Rijksdienst voor Ondernemend
Nederland

Inventarisatie expertise- en adviesloket kennisveiligheid

16 juli 2021

In opdracht van het ministerie van Onderwijs Cultuur en Wetenschap

Inventarisatie expertise- en adviesloket kennisveiligheid

16 juli 2021

Managementsamenvatting

Opdracht
OCW heeft RVO gevraagd een kortlopende uitvraag (“quick-scan”) voor een expertise- en adviesloket kennisveiligheid te doen, bestaande uit een inventarisatie van de behoeften en wensen van het Nederlandse kennisveld ten behoeve van het opzetten van een expertise- en adviesloket kennisveiligheid. Het Nederlandse kennisveld beslaat in dit onderzoek de Nederlandse hogescholen, universiteiten, UMC’s, (onderzoeks) instituten NWO en KNAW en de TO2-instellingen (Deltares, Marin, NLR, TNO en Wageningen Research).

Thema’s
Thema’s rondom kennisveiligheid waarbij de sterkste behoefte aan meedenken vanuit de Rijksoverheid bestaat:

1. IT-gerelateerd / cyber
2. Aangaan onderzoekssamenwerkingen met buitenlandse kennisinstellingen
3. Toelating van buitenlandse promovendi en/of onderzoekers
4. Omgang met buitenlandse studenten/onderzoekers i.r.t. ongewenste kennisoverdracht en/of ongewenste buitenlandse inmenging
5. Intellectueel eigendom / patenten

Randvoorwaarden
Onderstaande aanbevelingen komen voort uit de uitkomsten van de online enquête onder de kennisinstellingen en de diepte interviews met relevante personen in het veld. Het expertise- en adviesloket kennisveiligheid moet volgens de respondenten aan de volgende randvoorwaarden voldoen om meerwaarde te creëren:

1. **Algemene informatie** bieden over kennisveiligheidsrisico’s.
2. **Specifieke informatie bieden over bepaalde derde landen, hun strategische doelen, wet-en regelgeving, maar ook over gevoelige vakgebieden**. Bijvoorbeeld in de vorm van een database/ dashboards met informatie/ risicoprofiel van beoogd partner (kennisinstelling, bedrijf).
3. Antwoorden geven op **praktische vragen**. Bijvoorbeeld over welke informatie er in internationale overeenkomsten moet staan en wat zeker niet, maar ook over welke samenwerkingskansen er liggen in kennisveiligheidsgevoelige regio’s. Daarbij merken meerdere respondenten op dat er ‘echte’ experts moeten zitten die integraal antwoord geven op deze vragen over derde landen.
4. **Sparren over ‘twijfelgevallen’** voor samenwerking. Het voorleggen van dilemma’s.
5. Een duidelijk advies, dat al door een medewerker van het expertise- en adviesloket is **afgestemd met de verschillende ministeries**. Hierin wordt dus echt een samenwerking van ministeries en andere relevante partijen op het gebied van kennisveiligheid verwacht.
6. Een onafhankelijke en vrijblijvende **screening op studenten en medewerkers** aanbieden, maar ook op (bestaande) **samenwerkingsovereenkomsten met instellingen** uit derde landen. Bijvoorbeeld op het gebied van de herkomst van financiering.
7. Duidelijke en handelbare **nationale richtlijnen** over welke landen, onderwerpen en/of instellingen zich juist wel of niet lenen voor samenwerking. Begeleid door een open afwegingskader / stappenplan. Het doel is dat kennisinstellingen hetzelfde besluit kunnen nemen met dezelfde informatie die ze van buitenaf krijgen, zodat partijen uit derde landen geen ‘shop’ kansen langs verschillende kennisinstellingen krijgen.
8. Advies over **juridische zaken**.
9. Advies over (ICT) **maatregelen bij werkbezoeken** naar bepaalde derde landen.
10. **Bewustwording** over kennisveiligheid creëren / voorlichtingsfunctie bij kennisinstellingen.
11. **Netwerkfunctie** voor specifieke (deel)gebieden en/of thema’s.

No-go’s
Kritische geluiden tijdens de interviews en in de enquête waren in veel gevallen waarschuwingen over hoe een expertise- en adviesloket pertinent niet zou moeten functioneren. De respondenten waarschuwden:

- Het expertise- en adviesloket moet *geen* loket worden waar projecten ‘gecheckt’ worden om een goedkeuringsstempel te krijgen. Een soort van APK-keuring voor projecten verplicht langs moeten.
- Het expertise- en adviesloket moet *geen* extra administratieve last zijn. Een advies moet afgestemd richting de vraagsteller gaan.
- In het expertise- en adviesloket moet een advies *niet* maanden op zich laten wachten. Wetenschappers, maar ook kennisinstellingen werken onder tijdsdruk en hebben op redelijke termijn advies nodig om weer verder te kunnen met een project.

Contactmogelijkheden
De voorkeur voor contactmogelijkheden blijkt volgens de respondenten af te hangen van de aard van de vraag. In de praktijk is dus zowel behoefte aan een website met praktische informatie als aan een-op-een contact met een medewerker.

Leren van elkaar
Uit de diepte interviews bleek dat zowel binnen Nederland als in EU/internationaal verband al bij verschillende organisaties wordt nagedacht over een expertise- en adviesloket kennisveiligheid.

Aanbevelingen inrichting expertise- en adviesloket kennisveiligheid

In dit onderzoek vond een inventarisatie plaats van de behoeften en wensen van het Nederlandse kennisveld voor een expertise- en adviesloket kennisveiligheid. Onderstaande aanbevelingen komen voort uit de uitkomsten van de online enquête onder de kennisinstellingen en de diepte interviews met relevante personen in het veld en zijn verdeeld in aanbevelingen op het gebied van structuur en inhoud van het loket, de technische vereisten, het creëren van draagvlak en het lerend vermogen.

Structuur en inhoud

1. **Bied een combinatie van 'snelle' praktische informatie en informatie door deskundige medewerkers die inhoudelijk meedenken**
   Algemene richtlijnen over samenwerking met derde landen, een lijst met aandachtspunten en thematiek met mogelijke risico's zijn noodzakelijk. Daarnaast klinkt ook duidelijk de roep om meedenkende en inhoudelijk sterke adviseurs die een sparringspartner kunnen zijn om dilemma's rondom kennisveiligheid te bespreken (en informatie bij verschillende instanties ophalen om tot een advies te komen). Het loket moet dus niet enkel een doorverwijsfunctie krijgen, maar ook een serieuze gesprekspartner zijn.

2. **Benadruk de variëteit aan landen in het expertise- en adviesloket**
   Hoewel alle respondenten minimaal informatie over China wilden terugzien in het expertise- en adviesloket kennisveiligheid, gaf een groot deel van de respondenten ook aan behoefte te hebben aan informatie over Rusland, Iran en de VS. Het is dus in de communicatie van belang te benadrukken dat het loket ondersteuning biedt bij vragen over verschillende derde landen.

3. **Blijf oog houden voor de reikwijdte aan thema's rondom kennisveiligheid**
   De top-5 thema's waarbij meedenken vanuit de Rijksoverheid gewenst is, laat een breed spectrum aan onderwerpen zien. Het expertise- en adviesloket kennisveiligheid moet dus advies en informatie bieden op al deze vlakken om een solide positie op het gebied van kennisveiligheid te kunnen creëren.

Technische vereisten

4. **Begin met een eenvoudige, maar duidelijke website voor het expertise- en adviesloket**
   In de keuze voor platforms waarop de website van het expertise- en adviesloket kennisveiligheid kan draaien zijn verschillende mogelijkheden. Van professioneel beveiligde, met maatwerk ontwikkeld platforms tot eenvoudige, snel te realiseren platforms. Bij de Rijksoverheid, maar ook bij RVO ligt veel expertise op het gebied van platformmanagement. Wij raden dan ook aan om een studie uit te laten voeren naar het meest geschikte platform voor het loket. Vanuit het oogpunt van tijd- en kostenefficiëntie, en de huidige behoeften vanuit het veld, zou onze voorkeur op het moment uitgaan naar een snel te realiseren, eenvoudige variant. Mochten meer geavanceerde (beveiligings)opties nodig worden geacht, kan later altijd nog opgeschaald worden naar een maatwerk optie.

