WIJ WILLEM-ALEXANDER,
BIJ DE GRATIE GODS,
KONING DER NEDERLANDEN,
PRINS VAN ORANJE-NASSAU,
ENZ. ENZ. ENZ.

Regels tot invoering van een screening om ongewenste kennis- en technologieoverdracht via onderzoekers, studenten en technisch ondersteunend personeel van kennisinstellingen te voorkomen en daarmee risico's voor de nationale veiligheid te verminderen (Wet screening kennisveiligheid)

Voorstel van wet

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is om een screening van personen te introduceren voorafgaand aan het verkrijgen van toegang tot sensitieve technologie bij kennisinstellingen, met als doel ongewenste kennis- en technologieoverdracht met betrekking tot sensitieve technologie te voorkomen en daarmee risico's voor de nationale veiligheid te verminderen;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Hoofdstuk 1. Algemene bepalingen

Artikel 1. Begripsbepalingen

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

kennisinstelling: een rechtspersoon die een in de bijlage van de Wet op het hoger onderwijs en wetenschappelijk onderzoek opgenomen instelling of academisch ziekenhuis in stand houdt of is, een rechtspersoon voor hoger onderwijs als bedoeld in de Wet op het hoger onderwijs en wetenschappelijk onderzoek dan wel een in bijlage 1 bij deze wet opgenomen rechtspersoon;

nationale veiligheid: de nationale veiligheid als bedoeld in artikel 4, tweede lid, van het Verdrag betreffende de Europese Unie, openbare veiligheid als bedoeld in de artikel 45, derde lid en 52, eerste lid, en 65, eerste lid, onderdeel b, van het Verdrag betreffende de werking van de Europese Unie, of de wezenlijke belangen van de veiligheid van de staat, bedoeld in artikel 346, eerste lid, onderdeel a, van het Verdrag betreffende de

werking van de Europese Unie, die strekken tot bescherming van de belangen die binnen Nederland wezenlijk zijn voor het voortbestaan van de democratische rechtsorde, voor de veiligheid of voor andere gewichtige belangen van de staat, of voor de instandhouding van de maatschappelijke stabiliteit, voor zover die zien op het raakvlak tussen onderzoek en onderwijs en veiligheid, te weten:

i. de instandhouding van de continuïteit van vitale processen;

ii. het behoud van de integriteit en exclusiviteit van kennis en informatie met kritieke of strategische betekenis voor Nederland; of

iii. het voorkomen van ongewenste strategische afhankelijkheden van Nederland van andere landen;

Onze Minister: Onze Minister van Onderwijs, Cultuur en Wetenschap;

sensitieve technologie: sensitieve technologie als bedoeld in artikelen 5 en 6;

screening: screening als bedoeld in artikel 9;

screeningsbesluit: besluit als bedoeld in artikel 14;

screeningsplichtige: degene die screeningsplichtig is op grond van artikel 3, niet zijnde een persoon als bedoeld in artikel 4.

Artikel 2. Wijziging bijlage
1. Een wijziging van de statutaire naam van een rechtspersoon, genoemd in bijlage 1 van deze wet, wordt geacht met onmiddellijke ingang te zijn opgenomen in die bijlage.
2. In geval van omzetting, fusie of splitsing van een rechtspersoon als bedoeld in het eerste lid wordt of worden de daaruit voortkomende rechtspersoon of rechtspersonen geacht met onmiddellijke ingang te zijn opgenomen in bijlage 1 van deze wet.
3. Op de voordracht van Onze Minister in overeenstemming met Onze Minister of Ministers wie het mede aangaat, kunnen bij algemene maatregel van bestuur rechtspersonen aan bijlage 1 worden toegevoegd, indien door de rechtspersoon onderzoek wordt gedaan of onderwijs wordt verzorgd op het gebied van sensitieve technologie.

Hoofdstuk 2. Toepassingsbereik

Artikel 3. Screeningsplichtige
Screeningsplichtig is eenieder die:
a. voornemens is onderzoek te gaan doen of onderwijs te gaan verzorgen aan een onderdeel van een kennisinstelling als bedoeld in artikel 7 en daarbij toegang zou krijgen tot sensitieve technologie en voor wie geldt dat de kennisinstelling diegene wil belasten met dit onderzoek of dit onderwijs;
b. voornemens is technisch ondersteunende werkzaamheden ten behoeve van onderzoek of onderwijs te gaan verrichten aan een onderdeel van een kennisinstelling als bedoeld in artikel 7 en daarbij toegang zou krijgen tot sensitieve technologie en voor wie geldt dat de kennisinstelling diegene wil belasten met deze werkzaamheden; of
c. voornemens is te gaan studeren aan een onderdeel van een kennisinstelling als bedoeld in artikel 7 en daarbij toegang zou krijgen tot sensitieve technologie en van wie de kennisinstelling heeft vastgesteld dat die voldoet aan de bij of krachtens de Wet op het hoger onderwijs en wetenschappelijk onderzoek vastgestelde voorschriften voor de toelating tot de desbetreffende opleiding of onderwijseenheid daarvan.

Artikel 4. Uitzondering screeningsplicht
1. In afwijking van artikel 3 is niet screeningsplichtig een persoon als bedoeld in dat

artikel die:
a. voor hetzelfde onderzoek, onderwijs of ondersteunende werkzaamheden ten behoeve van onderzoek of onderwijs aan een kennisinstelling een verklaring als bedoeld in artikel 1, eerste lid, onderdeel b, van de Wet veiligheidsonderzoeken nodig heeft; of
b. voor dezelfde sensitieve technologie al een screeningsbesluit heeft ontvangen dat een verklaring bevat dat uit het oogpunt van de naleving van de beperkingen, bedoeld in artikel 9, tweede lid, en van de nationale veiligheid geen bezwaar bestaat tegen de toegang van de betrokken persoon tot een onderdeel van een kennisinstelling waar de betrokken persoon toegang zou krijgen tot die sensitieve technologie.
2. Het eerste lid, onderdeel b, is niet van toepassing indien het screeningsbesluit ziet op het doen van een studie en de betrokken persoon voornemens is onderzoek te gaan doen, onderwijs te gaan verzorgen of ondersteunende werkzaamheden ten behoeve van onderzoek of onderwijs te gaan verrichten.

Artikel 5. Sensitieve technologie
1. Sensitieve technologie omvat de in bijlage 2 en krachtens artikel 6 aangewezen technologieën voor zover:
a. het onderzoek op het gebied van de desbetreffende technologie niet experimenteel of theoretisch onderzoek is, dat vooral als doel heeft om nieuwe kennis te verkrijgen over de fundamentele oorzaken van fenomenen of observeerbare feiten zonder dat daarbij een specifieke toepassing voorzien is; en
b. de technologie voldoet aan een of meer van de volgende kenmerken:
1º. de technologie wordt gekenmerkt door een breed toepassingsbereik binnen verschillende vitale processen of processen die raken aan de nationale veiligheid; of
2º. de technologie kan van essentieel belang zijn voor het functioneren van defensie, opsporings-, inlichtingen- of veiligheidsdiensten bij de uitoefening van hun taken.
2. Bij algemene maatregel van bestuur kan worden bepaald dat het eerste lid, onderdeel a, niet van toepassing is bij het vaststellen van de sensitiviteit van een in bijlage 2 of krachtens artikel 6 aangewezen technologie.
3. Indien ten aanzien van een in bijlage 2 of krachtens artikel 6 aangewezen technologie of gedeelte daarvan beperkingen zijn gesteld aan het aanbieden van kennis erover in een of meer verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme en deze beperkingen bij ministeriële regeling zijn aangewezen, wordt deze technologie of het desbetreffende gedeelte daarvan geacht sensitieve technologie te zijn.
4. Bij ministeriële regeling kunnen regels worden gesteld over de uitvoering van dit artikel.

Artikel 6. Toevoegen sensitieve technologie
1. In aanvulling op bijlage 2, kunnen bij algemene maatregel van bestuur technologieën of delen hiervan worden aangewezen.
2. Artikel 5, eerste, tweede en derde lid, zijn van overeenkomstige toepassing op het aanwijzen van technologieën, bedoeld in het eerste lid.
3. In afwijking van het eerste lid kunnen bij ministeriële regeling technologieën of delen hiervan worden aangewezen indien beperkingen zijn gesteld aan het aanbieden van kennis over de desbetreffende technologie of delen hiervan in een of meer verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme, en:
a. spoed dit vereist; en
b. het verdrag of het bindend besluit van de volkenrechtelijke organisatie ten aanzien van de technologie of delen hiervan beperkt ruimte laat voor beleidsinhoudelijke keuzes.

Artikel 7. Verplichting aanwijzing onderdelen kennisinstelling
1. De kennisinstelling onderzoekt bij welke onderdelen van de kennisinstelling screeningsplichtigen in aanraking kunnen komen met sensitieve technologie en wijst

deze onderdelen op grond van dit onderzoek aan. De aanwijzing als onderdeel van de kennisinstelling als bedoeld in de vorige volzin is slechts mogelijk indien de sensitieve technologie in het onderdeel uitsluitend toegankelijk is voor diegenen die vanwege onderzoek, het verzorgen van onderwijs, het verrichten van ondersteunende werkzaamheden ten behoeve van onderzoek of onderwijs, of vanwege studie betrokken zijn bij dat onderdeel van de kennisinstelling.
2. Het onderzoek, bedoeld in het eerste lid, is niet noodzakelijk voor de onderdelen van een kennisinstelling waar de screeningsplichtige evident niet in aanraking kan komen met in bijlage 2 en krachtens artikel 6 aangewezen technologieën.
3. De kennisinstelling meldt de uitkomsten van het onderzoek en de aangewezen onderdelen, bedoeld in het eerste lid, aan Onze Minister.
4. Onder onderdelen van de kennisinstelling wordt onder andere verstaan opleidingen en postinitiële masteropleidingen of onderwijseenheden daarvan als bedoeld in de Wet op het hoger onderwijs en wetenschappelijk onderzoek.
5. Indien de kennisinstelling van oordeel is dat een onderdeel van de kennisinstelling dat op grond van het derde lid is gemeld aan Onze Minister niet langer dient te zijn aangewezen, volgt de kennisinstelling de procedure beschreven in het eerste en derde lid.
6. Bij ministeriële regeling worden regels gesteld over de uitvoering van dit artikel.

Artikel 8. Verzoek nadere informatie
1. Onze Minister verstrekt op verzoek van de kennisinstelling informatie over de toepassing van artikelen 3 tot en met 7 in de praktijk.
2. De informatie, bedoeld in het eerste lid, wordt zo spoedig mogelijk verstrekt.

Hoofdstuk 3. De screening en screeningsprocedure

Artikel 9. De screening
1. De screening is een onderzoek naar de screeningsplichtige door Onze Minister dat plaatsvindt voorafgaand aan de toegang tot een onderdeel van een kennisinstelling als bedoeld in artikel 7 waarbij de screeningsplichtige toegang zou krijgen tot sensitieve technologie.
2. Bij de screening onderzoekt Onze Minister:
a. of toegang van de screeningsplichtige tot een onderdeel van een kennisinstelling als bedoeld in artikel 7 waarbij de screeningsplichtige toegang zou krijgen tot sensitieve technologie, kan leiden tot een risico op overtreding van een of meer bij ministeriële regeling aangewezen beperkingen aan het aanbieden van kennis over een sensitieve technologie, gesteld in een of meer bij ministeriële regeling aangewezen verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme; en
b. of toegang van de screeningsplichtige tot dat onderdeel van een kennisinstelling kan leiden tot een risico voor de nationale veiligheid.
3.Onze Minister gebruikt voor het onderzoek, bedoeld in het tweede lid, het afwegingskader van artikel 11.
4. De kennisinstelling geeft de screeningsplichtige slechts toegang tot het onderdeel van de kennisinstelling indien het screeningsbesluit een verklaring bevat dat uit het oogpunt van de naleving van de beperkingen, bedoeld in het tweede lid, en van de nationale veiligheid geen bezwaar bestaat tegen de toegang van de screeningsplichtige tot het onderdeel van de kennisinstelling.

Artikel 10. Aanvraag screeningsbesluit
1. De screeningsplichtige vraagt het screeningsbesluit aan bij Onze Minister.
2. De kennisinstelling is verplicht de screeningsplichtige te wijzen op de screeningsplicht.
3. Bij ministeriële regeling wordt bepaald welke gegevens de screeningsplichtige en de kennisinstelling moeten aanleveren bij de aanvraag van het screeningsbesluit.

Artikel 11. Afwegingskader screeningsbesluit
1. Bij het nemen van het screeningsbesluit houdt Onze Minister uitsluitend rekening met de volgende factoren:
a. of de screeningsplichtige onderworpen is aan bij ministeriële regeling aangewezen beperkende maatregelen krachtens:
1°. hoofdstuk 7 van het Handvest van de Verenigde Naties;
2°. artikel 215 van het Verdrag betreffende de werking van de Europese Unie; of
3°. de Sanctiewet 1977;
b. persoonlijke gedragingen en omstandigheden, naar aanleiding waarvan betwijfeld mag worden of de toegang van de screeningsplichtige tot sensitieve technologie niet een risico voor de naleving van de beperkingen, bedoeld in artikel 9, tweede lid, of voor de nationale veiligheid met zich mee kan brengen;
c. of de screeningsplichtige banden heeft met of onder invloed staat van een statelijke actor waarvan Onze Minister concrete aanwijzingen heeft dat deze sensitieve technologie van kennisinstellingen tracht te verwerven;
d. of de screeningsplichtige een strafbaar feit heeft begaan; en
e. of de screeningsplichtige niet of onvoldoende heeft meegewerkt aan het onderzoek naar de factoren onder a tot en met d.
2. Voor de beoordeling van de gegevens van de screeningsplichtige wordt een bij ministeriële regeling te bepalen terugkijktermijn in acht genomen waarbij voor verschillende gegevens een verschillende terugkijktermijn kan worden bepaald.

Artikel 12. Strafbare feiten
1. Onze Minister stelt bij ministeriële regeling de strafbare feiten vast die op grond van artikel 11, onderdeel d, van invloed kunnen zijn op de beoordeling van een risico voor de nationale veiligheid.
2. Met een strafbaar feit als bedoeld in het artikel 11, onderdeel d, wordt gelijkgesteld een strafbaar feit naar buitenlands recht, dat naar het oordeel van Onze Minister gelijksoortig is aan een bij de ministeriële regeling, bedoeld in het eerste lid, vastgesteld strafbaar feit naar Nederlands recht.

Artikel 13. Termijn screening
1. Indien een aanvraag voor een screeningsbesluit is ingediend, neemt Onze Minister zo spoedig mogelijk, doch uiterlijk binnen vier weken na ontvangst van de aanvraag, een screeningsbesluit.
2. Onze Minister kan de termijn voor het nemen van een screeningsbesluit als bedoeld in het eerste lid verlengen met een redelijke termijn, doch uiterlijk met vier weken.
3. Onverminderd de toepasselijkheid van artikel 4:15 van de Algemene wet bestuursrecht, wordt de termijn voor het nemen van een screeningsbesluit als bedoeld in het eerste lid, opgeschort met ingang van de dag waarop Onze Minister op grond van artikel 18, tweede lid, verzoekt om aanvullende informatie, tot de dag waarop de verzochte informatie is verstrekt.

Artikel 14. Resultaat screening
1. Op grond van de screening neemt Onze Minister een screeningsbesluit, indien van toepassing, in overeenstemming met Onze Minister of Ministers die het mede aangaat.
2. Het screeningsbesluit bevat een verklaring dat uit het oogpunt van de naleving van de beperkingen, bedoeld in artikel 9, tweede lid, en van de nationale veiligheid geen bezwaar, dan wel bezwaar, bestaat tegen de toegang van de screeningsplichtige tot een onderdeel van de kennisinstelling als bedoeld in artikel 7, waarbij de screeningsplichtige toegang zou krijgen tot sensitieve technologie.
3. Indien op grond van een verdrag of bindend besluit van een volkenrechtelijke organisatie als bedoeld in artikel 9, tweede lid, ontheffing of toestemming nodig is van de bevoegde autoriteit voor het verkrijgen van toegang tot de desbetreffende sensitieve technologie, bevat het screeningsbesluit tevens die ontheffing of toestemming of de weigering daarvan.

4. Onze Minister kan, indien nodig, andere Ministers dan bedoeld in het eerste lid raadplegen, alvorens een screeningsbesluit wordt genomen.

Hoofdstuk 4. Toezicht en handhaving

Artikel 15. Aanwijzing toezichthouder
Met het toezicht op de naleving van deze wet zijn belast de bij besluit van Onze Minister aangewezen ambtenaren.

Artikel 16. Handhavingsbevoegdheden
1. Onze Minister is bevoegd tot oplegging van een last onder dwangsom ter handhaving van de artikelen 7 en 10, tweede lid.
2. Onze Minister kan een bestuurlijke boete opleggen in geval van overtreding van artikel 7, 9, vierde lid, of artikel 10, tweede lid.
3. De bestuurlijke boete die op grond van het tweede lid kan worden opgelegd, bedraagt ten hoogste het bedrag dat is vastgesteld voor de zesde categorie, bedoeld in artikel 23, vierde lid, van het Wetboek van Strafrecht.

Hoofdstuk 5. Gegevensverwerking

Artikel 17. Gegevensverwerking
1. Onze Minister kan, voor zover dit noodzakelijk is voor de uitvoering van deze wet, gegevens, waaronder persoonsgegevens, verwerken:
a. ontvangen op grond van artikel 18;
b. verkregen krachtens de Wet justitiële en strafvorderlijke gegevens en de Wet op de inlichtingen- en veiligheidsdiensten 2017; en
c. afkomstig uit publiek toegankelijke informatiebronnen.
2. Onze Minister is verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens in het kader van deze wet.
3. Persoonsgegevens die op grond van het eerste lid zijn verwerkt, worden binnen twee jaar na opslaan vernietigd, met uitzondering van het screeningsbesluit dat een bezwaar bevat tegen de toegang van de screeningsplichtige tot een onderdeel van de kennisinstelling als bedoeld in artikel 7 waarbij de screeningsplichtige toegang zou krijgen tot sensitieve technologie, dat gedurende 15 jaar nadat het besluit onherroepelijk is geworden wordt bewaard.

Artikel 18. Gegevensverstrekkingen aan Onze Minister
1. Voor zover noodzakelijk voor de uitvoering van deze wet, verstrekken de volgende natuurlijke personen, rechtspersonen of bestuursorganen gegevens, waaronder persoonsgegevens, aan Onze Minister:
a. de kennisinstelling;
b. de screeningsplichtige;
c. de referenten van de screeningsplichtige;
d. Onze Minister van Asiel en Migratie, voor zover het gegevens betreft met betrekking tot het verblijfsrecht; en
e. Stichting Nuffic, voor zover het gegevens betreft met betrekking tot de erkenning en waardering van diploma's.
2. Voor zover de gegevens die de screeningsplichtige bij de aanvraag, bedoeld in artikel 10, eerste lid, heeft aangeleverd en de verzameling of verstrekking, bedoeld in het eerste lid, niet de benodigde gegevens hebben opgeleverd voor het nemen van een screeningsbesluit, verstrekt de screeningsplichtige desgevraagd alle informatie aan Onze Minister die noodzakelijk is voor de uitvoering van deze wet.

Artikel 19. Gegevensverstrekkingen door Onze Minister
1. Onze Minister verstrekt aan de screeningsplichtige het screeningsbesluit.
2. Onze Minister deelt aan de desbetreffende kennisinstelling mede dat een screeningsbesluit is genomen en welke verklaring als bedoeld in artikel 14, tweede lid,

deze bevat.
3. Onze Minister verstrekt desgevraagd of indien daartoe aanleiding is het screeningsbesluit aan Onze Minister van Buitenlandse Zaken voor zover dit noodzakelijk is voor de uitvoering van de Visumcode.
4. Onze Minister deelt gegevens die op grond van deze wet zijn verkregen met Onze Minister van Justitie en Veiligheid en, indien van toepassing, Onze Minister of Ministers die het mede aangaat als bedoeld in artikel 14, eerste lid, en andere ministers als bedoeld in artikel 14, vierde lid, voor zover dit noodzakelijk is voor de uitvoering van deze wet.
5. Onze Minister verstrekt diplomagegevens van de screeningsplichtige aan Nuffic voor zover dit noodzakelijk is voor de erkenning en waardering van diploma's tijdens de screening.

Artikel 20. Verwerking van bijzondere categorieën van persoonsgegevens
Gelet op artikel 9, tweede lid, onderdeel g, van de Algemene verordening gegevensbescherming, is het verbod om gegevens over politieke opvattingen, ras of etnische afkomst, het lidmaatschap van een vakbond, religieuze of levensbeschouwelijke overtuigingen, verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gezondheid of gegevens met betrekking tot iemand seksueel gedrag of seksuele gerichtheid te verwerken niet van toepassing indien de verwerking geschiedt door Onze Minister voor zover de verwerking noodzakelijk is voor de doelmatige en doeltreffende uitvoering van deze wet.

Artikel 21. Verwerking strafrechtelijke gegevens en burgerservicenummer
Persoonsgegevens van strafrechtelijke aard en het burgerservicenummer, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen burgerservicenummer kunnen worden verwerkt, voor zover deze gegevens noodzakelijk zijn voor de doelmatige en doeltreffende uitvoering van deze wet.

Hoofdstuk 6. Wijziging andere wetten

Artikel 22. Wijziging Algemene wet bestuursrecht
In artikel 2 van bijlage 2 bij de Algemene wet bestuursrecht wordt in de alfabetische volgorde ingevoegd:
Wet screening kennisveiligheid: artikel 14.

Artikel 23. Wijziging Wet justitiële en strafvorderlijke gegevens
Aan artikel 2a eerste lid, van de Wet justitiële en strafvorderlijke gegevens wordt, onder vervanging van de punt aan het slot van dat lid door een puntkomma, een onderdeel i toegevoegd, luidende:
i. de screening, bedoeld in artikel 9 van de Wet screening kennisveiligheid.

Artikel 24. Wijziging van de Wet op het hoger onderwijs en wetenschappelijk onderzoek
De Wet op het hoger onderwijs en wetenschappelijk onderzoek wordt als volgt gewijzigd:

A

In artikel 7.34, eerste lid, onderdeel a, wordt 'of 7.57h' vervangen door ', 7.57h of 7.58'.

B

Artikel 7.58 komt te luiden :

Artikel 7.58. Toegang tot sensitieve technologie

1. Indien een onderwijseenheid van een opleiding of postinitiële masteropleiding is aangewezen als onderdeel van een kennisinstelling als bedoeld in artikel 7 van de Wet screening kennisveiligheid, staat toegang tot deze onderwijseenheid van de opleiding of postinitiële masteropleiding slechts open voor een student die beschikt over een screeningsbesluit als bedoeld in artikel 14 van die wet die een verklaring bevat dat uit het oogpunt van de naleving van de beperkingen, bedoeld in artikel 9, tweede lid, van die wet en van de nationale veiligheid geen bezwaar bestaat tegen de toegang van de screeningsplichtige tot dat onderdeel van de kennisinstelling.
2. Indien een opleiding of postinitiële masteropleiding is aangewezen als onderdeel van een kennisinstelling als bedoeld in artikel 7 van de Wet screening kennisveiligheid, staat inschrijving tot deze opleiding of postinitiële masteropleiding slechts open voor een student die beschikt over een screeningsbesluit als bedoeld in artikel 14 van die wet die een verklaring bevat dat uit het oogpunt van de naleving van de beperkingen, bedoeld in artikel 9, tweede lid, van die wet en van de nationale veiligheid geen bezwaar bestaat tegen de toegang van de screeningsplichtige tot dat onderdeel van de kennisinstelling.

Artikel 25. Wijziging Wet subsidiëring landelijke onderwijsondersteunende activiteiten 2013
Aan artikel 3a, tweede lid, onder a, onder 2°, van de Wet subsidiëring landelijke onderwijsondersteunende activiteiten 2013 wordt toegevoegd 'en in het kader van de screening, bedoeld in artikel 1 van de Wet screening kennisveiligheid'.

Hoofdstuk 7. Overgangs- en slotbepalingen

Artikel 26. Overgangsbepaling zittende onderzoekers, studenten en technisch ondersteunende personeelsleden

Artikel 27. Openbare lichamen BES
Deze wet is mede van toepassing in de openbare lichamen Bonaire, Sint Eustatius en Saba.

Artikel 28. Evaluatiebepaling
Onze Minister zendt vijf jaar na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk.

Artikel 29. Inwerkingtreding
Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel 30. Citeertitel
Deze wet wordt aangehaald als: Wet screening kennisveiligheid.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Onderwijs, Cultuur en Wetenschap,

De Minister van Justitie en Veiligheid,

Bijlage 1, behorende bij artikel 1 van de Wet screening kennisveiligheid

De namen van de privaatrechtelijke rechtspersonen in deze bijlage worden weergegeven, zoals zij luiden op DDMMJJJJ.

Rechtspersonen:

- Stichting Deltares te Delft;
- De Koninklijke Nederlandse Akademie van Wetenschappen, bedoeld in artikel 1.16 van de Wet op het hoger onderwijs en wetenschappelijk onderzoek;
- Stichting Maritiem Research Instituut Nederland te Wageningen;
- Stichting Koninklijk Nederlands Lucht- en Ruimtevaartcentrum te Amsterdam;
- De Nederlandse organisatie voor wetenschappelijk onderzoek, bedoeld in artikel 2 van de Wet op de Nederlandse organisatie voor wetenschappelijk onderzoek;
- De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek, bedoeld in artikel 3 van de TNO-wet;
- Stichting Nederlandse Wetenschappelijk Onderzoek Instituten te Utrecht;
- Stichting Wageningen Research te Wageningen;
- Stichting Wetsus, European Centre of Excellence for Sustainable Water Technology te Leeuwarden.

Bijlage 2, behorende bij artikel 5, eerste lid, van de Wet screening kennisveiligheid

Technologie	**Voor zover het betreft:**
Advanced computing and systems	-High-performance computing (HPC) -Edge Computing
Artificiële Intelligentie	-Machine learning -Deep learning -General Purpose AI -Generatieve AI -Natural language processing -Reinforcement learning -Expert systems
Advanced Data Analytics	-Predictive analytics -Prescriptive analytics
Biotechnologie	-Genetische modificatie -Gene editing/genome engineering/precise genetic engineering -Gendruk (gene-drive) -Protein engineering -Synthetische biologie -Bioprinting -Bioprocessing technologies -Biofabrication -Biological weapons detection and characterization -Emerging pathogens detection and characterization
Chemische technologie	-Micro- en nanoreactoren
Communicatie en netwerktechnologie	-Radiofrequency (RF) en gemengde signaalcircuits, antennes, filters en componenten -High Power Microwave -Elektromagnetische Puls -Hoge-energie radiofrequentie (RF) -mobiele en draadloze netwerk technologieën -Satellietcommunicatie
Cyberveiligheidstechnologie	-Versleutelingstechnologieën/toegepaste cryptografie -Emission security/telecommunications electronics materials protected from emanating spurious transmissions (EMSEC/TEMPEST technology) -Geautomatiseerde cyberbeveiligingstechnologieën
Energie technologie	-Gasturbine technologie -Energieopslag -Waterstoftechnologie
Geavanceerde Materialen	-Energie materialen -Optische, elektronische, magnetische materialen en nanomechanische materialen, inclusief 2D en grafeen -Thin films en coatings

	-Bouw- en constructiematerialen (slimme materialen, metamaterialen, composieten en keramieken, High Entropy Alloys (HEA))
Halfgeleidertechnologieën	-Design and electronic design automation tools -Manufacturing process technologies and manufacturing equipment -Beyond complementary metal-oxide-semiconductor (CMOS) technology -Heterogeneous integration and advanced packaging -Specialized/tailored hardware components -Novel materials for advanced microelectronics -Wide-bandgap and ultra-wide-bandgap technologies for power management, distribution and transmission
Hypersonische technologie	-Hypersonische aandrijvingstechnologie (ramjet, scramjet) -Besturing en aerodynamica voor hypersonische systemen -Thermische bescherming/koeling voor hypersonische systemen -Counter-Hypersonic Technologies -Detection, tracking, guiding and characterization of hypersonic systems Divert and Attitude Control System (DACS), specialized counter-hypersonic warheads and seekers -Hypersonic intercept and Endgame technology
Kwantumtechnologie	-Kwantumcomputing -Kwantumcryptografie -Kwantumcommunicatie -Kwantumsensoren
Militair toepasbare technologie	-Wapentechnologieën -Technologie voor munitie en explosieven -Militaire platformtechnologieën
Nanotechnologie	-Micro- en nanovloeistofdynamica -Nanofabricage-technologie -Nanomaterialen -Functionele apparaten en structuren (op nanoschaal) -Nanobiotechnologie / bio-nanotechnologie
Nucleaire technologie	-Kernenergie-technologieën -Kernenergie- en aandrijvingstechnologieën -Kerntechnologieën voor andere doeleinden -Detectie- en karakteriseringstechnologieën voor kernmaterialen -Verrijkingstechnologie -Radiation implosion technologie

Optica en Fotonica	-Geïntegreerde fotonica -Geavanceerde beeldvormingstechnologieën -Fotonische detectie -Foton generatie technologieën -Hoge-vermogen lasers -Optische sensoren/fotonische sensoren -Adaptieve optica -Optomechatronica -Optische componenten
Positie-, Navigatie- en Tijdsbepaling (PNT) technologie	-Satellite Space based PNT systems -Ground air and sea based PNT systems -Hybride en autonome navigatiesystemen -Inertiële navigatiesystemen (INS) -Gravitatiekrachtdetectoren -Atomische klokken -Magnetische veldsensoren -Gelijktijdige lokalisatie en mapping (SLAM)
Robotica en autonome systemen	-Onbemande voertuigen (UxV's) -Autonome onbemande voertuigen -Op afstand bestuurde onbemande voertuigen -Robotzwermen -Human-machine teaming and interfaces -Brain-computer interfaces
Ruimtevaarttechnologie	-Launch vehicles -Ruimte-aandrijvingstechnologie -On-orbit servicing, assembly and manufacturing (On-orbit servicing, On-orbit assembly en On-orbit manufacturing) -Satellietbussen -Remote sensing instruments -Cryogene vloeistofbeheer -Entry, descent and landing -Kleine satellieten -Human spaceflight
Sensortechnologieën	-Sonar (sound navigation and ranging) -Radar -Akoestische sensoren -Sensor fusion and array technologies -Data fusion -Signature management and pattern recognition -Sensornetwerken en omgevingstechnologieën -Lidar -Infrarood en ultraviolet sensoren (IR- and UV-sensoren)
Simulatie technologie	-Digital twinning technologies -Extended Reality (XR) -Virtual Reality (VR) -Augmented Reality (AR) -Mixed Reality (MR)

Memorie van toelichting

I. **Algemeen deel**

Inhoudsopgave

Hoofdstuk 1. Inleiding

Deze toelichting wordt gegeven mede namens de Minister van Justitie en Veiligheid en in overeenstemming met de Minister van Economische Zaken.

Nederlandse kennisinstellingen nemen internationaal een sterke positie in als het gaat om de ontwikkeling en toepassing van hoogwaardige kennis en technologie. Nederland scoort al jaren goed op verschillende internationale ranglijsten, zoals de European Innovation Scoreboard[1] en de Global Innovation Index[2]. Binnen de EU doet Nederland mee in de top als het gaat om de ontwikkeling van sleuteltechnologieën, bijvoorbeeld op het gebied van biotechnologie en kwantumtechnologie.[3]

De vooraanstaande positie en goede academische reputatie van Nederlandse kennisinstellingen hangen samen met de academische vrijheid die in ons land gegarandeerd wordt en de openheid van onze kennisinstellingen naar de wereld.[4] Tegelijkertijd wordt duidelijk dat Nederland en de EU steeds vaker geconfronteerd worden met handelingen van statelijke actoren, gericht op het verkrijgen van hoogwaardige kennis en technologie, die onze nationale veiligheid en Europese fundamentele waarden kunnen schaden.[5] Ook kennisinstellingen zijn hiervan het doelwit. Uit dreigingsanalyses[6] blijkt dat via individuele onderzoekers en studenten ongewenste overdracht van kennis en technologie aan statelijke actoren kan plaatsvinden.[7] Onderzoekers en studenten kunnen gericht gestuurd worden door statelijke actoren of juist naderhand onder druk worden gezet om informatie over te brengen. Medewerking is in sommige gevallen (wettelijk) verplicht voor de student of onderzoeker.

In navolging van landen als Frankrijk, het Verenigd Koninkrijk en Australië voert Nederland nu ook een vorm van screening in. Met dit wetsvoorstel wordt beoogd de weerbaarheid van de Nederlandse kennissector te vergroten, om zo de sterke kennispositie van Nederland te behouden en fundamentele academische kernwaarden zoals de academische vrijheid, internationale samenwerking en open wetenschap te beschermen en de nationale veiligheid te waarborgen. Dit doet de regering door, daar waar de risico's voor de nationale veiligheid het grootst zijn, een preventieve screening te introduceren voor individuele onderzoekers en studenten die aan Nederlandse kennisinstellingen toegang kunnen krijgen tot sensitieve technologie. Het doel is hierbij nadrukkelijk om risico's voor de nationale veiligheid die kunnen optreden bij ongewenste kennis- en technologieoverdracht te voorkomen of mitigeren, maar niet om alle risico's uit te sluiten. Het geheel voorkomen van ongewenste kennisoverdracht is niet mogelijk. Bij het wetsvoorstel wordt ook het uitgangspunt gehanteerd dat open

[1] European Commission: Directorate-General for Research and Innovation, *European Innovation Scoreboard 2024*, Publications Office of the European Union, 2024.
[2] World Intellectual Property Organization (WIPO) Global Innovation Index 2024*: Unlocking the Promise of Social Entrepreneurship*.
[3] Sleuteltechnologieën zijn technologiegebieden waar Nederland een sterke wetenschappelijke positie op inneemt en waarin de komende jaren grote maatschappelijke en economische impact wordt verwacht. Deze technologieën kenmerken zich door een brede toepasbaarheid of bereik in innovaties en sectoren en maken de ontwikkeling van innovaties op de middellange termijn mogelijk. Ze zijn essentieel om maatschappelijke uitdagingen aan te gaan, de nationale veiligheid te versterken en een grote bijdrage te leveren aan de economie, mede door het ontstaan van nieuwe bedrijvigheid en markten.
[4] Kamerstukken II 2020/21, 31288, nr. 894.
[5] Kamerstukken II 2022/23, 36200, nr. 213 en Kamerstukken II 2022/23, 30821, nr. 175.
[6] Aanpak statelijke dreigingen en aanbieding DBSA 2, 28 november 2022. Kamerstukken II 2022/23, 30821, nr. 175 en bijlage.
[7] Waar in deze toelichting wordt gesproken over 'onderzoekers' wordt tevens bedoeld het ondersteunend personeel dat werkzaamheden van technische aard verricht. Dit wordt toegelicht in paragraaf 3.1.

wetenschapsbeoefening en internationale samenwerking slechts ingeperkt worden indien sprake is van (potentiële) risico's voor de nationale veiligheid.

Met onderhavig voorstel willen we die openheid en de mogelijkheden voor internationale samenwerking behouden. We willen de wetenschap niet op slot zetten, maar weerbaar maken met een balans tussen kansen en risico's en tussen het behoud van de open wetenschap en het beschermen van de nationale veiligheid. Hierbij geldt: open waar mogelijk, beschermen waar nodig. De reikwijdte van de screeningsplicht wordt zo risicogericht en precies als mogelijk bepaald, samen met de kennissector. Daarom worden hoog-risico onderdelen binnen sensitieve technologiegebieden aangewezen waar de screeningplicht gaat gelden.[8] Bij dit proces krijgen de kennisinstellingen een centrale rol en verantwoordelijkheid. Zij hebben immers zelf het beste zicht op de onderdelen van de instelling waar sensitieve kennis of technologie aanwezig is.[9] Op die hoog-risico onderdelen is de screeningsplicht van toepassing. Aan de hand van een lijst sensitieve (sub)technologieën en een door het Rijk ontwikkeld beoordelingskader gaan de kennisinstellingen zelf aanwijzen waar die hoog-risico onderdelen zich binnen de instelling bevinden. Bij de uitwerking van dat beoordelingskader wordt de kennissector betrokken.

Om dit mogelijk te maken en om de reikwijdte van de screeningsplicht te bepalen, wordt in dit wetsvoorstel een lijst met sensitieve (sub)technologieën opgenomen. Bij de totstandkoming van de lijst met sensitieve (sub)technologieën is ook de kennissector geconsulteerd. Indien op grond van de screening wordt geconstateerd dat toegang van een screeningsplichtige tot sensitieve kennis of technologie kan leiden tot risico's voor de nationale veiligheid, is het de kennisinstelling niet toegestaan om een screeningsplichtige onderzoeker of student toegang te geven tot het betreffende onderdeel.

Voorts regelt dit voorstel ook dat er op de naleving van het wetsvoorstel toezicht komt en handhaving mogelijk wordt. De toelichting gaat ook in op de uitvoerbaarheid, het beperken van de administratieve lasten, het voorkomen van stigmatisering en discriminatie en de kosten die met dit voorstel gemoeid zijn.[10]

Tot slot is het zo dat kennis- en technologieoverdracht naar bepaalde landen al verboden is op grond van beperkende maatregelen (oftewel 'sancties') van de EU. Die maatregelen worden vastgelegd in besluiten van de Raad en EU-verordeningen, overeenkomstig de doelstellingen van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB). Voor wat betreft het verbod op kennisoverdracht, wordt ook gesproken over het zogeheten verbod op het verlenen van technische bijstand. Dit omvat ook het aanbieden van kennis via hoger onderwijs en onderzoek.[11] Tijdens de screening zal ook worden getoetst aan de verboden waaraan reeds wordt getoetst middels het verscherpt toezicht.[12]

[8] Onderdelen kunnen (delen van) opleidingen en postinitiële masteropleidingen, projecten, programmalijnen, vakgroepen, onderzoeksgroepen, studentenprojecten of bepaalde (studenten)teams en laboratoria zijn. Deze opsomming is niet limitatief.
[9] In paragraaf 4.4 tot en met 4.4.7 van dit voorstel wordt deze systematiek toegelicht.
[10] In paragraaf 6, 8 en 9 van dit voorstel wordt hier nader op ingegaan.
[11] Commission opinion of 5.8.2019 on a request for interpretation concerning the provision of higher education and the undertaking of applied research in the framework of a prohibition to provide technology or technical assistance to a third country (C(2019) 5883 final). C(2019) 5883 final.
[12] Het verscherpt toezicht houdt in de praktijk in, dat het OCW-Loket Kennisembargo en de Taskforce Ongewenste Kennisoverdracht (OCW) belast zijn met de toetsing van onderzoekers en studenten die willen werken of studeren in een van de richtingen op de lijst van aangewezen vakgebieden. Het is verboden om zonder ontheffing aan een opleiding of onderzoek te beginnen of te werken binnen deze (vak)gebieden.

Hoofdstuk 2. Hoofdlijnen van het voorstel

Dit hoofdstuk beschrijft allereerst de achtergrond waartegen dit wetsvoorstel is ontstaan en een aantal daarmee samenhangende beleidsontwikkelingen uit de afgelopen jaren. Daarna wordt een probleembeschrijving gegeven. Vervolgens wordt ingegaan op de doelstelling van dit wetsvoorstel, waarna wordt ingegaan op de motivering van de instrumentkeuze en hoe dit wetsvoorstel zich verhoudt tot het brede beleid gericht op kennisveiligheid. Tot slot wordt ingegaan op de onderzochte alternatieven.

2.1 Aanleiding

Nederlandse kennisinstellingen beschikken over hoogwaardige kennis en technologie en Nederland behoort tot de top in de ontwikkeling en toepassing daarvan. Dit maakt Nederlandse kennisinstellingen een aantrekkelijk doelwit voor statelijke actoren die hoogwaardige kennis en technologie willen bemachtigen. Uit de dreigingsbeelden is gebleken dat onder meer Nederlandse kennisinstellingen en wetenschappers op grote schaal doelwit zijn van statelijke actoren die proberen hoogwaardige kennis en technologie te verwerven op Nederlandse kennisinstellingen.[13] Dit brengt onder meer het risico van ongewenst eindgebruik voor bijvoorbeeld militaire doeleinden met zich mee, zoals toepassingen voor surveillance, *human enhancement*[14], versterking van het militaire apparaat of de verbetering van digitale aanvallen.

Geopolitieke ontwikkelingen van de afgelopen jaren laten ook zien dat kennis en technologie door statelijke actoren worden ingezet om de eigen militaire, technologische, politieke en economische macht te vergroten. Kennis en technologie zijn daarmee ook in toenemende mate een strategisch machtsmiddel geworden. Ook zijn landen in toenemende mate bereid om risicovolle strategische afhankelijkheden in te zetten als geopolitiek wapen.[15] Deze ontwikkelingen hebben grote gevolgen voor de weerbaarheid van Nederland en de EU. De risico's voor de nationale veiligheid die kunnen voortvloeien uit risicovolle strategische afhankelijkheden kunnen namelijk verstrekkende gevolgen hebben voor onze nationale veiligheid, maatschappij en economie, bijvoorbeeld wanneer we voor technologie, producten of diensten afhankelijk zijn van een klein aantal andere landen.

In het licht van deze geopolitieke ontwikkelingen kondigde de regering op 27 november 2020 in de brief 'Kennisveiligheid hoger onderwijs en wetenschap'[16] een pakket van maatregelen aan dat een handelingsperspectief biedt aan zowel de kennisinstellingen als de rijksoverheid. Daarin is ingezet op zowel bewustwording en zelfregulering binnen het kennisveld(de kennisveiligheidsdialoog, richtsnoeren kennisveiligheid[17], de bestuurlijke afspraken en het Loket Kennisveiligheid), als om een bindend toetsingskader voor ongewenste kennis- en technologieoverdracht. In de voortgangsbrief kennisveiligheid hoger onderwijs en wetenschap van 23 december 2022[18] is dit nader uitgewerkt. Met de brief van 5 april 2023[19] is aangekondigd dat niet meer wordt gesproken van een toetsingskader ongewenste kennis- en technologieoverdracht, maar van een wetsvoorstel screening kennisveiligheid.

---

[13] Aanpak statelijke dreigingen en aanbieding DBSA 2, 28 november 2022. Kamerstukken II 2022/23, 30821, nr. 175 en bijlage.
[14] 'Human enhancement' betreft (biomedische) technologieën die als doel hebben de lichamelijke of geestelijke capaciteiten van de mens te vergroten.
[15] Dreigingsbeeld Statelijke Actoren 2 en Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport. Kamerstukken 2022/23, 30821, nr. 175, bijlage respectievelijk Kamerstukken 2023/24, 30821, nr. 231.
[16] Kamerstukken II 2020/21, 31288, nr. 894.
[17] De richtsnoeren kennisveiligheid staan nu bekend als de Nationale Leidraad Kennisveiligheid (2022).
[18] Kamerstukken II 2022/23, 31288, nr. 1003.
[19] Kamerstukken II 2022/23, 36200, nr. 213.

Op grond van de EU-verordeningen en besluiten in het kader van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB) is het overdragen van bepaalde kennis of technologieën door kennisinstellingen naar enkele gesanctioneerde landen al verboden. Met het zogenoemde verscherpt toezicht zet de regering al enkele jaren in op het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht naar Noord-Korea, Iran en Rusland[20] op bepaalde kennisgebieden.[21] In 2020 kondigt de regering aan dat het verscherpt toezicht op termijn wordt geïntegreerd in het toetsingskader ongewenste kennis- en technologieoverdracht, nu bekend als de screening kennisveiligheid.[22] Het verscherpt toezicht zal hiermee ophouden te bestaan als zelfstandig instrument.

Verder verscheen in januari 2021 het Dreigingsbeeld Statelijke Actoren (DBSA 1) opgesteld door Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). In november 2022 werd een nieuwe versie uitgebracht, het DBSA 2 (hierna: de dreigingsbeelden[23]). Een dreigingsbeeld heeft tot doel het bewustzijn te vergroten over de aard en omvang van de dreiging vanuit statelijke actoren en biedt inzicht in de nationale veiligheidsbelangen die geschaad (kunnen) worden door statelijke actoren en op welke wijze dat gebeurt of kan gebeuren.

Uit de dreigingsbeelden volgt dat Nederlandse kennisinstellingen doelwit zijn van statelijke actoren die proberen hoogwaardige kennis en technologie te bemachtigen om de eigen militaire, technologische, politieke en economische macht te vergroten, of om kennis en technologie te verwerven die ingezet kan worden voor de versterking van het eigen militaire apparaat. Dit maakt dat kennisveiligheid onlosmakelijk verbonden is met de nationale veiligheid. Versterking van de brede aanpak kennisveiligheid en de introductie van een screening van onderzoekers en studenten zijn om die reden ook opgenomen in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden[24] en de aanpak tegen statelijke dreigingen.[25]

2.2. Probleembeschrijving

Modus operandi statelijke actoren
Uit de dreigingsbeelden blijkt dat statelijke actoren op grote schaal activiteiten ondernemen om hoogwaardige kennis en technologie te verwerven op Nederlandse kennisinstellingen. Ongewenste kennis- en technologieoverdracht kan plaatsvinden via personen, maar kan ook ontstaan zonder tussenkomst van personen. Bijvoorbeeld wanneer statelijke actoren via academische samenwerkingsverbanden tussen Nederlandse kennisinstellingen en buitenlandse kennisinstellingen bepaalde kennis of technologie proberen te verwerven.

Ongewenste kennis- en technologieoverdracht via personen wordt ook wel de 'insider threat' genoemd. Deze 'insider threat' betreft de dreiging die uitgaat van onderzoekers of andere medewerkers en studenten die studeren of werken, of hebben gestudeerd of gewerkt, binnen Nederlandse kennisinstellingen. Statelijke actoren maken gebruik van de 'insider threat' middels verschillende methoden. Zo zetten zij heimelijke middelen in, zoals digitale en fysieke spionage. Ook gebruiken statelijke actoren legitieme activiteiten

[20] Kamerstukken 30821, nr. 70.
[21] Voor welke technische studies heb ik een ontheffing van het kennisembargo nodig en hoe vraag ik deze aan? | Rijksoverheid.nl
[22] Kamerstukken 31288, nr. 894.
[23] Waar in wordt gesproken over het dreigingsbeelden wordt bedoeld: het Dreigingsbeeld Statelijke Actoren (DBSA 1, opgesteld door Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) uit februari 2021, alsmede de nieuwe versie, het DBSA 2 uit november 2022.
[24] Kamerstuk II 2022/23, 30821, nr. 178, bijlage. Veiligheidsstrategie voor het Koninkrijk der Nederlanden | Rijksoverheid.nl
[25] Kamerstukken II 2022/23, 30821, nr. 175.

zoals internationale uitwisselingen van onderzoekers en studenten, waarbij zij wel heimelijke intenties hebben. Soms gaat het om legitieme academische samenwerking zonder enige heimelijke intentie van degene die naar Nederland komt, maar wiens opgedane kennis en informatie op een later moment door een statelijke actor verworven wordt om voor ongewenste doeleinden in te zetten. Deze verschillende methoden worden zowel afzonderlijk als in combinatie ingezet. Dit verhoogt de kans van slagen om bepaalde hoogwaardige kennis of technologie succesvol te bemachtigen of te reproduceren.

Het onderscheid tussen wanneer statelijke actoren heimelijke intenties hebben en wanneer niet, is in de praktijk niet altijd eenvoudig te maken. Individuele onderzoekers en studenten kunnen gericht gestuurd worden door statelijke actoren of juist naderhand onder druk gezet om informatie over te dragen. De statelijke actor kan bijvoorbeeld in ruil voor de financiering van een buitenlandse stageplaats, opleidingsplaats of (tijdelijke) baan een tegenprestatie verlangen in de vorm van het (verplicht) delen van onderzoeksbevindingen of andere terugkeerverplichtingen. Medewerking met de statelijke actor kan ook (wettelijk) verplicht zijn voor de student of onderzoeker. Onderzoekers en studenten maken daarbij ook niet altijd kenbaar dat zij nog nevenactiviteiten of verplichtingen naar andere kennisinstellingen of statelijke actoren hebben.

Ook is bekend dat sommige statelijke actoren (ex-)landgenoten die inmiddels verblijven in Nederland en werken of studeren aan een Nederlandse kennisinstelling gebruiken of misbruiken voor de overdracht van kennis. In die gevallen wordt druk uitgeoefend op de student of onderzoeker in kwestie met als doel het overdragen van bepaalde kennis. Het komt ook voor dat naasten, zoals familie, vrienden en collega's, onder druk worden gezet. Statelijke actoren zetten ook actief in op rekrutering van onderzoekers en studenten en gebruiken hiervoor verschillende methoden, zoals *social engineering*, omkoping, chantage en intimidatie. Inlichtingenofficieren onderhouden soms heimelijke contacten met onderzoekers binnen Nederlandse kennisinstellingen en worden ook geregeld aangetroffen op conferenties. Ook vinden er online benaderingen plaats via sociale media om bronnen te vinden en te rekruteren. Hierbij werkt de onderzoeker of student niet altijd mee uit vrije wil en is het niet altijd duidelijk dat zij te maken hebben met een partij die banden heeft met een statelijke actor. Bepaalde vormen van rekrutering zoals *social engineering*, waarbij door psychologische manipulatie mensen worden bewogen om bepaalde acties uit te voeren of vertrouwelijke informatie openbaar te maken, vinden zeer geleidelijk en over een langere periode plaats. Het doelwit wordt langzaam 'binnengehaald' tot een moment dat er geen weg meer terug is.

Ook samenwerkingen die in beginsel legitiem zijn, kunnen leiden tot ongewenste kennis- en technologieoverdracht, zonder tussenkomst van personen. Bijvoorbeeld wanneer statelijke actoren via academische samenwerkingsverbanden tussen Nederlandse kennisinstellingen en buitenlandse kennisinstellingen bepaalde kennis of technologie proberen te verwerven. Kennis en technologie kunnen in deze gevallen ongewenst wegvloeien indien afgesproken kaders onvoldoende helder zijn of wanneer er diefstal van onderzoeksbevindingen plaatsvindt.

Dit voorstel is gericht op het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht via personen. Voor het tegengaan van ongewenste kennis- en technologieoverdracht door statelijke actoren waarbij gebruikt wordt gemaakt van andere verwervingsmethoden zijn er vanuit de rijksoverheid andere instrumenten voorhanden. In paragraaf 2.5. wordt hier nader op ingegaan.

Wanneer is kennis- en technologieoverdracht ongewenst?
In dit wetsvoorstel wordt steeds gesproken over ongewenste kennis- en technologieoverdracht. Echter, lang niet alle kennis- en technologieoverdracht is ongewenst. Sterker nog, de wetenschap is bij uitstek een wereld die open, internationaal

en toegankelijk is. Publicaties, studieloopbanen en werkzaamheden van wetenschappers zijn online vindbaar en verifieerbaar. Het delen van kennis staat centraal in de wetenschap en is een belangrijke voorwaarde voor wetenschappelijke vooruitgang. Veel kennis wordt openbaar gepubliceerd en slechts een beperkt deel van het wetenschappelijk onderzoek dat op kennisinstellingen plaatsvindt heeft mogelijke toepassingen die risico's kunnen hebben voor de nationale veiligheid.

Kennis- en technologieoverdracht wordt ongewenst als het gaat over de manieren waarop kennis wordt verworven, over het doel waarvoor kennis verworven wordt en over de risico's voor de nationale veiligheid die dat met zich mee kan brengen. Het is ongewenst wanneer statelijke actoren onderzoekers en studenten in Nederland onder druk zetten en daarmee handelen op manieren die in strijd zijn met onze normen en fundamentele academische kernwaarden. Het is ook ongewenst wanneer statelijke actoren deze verworven kennis en technologie inzetten op een manier die onze nationale veiligheid kan raken.

Het gaat voornamelijk om overdracht van kennis of technologie tijdens het onderzoeksproces, nog voordat het openlijk gepubliceerd is. Juist wanneer een onderzoek nog loopt is het onwenselijk dat statelijke actoren de kennis en technologie verwerven, omdat zij daarmee op een voorsprong kunnen raken die risico's voor de nationale veiligheid met zich mee kunnen brengen. Sensitieve kennis en technologie kan ook nog ongewenst over worden gedragen na het onderzoeksproces en publicatie. In geval van sensitieve kennis en technologie worden immers niet altijd alle onderzoeksresultaten of data gepubliceerd.

Tot slot is kennis- en technologieoverdracht in enkele gevallen al verboden en daarom ongewenst. Op grond van internationale sancties[26] mag geen gespecialiseerde kennis worden overgedragen aan bepaalde landen, bijvoorbeeld als dit gebruikt kan worden voor proliferatiegevoelige activiteiten. In de screening kennisveiligheid wordt ook getoetst aan een deel van deze verboden die volgen uit internationale sancties. Dit wordt nader uitgewerkt in paragraaf 4.4.

Ongewenste kennis- en technologieoverdracht in relatie tot nationale veiligheid
Bij ongewenste kennis- en technologieoverdracht gaat het met name om twee categorieën die risico's voor de nationale veiligheid kunnen opleveren: ongewenst eindgebruik van sensitieve kennis en technologie en het ontstaan van risicovolle strategische afhankelijkheden.

De overdracht van sensitieve kennis of technologie kan leiden tot ongewenst eindgebruik door een statelijke actor, door bijvoorbeeld de inzet van of dreiging met een massavernietigingswapen, in militaire toepassingen, in toepassingen voor surveillance of *human enhancement*, of de verbetering van digitale aanvallen of de verstoring van vitale processen.[27]

Daarnaast kan ongewenste kennis- en technologieoverdracht leiden tot het ontstaan van risicovolle strategische afhankelijkheden. Statelijke actoren ondernemen in toenemende mate activiteiten om hoogwaardige kennis en technologie te verwerven om zo de eigen militaire, technologische, politieke en economische macht te vergroten. Bepaalde kennis en technologie worden daarmee ook in toenemende mate een strategisch machtsmiddel. Dit kan risico's voor de nationale veiligheid met zich meebrengen. Staten die beschikken over hoogwaardige kennis en technologie zullen in de toekomst bepalend worden in de

[26] De Verenigde Naties (VN) en de EU kunnen beperkende maatregelen ('sancties') opleggen. Indien in een resolutie van de VN-veiligheidsraad sancties zijn aangenomen, worden die sancties door de EU geïmplementeerd. De EU kan echter ook autonoom sancties instellen, overeenkomstig de doelstellingen van het Gemeenschappelijk Buitenlands en Veiligheid Beleid.
[27] Dreigingsbeeld Statelijke Actoren 2, november 2022 en Trendanalyse Nationale Veiligheid 2024, juni 2024. Zie voor het overzicht van vitale processen: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

geopolitieke machtsverhoudingen. Hoewel internationale samenwerking juist gebaat is bij wederzijdse afhankelijkheden laten geopolitieke ontwikkelingen van de afgelopen jaren zien dat aan afhankelijkheden ook steeds meer risico's kleven.

In het kader van dit wetsvoorstel zijn voornamelijk strategische afhankelijkheden op het terrein van de kennis- en innovatiepositie van Nederland relevant. Een afhankelijkheid is strategisch wanneer een product, dienst of technologie cruciaal is voor het borgen van publieke belangen van Nederland en/of de EU, of de afhankelijkheid een risico vormt voor de continuïteit van vitale processen of de toegang tot gevoelige informatie voor derden. Bij een hoog risico van leveringsonderbrekingen, waarbij onder andere wordt gekeken naar de aard van de betrekkingen met het land, spreken we van een risicovolle strategische afhankelijkheid.

Risicovolle strategische afhankelijkheden kunnen risico's voor de nationale veiligheid met zich mee brengen zoals bedoeld in dit wetsvoorstel, bijvoorbeeld daar waar de ontstane afhankelijkheden raken aan vitale processen en sensitieve technologie en wanneer Nederland en de EU voor kritieke grondstoffen, hoogwaardige technologie, producten of diensten afhankelijk zijn van andere landen. Risico's voor de nationale veiligheid kunnen tevens ontstaan wanneer statelijke actoren invloed uitoefenen op Nederlandse publieke belangen door middel van het misbruiken van risicovolle strategische afhankelijkheden. Daarnaast kunnen risicovolle strategische afhankelijkheden Nederland op termijn mogelijk nog kwetsbaarder maken voor (digitale) spionage en mogelijk ook sabotage.

