Reactie TO2-organisaties op voorstel Wet screening kennisveiligheid

TO2 federatie
De samenwerkende organisaties in toegepast onderzoek

27 juni 2025

Met belangstelling hebben wij kennisgenomen van het voorstel Wet screening kennisveiligheid zoals dat voor consultatie is gepubliceerd. De vijf TO2-instellingen (Deltares, MARIN, NLR, TNO, Wageningen Research) onderschrijven het belang van het beschermen van gevoelige kennis en technologieën waar het gaat om onze nationale veiligheid. Drie instellingen hebben op dat gebied ook een jarenlange staat van dienst in het defensieonderzoek. Tegelijkertijd zal invoering van de Wet screening kennisveiligheid in zijn huidige vorm aanzienlijke gevolgen hebben voor onze organisaties. In deze reactie maken wij onze zorgen, overdenkingen en vragen in relatie tot de wettekst kenbaar.

1. Ongelijk speelveld en schijnveiligheid

De voorgestelde wetgeving creëert een ongelijk speelveld. Onderzoekers die niet door de screening komen, kunnen zonder belemmering elders in Nederland bij een privaat bedrijf of binnen Europa bij een onderwijs- of kennisinstelling aan de slag in hetzelfde kennisgebied. Ook vestigingen van buitenlandse onderzoeksinstellingen in Nederland, zoals Fraunhofer en Imec, vallen buiten deze wet. In de praktijk betekent dit dat met name TO2-instellingen, die sterk gericht zijn op samenwerking met bedrijven en internationale kennisinstellingen, deze onderzoekers opnieuw kunnen tegenkomen in gezamenlijke projecten, consortia of publiek-private samenwerkingen.

De wet houdt onvoldoende rekening met deze realiteit[1]. Samenwerking met externe partijen is een structureel onderdeel van het Nederlandse kennisecosysteem. Tegelijkertijd gelden de eisen in deze wet niet voor private bedrijven en Europese kennisinstellingen. Hierdoor ontstaat een situatie waarin instellingen wél verantwoordelijk zijn voor het beschermen van gevoelige kennis, maar geen mogelijkheden hebben om dit effectief te doen zodra samenwerking buiten de eigen organisatie plaatsvindt.

Hiermee ontstaat een risico op schijnveiligheid: de toegang tot gevoelige kennis wordt formeel beperkt, maar in de praktijk blijft het risico van het weglekken van gevoelige informatie bestaan, juist op de plekken waar samenwerking essentieel is.

2. Sensitiviteitstoetsing

Volgens de huidige inschatting wordt uitgegaan van 8000 screenings per jaar voor alle instellingen[2]. Daarbij is verondersteld dat de lijst met sensitieve kennis- en technologiegebieden voldoende werkbaar is om instellingen in staat te stellen gericht

[1] Dit in tegenstelling tot de Wet veiligheidsonderzoeken, die ook van toepassing is op private organisaties.

[2] Bij dat aantal zetten wij vraagtekens in het licht dat alleen al TNO een schatting van ongeveer 1000 aanvragen per jaar heeft gemaakt (zie paragraaf 5).

hoogrisico-onderdelen aan te wijzen. Er zijn echter drie fundamentele knelpunten die een effectieve uitvoering in de weg staan:

Onduidelijke criteria
De criteria voor sensitiviteit (artikel 5 in de wet) maken het aanwijzen van risicovakgebieden eerder complexer dan concreter. In plaats van houvast te bieden, vergroten ze de interpretatieruimte en daarmee de onzekerheid bij instellingen. Gezien de breedte van technologieën waarvan defensie, opsporings-, inlichtingen en veiligheidsdiensten bij de uitoefening van hun taken gebruik maken, zou bijna elke technologie op basis van een dergelijk criterium als sensitief kunnen worden aangemerkt (en dat is in brede lijst in bijlage 2 van het wetsvoorstel ook zichtbaar). Dit heeft vooral te maken met de voorstelbaarheid en voorspelbaarheid wat zwaarwegend is in de aanwijzing. In de eerdere feedbackrondes op de lijst met sensitieve kennis- en technologiegebieden is al gebleken dat een mogelijke risicovolle toepassing al snel voorstelbaar is en dat de technologie een bijdrage kan leveren aan risico's voor de nationale veiligheid. Op basis van de voorstelbaarheid is de verwachting dat instellingen voor de zekerheid de betreffende onderzoeksgroep of het vakgebied aanwijzen als hoogrisico-onderdeel, ongeacht de voorspelbaarheid. Dit resulteert in buitenproportionaliteit.

