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

www.tno.nl

T +31 88 866 10 00

TNO-rapport

TNO 2022 R11656

Sensitieve Technologie

Datum	Augustus 2022
Auteur(s)	Dr. H.L. Duijnhoven I.N. Melman MSc Drs. P.G.M. van Scheepstal
Rubricering rapport	TNO Publiek
Aantal pagina's	29
Aantal bijlagen	-
Opdrachtgever	Ministerie van Buitenlandse Zaken, Ministerie van Economische Zaken en Klimaat Nationaal Coördinator Terrorismebestrijding en Veiligheid
Projectnaam	Werkzaamheden Analistennetwerk Nationale Veiligheid 2020 – deelproject Sensitieve Technologie
Projectnummer	060.43591/01.05

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

De Nederlandse overheid is zich bewust van het belang van technologische ontwikkeling en innovatie voor de Nederlandse economie en samenleving. Tegelijkertijd realiseert zij zich dat technologische ontwikkeling ook nationale veiligheidsrisico's met zich mee kan brengen, bijvoorbeeld wanneer technologieën een militaire toepassing of dual-use[1] toepassing kennen waarmee deze ingezet kunnen worden tegen de veiligheidsbelangen van Nederland en/of haar bondgenoten. Ook kunnen technologische ontwikkelingen risico's zoals spionage, sabotage en ongewenste strategische afhankelijkheden met zich meebrengen, waardoor de Nederlandse economie en samenleving aangetast kan worden.

De Nederlandse overheid heeft reeds een aantal instrumenten en beleidskaders om risico's die samenhangen met technologieontwikkeling en toepassingen van technologie te mitigeren. Voorbeelden hiervan zijn beleidskaders voor exportcontrole en een kennisembargo voor speciale gebieden van onderwijs en onderzoek om ongewenste overdracht van technologie tegen te gaan. Op dit moment worden daarnaast nog aanvullende maatregelen en beleidskaders voorbereid, zoals de investeringstoets.

Voor een gedegen uitwerking van overheidsinstrumentarium is behoefte aan meer kennis van ontwikkelingen op het gebied van sensitieve technologieën, alsmede de dynamiek daarvan in Nederland en daarbuiten. Deze kennis geeft de overheid inzage in welke (hoogwaardige) technologieën ze wil beschermen tegen risico's voor nationale veiligheid. Dit is noodzakelijk voor een heldere strategie, een duidelijke inzet op Europees en/of internationaal terrein en nieuw te ontwikkelen beleid. Op dit moment is het lastig aan te geven welke hoogwaardige technologieën binnen de reikwijdte van het verschillende instrumentarium ter borging van de nationale veiligheid valt.

De term sensitieve technologie wordt in dit kader gebruikt om te verwijzen naar technologische ontwikkelingen en toepassingen die een risico vormen voor nationale veiligheid.

1.2 Doelstelling

Het ministerie van Buitenlandse Zaken (BZ), het ministerie van Economische Zaken en Klimaat (EZK) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) hebben namens de Interdepartementale Werkgroep (IWG) Sensitieve Technologie[2] het Analistennetwerk Nationale Veiligheid (ANV)[3] gevraagd om een

[1] Het ministerie van Buitenlandse Zaken definieert Dual-use als volgt: Dual-use-goederen hebben doorgaans een normale civiele toepassing, maar kunnen ook gebruikt worden om bijvoorbeeld massavernietigingswapens, ballistische raketten of conventionele militaire goederen te maken.

[2] In deze werkgroep nemen naast BZ, EZK en NCTV ook de ministeries van Defensie, Binnenlandse Zaken en Koninkrijksrelaties (BZK), en Onderwijs, Cultuur en Wetenschap (OC&W) deel.

[3] TNO heeft namens het ANV deze studie uitgevoerd.

rijksbreed toepasbare systematiek te ontwikkelen. Deze systematiek dient sneller dan nu inzichtelijk te maken welke technologieën mogelijk een risico vormen voor de nationale veiligheid. Met deze systematiek willen de verschillende departementen die vertegenwoordigd zijn in de interdepartementale werkgroep beter in staat zijn om beleid bij te sturen en (bestaande) instrumenten te actualiseren. Naast de systematiek is ook gevraagd om een begrippenkader te ontwikkelen dat als uitgangspunt kan dienen voor de systematiek door het gemeenschappelijk denken over sensitieve technologie binnen de rijksoverheid te faciliteren.

Uitgangspunten hierbij zijn dat in de systematiek zoveel mogelijk de technologie centraal wordt gesteld (sensitiviteit als *eigenschap* van de technologie). Tevens wordt primair gekeken naar risico's voor de nationale veiligheid die in de moedwillige sfeer liggen. Dit betekent dat risico's die voortkomen uit technisch falen in principe buiten beschouwing blijven in de duiding van sensitiviteit.

De doelstellingen van het project zijn als volgt:

1 Het formuleren van een gemeenschappelijk begrippenkader waarmee huidige en opkomende sensitieve technologieën afgewogen kunnen worden.
2 Het opstellen van een dynamische systematiek waarlangs huidige en opkomende sensitieve technologieën in kaart kunnen worden gebracht.

1.3 Leeswijzer

Deze rapportage bevat de hoofdresultaten van deze studie. In de eerste plaats het begrippenkader (Hoofdstuk 2). Hierin wordt een beeld gevormd van de begrippen technologie, nationale veiligheid en sensitiviteit, en hoe deze begrippen zich tot elkaar verhouden. Hierbij wordt gebruik gemaakt van de operationalisering van Nationale Veiligheid zoals deze in de Nationale Veiligheidsstrategie en het methodologisch kader van het Analistennetwerk Nationale Veiligheid wordt gehanteerd (ANV, 2019b).

Hoofdstuk 3 bevat de systematiek zoals deze in afstemming met de Interdepartementale Werkgroep Sensitieve Technologie is opgesteld. De systematiek is bedoeld om op een gestructureerde manier inzicht te krijgen in, en duiding te geven aan de sensitiviteit van technologieën in het kader van Nationale Veiligheid. De resultaten van het toepassen van de systematiek kunnen door de departementen worden gebruikt om te bepalen of er (aanvullende) maatregelen moeten worden genomen om sensitieve technologieën te beschermen. Het formuleren van maatregelen wordt door de departementen uitgevoerd en is geen onderdeel van de systematiek.

2 Begrippenkader

In dit hoofdstuk bespreken we de begrippen die van belang zijn om de sensitiviteit van technologie in de context van de nationale veiligheid te evalueren. Dit begrippenkader vormt het uitgangspunt voor de systematiek en draagt bij aan de gezamenlijke begripsvorming over deze onderwerpen.

2.1 Technologie

Om te kunnen bepalen op basis waarvan een technologie als sensitief in de context van nationale veiligheid moet worden beschouwd is het belangrijk om een beeld te hebben van wat een technologie is. Technologie is een veel gebruikte en daardoor gangbare term, maar tegelijkertijd is het ook een term die zich moeilijk laat vatten in een concrete, bruikbare definitie. We zullen in deze paragraaf ingaan op de betekenis van het begrip technologie en daarnaast een aantal andere relevante aspecten bespreken die te maken hebben met technologie en technologische ontwikkelingen.

2.1.1 Het begrip technologie

Hoewel het lastig is om een eenduidige, geaccepteerde definitie te vinden, is het nuttig om in te gaan op de historische oorsprong van het begrip. Vanuit historisch perspectief valt op dat de definitie en het gebruik van de term technologie in de loop van de eeuwen sterk is veranderd (Agar, 2020).

Het woord technologie vindt haar oorsprong in het Grieks en bestaat uit twee delen:

- {‘techne’ = ‘vakmanschap’};
- {‘logia’ = ‘theorie, systematische kennis’}.

Hieruit volgt dat technologie de kennis (theorie) over het vakmanschap (ook wel de vaardigheid om een specifiek product te vervaardigen) betreft. Traditioneel gezien verwees de term technologie dan ook naar de leer van de ambachtskunst, oftewel de kennis die een metselaar of schilder nodig had om het vak uit te voeren en te worden gekwalificeerd als een goede metselaar of schilder (Rip & Kemp, 1998). Vanaf het begin van de negentiende eeuw werd de kennis over ambachten steeds meer gestandaardiseerd. Ook werd in de betekenis van het begrip technologie steeds meer nadruk gelegd op doelgerichte ‘uitvindingen’ en de toepassing daarvan (Rip & Kemp, 1998).

In tegenstelling tot het Engelse begrip *technology* bestaan er in de Nederlandse taal twee woorden om twee verschillende aspecten van technologie aan te duiden: ‘techniek’ – “de vaardigheid om vernuftige producten te maken” (Rip, 1995: 15) en ‘technologie’ – “de systematische kennis van technieken” (Rip, 1995: 15). In de praktijk wordt dit onderscheid echter vaak niet gemaakt, waardoor technologie als term wordt gebruikt om zowel de kennis als de vaardigheid aan te duiden. Daar komt nog bij dat wanneer het gaat om het belang van technologie voor de samenleving vaak met name het product zelf (ook wel artefacten of de ‘dingen’ die de uitkomst zijn van het vervaardigen op basis van systematische kennis) als technologie wordt bestempeld. Dit is logisch omdat dit hetgeen is wat het meest betekenisvol is in de samenleving.