Met het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht kunnen risicovolle strategische afhankelijkheden of de risico's daarvan op de lange termijn worden verminderd of voorkomen. Door de eigen kennispositie te beschermen en versterken, ontnemen we statelijke actoren zoveel mogelijk de kans om Nederland of de EU onder druk te zetten en beschermen we de nationale veiligheid. De ontwikkeling van hoogwaardige kennis en technologie op Nederlandse kennisinstellingen speelt hierin een belangrijke rol. Het behouden of opbouwen van een voorsprong op het gebied van sensitieve kennis en technologie is van strategisch belang voor Nederland.
Een voorbeeld van een technologie waarvan de verwerving door een statelijke actor kan leiden tot risico's voor de nationale veiligheid is halfgeleidertechnologie. Halfgeleidertechnologie is onder meer belangrijk voor de ontwikkeling van microchips, en de bouw van machines om microchips te maken. Nederland is een belangrijke en strategische speler in de mondiale halfgeleiderwaardeketen. Nederlandse kennisinstellingen nemen daarbij een internationaal sterke positie in voor wat betreft de ontwikkeling van deze technologieën.

Omdat halfgeleidertechnologie de drijvende kracht is achter alle elektronisch aangestuurde apparaten en machines, zijn ook veel vitale processen afhankelijk van apparatuur en systemen waarin halfgeleidertechnologie is verwerkt. Daarnaast kent halfgeleidertechnologie zeer hoogwaardige toepassingen op het gebied van defensie, bijvoorbeeld in wapensystemen. Deze toepassingen maken dat halfgeleidertechnologie risico's voor de nationale veiligheid met zich mee kan brengen. Vanwege het strategische belang voor Nederland en de EU kan halfgeleidertechnologie in de context van geopolitieke rivaliteit ook ingezet worden als strategisch machtsmiddel. Daarom vormt een verlies in de kennispositie op dit technologiegebied een risico voor de nationale veiligheid.

2.3 Doelstellingen van de screening kennisveiligheid

In deze paragraaf worden de doelstellingen van dit wetsvoorstel beschreven. Hierbij wordt onder meer ingegaan op hoe de screening zich verhoudt tot het begrip nationale veiligheid, sanctiewet- en regelgeving en de academische kernwaarden academische vrijheid en open science.

2.3.1. 'Open waar mogelijk, beschermen waar nodig'

Door het introduceren van een screening borgen we de sterke kennispositie van Nederland en beschermen we de fundamentele academische kernwaarden die daarmee samenhangen: de academische vrijheid, internationale samenwerking en open wetenschap. Met dit voorstel wordt beoogd de openheid en de mogelijkheden voor internationale samenwerking te behouden. De wetenschap mag niet op slot worden gezet, maar moet wel weerbaarder worden gemaakt. Hierin wordt een balans gevonden tussen kansen en risico's en tussen het behoud van de open wetenschap en het beschermen van de nationale veiligheid.

In het licht van het voornoemde wordt met dit voorstel derhalve ook beoogd een bijdrage te leveren aan de bescherming van de nationale veiligheid. Dit voorstel draagt eraan bij dat onderzoekers en studenten vrij en veilig onderzoek kunnen doen en dat veilige internationale samenwerking mogelijk blijft. Dat doen we door de risico's voor de nationale veiligheid, die kunnen ontstaan door ongewenste kennis- en technologieoverdracht via Nederlandse kennisinstellingen aan statelijke actoren, te voorkomen of te mitigeren middels een screening. De screening maakt mogelijk dat in concrete gevallen risico's worden geconstateerd, en zorgt ook voor meer bewustwording binnen een kennisinstelling. In paragraaf 2.4.1. wordt hier nader op ingegaan.

Om de vooraanstaande positie van Nederland te kunnen behouden moet naast het voorkomen of mitigeren van risico's, nadrukkelijk worden ingezet op de ontwikkeling van hoogwaardige technologieën door internationale samenwerking te blijven zoeken. De ontwikkeling van hoogwaardige technologie op Nederlandse kennisinstellingen is namelijk cruciaal voor het oplossen van maatschappelijke uitdagingen, belangrijk voor het beschermen van de nationale veiligheid, en zorgt ervoor dat Nederland een koppositie kan behouden of verkrijgen in bepaalde sectoren. Dit wetsvoorstel richt zich daarom ook alleen op de grootste risico's voor de nationale veiligheid: alleen daar is een screening aan de orde en bescherming noodzakelijk.

De screeningsplicht geldt alleen indien de onderzoeker of student toegang kan krijgen tot sensitieve kennis of technologie binnen een hoog-risico onderdeel van een kennisinstelling. In paragraaf 4.4. wordt hier nader op ingegaan. Met de scherpe afbakening van de sensitieve technologieën en de aanwijzing van hoog-risico onderdelen van de kennisinstelling wordt beoogd deze risico's zo gericht mogelijk af te bakenen. Door alleen te richten op de grootste risico's voor de nationale veiligheid, kan de rest van de wetenschap zo open mogelijk blijven. Zo wordt een balans tussen kansen en risico's gevonden, waarbij geldt: 'open waar mogelijk, beschermen waar nodig'.

Opmerking verdient hierbij dat met de screening risico's worden gemitigeerd en niet volledig worden uitgesloten. Het totaal voorkomen van ongewenste kennis- en technologieoverdracht is niet mogelijk en ook niet het doel van de screening. Een screening betreft altijd een momentopname, gebaseerd op relevante informatie die op dat moment bekend is. Het is nadrukkelijk een preventief instrument. De invoering van een screening zal ook niet betekenen dat er geen sensitief onderzoek meer kan plaatsvinden, of dat onderzoekers of studenten op voorhand niet meer mogen deelnemen daaraan. De screening zal wel betekenen dat voor sommige onderzoekers en studenten extra voorwaarden worden gesteld voordat zij toegang kunnen krijgen tot sensitieve kennis of technologie. Slechts in gevallen waar (potentiële) risico's voor de nationale veiligheid worden geconstateerd kan besloten worden dat een onderzoeker of student geen toegang kan krijgen tot sensitieve kennis of technologie.

Screening betreft ook het sluitstuk van het bredere beleid op kennisveiligheid. Om de effecten van de screening te vergroten is het van belang dat screening in samenhang met de andere kennisveiligheidsinstrumenten wordt ingezet. In paragraaf 2.4.1. wordt hier nader op ingegaan.

Wanneer is screening aan de orde?
De screening kennisveiligheid is enkel aan de orde daar waar de risico's voor de nationale veiligheid het grootst zijn. Daarom moet met dit voorstel ook worden bepaald wanneer deze risico's zo groot zijn dat de inzet van dit instrument gerechtvaardigd is.

De vraag wanneer in geval van overdracht van hoogwaardige kennis en technologie risico's kunnen ontstaan voor de nationale veiligheid, wanneer deze risico's acceptabel zijn en wanneer niet, is sterk gerelateerd aan welke technologieën met dit wetsvoorstel als sensitief worden aangemerkt. Dit komt omdat een technologie alleen als sensitief wordt aangemerkt als de verwerving hiervan risico's voor de nationale veiligheid kunnen opleveren.

Zoals eerder in de toelichting is benoemd, gaat het bij ongewenste kennis- en technologieoverdracht om twee categorieën risico's voor de nationale veiligheid: ongewenst eindgebruik van sensitieve kennis en technologie en het ontstaan van risicovolle strategische afhankelijkheden. Om bepaalde kennis en technologie als sensitief aan te merken, moeten deze risico's ook aannemelijk zijn. Met andere woorden: voorzienbaar of voorstelbaar. Wanneer de risico's niet of nog niet voorstelbaar of voorzienbaar zijn, is een screening (nog) niet noodzakelijk. Per specifiek technologiegebied kan dit verschillen. In de bijlage bij deze toelichting wordt per technologiegebied gemotiveerd waarom sprake is van voorstelbare of voorzienbare risico's voor de nationale veiligheid. In die gevallen wordt screening als instrument noodzakelijk geacht.

Definitie nationale veiligheid
In dit wetsvoorstel wordt dezelfde definitie van nationale veiligheid als in de Wet vifo gehanteerd: nationale veiligheid ziet op het beschermen van de belangen die binnen Nederland wezenlijk zijn voor het voortbestaan van de democratische rechtsorde, voor de veiligheid of andere gewichtige belangen van de staat, of voor de instandhouding van de maatschappelijke stabiliteit. Net als in de Wet vifo wordt deze definitie wat betreft de te beschermen belangen verbonden aan de specifieke context en doelstelling van dit wetsvoorstel, door de toevoeging van de woorden 'voor zover die zien op het raakvlak tussen onderzoek en onderwijs en veiligheid'.

Bovengenoemde definitie van nationale veiligheid wordt in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (2023) nader ingekaderd: "Onder nationale veiligheid verstaan we de bescherming van onze nationale veiligheidsbelangen tegen dreigingen die deze belangen kunnen schaden en daarmee maatschappelijke ontwrichting kunnen veroorzaken." Er is sprake van een mogelijk ontwrichtend effect op de samenleving als één of meer van de zes nationale veiligheidsbelangen ernstig worden aangetast. De zes nationale veiligheidsbelangen zijn: territoriale veiligheid; fysieke veiligheid; economische veiligheid; ecologische veiligheid; sociale en politieke stabiliteit; en internationale rechtsorde en stabiliteit.

Met dit wetsvoorstel wordt beoogd de nationale veiligheid te beschermen tegen dreigingen die meerdere nationale veiligheidsbelangen kunnen aantasten. De inzet van kennis en technologie voor militaire doeleinden kan duidelijke gevolgen hebben voor de territoriale en fysieke veiligheid van Nederland en haar bondgenoten. De geopolitieke realiteit maakt echter ook dat dreigingen op onder meer het gebied van economische veiligheid en sociale en politieke stabiliteit steeds groter worden. Staten oefenen in toenemende mate macht uit door inzet van economische instrumenten, controle over hoogwaardige technologieën en misbruik van risicovolle strategische afhankelijkheden. Zie tevens paragraaf 4.3 van dit voorstel.

Nationale veiligheid en economische veiligheid
Dit voorstel ziet op het beschermen van de nationale veiligheid, door het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht via Nederlandse kennisinstellingen. De risico's voor de nationale veiligheid die hieruit kunnen ontstaan raken deels aan thema's op het terrein van economische veiligheid, maar ontstaan wel altijd vanuit de ontwikkeling van hoogwaardige kennis en technologie binnen de Nederlandse kennissector en de open wetenschap. Dit voorstel is dan ook nadrukkelijk niet bedoeld enkel ter bescherming van het verdienvermogen van Nederland.

Strategische autonomie is niet een doel op zich dat direct met dit wetsvoorstel wordt nagestreefd. Risicovolle strategische afhankelijkheden kunnen echter een drukmiddel zijn voor geopolitieke doeleinden. Dit kan leiden tot maatschappelijke ontwrichting en daardoor tot risico's voor de nationale veiligheid. Ook kan het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht het ontstaan van risicovolle strategische afhankelijkheden op de lange termijn beperken, uitstellen of voorkomen. Het valt dus niet uit te sluiten dat een technologie op het eerste gezicht niet evident risico's met zich meebrengt voor de nationale veiligheid, maar toch om de hiervoor genoemde redenen in dit wetsvoorstel is opgenomen.

Verscherpt toezicht en sanctieregelgeving
In de screening kennisveiligheid zal ook worden getoetst aan enkele verboden op het verlenen van technische bijstand, zoals opgenomen in verschillende EU-sanctieverordeningen. Technische bijstand omvat alle technische ondersteuning met betrekking tot reparatie, ontwikkeling, fabricage, assemblage, testen, onderhoud of enige andere technische dienst, en kan vormen aannemen zoals instructie, advies, training, overdracht van praktische kennis of vaardigheden of adviesdiensten. Volgens de Europese Commissie kan daaronder ook "het voorzien in hoger onderwijs en het faciliteren van toegepast onderzoek" vallen, maar tussen verschillende sanctieregimes kunnen (kleine) verschillen bestaan wat betreft de definitie van technische bijstand.[28]

Nederland dient als lidstaat van de EU maatregelen te nemen om te zorgen dat de verboden uit EU-sanctieverordeningen worden nageleefd en is verantwoordelijk voor de handhaving van die verboden. Ook kennisinstellingen zijn rechtstreeks gebonden aan de verboden uit sanctieverordeningen. De overheid ondersteunt kennisinstellingen sinds 2019 met het zogeheten verscherpt toezicht bij de naleving van deze verboden, specifiek als het gaat om het overdragen van bepaalde kennis en technologie naar Noord-Korea, Iran en Rusland. Het verscherpt toezicht houdt in de praktijk in, dat het OCW-Loket Kennisembargo en de Taskforce Ongewenste Kennisoverdracht (OCW) belast zijn met de toetsing van onderzoekers en studenten die willen werken of studeren in een van de richtingen op de lijst van aangewezen vakgebieden.[29] Het is verboden om zonder ontheffing aan een opleiding of onderzoek te beginnen of te werken binnen deze (vak)gebieden.

Het is van belang om te benadrukken dat kennisinstellingen gebonden zijn en blijven aan alle sanctieregiems en verboden die op hen van toepassing zijn, deze hebben immers rechtstreekste werking. Internationale sancties kunnen ook andere doelen dienen dan alleen de door dit wetsvoorstel beoogde bescherming van de nationale veiligheid. Sancties dienen onder meer de handhaving van de vrede, en de consolidering en ondersteuning van de democratie, de rechtsstaat, de mensenrechten en de beginselen van het internationaal recht, en de voorkoming van conflicten en versterking

[28] Commission opinion of 5.8.2019 on a request for interpretation concerning the provision of higher education and the undertaking of applied research in the framework of a prohibition to provide technology or technical assistance to a third country (C(2019) 5883 final). C(2019) 5883 final.
[29] Voor welke technische studies heb ik een ontheffing kennisembargo nodig?

van de internationale veiligheid.[30] Het belang van de naleving van alle sancties, ook door de kennissector, blijft onverminderd groot.

Het verscherpt toezicht als zelfstandig instrument zal ophouden te bestaan met de invoering van de screening kennisveiligheid. Met dit wetsvoorstel wordt geregeld dat het verscherpt toezicht wordt geïntegreerd in de screening kennisveiligheid, voor zover dit de toets op de verboden betreft die volgen uit sancties die onder het verscherpt toezicht vallen. Het verscherpt toezicht ziet momenteel op de sanctieregimes tegen Noord-Korea, Iran en Rusland. Er bestaan ook andere sanctieregimes waarin verboden op technische bijstand zijn opgenomen, echter daar ziet het verscherpt toezicht momenteel niet op.[31] Wel is met dit voorstel de mogelijkheid gecreëerd om bij ministeriële regeling het aantal landen en verboden op technische bijstand waar met de screening naar wordt gekeken uit te breiden.[32] Hierbij hanteert de Minister van OCW als uitgangspunt dat er sprake moet zijn van risico's voor de nationale veiligheid vanwege risico's op overdracht van de betreffende kennis en technologie van Nederlandse kennisinstellingen naar de gesanctioneerde landen in kwestie. Voor deze sanctieregimes en verboden staat buiten twijfel dat deze relevant zijn voor de nationale veiligheid. Er is sprake van technologieën waarvoor op grond van juridisch bindende internationale sanctieregelgeving reeds beperkingen gelden, waardoor beperkt ruimte bestaat voor beleidsinhoudelijke keuzes. Hoe de Minister van OCW kan besluiten om de sanctieregimes en verboden op technische bijstand onder de werking van dit voorstel te brengen wordt nader toegelicht in paragraaf 4.4.5.

Tot slot komen de kennis en technologie, die op grond van internationale sancties verboden zijn om over te dragen, voor een deel overeen met de technologieën die met dit wetsvoorstel zijn aangewezen als sensitief. De screening kennisveiligheid is daarmee een effectieve manier om uitvoering te geven aan het toetsen aan de relevante verboden die volgen uit sancties die gelden voor de kennissector, voor die vakgebieden waar risico's voor de nationale veiligheid aan verbonden zijn ingeval van overdracht van de betreffende kennis en technologie van Nederlandse kennisinstellingen naar de gesanctioneerde landen in kwestie.

In hoofdstuk 3, paragraaf 3.2.1, wordt nader ingegaan op hoe de toets op het verbod op het verlenen van technische bijstand in het screeningsproces is verwerkt. In hoofdstuk 4, paragraaf 4.4.4, wordt ingegaan op de verhouding tussen sensitieve technologieën die reeds vallen onder sanctieregelgeving en de overige technologieën die met dit wetsvoorstel als sensitief zijn aangewezen. In hoofdstuk 7 wordt nader toegelicht hoe toezicht en handhaving op naleving van technische bijstandsverboden in sanctieregelgeving, die onder de werking van de screening kennisveiligheid zijn gebracht, wordt gewaarborgd.

De screening kennisveiligheid in relatie tot academische vrijheid
Academische vrijheid is een fundament en kernwaarde van de wetenschap. Academische vrijheid is essentieel in een democratische samenleving en nauw verbonden aan enkele grondrechten, zoals de vrijheid van meningsuiting, maar zij valt er niet mee samen. Voor dit voorstel hanteren we de breed gedragen definitie van de KNAW: 'het beginsel dat medewerkers aan wetenschappelijke instellingen in vrijheid hun wetenschappelijk onderzoek kunnen doen, hun bevindingen naar buiten kunnen brengen en onderwijs kunnen geven.'[33] Academische vrijheid is gekoppeld aan mensen in hun functie als

[30] Zie in artikel 21, tweede lid, van het Verdrag betreffende de EU (VEU) alle doelstellingen van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid, waar de Raad rekening mee dient te houden wanneer sancties worden opgelegd.
[31] Alle actueel geldende sancties staan gepubliceerd op de EU Sanctions Map.
[32] Zie artikelen 6, derde lid, en 9, tweede lid.
[33] Academische vrijheid in Nederland. Een begripsanalyse en richtsnoer (2021) Academische vrijheid in Nederland. Een begripsanalyse en richtsnoer (2021) Vgl. de UNESCO definitie (1997), die ook het recht omvat van docenten in hoger onderwijs om hun mening kenbaar te maken over

docent of onderzoeker, of aan studenten, en is onderworpen aan bepaalde kwaliteitseisen. Deze kwaliteitseisen bestaan uit de normen en waarden die gelden in de academische gemeenschap.

Binnen het concept van academische vrijheid kan er een onderscheid worden gemaakt tussen individuele academische vrijheid, institutionele academische vrijheid en de rol van de overheid in het borgen van academische vrijheid. De verantwoordelijkheid om academische vrijheid te borgen rust niet alleen op medewerkers van kennisinstellingen, ook besturen van deze instellingen, opdrachtgevers (van onderzoek) en de overheid hebben een verantwoordelijkheid om de academische vrijheid te respecteren, dan wel te borgen.

Wettelijk is academische vrijheid verankerd in artikel 1.6 WHW: "Aan de instellingen voor hoger onderwijs en aan de academische ziekenhuizen wordt de academische vrijheid in acht genomen." Academische vrijheid is ook verankerd in het Handvest van de grondrechten van de Europese Unie (artikel 13). Daarbij is in de beperkingsclausule in artikel 52 van datzelfde Handvest bepaald dat alle beperkingen op academische vrijheid aan het evenredigheidsbeginsel moet voldoen.

De academische vrijheid is niet onbeperkt. De grenzen vloeien onder andere voort uit eerdergenoemde professionele normen en waarden, voor wetenschappelijk onderzoek vastgelegd in de Nederlandse Gedragscode Wetenschappelijke Integriteit.[34] Ook kan de overheid beperkingen stellen om haar beschermende en faciliterende taak te kunnen vervullen, mits daarvoor een wettelijke grondslag aanwezig is, de beperkingen een legitiem doel dienen, en tevens noodzakelijk zijn in een democratische samenleving.[35]

Academische vrijheid kan onder druk komen te staan door de ongewenste inmenging van statelijke actoren. Deze actoren zijn bijvoorbeeld op zoek naar hoogwaardige kennis en technologie, en schromen daarbij niet om methoden te hanteren die haaks staan op onze normen en waarden, terwijl die verkrijging niet in het belang is van Nederland of onze bondgenoten.

Tegen deze achtergrond is er sprake van een gedeelde verantwoordelijkheid voor het kennisveld en de overheid om deze ongewenste inmenging tegen te gaan. Het vrij en veilig houden van de Nederlandse wetenschap is de kernopgave van kennisveiligheid. Daartoe heeft de overheid de afgelopen jaren verschillende onderling samenhangende beleidsinstrumenten ontwikkeld. Sluitstuk van dit beleid is de screening kennisveiligheid. Met het preventieve en persoonsgerichte karakter zal de screening kennisveiligheid de kans op ongewenste inmenging van statelijke actoren verkleinen en de weerbaarheid van kennisinstellingen vergroten. Daarmee zal de screening niet alleen de nationale veiligheid dienen, maar ook bijdragen aan vrij en veilig onderzoek.

De screening kennisveiligheid in relatie tot open science
Open science is een fundamentele academische kernwaarde, die erop toeziet dat kennis die met publieke middelen is vergaard ook beschikbaar moet zijn voor de samenleving.[36] Open science staat voor een open en participatieve onderzoekspraktijk waarbij publicaties, data, software en andere vormen van wetenschappelijke informatie in een

---

de instelling of het systeem waarbinnen zij werken, gevrijwaard te blijven van institutionele censuur, en deel te nemen aan professionele en representatieve academische organen (par. 27). Daarnaast vallen studenten buiten de definitie van de KNAW, wat niet wegneemt dat er elementen van academische vrijheid kunnen zijn die ook voor hen gelden. Of en in hoeverre zij een beroep kunnen doen op academische vrijheid dient van geval tot geval te worden bezien.

[34] Nederlandse gedragscode wetenschappelijke integriteit | NWO.

[35] Academische vrijheid in Nederland. Een begripsanalyse en richtsnoer (2021) Academische vrijheid in Nederland. Een begripsanalyse en richtsnoer (2021) , p. 29. Vgl. Handvest van de grondrechten van de Europese Unie, artikel 52, eerste lid.

[36] Uit artikel 27 van de Universele Verklaring van de Rechten van de Mens volgt onder meer dat wetenschap beschikbaar en toegankelijk moet zijn. Artikel 27 bepaalt dat ieder mens voordeel moet kunnen hebben van wetenschappelijke vooruitgang.

zo vroeg mogelijk stadium met de samenleving gedeeld worden en voor hergebruik beschikbaar gesteld worden. Open science leidt tot meer impact, draagvlak en transparantie in de wetenschap. Dat komt zowel de wetenschap zelf als de maatschappij ten goede.

Open science betekent niet 'onvoorwaardelijk' open. Open science is het uitgangspunt, maar er zijn kaders en begrenzingen, voornamelijk bij het vrijelijk delen van onderzoeksdata door onderzoekers. In de Raadsconclusies[37] over open science uit 2016 nemen de lidstaten, de Europese Commissie en belanghebbenden optimaal hergebruik van onderzoeksdata als uitgangspunt.[38] Daarbij moeten wel verschillende toegangsregimes worden onderkend, waaronder intellectuele eigendomsrechten, bescherming van persoonsgegevens en vertrouwelijkheid, *veiligheidsoverwegingen* en het mondiale economische concurrentievermogen en andere legitieme belangen. Daarom bevelen de Raadsconclusies aan dat het onderliggende principe in geval van het optimaal hergebruiken van onderzoeksdata zou moeten zijn: "zo open als mogelijk, zo gesloten als nodig". In de Raadsconclusies over 'Wetenschappelijk publiceren op een hoogwaardige, transparante, open, betrouwbare en rechtvaardige manier' uit 2023 is het belang van "zo open als mogelijk, zo gesloten als nodig" nog eens herhaald.[39] Dit principe past bij de principes van kennisveiligheid en het daarbij gehanteerde uitgangspunt 'open waar mogelijk, beschermen waar nodig', dat van het principe van open science is afgeleid.

Het bredere kennisveiligheidsbeleid, waar de screening kennisveiligheid onderdeel van uitmaakt, beoogt het uitvoeren van onderzoek op een open én veilige manier, waarbij de academische kernwaarden, integriteit en onafhankelijkheid worden gewaarborgd. Het doel van de screening kennisveiligheid is daarmee dan ook niet tegenstrijdig, maar complementair aan de doelen van open science. Met de screening kennisveiligheid wordt niet beoogd om beperkingen op te leggen ten aanzien van het (geheel of gedeeltelijk) publiceren van onderzoeksresultaten, maar op het voorkomen of mitigeren van de risico's op het ongewenst weglekken van hoogwaardige kennis en technologie voorafgaand aan publicatie.

Wat regelen we niet?
De screening richt zich op ongewenste kennis- en technologieoverdracht via personen. Dat betekent dat met dit instrument een instelling niet kan worden verboden om bepaalde samenwerkingsverbanden met andere buitenlandse instellingen aan te gaan. Wel kan een affiliatie met een instelling waarmee wordt samengewerkt een indicator zijn dat er rondom een persoon risico's op ongewenste kennis- en technologieoverdracht kunnen bestaan. Kennisinstellingen kunnen het Loket Kennisveiligheid advies vragen over risico's rondom samenwerkingsverbanden met buitenlandse instellingen.

De brede aanpak kennisveiligheid ziet ook op het voorkomen van heimelijke beïnvloeding en de ethische vraagstukken die kunnen spelen rondom internationale samenwerking. De screening kennisveiligheid is niet direct gericht op het voorkomen van heimelijke beïnvloeding of om te ondersteunen bij ethische kwesties.

Er is sprake van heimelijke beïnvloeding wanneer landen proberen het Nederlandse politieke en sociale systeem onopgemerkt te beïnvloeden. Kennisinstellingen en individuele studenten, onderzoekers en medewerkers kunnen doelwit zijn van statelijke actoren, doordat statelijke actoren meningen, publicaties en onderzoeksresultaten proberen te beïnvloeden en wetenschappelijk onderzoek proberen te censureren. Het

[37] Via een Raadsconclusie maakt de Raad van de EU zijn politiek standpunt kenbaar over een onderwerp dat tot de werkterreinen van de EU behoort. Dergelijke documenten dienen enkel om politieke toezeggingen of standpunten te verwoorden. Zij zijn niet juridisch bindend.
[38] Europese Commissie: Open Innovation, Open Science, Open to the World (2016).
[39] Raadsconclusie Wetenschappelijk publiceren op een hoogwaardige, transparante, open, betrouwbare en rechtvaardige manier (2023).

kan dan bijvoorbeeld gaan om onderzoek naar voor een statelijke actor onwelgevallige onderwerpen, zoals mensenrechtenschendingen en niet alleen over sensitieve kennis of technologie. Het voorkomen van heimelijke beïnvloeding is niet het hoofddoel van de screening kennisveiligheid. Indien tijdens de screening wordt geconstateerd dat een screeningsplichtige mogelijk kwetsbaar is voor heimelijke beïnvloeding, is dat wel relevante informatie in het kader van de nationale veiligheid om te betrekken in de risicobeoordeling.

De screening kennisveiligheid is ook niet direct gericht op het voorkomen van ethische kwesties rondom internationale samenwerking. Hiervan kan bijvoorbeeld sprake zijn wanneer bepaalde kennis of technologie hier wordt verworven en door statelijke actoren wordt ingezet om de eigen bevolking te onderdrukken. Denk aan bepaalde surveillancetechnologie, waarmee statelijke actoren door middel van camera's met gezichtsherkenning de eigen bevolking in de gaten kunnen houden. In dat geval is de overdracht van deze kennis en technologie wel ongewenst, maar is er geen sprake voor een potentieel risico voor onze nationale veiligheid of die van onze bondgenoten. Het voorkomen dat de verwerving van sensitieve kennis en technologie leidt tot dergelijke ethische kwesties valt niet onder het toepassingsbereik van dit wetsvoorstel. Verschillende beleidsinstrumenten, zoals het Loket Kennisveiligheid, de bestuurlijke dialoog en de Nationale Leidraad Kennisveiligheid, bieden hulp bij het zorgvuldig afwegen van risico's bij internationale samenwerking, inclusief heimelijke beïnvloeding en ethische kwesties die daarbij kunnen spelen. Ook werkt de regering samen met de kennissector aan een landelijke set uniforme criteria op grond waarvan kennisinstellingen betere inschattingen kunnen gaan maken van de verschillende bovengenoemde kennisveiligheidsrisico's bij het aangaan van internationale samenwerkingen.[40]

2.4 Motivering instrumentkeuze

2.4.1. Waarom screening?

Met een screening kan, voordat toegang wordt verleend tot sensitieve technologie, aan de hand van verschillende bronnen worden gekeken naar personalia, studie- of arbeidsverleden, sociaal en wetenschappelijk netwerk, landen van verblijf, publicaties, financiering en eventuele risico's verbonden aan partner en/of familie. Zo kunnen kwetsbaarheden worden ingeschat die kunnen leiden tot risico's op ongewenste kennis- en technologieoverdracht. Vervolgens vindt met de screening een belangenafweging plaats waarbij het belang van het individu en de wetenschap wordt gewogen ten opzichte van het belang van de nationale veiligheid. In hoofdstuk 3 wordt het proces van de screening nader toegelicht.

Naast dat met een screening in een individueel geval risico's kunnen worden geadresseerd, werkt een screening ook normstellend. Het bestaan van de screening geeft het signaal af aan statelijke actoren dat ongewenste hoogwaardige kennis- en technologieoverdracht niet wordt getolereerd en werpt een barrière op voor statelijke actoren om sensitieve kennis en technologie te kunnen verwerven.

Daarnaast kan de screening voor zelfselectie bij (potentiële) aanvragers zorgen en ligt het voor de hand dat statelijke actoren minder snel een onderzoeker of student gericht zullen sturen om sensitieve kennis en technologie te verwerven. Dit betekent dat onderzoekers en studenten met een belastend netwerk minder vaak opteren of solliciteren naar posities die vallen onder het toepassingsbereik van deze wet en mogelijk uitwijken naar andere posities zonder screeningsplicht.[41] De screening

[40] Kamerstukken II 2023/24, 31288, nr. 1134.
[41] Om dit waterbed-effect tegen te gaan zet Nederland in op het stimuleren van veiligheidsscreenings bij andere EU-lidstaten en gelijkgezinde landen.

kennisveiligheid is daarmee een belangrijk preventief instrument waarmee wordt beoogd om risico's aan de voorkant te voorkomen of te mitigeren.

Een verplichte screening maakt ook duidelijk dat er hoge integriteit- en veiligheidseisen worden gesteld als een individu in aanraking wil komen met sensitieve kennis en technologie en zal naar verwachting het gesprek op de werkvloer over kennisveiligheid bevorderen, waardoor de weerbaarheid van kennisinstellingen wordt vergroot.

Een andere belangrijke functie van de screening is dat de toekomstige screeningsautoriteit risicotrends kan signaleren. Denk hierbij aan interesse van actoren in specifieke kennis of technologie. De regering wil deze risicotrends bij bevoegde organisaties – zoals kennisinstellingen, het Loket Kennisveiligheid en de inlichtingen- en veiligheidsdiensten – adresseren zodat de weerbaarheid binnen de gehele kennissector wordt vergroot.[42]

De screening vormt het sluitstuk van de brede aanpak kennisveiligheid van OCW. De sluitstukgedachte omvat niet alleen het adresseren van de risico's rondom personen, die niet kunnen worden ondervangen met de bestaande beleidsinstrumenten, maar ook hoe de screening samenhangt met bestaande beleidsinstrumenten gericht op zelfregulering en bewustwording. Omdat met de screening niet alle risico's kunnen worden voorkomen of gemitigeerd, kan de screening enkel effectief zijn als kennisinstellingen zelf ook goed in staat zijn om kennisveiligheidsrisico's te herkennen en maatregelen kunnen nemen, zoals het toepassen 'due dilligence' onderzoek en een pre-employment check. Ook zal het beschermen van kennis en technologie door middel van de screening weinig effectief zijn als dezelfde kennis of technologie niet goed (fysiek of digitaal) is beveiligd of gecompartimenteerd en dus op andere manieren kan worden verkregen. Hierbij is ook van belang om te benoemen dat screening een zwaarder en ingrijpender middel is dan de hiervoor genoemde maatregelen gericht op zelfregulering en bewustwording en daarom ook pas aan de orde kan komen als eerst andere, minder ingrijpendere maatregelen zijn ingevoerd. In paragraaf 2.5. wordt uitgebreid stilgestaan op de verhouding van de screening tot de concrete maatregelen omtrent kennisveiligheid en het tegengaan van ongewenste kennis- en technologieoverdracht.

2.4.2. Uitgangspunten van het wetsvoorstel

Generiek en toekomstbestendig
Een belangrijk uitgangspunt van het wetsvoorstel is dat de aanpak generiek en toekomstbestendig is, omdat zij in het geval van een veranderend dreigingsbeeld direct toepasbaar is op elk land waar een eventueel (toekomstig) risico voor de nationale veiligheid van uitgaat. Dit betekent dat alle onderzoekers en studenten worden gescreend indien zij willen werken of studeren aan een Nederlandse kennisinstelling en daarbij toegang krijgen tot sensitieve kennis of technologie of een onderdeel daarvan, tevens in lijn met het non-discriminatiebeginsel. Ook is de voorgestelde wetgeving toekomstbestendig doordat technologieën die momenteel niet sensitief zijn, maar dat in de toekomst wel kunnen worden, ook onder de werking van dit wetsvoorstel kunnen worden gebracht. Andersom is het ook mogelijk dat technologieën die nu als sensitief worden beoordeeld, in de toekomst minder sensitief zijn en niet meer onder de werking van de screening kennisveiligheid hoeven te vallen.

Centraal georganiseerd
Een centraal georganiseerde screening is noodzakelijk om op een uniforme, onafhankelijke en zorgvuldige manier persoonsgebonden risico's te kunnen adresseren. Alleen de rijksoverheid heeft toegang tot alle relevante informatie om tot een zo scherp

[42] Signaleren dat bepaalde door actoren aangestuurde netwerken toegang proberen te krijgen tot Nederlandse kennisinstellingen. Deze informatie kan worden gedeeld met de inlichtingen- en veiligheidsdiensten en ook met kennisinstellingen.

mogelijke risicobeoordeling te kunnen komen en dit op landelijk niveau gelijksoortig toe te passen.

Onderzocht is of kennisinstellingen zelf een screening van onderzoekers en studenten die in aanraking komen met sensitieve technologie zouden kunnen uitvoeren. Deze optie is afgevallen, omdat kennisinstellingen niet over voldoende kennis en expertise beschikken om zelf in concrete gevallen een volledige risicobeoordeling op het gebied van de nationale veiligheid te kunnen maken. Die kennis en expertise zit bij de rijksoverheid, die gebruik kan maken van relevante informatie, waaronder informatie van de inlichtingen- en veiligheidsdiensten. De overheid kan dit echter niet alleen, daarom wordt de kennissector zoveel als mogelijk betrokken in deze opgave, bijvoorbeeld bij het vaststellen van hoog-risico onderdelen van de instelling. In de volgende paragraaf wordt hier nader op ingegaan.

Daarnaast is een centraal georganiseerde screening noodzakelijk om gelijke gevallen gelijk te kunnen handelen. Indien de screening door kennisinstellingen zelf zou worden uitgevoerd kan dat in de praktijk leiden tot een ongelijke behandeling tussen onderzoekers of studenten al naar gelang de instelling waar zij naartoe willen, als kennisinstellingen risicobeoordelingen en belangenafwegingen op een verschillende manier maken.

Met de screening wordt in de persoonlijke levenssfeer van een individu getreden. Het is ook om die reden van belang te voorzien in een effectieve en uniforme wijze van rechtsbescherming en privacybescherming voor het individu. Een centraal door de overheid georganiseerde screening maakt het beter mogelijk dat wordt voorzien in effectieve rechtsbescherming doordat tegen het screeningsbesluit bezwaar en beroep bij de bestuursrechter kan worden ingesteld, waarbij kan worden getoetst aan uniform beleid.

Samen met de kennissector
Het voorgestelde instrument moet daarnaast risicogericht en proportioneel zijn. Deze risicogerichte aanpak hangt nauw samen met de met dit voorstel aangewezen sensitieve technologieën en het vaststellen waar deze sensitieve kennis en technologie zich bevinden binnen een kennisinstelling. Dit bepaalt immers (mede) het toepassingsbereik van dit wetsvoorstel, omdat screening alleen aan de orde is als een onderzoeker of student toegang krijgt tot een hoog-risico onderdeel van een instelling. Om dit zo risicogericht en responsief als mogelijk te kunnen vormgeven, stellen we de hoog-risico onderdelen van de kennisinstellingen vast samen met de kennissector. Kennisinstellingen hebben immers zelf in beeld binnen welke onderdelen van de instelling sensitieve kennis of technologie aanwezig is.

De kennissector krijgt hiermee een belangrijke rol bij het mede bepalen waar de risico's voor de nationale veiligheid het grootst zijn. De kennissector is in verschillende consultatierondes betrokken bij de afbakening van de sensitieve technologieën en kennisinstellingen krijgen nu een centrale taak bij het identificeren van de onderdelen binnen de eigen instelling. Dat gebeurt aan de hand van een beoordelingskader dat door de rijksoverheid en het kennisveld gezamenlijk is ontwikkeld. Aan de hand van dit beoordelingskader wijst de kennisinstelling aan binnen welke onderdelen van de instelling sensitief onderzoek en onderwijs plaatsvinden en meldt dit aan de Minister van OCW. Dit proces wordt in paragraaf 4.4. nader uitgewerkt en toegelicht.

De hier bedoelde risicogerichte aanpak maakt dat de screening zo effectief en proportioneel mogelijk is, vanuit de gedachte 'open waar mogelijk, beschermen waar nodig'. Ook is deze aanpak responsief en daarmee flexibel, omdat zo snel kan worden ingespeeld op organisatorische veranderingen binnen een kennisinstelling en op nieuwe wetenschappelijke ontwikkelingen.

2.5 Verhouding met breder beleid omtrent kennisveiligheid

Beleidsaanpak voor de kennissector
Bij de aanpak van kennisveiligheid speelt bewustwording en zelfregulering bij kennisinstellingen een centrale rol. Dit omdat kennisveiligheid niet alleen ziet op concrete risico's rondom personen, maar veel breder is en bijvoorbeeld ook ziet op heimelijke beïnvloeding en ethische vraagstukken bij internationale samenwerkingen. Kennisinstellingen hebben zelf zicht op de verscheidenheid aan risico's en vraagstukken die kunnen spelen binnen de instelling. Daarom houdt deze aanpak in dat de kennisinstelling zelf veiligheidsrisico's monitort, een aanpak formuleert en instrumenten ontwikkelt en zo actief investeert in de weerbaarheid. Organisaties zoals de Vereniging Hogescholen (VH), Universiteiten van Nederland (UNL), de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), de Nederlandse Federatie van Universitair Medische Centra (NFU) en de TO2-federatie (samenwerkingsverband van Nederlandse instituten voor toegepast onderzoek), spelen daarin een initiërende en faciliterende rol, bijvoorbeeld door kennisinstellingen met elkaar in gesprek te brengen. Het beschermen van de nationale veiligheid blijft echter altijd een kerntaak van de overheid. Daarom is ook voor de Rijksoverheid een actieve rol weggelegd. De Rijksoverheid werkt samen met de kennissector, zodat kennisinstellingen invulling kunnen geven aan de verantwoordelijkheid die zij op grond van hun institutionele autonomie hebben. Daarbij gaat het om informeren, faciliteren en adviseren door de Rijksoverheid, door middel van verschillende instrumenten.

De Nationale Leidraad Kennisveiligheid is bedoeld om aan bestuurders, veiligheidscoördinatoren, projectleiders en individuele onderzoekers van kennisinstellingen handvatten te bieden voor veilige internationale samenwerking. Daarbij wordt middels externe audits bij universiteiten, hogescholen, UMC's en de NWO- en KNAW-instituten, in beeld gebracht hoe ver kennisinstellingen zijn met de implementatie van de Nationale Leidraad Kennisveiligheid. Verder wordt met de externe audit onder meer onderzoek gedaan naar de aanpak en uitkomsten van de door de kennisinstellingen uitgevoerde risicoanalyse op internationale samenwerkingen en financieringsbronnen.

Het Loket Kennisveiligheid is een rijksbreed initiatief en is bedoeld als een laagdrempelig centraal contactpunt van de hele rijksoverheid, waar kennisinstellingen terecht kunnen met hun aan kennisveiligheid gerelateerde vragen. Denk aan vragen rond het aangaan van samenwerkingsverbanden met buitenlandse kennisinstellingen. Het Loket Kennisveiligheid verstrekt informatie en adviseert kennisinstellingen over concrete kennisveiligheidsvraagstukken bij internationale samenwerking. Deze adviezen zijn juridisch niet-bindend en zijn alleen bedoeld om kennisinstellingen te ondersteunen bij het maken van een inschatting van de kansen en risico's rondom internationale samenwerkingen, en hoe instellingen deze risico's kunnen mitigeren. Ook organiseert de learning community van het Loket Kennisveiligheid kennissessies, webinars en e-learnings. Daarbij geldt dat de Rijksoverheid informatie deelt en ondersteunt, maar dat de kennisinstellingen - in lijn met hun institutionele autonomie - zelf verantwoordelijk blijven. De Rijksdienst voor Ondernemend Nederland (RVO) verzorgt het voorportaal (frontoffice). Daar komen de vragen binnen, die zo spoedig mogelijk worden beantwoord. De backoffice wordt gevormd door de inhoudelijk experts van de betrokken departementen. Zo wordt vanuit een *whole of government-approach* door betrokken departementen specifieke expertise geleverd bij het opstellen van de adviezen van het Loket.[43]

[43] Dit zijn: OCW , EZ, BZ, LVVN, NCTV, AIVD en MIVD. Andere onderdelen van de rijksoverheid kunnen op ad hoc-basis betrokken worden.

De kennisveiligheidsdialogen zijn een reeks gesprekken tussen de rijksoverheid en kennisinstellingen, bedoeld om onderling kennis en ervaringen uit te wisselen over kansen, risico's en instrumenten om op een verantwoordelijke manier internationale samenwerkingsrelaties aan te gaan.

Echter, daar waar de risico's het grootst zijn volstaat alleen zelfregulering en bewustwording niet. Hoewel de bestaande instrumenten effectief zijn, zijn zij niet in staat om risico's rondom personen effectief en uniform te adresseren. Om een nauwkeurige risicobeoordeling op het gebied van ongewenste kennis- en technologieoverdracht te kunnen maken is het noodzakelijk dat onderzoekers en studenten worden gescreend op persoonsniveau door de rijksoverheid.

Wanneer de screening gezamenlijk met de bestaande beleidsinstrumenten wordt ingezet wordt de werking van de screening versterkt, en andersom. Denk hierbij aan het implementeren van de Nationale Leidraad Kennisveiligheid door kennisinstellingen, het toepassen van adviezen van het Loket Kennisveiligheid en het treffen van (extra) veiligheidsmaatregelen rondom sensitieve kennis en technologie. Dit wetsvoorstel is daarom een effectief en noodzakelijk aanvullend middel, als sluitstuk op de bestaande instrumenten.

Overige instrumenten voor het tegengaan van ongewenste kennis- en technologieoverdracht
Dit wetsvoorstel is één van de instrumenten om de bescherming te verhogen van het Nederlandse kennis- en innovatielandschap tegen statelijke dreigingen. Dit wetsvoorstel is dan ook niet alleen onderdeel van de brede aanpak van beleidsinstrumenten gericht op de kennissector onder (primaire) verantwoordelijkheid van de minister van OCW, maar is ook onderdeel van de Rijksbrede aanpak gericht op het beheersen van risico's voor de nationale veiligheid.

Op grond van VN- en EU-sancties is het verboden technische bijstand te verlenen of goederen of technologie over te dragen voor bepaalde kennisgebieden naar een aantal gesanctioneerde landen. De sancties tegen Noord-Korea en Iran verbieden (of stellen vergunningplichtig) bijvoorbeeld dat kennis over het maken van kernwapens en raketten aan deze landen wordt overgedragen. Voor zover sancties gaan om het voorkomen van kennis- en technologieoverdracht heeft dit raakvlakken met kennisveiligheid. Echter, sancties zijn niet altijd enkel bedoeld om de nationale veiligheid te beschermen, maar kunnen ook andere doelen dienen. Zoals de handhaving van de vrede, en de consolidering en ondersteuning van de democratie, de rechtsstaat, de mensenrechten en de beginselen van het internationaal recht, en de voorkoming van conflicten en versterking van de internationale veiligheid.

Exportcontrole behelst wet- en regelgeving die Nederland implementeert om de export van bepaalde strategische goederen, technologieën en diensten te controleren om redenen van nationale veiligheid. De controles zijn bedoeld om de ongewenste verspreiding van wapens te voorkomen, de verspreiding van gevoelige technologieën te beheersen en ervoor te zorgen dat export geen activiteiten ondersteunt die in strijd zijn met het belang van Nederland. Strategische goederen zijn goederen waarvan de uit-, in- of doorvoer naar bepaalde landen niet, of alleen onder bepaalde voorwaarden, is toegestaan. Redenen daarvoor zijn veiligheid en internationale afspraken. Het gaat om specifieke goederen die kunnen worden gebruikt voor militaire doeleinden, voor zowel burgerlijke als militaire doeleinden of bij de productie van massavernietigingswapens en/of overbrengingsmiddelen voor dergelijke wapens. Exportcontrole richt zicht verder ook op zogenoemde 'sanctiegoederen', waarover is besloten dat deze gevoelig genoeg zijn om te controleren. Tevens zijn er nationale aanvullende exportcontrolemaatregelen

van kracht, bijvoorbeeld op het gebied van halfgeleiders, halfgeleiderproductieapparatuur, additive manufacturing en quantum technologie.[44]

Om ongewenst eindgebruik tegen te gaan, geldt een vergunningplicht voor de uitvoer van strategische goederen en diensten. Bedrijven of personen die goederen en technologie willen uitvoeren die op de Gemeenschappelijke EU-lijst van militaire goederen of de bijlage van de EU dual-use verordening (2021/821) staan, dienen bij de Centrale Dienst voor In- en Uitvoer (CDIU) een aanvraag in voor een uitvoervergunning. De CDIU, onderdeel van de Douane, staat voor de verlening van uitvoervergunningen onder beleidstoezicht van het ministerie van Buitenlandse Zaken.

Militaire goederen zijn goederen die zijn opgenomen in de gemeenschappelijke EU-lijst van militaire goederen die jaarlijks wordt herzien. De export van deze goederen is onderworpen aan een toetsing aan de criteria van het EU Gemeenschappelijk Standpunt inzake wapenexportcontrole.[45]

Met de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) zijn regels vastgelegd waarmee risico's voor de nationale veiligheid als gevolg van bepaalde verwervingsactiviteiten, zijnde investeringen, fusies en overnames, beheerst kunnen worden. Statelijke actoren proberen namelijk niet alleen via personen kennis en technologie te verwerven, maar doen dit ook door overnames van en investeringen in bedrijven die beschikken over hoogwaardige kennis en technologie, het aankopen van bepaalde technologie en het aangaan van internationale samenwerkingsverbanden.

In het voorjaar van 2024 is door de Tweede Kamer het wetsvoorstel uitbreiding strafbaarheid spionageactiviteiten aangenomen.[46] Dit wetsvoorstel ligt momenteel in de Eerste Kamer. Met deze nieuwe strafbaarstelling worden verschillende vormen van spionageactiviteiten strafbaar die worden verricht ten behoeve van een buitenlandse mogendheid en schade toebrengen aan zwaarwegende belangen. Dit is een uitbreiding van de huidige strafbaarstelling die slechts enkele klassieke spionageactiviteiten strafbaar stelt gericht op het stelen van staatsgeheime informatie. Met het wetsvoorstel uitbreiding strafbaarheid spionageactiviteiten wordt beoogd om ook andere verschijningsvormen van spionageactiviteiten (zoals sabotageactiviteiten, het interveniëren in besluitvormingsprocessen, diasporaspionage) te kunnen aanpakken die risico's voor de nationale veiligheid kunnen opleveren. Spionageactiviteiten kunnen zich namelijk zowel richten op overheden en volkenrechtelijke organisaties als op bijvoorbeeld bedrijven en kennisinstellingen. Waar de screening kennisveiligheid een preventief instrument is, is dit instrument bedoeld om in voorkomende gevallen op te kunnen treden als ongewenste kennis- en technologieoverdracht reeds heeft plaatsgevonden, mits sprake is van een vermoeden van spionageactiviteiten. Belangrijke kanttekening is dat ongewenste kennis- en technologieoverdracht zoals bedoeld in onderhavig wetsvoorstel niet altijd via (digitale of fysieke) spionage plaatsvindt[47] en met de uitbreiding strafbaarheid spionageactiviteiten slechts deels en alleen achteraf kan worden opgetreden tegen ongewenste kennis- en technologieoverdracht. Met het wetsvoorstel screening kennisveiligheid wordt voorzien in een instrument om deze risico's preventie en aan de voorkant te kunnen mitigeren.

Daarnaast zijn er verschillende beleidsmaatregelen in ontwikkeling die interventies plegen in de keten van kennisontwikkeling, zowel bij kennisinstellingen als bij bedrijven.

[44] wetten.nl - Regeling - Regeling geavanceerde productieapparatuur voor halfgeleiders - BWBR0048439, wetten.nl - Informatie - Regeling aanvullende controlemaatregelen op de Verordening producten voor tweeërlei gebruik - BWBR0050313
[45] Besluit - 2019/1560 - EN - EUR-Lex
[46] Kamerstukken 36280, nr. 2.
[47] In paragraaf 2.2. van dit voorstel staat beschreven op welke manieren ongewenste kennis- en technologieoverdracht kan plaatsvinden.

Bedrijven die omgaan met bijzondere informatie, gevoelig materieel, gevoelige goederen of gevoelige objecten – collectief ook wel een 'te beschermen belang (TBB)' genoemd - moeten voldoen aan de beveiligingseisen van Defensie.[48] Deze staan in de Algemene Beveiligingseisen voor Defensieopdrachten 2019 (ABDO 2019). Medio 2025 is voorzien dat ABDO wordt vervangen door de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO).

Ook werkt de minister van Asiel en Migratie, samen met de ministers van Economische Zaken, van Sociale Zaken en Werkgelegenheid en van Justitie en Veiligheid aan maatregelen omtrent het erkend referentschap in relatie tot nationale veiligheid en de daar aanpalende maatregelen in relatie tot uitleenconstructies en individuele migranten.[49] Daarnaast onderzoeken deze betrokken ministeries gezamenlijk hoe ongewenste kennis- en technologieoverdracht via individuele (kennis)migranten bij in Nederland gevestigde bedrijven kan worden tegengegaan en de hierbij komende risico's kunnen worden voorkomen en gemitigeerd.

Internationaal gelijk speelveld
Nederland zet ook actief in op het bevorderen van een gelijk speelveld op het gebied van kennisveiligheidsbeleid in de EU, en ook breder internationaal. De aanpak op kennisveiligheid is het meest effectief als andere landen ook beleid op kennisveiligheid voeren. Zo voorkomen we dat potentiële risicovolle wetenschappelijke samenwerking zich verplaatst en zorgen we ervoor dat Nederland een aantrekkelijke plek blijft voor internationaal talent en wetenschappelijke samenwerking.

Met de aanname van de Raadsaanbeveling over kennisveiligheid in de EU is daarmee al een goede stap gezet.[50] De Raadsaanbeveling bevat een overkoepelend Europees kader voor alle lidstaten en de Europese Commissie om kennisveiligheid te versterken. Nederland speelt een voortrekkersrol om ervoor te zorgen dat de aanbevelingen uit de Raadsaanbevelingen breed worden geïmplementeerd in Europa.

Daarnaast is breder internationaal ook structureel aandacht voor kennisveiligheid. Met landen als Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten maken we onderdeel uit van een internationaal netwerk van gelijkgezinde landen. Het netwerk van de onderwijs- en wetenschapsattachés en de innovatieattachés zorgen samen met de Nederlandse ambassades voor verdere versteviging en uitbreiding van de internationale samenwerking op kennisveiligheid. Ook zetten we internationaal in op samenwerking op concrete beleidsinstrumenten. Met buitenlandse partners zoals het SECURE Centre (VS), het Research Security Centre (Canada) en het Research Collaborative Advise Teams (VK) wisselen we hierover kennis uit.

2.6 Alternatieven

Onderzocht is of er al alternatieve maatregelen bestaan om hetzelfde doel, het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht via individuele onderzoekers en studenten bij Nederlandse kennisinstellingen, te bereiken en of bestaande wettelijke kaders een grondslag kunnen bieden voor de beoogde preventieve screening.

Advisering Loket Kennisveiligheid
De screening kennisveiligheid heeft in de brede aanpak kennisveiligheid een wezenlijk andere functie dan het Loket Kennisveiligheid, namelijk om daar waar de risico's het

[48] Het gaat bij ABDO en (in de toekomst) ABRO om opdrachten die een impact hebben op de nationale veiligheid. Als de overheid beschikt over een te beschermen belang, en dat overdraagt aan een leverancier of contractant dan is ABDO, en in de toekomst ABRO van toepassing.
[49] Kamerstukken II 2023/24, 30 573, nr. 211.
[50] Raadsaanbeveling 9097/1/24 REV 1, te raadplegen op https://data.consilium.europa.eu/doc/document/ST9 0 97-2024-REV-1/en/pdf. De reactie op het voorstel van deze Raadsaanbeveling van de Europese Commissie, zie Kamerstuk 22 112, nr. 3906.

grootst zijn, wettelijk bindende kaders te stellen. In plaats daarvan adviseert en informeert het Loket Kennisveiligheid, op een case by case basis. De technologiegebieden en toepassingen die sensitief zijn vanuit het perspectief van nationale veiligheid worden voor de screening kennisveiligheid zo strikt mogelijk afgebakend om het instrument zo risicogericht en proportioneel mogelijk te maken en alleen te focussen op de grootste risico's voor de nationale veiligheid. Loket Kennisveiligheid adviseert breder, namelijk: over alle technologiegebieden en over alle mogelijke kennisveiligheidsrisico's die kunnen bestaan rondom internationale samenwerkingen. Het bredere kennisveiligheidsbeleid ziet namelijk niet alleen op het voorkomen of mitigeren van ongewenste kennis- en technologieoverdracht op een beperkt aantal technologiegebieden, maar ook op heimelijke beïnvloeding en ethische kwesties rondom internationale samenwerking. Het is daarom van belang dat deze beide instrumenten naast elkaar blijven bestaan.

Daarnaast vereist het screenen van personen specialistische expertise van een organisatie die ervaring heeft met het wegen van belangen van het individu ten opzichte van de maatschappij.[51] Screening is gebaat bij enige luwte. In de meeste gevallen vindt screening daarom achter gesloten deuren plaats. Dit gebeurt met het oog op de privacy en ook omdat de geraadpleegde bronnen niet zichtbaar mogen of kunnen zijn voor iedereen.[52] Het Loket Kennisveiligheid heeft juist baat bij het zo toegankelijk mogelijk zijn voor kennisinstellingen. De adviezen van het Loket zijn weliswaar vertrouwelijk, maar in de adviezen wordt wel zo uitgebreid mogelijk gemotiveerd hoe risicobeoordelingen tot stand zijn gekomen, zodat dit bijdraagt aan het zelfregulerend vermogen en de weerbaarheid van de kennisinstelling. Dit in tegenstelling tot de screening kennisveiligheid, waar de motivering van negatieve besluiten beknopt zal zijn. Daarom wordt het onderbrengen van de screening kennisveiligheid bij het Loket Kennisveiligheid niet geschikt geacht.

Verscherpt toezicht en sanctieregelgeving
Het aanpassen of uitbreiden van de sanctieregelgeving en het daarop gebaseerde verscherpt toezicht, is geen geschikte grondslag gebleken voor de screening kennisveiligheid. Andersom is dit wel mogelijk: onderhavig wetsvoorstel kan wel de basis geven voor het naleven van sancties.

Nederland legt niet zelfstandig sancties op, op EU-niveau worden sancties vastgelegd in besluiten van de Raad en EU-verordeningen, overeenkomstig de doelstellingen van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB).[53] Dit maakt dat een screeningsinstrument volledig gebaseerd op sanctieregelgeving onvoldoende flexibiliteit biedt om snel in te spelen op actuele dreigingsbeelden.