Reikwijdte en interpretatie
De lijst met sensitieve kennis- en technologiegebieden (bijlage 2 in het wetsvoorstel) is te breed. Hoewel de lijst naar aanleiding van eerdere feedbackrondes inhoudelijk is aangescherpt - met verbeterde definities en aanvullende voorbeelden waar experts zich over het algemeen in kunnen vinden - zijn de definities ruim geformuleerd en laten veel ruimte voor interpretatie. Hierdoor wordt het voor instellingen lastig om met precisie te bepalen welke onderdelen daadwerkelijk onder de screeningplicht vallen. In veel gevallen is niet de kennis zelf, maar de toepassing ervan bepalend voor de mate van sensitiviteit. Dat leidt tot een grijs gebied waarin instellingen zelf moeten inschatten of een kennisgebied onder de wet valt, met als gevolg een verhoogd risico op uiteenlopende interpretaties en onbedoelde overtredingen.

Actualiteit
De lijst met sensitieve kennisgebieden die in deze wet is opgenomen is statisch, terwijl technologische ontwikkelingen zich in hoog tempo en op dynamische wijze voltrekken. Innovaties binnen kennisintensieve domeinen veranderen voortdurend van aard, reikwijdte en gevoeligheid. De ervaring met de totstandkoming van de lijst - inclusief twee feedbackrondes - heeft al aangetoond hoe snel de inschatting van wat als sensitief wordt beschouwd, kan verschuiven. In de wet wordt daarom de mogelijkheid voorzien om via een algemene maatregel van bestuur aanvullingen op de lijst vast te leggen. Dat komt de actualiteit van de lijst ten goede, maar roept de vraag op waarom niet gelijk de hele lijst via een algemene maatregel van bestuur wordt vastgelegd. Dit biedt meer flexibiliteit en een doelmatige mogelijkheid om de lijst continu te actualiseren en langdurige wetswijzigingsprocedures te voorkomen.

3. Uitvoerbaarheid

Er bestaan serieuze zorgen over de uitvoerbaarheid van het wetsvoorstel. Cruciale onderdelen ontbreken nog - zoals het beoordelingskader en de nadere regels voor het aanwijzen van hoogrisico-onderdelen - en zullen pas op een later moment via ministeriële regelingen worden vastgesteld. Het gebrek aan duidelijkheid maakt het voor kennisinstellingen niet mogelijk om zich tijdig en adequaat voor te bereiden. Voor een werkbare implementatie is het essentieel dat instellingen ruim vóór inwerkingtreding beschikken over alle noodzakelijke informatie om interne processen zorgvuldig aan te passen. Daarnaast zijn de volgende randvoorwaarden van groot belang.

Versnelling van doorlooptijd
De voorgestelde termijn van vier weken voor een kennisveiligheidsscreening is te lang. In een onderzoeksomgeving waar snelheid en flexibiliteit cruciaal zijn, belemmert dit de voortgang van projecten en de inzet van personeel. De TO2-instellingen hebben eerder gepleit voor een maximale doorlooptijd van twee weken, een termijn die recht doet aan de dynamiek van de sector.

Transparantie in toetsing en besluitvorming
Er is onvoldoende duidelijkheid over de toetsingscriteria, de terugkijktermijn en het proces bij een eventuele afwijzing van een kandidaat. Ook moeten instellingen en screeningplichtigen kunnen vertrouwen op een transparante, navolgbare procedure en directe communicatie met de uitvoeringsinstantie (een afwijzing in de screening moet ook juridisch kunnen standhouden in een eventuele procedure die de screeningplichtige aanspant). Op deze manier kan ook worden voorkomen dat een persoon wordt geselecteerd voor wie de instelling zelf al een inschatting kan maken dat er een groot risico bestaat dat deze niet door de screening heen komt. Deze basisvoorwaarden zijn op dit moment niet geborgd.

Eenduidige afbakening
De definitie van een hoogrisico-onderdeel is niet duidelijk opgenomen in de wettekst. Het is voor de TO2-instellingen onduidelijk of Defensie-gerelateerde onderdelen onder de screeningsplicht vallen. Deze onduidelijkheid kan leiden tot verwarring over verantwoordelijkheden, risico op dubbele regelgeving en overlap in toezicht[3]. Een heldere definitie en afbakening zijn noodzakelijk om dit te voorkomen. Net als medewerkers in het bezit van een geldige Verklaring Geen Bezwaar (VGB) worden uitgezonderd van de screening kennisveiligheid, pleiten we voor een soortgelijke uitzonderingsbepaling voor onderdelen specifiek gericht op defensieonderzoek, die reeds onder toezicht van het Ministerie van Defensie vallen.