Als het gaat om de beoordeling van risico's van technologie ligt het wellicht voor de hand om vooral te richten op de 'producten' die voortkomen uit technologische ontwikkeling. Hierbij moet het begrip 'product' overigens breed worden opgevat. Het zijn niet altijd tastbare fysieke producten, maar het kan bijvoorbeeld ook gaan om software. De reden om bij het nadenken over risico's van technologie te richten op de risico's die voortkomen uit de technologische producten is op zich logisch. Immers, dat is hetgeen wat in de samenleving 'gebruikt' wordt en wat daarmee ook de grootste impact (zowel positief als negatief) op de samenleving kan hebben.

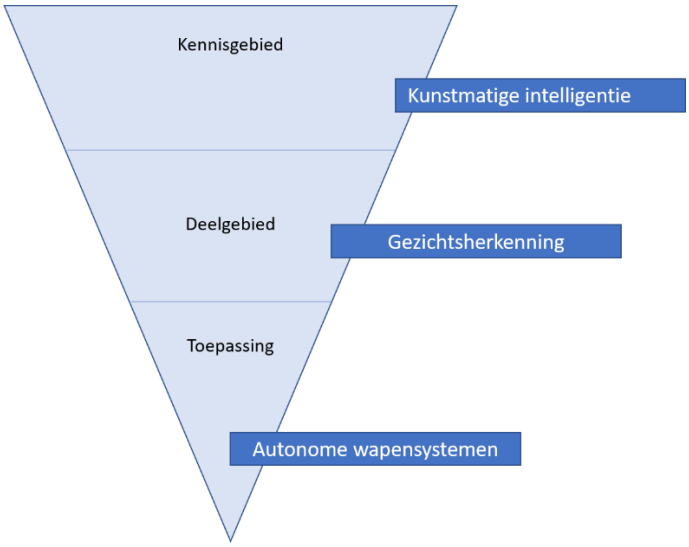
Carlsen et al. (2010) geven daarbij terecht aan dat hierbij niet alleen naar het bedoelde gebruik moet worden gekeken maar (juist) ook naar het daadwerkelijke (bedoelde en onbedoelde) gebruik van een technologie. Echter, een duidelijk beeld van het daadwerkelijke gebruik van een technologie (in de vorm van een product) suggereert dat het product ook al beschikbaar is voor gebruik. Een inschatting maken van mogelijk toekomstig gebruik van een technologisch product is een stuk lastiger omdat hierbij ook rekening moet worden gehouden met veranderende omstandigheden in de samenleving (Carlsen et al., 2010).

En wanneer we niet op het eindproduct focussen maar op de *kennis* die daaraan ten grondslag ligt wordt het nog complexer om de potentie daarvan in allerlei verschillende domeinen en combinaties te voorspellen of in te schatten. Toch is dat laatste vanuit het oogpunt van sensitieve technologie wellicht het meest interessant. Het gaat hierbij om het identificeren van die stukken technologische kennis die niet alleen grote impact op de samenleving kunnen hebben, maar vooral ook als aanjager van de ontwikkeling van weer andere technologieën kunnen dienen. Op die manier kunnen ze weer leiden tot veel verschillende nieuwe producten en toepassingen met potentiele risico's voor de nationale veiligheid.

2.1.2 Afbakening van 'een technologie'

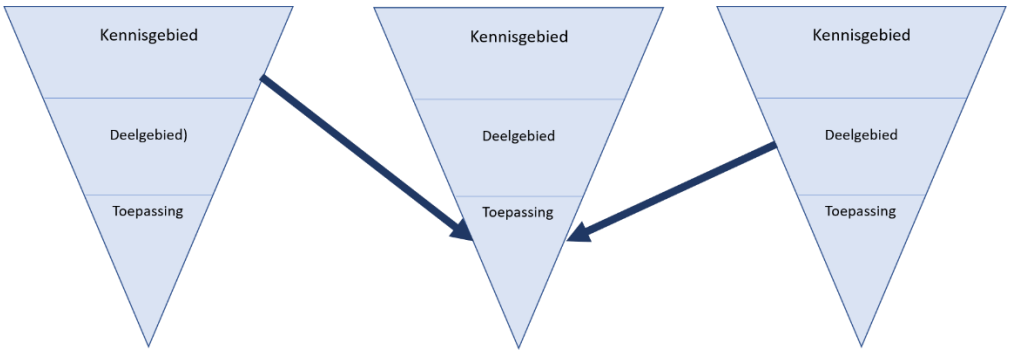
Als het gaat om een bruikbare afbakening of definitie van technologie voor de evaluatie van sensitiviteit is het vooral belangrijk om bewust te zijn van de verschillende componenten die vaak onder de noemer 'technologie' worden gevat, zoals in voorgaande paragraaf is toegelicht. Het is belangrijk om expliciet te maken of het bij de beoordeling van sensitiviteit gaat om de kennis als basis van de technologie, de vaardigheden om een technologisch product te vervaardigen, het (eind)product van de technologie of een combinatie hiervan. Deze explicitering is in de systematiek (zie hoofdstuk 4 van deze rapportage) onderdeel van de **beschrijving van de technologie** die wordt geëvalueerd.

De afbakening van een technologie gaat niet alleen over de vraag of het over de kennis, de vaardigheden of het product gaat maar ook wat het **aggregatieniveau** is van hetgeen er wordt beoordeeld op sensitiviteit. De term technologie wordt zowel gebruikt om een overkoepelend kennisgebied aan te duiden (bijvoorbeeld kunstmatige intelligentie) als om een specifiek onderdeel van het overkoepelende kennisgebied aan te duiden (bijvoorbeeld gezichtsherkenning). Ook kan technologie gaan om een toepassing, ofwel de combinatie van een kennisgebied en een bepaalde gebruikerscontext (bijvoorbeeld autonome wapensystemen) (zie Figuur 1).



Figuur 1 Aggregatieniveau van technologie.

Tenslotte kan het ook gaan om de combinatie van verschillende kennisgebieden, ook wel convergentie genoemd (bijvoorbeeld brein-computer interfaces), waarbij ook weer specifieke toepassingen in verschillende gebruikerscontexten denkbaar zijn (zie Figuur 2).



Figuur 2 Convergentie tussen technologiegebieden.

Voor een goede beoordeling van de sensitiviteit is het belangrijk om te zoeken naar een **zo concreet mogelijke beschrijving van de technologie**, zonder daarbij de complexiteit en samenhang met de mogelijke gebruikscontext uit het oog te verliezen.

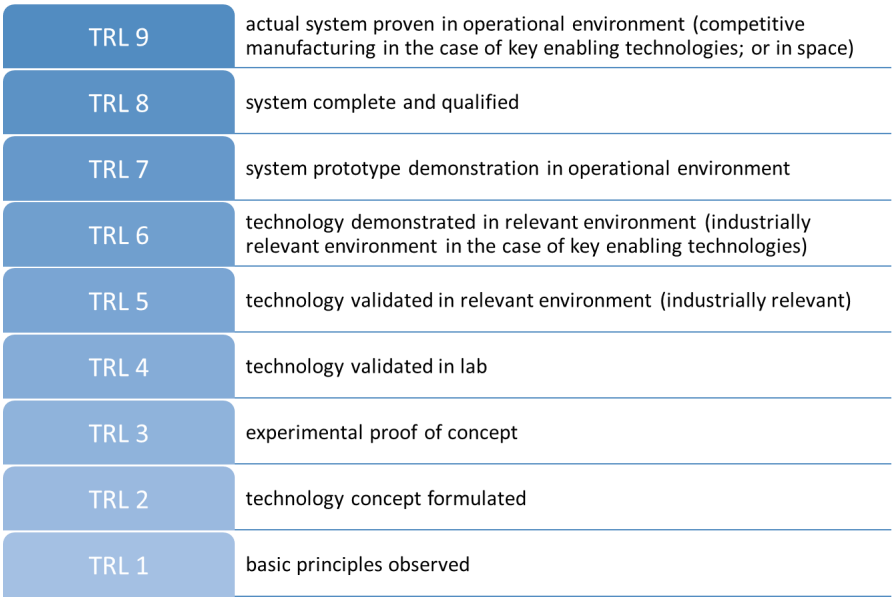
2.1.3 Technology Readiness Level

Een ander aspect van de technologie dat belangrijk is om mee te nemen bij de beoordeling van de sensitiviteit van de betreffende technologie is de fase van ontwikkeling waarin de technologie zich bevindt. Gaat het om een technologie die nog in de kinderschoenen staat of is het een technologie die (bijna) klaar is om (grootschalig) te gaan toepassen in de praktijk?