Daarnaast zijn sancties niet altijd bedoeld om de nationale veiligheid te beschermen, maar kunnen ook andere doelen dienen. Zoals de handhaving van de vrede, en de consolidering en ondersteuning van de democratie, de rechtsstaat, de mensenrechten en de beginselen van het internationaal recht, en de voorkoming van conflicten en versterking van de internationale veiligheid.

De Verklaring Omtrent Gedrag (VOG)
Voor bepaalde functies is een Verklaring Omtrent het Gedrag (VOG) nodig. In sommige branches, zoals de kinderopvang, is dit zelfs wettelijk verplicht. Justis is de instantie die de VOG-aanvragen afhandelt. Een VOG is een verklaring waaruit blijkt dat het (justitiële) verleden van de persoon geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving. Bij de beoordeling van een VOG-aanvraag kijkt Justis of de

[51] Schram e.a., Meerwaarde(n) van screening, Nederlandse School voor Openbaar Bestuur (NSOB).
[52] Idem.
[53] De Verenigde Naties (VN) leggen ook sancties op. Indien in een resolutie van de VN-veiligheidsraad sancties zijn aangenomen, worden die sancties door de EU geïmplementeerd.

persoon strafbare feiten op diens naam heeft staan die een risico vormen voor de functie of het doel waarvoor de VOG wordt aangevraagd.

Een strafrechtelijke veroordeling kan relevant zijn voor de beoordeling van potentiële risico's op ongewenste kennis- of technologieoverdracht, maar is op zichzelf niet doorslaggevend. Daarvoor is meer informatie benodigd om een goede risicobeoordeling te kunnen maken, zoals ook beoogd in de screening kennisveiligheid.

Daarnaast geldt voor een deel van de doelgroep, te weten onderzoekers en studenten van buiten de EU, dat in Nederland van hen veelal geen strafrechtelijke gegevens bekend zullen zijn. Dat is slechts anders wanneer deze persoon in Nederland of de EU (onherroepelijk) is veroordeeld voor een strafbaar feit. Voor deze groep zou dan in veel gevallen geen VOG kunnen worden afgegeven. Een VOG is om deze redenen geen geschikt alternatief.

De Verklaring van Geen Bezwaar (VGB)
Verder is onderzocht of bepaalde onderzoeksplekken of studies als vertrouwensfunctie kunnen worden aangewezen op grond van de Wet veiligheidsonderzoeken (Wvo). De Wvo bevat in algemene zin de verplichting om functies die de mogelijkheid bieden de nationale veiligheid te schaden als vertrouwensfuncties aan te wijzen en personen te screenen voordat zij een dergelijke functie kunnen vervullen. Alleen wanneer voldoende waarborgen aanwezig zijn dat de betrokkene onder alle omstandigheden de uit de vertrouwensfunctie voortvloeiende plichten getrouwelijk zal volbrengen, kan een verklaring van geen bezwaar (hierna: VGB) worden afgegeven. De AIVD en de MIVD zijn belast met de uitvoering.

De Wvo stelt geen beperking aan sectoren, dus ook in het onderwijs en de wetenschap kunnen vertrouwensfuncties worden aangewezen. Echter, een studie is geen functie, waardoor op studenten de Wvo niet van toepassing is. Alleen onderzoekers met een arbeidsovereenkomst bij een Nederlandse kennisinstelling zouden kunnen vallen onder de Wvo.

Bij het aanwijzen van een vertrouwensfunctie gaat het om personen die in die functie over de mogelijkheid beschikken om de nationale veiligheid te schaden, door misbruik te maken van toegang tot staatsgeheime informatie of specifieke locaties. Het doel van de screening kennisveiligheid is het voorkomen van risico's voor de nationale veiligheid door ongewenste kennis- en technologieoverdracht, maar van wetenschappelijk onderzoek kan niet altijd worden gezegd dat de aard van deze functie ook maakt dat een onderzoeker ook altijd uit zijn functie voortvloeiende plichten heeft die hij getrouwelijk dient te volbrengen, zoals in geval van een vertrouwensfunctie. Het gaat bij wetenschapsbeoefening namelijk primair om het verkrijgen van kennis (door systematische studie en denken, observeren en experimenteren), met als doel de wereld beter te begrijpen en om deze kennis te delen met de rest van de wereld. Kennis en technologie is niet altijd staatsgeheime informatie, maar kan in sommige gevallen wel als sensitief in de zin van de nationale veiligheid worden aangemerkt. Om deze redenen is de VGB geen geschikt alternatief.

Een VGB wordt daarnaast ook geweigerd indien het veiligheidsonderzoek onvoldoende gegevens heeft kunnen opleveren om een oordeel te kunnen geven of er voldoende waarborgen aanwezig zijn dat de betrokkene onder alle omstandigheden de uit de vertrouwensfunctie voortvloeiende plichten getrouwelijk zal volbrengen. Bij de beoordeling van het veiligheidsonderzoek wordt ook het verblijf van betrokkene en eventueel diens partner in het buitenland betrokken. Over een verblijf in een land waarmee de Nederlandse inlichtingen- en veiligheidsdiensten geen samenwerkingsrelatie hebben kan dus geen informatie worden betrokken bij de beoordeling van het veiligheidsonderzoek en kan er sprake zijn van onvoldoende gegevens en een weigering van de verklaring van geen bezwaar. Dit kan betekenen dat onderzoekers uit landen

waarmee de Nederlandse inlichtingen- en veiligheidsdiensten geen samenwerkingsrelatie hebben, veelal geen verklaring van geen bezwaar kunnen krijgen. Niet gezegd kan worden dat het ontbreken van informatie van buitenlandse inlichtingen- en veiligheidsdiensten met zich mee brengt dat ook in alle gevallen sprake is van een risico op ongewenste kennis- en technologieoverdracht zoals wordt beoordeeld met de screening kennisveiligheid. Ook hierom is de VGB geen geschikt alternatief.

Algemene Beveiligingseisen voor Defensieopdrachten (ABDO)
Defensie doet zaken met bedrijven. Bij sommige opdrachten krijgen bedrijven bijzondere informatie of een ander TBB. Bijzondere informatie heeft een rubriceringsniveau. Bij die opdrachten doet de MIVD onderzoek naar de beveiliging van bedrijven die omgaan met deze bijzondere informatie. Deze bedrijven moeten voldoen aan de veiligheidseisen van conform de Algemene Beveiligingseisen voor Defensieopdrachten 2019 (ABDO 2019). Medio 2025 is voorzien dat ABDO wordt vervangen door de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO). Dan is er een algemeen kader met beveiligingseisen voor bedrijven die opdrachten uitvoeren voor de rijksoverheid en waarmee bijzondere informatie of een ander TBB gemoeid is.

De beveiligingsfunctionaris is verantwoordelijk voor de beveiliging van de bijzondere informatie binnen het bedrijf. Medewerkers die toegang hebben tot bijzondere informatie moeten worden gescreend. Afhankelijk van het geldende rubriceringsniveau moet de medewerker over een VOG of een VGB beschikken. ABDO of ABRO is dus geen aparte of zelfstandige screening, maar een waarborg dat bij de opdrachtnemer de juiste beveiliging wordt toegepast. Kennisinstellingen die vallen onder de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) vallen in beginsel buiten het bereik van ABDO of ABRO, omdat deze kennisinstellingen niet als opdrachtnemer van Defensie of de Rijksoverheid te kwalificeren zijn.[54]

Daarbij komt dat naar verwachting zeer weinig wetenschappelijk onderwijs of onderzoek zal kunnen kwalificeren als een opdracht vanuit Defensie of de rijksoverheid. Hierdoor kunnen risico’s onvoldoende worden afgedekt.

ABDO of ABRO is om voornoemde redenen geen geschikt middel om de met dit wetsvoorstel benoemde risico’s op ongewenste kennis- en technologieoverdracht te voorkomen of te mitigeren.

2.6.1 Alternatieven bestaande regelgeving

Exportregelgeving en dual-use
Exportcontrole behelst wet- en regelgeving die Nederland implementeert om de export van bepaalde strategische goederen, technologieën en diensten te controleren om redenen van nationale veiligheid. De controles zijn bedoeld om de ongewenste verspreiding van wapens te voorkomen, de verspreiding van gevoelige technologieën te beheersen en ervoor te zorgen dat export geen activiteiten ondersteunt die in strijd zijn met het belang van Nederland. Het Nederlandse beleid voor exportcontrole richt zich op strategische goederen en diensten.

Strategische goederen zijn militaire goederen, dual-use-goederen, en sanctiegoederen. Om ongewenst eindgebruik tegen te gaan, geldt een vergunningplicht voor de uitvoer hiervan. Is sprake van een onderzoek dat betrekking heeft op dual-use of militaire goederen, producten, programmatuur of technologie, dan mag dit onderzoek alleen worden geëxporteerd met een vergunning van de Centrale Dienst voor In- en Uitvoer

[54] Deze kennisinstellingen kunnen – in hun rol als inkopende overheidspartijen – in de toekomst mogelijk wel ABRO van toepassing verklaren in hun overeenkomsten met leveranciers van Bijzondere Opdrachten. Het Nationaal Bureau Industrieveiligheid (NBIV) heeft vervolgens de mogelijkheid om deze leveranciers van een ABRO-verklaring te voorzien. De kennisinstellingen zelf worden daarmee niet voorzien van een ABRO-verklaring.

(CDIU) van de Douane. In bijlage I van de dual-use Verordening staat wat in ieder geval wordt beschouwd als dual-use producten, programmatuur en technologie.[55]

Ongewenste kennis- en technologieoverdracht als bedoeld in dit wetsvoorstel kan echter ook op andere manieren plaatsvinden. Bijvoorbeeld via onderzoekers en studenten die op Nederlandse kennisinstellingen in aanraking komen met sensitieve kennis en technologie. In deze gevallen volstaat het beleid voor exportcontrole niet om risico's op ongewenste kennis- en technologieoverdracht via kennisinstellingen voldoende te kunnen beperken.

Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW)
De Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) richt zich op de kwaliteit, toegankelijkheid, doelmatigheid en inrichting van het onderwijs. De wet stelt geen specifieke eisen aan het veiligheidsbeleid van instellingen in het hoger onderwijs gericht op het tegengaan van ongewenste kennis- en technologieoverdracht. Daarnaast regelt de WHW alleen de toelating tot het hoger onderwijs van studenten en gaat niet over de aanstelling van onderzoekers bij kennisinstellingen op basis van arbeidsovereenkomsten, terwijl dit een groot deel van de doelgroep betreft.

De WHW als grondslag gebruiken voor de screening kennisveiligheid zou zich moeilijk verhouden met de doelen van de WHW en is hierom geen geschikte grondslag gebleken.

Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017)
De Wiv 2017 vormt het wettelijk kader voor de taakuitvoering van de inlichtingen- en veiligheidsdiensten in Nederland, de AIVD en MIVD. De inlichtingen- en veiligheidsdiensten opereren gesloten en afgeschermd van de rest van de rijksoverheid - onder verantwoordelijkheid van de ministers van Binnenlandse Zaken en Koninkrijksrelaties (AIVD) en Defensie (MIVD). Alleen de verantwoordelijke ministers kunnen sturen op de diensten en de AIVD en MIVD rapporteren enkel aan hen[56] en aan de Tweede Kamer.[57] De Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD) houdt toezicht op de rechtmatigheid van het handelen van de AIVD en MIVD. Een rol voor de Minister van OCW en alle andere bij kennisveiligheid betrokken departementen, zou zich moeilijk verhouden tot deze wettelijk vastgelegde taken en verantwoordingsprocessen.

In artikel 8, tweede lid, Wiv 2017 en artikel 10, tweede lid, Wiv 2017 zijn de taken van de AIVD en de MIVD limitatief opgesomd. De in artikel 8 van de Wiv 2017 omschreven wettelijke taken van de AIVD en artikel 10 van de Wiv 2017 omschreven wettelijke taken van de MIVD bieden geen ruimte voor een preventieve screening op risico's voor ongewenste kennis- en technologieoverdracht zoals beoogd. In dit verband is gekeken naar de zogenoemde b- en f-taak van artikel 8, tweede lid (AIVD) en de b- en g-taak van artikel 10, tweede lid (MIVD) te weten het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken (Wvo, zoals hiervoor benoemd) en het verrichten van naslagen.

De b-taak ziet op de taak van het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken. In de vorige paragraaf is al stilgestaan bij het

[55] Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (herschikking)
[56] Wel kan door afnemers van de informatie van de diensten worden bepaald op welke terreinen de onderzoeken kunnen worden gericht. Dit betreft zowel de onderzoeken voor de binnenlandse veiligheid als waar het gaat om de onderzoeken naar andere landen, de politieke inlichtingen. Dit is vastgelegd in de 'geïntegreerde aanwijzing'. De afnemers van de AIVD zijn onder andere het ministerie van Algemene Zaken, Buitenlandse Zaken, Defensie en het Openbaar Ministerie.
[57] Dit gebeurt in de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD), ook wel de 'Commissie Stiekem' genoemd.

veiligheidsonderzoek, en waarom dat niet als geschikt alternatief instrument wordt gezien.

De f-taak (AIVD) en g-taak (MIVD) zien op het verrichten van naslagen, op verzoek van aangewezen personen of instanties. Deze taak houdt in dat de AIVD en MIVD op verzoek van een externe partij een zoekslag in de eigen systemen doet. Het doel van deze naslag is om na te gaan of er bij de AIVD of MIVD informatie beschikbaar is ten aanzien van een persoon of organisatie, waaruit een mogelijke dreiging voor de nationale veiligheid blijkt. Dit betekent dat de gegevens waarin wordt gezocht al beschikbaar zijn bij de diensten en niet nieuw worden verzameld.[58] Er mag naar aanleiding van het verzoek om naslag geen onderzoek worden verricht (ook niet in open bronnen) of externe bestanden worden geraadpleegd. Wie een naslagverzoek kan doen en in welke gevallen is in de Regeling naslag Wiv 2017 opgenomen. Door aanpassing van de Regeling naslag Wiv 2017 wordt geregeld dat de Minister van OCW een naslagverzoek kan indienen, op grond van de Regeling naslag Wiv 2017.

Omdat bij naslag geen nieuwe informatie wordt verzameld zal in de meeste gevallen dan ook geen volledige inschatting van risico's op kennis- en technologieoverdracht kunnen worden gemaakt. Naslag kan wel aan de orde zijn als onderdeel van de screening kennisveiligheid, maar het vormt geen alternatief daarvoor. Het doen van een naslagverzoek is alleen mogelijk wanneer een onderzoeker of student in een positie kan komen waarin hij of zij de nationale veiligheid schade kan toebrengen. De aanvrager van het verzoek moet goed beargumenteren op welke wijze er sprake is van een specifieke situatie waarin de betreffende persoon een gevaar voor de nationale veiligheid kan vormen. Ook moet de aanvrager eerst alle beschikbare mogelijkheden zelf hebben benut om mogelijke risico's voor de nationale veiligheid te identificeren.

Hoofdstuk 3. Inhoud van het wetsvoorstel

In dit hoofdstuk wordt ingegaan op de inhoud van het wetsvoorstel aan de hand van een introductie van de screeningsplicht, de beoordeling en de behandeling van de screeningsaanvraag en de beslistermijn.

3.1. Hoofdlijnen van de screeningsplicht

Screeningsplichtigen
Met dit wetsvoorstel wordt een screeningsplicht geïntroduceerd voor eenieder die voornemens is onderzoek te gaan doen, onderwijs te volgen of geven of ondersteunende werkzaamheden van technische aard te gaan verrichten ten behoeve van dat onderzoek of onderwijs, en daarbij toegang kan krijgen tot sensitieve technologie. Deze personen zijn screeningsplichtig en worden aangeduid als de screeningsplichtige(n).

Voor het aanwijzen van sensitieve technologie is een afbakeningssystematiek ontwikkeld. In paragraaf 4.4 wordt deze systematiek toegelicht.

Ondersteunende werkzaamheden van technische aard

Het personeel is onder te verdelen in wetenschappelijk en onderwijspersoneel en ondersteunend en beheerpersoneel. Enkele voorbeelden van ondersteunende werkzaamheden van technische aard zijn: personeel dat assisteert bij de bediening of het onderhoud van apparatuur en het ICT-personeel dat systemen onderhoudt die worden gebruikt in hoog-risico onderdelen. Door het toepassingsbereik van dit wetsvoorstel te beperken tot werkzaamheden van 'technische aard', wordt afgebakend dat het niet gaat om personeel dat bijvoorbeeld administratieve taken

[58] Kamerstukken II 2016/17, 34588, 3, p. 21.

verricht, of om schoonmakers, beleidsmedewerkers of leden van het College van Bestuur die ook te scharen zijn onder ondersteunend en beheerpersoneel.

De personen die voornemens zijn te gaan werken of studeren in een technologiegebied dat niet als sensitief is aangemerkt, vallen niet onder de reikwijdte van dit wetsvoorstel.

De kennisinstelling is verplicht de screeningsplichtige op de hoogte te stellen van de screeningsplicht. Daarbij is het voornemen dat de kennisinstelling digitaal relevante informatie invult op het aanvraagformulier voor de screening en deze vervolgens digitaal doorzet naar de screeningsplichtige. De kennisinstelling zet daarmee de aanvraag voor het screeningsproces klaar voor de screeningsplichtige.

De screeningsplichtige bepaalt vervolgens zelf of hij de screening wil ondergaan. Afzien van de screening is enkel mogelijk indien screeningsplichtige tevens afziet van het voorgenomen onderzoek, de ondersteunende werkzaamheden of studie op het gebied van sensitieve technologie bij het hoog-risico onderdeel van de kennisinstelling. Als diegene de toegang toch wil krijgen, dan is de screeningsplichtige verplicht de screening te ondergaan.

De screening wordt vervolgens uitgevoerd door de rijksoverheid. De Minister van OCW is in gesprek met screeningsautoriteit Justis, als beoogd uitvoerder. Justis doet met het oog hierop een uitvoeringstoets op dit wetsvoorstel, waarna wordt bepaald of de screening voor Justis uitvoerbaar is en zo ja, of Justis de opdracht voor de uitvoerings van de screening kennisveiligheid aanneemt.

De screeningsplichtige dient het aanvraagformulier volledig en naar waarheid in te vullen en te voorzien van de bij ministeriële regeling nader te bepalen gegevens.

Wanneer de screening resulteert in de vaststelling dat er sprake is van (potentiële) risico’s voor de nationale veiligheid, dan is het de kennisinstelling niet toegestaan om de screeningsplichtige toegang te verlenen tot de sensitieve technologie en het hoog-risico onderdeel.

In de meeste gevallen zal de vraag of de screeningsplichtige toegang mag krijgen tot de sensitieve technologie en het hoog-risico onderdeel van de kennisinstelling gesteld worden naar aanleiding van een verzoek om inschrijving van een aspirant-student voor (een bepaald vak binnen) een opleiding, of naar aanleiding van een succesvolle sollicitatie van een onderzoeker of werknemer. Nadat er is geoordeeld dat de aspirant-student aan de toelatingsvereisten uit de WHW voldoet, of wanneer de selectieprocedure en sollicitatieprocedure succesvol zijn afgerond, zal de kennisinstelling een screeningsplichtige wijzen op het proces voor de screening. Het is dus uitdrukkelijk niet de bedoeling dat de kennisinstelling meer dan één kandidaat laat screenen. Dit zou niet te verenigen zijn met het streven om de noodzakelijke beperking van het recht op eerbiediging van de persoonlijke levenssfeer. Ook is het in strijd met de rechtszekerheid om twee of meer kandidaten uitzicht te bieden op de positie en de toelating en vervolgens de daadwerkelijke verlening van de positie of de toelating te laten afhangen van de uitkomst van de screening. Het is immers goed denkbaar dat meerdere kandidaten de screening met positief resultaat doorstaan. Het moet voor een kandidaat duidelijk zijn dat hij aanspraak maakt op de positie en dat hij de screening ondergaat met als doel de positie te kunnen krijgen.

De WHW geeft geen voorschriften die zien op de arbeidsrechtelijke relatie tussen onderzoekers en de kennisinstelling. Het arbeidsrecht is op deze overeenkomsten van toepassing. Een positief screeningsbesluit is verplicht voordat toegang tot het betreffende hoog-risico onderdeel kan worden verleend. De gevolgen die een negatief screeningsbesluit heeft voor de arbeidsrechtelijke relatie worden met onderhavig

voorstel niet geregeld. Die gevolgen zullen immers moeten worden bepaald aan de hand van de rechtsnormen die de relatie tussen de werkgever en de betrokkene beheersen; meestal zal het daarbij gaan om het civiele arbeidsrecht. Dit laat onverlet dat de instelling ervoor kan kiezen om of nog geen arbeidsovereenkomst aan te gaan voordat er een positief screeningsbesluit is, of een ontbindende of opschortende voorwaarde in een arbeidsovereenkomst op kan nemen. Hierdoor vervalt de arbeidsovereenkomst bij een negatief screeningsbesluit of treedt deze pas in werking bij een positief screeningsbesluit. Het arbeidsrecht is in beginsel bedoeld om de werknemer te beschermen. Dit is een ander doel dan dit wetsvoorstel beoogt.

In de Wvo is voor aangewezen vertrouwensfuncties geregeld dat personen pas toegang krijgen tot de vertrouwensfunctie nadat een VGB is afgegeven. Voor onderhavig voorstel wordt eveneens geregeld dat de kennisinstelling een persoon pas toegang tot een hoog-risico onderdeel mag verlenen nadat Onze Minister van OCW ten aanzien van die persoon met de screening kennisveiligheid een verklaring van geen bezwaar heeft afgegeven.[59] Dit laat onverlet dat de kennisinstelling de onderzoeker of werknemer kan toelaten tot een onderdeel dat niet als hoog-risico onderdeel is aangemerkt en waarvoor geen screeningsplicht geldt.

Voor de aspirant-student wordt de screening eveneens verplicht in geval van hoog-risico onderdelen. De aspirant-student wordt niet toegelaten tot het betreffende hoog-risico onderdeel van de kennisinstelling bij een negatief screeningsbesluit van de screening (een verklaring van bezwaar). Dit laat onverlet dat de kennisinstelling de aspirant-student kan toelaten tot een onderdeel dat niet als hoog-risico onderdeel is aangemerkt en waarvoor geen screeningsplicht geldt, indien aan de overige toelatingsvereisten uit de WHW is voldaan.

Beoordelingscriteria screening kennisveiligheid
Bij het nemen van het screeningsbesluit wordt uitsluitend rekening gehouden met de in dit wetvoorstel geregelde indicatoren en factoren.

Allereerst is relevant of de tegen de screeningsplichtige op grond van (internationaal) recht sancties zijn uitgevaardigd. Deze indicator moet worden meegewogen bij de bepaling van het risico of toegang van de screeningsplichtige tot een hoog-risico onderdeel van een kennisinstelling kan leiden tot een risico op overtreding van internationale sanctieregelgeving of tot een risico voor de nationale veiligheid. Ook is relevant of er een risico bestaat op het overtreden van een of meer verboden op het aanbieden van kennis over een sensitieve technologie, gesteld in een of meer bij ministeriële regeling aangewezen verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme.

Ten tweede betreft het persoonlijke gedragingen en omstandigheden, naar aanleiding waarvan betwijfeld mag worden of de screeningsplichtige een risico kan vormen voor de nationale veiligheid. Hierbij wordt onder meer gekeken naar personalia, studie- of arbeidsverleden, sociaal en wetenschappelijk netwerk, landen van verblijf, publicaties en eventuele risico's verbonden aan een partner, ouders of kinderen. Ook de wijze waarop een studie of onderzoek aan een Nederlandse kennisinstelling wordt gefinancierd en het beoogde carrièrepad van de screeningsplichtige zijn factoren die worden meegewogen. Ook is het (wetenschappelijk) netwerk van de screeningsplichtige relevant en bijvoorbeeld eerdere publicaties op het gebied van sensitieve technologie, al dan niet in samenwerking met risicovolle personen en/of instellingen.

[59] Zie artikel 4, derde lid, Wvo.

Ten derde is relevant of de screeningsplichtige banden heeft met of onder invloed staat van een statelijke actor waarvan onze Minister concrete aanwijzingen heeft dat deze sensitieve technologie tracht te verwerven. Van dergelijke banden kan ook sprake zijn via een natuurlijke persoon of rechtspersoon die banden heeft met een statelijke actor. Wat onder deze banden wordt verstaan, wordt nader uitgewerkt. Hiervan is bijvoorbeeld sprake als de screeningsplichtige nog contact onderhoudt met de statelijke actor, natuurlijke persoon of rechtspersoon. Hierbij kan ook relevant zijn of de screeningsplichtige eerder verbonden is geweest aan risicovolle of gesanctioneerde instellingen, organisaties, bedrijven of personen of een relevant militair verleden heeft.

Ten vierde is relevant of de screeningsplichtige een strafbaar feit heeft begaan. Gedragingen in het domein van de openbare orde en veiligheid kunnen relevant zijn voor de vraag of de screeningsplichtige een risico kan vormen voor de nationale veiligheid, hier wordt in paragraaf 3.2.1 en 5.1.2. nader op ingegaan.

Gesanctioneerde instellingen zijn instellingen in landen, waartegen EU-sancties zijn ingesteld, en personen die daardoor op een EU-sanctielijst vermeld staan.[60] Risicovolle instellingen zijn instellingen die bijvoorbeeld zijn te linken aan een statelijke actor of aan het militaire, inlichtingen of veiligheidsapparaat van landen met een offensief cyberprogramma, gericht tegen de veiligheidsbelangen van Nederland, de EU- en NAVO-bondgenoten. Voorbeeld van landen met een dergelijk offensief cyberprogramma zijn Rusland, China, Iran en Noord-Korea die met de dreigingsbeelden zijn aangemerkt als risicovol.[61]

Tot slot is relevant of de screeningsplichtige niet of onvoldoende heeft meegewerkt aan het onderzoek naar de hiervoor genoemde factoren. Het bewust achterhouden van informatie of het niet vermelden van eerdere activiteit op een hoog-risico onderdeel is heimelijk gedrag, en kan een indicator zijn voor een negatieve risicobeoordeling. De betrachte mate van volledigheid en waarheidsgetrouwheid bij het invullen van de screeningsaanvraag zijn factoren van belang.

De risicobeoordeling tijdens de screening
Om een goede beoordeling te maken van potentiële risico's voor de nationale veiligheid zal informatie vanuit verschillende bronnen geraadpleegd en gewogen worden. Daarnaast moet ook de informatie, die de aanvrager aanlevert, worden beoordeeld. De risico-beoordeling, die met dit wetsvoorstel wordt beoogd, valt daarmee binnen de definitie van screening van de Autoriteit Persoonsgegevens. Het is een hulpmiddel om risico's te beperken en het betreft een screening van natuurlijke personen.

Aan de hand van risico-indicatoren, onder meer gebaseerd op de dreigingsbeelden, ambtsberichten of berichten van de inlichtingen- en veiligheidsdiensten, landenspecifieke dreigingsanalyses, open bronnen, justitiële documentatie en informatie die wordt verstrekt door de screeningsplichtige zelf en de kennisinstelling, wordt beoordeeld of de toegang van de screeningsplichtige kan leiden tot een risico voor de nationale veiligheid of dat er een risico is op overtreding van de voor het verscherpt toezicht relevante verboden op technische bijstand.

De kennisinstelling maakt na het screeningsbesluit derhalve geen eigen afweging meer ten aanzien van eventuele acceptatie van de geconstateerde risico's als het gaat om verlenen van toegang tot hoog-risico onderdelen van de kennisinstelling.

De kwalificatie van de uitkomst van de screening en de wijze waarop is voorzien in rechtsbescherming
De uitkomst van de screening is een besluit in de zin van artikel 1:3, tweede lid, van de Algemene wet bestuursrecht (Awb). Hiermee is voorzien in effectieve

[60] Deze zijn te vinden via EU Sanctions Map.
[61] Zie voetnoot 14.

rechtsbescherming, zodat de screeningsplichtige in rechte voor zijn belangen en tegen het screeningsbesluit kan opkomen. Het screeningsbesluit is daarmee een voor bezwaar en beroep vatbaar besluit als bedoeld in de Awb en kan daarmee voor de Nederlandse bestuursrechter aangevochten. De screeningsplichtige ontvangt een gemotiveerd besluit en wordt met het besluit geattendeerd op zijn rechten. De screeningsplichtige kan na de bezwaarfase te hebben doorlopen ook in beroep. Het betreft beroep in eerste en enige aanleg bij de Afdeling bestuursrechtspraak van de Raad van State (ABRvS). Dit komt de snelheid waarmee screeningsplichtigen een finale rechtelijke uitspraak tegemoet kunnen zien, ten goede. Zie verder de artikelsgewijze toelichting bij artikel 22 van dit voorstel.

3.2. De behandeling van de aanvraag voor een screening kennisveiligheid

De screening wordt aangevraagd door de screeningsplichtige. De kennisinstelling draagt zorg voor het laten plaatsvinden van de screening. Hiervoor start de kennisinstelling het aanvraagproces door optioneel en indien van toepassing relevante informatie[62] in te vullen op het aanvraagformulier en dit formulier vervolgens toe te sturen naar de screeningsplichtige.

De screeningsplichtige besluit vervolgens zelfstandig of de screening kan worden gestart door het aanvraagformulier verder in te vullen, de bewijsstukken (zoals bijvoorbeeld een kopie van het identiteitsbewijs, het curriculum vitae, diploma's en publicatielijsten) toe te voegen en de aanvraag in te dienen. Na ontvangst zal de screeningautoriteit zowel aanvrager als de kennisinstelling een ontvangstbevestiging sturen (artikel 4:3a van de Awb).

De aanvraag wordt in behandeling genomen indien deze volledig is ingevuld en is voorzien van de gevraagde (bewijs)stukken. Is de aanvraag incompleet dan wordt een herstelmogelijkheid geboden waarbij de aanvrager in de gelegenheid wordt gesteld de aanvraag aan te vullen. Wordt het gebrek niet hersteld, dan wordt de aanvraag niet in behandeling genomen.[63]

3.2.1. De beoordeling van de screeningsaanvraag

Is er sprake van een volledige aanvraag, dan wordt deze in behandeling genomen en vangt een eerstelijns risicobeoordeling aan.

Eerstelijns risicobeoordeling
De eerstelijns risicobeoordeling bestaat uit een aantal stappen:

1: Controle van de volledigheid en authenticiteit van de aangeleverde gegevens en raadpleging justitiële gegevens
De beoordeling omvat allereerst een controle op de volledigheid van de door screeningsplichtige aangeleverde publicatielijst. Het kan immers relevant zijn of sprake is van eerdere publicaties op risicovakgebieden met risicovolle personen en/of instellingen. De volledigheid van de publicatielijst is noodzakelijk om dit te kunnen beoordelen. In aanvulling daarop wordt, indien van toepassing, ook de authenticiteit gecontroleerd van de aangeleverde bewijsstukken, en worden justitiële gegevens geraadpleegd.

2: Controle op (potentieel) risico op overtreding van de relevante EU-sanctieverordeningen en de relevante verboden op het verlenen van technische bijstand

[62] Onder relevante informatie wordt bijvoorbeeld verstaan informatie die van belang is voor de voorgenomen aanstelling of toelating, en adequate informatie over de aard van het door de kandidaat te verrichten onderzoek alsook tot welke (facultaire) systemen en of data, onderzoeksruimtes en onderzoeksapparatuur de kandidaat toegang zal verkrijgen.
[63] Gelet op artikel 4:5 van de Awb.

Het beoordelingsproces voor het huidige verscherpt toezicht, dat na inwerkingtreding van dit wetsvoorstel als apart instrument niet meer bestaat, zal eerst worden doorlopen. Bij de eerstelijns beoordeling wordt bekeken of toegang tot het betreffende hoog-risico onderdeel moet worden geweigerd omdat de screeningsplichtige voorkomt op internationale, door Nederland erkende sanctielijsten, en of de toegang tot een hoog-risico onderdeel van een kennisinstelling kan leiden tot een risico op overtreding van één meer verboden op het aanbieden van kennis over een sensitieve technologie, gesteld in een of meer van de bij ministeriële regeling aangewezen sanctieverordeningen.[64] Als uit de onder stap 1 beschreven informatie blijkt dat er een potentieel risico bestaat op het overtreden van de verboden op technische bijstand uit de bij ministeriële regeling aangewezen sanctieverordeningen, kan dit reeds een reden zijn om met het screeningsbesluit een verklaring van bezwaar af te geven.

3. Controle op (potentieel) risico voor de nationale veiligheid
Is van bovenstaande geen sprake, of wordt geen potentieel risico op overtreding van de verboden op het verlenen van technische bijstand geconstateerd, dan wordt als tweede stap beoordeeld of ten aanzien van de aanvrager redenen zijn om een (potentieel) risico voor de nationale veiligheid vanwege een risico op ongewenste kennis- en technologieoverdracht te vermoeden. Op dit moment in de beoordeling wordt, indien dit nog niet heeft plaatsgevonden, een controle gedaan op de volledigheid van de door aanvrager aangeleverde publicatielijst. Ook wordt gekeken naar het studie- en arbeidsverleden en worden justitiële gegevens geraadpleegd. Hierbij kan gebruik worden gemaakt van voor publiek toegankelijke bronnen.

Relevant kan zijn of de betrokkene eerder verbonden is geweest aan of onder invloed heeft gestaan van risicovolle of gesanctioneerde instellingen, bedrijven of personen. Wanneer dit nog niet heeft plaatsgevonden wordt ook gekeken naar publicaties. Tevens wordt gekeken naar landen van eerder verblijf, de wijze van financiering van de onderzoeks- of studieplek en eventuele risico's verbonden aan de partner en/of ouders.

Ook gedragingen in het domein van de openbare orde en veiligheid kunnen relevant zijn voor de risico-beoordeling. Bij ministeriële regeling zullen de relevante strafbare feiten uitputtend worden opgesomd en toegelicht. De meeste strafbare feiten zijn niet relevant voor de beoordeling van een potentieel risico op ongewenste kennis- en technologieoverdracht en worden niet betrokken bij de risico-beoordeling zoals bedoeld in deze wet. Het gebruik van justitiële gegevens ten behoeve van de screening wordt noodzakelijk geacht om een gedegen risico-beoordeling te kunnen maken. Bij het gebruik van justitiële gegevens gaat het expliciet niet om alle justitiële informatie, maar uitsluitend om die informatie die relevant is voor de beoordeling of er sprake kan zijn van een risico op ongewenste kennis- en technologieoverdracht en daarmee van een risico voor de nationale veiligheid. Het kan bijvoorbeeld gaan om veroordelingen voor misdrijven tegen de veiligheid van de staat, schending van ambtsgeheimen, valsheid in geschrift, fraude en diefstal. Indien justitiële gegevens niet kunnen worden meegewogen in de screening, kan mogelijk relevante informatie niet betrokken worden bij de risico-beoordeling van de screening kennisveiligheid. Dit maakt de screening kennisveiligheid minder effectief en levert mogelijk risico's voor de nationale veiligheid op. Bijvoorbeeld wanneer achteraf blijkt dat een onderzoeker of student door de screening is gekomen, maar dat sprake is van een relevante veroordeling die van invloed had kunnen zijn op de risicobeoordeling. De beschikking over justitiële gegevens heeft tot slot ook een signaalfunctie en een preventieve werking.

[64] Het betreft verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme.

Het gebruik van Ecris(-TCN)
Het Europees strafregistersysteem bestaat uit twee onderdelen, namelijk Ecris en Ecris-TCN. Het gebruik van Ecris(-TCN) is noodzakelijk ten behoeve van een betere informatie positie ten aanzien van een deel van de doelgroep, te weten Unieburgers en derdelanders. Dit deel van de doelgroep heeft een internationale karakter, het zal geregeld voorkomen dat zij al eerder hebben gereisd en mogelijk al eerder hebben verbleven in de EU. Dit maakt informatie uit Ecris(-TCN) relevant. De omstandigheden van het geval zullen altijd worden betrokken bij de beoordeling of een eerdere veroordeling meeweegt bij de risico-beoordeling. Zo kan diefstal niet relevant zijn als het gaat om een winkeldiefstal, maar wel relevant zijn als het gaat om diefstal van (gevoelige) informatie. Nadat een strafbaar feit relevant is geacht en is aangewezen met het wetsvoorstel moet in een concreet geval nog een afweging worden gemaakt of het strafbare feit daadwerkelijk relevant is voor het beoordelen op risico's voor de nationale veiligheid.

Indien is geconstateerd dat de onderzoeker of student in het verleden is veroordeeld voor een strafbaar feit en het strafbare feit is opgenomen bij ministeriële regeling, moet een afweging worden gemaakt of het strafbare feit daadwerkelijk relevant is voor het beoordelen op potentiële risico's op ongewenste kennis- en technologieoverdracht en daarmee de nationale veiligheid. Bij de beoordeling of een strafbaar feit daadwerkelijk meeweegt bij de risico-beoordeling moeten de omstandigheden van het geval en de aard van het strafbare feit worden betrokken. Zo kan diefstal niet relevant zijn als het gaat om een winkeldiefstal, maar zal diefstal wel relevant zijn als het gaat om diefstal van (gevoelige) informatie, zoals bedrijfsgeheimen.

Tot slot kan in dit verband ook de door aanvrager betrachte mate van volledigheid en waarheidsgetrouwheid bij het invullen van de screeningsaanvraag relevant zijn. Ook het bewust achterhouden van informatie of het niet vermelden van een eerdere activiteit op een risicovakgebied is heimelijk gedrag, en kan een indicator zijn voor een negatieve risicobeoordeling.

Uitkomsten eerstelijns risicobeoordeling
Indien reeds in de eerstelijns beoordeling wordt geconstateerd dat zich bij toelating van aanvrager tot het hoog-risico onderdeel van de kennisinstelling risico's op overtreding van de verboden op technische bijstand uit de relevante sanctieverordeningen of voor de nationale veiligheid zullen voordoen, volgt een screeningsbesluit waarmee dit wordt vastgesteld. Het screeningsbesluit bevat in dat geval een verklaring dat uit een oogpunt van de sanctienaleving of de nationale veiligheid bezwaar bestaat tegen toelating van de screeningsplichtige tot het hoog-risico onderdeel bij de kennisinstelling.

Als met de screening geen risico's geconstateerd worden op overtreding van de verboden op technische bijstand uit de relevante sanctieverordeningen of voor de nationale veiligheid en er evenmin indicaties voor nader onderzoek aanwezig zijn geacht, dan volgt eveneens een screeningsbesluit op de aanvraag. Het screeningsbesluit bevat in dat geval een verklaring dat uit een oogpunt van de sanctienaleving of de nationale veiligheid geen bezwaar bestaat tegen toelating van de screeningsplichtige tot het hoog-risico onderdeel bij de kennisinstelling.

Indien ten aanzien van aanvrager indicaties voor nader onderzoek worden geconstateerd, dan vindt dat nader onderzoek plaats in een tweedelijns risicobeoordeling.

Tweedelijns risicobeoordeling
Dit tweedelijns onderzoek betreft een nadere analyse van de eerdere bevindingen, bijvoorbeeld door middel van (persoonsgericht) openbronnenonderzoek of technische

duiding door experts.[65] Tevens bestaat er een mogelijkheid tot het afnemen van een interview met de aanvrager. In enkele gevallen kan het noodzakelijk zijn om nadere informatie mondeling te vragen en verkrijgen in de vorm van een interview, bijvoorbeeld in geval van onduidelijkheden over een curriculum vitae. Er kan tot slot een verzoek tot naslag worden gedaan bij de inlichtingen- en veiligheidsdiensten. Dit is nader toegelicht in paragraaf 2.6.

De verzamelde informatie wordt gebruikt voor de risico-beoordeling, belangenafweging en de beoordeling of sprake is van mogelijke risico's voor de nationale veiligheid vanwege ongewenste kennis- en technologieoverdracht of vanwege overtreding van de relevante verboden op technische bijstand uit de sanctieverordeningen. In deze afweging, die maatwerk betreft en waarbij alle relevante omstandigheden van het geval worden meegenomen, wordt het belang van het individu en van de kennisinstelling gewogen tegen het belang van de Nederlandse staat om de nationale veiligheid te beschermen.

Uitkomsten tweedelijns risicobeoordeling
Indien in de tweedelijns risicobeoordeling wordt geconstateerd dat er potentiële risico's op overtreding van de verboden op technische bijstand uit de relevante sanctieverordeningen of voor de nationale veiligheid voordoen, volgt een screeningsbesluit waarmee dit wordt vastgesteld. Het screeningsbesluit bevat in dat geval een verklaring dat uit een oogpunt van naleving van de sanctieverordeningen of de nationale veiligheid bezwaar bestaat tegen toelating van de screeningsplichtige tot het hoog-risico onderdeel bij de kennisinstelling.

Worden ten aanzien van de aanvrager bij toelating tot het hoog-risico onderdeel van de kennisinstelling geen risico's voortvloeiende uit de relevante sanctieverordeningen of voor de nationale veiligheid geconstateerd, dan volgt eveneens een screeningsbesluit.

Indien sprake is van een risico op overtreding van de relevante sanctieverordeningen, dan vormt de beoordeling dat toelating van de student of onderzoeker een schending oplevert van internationale sanctieregelgeving en het verbod op technische bijstand een aparte afwijzingsgrond. Indien echter naast schending van sanctieregelgeving tevens een potentieel risico voor de nationale veiligheid vanwege een risico op ongewenste kennis en technologieoverdracht wordt geconstateerd, dan worden beide afwijzingsgronden gebruikt in het screeningsbesluit. Het is immers denkbaar dat zowel een risico op overtreding van de sanctiewet- en regelgeving als een risico voor de nationale veiligheid wordt geconstateerd.

Voor de screening kennisveiligheid is de regering voornemens een terugkijktermijn van tien jaar te hanteren, omdat sprake is van toegang tot kennis en technologie waarvoor hoge veiligheidseisen gelden. Personen die deze toegang krijgen zullen de beschikking hebben over informatie (kennis en technologie) die de nationale veiligheid kan schaden. Dit wordt in afstemming met de uitvoeringsorganisatie nader uitgewerkt en vastgelegd in een ministeriële regeling.

3.2.2. Beslistermijn

Indien een aanvraag voor een screeningsbesluit volledig is, neemt Onze Minister zo spoedig mogelijk, doch uiterlijk binnen vier weken na ontvangst van de aanvraag een screeningsbesluit. In de meeste gevallen zal de doorlooptijd korter zijn dan vier weken,

[65] Technische duiding kan worden ingezet wanneer onduidelijkheid bestaat over bijvoorbeeld de aard van de activiteiten die de aanvrager zal gaan uitvoeren, over hetgeen de aanvrager eerder aan kennis heeft opgedaan, of over de inhoud van het onderdeel van de studie of het onderzoek waaraan de aanvrager zal deelnemen. Dit houdt in dat informatie kan worden ingewonnen bij experts op het betreffende vakgebied.

met name in de gevallen waarin na de eerstelijns beoordeling blijkt dat er geen reden is voor nader onderzoek.

De termijn voor het nemen van een screeningsbesluit kan worden verlengd met een redelijke termijn, doch uiterlijk met vier weken. Een verlenging is slechts aan de orde wanneer nader onderzoek noodzakelijk is voor het nemen van het screeningsbesluit.

De beslistermijn kan na aanvang van de screening worden opgeschort met ingang van de dag waarop wordt verzocht om aanvullende informatie, tot de dag waarop de verzochte informatie is verstrekt. De beslistermijn wordt dan onderbroken. In dat geval geldt de wettelijke beslistermijn plus de periode waarin aan de voorwaarden voor opschorting is voldaan.

3.2.3. De bekendmaking van het screeningsbesluit

Nadat de screening is afgerond ontvangt de screeningsplichtige een screeningsbesluit. Het screeningsbesluit bevat een verklaring dat uit een oogpunt van nationale veiligheid en de naleving van internationale sancties geen bezwaar, dan wel bezwaar, bestaat tegen toelating van de screeningsplichtige tot het hoog-risico onderdeel bij de kennisinstelling, met een motivering. Zoals aangegeven in paragraaf 3.1 kan de student of onderzoeker rechtsmiddelen aanwenden tegen het screeningsbesluit.

Ook de kennisinstelling ontvangt bericht over de uitkomst van de screening. De kennisinstelling ontvangt niet het gemotiveerde screeningsbesluit, maar alleen de mededeling dat er vanuit een oogpunt van nationale veiligheid en sanctieregelgeving geen bezwaren, dan wel bezwaren zijn tegen toelating van betrokkene tot het hoog-risico onderdeel van de instelling. Het is aan de student of onderzoeker om te bepalen of hij het volledig gemotiveerde screeningsbesluit aan de kennisinstelling overlegt.

Hoofdstuk 4. Reikwijdte van het wetsvoorstel

De reikwijdte van het wetsvoorstel wordt bepaald door meerdere elementen: welke kennisinstellingen vallen onder het wetsvoorstel; welke individuen zijn screeningsplichtig; wat wordt verstaan onder nationale veiligheid en daarmee samenhangend welke sensitieve (sub)technologieën en hoog-risico onderdelen daarbinnen vallen onder het bereik van het wetsvoorstel. Deze elementen worden hierna besproken.

4.1 Kennisinstellingen

Het wetsvoorstel richt zich op het voorkomen van ongewenste kennis- en technologieoverdracht via Nederlandse kennisinstellingen op het gebied van risico's voor de nationale veiligheid en het naleven van de relevante sanctieverordeningen. Het wetsvoorstel heeft in de eerste plaats betrekking op bekostigde en niet-bekostigde instellingen als bedoeld in de WHW, voor zover zich bij deze instellingen sensitieve technologie bevindt (universiteiten, hogescholen en academische ziekenhuizen). In de tweede plaats heeft het betrekking op de instellingen voor toegepast onderzoek (zogenoemde TO2-instellingen), en KNAW- en NWO(-I)- en andere instituten, voor zover zich daar sensitieve technologie bevindt. Voornoemde kennisinstellingen, niet zijnde bedrijven, waar sensitieve technologie aanwezig is, vallen daarmee onder de werking van deze wet. In de begripsbepaling en de eerste bijlage bij het wetsvoorstel zijn de kennisinstellingen genoemd die onder de werking van dit wetsvoorstel vallen. Het voorstel maakt het mogelijk om nieuwe instellingen in de bijlage op te nemen (artikel 2). Dit kan wenselijk zijn als er bijvoorbeeld een nieuwe instelling tot de TO2-federatie toetreedt.

4.2. Screeningsplichtige personen

De huidige doelgroepafbakening betreft, zoals hiervoor aangegeven, eenieder die als onderzoeker of student toegang wil krijgen tot een hoog-risico onderdeel van de kennisinstelling waar sensitieve technologie aanwezig is, ongeacht nationaliteit of verblijfsstatus. Dit vormt een wijziging ten opzichte van het aanvankelijke voornemen om alleen personen van buiten de EU/EER, die een verblijfsrecht voor studie of onderzoek nastreven, te screenen. Hiervoor is om verschillende redenen gekozen. In de eerste plaats wordt hiermee het risico van (indirecte) discriminatie zoveel mogelijk beperkt. In de tweede plaats kunnen, kijkend naar de dreigingsbeelden, risico's voor de nationale veiligheid uitgaan van personen van alle nationaliteiten en ongeacht verblijfstatus. Hiermee wordt tevens de kans op het verschuiven van risico's beperkt.

1. Het risico op (in)directe discriminatie beperken
Met de huidige doelgroepafbakening wordt er geen onderscheid gemaakt naar nationaliteit of verblijfstatus. Er wordt wel onderscheid gemaakt tussen studenten en onderzoekers die actief willen zijn op een vakgebied waarbij toegang bestaat tot (onderdelen van) sensitieve technologie, en studenten en onderzoekers die actief willen zijn op andere vakgebieden. De eerstgenoemde groep kan worden gescreend, de tweede groep niet. Indien sprake is van een verschil in behandeling, dient beoordeeld te worden of er sprake is van vergelijkbare gevallen. Alleen dan dient het onderscheid gerechtvaardigd te worden, en kan sprake zijn van (in)directe discriminatie. Gelet op het feit dat met de screening specifiek wordt beoogd om potentiële risico's voor de nationale veiligheid te beperken, en deze risico's niet of in aanzienlijk mindere mate aanwezig zijn op onderdelen waar niet gewerkt wordt met sensitieve technologie, gaat het hier naar het oordeel van de regering niet om vergelijkbare gevallen.

2. Dreigingsbeelden
Uit de dreigingsbeelden volgt dat de dreiging voornamelijk afkomstig is van statelijke actoren van buiten de EU/EER. Daarmee is de dreiging niet per definitie of uitsluitend enkel afkomstig van derdelanders die verblijf beogen op grond van studie of onderzoek. Ook onder Unieburgers, waaronder Nederlanders, kan een risico op ongewenste kennisoverdracht bestaan. Nationaliteit en verblijfsstatus is immers niet de exclusieve factor. In geval van Nederlanders en Unieburgers kan ook een risico bestaan dat de betreffende onderzoeker of student door een statelijke actor wordt "verleid" om de verkregen kennis te delen. Ook volgt uit de dreigingsbeelden dat buitenlandse vormen van beïnvloeding en inmenging zich vaak richten op diasporagemeenschappen en op opposanten (bijvoorbeeld critici of politieke dissidenten) van buitenlandse overheden. Een statelijke actor ontplooit beïnvloedings- en inmengingsactiviteiten om zijn doelwit zodanig te beïnvloeden, dat het doelwit zich solidair verklaart met de politieke doelstellingen van de statelijke actor – of door solidair gedrag af te dwingen.

Zoals het eerste dreigingsbeeld (DBSA1) schetste, kunnen beïnvloedings- en inmengingsactiviteiten verschillende openlijke en heimelijke vormen aannemen, van beïnvloeding via (des)informatiecampagnes, tot intimidatie of bedreiging en zelfs tot het toepassen van geweld en liquidatie. Iran, China en Rusland ontplooien uiteenlopende inlichtingen- en beïnvloedingsactiviteiten, onder meer gericht op hun diaspora in Nederland. Beïnvloeding van diaspora kan iedereen betreffen, waarbij nationaliteit of verblijfsstatus geen onderscheidende factor is. Binnen de diasporagemeenschappen bestaat veelal een noodzaak om toegang tot het land van herkomst te behouden, vanwege nog daar wonende familie en aanwezige bezittingen. Ook is er een band met het herkomstland vanwege culturele en religieuze behoeften. Statelijke actoren kunnen hier gebruik en misbruik van maken en impliciete of expliciete druk leggen op diasporagemeenschappen om zich te conformeren. Dit conformisme kan verschillende vormen aannemen: van zelfcensuur in het politieke debat tot het actief meewerken met inlichtingendiensten.

Dat nationaliteit geen onderscheidende factor is in geval van risico's op beïnvloeding blijkt bijvoorbeeld – buiten de diasporagemeenschappen om – ook wanneer sprake is van derdelanders die reeds in het bezit zijn van een andere vorm van verblijfsrecht, bijvoorbeeld verblijf bij familie of op grond van een asielvergunning of wanneer de derdelander inmiddels de Nederlandse nationaliteit of de nationaliteit van een andere EU-lidstaat heeft verkregen. Ook dan kan de persoon in kwestie langdurig gewoond of gewerkt hebben in een derdeland of affiliaties hebben met een statelijke actor, waardoor van de persoon een risico kan uitgaan. Hetzelfde geldt voor Unieburgers die zich in een vergelijkbare situatie bevinden. Verder kan sprake zijn van een dubbel paspoort.

Derdelanders die verblijf beogen of reeds in het bezit zijn van een verblijfsvergunning op andere gronden dan studie of onderzoek, zoals verblijf bij familie, partner, of op grond van een asielvergunning, zouden aanvankelijk buiten de doelgroep vallen. Door de keuze voor de huidige doelgroepafbakening vallen ook zij onder de screeningsplicht. Dit doet recht aan de dreigingsbeelden en de doelen van dit wetsvoorstel.

Tot slot vallen derdelanders die gebruik maken van het recht op intra EU-mobiliteit nu ook onder de screeningsplicht. Het betreft hier derdelanders die in een andere EU-lidstaat reeds verblijfsrecht hebben verkregen en van hun recht op mobiliteit binnen de EU gebruik maken door aan een Nederlandse kennisinstelling een masterstudie te volgen dan wel (gast)onderzoek doen. Met de aanvankelijk voorgenomen doelgroepafbakening van derdelanders die verblijf beogen als onderzoeker of student zouden deze groepen buiten de screeningsplicht vallen.

Ook bij andere screeningsinstrumenten wordt geen onderscheid gemaakt naar nationaliteit, zoals bij het verscherpt toezicht op basis van sanctiewet- en regelgeving. Daarbij wordt iedereen, ongeacht nationaliteit of verblijfsstatus, getoetst. De doelgroepafbakening past bij de aard van de risico's die dit wetsvoorstel beoogt te voorkomen en te mitigeren. Dit leidt tot minder restrisico's en tot het verminderen van mogelijke routes tot omzeiling van de screeningsplicht. Dit heeft tot gevolg dat met de huidige doelgroepafbakening minder restrisico's voor de nationale veiligheid bestaan. Dat voor een deel van de doelgroep geldt dat er niet gelijk op voorhand sprake is van potentiële risico's voor de nationale veiligheid, doet er niet aan af dat screenen noodzakelijk is. Allereerst is het inherent aan screening dat het aantal screeningsplichtigen altijd hoger zal zijn dan het aantal personen waarbij wordt geconcludeerd dat sprake kan zijn van het risico wat de screening beoogt te voorkomen en mitigeren, in dit geval een potentieel risico voor de nationale veiligheid.

In hoofdstuk 9 wordt stilgestaan bij de impact op het individu, de kennisinstellingen en de wetenschap.

4.2.1. Onderzochte alternatieve doelgroepafbakening

4.2.1.1 Screenen voorafgaand aan en met het oog op de verblijfsrechtelijke procedure
Bij het ontwerp van dit wetsvoorstel was het voornemen aanvankelijk om alleen onderzoekers en studenten uit derdelanden (landen van buiten de EU en EER) te screenen, *voorafgaand aan* en *met het oog op* een eventuele verblijfsrechtelijke procedure voor studie of onderzoek. Deze variant leek proportioneel en doelmatig in het licht van de dreigingsanalyses. Bij de aanvraag om toelating tot Nederland op grond van een verblijfsvergunning bepaalde tijd verleend onder de beperking van studie of onderzoek (EU-Richtlijn 2016/801) of bij de aanvraag van een visum kortverblijf met het oog op onderzoek en studie op een hoog-risico onderdeel van de kennisinstelling waar sensitieve technologie aanwezig is, zou dan een screeningsbesluit moeten worden overgelegd.

De doelgroepafbakening is een essentieel onderdeel van het wetsvoorstel en bepaalt (mede) het toepassingsbereik van de screening. Vanuit het oogpunt van het voorkomen van discriminatie, zorgvuldigheid en uitvoerbaarheid is het noodzakelijk dat de juridische

houdbaarheid van de gekozen doelgroepafbakening boven alle twijfel is verheven. Om die reden is in november 2023 het College voor de Rechten van de Mens (hierna: het College) gevraagd om een advies over de doelgroepafbakening in geval van derdelanders. In april 2024 bracht het College een advies uit, dat in juli 2024 door het College op één onderdeel is gewijzigd. Uit het advies blijkt dat het College betwijfelt of het Unierecht voldoende ruimte laat voor een screening voorafgaand aan en met het oog op een aanvraag voor een verblijfsvergunning. Dit advies gaf niet op alle elementen, specifiek ten aanzien van de uitleg van het Unierecht, volledig uitsluitsel. Daarom is een *second opinion* over het Unie- en vreemdelingenrechtelijke deel van dit advies gevraagd aan de Landsadvocaat.

Aan het College en de Landsadvocaat is als belangrijkste vraag voorgelegd of – kort gezegd - EU-Richtlijn 2016/801 (hierna: de Richtlijn) de ruimte biedt om een screening *voorafgaand aan en met het oog op* de verblijfsrechtelijke procedure te laten plaatsvinden. De conclusie van het advies is dat de Landsadvocaat net als het College betwijfelt of de Richtlijn een grondslag biedt voor een screeningsplicht voorafgaand aan een aanvraag voor een verblijfsvergunning.