5. **Zorg voor een snelle en adequate vraagafhandeling (max. een week)**
   De meeste respondenten geven aan dat een week een redelijke termijn van beantwoording vormt. Om relevantie in het veld te houden en welwillendheid te kweken, raden wij aan deze termijn te volgen.

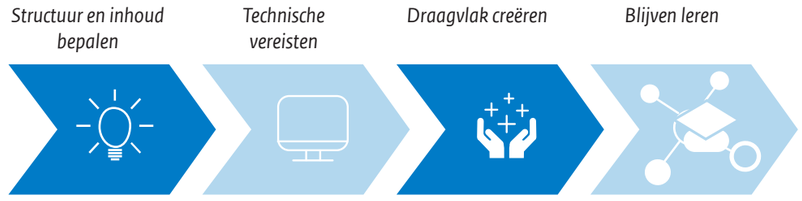
Het creëren en behouden van draagvlak

6. **Houd informatie te allen tijde up-to-date**
   Het thema van kennisveiligheid leeft sterk binnen het veld. Uit de enquête en interviews bleek ook de behoefte aan informatie op het thema. Het is van belang om dit momentum te benutten, maar het is net zo goed van belang dat het goed gebeurt. We kregen van respondenten de waarschuwing mee dat de informatie en richtlijnen op een website altijd up-to-date moet zijn. Bijvoorbeeld actief communiceren als er nieuwe beleidsinformatie of richtlijnen over een bepaalde derde land uitkomen. Anders kijken wetenschappers een keer, maar daarna niet meer, was de vrees vanuit het veld.

7. **Werk actief aan de beeldvorming van het loket / maak een duidelijk communicatieplan**
   De beeldvorming is van essentieel belang voor het succes van het expertise- en adviesloket. In de interviews merkten we in sommige gevallen nog weerstand ten aanzien van het loket. Mogelijk kan deze door juiste informatie weggenomen worden. Ook werden door respondenten seminars en webinars genoemd om medewerkers bekend te maken met het loket en het gebruikerspercentage omhoog te brengen.

Lerend vermogen

8. **Leer van elkaar en haak aan op bestaande initiatieven in binnen -en buitenland**
   Uit de interviews blijkt dat op het moment veel organisaties en overheden in binnen-en buitenland zich bezig houden met het thema van kennisveiligheid, ook in relatie tot informatiepunten. Wij raden dan ook aan om parallel aan de inrichting van het expertise- en adviesloket, nog een gedetailleerde studie te doen naar andere initiatieven en de tips en tops hiervan mee te nemen in de inrichting van het loket. Ook is het van belang om aangehaakt te blijven bij Brussel en de aanpak van andere EU-lidstaten.



Inhoudsopgave

1

Aanleiding, opdracht en aanpak

Aanleiding

In de Kamerbrief kennisveiligheid hoger onderwijs en wetenschap van november 2020[1] zijn verschillende maatregelen aangekondigd om de kennisveiligheid in het hoger onderwijs en de (toegepaste) wetenschap beter te borgen. De voorgestelde maatregelen beogen het bewustzijn over kennisveiligheid onder de betrokkenen te vergroten en te zorgen dat het veiligheidsbeleid binnen de instellingen nadrukkelijker vorm krijgt.

Een van de aangekondigde beleidsmaatregelen om de weerbaarheid van Nederlandse universiteiten, hogescholen en onderzoeksinstituten tegen kennisveiligheidsrisico's te verhogen, is de inrichting van een expertise- en adviesloket kennisveiligheid. Doel van dit loket is om hulp te bieden aan de mensen binnen kennisinstellingen die aan kennisveiligheid gerelateerde vragen hebben.

Hoewel het nu reeds mogelijk is voor kennisinstellingen om bij relevante onderdelen van de overheid advies en informatie in te winnen, is er behoefte aan één centraal punt waar instellingen terecht kunnen met vragen en waar zij advies krijgen dat ze kunnen gebruiken bij het maken van de afweging. OCW gaat daarbij uit van een opzet met een frontoffice (het eigenlijke loket) en een backoffice (gevormd door -bestaande- onderdelen van de rijksoverheid met relevante expertise).

Voordat dit loket ingericht kan worden, is het van belang om een beeld te krijgen van de behoeften en wensen van het Nederlandse kennisveld voor een expertise- en adviesloket kennisveiligheid. Het Nederlandse kennisveld beslaat in dit onderzoek de Nederlandse hogescholen, universiteiten, UMC's, (onderzoeks) instituten NWO en KNAW en de TO2-instellingen (Deltares, Marin, NLR, TNO en Wageningen Research).

Opdracht

OCW heeft RVO gevraagd om een kortlopende uitvraag ("quick-scan") voor dit loket te doen, bestaande uit een inventarisatie van de behoeften en wensen van het Nederlandse kennisveld en aanbevelingen ten behoeve van het opzetten van een expertise- en adviesloket kennisveiligheid.

Definitie kennisveiligheid
Bij kennisveiligheid gaat het in de kamerbrief in de eerste plaats om het voorkomen van ongewenste overdracht van (sensitieve) kennis en technologie, met negatieve gevolgen voor de nationale veiligheid van ons land en aantasting van de Nederlandse innovatiekracht. Daarnaast gaat het ook om heimelijke beïnvloeding van hoger onderwijs en wetenschap door statelijke actoren, die o.a. kan leiden tot vormen van (zelf)censuur met aantasting van de academische vrijheid tot gevolg. Tot slot draait het bij kennisveiligheid om ethische kwesties die kunnen samenhangen met samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd.

1 https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/27/kennisveiligheid-hoger-onderwijs-en-wetenschap

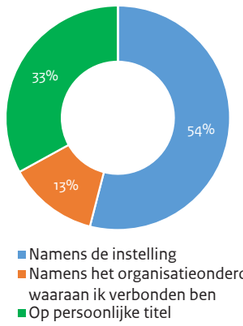
Aanpak

De resultaten van deze quick-scan zijn gebaseerd op een online enquête binnen het Nederlandse kennisveld (vragenlijst in Bijlage A), diepte interviews met relevante personen binnen de kennisinstellingen, VSNU en NWO, Innovatie Attachés uit een aantal landen (zie 'over RVO' voor de relatie van de Innovatie Attachés met het thema kennisveiligheid) en een werksessie met de TO-2 instellingen.

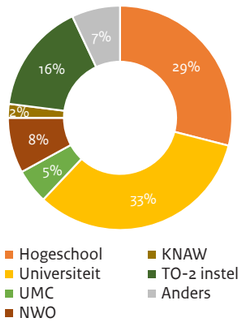
De online enquête stond open van 8 -21 juni 2021. In deze periode hebben 52 respondenten de enquête ingevuld. Uit de enquête blijkt een afspiegeling van verschillende type kennisinstellingen en functies van de respondenten (zie figuur 1). Respondenten op persoonlijke titel hebben ook hun persoonlijke ervaringen ingevuld (en niet noodzakelijke die van de instelling als geheel).

Fig. 1. Algemene informatie respondenten

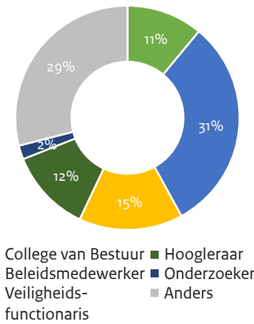
Namens wie is de enquete ingevuld



Type kennisinstelling waar de respondent werkzaam is



Functie van de respondenten binnen de kennisinstelling



In dezelfde periode zijn in totaal acht diepte interviews afgenomen met de hierboven genoemde instellingen en personen.

Het onderzoek is anoniem. Namen van kennisinstellingen of betrokkenen komen daarom niet voor in dit rapport. Om herkenbaarheid te voorkomen wordt in dit onderzoek 'hij' geschreven, ook als er eventueel met vrouwelijke contactpersonen gesproken is.