Een veelgebruikt systeem om de fase van de technologische ontwikkeling aan te duiden, is de indeling in ***technology readiness levels*** (TRL). Het TRL van een technologie verwijst naar de mate van maturiteit van een technologische ontwikkeling. In het raamwerk wordt onderscheid gemaakt tussen negen niveaus

van volwassenheid. TRL 1 betekent dat de ontwikkeling van de technologie nog helemaal aan het begin staat en TRL 9 betekent dat de technologie klaar is voor (commercieel) gebruik.

Het TRL raamwerk is oorspronkelijk ontwikkeld door NASA (Heder, 2017). Het raamwerk is in navolging van de NASA publicatie erover in 1989 breed geadopteerd in uiteenlopende sectoren, waarbij ook aangepaste varianten zijn ontwikkeld die minder expliciet refereren aan de oorspronkelijke '*space technology*' context waarin het NASA raamwerk is ontwikkeld. Vandaag de dag wordt het systeem over de hele wereld gehanteerd (Heder, 2017), bijvoorbeeld door de Europese Commissie in het kader van innovatiesubsidies zoals het Horizon2020 programma (zie Figuur 3).



Figuur 3 TRL niveaus zoals gehanteerd door de Europese Commissie voor H2020 (bron Europese Commissie, 2015).

Voor de inschatting van de sensitiviteit van een technologie geldt dat het relatief eenvoudiger wordt om potentiële risico's van het (onbedoelde of ongewenste) gebruik van de technologie voor te stellen naarmate het TRL hoger is. Immers, naarmate een technologische ontwikkeling dichterbij een daadwerkelijk gebruik in een operationele context komt is de technologie concreter af te bakenen en daarmee is de reikwijdte van mogelijke toepassingen ook kleiner geworden. Toch is het ook van belang om niet te wachten met het nadenken over potentiële risico's tot de technologie een hoge mate van volwassenheid kent. Om eventuele maatregelen te treffen voor het beschermen van de kennis of het voorkomen van ongewenst gebruik kan het juist belangrijk zijn om vroegtijdig na te denken over de potentiële toepassingen van een technologische ontwikkeling.

2.1.4 Dynamiek van technologische ontwikkelingen

Volgens Rip is technologie een "complex en veelvormig verschijnsel in onze maatschappij" (1995: 15) en is het ook niet eenvoudig om een strikte afbakening te hanteren. Sterker nog, hij beargumenteert dat het niet verstandig is om technologie als een exogene factor te zien in de samenleving, maar juist te kijken naar de betekenis van technologie als onderdeel van de samenleving (Rip 1995; Rip &

Kemp 1998). Een te nauwe of te instrumentele opvatting van technologie en de manier waarop technologische vernieuwing plaatsvindt, houdt te weinig rekening met de dynamieken die samenhangen met technologieontwikkeling en -toepassing.

Al in de jaren zestig en zeventig van de twintigste eeuw ontstond een debat over de vraag of technologische ontwikkelingen gedreven worden vanuit de vooruitgang in wetenschap en technologie (*technology-push*) of dat juist de (markt)vraag (*demand-pull*) bepalend is voor de richting en snelheid van technologische ontwikkelingen (Nemet 2009). Analyses laten zien dat technologische ontwikkelingen voortkomen uit een interactie tussen beide kanten (Nemet 2009, DiStefano et al. 2012), waarbij het ook van belang is om breder te kijken naar de vraagkant dan alleen de 'commerciële markt'. Technologische ontwikkelingen worden beïnvloed door sociale, economische en politieke krachten (Rip & Kemp, 1998) en de maatschappelijke uitdagingen waar de wereld voor staat, zoals bijvoorbeeld klimaatverandering of grondstoffenschaarste (Walrave & Raven, 2016). Tegelijkertijd wordt de samenleving ook beïnvloed door technologische ontwikkelingen, met name als deze leiden tot veranderingen in de manier waarop bepaalde processen of interacties ingericht en georganiseerd worden. De dynamiek of co-evolutie van technologie- en maatschappelijke verandering vindt met andere woorden plaats in een socio-technische configuratie (Geels, 2002; Geels & Kemp, 2007; Rip & Kemp, 1998).

2.1.5 Het disruptieve karakter van technologie

Om de dynamiek van technologische doorbraken en de maatschappelijke impact daarvan te duiden wordt vaak gesproken over **disruptieve technologie** (Carlsen et al., 2010). Andere termen die vaak gebruikt worden om de ingrijpende impact van technologische ontwikkelingen te duiden zijn '*emerging technologies*', '*emerging disruptive technologies*', '*radical breakthrough innovatons'* of '*radical technologies*' (e.g. Anderson & Tushman, 1990; Dahlin & Behrens, 2005; Reding & Eaton, 2020; Rotolo et al. 2015; Warnke et al., 2019). Hoewel de definities variëren gaat het over het algemeen om termen die gebruikt worden om het verschil aan te geven tussen 'normale' of 'incrementele' technologische ontwikkeling en technologische ontwikkelingen die een ingrijpende impact hebben en daardoor (mede) richting geven aan toekomstige ontwikkelingen.

Het ingrijpende ofwel 'disruptieve' karakter van technologie kan zowel aan de technologiekant zitten (omdat het een doorbraak betekent die als aanjager werkt voor ontwikkelingen in verschillende kennisgebieden) als aan de manier waarop de technologie effect heeft op de samenleving (de technologie vervangt bestaande technologieën waardoor een bepaald proces in de samenleving ingrijpend verandert). Het is van belang om beide aspecten van disruptiviteit in ogenschouw te nemen bij de evaluatie van sensitiviteit.

Het kan zijn dat een technologie zowel technologisch als maatschappelijk disruptief is. Het kan echter ook zijn dat een disruptieve technologie in de samenleving slechts tot incrementele veranderingen leidt of andersom dat een incrementele technologische ontwikkeling tot ingrijpende veranderingen in de samenleving leidt (Carlsen et al., 2010).

2.1.6 Gebruikscontext van technologie

Ook de gebruikscontext van de technologie is van belang om mee te nemen in de analyse van sensitiviteit. Hierbij gaat het enerzijds om de beoogde gebruikscontext van de technologie, en anderzijds om potentieel gebruik in andere contexten (zowel op de kortere termijn als de lange termijn).

Technologische ontwikkeling komt, zoals hiervoor ook is beschreven, tot stand vanuit een dynamische interactie tussen de wetenschappelijke mogelijkheden en de behoeften (vragen) vanuit de samenleving. Technologie is bovendien geen fundamentele wetenschap maar kennis gericht op een specifiek doel (het verbeteren van de efficiëntie of effectiviteit van bepaalde processen, het verhogen van de levensstandaard, het bevrijden van de mensheid van bepaalde ziekten, etc.). Dit betekent dat technologie over het algemeen wordt ontwikkeld met een bepaald toekomstig gebruik voor ogen (Carlsen et al., 2010). Dit kan betrekking hebben op een bepaalde sector (bijvoorbeeld transport of gezondheidszorg) of op een bepaald proces dat dwars door de samenleving gaat (bijvoorbeeld communicatie). Hoe concreter de technologie, des te specifieker het beoogde gebruik zal zijn. Door de gebruikscontext voor ogen te houden wordt het makkelijker om denkbare risico's van het toekomstig gebruik in te schatten. Hierbij is het van belang om niet alleen naar de korte- of middellange termijn te kijken maar ook naar mogelijke toepassingen op de langere termijn.

Daarnaast is het voor de analyse van sensitiviteit belangrijk om ook na te gaan wat mogelijke onbedoelde (en ongewenste) toepassingen (buiten de beoogde gebruikscontext) of effecten van de technologie kunnen zijn. Veel technologie die met een maatschappelijk doel is ontwikkeld kan bijvoorbeeld ook worden toegepast in een militaire context, wat weer aanvullende risico's met zich mee kan brengen. Dit wordt ook wel dual-use technologie genoemd[4]. Maar niet alleen gebruik in militaire context kan duiden op sensitiviteit in het kader van de nationale veiligheid. Ook gebruik van technologie door politie of veiligheidsdiensten brengt mogelijk risico's en kwetsbaarheden met zich mee die tot aantasting van de nationale veiligheid kunnen leiden. Daarnaast is ook van belang om oog te houden voor mogelijke toepassingen van de technologie in de context van de vitale processen, bijvoorbeeld vanuit het perspectief van dreiging door statelijke actoren of terrorismedreiging. De vitale processen zijn processen die zo essentieel zijn voor het functioneren van de samenleving dat uitval, verstoring of (digitale) compromittering ervan tot ernstige maatschappelijke ontwrichting leidt of nationale veiligheidsbelangen aantast en daarmee een bedreiging vormt voor de nationale veiligheid[5]. Welke processen vitaal zijn kan door de tijd veranderen en bij de analyse van sensitieve technologieën moet met deze ontwikkelingen rekening worden gehouden. Het gaat er steeds om te identificeren van welke technologieën de voor de samenleving als vitaal aangeduide processen afhankelijk zijn. Op dit moment worden de volgende processen als vitaal aangeduid (Figuur 4):

[4] Zie de EU-lijst dual-use goederen voor een uitgebreide lijst van dual-use goederen.
[5] Zie https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen voor meer toelichting en het meest recente overzicht van de Nederlandse vitale processen

Figuur 4 Overzicht vitale processen.