Er bestaat in de eerste plaats een risico dat een rechter de screeningsplicht zal aanmerken als extra voorwaarde voor toelating, bovenop de voorwaarden die in Richtlijn 2016/801 zijn opgenomen met als gevolg dat deze onverbindend is. De Richtlijn schrijft namelijk uitputtend voor welke voorwaarden mogen worden gesteld. De Richtlijn laat geen extra toelatingsvoorwaarden toe. In de tweede plaats betwijfelt de Landsadvocaat of de ruime beoordelingsmarge waarover een lidstaat beschikt bij de beoordeling van de vraag of een derdelander een bedreiging voor – in dit geval – de openbare veiligheid wordt geacht te vormen[66], het de lidstaten toestaat om van derdelanders te verlangen dat zij voorafgaand aan de aanvraag een screeningsplicht ondergaan om te bewijzen dat geen sprake is van (vrees voor) een bedreiging voor de openbare veiligheid. De huidige rechtspraak biedt daarvoor geen aanknopingspunten.

Dit betekent dat een screening voorafgaand aan en met het oog op een aanvraag voor een verblijfsvergunning als student of onderzoeker juridisch te kwetsbaar is gebleken.

4.2.1.2 Screenen tijdens de verblijfsrechtelijke procedure
Een variant van screening van derdelanders *tijdens de verblijfsprocedure* als variant is ook afgevallen, omdat het risico bestaat dat de rechter ook in dat geval de screening aanmerkt als een verboden extra toelatingsvoorwaarde, net als bij de screening *voorafgaand aan en met het oog op* de verblijfsprocedure.[67]

Hierdoor is screenen van derdelanders op generieke wijze niet mogelijk. Screenen op niet generieke wijze – waar de genoemde Richtlijn wel een grondslag voor biedt - zou een screening kunnen zijn op basis van signalen. Er zal dan sprake moeten zijn van meerdere indicatoren of 'rode vlaggen' die wijzen op (potentiële) risico's voor de nationale veiligheid, indien betrokkene toegang zou krijgen tot een hoog-risico onderdeel waar sensitieve technologie aanwezig is. Met deze werkwijze is het twijfelachtig in welke gevallen dan nog mag worden gescreend. Ook kan dit leiden tot meerdere omzeilroutes en bijbehorende restrisico's, waardoor het doel van de preventieve screening niet wordt behaald. Ook worden bij het uitvragen van aanvullende informatie al snel (bijzondere) persoonsgegevens gevraagd, verwerkt en beoordeeld, waardoor snel sprake zal zijn van screenen. Om te kunnen bepalen of er bepaalde indicatoren of 'rode vlaggen' zijn, moeten deze gegevens namelijk worden verwerkt en van een risicobeoordeling worden

[66] Artikel 7, zesde lid, van de Richtlijn. Derdelanders kunnen op grond van genoemd artikel ook worden geacht een gevaar voor de openbare orde, of volksgezondheid te vormen. Onder openbare veiligheid wordt nationale veiligheid verstaan.
[67] Advies Landsadvocaat van 19 november 2024, punt 3.22.

voorzien. Ook leidt het gebruik van 'rode vlaggen' voorafgaand aan het starten van een screening mogelijk tot ongerechtvaardigd onderscheid (indirecte discriminatie).[68]

4.2.1.3 Overige varianten doelgroepafbakening
Tot slot wordt hier volledigheidshalve nog ingegaan op de overige varianten die in het voortraject zijn onderzocht voordat het voornemen was ontstaan om de doelgroep af te bakenen tot derdelanders. Deze varianten betreffen het screenen van alleen onderzoekers en studenten afkomstig uit bepaalde aan te wijzen 'risicolanden' of het enkel screenen in geval van studenten en onderzoekers die voldoen aan een 'risicoprofiel'.

Risicolanden
Het screenen van alleen personen uit 'risicolanden' is juridisch te kwetsbaar en beleidsmatig onwenselijk gebleken. Het beperken van de screening tot personen uit risicolanden staat naar het oordeel van de regering op gespannen voet met het discriminatieverbod en kan leiden tot stigmatisering.[69] Deze variant doet ook geen recht aan de dreigingsanalyses waaruit volgt dat nationaliteit op zichzelf geen bepalende factor is. Een toekomstbestendige aanpak wordt hiermee ook niet bewerkstelligd.

Risicoprofiel
Bij een screening op basis van een risicoprofiel zou voordat de screening aanvangt een selectie gemaakt moeten worden of een persoon voldoet aan één of meerdere kenmerken uit dat risicoprofiel. Dit betekent dat of een screeningsautoriteit of de kennisinstelling deze selectie op basis van het profiel zou moeten maken. Wanneer de screeningsautoriteit deze selectie zou moeten maken, komt dit er in de praktijk op neer dat alsnog iedereen, ongeacht nationaliteit of verblijfsstatus, een vragenlijst zou moeten invullen en gegevens zou moeten aanleveren om te kunnen beoordelen of sprake is van kenmerken die voldoen aan het risicoprofiel. Dit heeft tot gevolg dat een screeningsautoriteit iedereen, ongeacht nationaliteit of verblijfsstatus, aan deze beoordeling zou moeten onderwerpen. De beoordeling of er sprake is van het voldoen aan een risicoprofiel als alternatief overlaten aan de kennisinstellingen zelf is eveneens te kwetsbaar. Dit leidt mogelijk tot willekeur en rechtsongelijkheid doordat de kennisinstellingen hier verschillend mee omgaan.

Daarnaast is deze variant juridisch kwetsbaar en beleidsmatig onwenselijk gebleken. In geval van deze variant zou bijvoorbeeld gebruik worden gemaakt van neutrale kenmerken en een risicoprofiel om het onderscheid op te baseren. Dit zou bijvoorbeeld moeten gaan om het land van studie, (langdurig) verblijf of het volgen van een opleiding in een ander land. Hierbij zal al snel sprake zijn van indirecte discriminatie op grond van nationaliteit.[70]

4.2.2. Uitzonderingen op de doelgroep

Er is sprake van drietal uitzonderingen op de gekozen doelgroep zoals hiervoor omschreven.

[68] Van indirecte discriminatie is sprake wanneer een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze personen met een bepaalde nationaliteit in vergelijking met personen met een andere nationaliteit bijzonder benadeelt. Een voorbeeld: als een screening bijvoorbeeld plaatsvindt ten aanzien van personen die recentelijk een studie in een risicoland hebben afgerond of het grootste deel van hun opleiding in een risicoland hebben genoten, dan wordt daarmee niet rechtstreeks verwezen naar de nationaliteit van die persoon en is er geen sprake van directe discriminatie. Maar aangezien naar alle waarschijnlijkheid met name personen met de nationaliteit van dat land aan universiteiten in dat land studeren, leidt dit wel tot indirecte discriminatie.
[69] Zie uitspraak van de Hoge Raad van 14 december 2012, ECLI:NL:HR:2012:BX8351, inzake de Sanctieregeling Iran 2007.
[70] Zie voetnoot 28.

Bachelorstudenten in beginsel uitgezonderd
Niet alle studenten vallen onder de werking van onderhavig wetsvoorstel. Studenten kunnen in beginsel pas in aanraking komen met sensitieve technologie vanaf de masterfase van bepaalde studies. In de bachelorfase is de lesstof in de regel niet als sensitief aan te merken. In deze fase wordt ervan uitgegaan dat lesstof niet vernieuwend is en daarnaast algemeen toegankelijk is. Bachelorstudenten zijn dan ook in beginsel uitgezonderd van de screening. De screening ziet in geval van studenten hoofdzakelijk op masterstudenten. Uitzondering hierop zijn specifieke studentenprojecten. Bachelorstudenten kunnen ook deelnemen aan studentenprojecten die als hoog-risico onderdelen waar sensitieve technologie aanwezig is kunnen worden gezien. In dat geval kan screening aan de orde zijn voor de betreffende bachelorstudent.

Zittende studenten en onderzoekers
Er is sprake van een grote groep onderzoekers en studenten die op het moment van inwerkingtreding van dit wetsvoorstel al werken of studeren aan een Nederlandse kennisinstelling binnen een hoog-risico onderdeel waar sensitieve technologie aanwezig. Deze groep wordt na inwerkingtreding van de wet niet alsnog gescreend.

Het alsnog screenen van deze groep na inwerkingtreding van de wet zou in de eerste plaats op gespannen voet staan met de rechtszekerheid. Ook worden eventuele risico's in deze groep ondervangen met het bredere kennisveiligheidsbeleid, waar de instellingen vorm aan geven. Verder is het ook met het oog op de uitvoerbaarheid van dit wetsvoorstel onwenselijk om deze grote groep alsnog te screenen na inwerkingtreding van de wet. Uitzondering hierop zijn onderzoekers of studenten die voor de inwerkingtreding van dit voorstel reeds zijn onderworpen aan het verscherpt toezicht. Het kan immers zo zijn dat een onderzoeker of student voor de inwerkingtreding reeds diende te beschikken over een ontheffingsbesluit van de Minister van OCW of dat reeds een risico-advies is afgegeven. Na inwerkintreding van dit voorstel is het daardoor mogelijk dat zij in het kader van kennisveiligheid aan de screening kennisveiligheid zullen worden onderworpen, ondanks een eerdere beoordeling in het kader van verscherpt toezicht. In die gevallen zal met de screening kennisveiligheid en een ongewijzigde studie of onderzoek, niet opnieuw getoetst worden aan de relevante verboden uit de sanctieregelgeving. Dit is anders wanneer zij na inwerkingtreding van het wetsvoorstel wisselen van studie of onderzoek.

Er bestaan andere wettelijke mogelijkheden of manieren om risico's in geval van deze groep onderzoekers en studenten te beperken. In geval van derdelanders en Unieburgers is het bijvoorbeeld mogelijk het verblijfsrecht in te trekken of te beperken wanneer daar een concrete aanleiding en voldoende onderbouwing voor te geven is. In geval van Nederlanders bestaat die optie niet, maar geldt dat indien sprake is van een vermoeden van ongewenste hoogwaardige kennis- en technologieoverdracht, onder omstandigheden achteraf strafrechtelijk kan worden opgetreden.

Personen die een VGB behoeven
Een onderzoeker, docent of technisch ondersteuner wordt ook niet gescreend indien voor het uitoefenen van dezelfde functie ook een VGB vereist is op grond van de Wet veiligheidsonderzoeken (Wvo). Samenloop van verschillende screeningsinstrumenten zou leiden tot extra administratieve lasten en tot een extra inbreuk op de persoonlijke levenssfeer, doordat twee organisaties elk een onderzoek verrichten. Dezelfde persoon vanuit verschillende wettelijke instrumentaria tweemaal screenen is om die reden niet wenselijk. De screening kennisveiligheid en het veiligheidsonderzoek hebben weliswaar een ander doel, maar in de enkele gevallen waarin sprake is van samenloop zal de VGB de veiligheidsrisico's die bij een vertrouwensfunctie behoren voldoende kunnen afdekken.

4.3 Wat wordt verstaan onder nationale veiligheid?

In dit wetsvoorstel wordt dezelfde definitie van nationale veiligheid als in de Wet vifo gehanteerd: nationale veiligheid ziet op het beschermen van de belangen die binnen Nederland wezenlijk zijn voor het voortbestaan van de democratische rechtsorde, voor de veiligheid of andere gewichtige belangen van de staat, of voor de instandhouding van de maatschappelijke stabiliteit. Net als in de Wet vifo wordt deze definitie wat betreft de te beschermen belangen verbonden aan de specifieke context en doelstelling van dit wetsvoorstel, door de toevoeging van de woorden 'voor zover die zien op het raakvlak tussen onderzoek en onderwijs en veiligheid'.

Nationale veiligheid wordt in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (2023) als volgt gedefinieerd: "Onder nationale veiligheid verstaan we de bescherming van onze nationale veiligheidsbelangen tegen dreigingen die deze belangen kunnen schaden en daarmee maatschappelijke ontwrichting kunnen veroorzaken."

Er is sprake van een mogelijk ontwrichtend effect op de samenleving als één of meer van de zes nationale veiligheidsbelangen ernstig worden aangetast.

De zes nationale veiligheidsbelangen zijn: territoriale veiligheid; fysieke veiligheid; economische veiligheid; ecologische veiligheid; sociale en politieke stabiliteit; en internationale rechtsorde en stabiliteit.

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.

Risico's voor de nationale veiligheid in geval van ongewenste kennis- of technologieoverdracht

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. Dit wordt ook bevestigd in de Trendanalyse Nationale Veiligheid 2024 (hierna: de Trendanalyse) en de verdieping op deze trendanalyse.[71] De Trendanalyse geeft onder meer inzicht in de technologische ontwikkelingen die de nationale veiligheid steeds meer beïnvloeden. De Trendanalyse besteedt aandacht aan de technologie-wedloop met technologie als machtsinstrument, wapen en kwetsbaarheid. Technologische ontwikkelingen gaan in grote mate de toekomstige veiligheidsomgeving beïnvloeden. Technologie biedt kansen, maar kent ook dreigingen. Niet alleen wanneer technologieën worden toegepast in bijvoorbeeld wapensystemen, maar ook heeft technologie in generieke zin op veel manieren impact op de nationale

[71] Trendanalyse Nationale Veiligheid 2024 - Hoofdrapport (clingendael.org) en Verdieping op de Trendanalyse Nationale Veiligheid 2024 | Rapport | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)
Zie ook Kamerstukken II 2023/24, 30 821, nr. 231, bijlagen.

veiligheid. In paragraaf 2.2 is ingegaan op de probleembeschrijving en de vraag wanneer sprake van ongewenste kennis- en technologieoverdracht.

Voor de definiëring van wat als sensitieve technologie moet worden gezien voor dit wetsvoorstel is op een gestructureerde manier onderzocht op welke wijze een technologie in potentie een groot risico vormt voor de nationale veiligheid. Hierbij ligt de focus op de risico's die voortkomen uit moedwillig en ongewenst (militair) gebruik of misbruik van de technologie door de inzet of dreiging van de inzet als strategisch machtsmiddel. De term sensitieve technologie wordt in dit wetsvoorstel gebruikt om te verwijzen naar technologische ontwikkelingen en toepassingen die een risico kunnen vormen voor nationale veiligheid. Vanaf paragraaf 4.4 wordt dit nader uitgewerkt.

4.4 Welke technologieën zijn sensitief en bij welke onderdelen van kennisinstellingen geldt de screeningsplicht?

4.4.1. Samenvatting

De screeningsplicht zal gelden voor aangewezen onderdelen van kennisinstellingen waar onderzoekers en studenten toegang hebben tot sensitieve technologie. Hiervoor is afgebakend wat sensitieve technologie betekent voor dit voorstel. Bij deze afbakening is gebruik gemaakt van een rijksbreed toepasbare systematiek en is ook gebruik gemaakt van de opbrengsten van consultatierondes die met het kennisveld zijn gehouden.

In het wetsvoorstel wordt een aantal technologieën en subtechnologieën aangewezen als sensitieve technologie.[72] Het wetsvoorstel voorziet in de mogelijkheid om bij algemene maatregel van bestuur nog andere (sub)technologieën aan te wijzen.[73] Tevens voorziet dit voorstel in de mogelijkheid om bij ministeriële regeling technologieën als sensitieve technologie aan te wijzen voor zover sprake is van technologieën waarvoor op grond van internationale sanctieregelgeving beperkingen gelden. Deze systematiek wordt nader toegelicht in paragraaf 4.4.5.

De aanwijzing van een technologie als sensitieve (sub)technologie, betekent nog niet dat de gehele (sub)technologie als sensitief wordt aangemerkt. Het kan ook zijn dat een gedeelte van de (sub)technologie sensitief is en overige gedeelten niet.

In de bijlage bij het algemeen deel van de toelichting is een beschrijving van de (sub)technologieën opgenomen die met dit wetsvoorstel als sensitief worden aangemerkt.

Algemeen uitgangspunt is dat technologie die reeds openbaar toegankelijk is, is uitgezonderd. Het gaat voor de toepassing van het wetsvoorstel met name om lopend onderzoek, voordat het wordt gepubliceerd of openbaar is. In geval van voor een ieder openbaar toegankelijke technologie is immers in de regel geen sprake (meer) van technologie die sensitief is en waarvoor de screening kennisveiligheid noodzakelijk is. De technologie kan dan op een legale, relatief eenvoudige wijze worden verkregen door een ieder.

Het wetsvoorstel bepaalt in verband hiermee dat de aangewezen (sub)technologieën sensitief zijn *voor zover* er wordt voldaan aan een of meer voorwaarden, die in het wetsvoorstel zijn uitgewerkt. Welke voorwaarden dit zijn wordt uitgelegd in paragraaf 4.4.4.

Met de afbakening van sensitieve technologie is nog niet bepaald waar (bij welke onderdelen van kennisinstellingen) screening aan de orde is. Dit laatste vraagt dan ook

[72] Artikel 5.
[73] Artikel 6.

om aanwijzing van de onderdelen van de kennisinstellingen waar de student of onderzoeker in aanraking kan komen met sensitieve technologie zoals afgebakend op de hiervoor beschreven manier. Binnen de in de wet opgenomen sensitieve technologieën kunnen dit (delen van) opleidingen en postinitiële masteropleidingen, projecten, programmalijnen, vakgroepen, onderzoeksgroepen, studentenprojecten of bepaalde (studenten)teams en laboratoria zijn. Deze opsomming is niet limitatief.

De kennisinstellingen krijgen de plicht om zelf vast te stellen welke onderdelen binnen de eigen instelling als hoog-risico onderdelen zijn aan te merken Hierbij vormen de in het wetsvoorstel opgenomen sensitieve technologieën en criteria de basis. Hiervoor gebruiken kennisinstellingen een door de overheid in samenspraak met het kennisveld ontwikkeld beoordelingskader. Deze werkwijze past bij de institutionele autonomie van de kennisinstellingen.

In aanvulling hierop wordt een wettelijke plicht geïntroduceerd die de kennisinstellingen verplicht om aan de minister van OCW te melden dát de vaststelling van de onderdelen heeft plaatsgevonden en wat daarvan de uitkomst is. Deze meldplicht maakt het beter mogelijk om toezicht te houden op dit proces van sensitiviteitsbeoordeling en of de kennisinstelling de plicht naleeft om tot vaststelling van hoog-risico onderdelen te komen. Bovendien creëert dit een gewenst overzicht en een betere samenhang en uniformiteit tussen de aangewezen onderdelen en daarmee een gelijk speelveld.

Tot slot dienen nieuwe onderdelen binnen een kennisinstelling op het moment van ontstaan ook te worden beoordeeld en te worden vastgesteld. Ook dient wederom gemeld te worden dat de vaststelling heeft plaatsgevonden en wat daarvan de uitkomst is. De minister van OCW houdt naar aanleiding van de meldingen een actueel en vertrouwelijk overzicht van hoog-risico onderdelen bij en zorgt middels toezicht voor samenhang tussen de aangewezen hoog-risico onderdelen. Ook wordt toezicht gehouden op het naleven van voornoemde meldplicht. In paragraaf 7 wordt op dit toezicht nader ingegaan.

4.4.2. Het begrip technologie

Het is belangrijk om bewust te zijn van de verschillende aspecten die onder de noemer ‘technologie’ kunnen vallen: de kennis als basis van de technologie, de vaardigheden om een technologisch product te vervaardigen, de instructies om het goed of het product te gebruiken of het (eind)product van de technologie. Naast de verschillende aspecten die onder de noemer ‘technologie’ kunnen vallen, wordt het begrip technologie in zijn algemeenheid ook op verschillende abstractieniveaus gehanteerd. 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 in dit voorstel is dit onderscheid soms gemaakt.

Daarnaast kan technologie gaan over een toepassing, ofwel de combinatie van een kennisgebied en een bepaalde gebruikerscontext (bijvoorbeeld autonome wapensystemen). Om tot een eenduidig abstractieniveau te komen wordt op onderdelen onderscheid gemaakt in technologiegebieden en sub-technologiegebieden, waar dit aan de orde is zal dat worden toegelicht.

In de hiernavolgende paragraaf wordt ingegaan op het proces om tot de afbakening van sensitieve technologieën in het kader van dit wetsvoorstel te komen. Daarbij wordt ingegaan op de gebruikte systematiek voor dit voorstel, een nadere duiding van het begrip technologie en de criteria die hierbij zijn betrokken. Tot slot richt een paragraaf zich op het proces rondom de vaststelling van hoog-risico onderdelen van de kennisinstellingen, de rol van de kennisinstellingen bij dit proces en wordt een systematiek geïntroduceerd voor herijking en actualisatie van de sensitieve

technologieën in het kader van dit wetsvoorstel en voor de vastgestelde hoog-risico onderdelen.

4.4.3. Gevolgde methodiek voor de afbakening van sensitieve technologieën in dit wetsvoorstel

Voor dit wetsvoorstel is eerst onderzocht welke technologieën en kennis over deze technologieën in geval van ongewenste overdracht potentieel risico's voor de nationale veiligheid met zich meebrengen. Daarbij is een nauwkeurige afbakening van belang, welke technologieën zijn zo sensitief dat ze als basis binnen de reikwijdte van het wetsvoorstel dienen te vallen. Dit waarborgt de effectiviteit en proportionaliteit van het instrument. Op risicogerichte wijze is afgewogen of een specifieke (sub)technologie grote gevolgen kan hebben voor de nationale veiligheid en in het bijzonder in geval van ongewenste overdracht van deze kennis- en technologie. Deze afbakening heeft via verschillende stappen plaatsgevonden, onder meer door de kennissector te betrekken.[74]

Voor de beoordeling of een technologische ontwikkeling of toepassing als sensitief kan worden gekwalificeerd, heeft het Analistennetwerk Nationale Veiligheid (ANV)[75] in opdracht van het ministerie van Buitenlandse Zaken, het toenmalige ministerie van Economische Zaken en Klimaat en de Nationaal Coördinator Terrorismebestrijding en Veiligheid een rijksbreed toepasbare systematiek ontwikkeld.[76] Deze systematiek maakt inzichtelijk welke technologieën mogelijk een risico vormen voor de nationale veiligheid. Met deze systematiek is de rijksoverheid beter in staat om beleid bij te sturen en bestaande instrumenten te actualiseren. Naast de systematiek is ook een begrippenkader ontwikkeld, dat als uitgangspunt kan dienen voor de systematiek. Dit faciliteert het gemeenschappelijk denken over sensitieve technologie binnen de rijksoverheid. Uitgangspunten hierbij zijn dat in de systematiek zoveel mogelijk de technologie centraal wordt gesteld (sensitiviteit als eigenschap van de technologie). Tevens is 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. Een heldere systematiek om dit soort risico's specifiek voor kennisveiligheid beheersbaar te maken is noodzakelijk gebleken. Dit start met het verkrijgen van inzicht in technologische ontwikkelingen en de potentiële risico's hiervan voor de nationale veiligheid.

Eerste stap
Samen met het ministerie van Economische Zaken en in samenspraak met de Nationaal Coördinator Terrorismebestrijding en Veiligheid in 2022 is als eerste stap advies gevraagd aan de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) om een basislijst sensitieve technologie op te stellen. TNO heeft hierbij gebruik gemaakt van de voornoemde, Rijksbreed toepasbare ANV-systematiek.

In september 2022 heeft TNO deze vertrouwelijke basislijst opgeleverd. Hiervoor heeft TNO een longlist van technologieën samengesteld en per technologie de risico's voor de nationale veiligheid geduid, met een daaruit volgend antwoord op de vraag of de betreffende technologie sensitief is in het licht van de nationale veiligheid. De sensitiviteit van de technologieën is door TNO met gebruikmaking van de ANV-systematiek onderzocht vanuit technologisch oogpunt: kan deze technologie op zichzelf een bedreiging vormen voor de nationale veiligheid? Daarbij is onder meer is van belang welke toepassingsgebieden de technologie heeft en of deze bijvoorbeeld van essentieel

[74] Kamerstukken II 2023/24, 31288, nr. 1108.
[75] Het Analistennetwerk is een kennisnetwerk dat sinds 2011 analyses maakt van risico's en bedreigingen voor de nationale veiligheid. Het netwerk kent een vaste kern van zes organisaties, te weten het Rijksinstituut voor Volksgezondheid en Milieu, TNO, het Nederlands Instituut voor Internationale Betrekkingen Clingendael, het Wetenschappelijk Onderzoek- en Documentatiecentrum, de Algemene Inlichtingen- en Veiligheidsdienst en ISS/Erasmus Universiteit Rotterdam.
[76] TNO 2022 R11656, Sensitieve Technologie.pdf (rivm.nl).

belang kunnen zijn voor het functioneren van defensie, opsporings- en inlichtingen- en veiligheidsdiensten bij de uitvoering van hun taken.

Tweede stap
Met behulp van het advies van TNO is de volgende stap mogelijk gemaakt, de beleidsmatige vertaalslag waarbij voor dit wetsvoorstel is bezien welke sensitieve technologieën hierin worden opgenomen. Bij de uitwerking is bezien bij welke (sub)technologieën of welke technologische toepassingen sprake is van sensitiviteit. Vervolgens is een afweging gemaakt of specifiek bij de geïdentificeerde sensitieve technologieën sprake is van grote risico's voor de nationale veiligheid als gevolg van ongewenste kennis- en technologieoverdracht via Nederlandse kennisinstellingen.

Voor deze stap is onder meer de reeds bestaande kennis en expertise binnen de rijksoverheid rondom nationale veiligheidskwesties en technologie benut en de kennis en expertise binnen de kennissector. Een interdepartementale werkgroep heeft samen met experts een eerste concept sensitiviteitsbeoordeling gemaakt die voor feedback is voorgelegd aan de kennissector in de periode maart tot juni 2023. Dit heeft reacties opgeleverd, die zijn verwerkt in een herziene conceptbeoordeling. Deze herziene conceptbeoordeling is in een tweede feedbackronde voorgelegd aan de interdepartementale werkgroep en het kennisveld. Ook zijn in januari 2024 goed bezochte bijeenkomsten met experts uit het kennisveld gehouden over de technologiegebieden: geavanceerde materialen, kunstmatige intelligentie (AI), biotechnologie en nanotechnologie. Verder heeft in april 2024 een rondetafelgesprek plaatsgevonden met experts uit het kennisveld.

In de daarop volgende fase is al de feedback uit deze afstemmingsrondes en sessies verwerkt en is de sensitiviteitsbeoordeling vastgesteld. Vervolgens heeft interdepartementale besluitvorming plaatsgevonden over welke technologieën sensitief zijn voor dit wetsvoorstel en op welke wijze de als sensitief beoordeelde technologieën in dit voorstel kunnen worden opgenomen.

Tijdens de fase van verwerken van de feedback en de besluitvorming is ook de eerder genoemde Trendanalyse Nationale Veiligheid 2024 en de verdieping op deze trendanalyse betrokken, aangezien de Trendanalyse een actueel inzicht geeft in technologische ontwikkelingen die de nationale veiligheid steeds meer beïnvloeden.[77]

4.4.4. De criteria voor het aanwijzen van sensitieve technologieën

In dit wetsvoorstel worden een aantal technologieën en subtechnologieën aangewezen die sensitief zijn *voor zover* aan een aantal wettelijke criteria is voldaan.

Criterium 1
Het onderzoek op het gebied van de desbetreffende technologie is niet experimenteel of theoretisch van aard, zonder dat daarbij een specifieke toepassing voorzien is.
De fase waarin het onderzoek zich bevindt is allereerst relevant. Het Technological Readiness Level (TRL) geeft een mate van ontwikkeling aan voor technologieën.[78] Bij een laag TRL is veelal sprake van fundamenteel onderzoek. Bij fundamenteel onderzoek wordt veelal gesproken van TRL 1-2. De OESO-definitie van fundamenteel onderzoek is: "experimenteel of theoretisch onderzoek dat vooral als doel heeft om nieuwe kennis te verkrijgen over de fundamentele oorzaken van fenomenen en/of observeerbare feiten, zonder dat daarbij een specifieke toepassing voorzien is".[79]

[77] Zie voetnoot 43.
[78] Bij het TRL wordt onderscheid gemaakt tussen vier fasen: de Discovery Phase (TRL 1-3); de Development Phase (TRL 4-6); de Demonstration Phase (TRL 7-8) en de Deployment Phase (TRL 9). Zie https://www.rvo.nl/onderwerpen/trl.
[79] Zie de Frascati Manual (OESO, 2015a).

Op basis van het TRL kan op het oog vrij gemakkelijk een onderscheid gemaakt worden tussen de verschillende fasen waarin een onderzoek zich bevindt. Het strikte onderscheid tussen fundamenteel en toegepast onderzoek is echter wel een vereenvoudiging van de werkelijkheid. Allereerst is het onderscheid in de praktijk gradueel en kan onderzoek zowel fundamentele als toegepaste elementen bevatten. Tevens gaan ontwikkelingen soms sneller dan verwacht richting een toepassing van sensitieve technologie. Ook dit kan nadelige effecten hebben op de nationale veiligheid. Tot slot is van belang dat niet in zijn algemeenheid kan worden gezegd dat aan fundamenteel onderzoek nooit risico's voor de nationale veiligheid zijn verbonden. Er kan immers ook sprake zijn van een technologie die zich nog in de fundamentele ontwikkelingsfase bevindt, maar waarbij een bijdrage aan risico's voor de nationale veiligheid wel al voorstelbaar is. Dit onderzoek kan alsnog aantoonbare risico's voor de nationale veiligheid opleveren. Fundamenteel onderzoek dat nog geen mogelijke risicovolle toepassingen kent, wordt met dit voorstel niet aangemerkt als sensitief.

Als uitgangspunt is gehanteerd dat bij een TRL hoger of gelijk aan 3 de sensitiviteitsbeoordeling samenhangt met de andere elementen. In geval van TRL 1 of 2 is het uitgangspunt gehanteerd dat de technologie doorgaans niet sensitief is, tenzij het vanwege een mogelijke risicovolle toepassing voorstelbaar is dat de technologie een bijdrage kan leveren aan risico's voor de nationale veiligheid. In een door het Rijk ontwikkeld beoordelingskader wordt dit nader uitgewerkt, zie paragraaf 4.4.6. Bij de uitwerking van dit beoordelingskader wordt de kennissector betrokken.

Tot slot is van belang dat technologieën met TRL 1 of 2 later wel aan de werking van de wet zouden kunnen worden toegevoegd, met name wanneer duidelijk wordt dat het onderzoek mogelijke risicovolle toepassingen kent, dan wel zich gaat richten op mogelijke risicovolle toepassingen. Daarmee is een bijdrage aan risico's voor de nationale veiligheid wel voorstelbaar geworden.

Afwijking van criterium 1
Met dit voorstel is in afwijking van het hiervoor geformuleerde uitgangspunt voorzien in een mogelijkheid om technologieën waarvoor geldt dat het onderzoek op het gebied van de desbetreffende technologie nog experimenteel of theoretisch van aard is, toch voor dit wetsvoorstel als sensitief aan te merken. Dit is aan de orde wanneer, ondanks dat sprake is van experimenteel of theoretisch onderzoek, het goed voorzienbaar of voorstelbaar is dat de technologie in de toekomst aantoonbare risico's voor de nationale veiligheid kan opleveren. Het mogelijke disruptieve karakter van de technologie is in dat geval groot en er zijn bijvoorbeeld grote of potentieel radicale veranderingen denkbaar die de toepassing van de betreffende technologie teweeg kan brengen. Bij technologieën die nog in een pril ontwikkelingsstadium verkeren, maar waarbij het voorstelbaar is dat deze in de toekomst een grote bijdrage kunnen gaan leveren aan een risico voor de nationale veiligheid, ligt het daarom in de rede deze technologie in weerwil van het prille ontwikkelingsstadium toch als sensitieve technologie aan te merken.

Criterium 2
Verder is een (sub)technologie sensitief wanneer het aan één van de twee volgende kenmerken voldoet.

<u>De (sub)technologie wordt gekenmerkt door een breed toepassingsbereik binnen verschillende vitale processen of processen die raken aan de nationale veiligheid</u>
Een volgend relevant element waar bij de sensitiviteitsbeoordeling naar moet worden gekeken zijn mogelijke toepassingen binnen processen die potentieel grote gevolgen kunnen hebben voor de nationale veiligheid. Risico's zitten in het mogelijke disruptieve karakter van de technologie voor de nationale veiligheid of de vitale infrastructuur. Zijn er bijvoorbeeld grote of potentieel radicale veranderingen denkbaar die de toepassing van de betreffende technologie teweeg kan brengen. Bij technologieën is het voorstelbaar dat deze een grote bijdrage kunnen leveren aan een risico voor de

nationale veiligheid. Een voorbeeld is nucleaire technologie. De technologie is niet meer nieuw, maar er wordt nog veel onderzoek gedaan en misbruik kan leiden tot grote disruptieve gevolgen.

Ook kan sprake zijn van mogelijke toepassingen in de (toekomstige) vitale processen. De continuïteit is van cruciaal belang voor de Nederlandse samenleving, zoals in het geval van (transport van) energie, de burgerluchtvaart en warmtevoorziening. Bescherming van de vitale infrastructuur ligt in de regel meer in de fysieke- en cyberveiligheid, maar wanneer technologie die ten behoeve van de vitale infrastructuur wordt ontwikkeld, is het mogelijk dat deze technologie als sensitieve technologie is aan te merken omdat een bijdrage aan een risico voor de nationale veiligheid voorstelbaar is. Een voorbeeld is Positie-, Navigatie- en Tijdbepaling (PNT). De burgerluchtvaart kan problemen gaan ondervinden met de positiebepaling omdat statelijke en niet-statelijke actoren deze via technologie trachten te verstoren. Het gevolg is dat vliegtuigen op een andere plaats of hoogte kunnen zijn dan hun apparatuur aangeeft en daardoor zichzelf of de omgeving in gevaar kunnen brengen. Dit kan ook gebeuren met voertuignavigatie. Risico's voor de nationale veiligheid zijn dan voorstelbaar. Van technologieën waarvan een dergelijke bijdrage aan een risico voor de nationale veiligheid (nog) niet voorstelbaar is, ligt het niet in de rede deze als sensitieve technologie aan te merken.

Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting kan leiden en daarmee een risico kan vormen voor de nationale veiligheid. Het identificeren en aanwijzen van vitale processen is staand beleid. Voorheen werd ook wel gesproken van vitale sectoren. Voor de aanwijzing van vitale processen zijn rijksbreed impactcriteria opgesteld. Deze criteria en de actuele lijst met vitale processen zijn te vinden op de website van de Nationaal Coördinator Terrorismebestrijding en Veiligheid.[80] Deze vitale processen zijn aangewezen door de vakminister die beleidsverantwoordelijk is voor dit vitale proces, in samenspraak met de Minister van Justitie en Veiligheid. Er gaat een zorgvuldig proces aan deze aanwijzing vooraf. De beoordeling of een proces vitaal is, wordt gemaakt wanneer maatschappelijke ontwikkelingen (bijvoorbeeld veranderde dreigingen of risico's en evaluaties van incidenten) daar aanleiding toe geven.

Het doel van dit overkoepelende beleid is dat het hierdoor mogelijk is om schaarse middelen efficiënt en gericht in te kunnen zetten. Daarnaast vormt het de basis voor de inrichting van verschillende instrumenten. Dit wetsvoorstel is daar een van.

De (sub)technologie kan van essentieel belang zijn voor het functioneren van defensie, opsporings-, inlichtingen- en veiligheidsdiensten bij de uitoefening van hun taken
Een ander relevant element is dat de technologie van essentieel belang kan zijn voor het functioneren van defensie-, opsporings-, inlichtingen- en veiligheidsdiensten bij de uitoefening van hun taken. Omdat het functioneren van deze organisaties van wezenlijk belang is voor onze nationale veiligheid kunnen technologieën die van essentieel belang kunnen zijn voor het functioneren onder het toepassingsbereik van de wet gebracht worden. De nationale veiligheid van Nederland is nauw verbonden met die van haar bondgenoten en de stabiliteit van de internationale rechtsorde. Het voorkomen van risico's voor de nationale veiligheid strekt zich daarmee dus ook uit tot technologieën die worden aangeboden aan bondgenoten van Nederland, die op grond van wederkerigheidsprincipes bijdragen aan het nationale veiligheidsbelang.

Indien sprake is van toepasbaarheid in sectoren en domeinen met een duidelijke relatie tot nationale veiligheid zal in de regel sprake zijn van sensitieve technologie. Daarbij geldt dat de technologie van essentieel belang kan zijn voor het functioneren van defensie-, opsporings- en inlichtingen- en veiligheidsdiensten bij de uitoefening van hun

[80] Overzicht vitale processen | Vitale infrastructuur | Nationaal Coördinator Terrorismebestrijding en Veiligheid.

taken. Hoewel de technologie zelf wellicht niet direct risico's voor de nationale veiligheid oplevert, kan de technologie niet helemaal los gezien worden van de risico's die samenhangen met de specifieke toepassingen in bepaalde cruciale sectoren of domeinen. Relevant hierbij is ook voor welke specifieke toepassingen de technologie wordt gebruikt of welke toepassingen in de toekomst voorstelbaar zijn, waaronder mogelijke dual-use toepassingen. Er is daarom voor gekozen om ook de technologieën die van essentieel belang kunnen zijn voor het functioneren van defensie-, opsporings-, inlichtingen- en veiligheidsdiensten bij de uitoefening van hun taken en met toepassingen in de sectoren en domeinen met een duidelijke relatie tot nationale veiligheid, aan te merken als sensitief.

Criterium 3
Zoals onder meer reeds uiteengezet in paragraaf 2.3.1 en paragraaf 3.2.1 is op grond van besluiten van de Raad en EU-verordeningen, die worden vastgesteld in het kader van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB), sprake van beperkende maatregelen en is het verlenen van technische bijstand of overdragen van bepaalde goederen of technologieën in specifieke gevallen verboden. Nederland dient als lidstaat van de Europese Unie maatregelen te nemen om te zorgen dat de verboden van de desbetreffende verordeningen worden nageleefd, en is verantwoordelijk voor de handhaving van die verboden. De kennisinstellingen zijn rechtstreeks gebonden aan de verboden uit de verordeningen.

De verhouding met sanctietechnologie
Met de screening kennisveiligheid zal ook worden getoetst aan enkele verboden op het verlenen van technische bijstand, zoals opgenomen in verschillende EU-sanctieverordeningen. De overheid ondersteunt kennisinstellingen met het zogeheten verscherpt toezicht bij de naleving van deze verboden, specifiek als het gaat om het overdragen van bepaalde kennis en technologie naar enkele landen, zoals Noord-Korea, Iran en Rusland. Het gaat voor Iran, Noord-Korea en Rusland om de verboden om goederen en (kennis over) technologieën over te dragen die betrekking hebben op (ballistische) rakketten en overbrengingsmiddelen, vallende onder het Missile Technology Control Regime (MTCR), en nucleaire technologie die kan worden ingezet voor de ontwikkeling van kernwapens.

Iran Sanctieverordening
Op grond van Verordening (EU) nr. 267/2012 is het verlenen van technische bijstand of het overdragen van goederen of technologie voor het Iraanse ballistische raketprogramma ook na het stopzetten van de nucleair-gerelateerde sancties verboden. Op basis van de verbodsbepalingen in de genoemde verordening is het verlenen van technische bijstand aan Iraanse personen, entiteiten of lichamen (als gedefinieerd in de Verordening) of voor gebruik in Iran verboden als het gaat om technologie en goederen – genoemd in bijlage III van genoemde verordening – voor de ontwikkeling van ballistische raketten.

Noord-Korea Sanctieverordening
Op grond van de Sanctieregeling Noord-Korea 2017 is het verboden dat gespecialiseerd onderwijs of gespecialiseerde opleiding aan onderdanen uit Noord-Korea wordt verstrekt op vakgebieden die zouden bijdragen tot proliferatiegevoelige nucleaire activiteiten van Noord-Korea, en tot de ontwikkeling van systemen voor de overbrenging van kernwapens. Het is verboden om dergelijke kennis in de vorm van onderwijs en onderzoek aan te bieden aan personen die niet beschikken over een ontheffing van de Minister van Onderwijs, Cultuur en Wetenschap. De bijlage bij de Sanctieregeling Noord-Korea 2017 vermeldt op welke gebieden van onderwijs en onderzoek het verbod in elk geval betrekking heeft.

Ruslandsancties
Op grond van Verordening (EU) nr. 833/2014 is het verlenen van technische bijstand of overdragen van goederen of technologie aan Rusland voor bepaalde kennisgebieden verboden. Tevens is het verboden om deze goederen of technologie te verkopen, te leveren, over te dragen aan of uit te voeren naar natuurlijke personen, rechtspersonen, entiteiten of lichamen in Rusland of voor gebruik in Rusland. Het betreft de in de artikelen 2, 2 bis en 3 quater van de verordening vermelde goederen en technologie. Voor Rusland is het aantal technologieën en vakgebieden dat onder de Ruslandsancties valt breder dan de huidige vakgebieden van het verscherpt toezicht. Voor de huidige uitvoering van het verscherpt toezicht is gekozen om het aantal vakgebieden gelijk te houden aan het aantal vakgebieden dat al onder het verscherpt toezicht in geval van Iran en Noord-Korea valt. Belangrijke kanttekening hierbij is dat de kennisinstellingen wel reeds rechtstreeks gebonden zijn aan alle verboden uit alle sanctieverordeningen, zo ook die uit Verordening (EU) nr. 883/2014. De regering onderzoekt of het in de rede ligt het verscherpt toezicht met extra vakgebieden uit de Ruslandsancties uit te breiden.

Technologieën waarvoor op grond van internationale sanctieregelgeving beperkingen gelden ten aanzien van het aanbieden van kennis erover (verbod op 'technische bijstand'), welke beperkingen zijn aangewezen in een ministeriële regeling, worden met dit voorstel geacht sensitief te zijn.

Voor de screening kennisveiligheid is het van belang dat de screeningsplicht van toepassing zal zijn op de sanctietechnologieën die ook met verscherpt toezicht worden gecontroleerd of in de toekomst zullen worden gecontroleerd. Het verscherpt toezicht houdt als zelfstandig instrument op met bestaan en gaat op in de screening kennisveiligheid.

Sancties omvatten echter meer en veel bredere verboden en kunnen ook zien op meer landen dan de landen die onder het verscherpt toezicht vallen. Niet alle gesanctioneerde technologie komt daarmee dus automatisch onder de werking van dit voorstel te vallen, maar slechts die technologie waar het verscherpt toezicht nu reeds op van toepassing is, of die technologie die onder het toepassingsbereik zal worden gebracht. Deze sanctieregimes worden in een ministeriële regeling aangewezen.

De betreffende sanctietechnologie komt ook voor op de met dit voorstel aangewezen lijst met sensitieve (sub)technologieën, omdat voor die betreffende technologie tevens geldt dat er grote risico's voor de nationale veiligheid kunnen ontstaan in geval van ongewenste kennis- en technologieoverdracht door toegang tot sensitieve technologie bij Nederlandse kennisinstellingen.

EU-exportcontroleregelgeving en commercieel beschikbare technologie
Exportcontrole behelst wet- en regelgeving die Nederland implementeert om de export van bepaalde strategische goederen, technologieën en diensten te controleren om redenen van nationale veiligheid. In geval van commercieel beschikbare technologieën geldt onverminderd de EU-exportregelgeving.

De EU dual-use verordening (nr. 2012/821) bepaalt dat voor tien categorieën technologieën en goederen een vergunning aangevraagd moet worden bij de export hiervan buiten de Europese Unie.[81] Technologieën die op de EU-exportcontrolelijsten zijn opgenomen kunnen ook voorkomen op de lijst met sensitieve technologieën als bedoeld in dit voorstel. Zowel de EU-exportcontroleregelgeving in geval van export (fysiek of elektronisch) van die betreffende technologie als de screening kennisveiligheid in geval van de toegang van een onderzoeker of student onderzoeker tot sensitieve technologie bij Nederlandse kennisinstellingen kunnen dan aan de orde zijn.

[81] EUR-Lex - 02021R0821-20241108 - EN - EUR-Lex.

De controles zijn bedoeld om de ongewenste verspreiding van wapens te voorkomen, de verspreiding van gevoelige technologieën te beheersen en ervoor te zorgen dat export geen activiteiten ondersteunt die in strijd zijn met het belang van Nederland. Het Nederlandse beleid voor exportcontrole richt zich op strategische goederen en diensten. Strategische goederen zijn militaire goederen, dual-use-goederen, en sanctiegoederen. Om ongewenst eindgebruik tegen te gaan, geldt een vergunningplicht voor de uitvoer van strategische goederen en diensten. Dual-use goederen zijn goederen die zowel voor civiele als militaire doeleinden kunnen worden gebruikt en zijn onderworpen aan strenge exportregels. Militaire goederen zijn goederen die zijn opgenomen in de gemeenschappelijke EU-lijst van militaire goederen die jaarlijks wordt herzien. De export van deze goederen is onderworpen aan een toetsing aan de criteria van het EU Gemeenschappelijk Standpunt inzake wapenexportcontrole[82].

Bedrijven of personen die goederen en technologie willen uitvoeren die op de gemeenschappelijke EU-lijst van militaire goederen of de bijlage van de EU dual-use verordening (nr. 2021/821) staan, dienen bij de Centrale Dienst voor In- en Uitvoer (CDIU) een aanvraag in voor een uitvoervergunning. De CDIU, onderdeel van de Douane, staat voor de verlening van uitvoervergunningen onder beleidstoezicht van het ministerie van Buitenlandse Zaken.

Ook kennis en technologie kunnen in sommige gevallen buiten de EU geëxporteerd worden, maar kennis en technologie kunnen ook op andere manieren door statelijke actoren verkregen worden. Bijvoorbeeld via onderzoekers en studenten bij kennisinstellingen die in aanraking komen met sensitieve kennis en technologie. Zoals reeds toegelicht in paragraaf 2.6.1 volstaat het exportcontrolebeleid niet om risico's op ongewenste kennis- en technologieoverdracht via kennisinstellingen voldoende te kunnen beperken. Vanwege de aanvulling op het beleid voor exportcontrole bestaat er overlap tussen technologieën die zowel voorkomen op de EU-exportcontrolelijsten als op de met dit voorstel aangewezen sensitieve technologieën.

4.4.5 Regelingsniveau

De (sub)technologieën die in het proces van sensitiviteitsbeoordeling zijn aangemerkt als sensitief, worden in het voorliggende wetsvoorstel opgenomen. Het is wenselijk vanuit het oogpunt van het primaat van de wetgever en de rechtszekerheid om zoveel mogelijk op het niveau van de wet duidelijkheid te geven over wat de sensitieve (sub)technologieën zijn.

Ook voor dit voorstel geldt dat voor de met dit voorstel als sensitief aangewezen (sub)technologieën een inhoudelijke herijking moet kunnen leiden tot een snelle actualisatie van de reikwijdte van het voorstel. Dit is nodig, omdat technologie zich snel kan ontwikkelen en ook het dreigingsbeeld aan snelle verandering onderhevig kan zijn. Ook kan sprake zijn van ontwikkeling van nieuwe (sub)technologieën waardoor een (sub)technologie momenteel nog niet sensitief is, maar dit wel kan worden. Dit maakt het noodzakelijk om het ook mogelijk te maken (sub)technologieën bij amvb aan te wijzen. Hiervoor is in het voorstel een grondslag opgenomen. Ook voor de (sub)technologiegebieden die bij amvb worden aangewezen, geldt dat bij ongewenst eindgebruik of het ontstaan van risicovolle strategische afhankelijkheden directe risico's kunnen bestaan voor de nationale veiligheid en dat deze risico's ook expliciet gemaakt kunnen worden.

Tot slot voorziet dit voorstel in de mogelijkheid om bij ministeriële regeling technologieën als sensitieve technologie aan te wijzen voor zover sprake is van technologieën waarvoor op grond van internationale sanctieregelgeving beperkingen gelden. In veel internationale sanctieregelgeving zijn beperkingen gesteld aan de

[82] Besluit - 2019/1560 - EN - EUR-Lex

overdracht van kennis over technologieën (verbod op technische bijstand). Deze technologieën zijn betrokken bij de opstelling van het overzicht van sensitieve technologieën in dit wetsvoorstel (bijlage 2). Er kunnen zich snel veranderingen voordoen in de bij internationale sanctieregelgeving aangewezen, te beschermen technologie. Daar komt bij dat internationale sanctieregelgeving vaak een korte implementatietermijn kent. In die omstandigheden acht de regering het wenselijk om bij ministeriële regeling sensitieve technologieën te kunnen aanwijzen, in aanvulling op de in bijlage 2 of bij amvb aangewezen technologieën.

De voorwaarden die dit wetsvoorstel stelt aan het bij ministeriële regeling aanwijzen van sensitieve technologieën zijn:

- Er moet altijd internationale sanctieregelgeving aan ten grondslag liggen (er kan dus geen andere aanleiding zijn om bij ministeriële regeling een sensitieve technologie toe te voegen).
- Het moet bij de internationale sanctieregelgeving bovendien gaan om een – juridisch bindend – verdrag of bindend besluit van een internationale organisatie, niet om een – juridisch niet bindende – aanbeveling van een internationale organisatie of internationale afspraak.
- De toevoeging van de sensitieve technologie moet een spoedeisend karakter hebben.
- De internationale sanctiemaatregel met betrekking tot de technologie moet slechts beperkt ruimte laten voor beleidsinhoudelijke keuzes.

Dit sluit aan bij de huidige mogelijkheid op grond van de Sanctiewet 1977 om bij ministeriële regeling uitvoering te geven aan bindende internationale sanctieregelgeving en daarbij maatregelen te treffen voor de bescherming van sensitieve technologie.[83] In het wetsvoorstel internationale sanctiemaatregelen is een vergelijkbare grondslag opgenomen om bij ministeriële regeling sanctiemaatregelen te treffen.[84]

Het ongedaan maken van de aanwijzing van een technologie als sensitieve technologie is mogelijk op hetzelfde niveau als waarop de technologie is aangewezen. Dit betekent dat in dit wetsvoorstel (bijlage 2) opgenomen technologieën bij wet kunnen worden geschrapt. Bij amvb aangewezen technologieën kunnen bij amvb worden geschrapt. Bij ministeriële regeling aangewezen technologieën kunnen bij ministeriële regeling worden geschrapt.

Dit voorstel voorziet niet in de mogelijkheid om bij amvb of ministeriële regeling technologieën die bij de wet zijn aangewezen te schrappen. Het is op grond van de Aanwijzingen van de regelgeving slechts in enkele gevallen mogelijk om het toepassingsbereik van een wet bij lagere regelgeving te verminderen.[85] Van deze uitzonderingen is bij dit voorstel geen sprake. In de responsieve aanpak en met de systematiek zoals uiteengezet in paragraaf 4.4.7 is wel voorzien in de mogelijkheid om (sub)technologieën die niet langer als sensitief zijn aan te merken bij een herijking van de lijst te schrappen.

4.4.6 De overeenkomsten met en verschillen ten opzichte van de Wet vifo

De Wet vifo regelt kort gezegd dat de verwerver gescreend wordt in het geval van een investering, fusie of overname bij een vitale aanbieder of een onderneming die actief is

[83] Zie artikel 2, tweede lid, van de Sanctiewet 1977 en de daarop gebaseerde Sanctieregeling Iran 2012, de Sanctieregeling Noord-Korea 2017 en de Sanctieregeling territoriale integriteit Oekraïne 2014.
[84] Artikel 2.1.1 van het wetsvoorstel internationale sanctiemaatregelen (https://www.internetconsultatie.nl/sanctiemaatregelen/b1).
[85] Aanwijzingen voor de regelgeving nr. 2.31 en 2.32 en zie verder Kamerstukken I 2006/07, 26 200 VI, nr 65, D.

op het gebied van sensitieve technologie. De overeenkomst met dit wetsvoorstel is er met name in gelegen dat er voorzien wordt in screening bij activiteiten op het gebied van sensitieve technologie om risico's voor de nationale veiligheid te mitigeren. In dit wetsvoorstel is gekozen voor een andere systematiek voor de afbakening van wat sensitieve technologie is dan die in de Wet vifo. Hierbij verdient opmerking dat het overgrote deel van de technologieën onder het bereik van beide wetten valt. Desondanks is het verschil in afbakeningssystematiek noodzakelijk om de volgende redenen.

Ten eerste richten dit wetsvoorstel en de Wet vifo zich op verschillende sectoren. De Wet vifo richt zich op zeggenschapsverhoudingen bij commerciële ondernemingen, terwijl dit wetsvoorstel zich richt op individuele onderzoekers en studenten bij kennisinstellingen. Dit verschil in doelgroep brengt een heel andere context met zich mee, waardoor de risico's voor de nationale veiligheid zich ook op een andere manier voordoen. Zo beoogt de Wet vifo bijvoorbeeld te voorkomen dat kwaadwillende actoren via een verwerving de mogelijkheid krijgen om direct vitale processen te verstoren. Ook is er bij kennisinstellingen vaker sprake van een laag TRL dan in het bedrijfsleven.

Ten tweede is er voor investeringsscreening in verschillende sectoren sectorspecifieke wetgeving waarin een investeringstoets is geregeld. Voor sommige sensitieve technologieën is er daarom voor gekozen die niet onder het bereik van de Wet vifo te brengen omdat de investeringstoetsing al geregeld was. Diezelfde technologieën kunnen wel onder het toepassingsbereik van dit wetsvoorstel vallen omdat screening van onderzoekers niet elders geregeld is.

Tegen die achtergrond is de afbakeningssystematiek op de volgende punten verschillend.

Zoals eerder uiteengezet is het vanuit het oogpunt van het primaat van de wetgever en de rechtszekerheid wenselijk om zoveel mogelijk op het niveau van de wet duidelijkheid te geven over wat de sensitieve (sub)technologieën zijn. Dit is in dit wetsvoorstel op een andere manier vormgegeven dan in de Wet vifo. In de Wet vifo is met verwijzing naar de EU-lijsten voor militaire goederen en producten voor tweeërlei gebruik een deel van de technologie op wetsniveau aangewezen. Bij algemene maatregel van bestuur kunnen hierop uitzonderingen worden gemaakt en aanvullingen op worden gedaan. Het onderhavige wetsvoorstel kent ook de systematiek dat er op wetsniveau technologieën worden aangewezen en dat er bij algemene maatregel van bestuur aanvullingen kunnen worden gedaan. Voor onderhavig voorstel is aanvankelijk onderzocht of dezelfde systematiek als de Wet vifo, met verwijzingen naar de eerder genoemde EU-lijsten, ook zou kunnen werken. Dit bleek niet mogelijk vanwege bovengenoemde verschillen tussen het bedrijfsleven en de kennissector. Waar de kennissector zich met name bezighoudt met onderzoek met in veel gevallen een lager TRL, houdt het bedrijfsleven zich met name bezig met (het ontwikkelen) van toepassingen en aldus meer met goederen/producten/diensten die op de EU-exportcontrolelijsten reeds als sensitief zijn aangewezen.

Ten aanzien van de criteria voor het bepalen of een technologie sensitief is, verdient verder het volgende opmerking. Allereerst is het eerste criterium van onderhavig voorstel, de uitzondering van onderzoek met een laag TRL ('experimenteel en theoretisch onderzoek'), voor de Wet vifo al min of meer verdisconteerd in artikel 8, eerste lid, van de Wet vifo. In dat artikel is bepaald dat sensitieve technologie kort gezegd de EU-exportcontrolelijsten omvat. Doordat de EU-exportcontrolelijsten onder de werking van de Wet vifo vallen en deze EU-exportcontrolelijsten doorgaans ook 'basic scientific research' uitzonderen, is het niet meer nodig geweest dit op wetsniveau in de Wet vifo als apart criterium op te nemen. In onderhavig voorstel past het daarnaast ook om dit criterium een prominente plek te geven, omdat in de kennissector veel vaker

sprake zal zijn van laag TRL en experimenteel en theoretisch onderzoek dan in het bedrijfsleven. Veelal is bij bedrijven al sprake van een hoger TRL. Ook laag TRL komt in het bedrijfsleven voor, maar via artikel 8 van de Wet vifo valt dit dan veelal niet onder het toepassingsbereik.

De andere twee criteria uit artikel 8 van de Wet vifo zijn wel identiek aan de criteria van onderhavig wetsvoorstel. Voor onderhavig wetsvoorstel is het criterium uit de Wet vifo van artikel 8, derde lid, onderdeel b, (in het kort: voorzieningszekerheid) niet overgenomen. Ook dit komt doordat het voor het bedrijfsleven veelal om technologische toepassingen gaat en niet om technologie in de experimentele en theoretische fase van onderzoek, zoals bij de kennissector veel vaker aan de orde is. Het risico voor de nationale veiligheid dat met voorzieningszekerheid gemoeid kan zijn, doet zich daarom in de kennissector veel minder vaak of zelfs geheel niet voor.