Over RVO

De Rijksdienst voor Ondernemend Nederland (RVO) voert opdrachten uit die ondernemende Nederlanders en beleidsmedewerkers vooruithelpen op het gebied van duurzaamheid, zakendoen over de grenzen, agrarisch ondernemen en innovatie, zowel binnen Nederland als daarbuiten. Om dit te realiseren, is RVO partner van Nederlandse en internationale kennisinstellingen, MKB, topsectoren en R&D.

RVO heeft ruime ervaring met rapportages, onderzoeken én de inrichting van loketten. In 2019-2020 is binnen de directie Internationale Programma's het onderzoek 'Verkenning wetenschappelijke samenwerking Nederlandse en Chinese kennisinstellingen' uitgevoerd. Aanbevelingen uit dit rapport komen terug in de Kamerbrief kennisveiligheid hoger onderwijs en wetenschap van november 2020.

Deze quick-scan is ondergebracht bij Team IRIS, een team binnen de afdeling Internationaal Innoveren dat zich voornamelijk bezighoudt met het adviseren van bedrijven en kennisinstellingen, bijvoorbeeld universiteiten, hogescholen en onderzoeksinstituten, over Europese fondsen als Horizon Europe en Eurostars/ Eureka. Hierdoor bestaat er een uitgebreid netwerk met Nederlandse kennisinstellingen binnen Team IRIS en zijn de adviseurs altijd op de hoogte over wat er in het veld speelt. Team IRIS heeft in 2020, aan het begin van Covid-19 crisis, meegewerkt aan de uitzondering op het inreisverbod voor onderzoekers van buiten de Europese Unie. Hierdoor bestaat er al kennis en ervaring over de omgang met onderzoekers uit derde landen.

Daarnaast werkt Team IRIS nauw samen met Innovatie Attachés (het IA-netwerk), die kansen signaleren voor R&D in het buitenland en helpen bij het maken van innovatieve matches tussen Nederland en derde landen. Het IA-netwerk is daarbij ook in contact met kennisinstellingen in het algemeen, zowel als met individuele hoogleraren en onderzoekers. De focus van het IA-netwerk ligt op maatschappelijke vraagstukken en sleuteltechnologieën, die relevant zijn voor regels rondom kennisdeling met bepaalde derde landen.

Leeswijzer

In Hoofdstuk 1 wordt de aanleiding, opdracht en aanpak besproken. In Hoofdstuk 2 wordt dieper ingegaan op de actuele dilemma's rondom kennisveiligheid die binnen de kennisinstellingen spelen, hoe het bewustzijn momenteel is en of informatie rondom kennisveiligheid binnen en buiten de kennisinstelling bereikbaar is. Hoofdstuk 3 richt zich op de rol van het adviesloket en inventariseert bij welke thema's meedenken van de overheid gewenst is bij de kennisinstellingen. Ook definieert het naar aanleiding van de opgehaalde data, de randvoorwaarden waar het loket aan moet voldoen en de reikwijdte. In Hoofdstuk 4 gaan we uit van de inrichting van een loket en halen we wensen en behoeften op rondom contactmogelijkheden, termijn van beantwoording en hoe het loket laagdrempelig gemaakt kan worden. In Hoofdstuk 5 staan de conclusies van het rapport. Als laatste volgen de Bijlagen.

2

Context thema kennisveiligheid

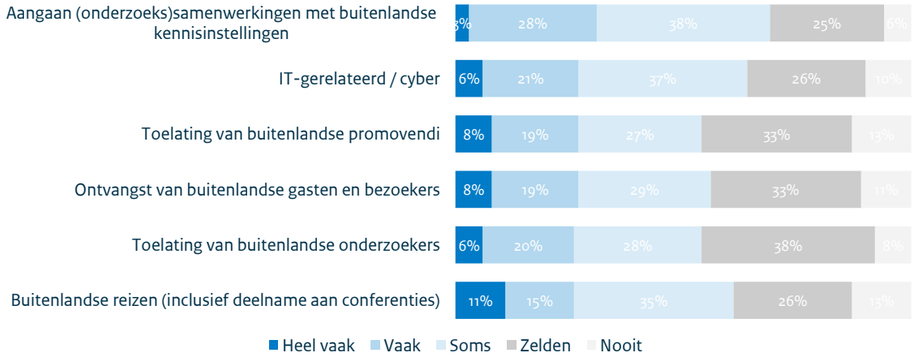
Actuele dilemma's rondom kennisveiligheid

Onderstaande lijst met dilemma's rondom kennisveiligheid geeft weer welke dilemma's momenteel binnen de kennisinstellingen spelen. Het geeft niet aan welke dilemma's volgens de kennisinstellingen in het expertise- en adviesloket zouden moeten komen. Dit komt later in het rapport aan de orde.

Uit de enquête komt naar voren dat de volgende dilemma's rondom kennisveiligheid in de grootste mate ("vaak" en "heel vaak" opgeteld) binnen de kennisinstellingen spelen (zie figuur 2):

1. Aangaan onderzoekssamenwerkingen met buitenlandse kennisinstellingen
2. IT gerelateerd – cyber
3. Toelating van buitenlandse promovendi en onderzoekers
4. Ontvangst van buitenlandse gasten en bezoekers
5. Buitenlandse reizen (inclusief deelname aan conferenties)

Fig. 2. Mate waarin bepaalde dilemma's rondom kennisveiligheid spelen binnen de kennisinstellingen (voor volledige grafiek, zie Bijlage B).

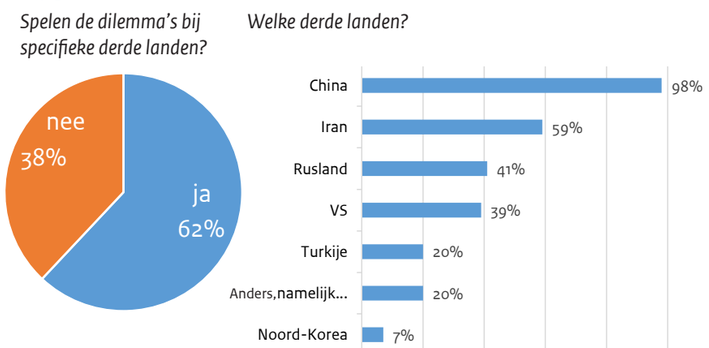


Landen waar kennisveiligheid een rol speelt

Van de 62% van de respondenten die aangeeft dat dilemma's rondom kennisveiligheid bij bepaalde derde landen voorkomen, heeft 98% minimaal China aangekruist.

China is dus een land waar dilemma's rondom kennisveiligheid volgens de respondenten vaker voorkomen dan in andere derde landen. Hierbij moet opgemerkt worden dat Iran, Rusland en de VS ook genoemd worden in dit kader. Andere derde landen die genoemd worden zijn: Saudi-Arabië, 'sommige Afrikaanse landen' (letterlijke verwoording van een respondent), Qatar, Indonesië, Israël, India, Pakistan en Irak.

Fig. 3. Landenvoorkeur



Kennis en bewustzijn binnen de kennisinstellingen

Uit de enquête blijkt dat respondenten verschillend denken over de vraag of ze het gevoel hebben dat risico's rondom kennisveiligheid binnen hun organisatie voldoende in beeld zijn.

> *"Er is geen duidelijke nationale richtlijn, dit leidt tot aarzelend formuleren van het intern beleid rondom kennisveiligheid."*

Een aantal respondenten geeft aan dat ze goed op de hoogte zijn van de risico's. Een respondent geeft ter nuance aan dat bewustzijn op bestuursniveau op orde is, maar dat dit niet het geval is bij wetenschappers. Dit beeld krijgen we ook terug uit een aantal diepte interviews; het niveau van de individuele wetenschappers op het gebied van kennisveiligheid schiet in sommige gevallen nog te kort. 'Daar is nog een wereld in te winnen', aldus een geïnterviewde.

> *"We handelen naar wat we weten maar we weten het niet precies."*

Aan de andere kant biedt een respondent uit de enquête een ander perspectief door juist te benadrukken dat kennis vaak decentraal belegd is en dat daardoor een totaaloverzicht ontbreekt.