Ook wordt onvoldoende duidelijk wat als technisch ondersteunend personeel wordt gekwalificeerd. Vermoedelijk gaat het hierbij om facilitaire diensten, maar het is niet duidelijk of ook interne ondersteunende afdelingen voor communicatie, export control, compliance, intellectueel eigendom , alsmede externe technische dienstverleners die op locaties onderhouds- en (ver)bouwwerkzaamheden verrichten hieronder vallen.

[3] Zie ook paragraaf 4

4. Toezicht en informatiepositie

De Inspectie van het Onderwijs wordt mogelijk betrokken bij toezicht en handhaving op de naleving van screenings en de juiste vaststelling van risicovakgebieden. Waar dat voor onderwijsinstellingen die onder OCW vallen een begrijpelijke keuze is, ligt die keuze voor de andere instellingen zoals genoemd in bijlage 1 van het wetsvoorstel niet voor de hand. De TO2-instellingen (met uitzondering van Wageningen) hebben geen toezichtrelatie met de Inspectie van het Onderwijs noch met het Ministerie van OCW. Een aantal TO2-instellingen heeft voor defensieonderzoek wel een toezichtrelatie op het gebied van veiligheid met Defensie (MIVD). Hoe deze toezichtrelaties zich tot elkaar verhouden, is onduidelijk. De hierboven bepleite uitzonderingspositie voor onderdelen die onder dit toezicht vallen, kan hier uitkomst bieden.

Gerelateerd hieraan zijn er ook zorgen over de informatie- en meldplicht die instellingen krijgen. Ook niet-hoogrisico-onderdelen moeten worden gemeld voor het uitvoeren van de juiste vaststelling, wat leidt tot ongewenst delen van vertrouwelijke en mogelijk staatsgeheime informatie. Hoe gaat dit worden gedeeld en opgeslagen, wie hebben daar toegang tot? Dit is niet wenselijk en het is daarom de vraag hoe andere betrokken ministeries en instanties aankijken tegen deze informatieplicht. Dit vraagt om een afwegings- en indieningskader om de eigen informatiepositie en die van betrokken partijen te beschermen.

5. Administratieve lastendruk

De invoering van de Wet screening kennisveiligheid brengt een aanzienlijke toename in het aantal screenings met zich mee, bovenop de grote aantallen screenings die nu al plaatsvinden bij de TO2-instellingen voor het verkrijgen van een Verklaring van Geen Bezwaar (VGB) voor een vertrouwensfunctie of een Verklaring Omtrent Gedrag (VOG) voor een andere functie. Zo zijn er bij TNO circa 3000 medewerkers en bij MARIN circa 200 medewerkers in het bezit van een VGB, waarvoor de kennisveiligheid-screening volgens dit wetsvoorstel niet van toepassing is. Echter, voor alle overige nieuwe medewerkers — inclusief technisch ondersteunend personeel dat in aanraking kan komen met gevoelige kennis of technologie — zal naar verwachting een kennisveiligheidscreening vereist zijn. Of huidig personeel dat overstapt naar een ander sensitief kennisgebied.

Dit zal voor TNO en MARIN leiden tot naar verwachting 1000 respectievelijk 100 extra screeningaanvragen kennisveiligheid per jaar (gemiddeld). Voor TNO is deze inschatting gebaseerd op de veronderstelling dat, op basis van de huidige lijst sensitieve kennis- en technologiegebieden, vrijwel al het onderzoekswerk binnen TNO als sensitief moet worden aangemerkt. De toegang tot gevoelige kennis strekt zich immers uit tot medewerkers binnen het vakgebied, ondersteunend personeel én samenwerkingen met andere afdelingen en onderzoeksgroepen.

Naast de screeningaanvragen worden instellingen ook geconfronteerd met de noodzaak om ontwikkelingen te monitoren, hoogrisico-onderdelen te bepalen, deze beoordelingen periodiek te herhalen en een informatie- en meldplicht bij het Ministerie van OCW. Dit

zorgt al met al voor een aanzienlijke toename van de administratieve lastendruk, zonder dat daar ondersteuning of compensatie tegenover staat.

Parallel aan de invoering van de Wet screening kennisveiligheid worden de TO2-instellingen ook geconfronteerd met de overgang van de Algemene Beveiligingseisen Defensie Opdrachten (ABDO) naar de Algemene Beveiligingseisen Rijksopdrachten (ABRO). Ook deze nieuwe regelgeving is gericht tegen risico's voor nationale veiligheid. Wij roepen de verschillende verantwoordelijke ministeries op de samenhang tussen en een doelmatige uitvoering van beide trajecten te bewaken.