Met de beoogde uitbreiding van het op de Wet vifo berustende Besluit toepassingsbereik sensitieve technologie, overlappen de sensitieve (sub)technologieën nagenoeg geheel. Waar er verschillen zijn, zijn die om bovengenoemde redenen uitlegbaar.

Tot slot kent dit wetsvoorstel, anders dan de Wet vifo, de mogelijkheid om onder strikte voorwaarden bij ministeriële regeling sensitieve technologie aan te wijzen, indien internationale sanctieregelgeving daar aanleiding toe geeft. Dit houdt verband met de specifieke rol die de screening kennisveiligheid speelt in de handhaving van internationale sanctieregelgeving.

4.4.7. Vaststellen van de hoog-risico onderdelen van een kennisinstelling

Het proces van afbakening van sensitieve (sub)technologie in het kader van onderhavig wetsvoorstel gefaseerd aangepakt. Het proces bestaat uit twee hoofdfasen. Allereerst zijn ten behoeve van het wetsvoorstel een aantal (sub)technologieën geïdentificeerd samen met criteria voor het nader bepalen van de sensitiviteit. Deze technologieën en criteria zijn in het wetsvoorstel opgenomen. Ook zijn in het wetsvoorstel sommige sanctietechnologieën aangeduid als sensitieve technologie (zie de voorgaande paragraaf).

Vervolgens dienen de plaatsen te worden aangewezen waar specifiek sensitief onderzoek of onderwijs plaatsvindt, de hoog-risico onderdelen van de kennisinstellingen. Het benoemen van sensitieve (sub)technologieën is op zichzelf niet voldoende om duidelijk te maken waar en op welke vakgebieden van welke kennisinstellingen screening straks precies aan de orde is. Naast het in regelgeving aanwijzen van (sub)technologiegebieden en criteria voor de nadere bepaling van de sensitiviteit, moeten om die reden ook de hoog-risico onderdelen in kaart worden gebracht. Hier krijgen de kennisinstellingen een belangrijke taak en plicht.

De hoog-risico onderdelen zijn de plaatsen binnen de kennisinstellingen waar de screening op van toepassing zal zijn. Dit kunnen opleidingen en potentiële masteropleidingen, projecten, programmalijnen, vakgroepen, onderzoeksgroepen, projectgroepen, studentenprojecten, en bijvoorbeeld ook bepaalde teams en laboratoria zijn. Deze opsomming is niet limitatief, er zijn immers verschillen in de interne structuur bij de instellingen.

Rol kennisinstellingen bij vaststellen hoog-risico onderdelen
Voorgesteld wordt om de taak om de hoog-risico onderdelen vast te stellen bij de kennisinstellingen te beleggen. De kennisinstellingen kunnen zelf het beste beoordelen waar de sensitieve kennis en technologie zich precies bevindt binnen de instellingen. Zij weten bijvoorbeeld het best in welke fase het onderzoek zich bevindt en wat de toepassingscontext is. Zij hebben het beste zicht op de aard en de fase van het

onderzoek dat aan de kennisinstelling wordt verricht en op de organisatiestructuur waarbinnen dat gebeurt.

Alle onderdelen van de instellingen die binnen het bereik van artikelen 5 en 6 vallen, omdat sprake is van sensitieve (sub-)technologie, moeten verplicht door de instellingen vastgesteld gaan worden. Zij hebben hiervoor de kennis. Dit doen ze aan de hand van de criteria uit artikel 5. Ter uitwerking van deze criteria zal een beoordelingskader worden vastgesteld. Dat wordt vastgelegd in een ministeriële regeling. Het beoordelingskader geeft handvatten voor kennisinstellingen om te bepalen of binnen een bepaald onderdeel sprake is van sensitieve technologie. Hiermee is de aanpak zo risicogericht als mogelijk en past deze bij de institutionele autonomie van de instellingen. Als er sprake is van een vakgebied waarvoor geldt dat technische bijstand verboden is op grond van de voor het verscherpt toezicht relevante sanctieverordeningen, dan is reeds om die reden sprake van een hoog-risico onderdeel (artikel 5, derde lid). Is hiervan sprake dan zal de kennisinstelling bij de beoordeling van de vraag of sprake is van een hoog-risico ook het beoordelingskader doorlopen, maar de sensitiviteit en de werking van de relevante verboden op technische bijstand in geval van de technologieën die onder het verscherpt toezicht vallen, is reeds in EU sanctieverordeningen bepaald. Gelet hierop is de wegingsruimte bij het beoordelen van deze onderdelen op hoog-risico en de toepassing van de screeningsplicht beperkt.

Met het doorlopen van het beoordelingskader komt de instelling tot een risicobeoordeling. Die risicobeoordeling leidt niet tot de conclusie dat de betreffende (sub)technologie niet sensitief is, dat is al bepaald met dit voorstel. De kennisinstelling kan wel tot de conclusie komen dat het desbetreffende onderdeel niet als hoog-risico onderdeel hoeft te worden aangemerkt. De kennisinstelling kan bijvoorbeeld tot het oordeel komen dat een project dat valt onder een specifieke (sub) technologie niet hoog-risico is vanwege de specifieke toepassingscontext of bijvoorbeeld de fase waarin het onderzoek zich bevindt.

Proces vaststellen hoog-risico onderdelen
De kennisinstelling heeft de kennis in huis en weet wat er speelt op het gebied van technologie en kan daardoor scherp en precies vaststellen waar de risico's zich bevinden. De kennisinstelling identificeert zelf bij welke onderdelen binnen de eigen instelling sprake is van sensitieve (sub)technologieën als bedoeld in de artikelen 5 en 6 van het wetsvoorstel. Onderdelen kunnen risicogericht worden vastgesteld, bijvoorbeeld alleen een bepaald project, in plaats van een hele vak- of onderzoeksgroep, zie hiertoe de paragraaf hierna.

De vaststelling gebeurt altijd aan de hand van de wettelijke criteria en het beoordelingskader, respectievelijk het overzicht van door sanctie- en dual-use verordeningen opgenomen technologieën.

Gedurende de beoordeling geldt per onderdeel het vierogenprincipe. Niet alleen de inhoudelijk eindverantwoordelijke, zoals de hoogleraar, lector, vakgroepvoorzitter of onderzoeksleider, maakt de beoordeling, maar ook de voor kennisveiligheid verantwoordelijke medewerker of kennisveiligheidscoördinator kijkt mee op navolgbaarheid van de beoordeling.

Fysiek en digitaal afscheiden (compartimenteren)
Randvoorwaardelijk is daarbij dat het betreffende onderdeel is afgescheiden of gecompartimenteerd (zowel fysiek als ICT-matig), zodat de kennis en technologie beschermd wordt en gecontroleerd toegankelijk is. Bij de vaststelling betrekt de kennisinstelling dus altijd de vraag: wie heeft er toegang tot het betreffende onderdeel waar sensitieve technologie aanwezig is. Toegang is daarmee een bepalend element in de risicogerichte aanpak.

Om een onderdeel van de kennisinstelling af te bakenen van de rest van de kennisinstelling, wordt in dit wetsvoorstel voorgeschreven dat de sensitieve technologie afgescheiden moet zijn van de rest van de kennisinstelling. Zou het betreffende onderdeel niet afgescheiden zijn van de rest van de kennisinstelling, dan zou de screeningsplicht eenvoudig te omzeilen zijn en daarmee niet doeltreffend. Het wordt dan immers relatief makkelijk om via een onderdeel dat niet als hoog-risico is aangemerkt dat zich bijvoorbeeld fysiek of in de digitale omgeving in dezelfde ruimte bevindt, alsnog toegang te verkrijgen tot het hoog-risico onderdeel zonder voorafgaande screening. Door dit voorgeschreven onderdeel van de risicogerichte aanpak wordt voorkomen dat een eenvoudige manier ontstaat om de wet te omzeilen.

Het compartimenteren of afscheiden kan zowel fysiek als digitaal zijn, bijvoorbeeld door toegangscontrole per beveiligingsschil, door deuren te voorzien van een elektronisch toegangsbeheer systeem en bijbehorende alarmen, camerabeveiliging, en verschillende typen passen voorzien van accreditatie waardoor alleen toegang wordt verkregen tot de benodigde ruimtes waarvoor is geaccrediteerd. Andere mogelijke vormen van afscheiding zijn digitale two-factor authenticatie en inperking van gebruikersrechten tot alleen de benodigde taken.[86] Ook tokens (digitaal) en biometrische (fysieke) toepassingen zijn goede manieren om de toegangsbeveiliging te verhogen. Deze opsomming is niet uitputtend. Voor beide domeinen, zowel fysiek als digitaal, is het noodzakelijk om toegang tot het compartiment op individueel niveau controleerbaar te maken. Bij toegangsbeveiliging moet ingeregeld zijn dat alleen geautoriseerde gebruikers toegang hebben, waarbij het systeem ongeautoriseerde toegang voorkomt. Voor bezoekers kan er tevens gebruik gemaakt worden van voorafgaande toegangsregistratie, zowel digitaal als fysiek. Hierdoor kunnen beveiligingsincidenten sneller gesignaleerd en conform interne protocollen afgehandeld worden.

Consequentie van dit voorgeschreven onderdeel van de risicogerichte aanpak is daardoor dat als het betreffende hoog-risicovol onderdeel niet fysiek of digitaal is af te scheiden van andere onderdelen waarvoor de screeningsplicht niet geldt, dat dan ook die onderdelen onder de screeningsplicht komen te vallen. Het is aldus met de risicogerichte aanpak mogelijk om zo klein mogelijk af te bakenen, mits de toegang tot het betreffende hoog-risicovol onderdeel goed fysiek en digitaal is af te scheiden van de overige onderdelen in bijvoorbeeld een team, vak- of onderzoeksgroep, laboratorium of ruimte. Is dit niet mogelijk, dan moet worden bezien voor welke onderdelen gezamenlijk de screeningsplicht dan zou moeten gelden. Dit kan dus inhouden dat – totdat het betreffende hoog-risico onderdeel wel voldoende fysiek als digitaal is af te scheiden van de andere onderdelen – een geheel team, vak-of onderzoeksgroep, laboratorium of ruimte onder de screeningsplicht komt te vallen. Mocht na verloop van tijd het betreffende hoog-risico onderdeel wel voldoende af te scheiden zijn van de overige onderdelen, dan kan aan OCW de nieuwe vaststelling worden gemeld, zodat de screeningsplicht enkel nog geldt voor het hoog-risico onderdeel in kwestie. Zie daartoe verder het proces van herijking en actualisatie, paragraaf 4.4.7.

Het hiervoor beschreven proces, ook wel de risicogerichte aanpak, en het door de instelling te gebruiken beoordelingskader, zullen periodiek met een afvaardiging van de kennisinstellingen worden getest. Waar nodig kan dit leiden tot aanscherping van het beoordelingskader, waarvan het voornemen is om dit in een ministeriële regeling op te nemen.

---

[86] Ook wel bekend als Role-Based Access Control (RBAC) en op basis van 'need-to-know' en 'need-to-use'.

Meldplicht
De kennisinstelling meldt de uitkomsten van het onderzoek en de vastgestelde onderdelen van alle onderdelen die onder de reikwijdte van artikel 5 en 6 vallen aan de Minister van OCW. Hiertoe wordt een wettelijke verplichting geïntroduceerd. De meldplicht is noodzakelijk omdat zo beter toezicht kan worden gehouden of de kennisinstelling de plicht naleeft om tot een overzicht te komen van de hoog-risico onderdelen en de daaraan gerelateerde screening voor (master)studenten en onderzoekers hier aan te koppelen. Het is eveneens in het belang van de kennisinstellingen als een uniforme beoordeling volgt uit de toepassing van het beoordelingskader.

Wanneer nieuwe hoog-risico onderdelen ontstaan binnen een kennisinstelling, dienen deze te worden beoordeeld, vastgesteld en te worden gemeld. De Minister van OCW houdt naar aanleiding van de meldingen een actueel overzicht van hoog-risico onderdelen bij en zorgt voor samenhang tussen de aangewezen onderdelen. Een toezichthouder houdt namens de Minister van OCW toezicht op dit proces en op het naleven van voornoemde verplichting waarop een meldplicht rust voor de kennisinstellingen. In het kader van dat toezicht zullen de vaststellingen die zijn gemeld worden onderworpen aan een controle op navolgbaarheid en uniformiteit. Dit wordt nader uitgewerkt in hoofdstuk 7.

De wijze waarop hoog-risico onderdelen worden vastgelegd
Voor het verscherpt toezicht is bekend om welke vakgroepen het gaat, hoewel dit gegeven niet in de nationale sanctieregelgeving is neergelegd. De vakgroepen die onder het verscherpt toezicht vallen zijn gepubliceerd op de website van de rijksoverheid.[87] Voor dit wetsvoorstel is ervoor gekozen om dit niet op een vergelijkbare wijze te regelen.

De kennisinstellingen wijzen aan om welke hoog-risico onderdelen het gaat, waarmee deze informatie vertrouwelijk blijft. Alleen de verantwoordelijke beleidsdepartementen (OCW en JenV), de kennisinstellingen die onder het toepassingsbereik van dit wetsvoorstel vallen, de uitvoeringsorganisatie en de toezichthouder krijgen inzicht in de lijst met vastgestelde hoog-risico onderdelen. Met dit voorstel wordt bij (lagere) regelgeving geen overzicht van hoog-risico onderdelen vastgesteld en gepubliceerd. Hiervoor zijn verschillende redenen te geven.

Belangrijkste reden is dat een dergelijk overzicht informatie bevat die tot risico's voor de nationale veiligheid kan leiden. Met een dergelijk overzicht zou immers op gedetailleerd niveau duidelijk worden waar de specifieke sensitieve kennis en technologie zich bevindt. Ook het kennisveld geeft aan dat zij, mede ter bescherming van de privacy van studenten, onderzoekers en ander personeel en ter voorkoming van bijvoorbeeld gerichte cyberaanvallen, geen voorstander is van publicatie van een dergelijk overzicht. De regering steunt dit. Daarnaast zou een dergelijk overzicht zeer omvangrijk zijn door de vele onderdelen die hier onder vallen en zou een dergelijk overzicht voortdurend aan verandering onderhevig zijn. Er worden immers geregeld nieuwe projecten of programmalijnen gestart of vak- of onderzoeksgroepen opgericht. Dit leidt tot zeer frequente herijking van het overzicht, waardoor zelfs een ministeriële regeling te vaak gewijzigd zou moeten worden. Hierdoor worden ook de administratieve lasten beperkt.

4.4.8. Responsieve aanpak en een proces voor monitoring en actualisatie

Door de risicogerichte aanpak ontstaat tevens een responsieve aanpak die zoveel als mogelijk meebeweegt met ontwikkelingen. Er is een proces voor de herijking van de lijst met sensitieve technologieën, zoals toegelicht in deze paragraaf. De lijst met sensitieve technologieën bepaalt niet voor welke onderdelen de screeningsplicht aan de orde zal

[87] Voor welke technische studies heb ik een ontheffing kennisembargo nodig en hoe vraag ik deze aan? | Rijksoverheid.nl

zijn, dat wordt bepaald door de vaststelling van de hoog-risico onderdelen door de kennisinstelling.

Tweejaarlijkse systematische monitoring van de lijst van sensitieve technologieën op basis van signalen en urgentie
Technologie is continu in ontwikkeling en een regelmatige herijking van de lijst van sensitieve technologieën is om die reden noodzakelijk, ook om de kansen die technologische ontwikkelingen met zich meebrengen te kunnen betrekken. Het wetsvoorstel voorziet in een evaluatie over de doeltreffendheid en de effecten van de wet vijf jaar na de inwerkingtreding. Deze evaluatie laat onverlet dat het gewenst is tussentijds een vinger aan de pols te houden. Zaken zoals de beschikbaarheid en de fase van het onderzoek kunnen immers in korte tijd wijzigen en technologie kan verouderd raken. Daarom zal systematische monitoring plaatsvinden van de in de wet opgenomen sensitieve technologieën.

Systematische monitoring van de lijst sensitieve technologieën
Het voornemen is dat eens in de twee jaar op basis van informatie uit signaleringen vanuit intern en extern onderzoek, het internationale netwerk, of naar aanleiding van casuïstiek vanuit de praktijk de in de wet of de amvb opgenomen sensitieve technologieën zo nodig worden herzien.[88]

De beleidsmatige beoordeling naar aanleiding van de systematische monitoring wordt geleid door de verantwoordelijke beleidsdepartementen, in afstemming met een interne commissie van experts.[89] Indien nodig worden voorgestelde wijzigingen getoetst aan strategische (expert-)tafels met een representatieve afspiegeling van de Nederlandse kennisinstellingen.

Dit kan als uitkomst hebben dat technologieën die met het wetsvoorstel als sensitief zijn aangewezen op een later moment worden geschrapt. Een andere uitkomst is dat de sensitiviteitsbeoordeling wordt gehandhaafd of dat technologieën worden toegevoegd. De opbrengst van deze consultatierondes wordt verwerkt in een voorstel tot aanpassing van de wet of de amvb, indien dat noodzakelijk wordt geacht.

Signalering in geval van urgentie
Hiervan te onderscheiden is signalering in geval van urgentie waarbij kan worden gedacht aan het vaststellen van veranderingen in de EU-exportcontrolelijsten, de EU- en VN-sanctieregelgeving, aan snel opkomende nieuwe technologieën, ook als deze (nog) geen onderdeel van sancties of de EU-exportcontrolelijsten zijn, geopolitieke ontwikkelingen en van eventuele afnemende relevantie van bestaande technologieën die eerder wel als sensitief zijn aangewezen.

Dergelijke signalen worden elk half jaar verzameld en in het licht van de wet en het beoordelingskader ook door de verantwoordelijke beleidsdepartementen beoordeeld, in afstemming met de commissie van experts. De frequentie en wijze van beoordeling kan in geval van signalering verschillen.

De wijze waarop (sub)technologieën weer van de lijst kunnen worden verwijderd
Met bovenstaande responsieve aanpak en systematiek is ook voorzien in de mogelijkheid om (sub)technologieën die niet langer als sensitief zijn aan te merken bij een herijking van de lijst van de lijst te verwijderen.

[88] Gelijk aan de Wet vifo, waar in het Besluit van 4 mei 2023 tot het nader bepalen van het toepassingsbereik van de Wet veiligheidstoets investeringen, fusies en overnames een systematische herijking eveneens eens in de twee jaar is voorzien.
[89] Een nog samen te stellen interne ambtelijke commissie van experts vanuit de verschillende betrokken departementen en de inlichtingen- en veiligheidsdiensten, zo nodig aangevuld met externe experts en/of peer review.

In de tussentijd is voor een (sub)technologie, waarvoor geldt dat overeenstemming bestaat tussen de rijksoverheid en de kennissector dat deze niet langer meer als sensitief is aan te merken, voorzien in een mogelijkheid de screeningsplicht reeds te laten vervallen voor vastgestelde hoog-risico onderdelen die onder de betreffende (sub)technologie vallen. Voor die onderdelen geldt dat de kennisinstellingen opnieuw het beoordelingskader kunnen doorlopen, waarbij een mogelijke uitkomst is dat het betreffende onderdeel niet langer meer als hoog-risico onderdeel is aan te merken. Ook hier zijn de wettelijke criteria van toepassing. Wanneer na het opnieuw doorlopen van deze stappen en het beoordelingskader de uitkomst is dat een onderdeel niet meer als hoog-risico onderdeel hoeft te worden aangemerkt, dan kan de kennisinstelling deze gemotiveerde vaststelling aan de minister van OCW voorleggen, waarna de minister van OCW het betreffende onderdeel kan verwijderen van het overzicht met vastgestelde hoog-risico onderdelen.

Alertheid in geval van technologieën die (momenteel) niet als sensitief zijn aangewezen
Met een systeem van monitoring en signalering geeft de regering er zich rekenschap van dat technologieën die nu niet als sensitief worden aangemerkt, in de toekomst wel relevant kunnen worden gelet op risico 's voor de nationale veiligheid. Daarnaast kunnen bepaalde technologiegebieden niet sensitief zijn bevonden ter bescherming van het belang van nationale veiligheid, maar kan ongewenste kennis- en technologieoverdracht van deze technologieën wel schadelijk zijn voor betrokken organisaties of partijen of op het verdienvermogen of de strategische autonomie van Nederland. Dat een technologiegebied niet voorkomt in de wet screening kennisveiligheid betekent dus niet dat het niet van belang blijft om alert te zijn op mogelijke nieuwe ontwikkelingen, op wie toegang krijgt tot de technologie en op welke wijze de technologie wordt gedeeld of verspreid.

Proces van monitoring en actualisatie van de vastgestelde hoog-risico onderdelen van een kennisinstelling
Voor de aangewezen onderdelen van de kennisinstellingen geldt dat de vraag of een onderdeel nog als hoog-risico onderdeel dient te worden aangemerkt, aan snellere verandering onderhevig kan zijn dan de vraag of een gehele (sub)technologie nog wel als sensitief is aan te merken. Nieuwe projecten, programmalijnen, nieuw onderzoek, nieuwe vakgroepen of onderzoeksgroepen, opleidingen of studentenprojecten kunnen immers snel ontstaan, de fase van het onderzoek kan veranderen of de technologie waar het onderdeel van de kennisinstelling mee bezig is kan verouderd raken.

De lijst met vastgestelde hoog-risico onderdelen moet daarom doorlopend herzien kunnen worden zodat een flexibele en responsieve aanpak ontstaat. Dat geldt zowel voor het toevoegen van nieuwe vastgestelde hoog-risico onderdelen, als voor het afvoeren van hoog-risico onderdelen van de kennisinstelling van de lijst, wanneer zij niet langer als hoog-risico onderdeel aangemerkt dienen te worden. Door de voorgestelde responsieve aanpak kan voorkomen worden dat een screeningsplicht langer dan noodzakelijk aan de orde is.

De vaststelling en melding van de hoog-risico onderdelen vormen een voortdurende verplichting. Bij het ontstaan of oprichten van nieuwe projecten, programmalijnen, vakgroepen, onderzoeksgroepen, studentenprojecten of opleidingen is de kennisinstelling dus verplicht te onderzoeken of er sprake is van een hoog-risico onderdeel en hier melding van te maken aan de minister van OCW. Deze lijst wordt beheerd door het Rijk.

De lijst met vastgestelde hoog-risico onderdelen wordt in de implementatiefase van het wetsvoorstel opgesteld. Na de inwerkingtreding van de wet is er zoals gezegd de voortdurende verplichting op nieuwe hoog-risico onderdelen te melden aan de minister van OCW. Ook kan de instelling in de fase na inwerkingtreding de toegang tot een hoog-risico onderdeel alsnog fysiek en digitaal afschermen, waardoor de screeningsplicht

enkel nog zal gelden voor dat hoog-risico onderdeel en niet meer voor bijvoorbeeld het gehele team, laboratorium of ruimte. Daarbij gelden de wettelijke criteria, de risicogerichte aanpak, het vierogen principe en het beoordelingskader opnieuw als uitgangspunten. Dit maakt de aanpak zo scherp en zo risicogericht als mogelijk.

Hoofdstuk 5. Verhouding tot hoger recht

5.1. Bescherming van de persoonlijke levenssfeer (artikel 8 EVRM, artikel 7 en 8 Handvest van de grondrechten van de Europese Unie, artikel 10 Grondwet, Algemene verordening gegevensbescherming)

5.1.1. Bescherming van de persoonlijke levenssfeer

Het wetsvoorstel strekt tot het vergroten van de weerbaarheid van de Nederlandse kennissector, om zo de sterke kennispositie van Nederland te behouden en fundamentele academische kernwaarden zoals de academische vrijheid, internationale samenwerking en open wetenschap te beschermen en de nationale veiligheid te waarborgen. Daartoe wordt met dit wetsvoorstel een preventieve screening geïntroduceerd voor individuele onderzoekers en studenten die aan Nederlandse kennisinstellingen toegang kunnen krijgen tot sensitieve technologie. Het wetsvoorstel behelst een inmenging van het recht op respect voor het privéleven respectievelijk een beperking van het recht op bescherming van de persoonlijke levenssfeer. Die inmenging bestaat uit het verrichten van een risico-beoordeling door middel van persoonsgericht onderzoek naar een screeningsplichtige waarvan de uitkomsten zullen worden betrokken bij de besluitvorming omtrent de screeningsuitkomst. Bescherming van de persoonlijke levenssfeer is een grondrecht dat zowel in internationaal als nationaal recht is vastgelegd.

Ten aanzien van het internationale recht zijn het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en het Handvest van de grondrechten van de Europese Unie (het Handvest) van belang. Aangezien het wetsvoorstel binnen het toepassingsgebied valt van het recht van de Europese Unie valt het tevens onder de werkingssfeer van het Handvest. Op grond van artikel 7 van het Handvest heeft eenieder recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie. In artikel 8 van het Handvest is bepaald dat eenieder tevens recht heeft op bescherming van de hem betreffende persoonsgegevens. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan. In artikel 8 van het EVRM zijn deze rechten op vergelijkbare wijze opgenomen, waarin is bepaald dat een ieder recht heeft op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Dit betreft geen absoluut recht. Uit het tweede lid van artikel 8 van het EVRM volgt dat inmenging in de uitoefening van dit recht slechts is toegestaan wanneer dit bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Ingevolge artikel 10, eerste lid, van de Grondwet heeft een ieder, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. Dit betekent dat beperkingen op dit grondrecht slechts zijn toegestaan indien dit, direct of indirect, herleidbaar is naar een wettelijke grondslag. Dit wetsvoorstel voorziet in de wettelijke grondslag voor een gerechtvaardigde beperking op het recht op privéleven.

Wet- en regelgeving die het recht op privéleven beperkt, moet duidelijk, voorzienbaar en voldoende toegankelijk zijn voor degenen die hierdoor worden geraakt, in dit geval onderzoekers en studenten. Een wet is voldoende duidelijk en voorzienbaar als zij een adequate indicatie geeft van de voorwaarden en omstandigheden waaronder autoriteiten bevoegd zijn om maatregelen te nemen. Verder moet de inmenging in het privéleven een legitiem doel dienen en in een democratische samenleving noodzakelijk zijn. De inmenging in het privéleven in dit wetsvoorstel kan door het belang van de nationale veiligheid worden gerechtvaardigd en dient daarom een legitiem doel.

In de jurisprudentie van het Europese Hof voor de Rechten van de Mens wordt aan de eis dat de inperking 'in een democratische samenleving noodzakelijk is' geacht te zijn voldaan als er sprake is van een dringende maatschappelijke behoefte. In dat kader is tevens van belang dat de maatregel proportioneel is en dat er geen alternatieven mogelijk zijn die minder ingrijpend zijn (subsidiariteit).

Legitiem doel
Het belang van de staat is primair gelegen in het beschermen van de nationale veiligheid. Ook een florerende kenniseconomie, het ongestoord functioneren van de economie, en een bloeiende wetenschap zijn aan te merken als belangen van de staat. Internationale samenwerking blijft noodzakelijk. Open wetenschapsbeoefening en internationale samenwerking worden slechts ingeperkt indien sprake is van (potentiële) risico's voor de nationale veiligheid. Bij de screening kennisveiligheid gaat het specifiek om de toegang tot technologieën die als sensitief in het licht van de nationale veiligheid moeten worden aangemerkt. De staat wil met de screening kennisveiligheid voorkomen dat die technologie of kennis hierover via individuen weglekken naar statelijke actoren die gebruik van deze technologie kunnen maken met nadelige gevolgen voor de nationale veiligheid.

Geschiktheid van het middel
Allereerst is het goed nogmaals te benadrukken dat het doel van de screening kennisveiligheid het voorkomen en mitigeren van risico's voor de nationale veiligheid is en niet om alle risico's volledig uit te sluiten. Het geheel voorkomen en mitigeren van ongewenste kennis- en technologieoverdracht is niet mogelijk. Ook blijft het noodzakelijk om samen te werken in geval van wetenschappelijk onderzoek. Bij de motivering van de instrumentkeuze in paragraaf 2.4 is reeds ingegaan op de effectiviteit van screening als instrument.

Ten behoeve van het voorkomen en mitigeren van ongewenste kennis- en technologieoverdracht die kan leiden tot een risico voor de nationale veiligheid is het instrument van de screening kennisveiligheid naar het oordeel van de regering een geschikt middel. Daarbij is het van belang om op te merken dat maatregelen en instrumenten die reeds zien op de bescherming tegen ongewenste kennis- en technologieoverdracht, zoals informatiebeveiligingsmaatregelen, niet zijn toegespitst op een beoordeling van de betrouwbaarheid en integriteit van individuele betrokkenen. Het screenen van onderzoekers en masterstudenten die toegang krijgen tot sensitieve kennis en technologie is noodzakelijk om ongewenste kennis- en technologieoverdracht te voorkomen. Daarmee kunnen risico's voor de nationale veiligheid zoveel mogelijk worden beperkt. Wanneer de betrouwbaarheid en integriteit van personen met toegang tot deze kennis en technologie niet gecontroleerd is, blijft het risico immers bestaan dat informatie via hen in verkeerde handen kan komen. De gevolgen daarvan zijn onomkeerbaar of slechts in zeer beperkte mate achteraf te herstellen door te treffen maatregelen en bijvoorbeeld sanctionering. Het is dus noodzakelijk om voorafgaand aan de toegang tot sensitieve kennis en technologie de achtergrond, motieven en mogelijke risico's van de betrokken personen te beoordelen.

Zoals reeds uiteengezet in paragraaf 2.1 en 2.2 wordt voor de onderbouwing van de dreiging en het dreigingsbeeld gekeken naar onder meer het DBSA 1 en DBSA 2 en de

jaarverslagen van de inlichtingen- en veiligheidsdiensten. In de dreigingsbeelden wordt bevestigd dat Nederlandse kennisinstellingen doelwit zijn van statelijke actoren die proberen hoogwaardige kennis en technologie te bemachtigen om de eigen militaire, technologische, politieke en economische macht te vergroten, of om kennis en technologie te verwerven die ingezet kan worden voor de versterking van het eigen militaire apparaat. Uit de dreigingsbeelden blijkt dat statelijke actoren op grote schaal activiteiten ondernemen om kennis en technologie te verwerven op Nederlandse kennisinstellingen. Ongewenste kennis- en technologieoverdracht via personen wordt ook wel de 'insider threat' genoemd. Deze 'insider threat' betreft de dreiging die uitgaat van onderzoekers en studenten die studeren of werken, of hebben gestudeerd of gewerkt, binnen Nederlandse kennisinstellingen. Statelijke actoren maken daarbij gebruik van verschillende methoden. Ongewenste kennis- en technologieoverdracht kan derhalve plaatsvinden via personen, om welke reden is gekozen voor de screening kennisveiligheid, waarbij risico's rondom een persoon in kaart kunnen worden gebracht. De dreiging van ongewenste kennis- en technologieoverdracht komt blijkens de hiervoor genoemde bronnen hoofdzakelijk vanuit bepaalde statelijke actoren van buiten de EU die sensitieve technologie en kennis willen bemachtigen voor doeleinden die een risico kunnen opleveren voor de nationale veiligheid. Zoals uiteengezet in paragraaf 4.2 is de dreiging daarmee niet hoofdzakelijk afkomstig van derdelanders, maar kan zich deze eveneens voordoen onder Unieburgers, waaronder Nederlanders.

Het kabinet is van mening dat de screening kennisveiligheid daardoor effectief zal zijn in het licht van de geconstateerde dreiging, door risico's voorafgaand aan de toegang tot sensitieve technologie en een hoog-risico onderdeel zo scherp en risicogericht als mogelijk te voorkomen en mitigeren. Een screening van studenten en onderzoekers die toegang willen krijgen tot een hoog-risico onderdeel is daardoor een geschikt middel om risico's op ongewenste kennis- en technologieoverdracht te voorkomen of mitigeren. Met de screening zoals omschreven in paragraaf 3 kunnen risico's rondom ongewenste kennis- en technologieoverdracht in kaart worden gebracht. Daarmee biedt een screeningsuitkomst voldoende beeld van de relevante aspecten om potentiële risico's voor de nationale veiligheid te kunnen identificeren.

Tot slot zijn bestaande screeningsinstrumenten, zoals de VOG en de VGB, geen geschikte alternatieve middelen gebleken, zoals reeds uiteengezet in paragraaf 2.5 van dit voorstel.

Proportionaliteit
Naast het belang van de staat, staat het belang van het individu. De individuele student of onderzoeker heeft als belang het kunnen volgen van een studie of het kunnen doen van onderzoek op een specifiek vakgebied. Hij of zij wil kort gezegd samenwerken en daarbij de eigen kennis vergroten of een bijdrage leveren aan onderzoek. Belangrijk is dat er geen sprake is van een absoluut recht, het individu heeft geen absoluut recht om op een hoog-risico onderdeel te mogen komen studeren of onderzoek te komen doen. Onderzoek of studie op een onderdeel dat niet als hoog-risico onderdeel is aangemerkt, zonder eerst een preventieve screening te hoeven ondergaan, blijft ook mogelijk.

Met dit wetsvoorstel wordt bovendien voorzien in effectieve rechtsbescherming, zodat de individuele student of onderzoeker die aan een screening kennisveiligheid wordt onderworpen in rechte voor zijn belangen en tegen het screeningsbesluit kan opkomen. Het screeningsbesluit is daarom een voor bezwaar en beroep vatbaar besluit dat voor de bestuursrechter kan worden aangevochten.

Met de afbakening van de sensitieve technologieën en de risicogerichte aanpak bij de vaststelling van de hoog-risico onderdelen wordt de doelgroep beperkt tot het noodzakelijke; alleen daar waar de risico's voor de nationale veiligheid het grootst zijn is een screeningsplicht aan de orde. Doordat het aannemelijk is dat in het geval van de betreffende technologie en het betreffende onderdeel inderdaad aantoonbaar risico voor

de nationale veiligheid kan bestaan, kan worden gezegd dat het belang van de staat bij het beschermen van de betreffende technologie en het betreffende onderdeel tegen ongewenste kennis- en technologieoverdracht zwaarder weegt dan het belang van het individu en de nadelige gevolgen van de screening voor het individu.

Ook met de doelgroepverruiming waarna iedereen, ongeacht nationaliteit of verblijfsstatus, wordt gescreend, blijft de maatregel proportioneel. Zoals in paragraaf 4.2 is uiteengezet is bij de gehele doelgroep sprake van mogelijke risico's.

Daarnaast dient voor de proportionaliteit van de maatregel ook een afweging te worden gemaakt tussen enerzijds nationale veiligheid en anderzijds het belang van open wetenschapsbeoefening. De screening kennisveiligheid is proportioneel wanneer risico's op ongewenste kennis- en technologieoverdracht, en daarmee voor de nationale veiligheid, zoveel mogelijk worden voorkomen en gemitigeerd, en daarmee het behoud van fundamentele academische waarden zoals de academische vrijheid, en veilige internationale samenwerking veilig worden gesteld. Daarbij is een balans gevonden tussen enerzijds de baten en anderzijds de lasten van het instrument. Open wetenschapsbeoefening en internationale samenwerking worden slechts ingeperkt indien sprake is van (potentiële) risico's voor de nationale veiligheid.

Subsidiariteit
In paragraaf 2.6 is reeds uiteengezet welke alternatieven zijn overwogen. Hieruit blijkt waarom de screening kennisveiligheid zoals geregeld in dit wetsvoorstel, het meest geschikte middel is om de doelstelling, de bescherming van de nationale veiligheid, te bereiken, en waarom de beschreven alternatieven niet of minder geschikt hiervoor zijn.

5.1.2. Bescherming persoonsgegevens

Artikel 10, tweede en derde lid, van de Grondwet geeft opdrachten aan de wetgever om regels te stellen in het kader van het verwerken van persoonsgegevens. Het tweede lid geeft de wetgever opdracht regels te stellen ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Het derde lid geeft de wetgever de specifieke opdracht om regels te stellen betreffende de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van de vastgelegde gegevens.

De Algemene Verordening Gegevensbescherming (AVG) is het wettelijk kader omtrent de bescherming van persoonsgegevens in de Europese Unie. Daarnaast geldt in Nederland de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Deze wet geeft uitvoering aan de AVG voor zover dit de regels betreffen die door lidstatelijk recht kunnen worden gespecificeerd of beperkt.

Onder *verwerking* wordt op grond van artikel 4, onder 2, van de AVG verstaan: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

De omvang en de aard van de verwerking van persoonsgegevens in het kader van de screening zullen variëren afhankelijk van de omstandigheden van het geval. Daarom moet ingevolge de AVG worden getoetst of de verwerking van de persoonsgegevens krachtens dit wetsvoorstel rechtmatig plaatsvindt en voldoet aan de beginselen van gegevensverwerking. Deze beginselen zijn opgenomen in artikel 5 van de AVG.

Rechtmatigheid, behoorlijkheid en transparantie
Artikel 5, eerste lid, onderdeel a, van de AVG vereist dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. In artikel 17, eerste lid, van het wetsvoorstel is expliciet vastgelegd dat de Minister persoonsgegevens kan verwerkten verwerkt voor zover dit noodzakelijk is voor de uitvoering van deze wet, dat wil zeggen voor de uitvoering van de (op bescherming van de nationale veiligheid en handhaving van internationale sanctiemaatregelen gerichte[90]) screening kennisveiligheid.

De Minister en de met dit voorstel aangewezen partijen mogen persoonsgegevens verwerken op grond van artikel 6, eerste lid, onderdeel c en e, juncto artikel 6, derde lid, van de AVG. Als gegevens verwerkt worden, is dit namelijk noodzakelijk om te voldoen aan de wettelijke verplichtingen, hetgeen op volgens artikel 6, eerste lid, onderdeel c, van de AVG een rechtmatige grond vormt voor de verwerking. Ook is de verwerking noodzakelijk voor de vervulling van een taak in het kader van de uitoefening van het openbaar gezag dat aan de Minister is opgedragen. Deze taak ziet op de bescherming tegen risico's voor de nationale veiligheid die voortvloeien uit ongewenste kennis- en technologieoverdracht. Dit vormt krachtens artikel 6, eerste lid, onderdeel e, van de AVG een rechtmatige grond voor de verwerking. In lijn met artikel 6, derde lid, van de AVG worden deze rechtsgronden door middel van dit wetsvoorstel die van toepassing is op de verwerkingsverantwoordelijke, zijnde de Minister, vastgelegd in nationaal recht.

Doelbinding
Uit artikel 5, eerste lid, onderdeel b, van de AVG volgt dat persoonsgegevens slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwekt (doelbinding). Op grond van artikel 17, eerste lid, van het wetsvoorstel kunnen persoonsgegevens worden verwerkt door de minister van OCW voor zover dit noodzakelijk is voor de uitvoering van deze wet, dat wil zeggen voor de uitvoering van de screening kennisveiligheid. Met deze bepaling en een aantal andere bepalingen die hierna worden besproken, wordt het doel waarvoor persoonsgegevens mogen worden verwerkt verankerd.

Een deel van de persoonsgegevens die door de minister van OCW kunnen worden verwerkt in het kader van de screening, is oorspronkelijk voor andere doelen verzameld. Voor deze (verdere) verwerking van persoonsgegevens verschaft hetzij dit wetsvoorstel (artikelen 17 en 18) een wettelijke grondslag, waarbij de uitvoering van de screening kennisveiligheid als doel is vastgelegd, hetzij zal bij of krachtens een tweetal andere wetten, de Wet justitiële en strafvorderlijke gegevens en de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) een wettelijke grondslag worden gecreëerd. Ter toelichting op dit laatste wordt het volgende opgemerkt.

Met dit wetsvoorstel kunnen mede strafrechtelijke persoonsgegevens worden verwerkt. Hiertoe is in artikel 17, eerste lid, van het wetsvoorstel geregeld dat gegevens verkregen krachtens de Wet justitiële en strafvorderlijke gegevens kunnen worden verwerkt voor zover dit noodzakelijk is voor de uitvoering van de Wet screening kennisveiligheid. Het Justitieel Documentatie Systeem (JDS) is het informatieregister over de justitiële documentatie en wordt beheerd door de Justitiële Informatiedienst (Justid), onderdeel van het ministerie van Justitie en Veiligheid. Verwerking van strafrechtelijke gegevens geschiedt met inachtneming van de Wet justitiële en strafvorderlijke gegevens (Wjsg). Voor de verwerking van strafrechtelijke gegevens voor het doel van dit wetsvoorstel zal – conform de systematiek van de Wjsg – een grondslag worden opgenomen in het Besluit justitiële en strafvorderlijke gegevens. Daarmee wordt tevens voldaan aan het vereiste van artikel 3, tweede lid, Wjsg, dat stelt dat justitiële gegevens slechts verwerkt

[90] Zie artikel 9 wetsvoorstel.

mogen worden voor zover dit noodzakelijk is voor de bij of krachtens de Wjsg geformuleerde doeleinden.

In het geval de screeningsplichtige (ook) beschikt over de nationaliteit van een Europese lidstaat, (ook) onderdaan is van een derde land, of wanneer de nationaliteit van de screeningsplichtige onbekend is of de screeningsplichtige is staatloos, kan Justid ook gebruik maken van het Europees strafregisterinformatiesysteem, bestaande uit Ecris en Ecris-TCN. De Wjsg omvat de doelen voor het gebruik van Ecris en Ecris-TCN voor zover deze voortvloeien uit Europese regelgeving. Door middel van een wijziging van de Wjsg wordt een extra grond toegevoegd aan artikel 2a, eerste lid, Wjsg voor het verwerken van deze persoonsgegevens ten behoeve van de uitvoering van de screening kennisveiligheid.

In bepaalde gevallen kunnen de inlichtingen- en veiligheidsdiensten worden verzocht om na te gaan of er ten aanzien van een bepaalde persoon relevante gegevens beschikbaar zijn. Dit betreft een van de verdiepende opties die is toegelicht in de paragraaf 2.6. De Minister van OCW kan, voor zover dit noodzakelijk is voor de uitvoering van deze wet, de Minister van Binnenlandse Zaken en Koninkrijksrelaties verzoeken een mededeling als bedoeld in artikel 8, tweede lid, onderdeel f, van de Wiv 2017 te doen of de Minister van Defensie verzoeken een mededeling als bedoeld in artikel 10, tweede lid, onderdeel g, van die wet te doen. De regels omtrent het aanwijzen van personen of instanties die een verzoek om mededeling kunnen doen omtrent door de diensten verwerkte gegevens omtrent personen of instanties zijn opgenomen in de Regeling naslag Wiv 2017. Artikel 2 van de Regeling naslag Wiv 2017 bevat een limitatieve opsomming van de gevallen waarin een verzoek tot naslag kan worden gericht aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties. In artikel 4 van de Regeling naslag Wiv 2017 zijn de gevallen benoemd waarin een verzoek door de tevens in het artikel benoemde personen en instanties kan worden gericht aan de Minister van Defensie voor het doen van naslag. De Regeling naslag Wiv 2017 zal voor dit doel worden gewijzigd, zodat ten behoeve van de screening kennisveiligheid de bedoelde naslagverzoeken kunnen worden gedaan. In verband hiermee is in artikel 17, eerste lid, van het wetsvoorstel geregeld dat gegevens verkregen krachtens de Wiv 2017 kunnen worden verwerkt voor zover dit noodzakelijk is voor de uitvoering van de Wet screening kennisveiligheid.

Minimale gegevensverwerking
Verder mogen persoonsgegevens volgens het beginsel van minimale gegevensverwerking alleen worden verwerkt indien zij toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, ingevolgde artikel 5, eerste lid, onderdeel c, van de AVG (minimale gegevensverwerking). De persoonsgegevens die voor de uitvoering van dit wetsvoorstel zullen worden verwerkt, zijn noodzakelijk ter beoordeling of er in een individueel geval sprake kan zijn van een risico op ongewenste kennis- en technologieoverdracht. In artikel 17, eerste lid, onderdelen a tot en met c, van het wetsvoorstel is beschreven uit welke bronnen gegevens, waaronder persoonsgegevens, afkomstig kunnen zijn. Als basisprincipe geldt dat specifieke gegevens slechts zullen worden betrokken voor zover dat noodzakelijk is ter uitvoering van het wetsvoorstel. Artikel 18 van het wetsvoorstel bevat een uitputtende opsomming van natuurlijke personen, rechtspersonen of bestuursorganen die gegevens kunnen verstrekken aan de Minister, indien en voor zover dit noodzakelijk is voor de uitvoering van de screening. Het grootste deel van de gegevens zullen door de screeningsplichtige zelf worden verstrekt aan de screeningsautoriteit. In het aanvraagformulier dienen persoonsgegevens te worden vermeld die noodzakelijk zijn om te komen tot een gedegen risicobeoordeling, in overeenstemming met het doel van de screening. Deze gegevens betreffen de NAW-gegevens, geboortedatum, gebruikersnamen op sociale media, informatie over een eventuele partner en directe familieleden, een kopie van het legitimatiebewijs, diploma's en een publicatielijst. Deze persoonsgegevens zijn noodzakelijk voor de uitvoering van dit wetsvoorstel en direct gerelateerd aan de beoordelingscriteria zoals genoemd in

paragraaf 3.1 die worden gebruikt om het risico op ongewenste kennis- en technologieoverdracht zoals bedoeld in dit wetsvoorstel te kunnen beoordelen.

Strafrechtelijke gegevens
Naast bovenstaande algemene persoonsgegevens is met dit wetsvoorstel tevens voorzien in een grondslag om justitiële gegevens in de zin van de Wet justitiële en strafvorderlijke gegevens te verwerken, zoals informatie over strafrechtelijke veroordelingen van onderzoekers of studenten, ook in andere EU-lidstaten. Dit is in lijn met artikel 10 van de AVG, dat bepaalt dat de verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid, of als dit bij lidstatelijk recht of Unierecht geregeld is. Verder geschiedt het verstrekken van justitiële gegevens met inachtneming van de Wet justitiële en strafvorderlijke gegevens. Op de daarop volgende verwerking van deze gegevens ten behoeve van het nemen van een screeningsbesluit is de AVG van toepassing en de regels voor de verwerking van persoonsgegevens van strafrechtelijke aard die in de UAVG zijn opgenomen.

Bij het gebruik van justitiële gegevens gaat het expliciet niet om alle justitiële informatie, maar uitsluitend om die informatie die relevant is voor de beoordeling of er sprake kan zijn van een risico op ongewenste kennis- en technologieoverdracht en daarmee van een risico voor de nationale veiligheid. Het kan bijvoorbeeld gaan om veroordelingen voor misdrijven tegen de veiligheid van de staat, schending van ambtsgeheimen, valsheid in geschrift, fraude en diefstal. Indien justitiële gegevens niet zouden worden meegewogen in de screening, kan mogelijk zeer relevante informatie niet betrokken worden bij de risicobeoordeling van de screening kennisveiligheid. Dit zou de screening kennisveiligheid aanzienlijk minder effectief maken en kan in bepaalde gevallen leiden tot aanzienlijke risico's voor de nationale veiligheid. Dit kan bijvoorbeeld het geval zijn als een onderzoeker of student veroordeeld is voor een relevant delict, zoals het opzettelijk verstrekken van staatsgeheime informatie aan een buitenlandse mogendheid, maar desondanks toegang zou krijgen tot sensitieve kennis en technologie op een onderdeel van een kennisinstelling doordat een positief screeningsbesluit is genomen waarbij het strafrechtelijk verleden geen onderdeel is geweest van de risicobeoordeling. Het betrekken van justitiële gegevens heeft tot slot ook een signaalfunctie en een preventieve werking.

Met dit voorstel wordt geregeld dat het strafrechtelijk verleden van een onderzoeker of student kan worden betrokken bij de beoordeling of toelating tot de kennisinstelling geoorloofd is met het oog op hetgeen is bepaald in deze wet. De onderzoeker of student die voornemens is te gaan studeren of onderzoek te gaan doen aan een onderdeel van een kennisinstelling en die daarbij toegang zou krijgen tot sensitieve technologie, dient in het aanvraagformulier informatie op te geven over een eventueel strafrechtelijk verleden. De screeningsautoriteit beoordeelt de aangeleverde informatie en raadpleegt het Justitieel Documentatie Systeem (JDS), en indien relevant justitiële documentatie uit EU-lidstaten, verkregen via Ecris of Ecris-TCN. Het wetsvoorstel voorziet in een grondslag voor een ministeriële regeling waarin limitatief zal worden geregeld welke strafbare feiten kunnen worden betrokken in de risicobeoordeling.[91]

Beperking van de verwerking van strafrechtelijke gegevens
In het geval een screeningsplichtige uitsluitend de Nederlandse nationaliteit bezit, wordt het JDS geraadpleegd. Het JDS wordt beheerd door de Justitiële Informatiedienst (Justid). Justid is, als daartoe aangewezen autoriteit, de ontvanger en verstrekker van de persoonsgegevens en strafrechtelijke gegevens uit het JDS. De screeningsautoriteit kan in eerste instantie door middel van een geautomatiseerde hit/no hit-bevraging controleren of zich daarin gegevens over de screeningsplichtige bevinden. Zijn er geen (relevante) justitiële gegevens over de persoon, dan wordt dit geautomatiseerd teruggekoppeld. Als het JDS wel gegevens bevat over de aanvrager, dan volgt een

[91] Zie artikel 12 wetsvoorstel.

geautomatiseerd signaal van een hit. In dat geval worden de inhoudelijke gegevens geraadpleegd. Deze uitwisseling van gegevens tussen Justid en de screeningsautoriteit omvat de uitkomsten van het onderzoek naar strafrechtelijke gegevens.

In het geval een screeningsplichtige onder andere beschikt over de nationaliteit van een Europese lidstaat, wordt Ecris bevraagd. In Ecris wordt informatie over strafregisters elektronisch uitgewisseld tussen de centrale autoriteiten van de lidstaten van de Europese Unie. Elke lidstaat houdt een database bij van alle onherroepelijke veroordelingen die jegens zijn onderdanen zijn uitgesproken door strafrechters in de andere EU-lidstaten, naast alle veroordelingen die in de lidstaat zelf zijn uitgesproken. Elke centrale autoriteit van de lidstaten is verplicht om alle via Ecris ontvangen informatie op te slaan en bij te werken, en om volledige informatie over strafregisters te verstrekken (antwoorden op verzoeken) wanneer daarom door een andere lidstaat wordt gevraagd (verzoeken om informatie). Justid is, als daartoe aangewezen centrale autoriteit in Nederland, de ontvanger en verstrekker van de persoonsgegevens en strafrechtelijke gegevens na bevraging van Ecris. Deze uitwisseling van gegevens tussen de screeningsautoriteit, Justid en de daartoe aangewezen autoriteit van de lidstaat omvatten strafrechtelijke gegevens.

Indien een screeningsplichtige (ook) onderdaan is van een derde land, of wanneer de nationaliteit van de screeningsplichtige onbekend is of de screeningsplichtige staatloos is, wordt Ecris-TCN geraadpleegd. Ecris-TCN is een gecentraliseerd systeem waarmee de centrale autoriteiten van de lidstaten kunnen identificeren welke andere lidstaten strafrechtelijke informatie hebben over derdelanders of staatlozen die worden gecontroleerd, zodat ze vervolgens het bestaande Ecris-systeem kunnen gebruiken om informatieverzoeken aan de geïdentificeerde lidstaten te richten. Ecris-TCN is in ontwikkeling en wordt beheerd door eu-LISA. Naar verwachting is ECRIS-TCN in de eerste helft van 2026 volledig operationeel. In eerste instantie kan een 'hit/no hit'-zoekopdracht worden uitgevoerd in het centrale TCN-systeem (European Search Portal). Hiermee wordt gecontroleerd of er gegevens over de screeningsplichtige zijn opgenomen in het systeem. Op die manier kan snel worden achterhaald in welke andere lidstaat(en) informatie over eerdere veroordelingen van een niet-EU-onderdaan is opgeslagen. Een "hit" identificeert de lidstaat die een bepaalde derdelander heeft veroordeeld. In het geval van een “hit” wordt vervolgens een informatieverzoek gericht aan de betreffende lidstaat om volledige strafregisterinformatie te verstrekken. De ontvangende lidstaat reageert conform zijn nationale wetgeving. Er is geen richtlijn die verplicht om inhoudelijk te reageren op een informatieverzoek. Justid is, als daartoe aangewezen autoriteit, de ontvanger en verstrekker van de persoonsgegevens en strafrechtelijke gegevens na raadpleging van Ecris-TCN. Deze uitwisseling van gegevens tussen de screeningsautoriteit, Justid en de daartoe aangewezen autoriteit van de lidstaat omvatten strafrechtelijke gegevens.

Bijzondere persoonsgegevens
Tot slot kunnen in het kader van de screening ook bijzondere persoonsgegevens worden verwerkt. Dit zijn, ingevolge artikel 9, eerste lid, AVG, gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

In beginsel is het verwerken van bijzondere persoonsgegevens verboden, tenzij aan een van de voorwaarden van artikel 9, tweede lid, AVG is voldaan. In het kader van dit wetsvoorstel is de uitzonderingsgrond genoemd in artikel 9, tweede lid, onder g, AVG van toepassing. Hieruit volgt dat de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en

specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. Het criterium dat van een zwaarwegend algemeen belang sprake moet zijn, houdt in dat het een algemeen belang betreft dat in de betreffende situatie zodanig is dat het zwaarder weegt dan het belang van de bescherming tegen inbreuk op de persoonlijke levenssfeer door het verwerken van bijzondere persoonsgegevens. In dit geval is daarbij relevant om op te merken dat het algemeen belang bestaat uit de bescherming tegen risico's voor de nationale veiligheid die kunnen voortvloeien uit ongewenste kennis- en technologieoverdracht en uit de handhaving van internationale sanctieregelgeving. Om te komen tot een gedegen risicobeoordeling kan het in specifieke situaties noodzakelijk zijn om een verdiepende screeningsoptie te benutten.

Onderdeel van de verdiepende opties is het verrichten van een OSINT-onderzoek (open source intelligence). De screeningsautoriteit krijgt hiervoor een wettelijke bevoegdheid toegekend in het wetsvoorstel.[92] Bij het OSINT-onderzoek worden gegevens verwerkt uit voor een ieder toegankelijke informatiebronnen. Op voorhand is niet te voorzien welke persoonsgegevens bij het OSINT-onderzoek zullen worden verwerkt. Dit kan per casus verschillen en is afhankelijk van de persoonsgegevens die in openbare bronnen is opgenomen en geraadpleegd kunnen worden gedurende het onderzoek. Aangezien op voorhand niet te bepalen is welke categorieën persoonsgegevens zullen worden verwerkt bij het OSINT-onderzoek is het mogelijk dat naast algemene ook bijzondere (en strafrechtelijke) persoonsgegevens verwerkt kunnen worden. De voor een ieder toegankelijke informatiebronnen die bij het OSINT-onderzoek worden geraadpleegd, kunnen allerlei (gevoelige) persoonsgegevens bevatten. Daarbij kunnen ook (indirect herleidbare) persoonsgegevens van derden kunnen verwerkt. Tijdens het OSINT-onderzoek worden personen niet gevolgd of gemonitord, er wordt alleen gezocht naar gepubliceerde gegevens. Van belang hierbij is dat de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. Deze maatregelen bestaan onder andere uit strikte beveiliging ten aanzien van de werkomgeving waarin de gegevensverwerkingen plaatsvinden en een beperking van de medewerkers die bevoegd zullen zijn om OSINT-onderzoeken te verrichten. Zij zijn daartoe speciaal opgeleid en gespecialiseerd en zijn bij uitstek in staat om alleen daadwerkelijk relevante gegevens met het oog op het doel verder te verwerken, voor zover dat noodzakelijk is. Een uitzonderlijk geval waarin dat noodzakelijk kan zijn, is als gedurende het OSINT-onderzoek blijkt dat een screeningsplichtige innige (politieke) banden heeft met een statelijke actor waarvan uit dreigingsbeelden blijkt dat deze op grote schaal activiteiten onderneemt om kennis en technologie te verwerven op Nederlandse kennisinstellingen. In een dergelijk specifiek geval, kunnen deze gegevens blijk geven van de politieke opvattingen van de screeningsplichtige. Het belang van het beschermen van de nationale veiligheid weegt in die gevallen zwaarder dan het voorkomen van een inbreuk op de persoonlijke levenssfeer door het verwerken van bijzondere persoonsgegevens. Daarbij dient te worden opgemerkt dat verdiepende opties, waaronder het OSINT-onderzoek, slechts in specifieke gevallen zullen worden ingezet, indien risico's zijn gesignaleerd naar aanleiding van de eerdere onderdelen van het screeningsproces. Zodoende worden de gevallen waarin verdiepende opties zullen worden ingezet zoveel mogelijk beperkt waardoor ook de verwerking van bijzondere persoonsgegevens zo veel mogelijk wordt beperkt.