Bereikbaarheid informatie

> *"Vragen over kennisveiligheid komen zelden aan bod bij onderzoeksprogrammering."*

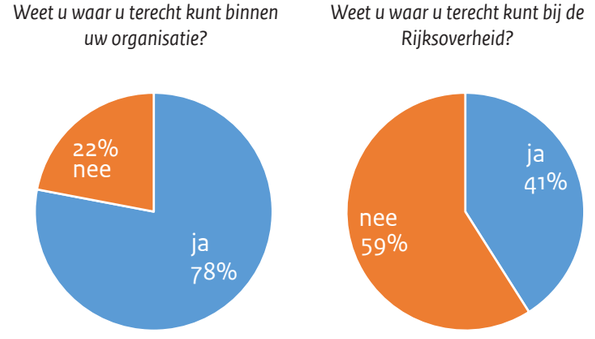
Het (niet) delen van informatie op het gebied van kennisveiligheid tussen de verschillende schaalniveaus, of dat nu binnen de kennisinstellingen tussen het college van bestuur en medewerkers of binnen de Rijksoverheid tussen ministeries is, lijkt hier een belangrijke belemmering te vormen.

Een ruime meerderheid (78%) van de respondenten van de online enquête geeft aan dat ze weten waar ze terecht kunnen binnen de organisatie met vragen over samenwerkingen met een derde land (zie figuur 4).

Een meerderheid (59%) van de respondenten van de online enquête geeft aan dat ze niet weten waar ze terecht kunnen bij de Rijksoverheid met vragen over samenwerkingen met een derde land (zie figuur 4).

Informatie over kennisveiligheid is binnen de kennisinstellingen dus beter bereikbaar dan bij de Rijksoverheid.

Fig. 4. Bereikbaarheid informatie



Belemmeringen in het contact met de Rijksoverheid

Van de groep respondenten die niet weet waar ze terecht kunnen bij de Rijksoverheid, is de algemene bereikbaarheid niet het grootste probleem, maar de versnippering van informatie bij verschillende departementen.

> *"Vandaar graag één loket. Je moet van alle kanten de informatie verzamelen. Via AIVD, MIVD, EZK, Douane, RVO, KVK en ga zo maar door om je een beeld te vormen of je als instelling de juiste keuze hebt gemaakt."*

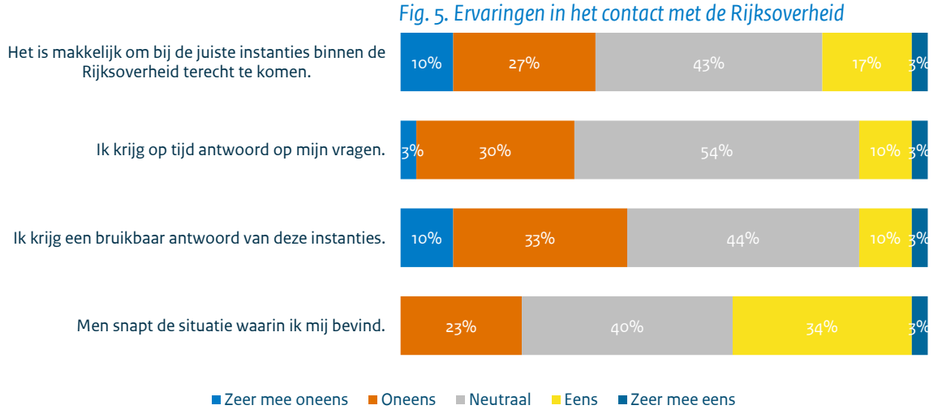
In de diepte interviews kregen we dat ook terug; informatie ligt bij verschillende ministeries en geen van die ministeries kan daardoor een helder eindadvies geven.

Ervaringen in het contact met de Rijksoverheid

51% van de respondenten heeft weleens contact gehad met de Rijksoverheid op het gebied van kennisveiligheid. De ministeries van OCW, EZK en BZ worden genoemd, maar ook AIVD, NCTV en RVO.

Deze groep is een viertal stellingen voorgelegd over hun ervaringen in het contact met de Rijksoverheid. Hieruit blijkt dat een groot deel van de respondenten neutraal in de 4 stellingen staat. Van diegenen die een positieve of negatieve waarde hebben ingevuld, is een groter deel negatief over hun contact met de Rijksoverheid dan positief (zie figuur 5).

Fig. 5. Ervaringen in het contact met de Rijksoverheid



3

Rol van het expertise- en adviesloket kennisveiligheid

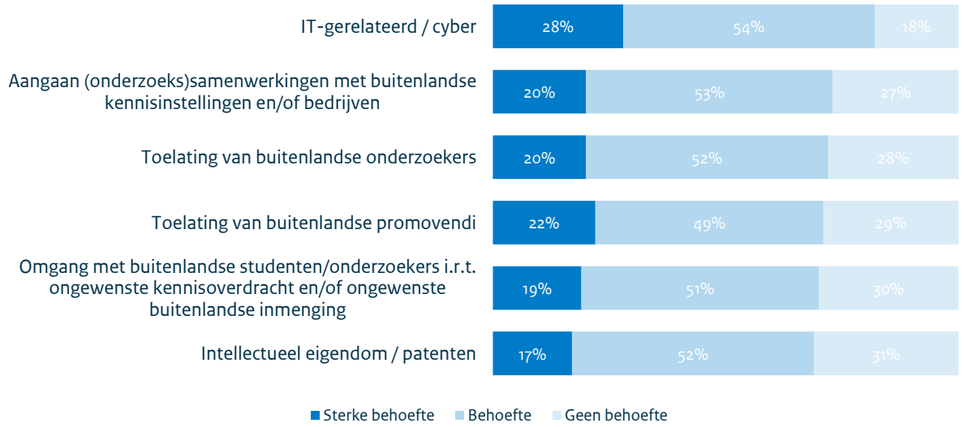
Thema's waarbij meedenken van de overheid gewenst is

Aan de respondenten is gevraagd in welke mate zij behoefte hebben aan meedenken vanuit de Rijksoverheid (in het loket) over risico's rondom kennisveiligheid bij een aantal aspecten van internationalisering. Eerder in de rapportage kwam aan bod welke aspecten rondom kennisveiligheid binnen de organisatie spelen. De vraag in dit hoofdstuk gaat specifiek in op welke thema's de behoeften liggen in meedenken vanuit de Rijksoverheid.

Uit de enquête komt naar voren dat de onderwerpen waarbij de sterkste behoefte aan meedenken bestaat vanuit de Rijksoverheid zijn (zie figuur 6):

1. IT-gerelateerd / cyber
2. Aangaan onderzoekssamenwerkingen met buitenlandse kennisinstellingen
3. Toelating van buitenlandse promovendi en/of onderzoekers
4. Omgang met buitenlandse studenten/ onderzoekers i.r.t. ongewenste kennisoverdracht en/of ongewenste buitenlandse inmenging
5. Intellectueel eigendom / patenten

Fig. 6. Behoefte aan meedenken Rijksoverheid (voor volledige grafiek, zie bijlage C)



Onderwerpen die niet op de lijst stonden, maar door twee respondenten zelf zijn ingebracht: nevenwerkzaamheden van medewerkers en meehelpen bij de analyse of bepaalde techproducten persoonlijke data buiten de EEA gaan brengen.

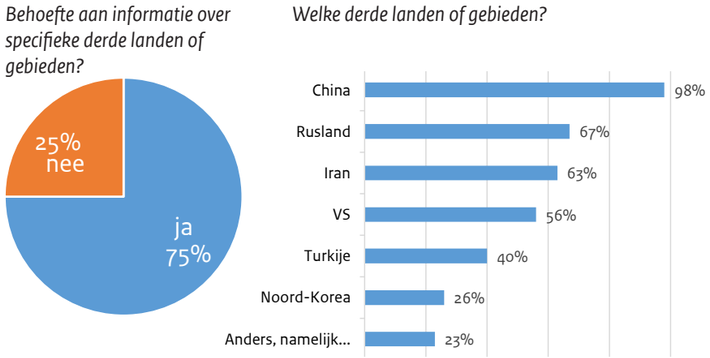
Thema's waarbij de minst sterke behoefte leeft aan meedenken vanuit de Rijksoverheid zijn (zie Bijlage C):

1. Afsluiten Memoranda of Understanding
2. Buitenlandse reizen (inclusief deelname aan conferenties)
3. Toelating van buitenlandse (gast)docenten

Specifieke landen en gebieden waarover informatie gewenst is

Van de 75% van de respondenten van de online enquête die aangeven dat ze behoefte hebben aan informatie over specifieke derde landen en gebieden, heeft 98% minimaal China aangekruist. China is dus een land waar medewerkers en bestuurders binnen de kennisinstellingen informatie over zouden willen hebben. Rusland, de Verenigde Staten en Iran volgen daarna (zie figuur 7). Daarnaast worden Israël, Syrië, India, Pakistan, Singapore, Saudi-Arabië en Hong Kong SAR genoemd.

Fig. 7. Landenvoorkeur voor informatiebehoefte



Uit de interviews komt naar voren dat China inderdaad een land is waar allen actief over nadenken in relatie tot kennisveiligheid. Hierbij merkte een geïnterviewde op dat 'China is de grootste concurrent, maar tegelijkertijd ook onze grootste samenwerkingspartner'.

Deze tegenstrijdigheid in belangen komt volgens een andere geïnterviewde ook terug in het advies van verschillende ministeries bij thema's rondom kennisveiligheid. Zo is het voorgekomen dat een ministerie zegt dat aan een samenwerking met een bepaalde organisatie in China risico's zitten, terwijl een ander ministerie vanuit het handelsperspectief wel toestaat dat naar dezelfde partner een missie wordt georganiseerd.

Randvoorwaarden expertise- en adviesloket kennisveiligheid

Uit de enquête en diepte interviews is het mogelijk een elftal overkoepelende, terugkerende elementen te destilleren waar een expertise- en adviesloket kennisveiligheid volgens de respondenten aan moet voldoen om meerwaarde te creëren:

1. **Algemene informatie** bieden over kennisveiligheidsrisico's.
2. **Specifieke informatie bieden** over bepaalde derde landen, hun strategische doelen, wet-en regelgeving, maar ook over gevoelige vakgebieden. Bijvoorbeeld in de vorm van een database/ dashboards met informatie/ risicoprofiel van beoogd partner (kennisinstelling, bedrijf).
3. Antwoorden geven op **praktische vragen.** Bijvoorbeeld over welke informatie er in internationale overeenkomsten moet staan en wat zeker niet, maar ook over welke samenwerkingskansen er liggen in kennisveiligheidsgevoelige regio's. Daarbij merken meerdere respondenten op dat er 'echte' experts moeten zitten die integraal antwoord geven op deze vragen over derde landen.
4. **Sparren over 'twijfelgevallen'** voor samenwerking. Het voorleggen van dilemma's.
5. Een duidelijk advies, dat al door een medewerker van het expertise- en adviesloket is **afgestemd met de verschillende ministeries.** Hierin wordt dus echt een samenwerking van ministeries en andere relevante partijen op het gebied van kennisveiligheid verwacht.
6. Een onafhankelijke en vrijblijvende **screening op studenten en medewerkers** aanbieden, maar ook op (bestaande) **samenwerkingsovereenkomsten met instellingen** uit derde landen. Bijvoorbeeld op het gebied van de herkomst van financiering.
7. Duidelijke en handelbare **nationale richtlijnen** over welke landen, onderwerpen en/of instellingen zich juist wel of niet lenen voor samenwerking. Begeleid door een open afwegingskader / stappenplan. Het doel is dat kennisinstellingen hetzelfde besluit kunnen nemen met dezelfde informatie die ze van buitenaf krijgen, zodat partijen uit derde landen geen 'shop' kansen langs verschillende kennisinstellingen krijgen.
8. Advies over **juridische zaken.**
9. Advies over (ICT) **maatregelen bij werkbezoeken** naar bepaalde derde landen.
10. **Bewustwording** over kennisveiligheid creëren / voorlichtingsfunctie bij kennisinstellingen.
11. **Netwerkfunctie** voor specifieke (deel)gebieden en/of thema's.

Reikwijdte van het loket

26% van de respondenten denkt bij het in te richten expertise- en adviesloket, naast kennisveiligheid, ook nog aan andere onderwerpen, te weten:

- Cybersecurity
- Inrichten van maatregelen die kennisverspreiding op een verantwoorde manier mogelijk maakt. Bijvoorbeeld met brochures om medewerkers te informeren.
- Bundelen van expertise in relatie tot de positieve kanten van internationale samenwerking en aantrekken internationaal talent.
- Ethische afwegingen over samenwerking met autocratische en/of landen waar mensenrechten worden geschonden.
- Data
- Radicalisering

No-go's

Kritische geluiden tijdens de interviews en in de enquête waren in veel gevallen waarschuwingen over hoe een expertise- en adviesloket pertinent niet zou moeten functioneren. Hieronder een aantal waarschuwingen van respondenten.

- Het expertise- en adviesloket moet *geen* loket worden waar projecten 'gecheckt' worden om een goedkeuringsstempel te krijgen. Een soort van APK-keuring voor projecten verplicht langs moeten.
- Het expertise- en adviesloket moet *geen* extra administratieve last zijn. Een advies moet afgestemd richting de vraagsteller gaan.

  "*Anders kunnen we net zo goed zelf contact opnemen met de verschillende ministeries*", liet een respondent weten tijdens het interview.
- In het expertise- en adviesloket moet een advies *niet* maanden op zich laten wachten. Wetenschappers, maar ook kennisinstellingen werken onder tijdsdruk en hebben op redelijke termijn advies nodig om weer verder te kunnen met een project.

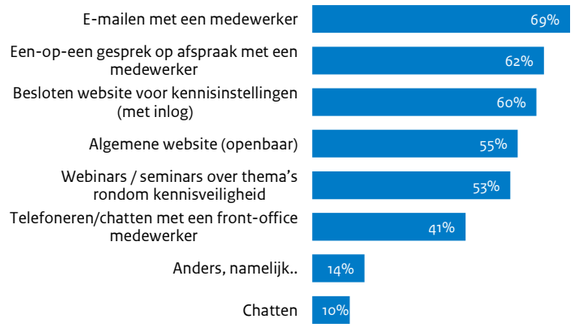
4

Praktische inregeling

Voorkeur contactmogelijkheden

De voorkeur voor contactmogelijkheden blijkt volgens de respondenten af te hangen van de aard van de vraag. In de praktijk is dus zowel behoefte aan een website met praktische informatie als aan een-op-een contact met een medewerker (zie figuur 8).

Fig. 8. Voorkeur om in contact te komen met het adviesloket



Zoals eerder in het rapport terugkomt, is voor veel respondenten een belangrijke voorwaarde dat de medewerker van het loket ook goede inhoudelijke kennis heeft om een afgestemd advies te kunnen geven.

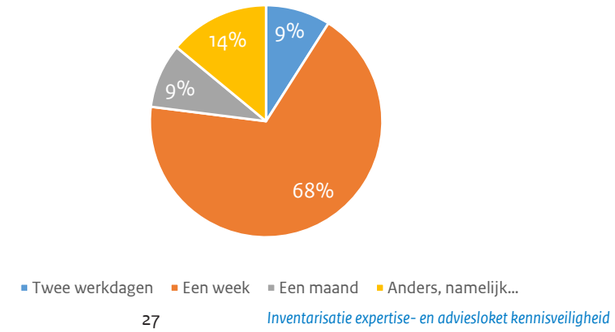
Een respondent benoemt nog dat informatie omtrent kennisveiligheid gevoelig kan zijn en dat rekening moet worden gehouden met een veilig verkeer van informatie.

Ook wordt de mogelijkheid tot actieve voorlichting op locatie nog aangestipt als een manier om in contact te komen. Kleine informatiebijeenkomsten of juist landelijk of specifiek richting kennisinstellingen die daar behoefte aan hebben. Dus niet enkel vraaggestuurd werken, maar ook pro-actief naar de kennisinstellingen toe (zowel fysiek als met pushberichten)

Redelijke termijn van beantwoording

De meerderheid van de respondenten (68%) ziet een week als een redelijke termijn om uitsluitsel te krijgen op een vraag aan het expertise- en adviesloket (zie figuur 9).

Fig. 9. Redelijke termijn van beantwoording



In de toelichting komt terecht naar voren dat de antwoordtermijn per vraag en thema kan verschillen. Zo stelt een respondent voor dat bij complexe vragen een week kan gelden en bij minder complexe vragen twee werkdagen. Een ander zou dat graag gezamenlijk met het loket bepalen per vraag, omdat ze de urgentie ook goed kan worden ingeschat.

Laagdrempelig maken van het loket

Zowel aan de respondenten van de enquête als in de diepte interviews hebben we de vraag gesteld wat er binnen hun organisatie nodig is om het expertise- en adviesloket kennisveiligheid benaderbaar en laagdrempelig te maken. Een overzicht van de belangrijkste punten zijn:

- Goede (digitale) toegankelijkheid en beschikbare **informatie op een eenvoudige en herkenbare manier presenteren.** Meerdere mogelijkheden aanbieden om in contact te komen met het loket.
- **Adequate en tijdige afhandeling** van vragen.
- Vertrouwen dat informatie in wederzijds vertrouwen wordt gedeeld. **Geen dossiervorming** per organisatie op basis van vragen aan het loket.
- **Kundige medewerkers** bij het loket waarmee dilemma's besproken kunnen worden. Duidelijke verdeling van dossiers en **centrale aanspreekpunten** op bepaalde thema's zoals bijvoorbeeld juridische zaken.
- Een goed ingevoerde medewerker die als een **linking pin kan fungeren tussen de kennisinstelling en het loket**. Of een centraal loket binnen de kennisinstelling die toegang heeft tot het expertiseloket kennisveiligheid.
- **Opzetten vanuit de vragen van medewerkers** van kennisinstellingen. Deze vragen kunnen gaan over een specifieke partner of land, maar ook over algemene richtlijnen of over de toelating van personen.
- **Bewustwording bij medewerkers** dat kennisveiligheid een issue is. Dit moet onderschreven worden door de leiding van de organisatie.
- **Webinars / meetings of masterclasses** rondom het thema.

- Wetenschappers hun **eigen peers laten mobiliseren. om het loket te raadplegen. Dat maakt meer indruk dan een landelijke, algemene campagne.**

Input gebruiken voor beleidsontwikkeling

94% van de respondenten staat positief tegenover het gebruik van de input in het loket voor beleidsontwikkeling.

Overige opmerkingen

Uit de diepte interviews bleek dat zowel binnen Nederland als in EU/internationaal verband al bij verschillende organisaties wordt nagedacht over een adviesloket: een organisatie heeft een werkend adviesloket voor een specifieke derde land, in Duitsland is de regio Nordrhein Westfalen bezig met een adviesloket kennisveiligheid, maar ook verder van huis in Japan, is de overheid al langer met dit thema bezig. Er wordt dus al veel informatie op het thema gegenereerd. Landen zoals de Verenigde Staten zijn juist weer nieuwsgierig naar hoe Nederland dit loket oppakt.

5

Conclusies

Conclusies

Dit onderzoek biedt een inventarisatie van de behoeften en wensen van het Nederlandse kennisveld en aanbevelingen ten behoeve van het opzetten van een expertise- en adviesloket kennisveiligheid. Het Nederlandse kennisveld beslaat in dit onderzoek de Nederlandse hogescholen, universiteiten, UMC's, (onderzoeks) instituten NWO en KNAW en de TO2-instellingen (Deltares, Marin, NLR, TNO en Wageningen Research).

Onderwerpen
Onderwerpen rondom kennisveiligheid waarbij de sterkste behoefte aan meedenken bestaat vanuit de Rijksoverheid zijn IT-gerelateerd / cyber, aangaan onderzoekssamenwerkingen met buitenlandse kennisinstellingen, de toelating van buitenlandse promovendi en/of onderzoekers, de omgang met buitenlandse studenten/ onderzoekers en het intellectueel eigendom / patenten.

Randvoorwaarden
Het expertise- en adviesloket kennisveiligheid moet volgens de respondenten aan een aantal randvoorwaarden voldoen om meerwaarde te creëren. Zo moet het niet alleen algemene informatie bieden over kennisveiligheidsrisico's, maar ook specifieke informatie over bepaalde derde landen, hun strategische doelen, wet-en regelgeving, maar ook over gevoelige vakgebieden. Bijvoorbeeld in de vorm van een database/ dashboards met informatie/ risicoprofiel van beoogd partner (kennisinstelling, bedrijf).

Het expertise- en adviesloket moet snel antwoord geven op praktische vragen (ook over juridische zaken), maar ook medewerkers hebben die de expertise hebben om te kunnen sparren over 'twijfelgevallen'. Deze medewerkers moeten een duidelijk advies geven, dat al is afgestemd met verschillende ministeries. Hierin wordt dus echt een samenwerking van ministeries en andere relevante partijen op het gebied van kennisveiligheid verwacht.

Screening van studenten, medewerkers en samenwerkingsovereenkomsten met instellingen uit derde landen worden ook als randvoorwaarden beschouwd. Net zoals duidelijke en handelbare nationale richtlijnen, begeleid door een open afwegingskader of stappenplan.

Als laatste kwamen het creëren van bewustwording en de netwerkfunctie vaak naar voren als wensen aan het loket. Webinars en seminars werden in dat kader genoemd als mogelijke tools.

No-go's
Het expertise- en adviesloket moet *geen* loket worden waar projecten 'gecheckt' worden om een goedkeuringsstempel te krijgen. Ook moet het expertise- en adviesloket *geen* extra administratieve last zijn.

Contactmogelijkheden
De voorkeur voor contactmogelijkheden blijkt volgens de respondenten af te hangen van de aard van de vraag. In de praktijk is dus zowel behoefte aan een website met praktische informatie als aan een-op-een contact met een medewerker.

Leren van elkaar
Uit de diepte interviews bleek dat zowel binnen Nederland als in EU/internationaal verband al bij verschillende organisaties wordt nagedacht over een expertise- en adviesloket kennisveiligheid

Aanbevelingen inrichting expertise -en adviesloket kennisveiligheid

In dit onderzoek vond een inventarisatie plaats van de behoeften en wensen van het Nederlandse kennisveld voor een expertise- en adviesloket kennisveiligheid. Onderstaande aanbevelingen komen voort uit de uitkomsten van de online enquête onder de kennisinstellingen en de diepte interviews met relevante personen in het veld en zijn verdeeld in aanbevelingen op het gebied van structuur en inhoud van het loket, de technische vereisten, het creëren van draagvlak en het lerend vermogen.

Structuur en inhoud

1. **Bied een combinatie van 'snelle' praktische informatie en informatie door deskundige medewerkers die inhoudelijk meedenken**
   Algemene richtlijnen over samenwerking met derde landen, een lijst met aandachtspunten en thematiek met mogelijke risico's zijn noodzakelijk. Daarnaast klinkt ook duidelijk de roep om meedenkende en inhoudelijk sterke adviseurs die een sparringspartner kunnen zijn om dilemma's rondom kennisveiligheid te bespreken (en informatie bij verschillende instanties ophalen om tot een advies te komen). Het loket moet dus niet enkel een doorverwijsfunctie krijgen, maar ook een serieuze gesprekspartner zijn.

2. **Benadruk de variëteit aan landen in het expertise- en adviesloket**
   Hoewel alle respondenten minimaal informatie over China wilden terugzien in het expertise- en adviesloket kennisveiligheid, gaf een groot deel van de respondenten ook aan behoefte te hebben aan informatie over Rusland, Iran en de VS. Het is dus in de communicatie van belang te benadrukken dat het loket ondersteuning biedt bij vragen over verschillende derde landen.

3. **Blijf oog houden voor de reikwijdte aan thema's rondom kennisveiligheid**
   De top-5 thema's waarbij meedenken vanuit de Rijksoverheid gewenst is, laat een breed spectrum aan onderwerpen zien. Het expertise- en adviesloket kennisveiligheid moet dus advies en informatie bieden op al deze vlakken om een solide positie op het gebied van kennisveiligheid te kunnen creëren.

Technische vereisten

4. **Begin met een eenvoudige, maar duidelijke website voor het expertise- en adviesloket**
   In de keuze voor platforms waarop de website van het expertise- en adviesloket kennisveiligheid kan draaien zijn verschillende mogelijkheden. Van professioneel beveiligde, met maatwerk ontwikkeld platforms tot eenvoudige, snel te realiseren platforms. Bij de Rijksoverheid, maar ook bij RVO ligt veel expertise op het gebied van platformmanagement. Wij raden dan ook aan om een studie uit te laten voeren naar het meest geschikte platform voor het loket. Vanuit het oogpunt van tijd- en kostenefficiëntie, en de huidige behoeften vanuit het veld, zou onze voorkeur op het moment uitgaan naar een snel te realiseren, eenvoudige variant. Mochten meer geavanceerde (beveiligings)opties nodig worden geacht, kan later altijd nog opgeschaald worden naar een maatwerk optie.

5. **Zorg voor een snelle en adequate vraagafhandeling (max. een week)**
   De meeste respondenten geven aan dat een week een redelijke termijn van beantwoording vormt. Om relevantie in het veld te houden en welwillendheid te kweken, raden wij aan deze termijn te volgen.

Het creëren en behouden van draagvlak

6. **Houd informatie te allen tijde up-to-date**
   Het thema van kennisveiligheid leeft sterk binnen het veld. Uit de enquête en interviews bleek ook de behoefte aan informatie op het thema. Het is van belang om dit momentum te benutten, maar het is net zo goed van belang dat het goed gebeurt. We kregen van respondenten de waarschuwing mee dat de informatie en richtlijnen op een website altijd up-to-date moet zijn. Bijvoorbeeld actief communiceren als er nieuwe beleidsinformatie of richtlijnen over een bepaalde derde land uitkomen. Anders kijken wetenschappers een keer, maar daarna niet meer, was de vrees vanuit het veld.

7. **Werk actief aan de beeldvorming van het loket / maak een duidelijk communicatieplan**
   De beeldvorming is van essentieel belang voor het succes van het expertise- en adviesloket. In de interviews merkten we in sommige gevallen nog weerstand ten aanzien van het loket. Mogelijk kan deze door juiste informatie weggenomen worden. Ook werden door respondenten seminars en webinars genoemd om medewerkers bekend te maken met het loket en het gebruikerspercentage omhoog te brengen.

Lerend vermogen

8. **Leer van elkaar en haak aan op bestaande initiatieven in binnen -en buitenland**
   Uit de interviews blijkt dat op het moment veel organisaties en overheden in binnen-en buitenland zich bezig houden met het thema van kennisveiligheid, ook in relatie tot informatiepunten. Wij raden dan ook aan om parallel aan de inrichting van het expertise- en adviesloket, nog een gedetailleerde studie te doen naar andere initiatieven en de tips en tops hiervan mee te nemen in de inrichting van het loket. Ook is het van belang om aangehaakt te blijven bij Brussel en de aanpak van andere EU-lidstaten.

Bijlagen

Bijlage A: vragenlijst enquete

Welkomsttekst start online enquete

I Algemeen

1. Namens wie vult u deze enquête in?
a. Namens de instelling
b. Namens het organisatieonderdeel waaraan ik verbonden ben
c. Op persoonlijke titel
d. Anders, namelijk..

2. Aan welk type (kennis)instelling bent u werkzaam? Antwoorden worden geanonimiseerd verwerkt. Deze vraag wordt gebruikt voor de statistieken en om algemene conclusies te kunnen trekken.
a. Hogeschool
b. Universiteit
c. Universitair Medisch Centrum
d. Onderzoeksinstituut NWO
e. Onderzoeksinstituut KNAW
f. TO-2 instelling
g. Anders, namelijk..

3. Welke functie bekleedt u binnen de kennisinstelling? Antwoorden worden geanonimiseerd verwerkt. Deze vraag wordt gebruikt voor de statistieken en om algemene conclusies te kunnen trekken.
a. College van Bestuur
b. Beleidsmedewerker
c. Veiligheidsfunctionaris
d. Hoogleraar
e. Onderzoeker
f. Anders, namelijk..

II Situatie binnen uw organisatie

4. In welke mate spelen er binnen uw organisatie dilemma's rondom kennisveiligheid bij de volgende aspecten van internationalisering? Alle aspecten zijn in relatie tot derde landen. Matrixvraag 'nooit' 'zelden' 'soms' 'vaak' 'heel vaak' 'nvt':
- Aangaan (onderzoeks)samenwerkingen met buitenlandse kennisinstellingen en/of bedrijven
- Afsluiten Memoranda of Understanding (MoU's)
- Toelating van buitenlandse studenten
- Toelating van buitenlandse promovendi
- Toelating van buitenlandse onderzoekers
- Toelating van buitenlandse (gast)docenten
- Omgang met buitenlandse studenten/onderzoekers i.r.t. ongewenste kennisoverdracht en/of ongewenste buitenlandse inmenging
- Aannemen van financiering voor contractonderzoek
- Buitenlandse reizen (inclusief deelname aan conferenties)

- Ontvangst van buitenlandse gasten en bezoekers
- Exportcontrole van (dual use) goederen
- Intellectueel eigendom / patenten
- IT-gerelateerd / cyber
- Onderzoeksresultaten delen met buitenlandse kennisinstellingen
- Zicht op uiteindelijke toepassing van gezamenlijke onderzoeksresultaten
- Anders, namelijk..

5. Spelen deze dilemma's in uw organisatie bij specifieke derde landen? Antwoorden worden geanonimiseerd verwerkt.
a. Ja
i. Welke derde landen? Meerdere antwoorden mogelijk.
b. Nee

6. In hoeverre heeft u het gevoel dat de risico's rondom kennisveiligheid voldoende in beeld zijn binnen uw organisatie? Slider vraag
a. Zeer goed in beeld
b. Goed in beeld
c. Noch slecht noch goed in beeld
d. Slecht in beeld
e. Zeer slecht in beeld

i. Kunt u hier een toelichting op geven?

7. Weet u waar u terecht kunt binnen uw organisatie met vragen over of en hoe u gaat samenwerken met een derde land?
a. Ja
b. Nee

8. Wanneer heeft een expertise-en adviesloket kennisveiligheid voor uw organisatie echt een meerwaarde? Met andere woorden, welke expertise en kennis zouden u kunnen helpen om in de praktijk kansen en risico's rondom internationale samenwerking beter te kunnen afwegen?

9. Zijn er naast onderwerpen gerelateerd aan kennisveiligheid nog andere onderwerpen waar u denkt bij het loket?

III Rol van de overheid

10. In hoeverre heeft u behoefte aan meedenken vanuit de Rijksoverheid over risico's rondom kennisveiligheid bij de volgende aspecten van internationalisering? Alle aspecten zijn in relatie tot derde landen. Matrixvraag 'geen behoefte' 'behoefte' 'sterke behoefte' 'nvt'
- Aangaan (onderzoeks)samenwerkingen met buitenlandse kennisinstellingen en/of bedrijven
- Afsluiten Memoranda of Understanding (MoU's)
- Toelating van buitenlandse studenten
- Toelating van buitenlandse promovendi

- Toelating van buitenlandse onderzoekers
- Toelating van buitenlandse (gast)docenten
- Omgang met buitenlandse studenten/onderzoekers i.r.t. ongewenste kennisoverdracht en/of ongewenste buitenlandse inmenging
- Aannemen van financiering voor contractonderzoek
- Buitenlandse reizen (inclusief deelname aan conferenties)
- Ontvangst van buitenlandse gasten en bezoekers
- Exportcontrole van (dual use) goederen
- Intellectueel eigendom / patenten
- IT-gerelateerd / cyber
- Onderzoeksresultaten delen met buitenlandse kennisinstellingen
- Zicht op uiteindelijke toepassing van gezamenlijke onderzoeksresultaten
- Anders, namelijk..

11. Heeft u hierbij behoefte aan informatie over specifieke derde landen? Antwoorden worden geanonimiseerd verwerkt.
a. Ja
i. Welke derde landen? Meerdere antwoorden mogelijk.
b. Nee

12. Aan welke soort informatie heeft u precies behoefte?

13. Weet u waar u terecht kunt bij de Rijksoverheid met vragen over of en hoe u gaat samenwerken met een derde land?
a. Ja
b. Nee
i. Waar loopt u tegenaan?

14. Heeft u weleens contact gehad met onderdelen van de Rijksoverheid op het gebied van kennisveiligheid?
a. Ja [naar vraag 16]
i. Welk onderdeel was dit?
b. Nee [naar vraag 21]

15. Hoe ervaart u de contactmogelijkheden met de Rijksoverheid over dit soort (veiligheids)kwesties? Slider mogelijkheid
a. Zeer goed
b. Goed
c. Neutraal
i. Waar loopt u tegenaan?
d. Slecht
ii. Waar loopt u tegenaan?
e. Zeer slecht
iii. Waar loopt u tegenaan?

Hierna volgen een aantal stellingen waarin u kunt aangeven welk antwoord het

beste bij uw ervaring past in het contact met onderdelen van de Rijksoverheid op het gebied van kennisveiligheid.

16. Het is makkelijk om bij de juiste instanties binnen de Rijksoverheid terecht te komen.
a. zeer mee oneens
b. oneens
c. niet mee eens/niet mee oneens
d. eens
e. zeer mee eens

17. Ik krijg op tijd antwoord op mijn vragen.
a. zeer mee oneens
b. oneens
c. niet mee eens/niet mee oneens
d. eens
e. zeer mee eens

18. Ik krijg een bruikbaar antwoord van deze instanties.
a. zeer mee oneens
b. oneens
c. niet mee eens/niet mee oneens
d. eens
e. zeer mee eens

19. Men snapt de situatie waarin ik mij bevind.
a. zeer mee oneens
b. oneens
c. niet mee eens/niet mee oneens
d. eens
e. zeer mee eens

IV Inrichting van het expertise-en adviesloket

20. Hoe zou u graag in contact willen komen met een expertise- en adviesloket kennisveiligheid? Meerdere antwoorden mogelijk.
a. Algemene website (openbaar)
b. Besloten website voor kennisinstellingen (met inlog)
c. Telefoneren/chatten met een front-office medewerker
d. Een-op-een gesprek op afspraak met een medewerker
e. E-mailen met een medewerker
f. Chatten
g. Webinars / seminars over thema's rondom kennisveiligheid
h. Anders, namelijk..

21. Wat is volgens u een redelijke termijn om uitsluitsel op uw vraag te krijgen?
a. Twee werkdagen

b. Een week
c. Een maand
d. Anders, namelijk…

22. Het is belangrijk dat het expertise- en adviesloket kennisveiligheid benaderbaar en laagdrempelig is. Wat is er volgens u binnen uw organisatie nodig om dit te bewerkstelligen?

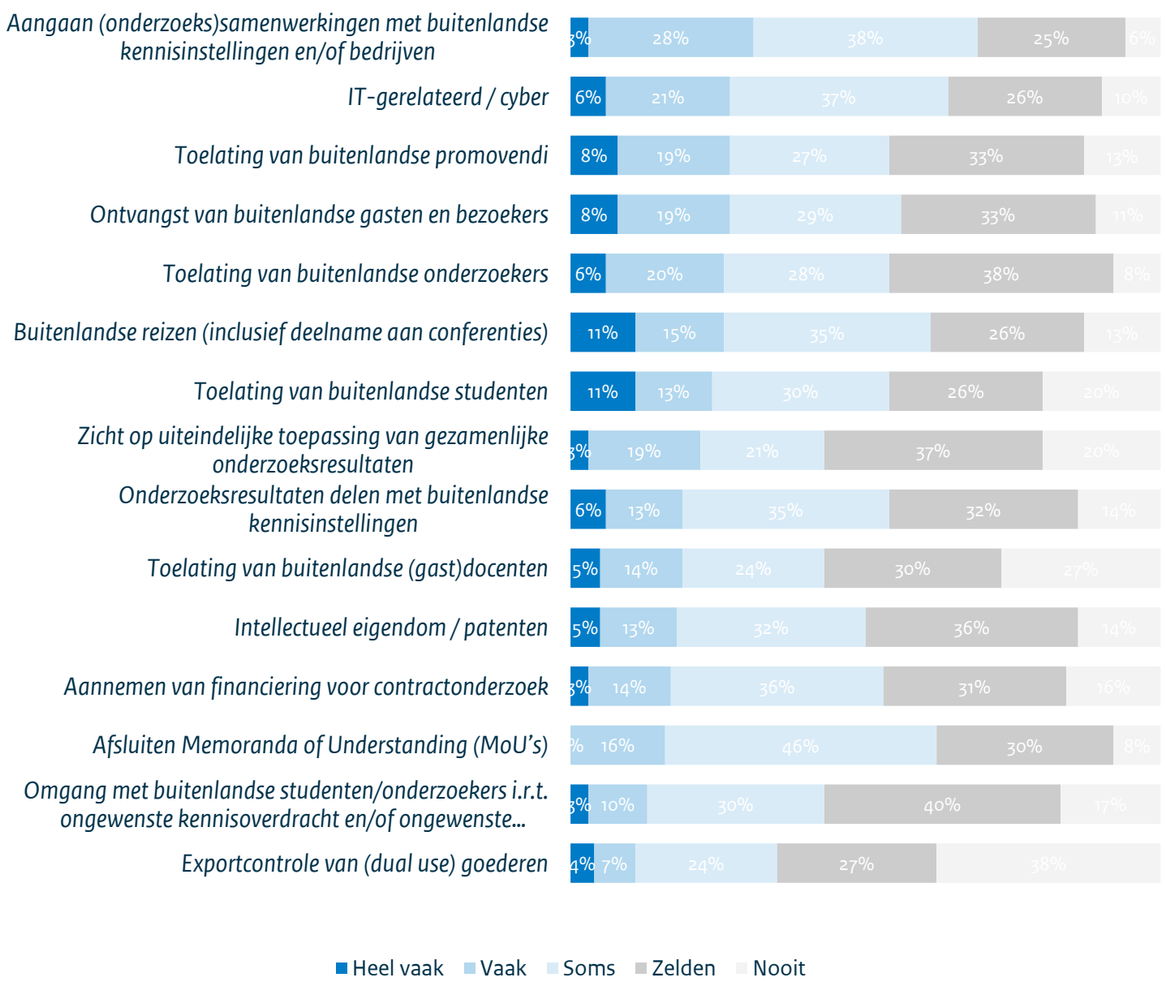
23. Stel, er komt een expertise-en adviesloket kennisveiligheid. Hoe staat u tegenover het gebruik van uw input voor beleidsontwikkeling? De vragen die u aan het loket stelt, zullen in dat geval (anoniem) worden verzameld en geanalyseerd ten behoeve van beleidsontwikkeling.
a. Positief
b. Negatief
i. Kunt u hier een toelichting op geven?

24. Heeft u nog overige opmerkingen en/of suggesties, dan kunt u die hier kwijt.

25. Naast deze online enquête, gaan we ook graag wat langer in gesprek met respondenten over dit onderwerp. Mocht u uw antwoorden willen toelichten en langer in gesprek met ons gaan om uw wensen kenbaar te maken, kunt u hieronder uw emailadres invullen. Dan nemen we graag contact met u op.

Hartelijk dank voor uw deelname.

Bijlage B: Mate waarin bepaalde dilemma's rondom kennisveiligheid spelen binnen de kennisinstellingen (volledige grafiek)



Bijlage C: Behoefte aan meedenken Rijksoverheid (volledige grafiek)

Dit is een publicatie van:

Rijksdienst voor Ondernemend Nederland
Prinses Beatrixlaan 2 | 2595 AL Den Haag
Postbus 93144 | 2509 AC Den Haag
T +31 (0) 88 042 42 42
F +31 (0) 88 602 90 23
W www.rvo.nl

Deze publicatie is tot stand gekomen in opdracht van het ministerie van Onderwijs Cultuur en Wetenschap

De Rijksdienst voor Ondernemend Nederland (RVO.nl) stimuleert duurzaam, agrarisch, innovatief en internationaal ondernemen. Met subsidies, het vinden van zakenpartners, kennis en het voldoen aan wet- en regelgeving. RVO.nl werkt in opdracht van ministeries en de Europese Unie.

RVO.nl is een onderdeel van het ministerie van Economische Zaken en Klimaat.