2.2 Nationale Veiligheid

Het begrip nationale veiligheid wordt door de Nederlandse overheid uitgedrukt in zes nationale veiligheidsbelangen (Figuur 5):

Zes nationale veiligheidsbelangen

We onderscheiden de volgende nationale veiligheidsbelangen:

1. Territoriale veiligheid	Het ongestoord functioneren van Nederland en haar EU- en NAVO-bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin.
2. Fysieke veiligheid	Het ongestoord functioneren van de mens in Nederland en zijn omgeving.
3. Economische veiligheid	Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie.
4. Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland.
5. Sociale en politieke stabiliteit	Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden.
6. Internationale rechtsorde	Het functioneren van het internationale stelsel van normen en afspraken, gericht op internationale vrede en veiligheid.

Figuur 5 De nationale veiligheidsbelangen (bron: NCTV, 2019).

De definitie van nationale veiligheid wordt in de Nationale Veiligheid Strategie (NCTV, 2019) als volgt geformuleerd: “De nationale veiligheid is in het geding wanneer een of meerdere nationale veiligheidsbelangen zodanig bedreigd worden, dat er sprake is van (potentiële) maatschappelijke ontwrichting”.

2.2.1 Nationale veiligheidsrisico’s

Om zicht te krijgen op de risico’s en dreigingen voor de nationale veiligheid voert het Analistennetwerk Nationale Veiligheid periodiek een nationale risicobeoordeling uit[6]. Hiervoor maakt het gebruik van een methodiek (ANV, 2019b) waarin de nationale veiligheidsbelangen zijn uitgewerkt in impactcriteria (Figuur 6).

[6] Tussen 2007 en 2014 werd een jaarlijkse Nationale Risicobeoordeling (NRB) gepubliceerd (zie https://www.rivm.nl/onderwerpen/nationale-veiligheid). In 2016 verscheen een eerste integrale analyse - het Nationaal Veiligheidsprofiel (ANV, 2016) en in 2019 is de opvolger daarvan verschenen – de Geïntegreerde Risicoanalyse Nationale Veiligheid (ANV, 2019a).

Nationaal veiligheidsbelang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het (Nederlands) grondgebied 1.2 Aantasting van de integriteit van de internationale positie van Nederland 1.3 Aantasting van de integriteit van de digitale ruimte
2. Fysieke veiligheid	2.1 Doden 2.2 Ernstig gewonden en chronisch zieken 2.3 Gebrek aan primaire levensbehoeften
3. Economische veiligheid	3.1 Kosten 3.2 Aantasting van de vitaliteit van de Nederlandse economie
4. Ecologische veiligheid	4.1 Langdurige aantasting van het milieu en de natuur
5. Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven 5.2 Aantasting van de democratische rechtstaat 5.3 Sociaal-maatschappelijke impact
6. Internationale rechtsorde	6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting 6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens 6.3 Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel 6.4 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties

Figuur 6 Nationale veiligheidsbelangen en onderliggende impactcriteria (bron: NCTV, 2019).

De risicobeoordeling hanteert een *all hazard* benadering waarbij verschillende typen risico's (risicocategorieën) – onderverdeeld in een aantal thema's – worden geanalyseerd op de impact en waarschijnlijkheid van optreden binnen 0-5 jaar. Hiervoor wordt per risicocategorie een of enkele scenario's uitgewerkt en beoordeeld. In de meest recente geïntegreerde risicoanalyse nationale veiligheid (ANV, 2019a) worden negen thema's en 27 risicocategorieën geïdentificeerd (Figuur 7).

Voor de analyse van de sensitiviteit van technologieën in de context van nationale veiligheid bieden de risicocategorieën en impactcriteria een nuttig aanknopingspunt. Hierbij is wel tijdens de gesprekken in de interdepartementale werkgroep aangegeven dat de focus bij de beoordeling van sensitiviteit moet liggen op de risico's die voortkomen uit moedwillig en ongewenst gebruik/misbruik van de technologie. Ongevallen of technisch falen worden als risico dan ook niet expliciet meegenomen. Ook situaties waarbij het gebruik van technologie indirect kan bijdragen aan het vergroten van een risico vallen buiten de scope van de sensitiviteitsanalyse. Het gaat hier bijvoorbeeld om een technologie die zorgt voor een verhoging van het energiegebruik, wat negatieve impact kan hebben op het klimaat, waardoor de kans op extreem weer of overstromingen kan toenemen.

Thema	Risicocategorie
Bedreigingen voor gezondheid en milieu	Infectieziekten humaan
	Dierziekten en zoönose
Natuurrampen	Extreem weer
	Overstroming
	Natuurbrand
	Aardbeving
Verstoring vitale infrastructuur	Verstoring vitale infrastructuur
Zware ongevallen	Stralingsongevallen
	Chemische incidenten
Cyberdreigingen	Digitale sabotage
	Aantasting functioneren internet
	Cyberspionage
	Cybercriminaliteit
Ondermijning democratische rechtsstaat	Niet-gewelddadig extremisme
	Ondermijnende criminaliteit (enclavevorming)
	Ongewenste buitenlandse inmenging
	Ongewenste buitenlandse beïnvloeding (via hybride operaties)
Gewelddadig extremisme en terrorisme	Gewelddadig extremisme
	Terrorisme
Financieel-economische bedreigingen	Criminele inmenging
	Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland (flow security)
	Handelskrimp/verstoring internationale handel
	Destabilisatie financieel systeem
Bedreigingen internationale vrede en veiligheid	Instabiliteit rondom Europa
	Militaire dreigingen (NAVO-lidstaat)
	CBRN-proliferatie
	Veiligheidsarrangementen onder druk (NAVO, EU)

Figuur 7 Overzicht thema's en risicocategorieën nationale veiligheid (bron: ANV, 2019a).

In de systematiek (zie hoofdstuk 4) worden de risicocategorieën en impactcriteria voor nationale veiligheid gebruikt als hulpmiddel om de vraag te beantwoorden welke mogelijke nationale veiligheidsrisico's kunnen ontstaan door het ongewenst gebruik van de betreffende technologie. Er is bewust gekozen om dit als *hulpvragen* – en daarmee op een kwalitatieve manier – te gebruiken omdat de inschatting van de mate van impact (van zeer beperkt tot catastrofaal) alleen mogelijk is wanneer er concrete scenario's worden geformuleerd. Een technologie *an sich* leidt niet zonder meer tot deze impact. De impactcriteria en risicocategorieën vormen dan ook aanknopingspunten om te beredeneren op welke manieren de technologie tot nationale veiligheidsrisico's en daarmee impact op de nationale veiligheidsbelangen kan leiden. Hiermee wordt in feite de eerste stap gezet om een aantal scenario's te formuleren. Indien gewenst kan voor een verdere verdieping van de analyse er voor gekozen worden om een aantal van deze scenario's verder uit te werken en te beoordelen aan de hand van de nationale veiligheid risicobeoordelingsmethodiek (ANV, 2019b).

2.2.2 Het thema economische veiligheid

De behoefte en urgentie om zicht te krijgen op de sensitiviteit van technologie in de context van nationale veiligheid komt in belangrijke mate voort uit het toenemend besef dat technologische, economische en (geo)politieke ontwikkelingen steeds nauwer verweven raken en dat dit ingrijpende gevolgen kan hebben voor de economie en de nationale veiligheid (Inspectie van Rijksfinanciën, 2020). In dit

kader spreekt men ook wel over het thema economische veiligheid[7]. Belangrijk aandachtspunt in dit thema is het belang van kennis en technologie voor de economie en voor internationale politieke verhoudingen. De NCTV (2018) benoemt in de context van economische veiligheid drie belangrijke risico's:

- Verstoring van de continuïteit van de vitale infrastructuur;
- Het weglekken van hoogwaardige kennis of vertrouwelijke informatie (zoals staatsgeheimen);
- Een sterke ongewenste afhankelijkheid van partijen en landen met wie Nederland niet dezelfde geopolitieke belangen deelt.

Binnen dit thema economische veiligheid gaat het dus om risico's die zich voordoen op het snijvlak van politieke, economische en veiligheidsbelangen. Het gaat om de positie van Nederland als autonome staat, de concurrentiekracht van onze economie en het beschermen van de maatschappij tegen grootschalige ontwrichting.

Hoewel in dit project gekeken wordt naar de sensitiviteit van technologie in de context van nationale veiligheid kunnen de nationale veiligheidsbelangen niet volledig los gezien worden van politieke of economische belangen. Sterker nog, in de operationalisering van het begrip nationale veiligheid komen ook expliciet politieke en economische elementen terug in de zes nationale veiligheidsbelangen (zie Figuur 5).