Proportionaliteit

[92] Artikel 17, eerste lid, onderdeel c, wetsvoorstel.

De verwerking van de in dit wetsvoorstel beschreven persoonsgegevens is proportioneel omdat op geen andere wijze de risico's op ongewenste kennis- en technologieoverdracht kunnen worden beoordeeld en omdat een risico-beoordeling op persoonsniveau moet worden gemaakt. Door de persoonsgegevens duidelijk af te bakenen en alleen te verwerken om risico's in een individueel geval te beoordelen gaat de gegevensverwerking niet verder dan noodzakelijk is. Ook bevat het screeningsproces enkele verdiepende opties die alleen zullen worden benut indien dat noodzakelijk is om een gedegen risicoanalyse te kunnen opstellen. Als het aanwenden van deze verdiepende opties, zoals het verrichten van OSINT-onderzoek, het afnemen van een interview of het richten van een verzoek tot naslag aan de inlichtingen- en veiligheidsdiensten, niet nodig is ter vervulling van de taak in het kader van de uitoefening van het openbaar gezag, zal dit achterwege blijven. Hiermee wordt geborgd dat de gegevensverwerking niet verder gaat dan noodzakelijk is.

Juistheid
Het beginsel van juistheid dat volgt uit artikel 5, eerste lid, onderdeel d, van de AVG, vereist dat persoonsgegevens juist zijn en zo nodig worden geactualiseerd en dat alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. Voor het maken van een deugdelijke risicobeoordeling en het uitvoeren van de wettelijke taak door de Minister, is het daarom van belang dat de gegevens die over een onderzoeker of student worden verwerkt, juist zijn. Ten behoeve van een goede uitvoering van de screening is het benodigd dat het nationaal identificatienummer (in Nederland: BSN) van de screeningsplichtige wordt verwerkt. Het gebruik van het nationaal identificatienummer van de screeningsplichtige minimaliseert de kans op onjuistheden bij het onderzoek naar het strafrechtelijk verleden van de screeningsplichtige. Daarmee vormt het verwerken van het nationaal identificatienummer een belangrijke waarborg tegen persoonsverwisselingen die kunnen leiden tot het screenen van de verkeerde persoon. Aan het verwerken van het nationaal identificatienummer zijn beperkte privacy risico's verbonden. Een van die risico's is dat de gegevens kunnen belanden bij een onbevoegd persoon, hetgeen kan leiden tot identiteitsfraude. Dit risico wordt echter geminimaliseerd door de technische en organisatorische maatregelen die zullen worden getroffen. Dit is in lijn met artikel 87 van de AVG, dat stelt dat voor het verwerken van het nationaal identificatienummer passende waarborgen voor de rechten en vrijheden van de betrokkene worden getroffen. Een belangrijk deel van de persoonsgegevens die worden verwerkt, wordt door de onderzoeker of student zelf aangeleverd middels het formulier bij de aanvraag van de screening. Dit zal bijdragen aan het bevorderen van de juistheid van deze informatie. Tot slot geldt op grond van artikel 3:2 van de Awb dat de Minister het zorgvuldigheidsbeginsel moet toepassen. Dat vereist dat geconstateerde fouten gerectificeerd moeten kunnen worden.

Opslagbeperking
Verder geldt ingevolge artikel 5, eerste lid, onderdeel e, van de AVG het beginsel van opslagbeperking. Dit betekent dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking. Om te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk, wordt onderscheid gemaakt tussen positieve screeningsbesluiten (geen bezwaar tegen toegang tot de kennisinstelling) en negatieve screeningsbesluiten (bezwaar tegen toegang tot de kennisinstelling). Bij een positief besluit geldt als bewaartermijn twee jaar na het opslaan van de gegevens. De bewaartermijn sluit daarmee aan bij het doel, te weten: de beoordeling van de geschiktheid van de screeningsplichtige met het oog op toegang tot de kennisinstelling. Teneinde nog verantwoording af te kunnen leggen over de inhoud van het screeningsbesluit, en daarin inzicht te kunnen geven, eindigt de bewaartermijn twee jaar nadat de gegevens zijn opgeslagen.

Bij een negatief screeningsbesluit wordt de screeningsplichtige niet toegelaten tot een kennisinstelling in verband met risico's voor de nationale veiligheid. De noodzaak tot bewaring van de persoonsgegevens is in die gevallen anders, aangezien dit direct raakt aan het belang van bescherming van de nationale veiligheid. Voor gegevens die wijzen op risico's voor de nationale veiligheid geldt dat deze voor langere duur moeten kunnen worden bewaard om toekomstige risico's te kunnen beperken en te voorkomen. Een bewaartermijn van 15 jaar wordt proportioneel geacht gezien de noodzaak om nationale veiligheidsrisico's te beheren en is proportioneel gezien de ernst van deze risico's.

Integriteit en vertrouwelijkheid
De AVG vereist tot slot dat persoonsgegevens op passende wijze beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Dit is het beginsel van integriteit en vertrouwelijkheid en is neergelegd in artikel 5, eerste lid, onderdeel f, van de AVG. Dit betekent dat passende technische en organisatorische maatregelen moeten worden getroffen om hier aan te voldoen.

De verwerking van persoonsgegevens vindt plaats bij de screeningsautoriteit. Het verwerken van persoonsgegevens geschiedt uitsluitend in het kader van concrete screeningsaanvragen waarbij de screeningsplichtige in een beveiligde digitale omgeving het aanvraagformulier invult. De aanvragen worden elektronisch opgeslagen in een beveiligde database die uitsluitend toegankelijk is voor geautoriseerd personeel van de screeningsautoriteit. De verwerking van de gegevens gebeurt grotendeels geautomatiseerd.

Aangezien de screeningsautoriteit zowel gewone als bijzondere persoonsgegevens verwerkt in het kader van deze wet, moet worden voldaan aan verschillende beveiligingskaders en wettelijke verplichtingen. De belangrijkste zijn de AVG en de UAVG, de Baseline Informatiebeveiliging Overheid (BIO) en het Voorschrift Informatiebeveiliging Rijksdienst (VIRBI 2013). Artikel 32 van de AVG vereist passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking. Artikel 9 AVG stelt aanvullende eisen die zien op de verwerking van bijzondere persoonsgegevens. De UAVG bevat aanvullende nationale regels voor de verwerking van bijzondere persoonsgegevens.

De BIO is het verplichte beveiligingskader voor overheidsorganisaties en semi-overheidsorganisaties. Het is gebaseerd op ISO 27001/27002 en beschrijft beveiligingsmaatregelen op basis van risicomanagement. Het VIRBI 2013 geldt voor rijksorganisaties die bijzondere categorieën gegevens verwerken, waaronder strafvorderlijke en bijzondere persoonsgegevens. Hierin worden strengere eisen gesteld aan de classificatie en beveiliging van gevoelige informatie.

De screeningsautoriteit treft passende technische en organisatorische maatregelen op het gebied van Informatiebeveiligingsbeleid, procedures en ICT om de rechtmatigheid, proportionaliteit en beveiliging van de gegevens zoveel mogelijk te garanderen. Hierbij wordt rekening gehouden met de aard en het doel van de gegevensverwerking, de stand der techniek en mogelijke privacy risico's voor betrokkenen. Ook zijn strikte beveiligingsmaatregelen van toepassing, waaronder encryptie van de opgeslagen gegevens en een beveiligde omgeving om de integriteit en vertrouwelijkheid van persoonsgegevens te waarborgen. Waar mogelijk zijn de maatregelen gericht op dataminimalisatie en pseudonimisering. Voornamelijk voor bijzondere categorieën persoonsgegevens, zoals strafgegevens over het justitieel verleden, zijn passende maatregelen en waarborgen van belang. [deze zullen in afstemming met de screeningsautoriteit nader worden uitgewerkt.]

Op de huisvesting is daarnaast het Normenkader Beveiliging Rijkskantoren 2.0 (NkBR) van toepassing. Het NkBR is een referentiekader en baseline van de beveiligingsmaatregelen voor rijkskantoren. In deze kaders staan onder andere op het

gebied van huisvesting beschreven welke beveiligingseisen van toepassing zijn per TBB-categorie. Hieruit blijkt dat de beoordelingsfase van de screening waarbij STG-C informatie wordt verwerkt enkel kan plaatsvinden in een zogenaamde Zone 3A. Dit heeft gevolgen voor de beveiligingsmaatregelen, waaronder de fysieke werkomgeving, de toegang, de digitale beveiliging en de manier van werken. Op het gebied van huisvesting betekent dit onder andere toegang via tourniquets/sluiswerking, aparte kaartlezers, detectiesystemen, afgesloten ruimtes en kluizen. [deze beveiligingsmaatregelen zullen in afstemming met de screeningsautoriteit nader worden uitgewerkt.]

Ingevolge de AVG wordt als verwerkingsverantwoordelijke aangemerkt de instantie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In artikel 17, tweede lid, van dit wetsvoorstel is de Minister van OCW aangewezen als verwerkingsverantwoordelijke. Hieruit volgt dat op de Minister van OCW de verantwoordingsplicht rust op grond van artikel 5, tweede lid, van de AVG. Die plicht ziet op naleving van de beginselen inzake de verwerking van persoonsgegevens in het kader van deze wet.

Ook de Minister van Justitie en Veiligheid en de Minister van Economische Zaken en bepaalde andere instanties zullen in nader te bepalen gevallen persoonsgegevens verwerken in het kader van de uitvoering van deze wet. In voorkomende gevallen neemt de Minister een screeningsbesluit in overeenstemming met de Minister van Justitie en Veiligheid, en indien van toepassing, de beleidsmatig verantwoordelijke Minister. Hiervoor is noodzakelijk dat ook andere Ministers dienen te beschikken over de benodigde informatie, waaronder persoonsgegevens.

Daarnaast wordt opgemerkt dat een aantal rechtspersonen en bestuursorganen gegevens verstrekken aan de minister van OCW ten behoeve van de screening, dan wel gegevens ontvangen van de minister van OCW ten behoeve van de uitvoering van hun (eigen) taken.[93] Voor deze verwerkingen van persoonsgegevens zijn deze instanties zelf aan te merken als verwerkingsverantwoordelijke.

5.2. Gelijke behandeling (artikel 14 EVRM, artikel 1 Twaalfde Protocol EVRM, artikel 26 IVBPR, artikel 21 Handvest van de grondrechten van de Europese Unie en artikel 1 Grondwet)

Met de in dit wetsvoorstel opgenomen doelgroepafbakening, wordt voor de screeningsplicht geen onderscheid gemaakt naar nationaliteit of verblijfsstatus. Er wordt wel een onderscheid gemaakt tussen onderzoekers, studenten en technische ondersteuners die actief willen zijn op een vakgebied waarbij toegang bestaat tot sensitieve technologie, en zij die actief willen zijn op een vakgebied waar geen sprake is van sensitieve technologie. De vraag kan worden gesteld hoe dit zich verhoudt tot het discriminatieverbod, dat in een aantal internationale verdragen en in de Grondwet is vastgelegd.

De toetsing aan het discriminatieverbod valt uiteen in een aantal vragen:
- Is er sprake van een verschil in behandeling?
- Indien er sprake is van een verschil in behandeling: gaat het bij degenen die verschillend worden behandeld om gelijke (voldoende vergelijkbare) gevallen?
- Indien sprake is van gelijke gevallen die verschillend worden behandeld: is het onderscheid objectief gerechtvaardigd?

Bij de eerste vraag kan worden opgemerkt dat dit wetsvoorstel, zoals aangegeven, voor de screeningsplicht onderscheid maakt tussen onderzoekers, studenten en technisch ondersteuners al naar gelang het vakgebied waarop zij actief willen zijn.

[93] Artikelen 17, eerste lid, onderdelen a en b, 18 en 19 wetsvoorstel.

Ten aanzien van de tweede vraag: het EHRM en het HvJ EU passen in hun rechtspraak over het discriminatieverbod een zogenaamde 'vergelijkbaarheidstoets' toe.[94] In dat verband gaan zij na of de gevallen die zijn voorgelegd voldoende vergelijkbaar zijn. Is er geen sprake van een ongelijke behandeling van vergelijkbare gevallen, dan zullen deze Hoven niet toekomen aan een rechtvaardigingstoets. Uit deze rechtspraak blijkt dat de vergelijkbaarheid moet worden beoordeeld in het licht van de doelstelling van de maatregel en niet in een abstracte context.[95]

De doelstelling van de screeningsplicht is het beperken van risico's voor de nationale veiligheid en van risico's op overtreding van internationale sanctieregelgeving, voor zover deze de bescherming van bepaalde (sensitieve) technologieën betreft. Vanuit deze doelstelling bezien, en gelet op het feit dat deze risico's niet of in aanzienlijk mindere mate aanwezig zijn op vakgebieden waar niet gewerkt wordt met sensitieve technologie, is de groep die onder de screeningsplicht valt naar het oordeel van de regering onvoldoende vergelijkbaar met de groep waarvoor de screeningsplicht niet geldt. De regering acht dit wetsvoorstel dan ook in overeenstemming met het discriminatieverbod.

5.3. Overig internationaal recht

Sanctieregelgeving
Zoals eerder uiteengezet zal het verscherpt toezicht opgaan in de screening kennisveiligheid en als zelfstandig instrument dus ophouden te bestaan. De relevante sanctieverordeningen regelen wat verboden is middels verbodsbepalingen en eventuele vrijstellingsmogelijkheden op de verbodsbepalingen. Met andere woorden, de verbodsbepalingen in Verordening 267/2012 en Besluit (GBVB) 2016/849 regelen niet een screening van personen dan wel de eisen voor toelating van personen die in Nederland willen studeren of onderzoek verrichten. De verbodsbepalingen regelen, samengevat, een verbod op bepaalde overdracht en technische bijstand respectievelijk onderwijs en onderzoek. In de nationale regelgeving is de screening van personen verder vormgegeven en uitgewerkt en zijn de bevoegde autoriteiten aangewezen.

Technologieën die reeds bij sanctieregelgeving als sensitief zijn aangewezen kunnen ook op de lijst met sensitieve technologieën voorkomen, omdat in bredere zin sprake kan zijn van risico's voor de nationale veiligheid. Dit is toegelicht in paragraaf 4.4.4.1. Zowel het verbod op technische bijstand in geval van de betreffende technologieën, als de screening kennisveiligheid in geval van de toegang van een onderzoeker of student tot sensitieve technologie, kunnen dan aan de orde zijn. De toets aan de verboden op technische bijstand en de screening kennisveiligheid worden in één keer gedaan tijdens de screening kennisveiligheid. Voor de verhouding tot de sanctieregelgeving wordt verwezen naar de betreffende paragrafen.

Exportregelgeving, dual-use
Zoals uiteengezet in paragrafen 2, 3 en 4 is onderhavig voorstel een aanvulling op de EU-exportcontroleregelgeving en de gemeenschappelijke EU lijst van militaire goederen en wapens en komt zij hiervoor niet in de plaats. Kennis en technologie kunnen in sommige gevallen geëxporteerd worden, maar kennis en technologie kunnen ook op andere manieren door statelijke actoren verkregen worden. Bijvoorbeeld via onderzoekers en studenten bij kennisinstellingen die in aanraking komen met sensitieve kennis en technologie en deze 'in hun hoofd' meenemen. In deze gevallen volstaat de regelgeving exportcontrole niet om risico's op ongewenste kennis- en technologieoverdracht via Nederlandse kennisinstellingen voldoende te kunnen beperken.

[94] Zie bijvoorbeeld HvJ EU 22 mei 2014, zaak C-356/12, Wolfgang Glatzel tegen Freistaat Bayern; EHRM 22 mei 2008, zaak nr. 15197/02, Petrov tegen Bulgarije.
[95] Zie Europees Grondrechtenagentschap (FRA) en EHRM, *Handboek over het Europese non-discriminatierecht* (2018), p. 50 en 52 en de daar genoemde jurisprudentie.

Technologieën die op de dual-use lijst staan en op de gemeenschappelijke EU-lijst van militaire goederen kunnen ook op de lijst met sensitieve technologieën staan. Dit is toegelicht in paragraaf 4.4.4. Zowel de exportregels in geval van export van die betreffende technologie als de screening kennisveiligheid in geval van de toelating van een onderzoeker of student onderzoeker van buiten de EU kunnen dan aan de orde zijn.

Hoofdstuk 6. Uitvoerings- en handhaafbaarheidstoets

Onze Minister van Onderwijs, Cultuur en Wetenschap geeft uitvoering aan deze wet. De Minister van OCW is in gesprek met screeningsautoriteit Justis, als beoogd uitvoerder. Justis doet met het oog hierop een uitvoeringstoets op dit wetsvoorstel, waarna wordt bepaald of de screening voor Justis uitvoerbaar is en zo ja, of Justis de opdracht voor de uitvoering van de screening kennisveiligheid aanneemt [deze paragraaf wordt verder aangevuld nadat de uitvoerings- en handhaafbaarheidstoetsen zijn gedaan].

Hoofdstuk 7. Toezicht en handhaving

Hoofdstuk 7. Toezicht en handhaving

In dit hoofdstuk wordt ingegaan op het toezicht op naleving van de wet en de mogelijkheden tot handhaving. De Minister van OCW voert verkennende gesprekken met de Inspectie van het Onderwijs over de positionering van het toezicht. De Inspectie van het Onderwijs doet met het oog hierop een uitvoerbaarheids- en handhaafbaarheidstoets op dit wetsvoorstel, waarna wordt bepaald of het toezicht op de naleving van de wet en de mogelijkheden tot handhaving uitvoerbaar en handhaafbaar zijn en zo ja, of de Inspectie van het Onderwijs de opdracht voor het toezicht en handhaving op naleving van de Wet screening kennisveiligheid aanneemt [deze paragraaf wordt verder aangevuld nadat de uitvoerings- en handhaafbaarheidstoetsen zijn gedaan].

7.1 Toezicht

Het toezicht op de naleving van deze wet wordt uitgeoefend door de ambtenaren die de Minister op grond van artikel 15 heeft aangewezen als toezichthouder. De toezichthouder kan ter uitvoering van zijn taak advies vragen aan een externe partij, als de technische aard van de materie hierom vraagt. Dit is ter nadere uitwerking.

Het toezicht op de naleving van deze wet ziet op twee zaken.

Individuele naleving van de screeningsplicht per screeningsplichtige
Het toezicht ziet allereerst op de individuele naleving van de screeningsplicht door de kennisinstelling per screeningsplichtige. Er moet kunnen worden gecontroleerd of screeningsplichtigen die werkzaam zijn of studeren binnen een hoog-risico onderdeel van de kennisinstelling ook daadwerkelijk gescreend zijn en uit de screening geen bezwaar naar voren is gekomen. Het betreft hier toezicht op het naleven van de screeningsplicht door de kennisinstelling. De taak ziet niet toe op het proces van screening en op de inhoudelijke totstandkoming van het besluit. Onderdeel van de controle beslaat wel of een screeningsbesluit is afgegeven voordat door de kennisinstelling toegang tot het hoog-risico onderdeel is verleend door de kennisinstelling aan de screeningsplichtige en of dit screeningsbesluit op de juiste wijze is nageleefd door de kennisinstelling. Hiermee wordt tevens toezicht gehouden op de naleving van de technische bijstandsverboden die bij ministeriële regeling onder de werking van de screening kennisveiligheid zijn gebracht.

Toezicht op de vaststelling van hoog-risico onderdelen
Verder ziet het toezicht op de plicht tot vaststelling van de hoog-risico onderdelen door de kennisinstellingen. Een kennisinstelling stelt middels de lijst van met dit voorstel als sensitief aangewezen (sub)technologieën en het vooraf vastgestelde beoordelingskader

vast bij welke onderdelen van de instelling zich sensitieve technologie bevinden en welke van die onderdelen hoog-risicovol zijn. In dit wetsvoorstel is ook een meldplicht aan de Minister van OCW opgenomen voor kennisinstellingen. Wanneer individuen bij een kennisinstelling evident niet in aanraking kunnen komen met de als sensitief aangewezen (sub)technologieën, heeft deze kennisinstelling geen meldplicht.

De vaststelling en melding van de hoog-risico onderdelen vormen een voortdurende verplichting. Bij het ontstaan of oprichten van nieuwe projecten, programmalijnen, vakgroepen, onderzoeksgroepen, studentenprojecten of opleidingen is de kennisinstelling dus verplicht te onderzoeken of er wel of geen sprake is van een hoog-risico onderdeel en hier melding van te maken aan de minister van OCW. De meldplicht is noodzakelijk omdat zo beter toezicht kan worden gehouden of de kennisinstelling de plicht naleeft om tot een overzicht te komen van de hoog-risico onderdelen en de daaraan gerelateerde screening voor (master)studenten en onderzoekers te koppelen. Toezicht moet voorkomen dat kennisinstellingen te weinig onderdelen aanwijzen, waardoor het risico onvoldoende wordt gemitigeerd. Een belangrijk element van het toezicht betreft of de gemelde resultaten van het onderzoek compleet, uniform en navolgbaar zijn. Voor deze taak is het relevant dat de toezichthouder een externe partij om advies kan vragen als de technische aard van de materie hierom vraagt.

Wijze van toezicht
Het voornemen is om het toezicht zoveel mogelijk risicogericht te organiseren. Dit kan onder meer inhouden dat op basis van signalen, analyses en beschikbare data kennisinstellingen om aanvullende informatie gevraagd wordt of bezocht worden. Op basis van de risicogerichte aanpak bepaalt de toezichthouder of er reden is tot verdere interventie waaronder het instellen van een onderzoek bij de kennisinstelling. De bevindingen en oordelen van een nalevingsonderzoek bij een instelling worden in een rapport vastgelegd. Voordat het definitief rapport wordt opgemaakt en gepubliceerd vindt er hoor- en wederhoor plaats. Afhankelijk van het oordeel in het rapport kan handhavend worden opgetreden. Dit kan een herstelopdracht betreffen, maar er kan ook besloten worden tot het direct inzetten van een bestraffende sanctie. Bovendien kunnen zowel een herstelopdracht als een bestraffende sanctie worden ingezet als de situatie hierom vraagt. De keuze van het instrument hangt af van doel (herstellen dan wel bestraffen). Deze aanpak zorgt voor een zo laag mogelijke impact op kennisinstellingen.

Zo houdt de toezichthouder toezicht op risico's die ertoe doen en is het instrument van toezicht en handhaving doelmatig en proportioneel.

7.2 Handhaving

Een ander deel van de taken van de door de Minister aangewezen toezichthouder betreft handhaving van wettelijke voorschriften en het sanctioneren van daarbij geconstateerde overtredingen. De Minister beschikt over diverse bevoegdheden en instrumenten voor het uitvoeren van deze handhavingstaken. Deze sluiten grotendeels aan bij de bevoegdheden en instrumenten van de Awb.

Indien de toezichthouder risico's ziet op niet-naleving van de wettelijke voorschriften volgend uit deze wet, kan eerst het gesprek worden gevoerd met een kennisinstelling. Zo kan worden vastgesteld welke feiten en omstandigheden een rol hebben gespeeld bij een niet-naleving en hoe in de toekomst niet-naleving kan worden voorkomen. Het voeren van het bestuurlijke gesprek past bij het proportionele toezicht dat de regering met dit wetsvoorstel voorstaat. Als deze gesprekken worden gevoerd vinden zij plaats voordat een onderzoek wordt ingesteld en een rapport wordt opgemaakt. Het voeren van een gesprek is echter geen voorwaarde om over te kunnen gaan tot het instellen van een onderzoek. Als de situatie daarom vraagt kan de toezichthouder ook meteen daartoe overgaan zonder dat eerst een gesprek heeft plaatsgevonden.

Een belangrijke voorwaarde voor het effectief mitigeren van de risico's voor de nationale veiligheid, is dat van toezicht en handhaving ook een afschrikwekkende werking kan uitgaan. De afschrikwekkende werking wordt mede bepaald door de gevolgen die eventuele handhavingsmaatregelen voor een overtreder hebben of kunnen hebben. Daarom is het van belang om, indien sprake is van ernstige of hardnekkige overtredingen, ook de bevoegdheid te hebben om bestuursrechtelijke sancties op te kunnen leggen bij niet-naleving van de wettelijke voorschriften. Een eventuele sanctie moet ook voldoende zwaar zijn om afschrikwekkend te kunnen zijn en naleving te stimuleren.

De Minister van OCW kan hierbij een last onder dwangsom of een bestuurlijke boete opleggen. Een last onder dwangsom kan worden ingezet om een (voortdurende) overtreding van wettelijke voorschriften te beëindigen, of om herhaling van overtreding te voorkomen.[96]

Bij de plichten rondom de vaststelling van de hoog-risico onderdelen ligt een last onder dwangsom het meest in de rede. Er zou immers sprake kunnen zijn van een voortdurende overtreding. Wanneer het duidelijk is dat in een onderdeel onderwijs of onderzoek in een sensitieve technologie wordt verricht, maar de kennisinstelling het betreffende onderdeel niet heeft aangewezen als hoog-risico onderdeel, ook niet na er door de toezichthouder op te zijn gewezen dat dit wel zou moeten gebeuren, zou een last onder dwangsom kunnen worden opgelegd, met daarin een termijn waarbinnen de kennisinstelling het onderdeel alsnog als hoog-risico onderdeel moet vaststellen.

Bij het zorgdragen voor screening voorafgaand aan de toegang tot het hoog-risico onderdeel is een *voortdurende* overtreding minder goed voorstelbaar. De last onder dwangsom is een herstelsanctie, maar in de meeste gevallen zal de toegang al verleend zijn en is het preventieve instrument van de screening niet meer van toepassing. In die gevallen ligt een bestuurlijke boete meer voor de hand. Wanneer is gebleken dat een instelling de plicht om zorg te dragen voor screening voorafgaand aan de toelating in een aantal gevallen niet is nagekomen, zou een last onder dwangsom kunnen worden opgelegd om *herhaling* van de overtreding te voorkomen.

Daarnaast regelt dit wetsvoorstel de mogelijkheid tot opleggen van een bestuurlijke boete. Voor de mogelijkheid om ook een punitieve sanctie op te kunnen leggen is gekozen omdat:

- met een punitieve sanctie een duidelijk signaal kan worden afgegeven bij ernstige of hardnekkige overtredingen; en
- de wettelijke voorschriften in dit wetsvoorstel zijn gesteld ter bescherming van de nationale veiligheid. Gezien de ernst en aard hiervan, is het kunnen opleggen van een sanctie met een bestraffend karakter passend. Er is niet gekozen voor een strafrechtelijke boete, omdat het inzetten van het strafrecht ultimum remedium dient te zijn. Bovendien zou dit handhavingsmiddel zorgen voor criminalisering van kennisinstellingen, hetgeen onwenselijk wordt geacht.

Voor de maximale hoogte van de boete is, vanuit het oogpunt van eenheid van wetgeving, gekozen voor de zesde categorie nu dit aansluit op de Wet vifo. De Wet vifo kent eveneens voor het grootste deel van de in die wet benoemde overtredingen zowel een bevoegdheid voor een bestuurlijke boete als een bevoegdheid voor een last onder dwangsom.[97]

[96] Daarnaast is onder omstandigheden een last onder dwangsom mogelijk om een (dreigende) overtreding te voorkomen (preventieve last onder dwangsom). Deze mogelijkheid is hier niet uitgewerkt.
[97] Artikel 51 Wet vifo.

Hoofdstuk 8. Financiële gevolgen

8.1 Apparaatskosten uitvoering

De uitvoering van de screeningsplicht kost naar schatting €15,3 mln per jaar. Dit is als volgt berekend.

Op het moment van opstellen van dit voorstel worden circa 8000 screenings per jaar verwacht. Dit aantal is een beredeneerde schatting mede gebaseerd op de personeelsaantallen van de Nederlandse kennisinstellingen uitgesplitst naar onderwijs- of wetenschapsgebied en de verwachte jaarlijkse instroom. Verondersteld wordt dat voor ongeveer 40% van de personen die in de sectoren bèta en techniek jaarlijks starten met een aanstelling of dienstverband, een screeningsplicht van toepassing zal zijn. Het feitelijke aantal zal afhangen van welke onderdelen van een kennisinstellingen als hoog-risico zullen worden aangemerkt.

Op basis van de informatie die tijdens de screening wordt verzameld zullen sommige gevallen meer onderzoek vergen dan andere. Zie hiertoe paragraaf 3 waarin het screeningsproces uiteen is gezet. Ten behoeve van deze paragraaf wordt gewerkt met een schatting. Daarbij worden de kosten per screening ingeschat op een bedrag variërend tussen €1200 en €3000, en de gemiddelde kostprijs per screening iets meer dan €1500. Bij ongeveer 10% van de screenings zal naar verwachting nader onderzoek in de tweedelijn vereist zijn. Deze schatting is mede gebaseerd op ervaringen met het verscherpt toezicht. Voor dit soort trajecten zullen de kosten per screening relatief hoog uitvallen. Voor een substantieel deel van de screenings (ca. 70%) zal een minder intensief eerstelijns onderzoek volstaan, en zullen de kosten beduidend lager zijn. Deze schattingen zijn mede gebaseerd op een vooronderzoek dat de beoogde uitvoerder heeft uitgevoerd.

Incidentele kosten in aanloop naar de feitelijke uitvoering van de wet betreffen onder andere de ontwikkeling van een IT-structuur en andere voorzieningen voor de beoogde uitvoerder. Deze kosten worden geraamd op ca. €7,9 mln.

8.2 Regeldruk: kosten instellingen en burgers

Voor de screening brengt de overheid geen bedrag in rekening bij de aanvrager of de kennisinstelling. Wel wordt verwacht dat zij kosten maken om de wet na te kunnen leven en daarvoor administratieve handelingen te verrichten.

Dit is naar schatting voor de kennisinstellingen €8,1 mln. per jaar en eenmalig €32 mln. De kosten voor burgers, te weten de gehele groep screeningsplichtigen, wordt geschat op €250.000 per jaar. Dit is als volgt berekend.

Kennisinstellingen
De kennisinstellingen zullen nagaan welke onderdelen van de instelling aangemerkt moeten worden als hoog-risico. Ongeveer 37 instellingsbesturen zullen hiermee te maken krijgen, omdat zij naar inschatting sensitieve technologie en hoog-risico onderdelen in huis hebben. Geschat wordt dat bij de inwerkingtredig eenmalig landelijk ca. 640 onderdelen worden vastgesteld (bijvoorbeeld vakgroepen en permanente eenheden), en jaarlijks 160 onderdelen (bijvoorbeeld nieuwe projecten en programma's).

De betreffende onderdelen zullen digitaal of fysiek afgescheiden moeten zijn, zodat de kennis en technologie beschermd wordt en er controle is op de toegang. Kennisinstellingen hebben reeds een verantwoordelijkheid om te zorgen voor fysieke en

digitale beschermingsmaatregelen.[98] Toch zal de invoering van de screeningsplicht ertoe leiden dat instellingen hun restrictieve maatregelen intensiveren en uitbreiden. Met een gemiddelde besteding van ongeveer €50.000 per onderdeel zal dit leiden tot een uitgave van €8 mln. per jaar, en eenmalig ca. €32 mln. Dit vormt voor instellingen de belangrijkste kostenpost.

Daarnaast zullen de instellingen kosten maken voor het kennisnemen van de geldende wet- en regelgeving (ca. 37 instellingen, elk 2 uur); het doen van meldingen bij het ministerie van OCW over de vaststelling van hoog-risico onderdelen (ca. 800 onderdelen, elk 0,3 uur); het aanleveren van informatie aan de screeningsautoriteit voor indiening van de aanvraag (idem); en het verstrekken van informatie indien de toezichthouder hierom vraagt (ca. 2 instellingen per jaar, elk 12 uur). De kosten hiervoor worden voor alle instellingen gezamenlijk geschat op €70.000 per jaar, en eenmalig €280.000. Hierbij wordt gerekend met een tarief van €50 per uur.

Ongeveer 37 kennisinstellingen zullen deze kosten moeten dragen. De gemiddelde kosten per instelling komen daarmee op €218.000 per jaar, en eenmalig €870.000. De kosten kunnen echter per instelling sterk uiteenlopen, afhankelijk van hoeveel hoog-risico onderdelen bij de instelling aanwezig zijn.

Naast de kwantitatieve regeldruk kan er ook sprake zijn van ervaren regeldruk. Dit ziet deels toe op de werkbaarheid. Daarbij ziet de regering als specifieke aandachtspunten de doorlooptijd van de screening, de mate waarin de screeningsprocedure aansluiting vindt bij het personeelsbeleid van kennisinstellingen en de toelating van studenten, en de samenwerking tussen overheidspartijen in de aanpak kennisveiligheid (zoals het Loket Kennisveiligheid en de beoogde screeningsautoriteit). De regering heeft deze aandachtspunten betrokken bij de vormgeving van voorliggende wet en blijft zich hiervoor ook inspannen bij de uitvoering.

Daarnaast is een aandachtspunt de perceptie bij wetenschappers en andere functionarissen binnen de kennisinstellingen van het nut van de screeningsplicht en de proportionaliteit van de maatregel. De overheid heeft sinds enkele jaren samen met de kennisinstellingen intensief gewerkt aan het vergroten van bewustwording binnen de instellingen over statelijke dreigingen en het belang van kennisveiligheid. Hierin zijn belangrijke stappen gezet. De regering neemt zich voor om, in elk geval in de periode voorafgaand aan de inwerkingtreding van voorliggende wet, gezamenlijk met de kennissector een communicatielijn te ontwikkelen. Deze heeft als doel om voor screeningsplichtigen en betrokkenen binnen de instelling te verduidelijken waarom de screeningsplicht geldt.

Burgers
Naar schatting 8000 personen per jaar worden gescreend. Zij zullen kennis moeten nemen van de screeningplicht en bijbehorende procedure; en een aanvraagformulier indienen, voorzien van gevraagde stukken. Met iets meer dan twee uur tijdsinvestering en een tarief van €15 per uur leidt dit tot een bedrag van €250.000 per jaar.

Hoofdstuk 9. Gevolgen (met uitzondering van financiële gevolgen)

9.1 Nationaal

De screening draagt bij aan het beschermen van de nationale veiligheid en een weerbare wetenschap. Doordat zoveel mogelijk wordt voorkomen dat statelijke actoren via onderzoekers en studenten de beschikking krijgen over sensitieve kennis en technologie wordt de kennispositie van Nederland beschermd. De wetenschap wordt weerbaarder

[98] De sectorbeelden kennisveiligheid opgesteld in 2023-2024 wijzen uit dat de meeste kennisinstellingen restrictief beleid hanteren bij bepaalde ruimtes en documenten, of hieraan werken.

doordat minder ongewenste kennis- en technologieoverdracht mogelijk is via onderzoekers en studenten. Internationale samenwerking in de wetenschap blijft mogelijk, waarbij kansen voor de wetenschap en risico's voor de nationale veiligheid worden afgewogen.

9.2 Kennisinstellingen

Voor kennisinstellingen duurt het proces van aanstelling van onderzoekers en toelating van studenten op wie de screeningsplicht van toepassing is langer, omdat een extra stap aan dat proces wordt toegevoegd. De Nederlandse instellingen hebben er belang bij dat de administratieve lasten zo laag mogelijk worden gehouden en dat de doorlooptijden voor het behandelen van een aanvraag voor een screening zo kort mogelijk zijn, zodat de Nederlandse kennissector aantrekkelijk blijft voor internationaal talent. Dit is tevens in het belang van Nederland als concurrerende kenniseconomie. De regering onderschrijft deze belangen en heeft daarom de in paragraaf 4.4. en verder omschreven afbakeningssystematiek ontwikkeld waarbij samen met de kennissector heel scherp en precies wordt bepaald waar de risico's het grootst zijn, de risicogerichte aanpak. Ook neemt de regering zich voor om, in samenwerking met de beoogde screeningsautoriteit, de beslistermijn te monitoren en evalueren.

Een neveneffect van de introductie van een preventieve screening is dat het bewustzijn ten aanzien van kennisveiligheidsrisico's bij studenten, wetenschappers, bestuurders en andere medewerkers van kennisinstellingen wordt vergroot. Het draagt ook bij aan het compartimenteren en het veilig doen van onderzoek. Het wetsvoorstel beoogt het gevoel van veiligheid en vertrouwen tussen studenten, onderzoekers en kennisinstellingen, te versterken doordat de overheid wettelijke kaders stelt daar waar de risico's voor de nationale veiligheid het grootst zijn. Dit geschiedt door preventief actie te ondernemen door te screenen, voordat de student of onderzoeker toegang krijgt tot sensitieve kennis- en technologie en het betreffende hoog-risico onderdeel.

Het wetsvoorstel creëert hierdoor duidelijkheid over risico's op een aantal geselecteerde, sensitieve technologieën. Het combineren van de kennis van organisaties binnen de rijksoverheid, waaronder de inlichtingen- en veiligheidsdiensten, en van het kennisveld leidt tot een completer en risicogerichter beeld van waar de risico's aanwezig zijn. Het wetsvoorstel schept duidelijkheid door kennisinstellingen, studenten en onderzoekers, wettelijke kaders te geven. Dit heeft als resultaat dat er duidelijkheid ontstaat op welke thema's uitwisseling kan plaatsvinden zonder een screeningsplicht en op welke thema's de risico's voor de nationale veiligheid niet of in mindere mate aanwezig zijn. Het wetsvoorstel voorkomt bijvoorbeeld uitsluiting op voorhand, gebrek aan uniformiteit en discrepanties in toelatingsbeleid, vanwege het ontbreken van kaders en duidelijkheid over waar de risico's aanwezig zijn. Dit komt de uniformiteit en rechtszekerheid ten goede.

9.3 Gevolgen voor screeningsplichtigen

Met dit wetsvoorstel wordt een screeningsplicht geïntroduceerd voor personen die voornemens zijn onderzoek, onderwijs of ondersteunende technische werkzaamheden te verrichten en daarbij toegang behoeven tot een hoog-risico onderdeel van een kennisinstelling. Ook is de plicht van toepassing op personen die deze toegang behoeven vanwege een studie. Het gaat in de regel om nieuwe medewerkers en studenten die vanwege een aanstelling of inschrijving verbonden zullen zijn met de kennisinstelling.

Deze personen zullen, indien zij akkoord gaan met screening, niet alleen professionele maar ook persoonlijke informatie moeten delen met de screeningsautoriteit, zoals informatie over partners, familie en land van herkomst. Het delen van zulke informatie met een overheidsinstantie kan voor betrokkenen als ingrijpend worden ervaren. Ook zullen zij langer dan gebruikelijk moeten afwachten tot een beslissing is genomen over

de toelating tot de kennisinstelling. De regering stelt er daarom belang in dat kandidaten voor een functie of studie vooraf behoorlijk worden ingelicht over de te verwachten screeningsprocedure, en op de hoogte zijn over hun rechten. De regering is voornemens hierover nadere afspraken te maken met de screeningsautoriteit en de betreffende kennisinstellingen. Daarbij zal ook aandacht zijn voor specifieke doelgroepen die, bijvoorbeeld vanwege de nationaliteit, zich op voorhand ontmoedigd voelen om te solliciteren voor functies waarbij een screeningsplicht geldt.

9.4 Doenvermogen

Het doenvermogen betreft het vermogen van personen om niet alleen te begrijpen wat de wet- en regelgeving van hen vraagt, maar daar ook in de praktijk naar te kunnen handelen. Voor onderhavig wetsvoorstel zijn hierbij twee elementen van belang: het vaststellen van hoog-risico onderdelen door de kennisinstelling, en het aanvragen van de screening door de screeningsplichtige.

Kennisinstellingen krijgen de plicht om de hoog-risico onderdelen vast te stellen aan de hand een beoordelingskader. Bij de ontwikkeling van dit kader betrekt de regering de kennisinstellingen, in het bijzonder veiligheidsadviseurs en andere verantwoordelijke betrokkenen binnen de instelling, zodat het beoordelingskader in de praktijk voldoende begrijpelijk, hanteerbaar en toepasbaar is.

De regering is zich ervan bewust dat het juist toepassen van het beoordelingskader bij het vaststellen van hoog-risico onderdelen een ingewikkelde opgave kan zijn voor de verantwoordelijken binnen een kennisinstelling. Het hoger onderwijs en wetenschappelijk onderzoek is immers een dynamische sector. Dit geldt voor de organisaties van kennisinstellingen maar ook voor het domein van kennisontwikkeling en technologische innovatie. Het is te verwachten dat kennisinstellingen in dit opzicht van elkaar zullen moeten leren hoe zij dit het beste aanpakken. De regering is voornemens nadere afspraken te maken met de toezichthouder en de kennisinstellingen over wat zij kunnen doen om dit gezamenlijke leren te bevorderen. Ook de overheid is lerend, daar waar het beter kan zal worden bijgestuurd. Ook wordt de toezichthouder gevraagd om rekening te houden met de complexiteit van deze opgave voor instellingen bij het doorlopen van de interventieladder.

Bij het aanvragen van de screening is van belang dat voor de screeningsplichtige duidelijk is welke informatie deze moet opgeven en redelijkerwijs in staat is om de gevraagde documenten te leveren, met een beperkte tijdsinvestering. Het formulier en de administratieve procedure moet hierop voldoende ingericht zijn. De regering is voornemens hierover nadere afspraken te maken met de screeningsautoriteit en te voorzien in een periodieke evaluatie.

9.5 Caribisch Nederland

De wet is van toepassing op kennisinstellingen. In Caribisch Nederland is slechts één kennisinstelling gevestigd, te weten Saba University School of Medicine. Dit is een rechtspersoon voor hoger onderwijs als bedoeld in de WHW. Voor zover deze instelling personen toegang kan geven tot sensitieve technologie geldt de plicht tot het aanwijzen van hoog-risico onderdelen. Er zijn op dit moment geen aanwijzingen dat dit het geval is.

Wanneer de screeningsplicht van toepassing is, gelden geen afwijkende eisen voor onderzoekers, studenten en andere personen afkomstig uit Caribisch Nederland. De screeningsplicht maakt geen onderscheid naar herkomst.

9.6 Overige effecten

Indirect draagt de screening bij aan het tegengaan van heimelijke beïnvloeding van of via studenten en onderzoekers. Door middel van een preventieve screening kan aan de voorkant worden ingeschat of een student of onderzoeker kwetsbaar is voor dergelijke beïnvloeding, al dan niet via terugkeerverplichtingen, aan studiebeurzen gekoppelde voorwaarden, banden met statelijke actoren of door een risicovolle affiliatie bestaande uit verbondenheid met risicovolle organisaties, instellingen of personen. Door dergelijke banden of affiliaties kan er een groter risico op heimelijke beïnvloeding van de student of onderzoeker ontstaan. Indien met de screening risico's kunnen worden vastgesteld op ongewenste kennis- of technologieoverdracht en de student of onderzoeker krijgt vervolgens geen toegang tot het hoog-risico onderdeel in kwestie, dan is heimelijke beïnvloeding via die student of onderzoeker op dat onderdeel niet mogelijk. Dit is geen hoofddoel van dit wetsvoorstel, maar een neveneffect van de introductie van een preventieve screening.

10. Evaluatie

Na vijf jaar worden de effectiviteit van de wet en de resultaten geëvalueerd. Bij de evaluatie na vijf jaar wordt in elk geval gekeken naar de effecten van de screening op het individu en op de kennisinstellingen. Ook zal worden bezien of de screening niet onbedoeld tot gevolg heeft dat er indirecte discriminatie onstaat, of dat de screening onbedoeld leidt tot uitsluiting van bepaalde groepen individuen. Tot slot zal hierbij ook gekeken worden of het wenselijk is te komen tot een wettelijke geldigheidsduur van een screeningsbesluit.

Na twee jaar zal een invoeringstoets plaatsvinden. Met dit instrument is het mogelijk om al sneller dan bij de algehele evaluatie na vijf jaar een vinger aan de pols te kunnen houden, voornamelijk in geval van impactvol nieuw beleid. Dit acht de regering ook bij de screening kennisveiligheid wenselijk. Hierbij zal onder meer aandacht zijn voor de administratieve lasten en effectiviteit van de screening kennisveiligheid.
PM [met de uitvoeringsorganisatie, het kennisveld en de toezichthouder wordt afgestemd welke (management)informatie hiervoor nodig is].

11. Advies en consultatie

PM (wordt pas na de consultatie ingevuld)

12. Overgangsrecht

13. Inwerkingtreding

Beoogd wordt dit wetsvoorstel met ingang van [1 juli 2027] in werking te laten treden. Hierbij is voorzien in de mogelijkheid om verschillende onderdelen op verschillende tijdstippen in werking te laten treden.

II. Artikelsgewijze toelichting

Artikel 1. Begripsbepalingen

Kennisinstelling
Onder het begrip kennisinstelling valt een aantal categorieën van rechtspersonen:
1. Rechtspersonen die een in de in de bijlage van de WHW opgenomen instelling of academisch ziekenhuis in stand houden of zijn.
Dit betreffen de zogenoemde bekostigde hoger onderwijsinstellingen en academische ziekenhuizen.
2. De rechtspersonen voor hoger onderwijs (als bedoeld in de WHW).
Dit zijn de zogenoemde niet-bekostigde hoger onderwijsinstellingen. Dit zijn rechtspersonen die geaccrediteerde initiële opleidingen en postinitiële masteropleidingen verzorgen met uitzondering van de Staat.
3. De in bijlage 1 bij deze wet opgenomen rechtspersonen.
Van deze rechtspersonen is geen definitie beschikbaar en zij zijn evenmin in andere wetgeving aangewezen als kennisinstelling. Deze rechtspersonen worden daarom in de eerste bijlage bij deze wet aangewezen. Voor de Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam, de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek en de Nederlandse organisatie voor wetenschappelijk onderzoek geldt dat ook alle hieronder vallende instituten onder het toepassingsbereik van dit voorstel vallen.

Nationale veiligheid
In paragraaf 4.3 van de toelichting wordt dit begrip uiteen gezet.

Onze Minister
Hieronder wordt verstaan de Minister van Onderwijs, Cultuur en Wetenschap, die de eerstverantwoordelijke minister is voor de screening kennisveiligheid.

Sensitieve technologie
Zie hiervoor de artikelsgewijze toelichting bij artikelen 5 en 6.

Screeningsbesluit
Zie hiervoor de artikelsgewijze toelichting bij artikel 14.

Screeningsplichtige
Zie hiervoor de artikelsgewijze toelichting bij artikelen 3 en 4.

Artikel 2. Wijziging bijlage
In het eerste lid is bepaald dat een wijziging van de statutaire naam van een rechtspersoon, opgenomen in bijlage 1 bij deze wet, wordt geacht met onmiddellijke ingang te zijn opgenomen in die bijlage. In het tweede lid is bepaald dat hetzelfde geldt bij een omzetting, fusie of splitsing van een rechtspersoon.
Het derde lid bevat een grondslag om bij algemene maatregel van bestuur bijlage 1 te kunnen wijzigen. Dit kan op voordracht van Onze Minister in overeenstemming met Onze Minister(s) wie het mede aangaat. Een rechtspersoon kan alleen bij algemene maatregel van bestuur worden aangewezen, indien het een rechtspersoon betreft die onderzoek doet naar of onderwijs verzorgt in sensitieve technologie als bedoeld in artikelen 5 en 6.

Artikel 3. Screeningsplichtige
Dit artikel bepaalt de doelgroep van dit wetsvoorstel; welke personen zijn verplicht een screening te ondergaan voordat zij toegang kunnen krijgen tot een onderdeel van een kennisinstelling met sensitieve technologie. Dit artikel bepaalt daarmee mede de reikwijdte van dit voorstel.

Op grond van dit artikel is iemand screeningsplichtig indien:

a. deze persoon voornemens is onderzoek te doen, onderwijs te verzorgen, ondersteunende werkzaamheden van technische aard ten behoeve van onderzoek of onderwijs te verrichten, of te studeren aan een onderdeel van een kennisinstelling als bedoeld in artikel 7; en
b. bij dit onderzoek of onderwijs, deze ondersteunende werkzaamheden van technische aard of deze studie toegang zou krijgen tot sensitieve technologie (als bedoeld in artikelen 5 en 6).
c. de kennisinstelling de betrokkene wil belasten met het onderzoek, het onderwijs of de ondersteunende werkzaamheden, respectievelijk de voorwaarde dat de kennisinstelling heeft vastgesteld dat de student toelaatbaar is tot de opleiding of onderwijseenheid waar de student in aanraking kan komen met sensitieve technologie.
   Indien het bij onderzoekers en technische ondersteuners om nieuwe medewerkers gaat, is het niet de bedoeling dat verschillende deelnemers aan de selectieprocedure voor de betreffende functie voor screening in aanmerking worden gebracht. De screeningsplicht geldt alleen voor de geselecteerde kandidaat. Het screenen van verschillende kandidaten zou niet te verenigen zijn met het streven om de noodzakelijke beperking van het recht op eerbiediging van de persoonlijke levenssfeer zo beperkt mogelijk te laten zijn.
   Het kan hierbij ook gaan om medewerkers die al langer in dienst zijn bij een kennisinstelling en die door de kennisinstelling belast worden met een project waarin sensitieve technologie een rol speelt.

Artikel 4. Uitzonderingen screeningsplicht
Dit artikel geeft een aantal uitzonderingen op het begrip screeningsplichtig (artikel 3).

Dit betreft ten eerste personen die op grond van artikel 3 wel verplicht zijn een screening aan te vragen, maar voor het doen van hetzelfde onderzoek, onderwijs of ondersteunende werkzaamheden ten behoeve van onderzoek of onderwijs als waar de screeningsplicht aan verbonden is ook een verklaring nodig hebben als bedoeld in artikel 1, eerste lid, onderdeel b, van de Wet veiligheidsonderzoeken (de zogenoemde VGB), omdat de functie waarbinnen het onderzoek wordt verricht is aangemerkt als een vertrouwensfunctie als bedoeld in de Wet veiligheidsonderzoeken.
Ten tweede betreft dit personen die al eerder een screening hebben ondergaan, waarbij ze een positief screeningsbesluit hebben gekregen en overstappen naar een onderzoek of studie of een andere positie waarbij ze technisch ondersteunende werkzaamheden verrichten die zien op dezelfde sensitieve technologie. Dit nieuwe onderzoek, deze nieuwe studie of nieuwe functie kan zowel bij dezelfde kennisinstelling als een andere kennisinstelling zijn. Op grond van het tweede lid ziet deze uitzondering niet op personen die overstappen van een studie naar een onderzoeksfunctie, een onderwijsverzorgende functie of naar ondersteunende werkzaamheden van technische aard die zien op dezelfde sensitieve technologie.

Artikel 5. Sensitieve technologie
Dit artikel bepaalt wanneer sprake is van sensitieve technologie. Dit artikel bepaalt daarmee mede de reikwijdte van dit voorstel. Zie verder de artikelsgewijze toelichting bij artikel 6 voor de toelichting waarom zoveel mogelijk technologieën op het niveau van de wet zijn aangewezen.

Het vaststellen van de sensitieve technologie gebeurt in drie stappen:

Stap 1
1. Niet bij alle technologieën is mogelijk sprake van een risico voor de nationale veiligheid. Risico's voor de nationale veiligheid moeten echter wel aan de orde zijn. De specifieke technologieën waarbij hier mogelijk wel sprake van is worden daarom

opgenomen in bijlage 2 of worden aangewezen bij algemene maatregel van bestuur of ministeriële regeling (zie artikel 6). Zie verder paragraaf 4.4 van het algemeen deel van de toelichting voor nadere informatie over de verschillende technologieën.

Bij veel technologieën is slechts een deel van de technologie mogelijk sensitief. Daarom is in bijlage 2 en de bijlage bij de toelichting aangegeven welke subtechnologieën dit betreft. De onderdelen van de technologie die niet in bijlage 2 zijn opgenomen, worden voor de toepassing van deze wet momenteel niet als sensitief aangemerkt. Mocht een subtechnologie van een technologie genoemd in de bijlage 2 in de toekomst wel als sensitief worden aangemerkt, dan zal die aanwijzing plaatsvinden bij amvb of middels een wetswijziging (zie de artikelsgewijze toelichting bij artikel 6). Ook als alle subtechnologieën van een technologie sensitief zijn, zijn deze aangewezen in de tabel. Dit voorkomt onduidelijkheid over de reikwijdte van de technologieën.

Stap 2
2. Er moet nagegaan worden of er beperkingen zijn gesteld aan het aanbieden van kennis over een technologie, opgenomen in de lijst in bijlage 2 (stap 1), door een of meer verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme. Op grond van het derde lid worden deze technologieën (of gedeeltes van deze technologieën), die op grond van de aangewezen sancties worden omvat, sensitief geacht. De instelling heeft verder geen eigen afweging te maken. De beperkingen aan technologie-kennisoverdracht die in deze internationale sanctieregelgeving zijn opgenomen worden bij ministeriële regeling aangewezen, zodat voor de kennisinstellingen duidelijk is welke technologieën zonder meer als sensitief moeten worden beschouwd (in verband met de verplichting om hoog-risico onderdelen van de kennisinstelling aan te wijzen).
Hierbij wordt wel opgemerkt dat soms op grond van de hierboven genoemde internationale sanctieregimes een nader afwegingskader geldt om te bepalen of een bepaalde (sub-)technologie onder de reikwijdte ervan valt. De internationale sanctieregimes kunnen bijvoorbeeld bepalen dat slechts een zeer klein onderdeel van een technologie onder de reikwijdte van de het sanctieregime valt of dat doorgaans alleen niet-fundamenteel onderzoek eronder valt.
Indien een sanctieregime niet is aangewezen bij ministeriële regeling, betekent dit niet dat eventuele verboden op technische bijstand in dat sanctieregime niet van toepassing zijn voor kennisinstellingen.

Stap 3
3. Niet al het onderzoek of al het onderwijs op het gebied van een aangewezen technologie (stap 1) leidt tot mogelijke risico's voor de nationale veiligheid. Daarom zijn een aantal nadere voorwaarden opgenomen in het eerste lid, onderdelen a en b. Deze voorwaarden worden toegepast door de kennisinstelling. De voorwaarden onder a en b zijn cumulatief van aard. Dit betekent dat een technologie aan beide vereisten moet voldoen om als sensitieve technologie te worden aangemerkt. Binnen onderdeel b zijn de twee voorwaarden (1º en 2º) niet cumulatief van aard. Een technologie hoeft daarmee maar te voldoen aan één van de subonderdelen om aan deze voorwaarde te voldoen.
In het eerste lid, onderdeel b, onder 1º, wordt gesproken van vitale processen. Hiermee worden zowel de huidige als toekomstige vitale processen bedoeld.[99]
In het eerste lid, onderdeel b, onder 2º, wordt gesproken van opsporingsdiensten. Het opsporingsdomein is een breed domein en er is alleen mogelijk sprake van sensitieve technologie indien de toepassing van de technologie bij de opsporingsdiensten invloed heeft of kan hebben op de nationale veiligheid. Bij toepassingen bij bijvoorbeeld de aanpak van economische delicten of commune delicten, eveneens onderdeel van het opsporingsdomein, is niet altijd sprake van een mogelijk risico voor de nationale veiligheid.

[99] Zie hierover verder: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

Het voornemen is om een beoordelingskader ter uitwerking van deze wettelijke voorwaarden vast te stellen in een ministeriële regeling. Het vierde lid biedt hiervoor een grondslag.
Voor verdere uitleg over de onderdelen die een rol spelen bij de afbakening van sensitieve technologie zie paragraaf 4.4.6 van het algemeen deel van de toelichting.

Het tweede lid maakt het mogelijk om bij algemene maatregel van bestuur te bepalen dat het eerste lid, onderdeel a (dat regelt dat een technologie niet sensitief is voor zover het onderzoek op het gebied van de technologie een experimenteel of theoretisch karakter heeft), niet van toepassing is bij het vaststellen van de sensitiviteit van een bepaalde technologie. Zie voor de onderbouwing hiervan paragraaf 4.4.5 van het algemeen deel van de toelichting.

