrijke academische activa (trustvalidatie).

Talenten behouden
De maatregelen die in overweging kunnen worden genomen voor het behouden van talenten zijn academische ondersteuning, carrièreplanning en financiering voor onderzoek & ontwikkeling.

Blokkering in controle - sponsoring
Ontzeg particuliere sponsoring van academische afdelingen of kennisinstituten met juridische of andere middelen.

Q2: Invloed vergroten

Regelgeving en beleid
Beïnvloeden van de ontwikkeling en toepassing van EU-regelgeving, zoals certificatie voor ICT-security, cyber-risicomanagement en markttoegang, in de fases van definitie, onderhandeling, of implementatie (bv. middels referentie naar standaarden) van EU-beleid.

Het proactief agenderen van opkomende thema's door middel van het delen van analyses en nationale strategieën met andere lidstaten (samen met een 'coalition of the willing').

Belangen in bedrijven
In overleg met andere EU-lidstaten aanhangig maken van bedreiging van eigen bedrijven en die verdedigen middels een mededingingszaak of in restricties voor foreign direct investment.

Financiering
Inhoudelijke sturing en prioritering via de programma-comités van EU-programma's voor onderzoek & ontwikkeling, toepassing en implementatie van cyberoplossingen, vaardigheden en andere investeringen, zoals het Resilience & Recovery Fund, het Digital Europe programma, Connecting Europe Facility, Horizon Europe en het European Defense Fund).

Standaarden en normen
Het ondersteunen van deelname van lokale bedrijven en kennisinstituten in internationale standaardisering, multilaterale standaardisatie (zoals voor defensie met NATO of in de financiële sector) of bilaterale pre-standaardisatie (bijvoorbeeld met de Verenigde Staten).

Het ondersteunen van deelname van ministeries en stakeholders in internationale cybersecurity norms, confidence and capacity building measures (zoals in UN GGE en UN OEWG).

Het ondersteunen van deelname van onderzoekers en bedrijfsleven aan opensource-initiatieven.

Q3: Controle verkrijgen en opbouwen, kansen grijpen bij ons

O&O-financiering
Het financieren van de ontwikkeling van nieuwe sleuteltechnologieën door gecontroleerde ondernemingen. Het steunen van onderzoek & ontwikkeling door startende ondernemingen naar belangrijke technologieën.

Slimme aanbesteding
Bevoorrechte aankoop van 'gecontroleerde' bedrijven (uitzonderingen op overheidsopdrachten, slimme aankopen, launching customer). Het bieden van hulp aan startende ondernemingen (bijvoorbeeld door afname van Proof of Concept (PoC) tegen betaling, het bieden van uitzonderingen inzake bestaansduur en financiële criteria).

Deelname in kapitaal
Overheidsdeelname in ondernemingen die een sleuteltechnologie produceren (gouden aandeel, overheidsaandeel, voorwaarden in overeenkomsten).

Exportondersteuning
Het bieden van overheidssteun voor relevante vergunningen of het verzekeren van kredietrisico. Certificering van exploitatievoorwaarden.

Ontwikkeling en financiering van certificeringsregelingen die exploitanten in staat stellen kritieke infrastructuur te exploiteren of betrouwbare oplossingen aan te schaffen.

Standaarden
Implementatie van de normalisatie en interoperabiliteit van sleuteltechnologieën.

Vlaggenschepen
De totstandbrenging van grootschalige infrastructuurprojecten die kritieke diensten ondersteunen. Aansluiting bij Europese vlaggenschepen.

"Generation after next" – onderzoek & ontwikkeling
Gebruikmaken van innovatiefinanciering en financiering voor onderzoek & ontwikkeling voor de generation after next-technologieën op dit gebied.

Financiering borgen
Het borgen van financiering voor academische deskundigheid die het vertrouwen in (externe) marktoplossingen kan valideren. Onafhankelijke validatie van kernclaims door verkopers zodat kopers op deze claims kunnen vertrouwen.

Q4: Invloed verkrijgen en opbouwen, kansen grijpen in het algemeen

Investeringsklimaat
Het creëren van een juridisch kader dat risico-investeringen en ondernemerschap bevordert. Vergelijk de omgeving voor deze investeringen van het eigen land met landen die succesvol zijn in innovatie (bijvoorbeeld de Verenigde Staten, het Verenigd Koninkrijk, China en Israël), kijkend naar wettelijke, fiscale en financiële condities (bijvoorbeeld aandelenopties, aanwerving/ontslag).