Bij de afbakening van de scope voor dit project is er bewust voor gekozen om in de systematiek het technologieperspectief centraal te stellen. Dat betekent dat gekeken wordt naar de potentiële risico's van het (ongewenste) gebruik van de technologie zelf. Welke actoren daarbij een rol spelen wordt niet expliciet meegenomen. Wel is het van belang om zicht te hebben op de uniciteit van de technologie. Hoe uniek is de kennis, al dan niet in combinatie met de toegang tot benodigde hulpbronnen (*enabling technologies*, grondstoffen, etc.) om de technologie te ontwikkelen en/of te produceren? Het gaat er hierbij niet om de specifieke actoren te benoemen die over de technologie beschikken, maar wel om inzicht te krijgen in de mate waarin er eventueel sprake is van een al dan niet gekapitaliseerde strategische economische positie.

Concreet betekent dit dat ook een technologie die nog niet commercieel succesvol is (bijvoorbeeld van een startup zonder klanten) wel als sensitief kan worden bestempeld, vanwege de (strategisch-economische) potentie die het heeft.

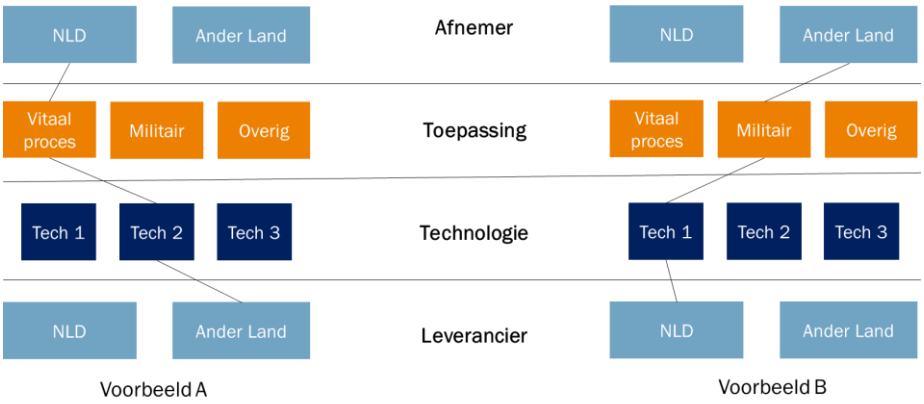
Naast de risico's van de technologieën zelf kunnen er ook risico's voor de nationale veiligheid ontstaan die te maken hebben met de positie van Nederland in het technologisch speelveld of specifieke transacties waardoor technologie in handen valt van actoren die er normen en waarden op nahouden die indruisen tegen de normen en waarden van Nederland en haar. In Figuur 8 wordt schematisch weergegeven hoe transacties en posities in de internationale waardenketen van technologieën van belang kunnen zijn.

[7] We maken hier een expliciet onderscheid tussen het thema economische veiligheid (de typen risico's die voortkomen uit technologische, politieke en economische ontwikkelingen) en het economische veiligheidsbelang (het derde van de zes nationale veiligheidsbelangen als onderdeel van de definitie van nationale veiligheid).

In **voorbeeld A** is Nederland voor een technologie die gebruikt wordt in de vitale infrastructuur afhankelijk van een leverancier uit een ander land. Dit kan leiden tot eventuele ongewenste strategische afhankelijkheden, waarmee het een potentieel risico voor de nationale veiligheid is.

In **voorbeeld B** is een Nederlandse partij de leverancier van een technologie met een toepassing in de militaire context. Een ander land wil deze technologie afnemen. Hierdoor kan de technologie in handen vallen van een actor die er normen en waarden op nahoudt die indruisen tegen de normen en waarden van Nederland of haar bondgenoten. Als gevolg hiervan kan het risico ontstaan dat de technologie wordt ingezet tegen Nederland of haar bondgenoten, of op een andere manier die de normen en waarden van Nederland of haar bondgenoten schaadt.

Beide transacties kunnen dus potentieel een risico vormen voor de nationale veiligheid, afhankelijk van de intenties van betreffende partijen en landen.



Figuur 8 Voorbeelden van transacties en posities in de internationale waardeketen van technologieën.

Dit zijn aspecten die moeten worden meegenomen in de beleidsafweging over de eventueel te nemen maatregelen om sensitieve technologieën te beschermen en risico's voor de nationale veiligheid te beheersen (zie paragraaf 4.7). In de systematiek wordt hier wel op voorbereid door bij de beschrijving van de technologie die wordt beoordeeld ook in te gaan op de **uniciteit** van deze technologie. Hierbij gaat het enerzijds om de vraag of de betreffende technologie een unieke oplossing is voor een belangrijk vraagstuk of dat er ook alternatieven bestaan (immers, in dat geval is er minder kans op een ongewenste afhankelijkheid van de betreffende technologie). Anderzijds wordt gevraagd of er sprake is van een dominante speler op de betreffende technologie (eenzijdige afhankelijkheid van een speler voor de toegang tot de technologie kan een risico vormen, ongeacht welke speler het hier betreft).

2.3 Sensitiviteit

Zoals aangegeven verwijst de sensitiviteit van een technologie naar de potentiële risico's voor de nationale veiligheid die voortkomen uit het ongewenst gebruik van de betreffende technologie. Om hier zicht op te krijgen is het belangrijk om een goed beeld te krijgen van de technologie die wordt beoordeeld. Het gaat hierbij

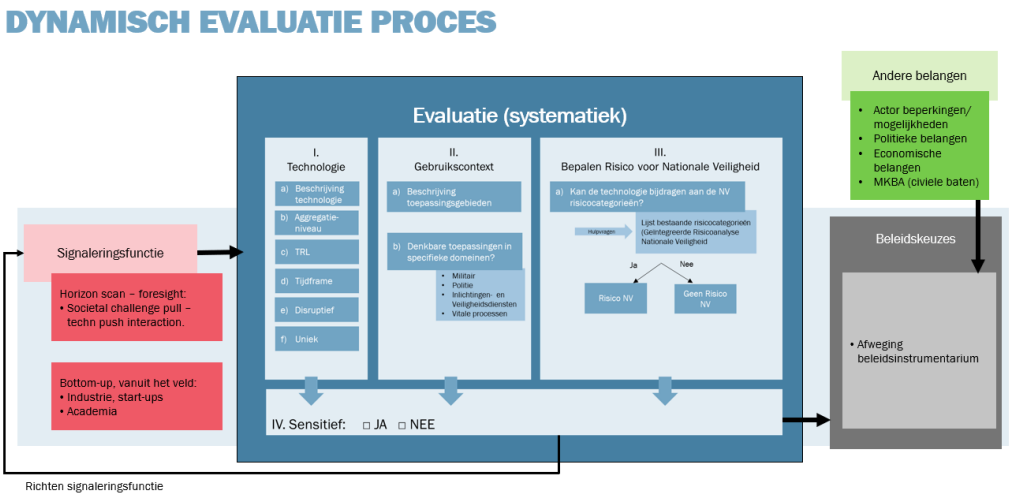
naast een concrete beschrijving en afbakening van de technologie ook om de status van de technologische ontwikkeling (TRL), de mate van disruptiviteit van de technologie (radicale impact op kennis en technologie ontwikkelen en/of in de samenleving) en de mate van uniciteit van de technologie. Ook het (bedoelde en onbedoelde) gebruik en potentiële toepassingen van de technologie in verschillende domeinen spelen een rol bij de beoordeling van de sensitiviteit. Deze factoren zijn in de systematiek in drie verschillende blokken uitgewerkt (technologie, gebruikscontext, risico's voor nationale veiligheid).

Belangrijk is om aan te geven dat de beoordeling van de sensitiviteit van een technologie een dynamisch karakter heeft. Een technologie kan door allerlei ontwikkelingen in de toekomst meer of minder sensitief worden. Ook verandert de mate van onzekerheid van de beoordeling van een technologie met een laag TRL naarmate het een hoger TRL bereikt. Het is dan ook zaak om de beoordeling van sensitiviteit van technologieën periodiek, bijvoorbeeld jaarlijks, te herhalen en daarnaast tussentijds te herzien als nodig.

3 Systematiek voor de afweging van sensitieve technologieën

3.1 Introductie

Technologie die als sensitief beschouwd wordt is voortdurend aan verandering onderhevig. Nieuwe technologieën kunnen op enig moment bijzonder zijn en grote veiligheidsconsequenties hebben, later kan het gangbare technologie zijn waar vele maatschappelijke processen gebruik van maken. Een systematiek waarmee sensitieve technologie geduid kan worden, moet met deze ontwikkeling om kunnen gaan. Figuur 9 geeft schematisch weer hoe het beoordelingsproces eruit ziet. Hierbij wordt er van uitgegaan dat het beoordelingsproces op interdepartementaal niveau, gemeenschappelijk wordt ingericht en uitgevoerd. Ook is het van belang om de juiste (interne en externe) kennis en expertise te betrekken. De manier waarop daar invulling aan wordt gegeven, valt buiten de scope van dit project.