Artikel 6. Toevoegen sensitieve technologie
De sensitieve technologieën worden zoveel mogelijk in het voorstel vastgelegd, in bijlage 2 bij artikel 5. Daarmee is beoogd zoveel mogelijk tegemoet te komen aan het primaat van de wetgever; de democratische betrokkenheid bij het vaststellen van de sensitieve technologie alsmede het rechtszekerheidsbeginsel. In dit artikel is wel een grondslag opgenomen om bij algemene maatregel van bestuur andere sensitieve (sub)technologieën aan te wijzen. De technologische ontwikkelingen gaan zeer snel en het is nodig om daarop in te kunnen spelen. Op het niveau van wet zijn technologische veranderingen minder goed bij te houden dan op een lager niveau van regelgeving. Het bijhouden hiervan is belangrijk, zodat relevante nieuwe sensitieve technologie tijdig onder het toepassingsbereik van dit voorstel kan worden gebracht. Door dit bij algemene maatregel van bestuur te doen, wordt hierin flexibiliteit met behoud van rechtszekerheid geboden. Ingeval van aanvullen, kan dat alleen als aan de criteria uit artikel 5, eerste, tweede en derde lid, is voldaan. Deze criteria waarborgen dat niet willekeurig iedere sensitieve technologie kan worden aangewezen. Dit betreffen dezelfde criteria als de criteria die gebruikt worden bij het bepalen van sensitiviteit van technologie. Zie over de criteria daarom verder de artikelsgewijze toelichting op artikel 5.
Het derde lid bevat een grondslag om bij ministeriële regeling technologieën of delen hiervan aan te wijzen. Rekening houdend met de terughoudendheid met delegatie van regelgevende bevoegdheden aan een minister is er voorzien in een clausulering. De aanwijzing bij ministeriële regeling is alleen mogelijk indien:
1. er beperkingen aan deze technologie zijn gesteld in een of meer verdragen of bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme;
2. deze verdragen of besluiten zijn bindend van aard (geen aanbevelingen of internationale afspraken);
3. er een spoedeisend belang is om deze technologie bij ministeriële regeling aan te wijzen;
4. de desbetreffende internationale sanctiemaatregel ten aanzien van de omgang met de technologie beperkt ruimte laat voor beleidsinhoudelijke keuzes.

De implementatie van internationale sanctiemaatregelen op grond van VN-resoluties en EU-verordeningen en Raadsbesluiten vindt sinds enkele decennia plaats bij ministeriële sanctieregeling. Het verplichtende karakter van deze internationale sanctiemaatregelen, de spoedeisendheid - internationale sanctiemaatregelen kennen vaak een korte implementatietermijn – en de beperkte ruimte voor beleidsinhoudelijke keuzes, maken de ministeriële regeling tot een passend regelingsniveau voor implementatie van internationale sanctiemaatregelen. Dezelfde overwegingen als voor de sanctieregelgeving in het algemeen gelden, gelden eveneens voor de daaruit voortvloeiende restricties als het gaat om de omgang met (delen van) technologieën. Vandaar dat is gekozen voor het aanwijzen bij ministeriële regeling van de minister van OCW.

Artikel 7. Verplichting aanwijzing onderdelen instelling
Dit betreft een verplichting van kennisinstellingen om te onderzoeken bij welke onderdelen van de instelling screeningsplichtigen in aanraking kunnen komen met sensitieve technologie als bedoeld in deze wet en vervolgens zelf vast te stellen bij welke onderdelen van de instellingen dit het geval is. Sensitieve technologie is namelijk verspreid binnen instellingen in bijvoorbeeld verschillende projecten, programmalijnen, vakgroepen, onderzoeksgroepen, laboratoria en (delen van) opleidingen. Hierbij is de begripsbepaling van sensitieve technologie, zoals opgenomen in deze wet, bepalend. Dit betekent dat instellingen de opsomming van sensitieve technologieën in bijlage 2, eventuele op grond van artikel 6 aangewezen technologieën en de criteria, beschreven in artikel 5, eerste, tweede en derde lid, gebruiken bij het aanwijzen van de onderdelen van de instelling waar sensitieve technologie als bedoeld in deze wet zich bevindt. Hiertoe wordt het eerder genoemde beoordelingskader ter uitwerking van de wettelijke voorwaarden van artikel 5 opgesteld, dat instellingen hierbij behulpzaam zal zijn. Het onderzoek is niet noodzakelijk indien een screeningsplichtige bij een onderdeel van een kennisinstelling evident niet in aanraking kan komen met de in bijlage 2 of op grond van artikel 6 aangewezen technologieën. Op deze manier wordt getracht de regeldruk voor kennisinstellingen te verlichten. Wel wordt het noodzakelijk geacht om voor alle onderdelen die raakvlakken hebben met de in bijlage 2 of op grond van artikel 6 aangewezen technologieën het beoordelingskader na te lopen.

Het begrip onderdeel is niet nader gedefinieerd, omdat er verschillen zijn in de interne structuur van kennisinstellingen. Onder het begrip wordt in ieder geval verstaan: (onderzoeks)projecten, onderzoekslijnen, programmalijnen, vakgroepen, onderzoeksgroepen, teams, laboratoria, of (delen van) opleidingen. Deze opsomming is niet limitatief vanwege de verschillen tussen instellingen wat betreft de interne structuur en de daarbij gehanteerde benamingen. Om een onderdeel van de kennisinstelling af te bakenen van de rest van de kennisinstelling, wordt in dit wetsvoorstel wel voorgeschreven dat de sensitieve technologie afgescheiden moet zijn van de rest van de kennisinstelling. Als bijvoorbeeld een onderzoeksproject niet afgescheiden kan worden van de onderzoeksgroep waarin dit onderzoek plaatsvindt, dient de hele onderzoeksgroep aangewezen te worden en niet alleen het onderzoeksproject. Hiermee wordt voorkomen dat dit een eenvoudige manier is om deze wet te omzeilen. Zie hierover verder paragraaf 4.4.6. van het algemeen deel van de memorie van toelichting.

Het aanwijzen van onderdelen waar zich sensitieve technologie bevindt, is een doorlopende verplichting; bij wijzigingen of het instellen van nieuwe onderdelen van een instelling, moet de instelling telkens nagaan of dit leidt tot een wijziging van de aanwijzing. Het vijfde lid schrijft ook voor dat het onderzoek, bedoeld in het eerste en derde lid, ook gevolgd moet worden indien een kennisinstelling van oordeel is dat een aangewezen onderdeel niet langer aangewezen dient te zijn. Dit kan bijvoorbeeld gebeuren indien een sensitief onderzoek is afgelopen.

Zowel de uitkomsten van het onderzoek als de aanwijzing van de onderdelen van de instelling die als hoog-risico onderdeel moeten worden beschouwd, worden gemeld aan Onze Minister van Onderwijs, Cultuur en Wetenschap. De uitkomsten worden ook gemeld indien het onderdeel uiteindelijk niet is aangewezen naar aanleiding van het onderzoek. Op deze manier kan Onze Minister erop toezien dat zowel het onderzoek als de uiteindelijke aanwijzing goed is verlopen. Indien een kennisinstelling een onderdeel niet meer wil aanwijzen, worden eveneens de uitkomsten van het onderzoek gemeld aan Onze Minister van Onderwijs, Cultuur en Wetenschap. Zo heeft Onze Minister altijd een compleet beeld van alle aangewezen onderdelen.

In het vierde lid is opgenomen dat onder het begrip onderdelen van de instelling onder andere wordt verstaan: (onderwijseenheden van) bacheloropleidingen, associate degree-opleidingen, masteropleidingen en postinitiële masteropleidingen als bedoeld in de WHW. Deze opleidingen betreffen namelijk niet organisatorische onderdelen van de

instelling, maar moeten wel onder het bereik van dit begrip worden gebracht. Het begrip onderwijseenheden wordt gebruikt om aan te sluiten op artikel 7.3, tweede lid, WHW. In tegenstelling tot andere zaken die als onderdeel kunnen worden aangewezen, zijn opleidingen en onderwijseenheden hiervan wettelijk gedefinieerd. Vandaar dat deze kunnen worden uitgelicht in het vierde lid.

Bij ministeriële regeling worden nadere regels gesteld over de uitwerking van de verplichtingen uit dit artikel. Hierbij wordt gedacht aan regels over de wijze waarop het in de toelichting op artikel 5 genoemde beoordelingskader dient te worden toegepast. Deze regels kunnen bijvoorbeeld de vorm van een vragenlijst of stappenplan hebben. Zo wordt voorkomen dat instellingen dit verschillend van elkaar gaan uitvoeren. Ook is voorgenomen om een vierogenprincipe voor te schrijven voor instellingen bij de aanwijzing van de onderdelen van de instelling.

Artikel 8. Verzoek nadere informatie
Bij twijfel over de reikwijdte van dit wetsvoorstel kan voor informatie contact worden opgenomen met het Ministerie van Onderwijs, Cultuur en Wetenschap. Zo kan het bijvoorbeeld lastig zijn voor instellingen om een deel van het beoordelingskader (zie artikel 7) toe te passen bij een specifiek onderdeel van de instelling. Ook kunnen er vragen zijn over de uitleg van sanctieverordeningen (artikel 5, derde lid).

Artikel 9. Hoofdlijnen screening
Het eerste lid bepaalt op welk moment de screening plaats dient te vinden. Dit is voorafgaand aan de toegang van de screeningsplichtige tot een onderdeel van een kennisinstelling als bedoeld in artikel 7 waarbij de screeningsplichtige toegang zou krijgen tot sensitieve technologie.

In het tweede lid wordt beschreven wat de screening inhoudt. Bij de screening onderzoekt Onze Minister of de toegang van een screeningsplichtige tot een onderdeel van de kennisinstelling waarbij de screeningsplichtige toegang krijgt tot sensitieve technologie:
a. kan leiden tot een risico op overtreding van een of meer bij ministeriële regeling aangewezen beperkingen op het aanbieden van kennis over een sensitieve technologie, gesteld in een of meer bij ministeriële regeling aangewezen verdragen, bindende besluiten van volkenrechtelijke organisaties met betrekking tot de handhaving of het herstel van de internationale vrede en veiligheid, de bevordering van de internationale rechtsorde of de bestrijding van terrorisme, of
b. kan leiden tot een risico voor de nationale veiligheid.

Een potentieel risico is voldoende om te concluderen dat er bezwaar bestaat tegen de toegang van de screeningsplichtige tot zo'n onderdeel van de kennisinstelling. Het potentiële risico moet op feiten zijn gebaseerd. Bij het onderzoek zal altijd gekeken worden naar zowel de eventuele risico's op overtreding van sancties (a-grond) als de risico's voor de nationale veiligheid (b-grond).

Bij ministeriële regeling zullen de internationale sanctieregimes en de daarin gestelde beperkingen aan de kennisoverdracht m.b.t. technologieën worden aangewezen waar bij de screening naar wordt gekeken. Het moet gaan om sanctieregimes en technologieën die raken aan de nationale veiligheid. Als uitgangspunt wordt gehanteerd dat er sprake moet zijn van risico's voor de nationale veiligheid vanwege risico's op overdracht van de betreffende kennis en technologie van Nederlandse kennisinstellingen naar de gesanctioneerde landen in kwestie (zie ook paragraaf 2.3 van het algemeen deel).

Op grond van het derde lid wordt bij het onderzoek het afwegingskader van artikel 11 gebruikt.

Het vierde lid bevat een verplichting aan de instelling. De kennisinstelling is verplicht om de screeningsplichtige alleen toegang te geven tot het betrokken onderdeel van de kennisinstelling, als uit het screeningsbesluit blijkt dat hier vanuit een oogpunt van naleving van sancties en nationale veiligheid geen bezwaar tegen bestaat.

Artikel 10. Aanvraag screeningsbesluit
Het eerste lid bepaalt dat de screeningsplichtige de aanvraag dient te doen voor het screeningsbesluit.
Het tweede lid bevat een verplichting voor de kennisinstelling. De kennisinstelling moet op grond van het tweede lid de screeningsplichtige wijzen op de screeningsplicht.
Het derde lid bevat tot slot de grondslag om bij ministeriële regeling te bepalen welke gegevens de kennisinstelling en screeningsplichtige moeten aanleveren bij de aanvraag voor een screeningsbesluit.

Artikelen 11 (afwegingskader screeningsbesluit*) en 12 (strafbare feiten)*
Artikel 11, eerste lid, schrijft limitatief het afwegingskader voor dat Onze Minister gebruikt bij het nemen van het screeningsbesluit. Dit afwegingskader betreft de factoren die Onze Minister betrekt bij het screeningsbesluit. De factoren zijn cumulatief opgesomd.
Zie voor de verdere toelichting van de verschillende factoren van het afwegingskader paragraaf 3 van het algemeen deel van de toelichting.
Het eerste lid, onderdeel c spreekt over statelijke actoren. Uit de dreigingsbeelden blijkt dat nationale veiligheidsbelangen kwetsbaar zijn en worden bedreigd en aangetast door andere staten. Ook andere organisaties die worden aangestuurd door die staten (statelijke actoren) houden zich hiermee bezig in Nederland.
Het eerste lid, onderdeel d spreekt over strafbare feiten die een rol kunnen spelen bij het nemen van het screeningsbesluit. In artikel 12 is bepaald dat de strafbare feiten die van invloed kunnen zijn op het screeningsbesluit bij ministeriële regeling worden vastgesteld.

Het tweede lid bevat een grondslag om bij ministeriële regeling terugkijktermijnen te kunnen bepalen voor de beoordeling van gegevens van de screeningsplichtige. Deze terugkijktermijnen kunnen verschillend worden vastgesteld voor verschillende soorten gegevens.

Artikel 13. Termijn screening
Dit artikel schrijft voor dat Onze Minister in beginsel uiterlijk binnen vier weken na ontvangst van de aanvraag het screeningsbesluit neemt. Dit moet wel een complete aanvraag betreffen. Bij een onvolledige aanvraag krijgt de screeningsplichtige de gelegenheid om binnen een door Onze Minister gestelde termijn de aanvraag aan te vullen, zie hierover verder artikel 4:5 Awb.

De termijn van het eerste lid, kan met vier weken worden verlengd (tweede lid).

Het derde lid is een uitzondering op de eerste twee leden. Hierin is opgenomen dat de termijn voor het nemen van het screeningsbesluit kan worden opgeschort indien Onze Minister om aanvullende informatie verzoekt. Deze aanvullende informatie kan nodig zijn voor een goede beoordeling. De termijn wordt dan weer hervat zodra deze nadere informatie is verstrekt. Deze nadere informatie zal in de meeste gevallen in schriftelijke vorm worden gevraagd door Onze Minister en geleverd door de screeningsplichtige. In enkele gevallen zal het noodzakelijk zijn om de nadere informatie mondeling te vragen en verkrijgen in de vorm van een interview.

Artikel 14. Resultaat screening
Nadat de screening is afgerond neemt Onze Minister een screeningsbesluit. Dit is een beschikking als bedoeld in artikel 1:3, tweede lid, Awb. Onze Minister doet dit in

overeenstemming met Onze Minister of Onze Ministers die het mede aangaat als dit noodzakelijk is.
Het screeningsbesluit bevat een verklaring dat uit het oogpunt van nationale veiligheid en uit het oogpunt van internationale sanctieregelgeving geen bezwaar, dan wel bezwaar, bestaat tegen de toelating van de screeningsplichtige tot de kennisinstelling. Indien volgens een internationale sanctieregeling ontheffing of toestemming van een bevoegde autoriteit nodig is voor het krijgen van toegang tot sensitieve technologie, bevat het screeningsbesluit ook die ontheffing of toestemming of de weigering daarvan.

Artikel 15. Aanwijzing toezichthouder
Zie voor de toelichting op dit artikel paragraaf 7 van het algemeen deel.

Artikel 16. Bevoegdheden toezichthouder
Zie voor de toelichting op dit artikel paragraaf 7 van het algemeen deel.

Artikel 17. Gegevensverwerking
Het eerste lid bepaalt dat voor zover dit noodzakelijk is voor de uitvoering van de wet gegevens waaronder persoonsgegevens kunnen worden verwerkt. Artikel 6, eerste lid, onderdelen c en e, AVG geven aan dat een verwerking van persoonsgegevens noodzakelijk kan zijn om te voldoen aan een wettelijke verplichting die op grond van de AVG rust en voor de vervulling van een taak in het kader van de uitoefening van openbaar gezag van de verwerkingsverantwoordelijke.
Het eerste lid, onderdeel b, van artikel 17, in combinatie met het bepaalde bij of krachtens de Wet justitiële en strafvorderlijke gegevens en de Wet op de inlichtingen- en veiligheidsdiensten 2017 geeft de grondslag om strafrechtelijke gegevens uit ECRIS en ECRIS TCN alsmede andere in Nederland aanwezige strafrechtelijke informatie over de screeningsplichtige te kunnen verwerken en om in voorkomende gevallen informatie te verwerken die is verkregen uit naslag bij de inlichtingen- en veiligheidsdiensten (zie nader paragraaf 5.1.2).

Het derde lid bepaalt de termijn waarbinnen gegevens moeten worden vernietigd. Het uitgangspunt is dat alle gegevens binnen twee jaar worden vernietigd. De enige uitzondering hierop zijn negatieve screeningsbesluiten. Deze worden voor 15 jaar bewaard nadat het besluit onherroepelijk is geworden. Bij een negatief screeningsbesluit wordt de screeningsplichtige niet toegelaten tot een kennisinstelling in verband met risico’s voor de nationale veiligheid. De noodzaak tot bewaring van de persoonsgegevens is dan anders, aangezien dit direct raakt aan het belang van de bescherming van de nationale veiligheid. Voor gegevens die wijzen op risico’s voor de nationale veiligheid geldt dat deze voor 15 jaar moeten kunnen worden bewaard om toekomstige risico’s te kunnen beperken en te voorkomen. Deze bewaartermijn wordt proportioneel geacht gezien de noodzaak om nationale veiligheidsrisico’s te beheren en is proportioneel gezien de ernst van deze risico’s.

Zie voor verdere toelichting paragraaf 5.1.2 van het algemeen deel.

Artikel 18. Gegevensverstrekkingen aan Onze Minister
Het eerste lid biedt grondslagen voor de levering van gegevens aan Onze Minister voor de uitvoering van de screening kennisveiligheid. Aan Onze Minister kunnen voor dit doel ook strafrechtelijke gegevens worden geleverd door Onze Minister van Justitie en Veiligheid, op grond van het bepaalde bij of krachtens de Wet op de justitiële en strafvorderlijke gegevens. Onze Minister kan daarnaast een verzoek doen tot naslag bij Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties of Onze Minister van Defensie. Dit zal worden opgenomen in de Regeling naslag Wiv 2017.
Op grond van het tweede lid, kan Onze Minister voor zover de bovengenoemde informatie niet de benodigde gegevens oplevert, aanvullende informatie vragen. Als Onze Minister op grond van dit lid om aanvullende informatie vraagt, dan wordt op grond van artikel 13, derde lid, de beslistermijn in afwachting van die aanvullende

informatie opgeschort. Dit is een bevoegdheid waarvan alleen gebruik gemaakt wordt als de verantwoordelijke Minister de benodigde gegevens niet op een andere wijze heeft kunnen achterhalen, zodat de administratieve lasten zo laag mogelijk gehouden worden.

Artikel 19. Gegevensverstrekkingen door Onze Minister
Dit artikel beschrijft aan welke personen en organisaties Onze Minister gegevens kan verstrekken in het kader van de screening kennisveiligheid.

Op grond van het eerste lid verstrekt Onze Minister het screeningsbesluit aan de screeningsplichtige. De kennisinstelling ontvangt slechts welke verklaring (bedoeld in artikel 14, tweede lid) de screeningsplichtige heeft ontvangen.
Op grond van het derde lid kan Onze Minister van Buitenlandse Zaken in sommige gevallen het screeningsbesluit krijgen. Dit gebeurt alleen als het screeningsbesluit mogelijk nuttige informatie bevat voor de procedure tot het verkrijgen van een visum. Op grond van artikel 107, zevende lid, Vreemdelingenwet 2000 kan Onze Minister van Asiel en Migratie ook beschikking krijgen over het screeningsbesluit indien Onze Minister van Asiel en Migratie dit screeningsbesluit behoeft voor de uitvoering van de Vreemdelingenwet 2000 of de Rijkswet op het Nederlanderschap.

Het vierde lid geeft Onze Minister de ruimte om ook informatie met andere betrokken ministers te delen. Dit is bijvoorbeeld Onze Minister van Binnenlandse Zaken en Koninkrijkrelaties als er een verzoek tot naslag is gedaan of een screeningsbesluit voor hen noodzakelijke informatie bevat.

Artikel 20. Verwerking van bijzondere categorieën van persoonsgegevens
Dit artikel biedt de grondslag voor Onze Minister om bijzondere persoonsgegevens te kunnen verwerken. De bijzondere persoonsgegevens kunnen bijvoorbeeld bij het openbare bronnenonderzoek worden verwerkt. Dit kunnen alle types van bijzondere persoonsgegevens betreffen. Dit is niet beoogd met het open bronnenonderzoek. De bijzondere persoonsgegevens worden alleen gebruikt om te beoordelen of er sprake is van risico's voor de nationale veiligheid of risico's op overtreding van internationale sanctieregelgeving die voortvloeien uit ongewenste kennis- en technologieoverdracht. Op grond van artikel 9, tweede lid, onderdeel g, AVG kunnen bijzondere persoonsgegevens alleen verwerkt worden 'om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene'.

Artikel 21. Verwerking strafrechtelijke gegevens en burgerservicenummer
Dit artikel biedt de (door artikel 10 AVG vereiste) grondslag aan Onze Minister om justitiële gegevens te verwerken. Bij de justitiële gegevens die relevant zijn voor de beoordeling of er sprake kan zijn van een risico voor de nationale veiligheid of een risico op overtreding van internationale sanctieregelgeving kan het bijvoorbeeld gaan om veroordelingen voor misdrijven tegen de veiligheid van de staat, schending van ambtsgeheimen, valsheid in geschrift, fraude en diefstal. Het verstrekken van deze gegevens geschiedt met inachtneming van de Wet justitiële en strafvorderlijke gegevens. Het verzoek van de minister van OCW aan de minister van JenV om verstrekking van justitiële gegevens ten behoeve van de screening kennisveiligheid, en de verstrekking van justitiële gegevens door de minister van JenV voor dat doel, zijn niet in dit wetsvoorstel geregeld, maar zullen - vanwege de systematiek van de Wet justitiële en strafvorderlijke gegevens en het Besluit justitiële en strafvorderlijke gegevens - in het Besluit justitiële en strafvorderlijke gegevens worden geregeld. Artikelen 9, eerste lid, en 13, eerste lid, van de Wet justitiële en strafvorderlijke gegevens bieden hiervoor de grondslag.

Daarnaast biedt dit artikel de (door artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming vereiste) grondslag voor het gebruik van het burgerservicenummer (BSN) van de screeningsplichtige bij de uitvoering van deze wet. Het gebruik van het BSN minimaliseert de kans op onjuistheden bij het onderzoek naar de screeningsplichtige in het kader van de screening. Het verwerken van het BSN vormt een belangrijke waarborg tegen persoonsverwisselingen.

Artikel 22. Wijziging Algemene wet bestuursrecht (Awb)
Dit artikel regelt dat beroep in eerste en enige aanleg bij de Afdeling bestuursrechtspraak van de Raad van State (ABRvS) open staat indien de screeningsplichtige beroep instelt tegen het screeningsbesluit. Dit komt de snelheid waarmee screeningsplichtigen een finale rechtelijke uitspraak tegemoet kunnen zien, ten goede. Voordat de screeningsplichtigen kunnen beginnen aan (een onderdeel van) een studie of onderzoek in Nederland hebben ze een positief screeningsbesluit nodig. Aangezien onderdelen van studies, zoals de onderzoeksfase van een masterscriptie of bepaalde vakken veelal maar eenmaal per jaar starten, hebben screeningsplichtige studenten een groot belang bij een korte doorlooptijd van de rechterlijke procedure. Het is voor studenten in zulke situaties belangrijk zo snel mogelijk te weten op welke manier zij hun onderwijsloopbaan kunnen vervolgen. Ook voor geschillen rondom de toelating tot een opleiding in het ho en mbo spreekt de ABRvS recht in eerste en enige instantie (zie artikel 2 van bijlage 2 Awb). Ook voor onderzoekers en technisch ondersteunend personeel geldt dat zij een groot belang hebben bij een korte doorlooptijd van de rechterlijke procedure. Wanneer het gaat om nieuwe medewerkers, zal een positief screeningsbesluit nodig zijn om een sollicitatieprocedure af te kunnen ronden en om te kunnen starten in een functie. Wanneer het gaat om bestaande medewerkers die actief willen worden op een hoog-risico onderdeel, is een positief screeningsbesluit ook nodig om daarmee te kunnen starten. Daarnaast zal het, gezien het internationale karakter van de wetenschap, ook regelmatig voorkomen dat onderzoekers en technisch ondersteunend personeel een screeningsbesluit afwachten terwijl zij nog in het buitenland verblijven. Tot slot is het vanuit het oogpunt van uniforme rechtsbescherming en eenheid van wetgeving wenselijk dat voor iedere screeningsplichtige dezelfde regels gelden voor bezwaar en beroep tegen het screeningsbesluit.

Artikel 23. Wijziging Wet justitiële en strafvorderlijke gegevens (WJSG)
Zoals besproken in paragrafen 3.2.1 en 5.1.2 van het algemeen deel van de memorie van toelichting, worden de gegevens uit Ecris-TCN gebruikt bij de screening kennisveiligheid. Om Onze Minister van Onderwijs, Cultuur en Wetenschap toegang te verlenen tot Ecris-TCN wordt in artikel 2a van de Wet justitiële en strafvorderlijke gegevens bepaald dat Ecris-TCN kan worden gebruikt ten behoeve van de screening kennisveiligheid.

Artikel 24. Wijziging Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW)
Met deze wijzigingen wordt de doorwerking van het screeningsbesluit in de WHW geregeld. Als een vaste onderwijseenheid van een opleiding wordt aangewezen als hoog-sensitief, dan moet de hele opleiding worden aangewezen als onderdeel van een kennisinstelling. De opleiding moet namelijk op grond van de WHW studeerbaar zijn.

Artikel 25. Wijziging Wet subsidiëring landelijke onderwijsondersteunende activiteiten 2013 (Wet SLOA)
In artikel 3a Wet SLOA zijn de taken van Stichting Nuffic aan haar opgedragen. Met dit voorstel wordt het tweede lid, onder a, uitbreid om te regelen dat ook in het kader van de screening, bedoeld in de Wet screening kennisveiligheid, door Onze Minister van Onderwijs, Cultuur en Wetenschap aan Stichting Nuffic gevraagd kan worden om advies over de waarde en authenticiteit van een in een ander land dan Nederland behaald diploma of opleidingsdocument.

Artikel 28. Evaluatiebepaling
Zie hiervoor paragraaf 10 van het algemeen deel van de toelichting.

De Minister van Onderwijs, Cultuur en Wetenschap,

Eppo Bruins

De Minister van Justitie en Veiligheid

David van Weel

III. Toelichting op de sensitieve technologieën, bedoeld in bijlage 2

In deze bijlage wordt een toelichting gegeven op de sensitieve (sub)technologieën als bedoeld in bijlage 2 van dit wetsvoorstel.

In paragraaf 4.4 van dit voorstel wordt uiteengezet op welke wijze de afbakening van sensitieve technologie is aangepakt, wat de criteria zijn die bepalend zijn voor de sensitiviteitsbeoordeling, wat de rol van het kennisveld in de risicogerichte aanpak is en op welke wijze is voorzien in herijking van de lijst met sensitieve (sub)technologieën.

Kort samengevat wordt de reikwijdte van de screeningsplicht zo risicogericht en precies als mogelijk bepaald, samen met de kennissector. Daarom worden hoog-risico onderdelen binnen sensitieve technologiegebieden aangewezen waar de screeningplicht gaat gelden.[100] Bij dit proces krijgen de kennisinstellingen een centrale rol en verantwoordelijkheid. Zij hebben immers zelf het beste zicht op waar de sensitieve (sub)technologie zich bevindt.[101] Op die hoog-risico onderdelen is de screeningsplicht van toepassing. Aan de hand van een lijst sensitieve (sub)technologieën en een door het Rijk ontwikkeld beoordelingskader gaan de kennisinstellingen zelf aanwijzen waar die hoog-risico onderdelen zich binnen de instelling bevinden. Bij de uitwerking van dit beoordelingskader wordt de kennissector betrokken.

De sensitieve (sub)technologieën als bedoeld in bijlage 2

Allereerst wordt verwezen naar het overzicht van de sensitieve (sub)technologieën in de tweede bijlage bij dit voorstel.

Onderstaande (sub)technologiegebieden vallen grotendeels onder verschillende categorieën van de EU Dual-Use Verordening en de gemeenschappelijke EU-lijst van militaire goederen.[102] In die gevallen is het vereist dat er een vergunning wordt aangevraagd voor de export van dergelijke goederen en technologie Tevens zijn er nationale aanvullende exportcontrolemaatregelen van kracht, bijvoorbeeld op het gebied van halfgeleiders, halfgeleiderproductieapparatuur, additive manufacturing en quantum technologie.[103]

Advanced Computing and Systems

Advanced computing technologie is een enabling technologie[104], en daarmee over het algemeen genomen breed verspreid en toegankelijk. De term verwijst naar het gebruik van supercomputers, of computerclusters die functioneren als een supercomputer, voor het uitvoeren van zeer grootschalige projecten. Met de digitalisering van de samenleving worden advanced computing technologieën en systemen overal in de samenleving gebruikt. Dit type computers en systemen zijn cruciaal voor de digitale transformatie en het bijdragen aan de oplossingen waar grootschalige rekenkracht vereist is. Zo wordt er onder andere gebruik gemaakt van deze technologie in transport en mobiliteit, werktuigbouwkunde, robotica, smart grids, civiele techniek, slimme gebouwen,

---

[100] Onderdelen kunnen (delen van) opleidingen en postinitiële masteropleidingen, projecten, programmalijnen, vakgroepen, onderzoeksgroepen, studentenprojecten of bepaalde (studenten)teams en laboratoria zijn.
[101] In paragraaf 4.4 tot en met 4.4.7 van dit voorstel wordt deze systematiek toegelicht.
[102] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri+celex%3A32021R0821
[103] wetten.nl - Regeling - Regeling geavanceerde productieapparatuur voor halfgeleiders - BWBR0048439, wetten.nl - Informatie - Regeling aanvullende controlemaatregelen op de Verordening producten voor tweeërlei gebruik - BWBR0050313
[104] Enabling technologieën zijn technologieën die andere innovaties of ontwikkelingen mogelijk maken of ondersteunen. Ze vormen de basis voor nieuwe producten, diensten of systemen die anders misschien niet zouden bestaan of veel trager ontwikkeld zouden worden. Het zijn technologieën die als fundament dienen voor het creëren van meer geavanceerde toepassingen in verschillende sectoren.

landbouw en de gezondheidszorg. Hoewel deze technologie vaak commercieel beschikbaar is, is de sensitiviteit gelegen in de verdere ontwikkeling van de technologie en de beveiliging van sensitieve data.

Sensitieve (sub)technologieën

Door de cruciale rol in vitale processen en de toepassingen in wapensystemen worden onderdelen van deze technologie als sensitief aangemerkt. Het betreft de onderdelen High Performance Computing (HPC) en Edge Computing.

High performance computing (HPC) staat voor het op hoge snelheid verwerken van grote hoeveelheden data om complexe berekeningen uit te voeren. Dit wordt gedaan via parallel computing, daarbij verwerken meerdere processors tegelijk data binnen één computer. Of via cluster computing, waarbij computers gelinkt worden, zodat verwerking plaats kan vinden op meerdere servers tegelijk, vaak via lokale netwerken. Of via grid computing, waarbij meerdere (vaak verschillende typen) computers zijn verbonden en (onderdelen van) een complexe taak uitvoeren.

Edge computing is een 'computing paradigm' dat staat voor het verplaatsen van een deel van de rekenbelasting van centrale data-servers richting de periferie ('Edge') van het netwerk, zodat er ook aanspraak wordt gemaakt op rekencapaciteit in deze laag van het netwerk (bijvoorbeeld van basisstations, routers en switches). Edge computing vermindert ook de behoefte aan communicatie/dataverkeer, waardoor sprake kan zijn van toenemende autonomie. Door de data lokaal of dichter bij de bron te verwerken, geeft edge computing de mogelijkheid tot snellere verwerkingstijden en verhoogt het de efficiëntie van data transmissie. Veel edge computing toepassingen zijn te beschouwen als gedistribueerde cloud computing.

Artificiële Intelligentie (AI)

Een AI-systeem is "een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen."[105] De sensitiviteit is gelegen in de kennis en/of data waarmee een model getraind is of de specifieke taken die het systeem meer of minder zelfstandig uitvoert (toepassing). Daarnaast maakt de brede toepasbaarheid van AI voor algemene doeleinden dat het, naast veel onschuldige, ook zeer hoog-risicovolle toepassingen kent. Als systeemtechnologie zal AI een rol gaan spelen in bijna alle facetten van onze samenleving.

AI valt onder de EU AI Act, waarmee controle wordt doorgevoerd op het type AI-technologieën die gebruikt kunnen worden. Hiertoe worden er eisen en kaders geïntroduceerd voor de ontwikkeling en het gebruik van AI-systemen opdat er veilig gebruik van gemaakt kan worden[106].

Sensitieve (sub)technologieën

Onderdelen van Artificiële Intelligentie worden als sensitief aangemerkt. Het betreft de groep technologieën die onder Machine Learning (ML) vallen, waar onder andere Generative AI, General Purpose AI, Deep learning, Reinforcement learning en Natural Language Processing onder vallen. Ook Expert Systems wordt als sensitief aangemerkt.

105 EU AI Act.

106 AI-verordening aangenomen door het Europees Parlement - Digitale Overheid

Machine Learning (ML), ofwel machinaal leren, is een tak van kunstmatige intelligentie die computers en systemen in staat stelt om te leren van data en ervaringen, zonder expliciet geprogrammeerd te worden voor elke taak. Het draait om het ontwikkelen van algoritmes en modellen die automatisch patronen en structuren in data kunnen ontdekken en daaruit kunnen leren om voorspellingen te doen of beslissingen te nemen. Het omvat verschillende methoden, inclusief gecontroleerd (supervised), ongecontroleerd (unsupervised) en versterkend (reinforcement) leren. Voorbeelden van toepassingsgebieden van ML zijn object detectie en classificatie, medische beeldanalyse, taalverwerking, en aanbevelingssystemen.

Deep Learning (DL) is een subset van ML waarbij gebruik gemaakt wordt van deep neural networks met meerdere verborgen lagen om complexe patronen in de data te kunnen modelleren. Het verschil tussen DL en traditionele ML technieken is dat de laatste gebruik maakt van simpelere algoritmen, waaronder 'shallow' neurale netwerken met een beperkt aantal lagen. ML en DL hebben overlappende toepassingsgebieden, waarbij DL voornamelijk wordt ingezet voor taken waarbij grote hoeveelheden data en complexe patronen aanwezig zijn. DL modellen in combinatie met Computer Vision (zie hieronder) kent meerdere sensitieve toepassingsgebieden, zoals het trainen van modellen voor automatische doelherkenning, objectdetectie, afbeelding- en video-analyse. Ook buiten CV zijn er sensitieve toepassingsgebieden van DL, voorbeelden zijn voorspellende algoritmen om bijvoorbeeld zwakheden in cyber infrastructuren te ontdekken, alsook het optimaliseren van logistieke planning en transport of toepassingen in de biotechnologie of chemie, zoals het ontwerpen van biologische of chemische wapens.

General Purpose AI (GPAI), ofwel AI voor algemene doeleinden, gaat over AI-systemen die zijn gebaseerd op een *AI-model voor algemene doeleinden* en dat verschillende doeleinden kan dienen, zowel voor direct gebruik als voor integratie in andere AI-systemen. Een AI-model voor algemene doeleinden is een AI-model dat een aanzienlijk algemeen karakter vertoont en in staat is op competente wijze een breed scala aan verschillende taken uit te voeren, ongeacht de wijze waarop het model in de handel wordt gebracht, en dat kan worden geïntegreerd in een verscheidenheid aan systemen verder in de AI-waardeketen of toepassingen verder in de AI-waardeketen. Vanwege de brede toepasbaarheid van AI voor algemene doeleinden, vindt dit ook sensitieve toepassing, bijvoorbeeld voor het creëren van wapens.

Generative AI (GAI), ofwel generatieve AI, wordt gebruikt voor het genereren van nieuwe data of content. Deze AI modellen kunnen patronen uit grote hoeveelheden bestaande data leren en deze kennis gebruiken om unieke en creatieve output te genereren. Voorbeelden van toepassingsgebieden zijn kunst en design (creëren van originele schilderijen / foto's / fashion), media en entertainment (games / visual effects), tekst generatie (ChatGPT, Gemini, etc.), gezondheidszorg (nieuwe moleculen ontwerpen voor medicijnontwikkeling), alsook desinformatie en deep fakes (afbeeldingen / video / stemmen). Vooral de laatste twee maakt de toepassing van GAI in bepaalde gevallen sensitief voor de nationale veiligheid.

Natural Language Processing (NLP), ofwel natuurlijke taalverwerking, is een onderzoeksgebied dat zich bezighoudt met het leren van machines om tekst te begrijpen, interpreteren, en genereren. Subtechnologiegebieden binnen NLP zijn bijvoorbeeld sentiment analyse, machine vertaling en chatbots. NLP kent enkele veiligheidstoepassingen, zoals het interpreteren van grote volumes tekstuele data om hier patronen uit te halen voor inlichtingendiensten.

Reinforcement Learning (RL), ofwel versterkend leren, is een subset van ML die focust op het trainen van agenten (agents) die sequentiële beslissingen kunnen maken in een omgeving met als doel beloningen te maximaliseren door acties te ondernemen die tot gunstige resultaten leiden. RL wordt voornamelijk toegepast in robotica en autonome

systemen, bijvoorbeeld bij het trainen van zelfrijdende auto's en drones om zelfstandig beslissingen te kunnen nemen gebaseerd op real-time sensor data. Deze autonome systemen kunnen militair worden ingezet wat maakt dat dit subveld sensitieve toepassingen kent.

Expert Systems (ES), ofwel expertsystemen, ook bekend als knowledge-based systems, zijn AI programma's ontworpen om de beslissingen van menselijke experts na te bootsen. Deze modellen vergen domein-specifieke kennis die de modellen gebruiken voor op kennis gebaseerd redeneren om complexe problemen op te lossen en aanbevelingen te doen. ES zijn over het algemeen statisch en beschikken niet over leervermogen. Ze vertrouwen op de kennis die in de regels is vastgelegd. Voorbeelden van toepassingsgebieden zijn de gezondheidszorg waarbij ES medici kunnen ondersteunen in medische diagnoses en de financiële sector waarbij ES beleggingsadvies kunnen uitbrengen voor bijvoorbeeld het beoordelen van kredietwaardigheid. ES kunnen ook gebruikt worden in militaire context, bijvoorbeeld door militaire commandanten te ondersteunen in het maken van tactische beslissingen.

Advanced Data Analytics

Daarnaast valt Advanced Data Analytics door de sterke overlap met AI onder dit technologiegebied. Door de snelle digitalisering van de samenleving zijn er steeds meer en verschillende typen data beschikbaar. Dit heeft een hele data-economie tot stand gebracht. Big data is een term die gebruikt wordt om te verwijzen naar een dataset met een grote hoeveelheid en een hoge variëteit aan informatie, die ook nog een hoge omloopsnelheid heeft. Advanced data analytics betreft het analyseren van data voor het verkrijgen van (waardevolle) informatie. Het verzamelen, voorbewerken en opschonen en de daaropvolgende analyse en visualisatie zijn in toenemende mate sterk gelieerd aan artificiële intelligentie methoden en technieken. De sensitiviteit van Advanced Data Analytics is voornamelijk gelegen in de grote datasets en de waardevolle uitkomsten van analyses, die vervolgens voor legio toepassingen in vitale sectoren en processen gebruikt kunnen worden.

Sensitieve (sub)technologieën

Voor Advanced Data Analytics betreft het de onderdelen Predictive Analytics en Prescriptive Analytics.

Predictive analytics is een type data-analyse dat uitkomsten voorspelt door historische data en statistische modellen te gebruiken. Het identificeert patronen en trends om toekomstige gebeurtenissen of gedragingen te voorspellen.

Prescriptive analytics is een vorm van data-analyse die aanbevelingen doet voor de beste acties om bepaalde doelen te bereiken. Het maakt gebruik van geavanceerde algoritmen, optimalisatietechnieken en simulaties om scenario's te analyseren en de meest effectieve beslissingen of acties te adviseren. Het richt zich niet alleen op wat er zou kunnen gebeuren, maar ook op hoe men het beste kan reageren om het gewenste resultaat te behalen.

Biotechnologie

Biotechnologie is de toepassing van wetenschap en technologie op levende organismen of delen daarvan, op producten en op modellen van levende organismen, met als doel om levende of niet-levende materialen te karakteriseren of te veranderen voor de productie van kennis, goederen en diensten. Dit technologiegebied kent zowel civiele als militaire toepassingen en is daarmee dual-use. Door de sterke opmars van andere technologieën, veelal enabling technologieën, die biotechnologische ontwikkelingen ondersteunen, gaat de ontwikkeling steeds sneller. De koppeling van

informatietechnologie en automatisering aan biotechnologie zorgt voor een steeds nauwkeurigere ontwikkeling en een potentieel gerichtere malafide toepassing.

Zo ligt er steeds meer nadruk op de risico's van biotechnologie bij opzettelijk misbruik. Met de technologie kunnen biologische wapens worden ontwikkeld die significante effecten kunnen hebben op mensen, planten en dieren. Biologische wapens kunnen bijvoorbeeld worden ingezet om (dodelijke) ziektes of genmodificaties te verspreiden onder mensen of dieren. Daarbij zijn door middel van biotechnologie ontwikkelde stoffen ook onderdeel van de Chemische, Biologische, Radiologische en Nucleaire (CBRN)stoffen[107], waarvoor er verhoogde risico's geconstateerd zijn en waarvan onwenselijke verspreiding tot grote verstoring van de maatschappij kan leiden. Biologische wapens worden vanwege hun potentieel grootschalige en catastrofale effecten tot de categorie 'massavernietigingswapens' gerekend.

Voor grote delen van biotechnologie bestaat internationale en EU-regelgeving om risico's voor mens, dier en milieu in te perken. Deze richten zich echter voornamelijk op genetisch gemodificeerde organismen (ggo's), en minder op de snelle doorontwikkeling van de technologie van de laatste jaren. Door nationale veiligheidsbelangen worden onderdelen van biotechnologie als sensitief aangewezen.

Sensitieve (sub)technologieën

Onderdelen van biotechnologie worden als sensitief aangemerkt. Het betreft de onderdelen genmodificatietechnieken, gene editing/genome engineering/precise genetic engineering, gendruk (Gene-drive), protein engineering, synthetische biologie, bioprinting, bioprocessing technologie, biofabrication, biomanufacturing, biocatalyse, emerging pathogens detection and characterization, en biological weapons detection and characterization.

Genetische modificatie (GM) is een techniek die de eigenschappen van planten, bacteriën of gisten verandert. Met GM wordt genetische informatie van het ene organisme toegevoegd aan een ander organisme. GM heet ook wel gentechnologie, of simpelweg gentech. Gene editing, genome engineering en/of precise genetic engineering omvat technieken die de mogelijkheid bieden het DNA of RNA van een organisme (mens, dier, plant, micro-organisme) op zeer specifieke plaatsen te veranderen. Gene drive, ook wel gendruk genoemd, is een vorm van genetische modificatie, waarbij het DNA zo wordt veranderd dat die mutatie via de geslachtelijke voortplanting aan alle nakomelingen doorgegeven wordt.

Protein engineering verwijst naar het ontwerpen en produceren van eiwitten (of polypeptiden) met nieuwe of verbeterde functies, vaak door modificatie van aminozuursequenties die in de natuur voorkomen. Dit kan computergestuurd of via gerichte evolutie in het laboratorium gebeuren.
Synthetische biologie maakt het mogelijk om nieuwe biologische systemen te ontwerpen, in tegenstelling tot de moleculaire biologie die de afgelopen decennia was gericht op modificatie van het genetisch materiaal van bestaande levensvormen. Met behulp van gesynthetiseerd DNA worden genetische onderdelen ontwikkeld, waarmee bio-ingenieurs levende systemen ontwerpen die optimaal bepaalde biochemische functies kunnen vervullen. Denk bijvoorbeeld aan efficiënte productie van medicijnen en biobrandstoffen en nieuwe behandelingsmethoden voor kanker en virusinfecties.

Bioprinting gebruikt 3D-printtechnieken om biologische structuren te maken, zoals weefsels, organen of cellen, door levende cellen en biomaterialen in een gecontroleerd patroon af te drukken. Het proces maakt gebruik van zogenaamde "bio-ink" die bestaat uit levende cellen en andere biologische stoffen. Synthetische biotechnologie speelt een

[107] Chemische, biologische, radiologische en nucleaire stoffen | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

sleutelrol in bioprinting, omdat het technieken omvat die het mogelijk maken om genetisch gemodificeerde cellen of op maat gemaakte biologische materialen te gebruiken.

Bioprocessing technologies verwijzen naar de technologieën en methoden die worden gebruikt voor het opschalen, optimaliseren en beheren van biologische processen, meestal voor de productie van biologische producten. Dit kan variëren van medicijnen, vaccins, bio-energie, tot voedingsmiddelen en biochemische stoffen. Biomanufacturing, oftewel biologische productie, verwijst naar het gebruik van biologische systemen, zoals micro-organismen, cellen of enzymen, om producten op industriële schaal te produceren. Het omvat processen waarbij levende organismen of biologische componenten worden gebruikt om waardevolle producten te maken, variërend van medicijnen en bio-energie tot chemische stoffen en voedingsmiddelen.

Biofabrication is een snel ontwikkelende high-tech tak van bioproductie. Biofabricage is de geautomatiseerde productie van biologisch functionele producten (weefsel, organ-on-a-chip) uit levende cellen, bioactieve moleculen en/of biomaterialen, vaak gebruikmakend van bioprinting of bioassembly.

Biocatalyse is het gebruik van natuurlijke katalysatoren (enzymen) om chemische reacties te versnellen. Enzymen zijn eiwitten die specifieke reacties mogelijk maken zonder zelf verbruikt te worden in het proces. Biocatalyse speelt een belangrijke rol in de biotechnologie en wordt gebruikt in een breed scala aan industriële toepassingen, van de productie van voedingsmiddelen en geneesmiddelen tot de verwerking van biobrandstoffen.

Daarnaast kunnen met biotechnologie potentiële biologische wapens worden gedetecteerd en gekarakteriseerd. Emerging pathogens detection and characterization is technologie die gebruikt wordt voor het detecteren en analyseren van nieuwe ziekteverwekkende organismen zoals virussen en bacteriën. Biological weapons detection and characterization is technologie die gebruikt wordt voor het detecteren en analyseren van biologische wapens. Daarbij wordt er middels de Uitvoeringswet verdrag biologische wapens ook toegezien op het ontwerp of productie van biologische wapens.

Chemische technologie

Chemische technologie is een tak van toegepaste chemie die zich bezighoudt met industriële technische methoden en apparaten om chemische producten te vervaardigen. Chemische technologieën zijn niet sensitief, met uitzondering van de subtechnologie micro- en nanoreactoren.

Microreactoren en nanoreactoren maken het mogelijk om chemische, biologische en nucleaire (strijd)middelen te produceren. Het voordeel ten opzichte van gebruikelijke productiemethodes is dat het veiliger is voor de producent, minder afval oplevert en sneller kan zijn (ook sneller op te bergen en op te ruimen). Daar komt bij dat het voor veiligheidsorganisaties lastiger is om dit soort activiteiten op het gebied van chemische wapens te detecteren, o.a. omdat er minder uitstoot van chemicaliën is. Het kleine formaat van micro- en nanoreactoren maakt het makkelijker om de technologie over te dragen aan kwaadwillenden. Combinatoire synthese op micro- of nanoreactor schaal kan leiden tot ontdekking van nieuwe dreiging agentia.

Een microreactor is een apparaat waarin chemische reacties plaatsvinden in een opsluiting met typische laterale afmetingen van minder dan 1 mm. De meest toegepaste vorm van een dergelijke opsluiting zijn microkanalen. De microreactor is meestal een continue stroomreactor (in tegenstelling tot een batchreactor). Microreactoren bieden veel voordelen ten opzichte van conventionele reactoren, waaronder enorme verbeteringen in energie-efficiëntie, reactiesnelheid en opbrengst, veiligheid,

betrouwbaarheid, beheersbaarheid, schaalbaarheid, on-site/on-demand productie en een veel fijnere mate van procescontrole. Nanoreactoren hebben veel vergelijkbare functies ten opzichte van microreactoren; het zijn nanofluïdische apparaten waarin chemische reacties optreden op nanoschaal.

Communicatie- en netwerktechnologie

Een voorbeeld van een technologie die door een statelijke actor kan worden ingezet om Nederland of haar bondgenoten te ondermijnen of saboteren, is communicatie- en netwerktechnologie. De sensitiviteit van communicatie- en netwerktechnologie ligt voornamelijk in de verwevenheid met de economie en de samenleving, omdat het de activiteiten van bedrijven, openbare veiligheidsorganisaties, de overheid, de bredere publieke sector, andere vitale infrastructuur en burgers ondersteunt.

Door de centrale rol van deze type technologieën en de hoge mate van digitalisering is de samenleving sterk afhankelijk van communicatie- en netwerktechnologie. Hoewel deze technologie alom vertegenwoordigd is in onze samenleving en veel producten niet uniek zijn, is onderzoek naar of met deze technologie per definitie een doorontwikkeling of vernieuwend. Communicatie- en netwerktechnologie is cruciaal voor een aantal vitale sectoren, waaronder telecommunicatie, energie en de financiële sector. Er wordt in Nederland onderzoek en ontwikkeling gedaan naar deze technologie, waarmee Nederland een vooruitstrevende rol en positie heeft. Gegeven de potentiële risicovolle toepassingen is het daarom van belang dat we kritisch kijken naar wie toegang krijgt tot hoog-risico onderzoek op dit gebied. Onderzoek naar of met communicatie- en netwerktechnologieën in de context van dit wetsvoorstel richt zich op het (door)ontwikkelen van bestaande en nieuwe technologieën die gebruikt kunnen worden in het militaire, politie-, en inlichtingen- en veiligheidsdomein, of die toegang kunnen geven tot een positie waardoor spionage of sabotage van vitale processen of andere processen die raken aan de nationale veiligheid mogelijk wordt.

Sensitieve (sub)technologieën

Onderdelen van communicatie- en netwerktechnologie worden als sensitief aangemerkt. Het betreft de onderdelen Radio-frequency (RF) and mixed signal circuits, antennas, filters and components, High-power microwave, Electromagnetic Pulse (EMP), High energy radio-frequency (RF) en Mobile and wireless network technologies en satellietcommunicatie.

Radiofrequentie (RF) en gemengde signaalcircuits, antennes, filters en componenten omvat elektronische componenten die nodig zijn voor zenders en/of ontvangers. Nieuwe technische ontwikkelingen zijn nodig om in de steeds grotere behoefte aan mobiele communicatiecapaciteit te kunnen voorzien, bijvoorbeeld het gebruik van hogere frequenties en steeds meer antennes bij de zender/ontvanger.[108] RF kent dual-use toepassingen en is sensitief omdat het kan worden toegepast in bijvoorbeeld wapensystemen en inzetbaar is in het defensiedomein.

High-power microwave verwijst naar het genereren en toepassen van krachtige microgolven, meestal boven de 1 gigawatt, voor militaire, wetenschappelijke of industriële doeleinden. Het wordt gebruikt in wapensystemen, communicatietechnologie en voor energieoverdracht over lange afstanden. HPM-systemen kunnen ook verstoringen veroorzaken in elektronische apparaten en netwerken door middel van elektromagnetische straling. High-power microwave kent dual-use toepassingen en is sensitief omdat het kan worden toegepast in bijvoorbeeld wapensystemen en inzetbaar is in het defensiedomein.

108 Multiple-input multiple-output (MIMO).

Een elektromagnetische puls (EMP) is een plotselinge, krachtige uitbarsting van elektromagnetische straling die kan ontstaan door kunstmatig gegenereerde technologie zoals high power microwaves. Deze puls heeft het vermogen om elektronische apparatuur te beschadigen of te verstoren door sterke elektrische stromen te induceren. EMP's kunnen zowel op grote schaal infrastructuren, zoals communicatie- en stroomnetwerken beïnvloeden, als kleinere apparaten in hun directe omgeving uitschakelen. EMP is sensitief omdat het tevens een militair goed is, kan worden toegepast in bijvoorbeeld wapensystemen en inzetbaar is in het defensiedomein.

Hoge-energie radiofrequentie (RF) technologie verwijst naar het gebruik van radiogolven met hoge energieën, vaak in de vorm van krachtige elektromagnetische straling, voor specifieke toepassingen zoals communicatie, radar of wapensystemen. Deze technologie wordt vaak ingezet voor het verstoren of beschadigen van elektronische apparatuur door middel van elektromagnetische interferentie, vergelijkbaar met een elektromagnetische puls (EMP). High Energy RF kan ook gebruikt worden voor energiedoeleinden, zoals draadloze energieoverdracht of het verhitten van materialen. Hoge-energie radiofrequentie is sensitief omdat het dual-use toepassingen kent, kan worden toegepast in bijvoorbeeld wapensystemen en inzetbaar is in het defensiedomein.

Mobiele en draadloze netwerktechnologieën omvatten ontwikkelingen ten behoeve van nieuwe generaties communicatie- en netwerktechnologieën zoals 5G/6G. Kenmerken zijn bijvoorbeeld hogere bandbreedte, lagere vertraging, zeer nauwkeurige plaatsbepaling en verdergaande integratie met edge computing, sensoren en radar. Ook wordt in toenemende mate gebruik gemaakt van AI om het netwerk te managen. Verwacht wordt dat het toepassingsbereik zal toenemen. Nationale veiligheidsrisico’s kunnen ontstaan bij misbruik van toegang tot (informatie over) gevoelige ICT-systemen in vitale processen en tot technologie, producten en diensten van leveranciers van netwerktechnologie.

Satellietcommunicatietechnologie kan zowel civiele als militaire toepassingen hebben. Satellietcommunicatie heeft veel van dezelfde toepassingen als normale telecommunicatietechnologieën, het verschil zit in de technologie. Satellietcommunicatie maakt gebruik van ruimtegebaseerde systemen, terwijl vormen van telecommunicatie vaak via aardse netwerken werken. Satellietcommunicatie heeft daarom net als telecommunicatie veel maatschappelijke toepassingen, maar is in toenemende mate van belang voor militair gebruik. Nederland beschermt via de ruimte de nationale veiligheid. Satellietcommunicatie wordt, zeker in meer afgelegen regio’s, vaak gebruikt voor militaire doeleinden. Het verlies van militaire communicatiecapaciteit tast onze capaciteiten stevig aan. Ook ontwikkelingen zoals laser-satellietcommunicatie dragen bij aan veel lager stroomverbruik en hogere efficiëntie van data-uitwisselingen. Daarnaast is laser-satellietcommunicatie veiliger dan radiocommunicatie, het is moeilijker af te luisteren. Dit maakt het ook voor militaire toepassingen erg interessant. Satellietcommunicatietechnologie maar ook sensitief omdat dit voor strategische autonomie heel belangrijk is en het kent dual-use toepassingen.

Cybersecuritytechnologieën

Cybersecuritytechnologieën zijn de digitale technische toepassingen die bedoeld zijn om digitale risico’s te verkleinen. Dit omvat ook het omgaan met risico’s op schade of uitval van digitale systemen en de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. Daarnaast zijn cybersecuritytechnologieën gericht op het voorkomen van cyberincidenten en, wanneer cyberincidenten zich hebben voorgedaan, deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Deze technologieën worden toegepast in vrijwel elk modern (hoog gerubriceerd) digitaal systeem of netwerk om te voorkomen dat het systeem of netwerk niet meer naar behoren kan functioneren door bijvoorbeeld verstoring, manipulatie, spionage.