Ecosysteem
Faciliteer een ecosysteem dat een startende onderneming helpt en aanmoedigt, bijvoorbeeld door het verstrekken van een overzicht met een inventarisatie van fondsen, netwerk van ondernemers en business angels. Vergelijk het ecosysteem (ondernemingsnetwerken, transparantie van de venture capital markt, activiteiten van business angels-, begeleiding/versnellers) tussen het eigen land en landen die zeer succesvol zijn in innovatie. Beschouw bijvoorbeeld verschillen in wettelijke, fiscale en financiële condities die kunnen worden omgezet.

Processen en hulpmiddelen
Beschouw voorbeelden van overheidsprocessen en -instrumenten die innovatie en industriële toepassing van nieuwe technologieën stimuleren. Er zijn goede praktijkvoorbeelden beschikbaar, zoals In-Q-Tel, Darpa/IARPA, Defense Strategy, Selective Purchase Policy (DIU in de VS), Key Technologies List.

Wetgeving/regelgeving
Het aanpassen van wetgeving om strategische autonomie te bevorderen. Denk bijvoorbeeld aan uitzonderingen voor overheidsopdrachten, mededingingsbeleid, beperkingen van buitenlandse investeringen, ontvlechting, gegevensbeheer, vertrouwde infrastructuur, etc. Beschouw voorbeelden in andere landen die inspirerend zijn om verder te gaan dan de EU-wetgeving op het gebied van Mergers and Acquisitions (M&A) en mobiliseer mogelijk cyberdiplomatie.

Standaarden
Bevorder actieve deelname aan de internationale normalisatie en interoperabiliteit van sleuteltechnologieën.

Certificering/accreditatie
Het implementeren van een infrastructuur en instrumenten om certificering en accreditatie te bevorderen, waarbij wordt gezorgd voor ingebouwde veiligheid en vertrouwen. Het bevorderen van een bredere toepassing van betrouwbare en betrouwbare technologie en het verschaffen van transparantie over het evenwicht tussen prijs en veiligheid.

Processen en hulpmiddelen
Het definiëren en implementeren van processen en hulpmiddelen die digitale autonomie op het gebied van leveranciers van kritieke diensten steunen. Leren van voorbeelden van door de overheid gefinancierde/georganiseerde processen en instrumenten in andere landen die innovatie en industriële toepassing van nieuwe technologieën die de veiligheid verbeteren stimuleren. Het beoordelen van mogelijkheden om inzichten van inlichtingendiensten te benutten om de bescherming van particuliere ondernemingen en de samenleving als geheel te verbeteren. Een ander voorbeeld is scenarioplanning en hoe andere landen dit doen.

Onderwijs, opleiding, begeleiding
Goede praktijken in andere landen om ondernemerschapsmentaliteit en -vaardigheden dichter bij de technische en wetenschappelijke faculteiten te brengen. Leren van de succesvolle recepten voor opleiding en incubatie. Steun uitwisselingsmechanismen om ondernemers een korte periode onder te dompelen in bloeiende ecosystemen. Bevorder ook de netwerken en uitwisseling tussen succesvolle ondernemers (exits, angels) en nieuwkomers.

Wetenschap- en technologieprocessen en -tools
Bevorder de excellentieknooppunten in geselecteerde sleuteltechnologieën, met gebruikmaking van de bestaande voorbeelden als inspiratie en vergelijking met andere EU-hotspots. Beschouw in welke mate we innovatie en groei kunnen stimuleren door investeringen in wetenschap, onderzoek & ontwikkeling in sleuteltechnologieën én de controle kunnen behouden. Hoe kan wellicht het effect worden verbeterd door succesvolle praktijken uit andere landen toe te passen?

Strategische autonomiebenadering
Ontwikkel een nationale aanpak van strategische autonomie en cyberveiligheid met geïntegreerde, proactieve processen en instrumenten voor beleidsontwikkeling en -monitoring.

Definitie van de gewenste situatie

"AS IS" situatie
Geef een samenvatting van de actuele situatie, met inbegrip van relevante gebieden, zoals leveranciers/klanten, factoromstandigheden (academische kennis en kritische hulpbronnen) en de aard van overheidsinterventie. De analyse moet een beschrijving bevatten van factoren waarover te weinig controle wordt uitgeoefend om de toekomst in de zin van strategische (digitale) autonomie te bepalen.

"TO BE" situatie
Geeft een beknopte beschrijving van de gewenste situatie, met inbegrip van relevante gebieden, zoals leveranciers/klanten, academische kennis, kritische hulpbronnen en de aard van overheidsinterventie. Besteed daarbij ook aandacht aan de doelgerichte uitbreiding van de controle. Hoe en in hoeverre verbeteren de voorgestelde maatregelen de strategische (digitale) autonomie? Zijn deze consistent en toereikend? Zijn de mogelijke schadelijke en negatieve gevolgen beoordeeld en verzacht?

Implementatieopties

Risicobeheer
Welk risicobeoordelingsmodel moet worden gevolgd (nationaal of Europees)? Wat is de risicobereidheid en in welke mate kunnen we het risico beperken? Wat is het resterende risico en hoe wordt dit ondervangen?

Strategisch partnerschap
Welke 'like-minded' regeringspartners zijn er en voor welke doelstellingen? Welke particuliere partners (PPP) zijn er en voor welke doelstellingen? Strategische interdependentie of aanpassing van het handels-/FDI-beleid? Is er een complementaire wederzijdse afhankelijkheid met niet-like-minded partijen? Zo ja, is deze afhankelijkheid stabiel of kan hier misbruik van worden gemaakt ('weaponised')?

Gemeenschappelijk globaal belang
Is er een wereldwijd platform beschikbaar die ter ondersteuning gebruikt kan worden? Zo ja, voor welk doel en op welke wijze? Welke niet-gouvernementele partners moeten worden gesteund? Welke acties moeten worden gekozen voor Nederlandse (cyber)diplomatie om op wereldniveau het gemeenschappelijke belang te bevorderen?

Verificatie van compleetheid en coherentie (Porter modellen)

Wanneer de maatregelen betrekking hebben op een enkel bedrijf, maak dan gebruik van een model dat de relaties van het bedrijf met leveranciers, klanten, (opkomende) alternatieve producten/diensten en concurrenten inzichtelijk maakt. Mogelijke vragen zijn: hoe stabiel en sterk is de concurrentiepositie van dat bedrijf? Welke factoren bepalen deze positie, zoals overheidssteun? Hebben de maatregelen invloed op de concurrentiepositie? Zijn de maatregelen compatibel met EU-wetgeving of WTO-regels of juist een concrete implementatie van de nationale of EU-wetgeving?

In veel gevallen hebben de analyse en maatregelen betrekking op een sector als geheel. In dit geval kan gebruik worden gemaakt van een model dat de factoren en marktdynamiek voor de betreffende sector laat zien. Mogelijke vragen die hierbij behulpbaar kunnen zijn: Zijn alle relevante factoren en actoren en hun interacties meegenomen? Wat is de omvang en duurzaamheid van financiering? Is er een hefboomwerking van EU-gelden? Kan de overheid schaalgrootte bevorderen met exportpromotie? Is er een synergie tussen klantenbelangen en sectorbelangen, bijvoorbeeld middels vlaggenschip-projecten? Zijn er non-profit-initiatieven die de overheid moet ondersteunen, zoals opensource-ontwikkelingen of cybersecurity-analyse? Is de ondersteuning van een sector of selectieve samenwerking met een aantal bedrijven geoorloofd in relatie tot de concurrentieregels (EU, WTO) of juist te motiveren met uitzonderingsclausules, zoals Art 346 TFEU (nationale veiligheid)?

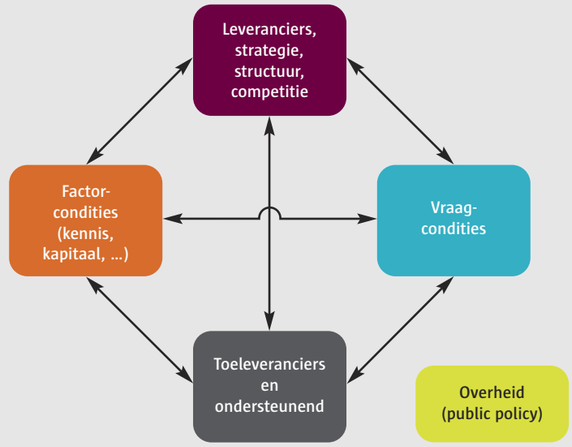
BIJLAGE 3: PORTER-MODELLEN

Michael Porter ontwikkelde in de jaren '80-'90 twee veelgebruikte modellen, te weten het Diamond-model en het Five Forces-model. Met behulp van deze modellen is het mogelijk om bestaande situaties en verschuivingen in kaart te brengen en te classificeren op nationaal niveau of op bedrijfsniveau. Ze laten toe om de dynamiek te beschrijven in een expliciete 'narrative'.