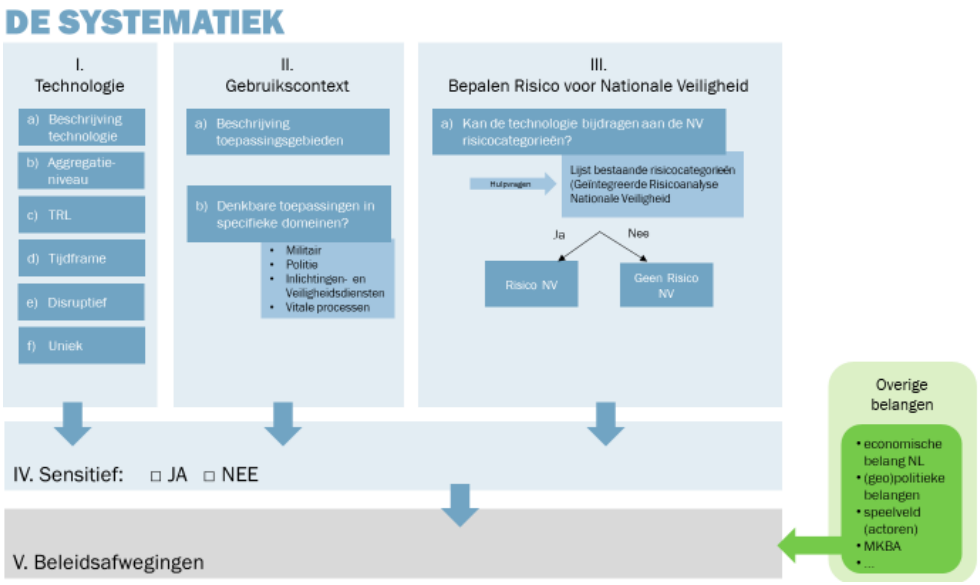


Figuur 9 Dynamisch evaluatie proces.

Allereerst is er behoefte aan een signaleringsfunctie op basis waarvan relevante technologieën in beeld komen. Aangedragen technologieën worden vervolgens op sensitiviteit beoordeeld met de evaluatiesystematiek. Deze evaluatie beoogt de technologie initieel op sensitiviteit te beoordelen ongeacht de betrokken actoren en andere beleidsafwegingen. In de laatste stap worden deze andere belangen meegenomen om tot een eindafweging te komen. De systematiek wordt in de volgende paragraaf stapsgewijs beschreven.

3.2 De systematiek

De systematiek bestaat uit vijf verschillende blokken (zie Figuur 10). Elk blok bestaat uit één of meerdere vragen. Per blok volgt een korte toelichting en vervolgens de vragen die beantwoord moeten worden. Na afloop van elk blok is er ruimte om de inzichten uit dat blok te formuleren in een samenvatting.



Figuur 10 Schematisch overzicht van de systematiek.

3.2.1 Blok I: Technologie

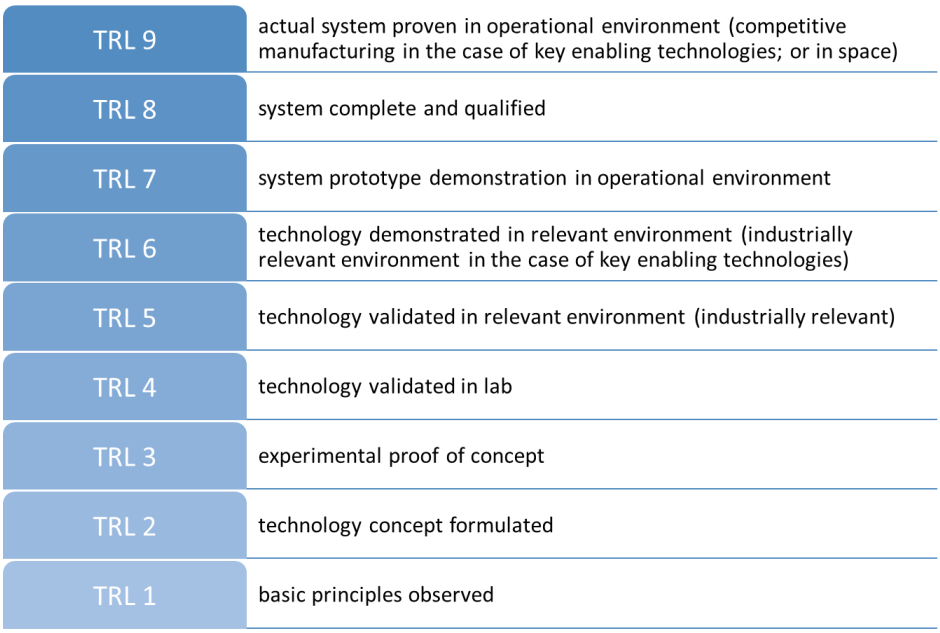
Het eerste blok is bedoeld om te bepalen van welke technologie de sensitiviteit wordt beoordeeld. De vragen in dit blok zijn bedoeld om het perspectief op te bouwen van waaruit de rest van de vragenlijst wordt ingevuld. Dit kan heel nauw zijn afgebakend (een technologie als onderdeel van een concreet, bestaand product) of breed (de mogelijkheden van een technologiegebied over 10 jaar).

Bij het beantwoorden van onderstaande vragen kan men tot de conclusie komen dat niet één maar meerdere onderscheidende technologieën beoordeeld moeten worden op sensitiviteit. In dat geval moeten alle blokken van de systematiek (kortweg de vragenlijst) voor elke technologie afzonderlijk doorlopen worden.

Bij vraag d) moet worden aangegeven in welk tijdsframe de sensitiviteitsanalyse wordt uitgevoerd. De risico's op korte termijn en op de langere termijn kunnen sterk uiteenlopen, zeker bij technologieën die pas op lange termijn in daadwerkelijke toepassingen beschikbaar komen. Wanneer de risico's op verschillende momenten in de tijd geanalyseerd moeten worden, dient ook hier de gehele systematiek voor elk tijdsframe afzonderlijk doorlopen te worden.

a) Beschrijving technologie	
Beschrijf kort welke technologie wordt beschouwd. • Wees zo concreet mogelijk. Indien het een product is, probeer dan de technologie die in het product gebruikt wordt te benoemen. Het gaat bij de beoordeling niet zozeer over de sensitiviteit van het product (bijv. een softwarepakket van een specifieke leverancier) maar om de technologie (bijv. gezichtsherkenningstechnologie). • Als het een combinatie betreft van meerdere technologieën is het van belang aan te geven of het alleen gaat om het beoordelen van de combinatie of ook om de individuele technologieën. In dat laatste geval moet de vragenlijst meerdere keren (voor elke technologie of combinatie) worden doorlopen.	
b) Aggregatieniveau	
Welk aggregatieniveau wordt beschouwd? • Gaat het om een concreet afgebakende (sub)technologie of een breed technologiegebied (e.g. quantum computing of AI)? • Hou er rekening mee dat het beoordelen van de sensitiviteit van een breed technologiegebied moeilijker is dan een concreter afgebakende technologie.	
c) TRL	
Wat is op dit moment de maturiteit van de technologie die wordt beschouw? • Wat is het Technology Readiness Level (1-9)? Zie Figuur 11 voor een toelichting van de verschillende niveaus. • Wat is de verwachtte/ingeschatte duur voordat TRL 9 zal worden bereikt?	
d) Tijdframe	
Voor welk tijdframe wordt de analyse uitgevoerd? • Gaat het om de technologie zoals deze nu al bestaat (huidige stand van zaken), waarbij breed gekeken wordt naar mogelijke toepassingen nu en op korte termijn (binnen enkele jaren) of gaat het om een technologie in ontwikkeling waarbij gekeken wordt naar de verwachte mogelijkheden in de toekomst (over 5 jaar, 10 jaar, langer)? • Indien zowel de huidige mogelijkheden als de mogelijkheden op de langere termijn beschouwd moeten worden, is het aan te raden de vragenlijst meerdere keren te doorlopen om de onzekerheden die samenhangen met inschattingen op verschillende tijdframes gescheiden gehouden.	

e) Hoe disruptief is de technologie?	
Licht toe in hoeverre het een 'disruptieve' technologie betreft. • Lost de technologie een cruciaal vraagstuk op? • Maakt de technologie het mogelijk om andere technologieën door te ontwikkelen?	
f) Hoe uniek is de technologie?	
Licht toe hoe uniek de technologie is • Zijn er alternatieven? • Is er sprake van één of enkele dominante speler(s) op de technologie?	



Figuur 11 Technology Readiness Levels.