Cybersecuritytechnologie is een cruciaal onderdeel voor de veiligheid van digitale infrastructuur. Daarbij blijft de digitale dreiging onverminderd hoog, waarbij op verschillende manieren de nationale veiligheidsbelangen geraakt kunnen worden. De territoriale veiligheid en de digitale veiligheid kunnen geraakt worden door cyberaanvallen van (statelijke) actoren. Wanneer kennis van cybersecuritytechnologie in verkeerde handen valt kan dit worden misbruikt om cybersecuritymaatregelen te omzeilen ten behoeve van spionage of sabotage.109 Wanneer dit gebeurt bij vitale processen kan dit potentieel ontwrichtend zijn en de sociale en politieke stabiliteit ontwrichten. Om goed te kunnen functioneren heeft cybersecuritytechnologie vaak verregaande systeemrechten nodig, waardoor dit in zichzelf ook riskante technologie betreft wanneer deze wordt gecompromitteerd. Cybersecuritytechnologie is daarmee sensitief wanneer dergelijke potentie mogelijk is. Wanneer cybersecuritytechnologie wordt gekenmerkt door een breed toepassingsbereik binnen verschillende vitale processen of andere processen die raken aan de nationale veiligheid of wanneer cybersecuritytechnologie van essentieel belang kan zijn voor het functioneren van defensie, opsporings-, inlichtingen- of veiligheidsdiensten bij de uitoefening van hun taken, is deze technologie sensitief.

Sensitieve (sub)technologieën

Versleutelingstechnologie, ook wel (toepaste) cryptografie, is de verzameling van kennis en technologieën die, in toepassing, ervoor zorgen dat digitale gegevens niet door ongeautoriseerde partijen gelezen of veranderd kunnen worden, en hun integriteit behouden. In dit technologieveld speelt cryptografie een belangrijke rol, maar ook autorisatie- en identificatietechnologieën en netwerktechnologie.

Hardware- en telecommunicatiebeveiligingstechnologieën die worden gebruikt voor de bescherming van de confidentialiteit, integriteit en/of beschikbaarheid van hoog gerubriceerde gegevens door middel van het voorkomen van interceptie en/of verstoring via het elektromagnetische spectrum dan wel het afluisteren van datacommunicatie op hardware niveau (side-channel attacks). Emission security (EMSEC)/ telecommunications electronics materials protected from emanating spurious transmissions (TEMPEST) kennen dual-use toepassingen en zijn sensitief omdat inzicht in deze technologie en de ontwikkeling daarvan een groot voordeel kan geven aan kwaadwillende statelijke actoren.

Detectie- en responsetechnologieën worden gebruikt voor de bescherming van de confidentialiteit, integriteit en/of beschikbaarheid van digitale gegevens en systemen door machinale uitvoering van beveiligingsacties, zoals het detecteren, onderzoeken en verhelpen van digitale dreigingen, met of zonder menselijke tussenkomst.

Energietechnologie

Energietechnologie betreft een breed gebied dat een scala aan technologieën voor de productie, opslag, transport en gebruik van energie omvat. Deze technologieën zijn volop in ontwikkeling door de overgang van fossiele energie naar hernieuwbare energie. Door gebruik van deze technologieën in vrijwel alle vitale processen en de sterke link met de energietransitie en -onafhankelijkheid zijn er in bepaalde gevallen risico’s voor de nationale veiligheid.

Sensitieve (sub)technologieën

Onderdelen van energietechnologie worden als sensitief aangemerkt. Het betreft de onderdelen: waterstoftechnologie, energieopslag en gasturbine technologie.

[109] Trendanalyse nationale veiligheid 2024 – verdieping op de trendanalyse.

Waterstoftechnologie kan een belangrijke bijdrage leveren aan de energietransitie en energie-onafhankelijkheid. Waterelektrolyse is daarmee een belangrijke technologie in ons toekomstige energiesysteem. Energieopslag omvat verschillende technologieën die opslagmethoden van energie mogelijk maken (waaronder batterijen) of technologie om waterstof op te slaan. Door het potentieel voor energieonafhankelijkheid, het belang van stabiele energietoevoer en de rol van energieopslagtechnologieën in de energietransitie zijn deze subtechnologiegebieden sensitief.

Gasturbinetechnologie wordt ingezet voor de ontwikkeling van (componenten voor) gasturbines. Gasturbinetechnologie wordt zowel toegepast in energieproductie als in voortstuwingsmechanismen in met name lucht- en scheepvaart. Door de mogelijke toepassingen in het militaire domein wordt gasturbinetechnologie als sensitief aangemerkt.

Geavanceerde materialen

Geavanceerde materialen hebben (veelal) gecombineerde mechanische, fysische en functionele eigenschappen die bepalend zijn voor nieuwe en revolutionaire toepassingen in verschillende domeinen. Zo spelen geavanceerde materialen een grote rol in de energietransitie, transportsector en de bouw, maar wordt veel van die kennis ook toegepast in het defensie- en veiligheidsdomein.
Geavanceerde materialen variëren (enorm) in schaalgrootte, van nano- en microschaal tot voorwerpen om ons heen. Van structuren op de kleinste schaal worden de mechanische, fysische en functionele eigenschappen van materialen gevormd. Zo kunnen additieven specifieke eigenschappen toevoegen aan materialen, zoals zelfreinigend vermogen. Synthese en karakterisatietechnieken zijn van belang voor de vervaardiging van geavanceerde materialen.

Sensitieve (sub)technologieën

Onderdelen van geavanceerde materialen worden als sensitief aangemerkt. Het betreft de onderdelen Energie materialen, Optische, elektronische, magnetische materialen en nanomechanische materialen, inclusief 2D en grafeen, thin films and coatings, bouw- en constructiematerialen (slimme materialen, designer en metamaterialen, composieten en keramieken, High Entropy Alloys (HEA)). Door de militaire toepassingen, dual-use eigenschappen en het potentiële disruptieve vermogen worden onderstaande onderdelen als sensitief aangemerkt.

Energiematerialen omvatten materialen die het mogelijk maken om (duurzaam opgewekte) energie op te slaan, te transporteren, efficiënt te vangen en efficiënt om te zetten naar een andere vorm of energiedrager. Optische, elektronische, magnetische en nanomechanische materialen omvatten materialen die het hart vormen van de geïntegreerde circuits- en sensortechnologie. De materialen geven functionaliteit aan communicatie toepassingen en gegevensverwerking en -opslag. Verdere miniaturisering en integratie met een vermindering van energiegebruik staat hierin centraal.

Thin films and coatings zijn dunne lagen materiaal, variërend van moleculaire- tot microschaal, die aangebracht kunnen worden op enkele of diverse oppervlakten en ondergronden. Door het aanbrengen van één of meerdere van dergelijke lagen of dunne films op andere materialen of oppervlakten kunnen extra functionaliteiten aan producten worden gegeven, zoals beschermende, zelfreinigende, zelfhelende, reflecterende (voor alle straling), absorberende, elektrische, optische of magnetische eigenschappen.

Slimme materialen reageren op veranderingen in de omgeving. Deze materialen kunnen onder externe invloeden veranderen of zichzelf herstellen. Metamaterialen zijn kunstmatig ontworpen materialen die vanwege hun ruimtelijke structuur andere eigenschappen hebben dan de samenstellende delen. Metamaterialen onderscheiden zich

door een functionaliteit die gegeven wordt door een hiërarchische structuur met verschillende lengteschalen. Dit geeft metamaterialen hun optische of mechanische eigenschappen gekoppeld aan hun macrostructuur. Designer materials omvat een volledig nieuwe methode om niet-natuurlijke materialen te ontwerpen waarbij (geavanceerde) computationele methodes worden ingezet, om op basis van gewenste eigenschappen, nieuwe materialen te ontwerpen. Composieten en keramieken zijn materialen die eigenschappen met een verbeterde sterkte laten zien. Dat werkt voornamelijk op basis van bijvoorbeeld vezels of een combinatie van meerdere vezels en/of materialen. Hieronder vallen composieten die bestaan uit samengestelde materialen met glas, keramiek, hout en/of polymeren. High-entropy alloys zijn legeringen met minimaal vijf elementen.

Halfgeleider technologieën

Nederland speelt wereldwijd een belangrijke rol in de productieapparatuur voor halfgeleiders (semiconductors). Deze halfgeleiders kunnen vanwege hun specifieke gebruiksmogelijkheden een cruciale bijdrage leveren aan bepaalde geavanceerde militaire toepassingen en kunnen worden aangewend voor de ontwikkeling van hoogwaardige militaire (wapen)systemen en massavernietigingswapens. Halfgeleiders zorgen dat elektriciteit 'getransporteerd' wordt. Halfgeleiders worden zo genoemd omdat ze een ‘half beschikbare’ eigenschap hebben tussen die van geleiders (waaronder materialen) en isolatoren (zoals rubber en glas). ‘Half’ verwijst naar het feit dat de materialen in sommige omstandigheden stroom kunnen geleiden, en in andere omstandigheden zich gedragen als isolatoren. Dit unieke gedrag maakt halfgeleiders essentieel voor de werking van vrijwel alle moderne elektronische apparaten. Zo worden microchips gemaakt van halfgeleiders. Halfgeleiderapparaten worden onder andere gebruikt om te schakelen, signalen te versterken en energie om te zetten. Vanwege de relevantie voor de (door)ontwikkeling van de defensie-industrie, geavanceerde wapensystemen en de integrale rol in veel vitale processen is het noodzakelijk om ongewenste toepassingen van de goederen en technologie wordt halfgeleidertechnologie als sensitief aangewezen.

Sensitieve (sub)technologieën
De productieketen van een halfgeleider omvat verschillende fasen. Zo wordt er ontworpen door middel van specialistische software, productie vindt plaats met specifieke materialen waarvan sommige in zeldzame ruwe aardmetalen zijn, gespecialiseerde machines en er wordt getest met behulp van specialistische apparatuur, alvorens hun weg te vinden in elektronische toepassingen. Deze stappen vertegenwoordigen verschillende onderzoeksfasen waar toegang tot kennis of technologie sensitief is in het kader van ongewenste kennis- en technologieoverdracht. Daartoe worden er softwaretools aangewezen als sensitief. Design and electronic design automation tools, ook bekend als electronic design automation (EDA) en electronic computer-aided design (ECAD) – is een categorie softwaretools voor het ontwerpen van elektronische systemen, zoals geïntegreerde circuits en geprinte circuit boards. De tools werken samen in een soort design flow en worden gebruikt door chipontwerpers om halfgeleiderchips te ontwerpen en analyseren.

Voor bepaalde toepassingen of toepassingsomgevingen van semiconductor technologies zijn specifieke materialen of ontwerpen vereist om de beoogde functie te kunnen uitvoeren. Deze staan bekend als specialized en tailored hardware components en omvatten ontwikkelde en toegespitste ontwerpen en ontwerpeisen op halfgeleidertechnologie.

Novel materials for advanced microelectronics duiden de recente ontwikkelingen op het gebied van halfgeleidermaterialen. De afgelopen jaren hebben halfgeleidermaterialen van de derde generatie (op basis van SiC en GaN) en nieuwe tweedimensionale halfgeleidermaterialen op basis van grafeen veel aandacht gekregen door hun grote

efficiëntie. Deze materialen spelen een zeer belangrijke rol bij de ontwikkeling van geïntegreerde schakelingen en kwantumopto-elektronische apparaten.

Voor het produceren van halfgeleiderchips zijn machines cruciaal, manufacturing process technologies and manufacturing equipment worden daartoe als sensitief aangewezen. Bij het ontwerpen van halfgeleiders vallen ook verschillende chiparchitecturen onder de werking van de wet. Een voorbeeld daarvan is de complementary metal oxide semiconductor (CMOS), een halfgeleidertechniek voor de productie van geïntegreerde schakelingen. Het belangrijkste voordeel van CMOS is dat het minder energie verbruikt dan andere technologieën, zoals Bipolar Junction Transistor (BJT)-technologie. Dat maakt het bijzonder geschikt voor toepassingen waarbij energie-efficiëntie belangrijk is, zoals draagbare elektronica.

Heterogeneous integration and advanced packaging richt zich op het integreren van alle functies in een enkele chip (bekend als system-on-a-chip (SoC)). Het verwijst naar de integratie van afzonderlijk vervaardigde componenten in een assemblage op een hoger niveau (System-in-Package, SiP) die, in totaal, verbeterde functionaliteit en verbeterde operationele kenmerken biedt.

Wide-bandgap and ultrawide-bandgap technologies for power management, distribution and transmission betreft halfgeleiders met een brede bandgap (ook bekend als WBG-halfgeleiders of WBGS's) en halfgeleidermaterialen met een grotere bandafstand dan conventionele halfgeleiders. Halfgeleiders met een brede bandgap zorgen ervoor dat apparaten bij veel hogere spanningen, frequenties en temperaturen kunnen werken dan het geval is bij conventionele halfgeleidermaterialen. Dit maakt ze zeer geschikt voor militaire toepassingen. Ze worden ook gebruikt in bepaalde radiofrequentietoepassingen, met name in militaire radars. Ultrawide bandgap halfgeleidermaterialen (UWBGS) zijn een subset van WBGS-materialen en worden gedefinieerd als die WBGS-materialen met een bandgap boven die van GaN, namelijk 3,4 eV.

Hypersonische technologie

Hypersonische vliegtuigen of raketten ontlenen hun naam aan hun zeer hoge snelheid: vijf keer of meer sneller dan de lokale geluidssnelheid (Mach 5, ongeveer 6000 km/uur op zeeniveau). Hypersonische systemen zijn niet nieuw; ook ruimtecapsules en ballistische raketten zijn de-facto hypersonisch bij terugkeer in de atmosfeer en bereiken deze hypersonische snelheden als gevolg van de val terug naar aarde. Vanwege de hoge weerstand in het hypersone Mach-regime houden ballistische raketten deze snelheid echter niet voor langere tijd vol en volgen een meer voorspelbare baan.

Sensitieve (sub)technologieën

Alle onderdelen van hypersonische technologie worden als sensitief aangemerkt. Hypersonische aandrijvingstechnologie is technologie die gebruikt wordt voor de doorontwikkeling van scramjet straalmotoren en de ontwikkeling van geheel nieuwe motoren bestemd voor acceleratie tot en handhaving van hypersone snelheden. Hieronder vallen ook zogenoemde ‘combined cycle’ motoren die traploos over kunnen schakelen van turbojet naar ramjet (supersoon) en naar scramjet. Deze technologie wordt onder andere gebruikt voor hypersone kruisraketten. Hypersone kruisraketten (HCM – Hypersonic Cruise Missiles) verzorgen hun eigen voortstuwing (raket, ramjet of scramjet) na lancering.

Hypersone glijvoertuigen (HGV – Hypersonic Glide Vehicles) beschikken niet over een eigen voortstuwingssysteem en maken gebruik van ballistische raketten voor hun lancering. Naast HGV’s en HCM’s bestaan er cross-overs waarbij bestaande raketten zijn doorontwikkeld tot een hypersone raket.

Thermische bescherming/koeling voor hypersonische systemen betreft materialen die de extremen van hypersone raketten kunnen weerstaan. Er zijn geavanceerde materialen nodig voor het oppervlak van de hypersone systemen die zowel de hoge temperaturen van meer dan 1000°C kunnen weerstaan als sterk genoeg zijn. Ook de aansturing vereist vergaande technologische ontwikkeling. Besturing en aerodynamica voor hypersonische systemen omvat de aansturing van hypersone systemen welke nieuwe ontwikkelingen vereist door de ongebruikelijke luchtstromingen/luchtwervelingen. Hierin spelen computermodellen en simulaties ook een grote rol. Hierbij kan gedacht worden aan Computational Fluid Dynamics (CFD) simulaties waarin de complexe fysica wordt meegenomen.

Om hypersonische raketten dan wel glijvoertuigen adequaat te kunnen counteren worden verschillende technologieën ontwikkeld. Hieronder vallen onder andere Divert and Attitude Control Systems (DACS). Dit zijn systemen met kleine raketmotors voor standregeling en baanmanoeuvres van een voertuig bij geringe aerodynamische druk (grote hoogte). Ook detection, tracking, guiding and characterization of hypersonic systems is een technologiegebied dat zich verder ontwikkelt. Hierbij wordt gefocust op detectie- en defensiesystemen voor hypersone raketten.

Hypersonische interceptie-technologie verwijst naar systemen die hypersonische wapens detecteren en onderscheppen, zoals geavanceerde radars en raketsystemen. Endgame-technologie betreft de laatste fase van raketafweer, waarbij systemen proberen inkomende raketten of warheads vlak voor hun doel te vernietigen. Dit vereist zeer snelle, nauwkeurige interceptie met behulp van geavanceerde sensoren en kunstmatige intelligentie.

Kwantumtechnologie

Kwantumtechnologie maakt gebruik van specifieke verschijnselen uit de kwantumfysica en benut het bijzondere gedrag van energie en materie op atomaire en subatomaire schaal, om op een radicaal nieuwe manier te kunnen rekenen, communiceren en meten[110]. Deze technologieën zullen naar verwachting veel van onze huidige standaarden op het gebied van cryptografie en sensoren drastisch veranderen. Kwantumtechnologie is momenteel nog in ontwikkeling en nog niet op grote schaal toepasbaar, maar het is de verwachting dat met deze technologie de meeste bestaande vormen van asymmetrische cryptografie doorbroken kunnen worden. Het is dan ook al voorzienbaar en voorstelbaar dat de inzet van de kwantumcomputer grote disruptieve gevolgen kan hebben en daarmee een risico vormt voor onze nationale veiligheid. De inzet van de kwantumcomputer kan leiden tot grote veranderingen in het militaire en veiligheidsdomein. Daarmee is de snelle ontwikkeling van de technologie voor Nederland en haar bondgenoten reeds een groot risico voor de nationale veiligheid. Het land dat als eerste kan beschikken over een kwantumcomputer heeft tevens ook een belangrijk strategisch machtsmiddel in handen

Het is voorstelbaar dat actoren nu al versleutelde informatie verzamelen om die, na de komst van een kwantumcomputer, te ontsleutelen. Dit wordt ook wel "store-now-decrypt-later" genoemd. Veruit de belangrijkste maatregel tegen het breken van bepaalde huidige cryptografie is om deze cryptografie zo spoedig mogelijk te mitigeren naar Post Quantum Cryptografie.[111] Bovendien is het belangrijk om nu al kritisch te zijn ten aanzien van wie we op die ontwikkeling mee laten kijken en dus toegang geven tot hoog-risico onderzoek naar kwantumtechnologie, in het bijzonder quantum computing. Op die manier beschermen we onze kennis- en technologieontwikkeling, maar ook de vitale infrastructuur en processen die door het breken van huidige cryptografie geraakt zullen worden.

[110] Trendanalyse nationale veiligheid 2024 – verdieping op de trendanalyse
[111] Het PQC-migratie Handboek | Publicatie | AIVD

Sensitieve (sub)technologieën

Onderdelen van kwantumtechnologie worden aangewezen als sensitief. Het betreft de onderdelen kwantumcomputing, kwantumcryptografie, kwantumcommunicatie, kwantumsensoren.

Kwantumcomputers bestaan uit verschillende lagen, waaronder onder andere de hard- en software, en maken gebruik van de mechanismen uit de kwantummechanica om problemen op te lossen die te complex zijn voor klassieke computers. Er wordt onderscheid gemaakt tussen gespecialiseerde kwantumcomputers, algemene (universele) kwantumcomputers en hybride vormen. Een gespecialiseerde kwantumcomputer kan maar één specifiek vraagstuk oplossen, bijvoorbeeld optimalisatievraagstukken. Een algemene (universele) kwantumcomputer heeft naar schatting miljoenen kwantum bits nodig om verschillende typen vraagstukken aan te kunnen. De kracht van een kwantumcomputer zit hem in het oplossen van specifieke vraagstukken, en zal naar verwachting de 'gewone' computer niet vervangen. Om optimaal gebruik te maken van een kwantumcomputer wordt er gewerkt aan het koppelen van een quantum computer met een High Performance Computer, ook wel hybride kwantum computing genoemd.

Binnen kwantumcommunicatie worden kwantum devices met elkaar verbonden en worden deeltjes op verschillende plaatsen in het netwerk, zowel via grondnetwerken als satellietnetwerken, met elkaar verbonden, zodat kwantuminformatie kan worden verstuurd. Voor de aansturing van een kwantumnetwerk is altijd een 'gewoon' digitaal netwerk nodig. Kwantumcommunicatie kan niet gekopieerd worden omdat (ongewilde) tussentijdse metingen (onderschepping) de kwantumtoestand die wordt verstuurd merkbaar veranderen. Dit gegeven is uniek voor kwantumcommunicatie.

Een belangrijk onderdeel van kwantumcommunicatie technologie is de kwantumcryptografie, wat zich richt op het gebruik van principes uit de kwantummechanica voor vernieuwende (onbreekbare) encryptiemethoden. Een voorbeeld van kwantumcryptografie is quantum key distribution (QKD), een techniek waarmee twee partijen cryptografisch sleutelmateriaal kunnen genereren om communicatiekanalen te beveiligen op een manier die zelfs een kwantumcomputer niet kan breken.

Kwantum sensing behelst de technologie van het toepassen van kwantumprincipes om een grotere meetnauwkeurigheid te bereiken dan die van conventionele sensoren. Hierbij kan gedacht worden aan onder andere de nieuwe generatie magnetometers, atoomklokken, versnellingsmeters, gyroscopen, en quantum imaging.

Militair toepasbare technologie

Militair toepasbare technologieën betreffen technologieën die specifiek ontwikkeld worden voor militaire goederen zoals wapensystemen, munitie en explosieven, militaire voer-, vaar- en vliegtuigen, en aanverwante componenten of systemen voor militaire toepassingen. Militaire technologieën zijn vrijwel uitsluitend gericht op toepassingen in wapensystemen. Deze wapensystemen worden in principe alleen gebruikt door militaire en andere veiligheidsorganisaties.

Militair toepasbare technologieën in de context van dit wetsvoorstel betreffen diverse categorieën van de gemeenschappelijke EU lijst van militaire goederen[112]. De beschrijvingen in dit wetsvoorstel dienen ter verduidelijking van het begrip militair toepasbare technologie in de context van dit wetsvoorstel en zijn geen vervanging van

of aanvulling op de definitie van militaire technologie in de context van wapenexportcontrole. Daarvoor is de gemeenschappelijke EU-lijst van militaire goederen leidend.

Sensitieve (sub)technologieën

Alle onderdelen van militair toepasbare technologie in de context van dit wetsvoorstel worden als sensitief aangemerkt. Vrijwel alle toepassingen van militair toepasbare technologieën zijn toegespitst op wapensystemen. Hieronder vallen wapentechnologieën, wat technologieën omvat voor het ontwikkelen van (componenten voor) wapensystemen. Ook technologie voor ammunitie en explosieven, waartoe technologieën worden ontwikkeld voor (componenten van) munitie en ander explosief materiaal vallen hieronder. Specialisaties als slimme munitie zijn recentelijke veelbelovende, maar ook risicovolle ontwikkelingen. Militaire platformtechnologieën zijn technologieën voor het ontwikkelen van (componenten voor) geïntegreerde platformen voor gebruik op land, in water, in de lucht of in de ruimte, specifiek bedoeld voor militair gebruik. Platformen voor gebruik in de ruimte vallen deels ook onder de categorie 'Ruimtevaarttechnologie'.

Nanotechnologie

Nanotechnologie werkt met verschijnselen op nanoschaal, dat wil zeggen ongeveer 1 tot 100 nanometer en met hoge precisie. Nanotechnologie omvat de beeldvorming, modellering, meting, ontwerp, karakterisering, productie en toepassing van structuren, apparaten en systemen door gecontroleerde manipulatie van grootte en vorm op nanometerschaal (atomaire, moleculaire en macromoleculaire schaal). Dit levert structuren, apparaten en systemen op met nieuwe en eventueel superieure kenmerken of eigenschappen. Daarmee is nanotechnologie *enabling* voor vele andere technologieën en zijn er duidelijke raakvlakken met andere sleuteltechnologieën via integratieve toepassingen.

Nanotechnologie kent zowel vreedzame als niet vreedzame toepassingen. Nanotechnologie wordt onder andere gebruikt in IT-toepassingen, medische toepassingen, maar ook de energie- en chipsector. Toepassingen van nanotechnologie kan echter ook ingezet worden als wapen[113] in conventionele en nieuw te ontwikkelen wapensystemen. Ook identiteitsmanipulatie, vergiftiging en bommen vallen binnen de mogelijkheden van nanotechnologie. Bijkomend maakt de schaalgrootte de dreigingen moeilijk of niet detecteerbaar, is verspreiding gemakkelijk en is het ongedaan maken van ingezette aanvalswapens niet eenvoudig.[114] Door deze dreigingen en een toenemende focus op miniaturisering wordt de rol van nanotechnologie steeds groter in verschillende domeinen. De Wet screening kennisveiligheid wijst nanotechnologie als sensitief.

Sensitieve (sub)technologieën

Nanomanufacturing omvat fabricageprocessen om structuren en functionaliteit op nanoschaal te bouwen. Nanomanufacturing heeft raakvlakken met de fabricage van nanomaterialen zelf (zie hieronder). Zo is ook voor nanofabricage-technologie het karakteriseren en (theoretisch) ontwerpen van materialen van belang, in combinatie met de instrumenten/methodes om nanomaterialen te maken of te laten groeien. Daarbij worden computationele methodes ingezet. Tevens omvat nanofabricage-technologie de opschaling van fabricage van één device naar grote aantallen. Tenslotte is het aanbrengen van nano-coatings op grote oppervlakten (depositie technologie) een belangrijke uitdaging in de productie van onder meer wafers en zonnepanelen.

[113] Technologieverkenning Nationale Veiligheid 2014.pdf (rivm.nl)
[114] Technologieverkenning Nationale Veiligheid 2014.pdf (rivm.nl)

Nanomaterialen zijn chemische stoffen of materialen die bestaan uit zeer kleine deeltjes van verschillende vorm en grootte (< 100nm, evenals 2D-materialen). Ze komen voor in de natuur, kunnen een incidenteel product van menselijke activiteit zijn (bv. lasrook) of doelbewust worden vervaardigd en gemanipuleerd om nieuwe kenmerken te vertonen of een specifieke structuur aan oppervlakten te geven. Voorbeelden zijn een grotere sterkte, chemische reactiviteit of geleidingsvermogen in vergelijking met hetzelfde materiaal zonder nanoschaalkenmerken. De vervaardiging van dergelijke materialen en nano-gestructureerde oppervlakten vereist instrumenten en methodes om deze te maken of te laten groeien en om het resultaat daarvan op nanoschaal te inspecteren en karakteriseren (zie ook Nanomanufacturing). Bij het ontwikkelen van nieuwe nanomaterialen worden computational methodes steeds meer ingezet, bijvoorbeeld ten behoeve van 'materials by design', waarin gewenste eigenschappen van de nanomaterialen het vertrekpunt vormen.

Micro- en nano-vloeistofdynamica verwijst naar het bestuderen en beheersen van vloeistoffen op micro- en nanoschaal, waarbij stroming, manipulatie en controle van vloeistoffen plaatsvinden in kanalen die slechts enkele micrometers of nanometers groot zijn. Deze technologieën worden toegepast in diverse gebieden zoals biotechnologie, geneeskunde (bijvoorbeeld in laboratorium-on-a-chip systemen), en chemie, waar ze het mogelijk maken om uiterst kleine hoeveelheden vloeistoffen met hoge precisie te analyseren of te verwerken. Micro- en nanofluidics maakt gebruik van de unieke fysische eigenschappen van vloeistoffen op zulke kleine schaal, zoals veranderingen in viscositeit, oppervlaktespanning en diffusie.

Functionele apparaten en structuren (op nanoschaal) omvat het combineren en integreren van elektronische, magnetische, nano-mechanische, optische, bio of quantum principes in componenten of apparaten die materie op atomaire of moleculaire schaal kunnen manipuleren. De nano-dimensies en materiaaleigenschappen maken complexe schakelingen en arrays mogelijk.

Nanobiotechnologie / bio-nanotechnologie behelst de toepassing van nanotechnologie op het bestuderen van het leven op nanoschaal om inzichten te krijgen in bijvoorbeeld cellen en virussen. Die inzichten zijn onder andere van belang in medische toepassingen, sensoren, life-inspired materialen, synthetische cellen. Bionanotechnologie is de toepassing van moleculaire biologie op nanotechnologie waarbij materialen en apparaten op nanoschaal worden vervaardigd.

Nucleaire technologie

Nucleaire technologieën zijn technologieën die gebruik maken van kernsplijting of kernfusie om energie op te wekken. Naast onderzoek, betreft dit ook aanverwante en ondersteunende toepassingen over het inrichten of operationaliseren van faciliteiten gericht op nucleaire activiteiten. Ook technologie voor detectie, bedoeld voor het detecteren en analyseren van nucleaire materialen (zoals bijvoorbeeld neutronendetectoren), wordt hieronder geschaard.

Nucleaire technologie valt onder Categorie 0 – Nucleaire goederen van de EU verordening over controle op producten voor tweeërlei gebruik[115]. Daarnaast komt deze technologie voor in bepaalde internationale sanctieregimes. Voor uitvoer van deze goederen en technologieën is reeds een vergunning vereist of is reeds sprake van een verbod op technische bijstand.

[115] VERORDENING (EU) 2021/821 VAN HET EUROPEES PARLEMENT EN DE RAAD van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (herschikking)

Sensitieve (sub)technologieën

Kernenergie-technologieënzijn technologieën die kernsplijting of kernfusie gebruiken voor het opwekken van energie. Dit kan ook worden gebruikt voor kernenergie- en aandrijvingstechnologieën, waarbij kernsplijting of kernfusie gebruikt wordt voor onder andere aandrijving en/of voortstuwing van voertuigen van diverse aard, bijvoorbeeld raketten, ruimtevoertuigen, schepen en onderzeeboten.

Nucleaire technologie kan ook voor andere doeleinden gebruikt worden. Deze technologie, genaamd kerntechnologieën voor andere doeleinden, gebruikt de deeltjes die vrijkomen bij kernsplijting of kernfusie, zoals bijvoorbeeld neutronen voor andere toepassingen dan hierboven genoemd. Denk bijvoorbeeld aan wetenschappelijk onderzoek, agrarische toepassingen, zoals het verbeteren van gewassen, en medische toepassingen, zoals de productie van medische isotopen.

Detectie- en karakteriseringstechnologieën voor kernmaterialen is technologie bedoeld voor het detecteren en analyseren van nucleaire materialen, bijvoorbeeld neutronendetectoren.

Verrijkingstechnologie als enabling technologie betreft technologieën die worden gebruikt om het percentage van de splijtbare isotoop uranium-235 (U-235) in natuurlijk uranium te verhogen. Dit proces is essentieel om uranium geschikt te maken voor gebruik in kernreactoren of als grondstof voor kernwapens. Verrijkingstechnologie kan daarnaast ook ten dienste van energie-toepassingen ingezet worden.

Radiation implosion technologie is een subtechnologie van nucleaire technologie. Dit is een belangrijke techniek die essentieel is voor bijvoorbeeld de detonatie van thermonucleaire wapens. Daarbij wordt intense straling gebruikt om een fusiebrandstof onder extreem hoge druk en temperatuur te comprimeren. In nucleaire fusie wordt deze techniek toegepast in apparaten zoals intertiale opsluiting fusie (ICF)-reactoren. Daarbij richten laserstraling op een klein pellet brandstof, waardoor dit implodeert en een fusie-reactie op gang komt. Hoewel de technologie potentie biedt voor energieopwekking, wordt de technologie ook gebruikt voor nucleaire wapens. Om die reden is radiation implosion technology als onderdeel van radiological technologies aangewezen als sensitief.

Optica and Fotonica

Fotonicatechnologie richt zich op het opwekken, transporteren en detecteren van lichtgolven en lichtdeeltjes, ook wel fotonen genoemd.[116] De technologie kent zeer brede toepassingsmogelijkheden in onder andere halfgeleiders, ICT en energiesectoren. De technologie wordt in zeer veel 'hightech' producten toegepast, niet alleen in consumentenproducten zoals beeldschermen, camera's, telefoons, internetverbindingen, zonnepanelen en verlichting, maar ook in specifieke militaire producten zoals nachtkijkers of diverse soorten sensoren voor veiligheidstoepassingen. Fotonica is tevens een basistechnologie voor diverse andere technologieën; zo zijn de machines om semiconductors te produceren gebaseerd op fotonicatechnologie en is fotonica een key enabling technology voor bijvoorbeeld kwantumtechnologie en kunstmatige intelligentie.[117] Daarbij staat de technologie in toenemende mate centraal in geopolitieke spanningen door de integratie in de halfgeleiderindustrie.[118] Ook wordt het voor toepassingen gebruikt in defensie- en veiligheidsdomein, waaronder het middels

[116] Trendanalyse nationale veiligheid 2024 – verdieping op de trendanalyse
[117] Trendanalyse nationale veiligheid 2024 – verdieping op de trendanalyse
[118] Trendanalyse nationale veiligheid 2024 – verdieping op de trendanalyse

lichtsignalen communiceren.[119] Fotonicatechnologie kent hierdoor meerdere sensitieve toepassingen en wordt als sensitief beschouwd.

Sensitieve (sub)technologieën

Onderdelen van Optica en Fotonica worden als sensitief aangemerkt. Het betreft de onderdelen geïntegreerde fotonica, geavanceerde beeldvormingstechnologieën, fotonische detectie, foton generatie technologieën, hoge-vermogen lasers, optische sensoren/fotonische sensoren, adaptieve optica, optomechatronica, optische componenten.

Geïntegreerde fotonica verkleint en integreert fotonische componenten samen met de vereiste elektronica op één chip. Deze integratie en miniaturisatie heeft verschillende voordelen, zoals lagere signaalverliezen, lagere kosten vanwege minder benodigd materiaal en een verbetering van de mogelijkheid tot massaproductie. Fotonisch geintegreerde circuits kennen vele toepassingen, voornamelijk in bekabelde communicatie, maar ook radio frequency, 3D-imaging, sensing, optische signaalverwerking en quantum computing. Dit leidt tot innovaties in ICT-applicaties die traditioneel op basis van elektronica en sensoren werken, bijvoorbeeld voor medische toepassingen en LIDAR (laser imaging detection and ranging).

Licht wordt binnen het subonderdeel geavanceerde beeldvormingstechnologieën gebruikt voor imaging en sensing. In computational imaging wordt geen lens gebruikt, dit gaat op basis van algoritmen. Een concreet voorbeeld hiervan zijn multispectral and hyperspectral imaging sensors. Dit zijn twee typen beeldvormende technologieën die gegevens van meerdere frequentiebereiken verzamelen en daarbij ook gegevens voorbij het spectrum van zichtbaar licht weergeven (zoals infrarood, nabij-infrarood en radar). Het verschil tussen deze technologieën is dat multispectrale sensoren gegevens verzamelen van twee tot tien frequentiebereiken, terwijl hyperspectrale sensoren gegevens verzamelen van wel duizenden frequentiebereiken.

Fotonische detectie betreft technologieën die individuele fotonen kunnen vastleggen en tellen. Deze worden onder andere gecreëerd door Foton generatie technologieën, waar middels technologie individuele fotonen worden gemaakt.

Laser technology is in de basis een vorm van lichtversterking door middel van een gestimuleerde uitzending van optische straling, om een geconcentreerde vorm van licht te genereren. Dit gebied kan worden opgedeeld in twee typen lasertechnologie waarvan alleen high power lasers sensitief zijn. Hoge-vermogen lasers zijn extra krachtige lasers met meestal een vermogen van minstens meerdere kilowatts. Deze lasers kennen meerdere toepassingen in het defensiedomein.

Optische sensoren/fotonische sensoren zijn fotonische sensoren welke zich richten op het detecteren, zenden, ontvangen en converteren van lichtenergie naar elektronische signalen. Deze sensoren zijn in staat om een breed scala aan gegevens vast te leggen, zoals temperatuur, druk, gasconcentraties, en chemische samenstellingen, door de interactie van licht met de omgeving. Door het vermogen om uiterst gedetailleerde en real-time informatie te verzamelen kennen optische en fotonische sensoren grote mogelijkheden in militaire toepassingen.

Adaptieve optica is een techniek om het beeldvertroebelende effect van de aardatmosfeer te reduceren/compenseren. Adaptieve optica kent mogelijke toepassingen in militaire systemen, bijvoorbeeld in geavanceerde verkenning en doelwitdetectie. Daarnaast kan de technologie ook worden gebruikt voor het ontwikkelen van verbeterde bewakings- en afweersystemen, wat zorgen oproept over spionage of

[119] Trendanalyse nationale veiligheid 2024 – verdieping op de trendanalyse

misbruik door tegenstanders. Het gebruik van adaptieve optica in combinatie met andere geavanceerde technologieën kan bovendien leiden tot verhoogde kwetsbaarheden, zoals het manipuleren van satelliet- of communicatiesystemen.

Optomechatronica behelst de ontwikkeling van technologieën om voorgaande technologieën en optische ontwerpen mechanisch mogelijk te maken. Hiervoor worden speciale componenten ontwikkeld, genaamd optische componenten. Dit zijn onderdelen die licht manipuleren, zoals lenzen, spiegels, prisma's en filters, om het in de gewenste richting of vorm te sturen. Ze worden gebruikt in toepassingen, zoals communicatie en medische technologie, en wetenschappelijk onderzoek. Deze componenten maken het mogelijk om licht te focussen, te splitsen of te filteren, afhankelijk van de specifieke functie in het systeem.

Positie-, Navigatie- en Tijdbepaling (PNT) technologieën

De technologieën die hieronder vallen richten zich op methoden en technieken voor positie-, navigatie- en tijdbepaling. Positiebepaling is het vermogen om nauwkeurig de eigen positie en oriëntatie te bepalen ten opzichte van een gestandaardiseerd geodetisch model. Navigatie gaat over het vermogen om de actuele positie te bepalen en om correcties toe te passen op de eigen koers, oriëntatie en snelheid om zodoende de gewenste bestemming te bereiken. Tijdsbepaling betreft het vermogen voor het verkrijgen en behouden van een nauwkeurige tijd die gerefereerd is aan een universele tijdstandaard.

Sensitieve (sub)technologieën

Satellite space-based PNT systems zijn op satellieten gebaseerde netwerken, die worden gebruikt om nauwkeurige informatie over positie, navigatie en tijd te verstrekken. Deze systemen bieden essentiële diensten voor transport, communicatie, defensie en vele andere sectoren, door real-time gegevens te leveren die cruciaal zijn voor tal van systemen en operationele activiteiten

Ground-, air- and sea-based PNT systems bieden locatie-, navigatie- en tijdsinformatie via verschillende platforms. Ground-based PNT maakt gebruik van terrestrische netwerken, air-based PNT van luchtvaarttechnologieën, en sea-based PNT van maritieme systemen zoals (ultra)sonische en radartechnologie. Deze systemen kunnen samenwerken met satellietgebaseerde PNT zoals GPS om nauwkeurige gegevens wereldwijd te leveren.

Inertiële navigatiesystemen (INS)betreft navigatiesystemen die de beweging van een voertuig volgen door gebruik te maken van versnellingsmeters en gyroscopen om veranderingen in snelheid en richting te meten. Deze systemen berekenen de positie, snelheid en oriëntatie van het voertuig op basis van interne metingen, zonder externe referenties zoals GPS.

Hybride en autonome navigatiesystemen combineren verschillende technologieën, zoals GPS, inertiële navigatie en sensoren, om voertuigen zonder menselijke tussenkomst te laten navigeren. Hybride systemen gebruiken meerdere bronnen voor nauwkeurigheid, vooral in gebieden met beperkte GPS-beschikbaarheid. Autonome navigatiesystemen maken gebruik van kunstmatige intelligentie om op basis van sensordata en daarop aansluitende besluitvormingsalgoritmes zelfstandig beslissingen te nemen en obstakels te vermijden.

Gravitatiekrachtdetectoren zijn apparaten die de zwaartekracht of veranderingen in de zwaartekracht meten, vaak door het detecteren van krachten die worden uitgeoefend op een massa in reactie op zwaartekrachtvelden. Deze sensoren worden vaak

gecombineerd met andere technologieën, zoals gyroscopen en magnetometers, om nauwkeurige navigatie-informatie te bieden.

Atomische klokken zijn klokken die de tijd meten op basis van de trillingen van atomaire deeltjes, zoals de overgang van elektronen tussen energieniveaus in atomen (meestal cesium of rubidium). Ze bieden extreem nauwkeurige tijdmeting, met afwijkingen van slechts een paar miljardsten van een seconde per dag. Atomische klokken worden gebruikt in GPS-systemen, bij wetenschappelijke experimenten, en bij netwerksynchronisatie, waar precisie essentieel is.

Magnetische veldsensoren worden gebruikt in navigatiesystemen om de oriëntatie en richting van objecten te bepalen door het meten van het aardmagnetisch veld. Ze worden gebruikt in een breed scala van toepassingen, zoals navigatie en geofysisch onderzoek.

Gelijktijdige lokalisatie en mapping (SLAM) is een technologie die wordt gebruikt door autonome systemen, zoals robots en zelfrijdende voertuigen, om een kaart van een onbekende omgeving te creëren, terwijl ze tegelijkertijd hun eigen positie binnen die omgeving bepalen. Deze techniek maakt gebruik van sensoren, zoals LiDAR, camera's en radar, om obstakels te detecteren en de omgeving in kaart te brengen. SLAM is essentieel voor toepassingen waarbij real-time navigatie en het vermijden van obstakels vereist zijn zonder voorafgaande kennis van de omgeving.

Robotica en autonome systemen

Robots zijn mechanische apparaten die zelfstandig (autonoom) taken kunnen uitvoeren. Om deze taken uit te voeren worden robots uitgerust met regeltechniek (control engineering) en sensoren (zoals optisch, radar en sonisch). Tegenwoordig wordt robotica ook vaak gecombineerd met kunstmatige intelligentie om robots met een enigszins lerend vermogen te laten anticiperen op wisselende omstandigheden.

Sensitieve (sub)technologieën

Onbemande voertuigen (UxV's) zijn onbemande systemen (voertuigen, luchtvaartuigen, oppervlaktevaartuigen en onderwatervaartuigen) en kunnen zichzelf vrijelijk in de omgeving (in de lucht, op de grond en op of onder water) verplaatsen zonder dat er een menselijke bestuurder aan boord is. Deze verplaatsing kan autonoom gebeuren of via aansturing op afstand. Onbemande voertuigen kunnen ook opereren zonder operator, de zogeheten autonome onbemande voertuigen. In het geval van autonome verplaatsing zijn UxVs in staat om hun werking bij te sturen of aan te passen op basis van (onverwachte) evenementen uit de omgeving of bijvoorbeeld obstakels. Omgevingsbewustzijn wordt gefaciliteerd door een combinatie van sensoren, dataverwerking en kunstmatige intelligentie. Bij autonome UxVs is de software-integratie, die zorgt voor dataverwerking en intelligentie, dus van groot belang.

Op afstand bestuurde onbemande voertuigen maken gebruik van een menselijke operator welke op afstand zorgt voor de aansturing en verplaatsing van de UxV. Met name de integratie met de communicatieve technologie die aansturing mogelijk maakt is hierbij zeer belangrijk.

Robotzwermen, ook bekend als distributed collaborative systems, zijn een troep UxVs die bewegen en acteren als een groep met beperkte menselijke tussenkomst. Grote technologische ontwikkelingen liggen onder andere op het compleet autonoom opereren van een robotzwerm.

Human-machine teaming en interfaces verwijzen naar de samenwerking tussen mensen en machines, waarbij technologie wordt ingezet om menselijke capaciteiten te

verbeteren en te ondersteunen. In deze context werken mensen samen met geavanceerde systemen waarbij de machine taken uitvoert die vaak repetitief, complex of gevaarlijk zijn, terwijl de mens toezicht houdt, beslissingen neemt (mens-AI interactie) en de richting aangeeft. Dit onderdeel heeft twee subgebieden, te weten brain-computer interfaces, waarbij hersenactiviteit wordt gemeten en omgezet in signalen waarmee computers worden aangestuurd, en human-machine teaming. Hierbij wordt gekeken naar het front waar mens en intelligente technologische systemen (zoals (semi-)autonome robotsystemen, AI-systemen of (gedistribueerde) controlekamers) samenkomen en samenwerken om een bepaald doel te bewerkstelligen.

Ruimtevaarttechnologie

Ruimtevaarttechnologieën zijn de technologieën die benodigd zijn voor gebruik bij reizen en activiteiten buiten de atmosfeer van de aarde, voor doeleinden zoals satellietcommunicatie, ruimtevluchten of ruimteverkenning. Ruimtevaarttechnologie is een voorbeeld van een technologie waarvan voorzienbaar of voorstelbaar en daarmee aannemelijk is dat ongewenste overdracht van deze kennis en technologie grote risico's voor de nationale veiligheid kan opleveren. Tegenwoordig staat ruimtevaarttechnologie in toenemende mate centraal in geopolitieke conflicten. Hierdoor wordt ook wel gesproken van de 'actieve militarisering van de ruimte,' omdat ruimtevaarttechnologie steeds vaker wordt gebruikt voor militaire doeleinden. Door bijvoorbeeld gebruik te maken van in de ruimte gestationeerde systemen, zoals satellieten, voor onder andere het vergaren van inlichtingen of het onderscheppen van communicatie. Ruimtebewapening komt ook in toenemende mate voor, door bijvoorbeeld het plaatsen van apparatuur of technologie in de ruimte voor potentieel destructief gebruik.

Sensitieve (sub)technologieën

Voor onderstaande subtechnologieën is de toelichting op de sensitiviteit reeds gegeven in de vorige alinea. Launch vehicles zijn lanceervoertuigen (draagraketten) die een 'payload' (zoals satellieten, ruimtevaartuigen, of andere wetenschappelijke instrumenten) van de aarde naar de ruimte transporteren (vaak in een baan om de aarde).

Ruimtevaartuigen maken gebruik van ruimte-aandrijvingstechnologie. Het betreft voortstuwingstechnologieën - zowel chemisch als niet-chemisch van aard - die worden gebruikt in het vacuüm van de ruimte. Waar lanceervoertuigen verantwoordelijk zijn voor de initiële opstijging en het overwinnen van de aardse zwaartekracht, bieden ruimte-aandrijvingstechnologieën de voortstuwing die nodig is om de missie voort te zetten, bijvoorbeeld voor interplanetaire reizen of lange termijn operaties in de ruimte.

On-orbit servicing, assembly en manufacturing zijn belangrijke (enabling) technologieën die de mogelijkheid bieden om in de ruimte zelf werkzaamheden uit te voeren en de efficiëntie van ruimteverkenning te verbeteren. On-orbit servicing betreft het wijzigen of onderhouden van een ruimtevaartuig na de initiële lancering. Dit gebeurt door een ander ruimtevaartuig dat de nodige reparaties of vervangingen van onderdelen uitvoert, zoals het bijvullen van brandstof, het repareren van satellieten of het vervangen van defecte systemen, wat de levensduur en werking van ruimtevaartuigen kan verlengen.

On-orbit assembly verwijst naar het proces van het in de ruimte samenstellen van componenten om een ruimtevaartuig of subsysteem te creëren. Dit kan het in elkaar zetten van grote satellieten of de assemblage van een ruimtestation omvatten, waarbij de componenten vanaf de aarde met andere ruimtevaartuigen naar de ruimte worden gebracht en daar in de juiste configuratie worden samengevoegd.

On-orbit manufacturing is het proces van het omzetten van grondstoffen in bruikbare onderdelen in de ruimte zelf. Dit stelt ruimtevaartuigen in staat om onderdelen te maken

of reparaties uit te voeren zonder terug te hoeven keren naar de aarde, waardoor kosten en tijd bespaard kunnen worden. Voorbeelden zijn het 3D-printen van onderdelen of het vervaardigen van gereedschappen in de ruimte. Deze technieken hebben het potentieel om de kosten van ruimteverkenning aanzienlijk te verlagen, de levensduur van ruimtevaartuigen te verlengen en meer complexe missies uit te kunnen voeren.

Satellietbussen zijn het hoofdlichaam en de structurele componenten van de satelliet waarin zich de payload en andere componenten van de satelliet bevinden, zoals communicatiesystemen, power systems, telemetrie, temperatuurcontrole en houdingscontrole.

De definities gegeven voor positioning, navigation and timing (PNT) evenals communication and networking technologies zijn ook van toepassing binnen de ruimtevaarttechnologie. De desbetreffende uitleg staat onder de genoemde kopjes.

Remote sensing instruments worden gebruikt als payload voor satellieten, vaak in combinatie met of naast PNT en communicatietechnologieën. Dit zijn sensoren die verder weg de ruimte inkijken of de aarde observeren. Deze sensoren kunnen zowel actief (radar, lidar) als passief (imagers, spectrometers) zijn, en gebruiken delen van vrijwel het hele elektromagnetische spectrum.

Cryogene vloeistofbeheer (CFM) is het tot zeer lage temperatuur koelen van gassen die gebruikt worden voor voortstuwing. Door het koelen worden van de gassen vloeistoffen gemaakt die veel minder ruimte innemen.

Entry, descent and landing betreffen technologieën die het mogelijk maken om een atmosfeer binnen te gaan, hierin af te dalen en te landen, bijvoorbeeld bij Marsmissies of bij het terugkeren op aarde.

Kleine satellieten zijn lichtgewicht satellieten die goedkoper en sneller geproduceerd kunnen worden dan traditionele grotere satellieten. CubeSats zijn nanosatellieten met gestandaardiseerde afmetingen die gestapeld kunnen worden. Kleine, lichtgewicht satellieten zijn belangrijk voor bijvoorbeeld communicatietoepassingen, internetdiensten, aardobservatie en plaatsbepalingsdiensten.

Human spaceflight omvat technologieën voor menselijke ruimtevaart en is voornamelijk gericht op het gezond in leven houden van mensen in de ruimte, bijvoorbeeld via ruimtepakken of recycling technologie, en om te zorgen dat astronauten effectief werk en onderzoek kunnen doen in de ruimte.

Sensortechnologieën

Het technologiegebied sensing technologies betreft enerzijds de sensoren die grootheden kunnen meten en omzetten in een leesbaar signaal, en anderzijds verschillende methoden en technieken om deze signalen (automatisch) verder te verwerken en/of aan een menselijke gebruiker aan te bieden. Er bestaan tientallen soorten grootheden en voor iedere grootheid zijn er typisch meerdere soorten sensoren. Veel andere technologiegebieden maken direct gebruik van sensing technologies.

Een deel van de sensortechnologieën wordt specifiek ontwikkeld voor militaire toepassingen, of heeft een duidelijk dual use karakter. Sensoren kunnen gebruikt worden voor het nauwkeuriger, betrouwbaarder en efficiënter uitvoeren van metingen. Praktische voorbeelden variëren van betere navigatiesystemen tot medische detectieapparatuur, en ook radars voor metingen op zee. Sensortechnologie is dus een breed technologiegebied dat een belangrijke rol speelt in andere technologiegebieden en met veel toepassingen in het defensie- en veiligheidsdomein, alsmede in vitale processen en is daarom als sensitief aangewezen.

Sensitieve (sub)technologieën

Onder specifieke sensortechnologieën vallen onder andere akoestische sensoren, Sonar en Radar. Akoestische sensoren detecteren passief de aanwezigheid van geluid, waarna dit wordt gebruikt om een apparaat te activeren. Sonartechnologie maakt gebruik van geluid om (onder water) te navigeren of om voorwerpen te detecteren. Radar betreft een (actief) object-detectiesysteem dat radiogolven gebruikt om objecten op bepaalde afstanden op te sporen, te volgen, te lokaliseren en te identificeren.

Onder sensor fusion and array technologies vallen combinaties van sensoren welke nauwkeuriger, sneller of meerdere signalen tegelijkertijd kunnen registreren. Denk aan een kleurencamera die zowel lichtsterkte als lichtfrequentie (kleur) meet. Daarmee registreert deze sensor een raster van signalen, d.w.z. een 2-dimensionaal beeld. Ook microfoon- of sonararrays om in een bepaalde richting geluid beter te kunnen onderscheiden vallen hieronder.

Data fusion omvat de technologieën die signalen van verschillende soorten sensoren kunnen combineren in één (analyse)instrument waar het mogelijk wordt om gebeurtenissen en attributen van objecten in de fysieke wereld beter te onderscheiden en bemonsteren.

Signature management and pattern recognition betreft technologieën voor het voorspellen, meten en mitigeren van meer of minder unieke patronen van objecten of gebeurtenissen. Denk bijvoorbeeld aan uitgezonden signaturen van militaire platforms (zowel infrarood, (elektro-) magnetisch, druk, als akoestisch) en kenteken- of gezichtsherkenning en het ontduiken daarvan.

Sensornetwerken en omgevingstechnologieën omvatten een groep sensoren waarbij elke sensor gegevens op een andere locatie bewaart en (een relevant deel van) die gegevens naar een centrale locatie verzendt voor verdere opslag, weergave en analyse. Domotica systemen voor thuisautomatisering zijn een voorbeeld van een sensornetwerk. Ook wordt vitale infrastructuur, zoals een wegennet of een spoornet, typisch gemonitord met behulp van gespecialiseerde soorten sensornetwerken.

LiDAR (Light Detection and Ranging) is een technologie die laserlicht en LiDAR-sensoren gebruikt om afstanden te meten en gedetailleerde 3D-kaarten van omgevingen te maken. Het werkt door een laserpuls uit te zenden, de reflectie van dat licht te meten en de tijd te analyseren die het kost voor het licht om terug te keren. LiDAR wordt vaak gebruikt in toepassingen zoals autonome voertuigen, topografische mapping, bosbeheer en archeologie vanwege de nauwkeurigheid en het vermogen om complexe, moeilijk bereikbare gebieden in kaart te brengen.

IR (Infrarood) en UV (Ultraviolet) sensoren zijn apparaten die respectievelijk infrarood- en ultravioletstraling detecteren, die buiten het zichtbare lichtspectrum liggen. IR-sensoren worden vaak gebruikt voor warmtebeeldvorming, nachtzichttoepassingen en afstandsmeting, omdat ze warmte of temperatuurverschillen kunnen detecteren. UV-sensoren worden gebruikt voor toepassingen zoals het detecteren van zonlichtintensiteit en het monitoren van de luchtkwaliteit.

Simulatie technologie

Simulatietechnologie is een verzamelnaam voor technologieën waarmee aspecten van de werkelijkheid in een digitale omgeving worden nagebootst. De technologie is vrij generiek, maar kan niet helemaal los worden gezien van de data die gebruikt wordt om specifieke toepassingen te ontwikkelen. Veelal worden simulatietechnologieën gebruikt om te modelleren, simuleren en/of transformeren. Op deze wijze worden elementen uit

de dagelijkse wereld gebruikt om voorspellingen te doen over toekomstige situaties. In beide gevallen zijn toepassingen in specifieke contexten (bijvoorbeeld in militaire context) risicovol omdat daardoor gevoelige informatie over de toepassingscontext evenals politie- en militaire data kan weglekken die gebruikt wordt om het model te voeden.

Sensitieve (sub)technologieën

Digital twinning technologies zijn digitale replica's van een entiteit zoals een object, proces of systeem. Met sensoren wordt data uit de echte wereld gecombineerd met bestaande modellen met daarin bekende wetenschappelijk onderbouwde kennis. Het is dus geavanceerde digitalisatie waarin data, model en doel worden gecombineerd tot een digitale verzameling van kennis die zich actualiseert op basis van de werkelijkheid.

Extended Reality (XR) is een paraplubegrip dat refereert naar echte (fysieke) en virtuele omgevingen gegenereerd door computertechnologie en *wearables* om een gepersonaliseerde en *immersive* ervaring te creëren. Er zijn verschillende technologieën die onder de noemer Extended Reality vallen. Virtual Reality (VR) is technologie die immersie in een synthetische wereld mogelijk maakt. De fysieke wereld wordt daarbij niet meer gezien. Augmented Reality (AR) is technologie waarin 'echte' en door computer-gegenereerde 'virtuele' elementen worden gecombineerd in een blik op de fysieke wereld. In dit geval wordt AR informatie als een semi-transparante laag over de fysieke wereld geprojecteerd. Mixed Reality (MR) is technologie waarin aspecten van VR en AR met elkaar worden gecombineerd. Het refereert aan alle varianten in de *reality-virtuality* continuüm, met uitzondering van de AR en VR extremen. Deze technologie creëert een nieuwe mixed reality wereld waarin de fysieke wereld en virtuele wereld samen komen. Bijzonder van MR is dat de gebruiker tegelijkertijd kan interacteren met zowel de echte als virtuele omgeving.