Diamond-model

Het eerste model[13] is bedoeld om op landsniveau de nationale concurrentiekracht, innovatie- en marktdynamiek te analyseren. Dit wordt ook wel het Diamond-model genoemd.

Figuur 11: **Diamond-model**



Een korte beschrijving van de elementen, gebaseerd op de gegeven referentie:

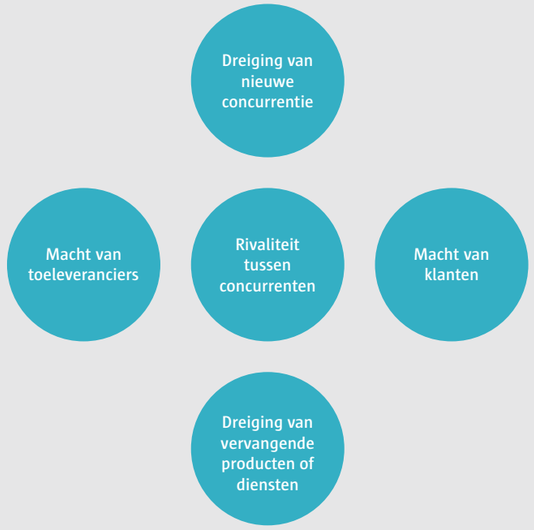
- *Factorcondities:* De positie van het land wat betreft productiefactoren die nodig zijn om te concurreren, zoals geschoolde arbeidskrachten, kennis, infrastructuur, kapitaal of ecosysteem meer bepaald in de betreffende sector.
- *Vraagvoorwaarden:* De aard van de vraag op de thuismarkt naar de producten of diensten in de betreffende sector.
- *Gerelateerde en ondersteunende industrieën:* De aan- of afwezigheid in het land van toeleveringsbedrijven en andere aanverwante bedrijfstakken, in het bijzonder de bedrijfstakken die internationaal aanwezig en concurrerend zijn.
- *Bedrijfsstrategie, structuur en rivaliteit:* De omstandigheden die bepalen hoe bedrijven worden opgericht, georganiseerd en beheerd, evenals de aard van binnenlandse rivaliteit.
- *Overheid:* Hier wordt de rol van de overheid bedoeld in de zin van beleid (public policy), waarbij de overheid zowel de condities oplegt aan de spelers in de markt alsook de markt stimuleert (government as challenger and as catalyst). De overheid kan alleen succesvol zijn als zij in tandem werkt met gunstige andere condities in het model.

13 https://hbr.org/1990/03/the-competitive-advantage-of-nations

Five Forces-model

Het tweede model, ook wel het Five Forces-model genoemd (zie Figuur 12), is bedoeld voor het ontwikkelen van een bedrijfsstrategie[14].

Figuur 12: **Five Forces-model**



Een korte beschrijving van de hoofdelementen in dit model:

- *Dreiging van nieuwe concurrenten:* nieuwe concurrenten brengen bijkomende productiecapaciteit in de markt, zetten bestaande spelers onder druk.
- *Onderhandelingspositie van leveranciers:* dominante leveranciers kunnen meer waarde voor zichzelf houden door prijzen op te drijven, de kwaliteit van hun producten te verminderen, of kosten over te hevelen naar hun afnemers.
- *Onderhandelingspositie van klanten:* dominante kopers kunnen meer waarde voor zichzelf houden door prijzen te drukken, meer kwaliteit of meer service te eisen en leveranciers tegen elkaar uit te spelen.
- *Dreiging van vervangingsproducten:* alternatieve oplossingen kunnen het product of de dienst vervangen door dezelfde functie op een andere wijze te realiseren.
- *Rivaliteit met de bestaande concurrenten:* kan allerlei vormen aannemen, zoals kortingen, advertising, nieuwe producten en verbetering van dienstverlening.

14 https://www.isc.hbs.edu/strategy/business-strategy/Pages/the-five-forces.aspx

CSR Cyber Security Raad