SAMENVATTING VAN TECHNOLOGIE PERSPECTIEF[8]:

[8] Indien er meerdere perspectieven (bijv. enkelvoudige of combinaties van technologieën of meerdere tijdframes) worden beschouwd, vul dan een nieuwe vragenlijst in per perspectief en beschrijf in dit vak het betreffende perspectief per vragenlijst.

3.2.2 Blok II: Gebruikscontext

In het volgende blok wordt een beeld gevormd van de (denkbare) gebruikscontext van een technologie. Het gaat hierbij zowel om beoogde toepassingen als toepassingen die voorstelbaar zijn. Hier wordt nog geen inschatting gemaakt van de mogelijke risico's die de technologie vormt voor deze domeinen.

a) Wat zijn de toepassingsgebieden van de technologie?	
Beschrijf kort wat de (verwachte of huidige) toepassingsgebieden van de technologie zijn. Wees zo concreet mogelijk. • Als dit er heel veel zijn, geef dan in elk geval een aantal voorbeelden. • Het kan helpen om te benoemen wat voor soort probleem of vraagstuk de technologie oplost.	
b) Zijn er toepassingen van de technologie denkbaar in de volgende domeinen?	
Geef in aanvulling op de algemene beschrijving van de gebruikscontext van de technologie aan welke denkbare toepassingen er zijn in de volgende domeinen. • Het gaat er dan om dat organisaties in deze domeinen gebruik maken van de technologie om hun werk (beter) te doen. • Het gaat in deze stap nog niet over het gericht inzetten van de technologie om het werk in deze domeinen te verstoren (dat valt onder de risico inventarisatie in stap III). • Licht toe wat de toepassing inhoudt en of deze toepassing op dit moment al denkbaar is of dat daarvoor nog andere voorwaarden benodigd zijn.	
Militair	
Politie	
Inlichtingen- en veiligheidsdiensten	
Vitale processen (zie Figuur 12)	

Figuur 12 Overzicht vitale processen (bron NCTV[9]).

[9] Zie https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen voor meer toelichting en het meest recente overzicht van de Nederlandse vitale processen.

SAMENVATTING VAN DE GEBRUIKSCONTEXT VAN DE TECHNOLOGIE

3.2.3 Blok III: Risico's voor de Nationale Veiligheid

In dit blok wordt bepaald of de technologie kan leiden tot aantasting van de nationale veiligheid. Hiervoor wordt gekeken of de technologie kan bijdragen aan specifieke typen risico's voor de nationale veiligheid. Bij het doorlopen van dit blok van de systematiek is het belangrijk om steeds voor ogen te houden welk technologieperspectief (blok I) beschouwd wordt. De in blok II geïdentificeerde gebruikscontext kan helpen om te beredeneren welke risico's denkbaar zijn.

De hulpvragen in dit blok zijn bedoeld om te ondersteunen in het identificeren van potentiële risico's voor de nationale veiligheid. Er is geen sprake van een weging van de vragen. Een enkel belangrijk risico kan ertoe leiden dat de technologie uiteindelijk als sensitief beoordeeld wordt. Ook kan het zijn dan meerdere risico's benoemd worden, maar dat die zo vergezocht zijn dat dit uiteindelijk niet als een reëel risico wordt gezien. Om aan het einde van dit blok de potentiële risico's te kunnen verwoorden is het belangrijk om bij de beantwoording van de vragen de redenering toe te lichten. Een lang en ingewikkeld verhaal met onwaarschijnlijke samenloop van omstandigheden kan er dan op wijzen dat het nationale veiligheidsaspect alleen zeer indirect aan de orde is.

a) Kan de technologie bijdragen aan de NV risicocategorieën?
Om de risico's van een technologie voor de nationale veiligheid te bepalen is het zinvol om uit te gaan van de typen risico's die in eerdere analyses naar voren zijn gekomen als risico voor de nationale veiligheid. Dit zijn de risicocategorieën zoals die in de risicobeoordeling voor nationale veiligheid[10] wordt gehanteerd (zie Figuur 13). Om te bepalen of de technologie kan bijdragen aan één of meer van deze risico's zijn een aantal hulpvragen geformuleerd. Door deze vragen (die gebaseerd zijn op de risicocategorieën) te doorlopen ontstaat een beeld van de typen risico's die vanuit de (ongewenste) toepassing van de technologie kunnen voortkomen. Zoals eerder aangegeven is het van belang om expliciet onderscheid te maken tussen verschillende tijdsdimensies van waaruit de technologie wordt geanalyseerd. Dit is met name ook in dit blok van belang om onderscheid te maken tussen risico's die nu al spelen en risico's die in de nabije of verdere toekomst mogelijk worden voorzien (en daarmee wellicht onzekerder).

[10] De meest recente risicobeoordeling is de Geïntegreerde Risicoanalyse (ANV, 2019). Deze is als input gebruikt voor de Nationale Veiligheid Strategie 2019.

HULPVRAGEN RISICOCATEGORIEËN	***huidig***	***binnen 5 jaar***	***binnen 10 jaar***
1. Kan de technologie ingezet worden als onderdeel van een wapensysteem? Licht toe. *NB. Het gaat hierbij om wapensystemen zoals bedoeld in de lijst van EU wapenverordening*			
2. Creëert de technologie (aanvullende/effectievere) mogelijkheden om de beschikbaarheid, integriteit of vertrouwelijkheid van digitale systemen of informatie aan te tasten? Licht toe.			
3. Kan de technologie ervoor zorgen dat toegang tot of beschikbaarheid van wapens en andere (digitale) aanvalsmiddelen laagdrempeliger wordt? Licht toe.			
4. Kan de technologie worden ingezet om nieuwe ziekten te ontwikkelen of te verspreiden? Licht toe.			
5. Kan de technologie leiden tot grotere aantallen onbeheerde CBRN bronnen of transporten en/of wordt controle lastiger? Licht toe.			
6. Kan de technologie ervoor zorgen dat chemische, biologische of fysische processen toegankelijker worden voor misbruik? (bijv. omdat er kleinschalig of gedecentraliseerd maatschappelijk gebruik ontstaat). Licht toe			
7. Kan de technologie ingezet worden om verstoring of uitval van vitale processen te veroorzaken? Licht toe.			
8. Kunnen bij toepassing van de technologie in de aansturing of monitoring van vitale processen nieuwe kwetsbaarheden ontstaan? Licht toe.			
9. Creëert de technologie een grotere afhankelijkheid tussen vitale processen onderling? Licht toe.			
10. Biedt de technologie mogelijkheden om bevolkingsgroepen te manipuleren, intimideren, onderdrukken of domineren? Licht toe.			
11. Biedt de technologie mogelijkheden om organisaties te controleren of manipuleren? Licht toe.			

12. Biedt de technologie mogelijkheden om het functioneren van politieke vertegenwoordiging, openbaar bestuur, rechtelijke macht en/of het openbare orde en veiligheidssysteem aan te tasten? Licht toe.			
13. Biedt de technologie (nieuwe) middelen voor extremisten of terroristen om hun doelen te bereiken? Licht toe.			
14. Biedt de technologie (nieuwe) mogelijkheden om ecosystemen (flora en fauna) grootschalig aan te tasten? Licht toe.			
Het is denkbaar dat er vanuit een nieuwe technologie ook nieuwe typen risico's voortkomen. Het is niet het doel van deze systematiek om een analyse te doen van alle denkbare nieuwe risico's die door technologie kunnen ontstaan. Wel is het interessant om na te gaan of er concrete aanwijzingen zijn dat de technologie op een andere wijze dan vanuit de bestaande typen risico's de nationale veiligheidsbelangen (zie Figuur 14) kan aantasten. Hiervoor is onderstaande extra vraag (15) toegevoegd.			
15. Zijn er aanwijzingen dat de technologie op een andere wijze de nationale veiligheidsbelangen kan aantasten? Licht toe.			

SAMENVATTING IDENTIFICATIE VAN POTENTIËLE RISICO'S VOOR NATIONALE VEILIGHEID

Thema	Risicocategorie
Bedreigingen voor gezondheid en milieu	Infectieziekten humaan
	Dierziekten en zoönose
Natuurrampen	Extreem weer
	Overstroming
	Natuurbrand
	Aardbeving
Verstoring vitale infrastructuur	Verstoring vitale infrastructuur
Zware ongevallen	Stralingsongevallen
	Chemische incidenten
Cyberdreigingen	Digitale sabotage
	Aantasting functioneren internet
	Cyberspionage
	Cybercriminaliteit
Ondermijning democratische rechtsstaat	Niet-gewelddadig extremisme
	Ondermijnende criminaliteit (enclavevorming)
	Ongewenste buitenlandse inmenging
	Ongewenste buitenlandse beïnvloeding (via hybride operaties)
Gewelddadig extremisme en terrorisme	Gewelddadig extremisme
	Terrorisme
Financieel-economische bedreigingen	Criminele inmenging
	Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland (flow security)
	Handelskrimp/verstoring internationale handel
	Destabilisatie financieel systeem
Bedreigingen internationale vrede en veiligheid	Instabiliteit rondom Europa
	Militaire dreigingen (NAVO-lidstaat)
	CBRN-proliferatie
	Veiligheidsarrangementen onder druk (NAVO, EU)

Figuur 13 Overzicht risicocategorieën nationale veiligheid (bron ANV, 2019).

Nationaal veiligheidsbelang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het (Nederlands) grondgebied 1.2 Aantasting van de integriteit van de internationale positie van Nederland 1.3 Aantasting van de integriteit van de digitale ruimte
2. Fysieke veiligheid	2.1 Doden 2.2 Ernstig gewonden en chronisch zieken 2.3 Gebrek aan primaire levensbehoeften
3. Economische veiligheid	3.1 Kosten 3.2 Aantasting van de vitaliteit van de Nederlandse economie
4. Ecologische veiligheid	4.1 Langdurige aantasting van het milieu en de natuur
5. Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven 5.2 Aantasting van de democratische rechtstaat 5.3 Sociaal-maatschappelijke impact
6. Internationale rechtsorde	6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting 6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens 6.3 Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel 6.4 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties

Figuur 14 Nationale veiligheidsbelangen en onderliggende impactcriteria (bron: NCTV, 2019).

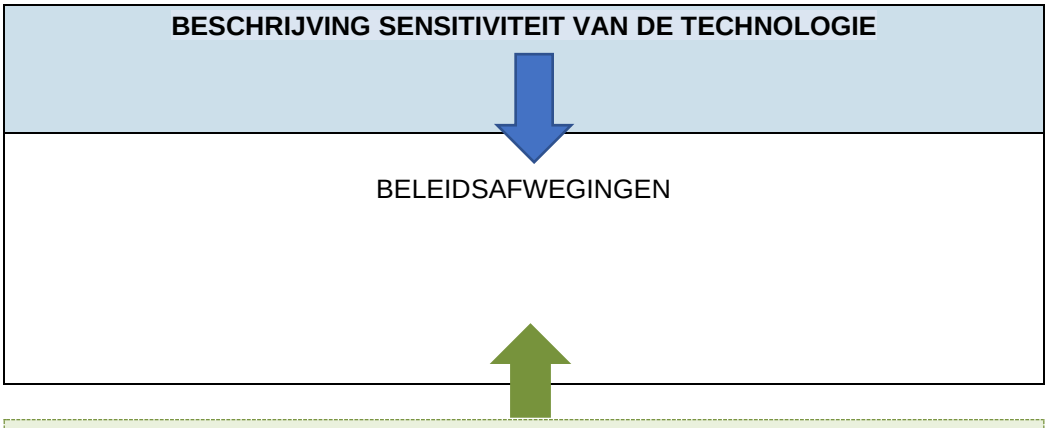
3.2.4 Sensitiviteit

Nadat is bepaald of de technologie potentiële risico's voor de nationale veiligheid met zich mee brengt moeten de uitkomsten van onderdeel I, II en III in gezamenlijkheid beschouwd worden om te bepalen of de technologie sensitief is. Indien de technologie sensitief is komt de technologie op de dynamische lijst van sensitieve technologieën. In sommige gevallen zal dat overduidelijk zijn. In andere gevallen zal meer twijfel bestaan omdat het onzeker is hoe groot de impact op de nationale veiligheid nu werkelijk kan worden. In zulke gevallen verdient het aanbeveling om een verdiepende analyse te doen, door bijvoorbeeld een scenario uit te werken en deze te beoordelen met de NV Methodiek van het ANV (zie Leidraad risicobeoordeling).

SAMENVATTING VAN TECHNOLOGIE PERSPECTIEF	**SAMENVATTING VAN DE GEBRUIKSCONTEXT VAN DE TECHNOLOGIE**	**SAMENVATTING IDENTIFICATIE VAN POTENTIËLE RISICO'S VOOR NATIONALE VEILIGHEID**
Is de technologie sensitief?		**Ja** ☐ **Nee** ☐

3.2.5 Beleidsafwegingen

Nu is bepaald of de technologie sensitief is, moet een eindafweging worden gemaakt. Hierbij worden alle uitkomsten uit de voorgaande onderdelen afgewogen tegen andere beleidsoverwegingen zoals het belang van de technologie voor de Nederlandse economie, (geo)politieke belangen, maatschappelijke kosten/baten en de posities in het speelveld rondom de technologie. Hierbij kunnen bepaalde aspecten die samenhangen met de technologie tegen elkaar afgewogen worden om te bepalen of er maatregelen moeten worden getroffen en zo ja, welke. Het betrekken van overige belangen in de beleidsafwegingen is geen onderdeel van de systematiek, dit betreft dus een vervolgstap voor de betrokken beleidsdepartementen. Voor de volledigheid staat deze stap wel gevisualiseerd.



Overige belangen (het belang van de technologie voor de Nederlandse economie, (geo)politieke belangen, maatschappelijke kosten/baten en de posities in het speelveld rondom de technologie.

4 Geraadpleegde bronnen

Agar, J. (2020). What is technology? *Annals of Science*, 77:3, 377-382, DOI: 10.1080/00033790.2019.1672788.

Analistennetwerk Nationale Veiligheid (2019a). *Geïntegreerde Risicoanalyse Nationale Veiligheid.* Bilthoven: RIVM.

Analistennetwerk Nationale Veiligheid (2019b). *Leidraad risicobeoordeling Geïntegreerde risicoanalyse Nationale Veiligheid.* Bilthoven: RIVM.

Anderson, P. & Tushman, M. L. (1990). Technological discontinuities and dominant designs: A cyclical model of technological change. *Administrative science quarterly*, 604-633.

Carlsen, H., Dreborg, K. H., Godman, M., Hansson, S. O., Johansson, L. & Wikman-Svahn, P. (2010). Assessing socially disruptive technological change. *Technology in Society*, 32(3), 209-218.

Dahlin, K. B. & Behrens, D. M. (2005). When is an invention really radical?: Defining and measuring technological radicalness. *Research policy*, 34(5), 717-737.

Di Stefano, G., Gambardella, A. & Verona, G. (2012). Technology push and demand pull perspectives in innovation studies: Current findings and future research directions. *Research policy*, 41(8), 1283-1295.

Europese Commissie (2015). *Horizon 2020 – Work Programme 2014-2015. Annes G. Technology readiness levels (TRL).* https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

Geels, F. W. (2002). Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study. *Research policy*, 31(8-9), 1257-1274.

Geels, F. W. & Kemp, R. (2007). Dynamics in socio-technical systems: Typology of change processes and contrasting case studies. *Technology in society*, 29(4), 441-455.

Heder, M. (2017). From NASA to EU: the evolution of the TRL scale in Public Sector Innovation. *The Innovation Journal*, 22: 1–23.

Inspectie der Rijksfinanciën (2020) Speelbal of spelverdeler? Concurrentiekracht en nationale veiligheid in een open economie. Brede maatschappelijke heroverwegingen (BMH 16). https://www.rijksoverheid.nl/documenten/rapporten/2020/04/20/bmh-16-speelbal-of-spelverdeler

NCTV (2018) *Factsheet Nationale veiligheid bij overnames en investeringen of inkoop en aanbesteding*. https://www.nctv.nl/onderwerpen/economische-veiligheid/documenten/publicaties/2018/06/21/factsheet-nationale-veiligheid-bij-overnames-en-investeringen-of-inkoop-een-aanbesteding

NCTV (2019) *Nationale Veiligheid Strategie 2019*. https://www.nctv.nl/documenten/publicaties/2019/6/07/nationale-veiligheid-strategie-2019

Nemet, G. F. (2009). Demand-pull, technology-push, and government-led incentives for non-incremental technical change. *Research policy*, 38(5), 700-709.

Reding, D.F. & Eaton, J. (2020). *Science & Technology Trends 2020-2040. Exploring the S&T Edge.* NATO Science & Technology Organization. https://www.nato.int/cps/en/natohq/news_175574.htm

Rip, A. (1995). What is this thing called technology?, in Achterhuis, H., Smits, R., Geurts, J., Rip, A., Roelofs, E. (reds.) (1995) *Technologie en samenleving.* (pp. 15-27). Leuven / Apeldoorn: Garant.

Rip, A. & Kemp, R. (1998). Technological change. *Human choice and climate change*, *2*(2), 327-399.

Rotolo, D., Hicks, D. & Martin, B. R. (2015). What is an emerging technology?. *Research policy*, 44(10), 1827-1843.

Walrave, B. & Raven, R. (2016). Modelling the dynamics of technological innovation systems. Research policy, 45(9), 1833-1844.

Warnke, P., Cuhls, K., Schmoch, U., Daniel, L., Andreescu, L., Dragomir, B., ... & Kuusi, O. (2019). *100 Radical Innovation Breakthroughs for the future*. European Commission. https://ec.europa.eu/jrc/communities/en/community/digitranscope/document/100-radical-innovation-breakthroughs-future

White House (2020) *National Strategy for Critical and Emerging Technologies.* White House, United States. https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf