

Nationale leidraad kennisveiligheid

Veilig internationaal samenwerken



Nationale leidraad kennisveiligheid

Veilig internationaal samenwerken

Januari 2022

Universiteiten
van Nederland }



Inhoudsopgave

3	Managementsamenvatting
8	1. Introductie
13	2. Het beschermen van academische kernwaarden
14	2.1 Academische vrijheid en wetenschappelijke integriteit
16	2.2 Open science
16	2.3 Ethiek in de wetenschap
17	2.4 Inclusiviteit en non-discriminatie
18	3. Dreigingsbeeld
19	3.1 Om welke dreigingen gaat het?
19	3.2 Verwerving van kennis en technologie
21	3.3 Beïnvloedings- en inmengingsactiviteiten
22	4. Juridische kaders en gedragscodes
23	4.1 Exportregels voor dual-use producten en technologie
25	4.2 Internationale sanctieregimes
27	4.3 Gedragscodes kennisveiligheid
28	5. Het inschatten van risico's
29	5.1 Welke kennisgebieden binnen uw instelling hebben een verhoogd risico?
30	5.2 Welke landen hebben een verhoogd risico?
31	5.3 Ken uw samenwerkingspartners, opdrachtgevers en financiers
33	6. Risicomanagement
34	6.1 Organiseer risicomanagement binnen uw organisatie
35	6.2 Organisatorische maatregelen
36	6.3 Zorg voor een accurate feitenbasis voor besluitvorming
37	6.4 Fysieke en digitale beschermingsmaatregelen
37	6.5 Veiligheidscultuur: bewustwording en alertheid
39	7. Internationale partnerschappen, inkopen en aanbesteden
40	7.1 Waar u op moet letten bij het aangaan van een samenwerking
42	7.2 Kennisveiligheid bij inkopen en aanbesteden
44	8. De rol van personeelsbeleid
45	8.1 Veiligheidscheck bij werving en selectie
46	8.2 Opleiding en training
46	8.3 Buitenlandse bezoekers en dienstreizen naar het buitenland
49	9. Cyberveiligheid in relatie tot statelijke dreigingen
50	9.1 Dreigingen en risico's
52	9.2 Handelingsperspectief: wat kunt u doen?
56	Overzicht contactgegevens en bronnen

Managementsamenvatting

- Bij kennisveiligheid gaat het allereerst om **ongewenste overdracht van sensitieve kennis en technologie**. Overdracht is ongewenst als deze de nationale veiligheid van ons land aantast. Daarnaast gaat kennisveiligheid om heimelijke beïnvloeding van onderwijs en onderzoek door statelijke actoren. Deze inmenging brengt de academische vrijheid en de sociale veiligheid in gevaar. Tot slot gaat het om **ethische kwesties** die kunnen spelen in de samenwerking met landen die de grondrechten niet respecteren.
- Hoger onderwijs en wetenschap van wereldklasse kunnen niet zonder internationale samenwerking en wetenschappelijk talent van over de hele wereld. Deze Nationale Leidraad Kennisveiligheid helpt u op weg om ervoor te zorgen dat **internationale samenwerking veilig** kan plaatsvinden.
- Bij het nemen van maatregelen is proportionaliteit essentieel. Uitgangspunt is steeds: 'open waar mogelijk, beschermen waar nodig'.
- Bij de aanpak van kennisveiligheid staat **zelfregulering** door de kennissector centraal. Organisaties als VH, UNL, KNAW, NWO, NFU en de TO2-federatie spelen een initiërende en faciliterende rol.
- Het beschermen van de nationale veiligheid is een kerntaak van de overheid. Daarom speelt de **Rijksoverheid een actieve rol** bij kennisveiligheid door kennisinstellingen te informeren, handelingsperspectief te bieden en -waar nodig- kaders te stellen. Zo kunnen kennisinstellingen vanaf 2022 terecht bij het loket kennisveiligheid voor expertise en advies van de betrokken ministeries en diensten.

Academische kernwaarden als uitgangspunt

- Academische kernwaarden zoals **academische vrijheid** en **wetenschappelijke integriteit** vormen het fundament van hoger onderwijs en wetenschap in Nederland.
- Ook bij **activiteiten met buitenlandse partners** zijn de academische kernwaarden richtinggevend. Ze bieden houvast bij het aangaan van buitenlandse samenwerkingen. Buitenlandse **(gast)onderzoekers en docenten** dienen, net als hun Nederlandse collega's, de gedragscode te onderschrijven en na te leven.
- **Open science** is binnen Europa de norm: het streven is om publiek gefinancierde onderzoeksresultaten voor iedereen toegankelijk te maken. Er kunnen echter legitieme redenen zijn om van openbaarmaking af te zien, zoals het beschermen van de **nationale veiligheid**. Maak vooraf goede afspraken om spanning tussen het streven naar maximale openheid en het treffen van legitieme beschermende maatregelen te voorkomen.
- **Ethische dilemma's** kunnen een rol spelen wanneer wordt samengewerkt met landen die de grondrechten niet respecteren. Hoe kan voorkomen worden dat onderzoeksresultaten daar worden gebruikt voor onderdrukking of schending van mensenrechten? Het is raadzaam om binnen uw instelling een **ethische commissie** te hebben die kan adviseren over ethisch gebruik van onderzoeksresultaten.
- Kennisinstellingen hebben een zorgplicht jegens werknemers en studenten als het gaat om hun **sociale veiligheid**. Bij studenten en onderzoekers uit landen waar de grondrechten niet worden gerespecteerd kan die veiligheid ernstig in het geding zijn door het handelen van de herkomststaat.
- Maatregelen rond kennisveiligheid mogen niet 'doorslaan' en leiden tot willekeurige uitsluiting, verdachtmaking of discriminatie.

Dreigingsbeeld

- Statelijke actoren gebruiken uiteenlopende methoden om **kennis en technologie te verwerven** die zij kunnen inzetten voor militaire doeleinden of doelen die indruisen tegen onze fundamentele waarden. Denk hierbij aan centraal aangestuurde talentenprogramma's, het onder druk zetten van geëmigreerde (ex-)landgenoten, digitale spionageactiviteiten of het rekruteren van individuen op strategische posities.
- Ook **samenwerkingsverbanden** worden als instrument ingezet. De academische samenwerkingspartner fungeert dan als een verlengstuk van de overheid. Hierdoor heeft de ogenschijnlijk academische samenwerking een **dubbele agenda**.
- Tot slot kunnen statelijke actoren **beïnvloedings- en inmengingsactiviteiten** ondernemen. Bijvoorbeeld om meningen (over het land) te beïnvloeden of om onderzoek naar onwelgevallige onderwerpen te verhinderen. Deze landen proberen **greep te houden op hun landgenoten**. De wetenschap dat zij vanuit hun herkomstland in de gaten worden gehouden zorgt bij de betrokken onderzoekers en studenten voor angst. Angst die leidt tot zelfcensuur en aantasting van academische kernwaarden.

Juridische kaders en gedragscodes

- Er is wet- en regelgeving om de dreigingen het hoofd te bieden, waaraan uw instelling dient te voldoen (*compliance*). Zo gelden er binnen de Europese Unie strenge regels voor de uitvoer van **dual-use producten en technologie** die naast civiele ook militaire toepassingen hebben. Het gaat om alle vormen van overdracht, dus **ook via e-mail of een clouddienst**. Zuiver fundamenteel wetenschappelijk onderzoek en technologie die zich reeds in het publieke domein bevinden zijn uitgezonderd van exportcontrole. Twijfelt u of de exportregels van toepassing zijn, dan kunt u een indelingsverzoek doen bij de **Centrale Dienst voor In- en Uitvoer** (CDIU).
- Daarnaast zijn er **internationale sanctieregimes** van kracht tegen landen, organisaties en personen. Het actuele overzicht is te vinden op www.sanctionsmap.eu. De sancties tegen **Noord-Korea** en **Iran** zijn voor kennisinstellingen in het bijzonder relevant: deze vormen de basis voor het **verscherpt toezicht** dat voor een beperkt aantal vakgebieden geldt.
- Het kabinet werkt aan maatregelen om het handelingsperspectief van kennisinstellingen en overheden verder te vergroten. Zo werkt het kabinet aan een **toetsingskader** dat voorziet in een gerichte toetsing van personen die toegang willen tot kennisgebieden met een hoog risico voor de nationale veiligheid. Het kabinet streeft ernaar dat dit kader in de loop van 2023 gaat gelden. Daarnaast heeft het kabinet een wetsontwerp gepresenteerd over **buitenlandse investeringen**, fusies en overnames. De wet richt zich op vitale aanbieders en op organisaties die beschikken over sensitieve technologie.
- Ook zijn er verschillende **gedragscodes** over kennisveiligheid. Deze zijn niet-bindend, maar wel richtinggevend. Zo is er het kennisveiligheidskader van UNL en zijn er *EU guidelines on tackling R&I foreign interference* van de Europese Commissie. Diverse landen hebben inmiddels vergelijkbare gedragscodes uitgewerkt. Deze codes maken het makkelijker om met buitenlandse partners het gesprek over kennisveiligheid te voeren.

Risicoanalyse

- Het is belangrijk om **sensitieve kennisgebieden** binnen uw instelling nauwkeurig te identificeren. Denk aan *dual-use* technologieën en kennis die onethisch ingezet kan worden. Breng ook uw **'kroonjuwelen'** in kaart; de gebieden waarop er risico's verbonden zijn aan kennisoverdracht en uw instelling internationaal toonaangevend is. Voer voor elk sensitief kennisgebied een korte risicoanalyse uit.
- Om een inschatting te maken van het **risicoprofiel van een land**, kunt u gebruik maken van openbare dreigingsinformatie, zoals het Dreigingsbeeld Statelijke Actoren van NCTV, AIVD en MIVD. Daarnaast kunt u internationale ranglijsten raadplegen: een slechte score op *rankings* over academische vrijheid en respect voor de rechtsstaat **moet alarmbellen doen afgaan**. Een slechte score betekent niet noodzakelijkerwijs dat u niet met instellingen uit dat land kunt samenwerken, wel moet u dan goede voorzorgsmaatregelen treffen.
- Vervolgens is het van belang dat u zich in het kader van **due diligence** verdiept in de achtergrond van de buitenlandse partner of opdrachtgever. Het gaat erom scherp te letten op **signalen**, zoals het ontbreken van informatie op internet of het feit dat de instelling bij niemand bekend is. Vraag u bij opdrachtgevers of onderzoeksfinciers af welke motieven er in het spel zijn en of deze belang heeft bij een bepaalde uitkomst. Bedenk dat u stap voor stap in een situatie van **(financiële) afhankelijkheid** kan worden gebracht. Betrek in geval van veiligheidsrisico's uw veiligheidscoördinator en zorg dat beslissingen over wel/niet in zee gaan met de partner door het bestuur van uw organisatie worden genomen als onderdeel van het **partneracceptatiebeleid**.

Risicomangement

- Het is raadzaam een aantal **standaardprocessen centraal in te regelen**. Afhankelijk van het risiconiveau zijn de benodigde risicoanalyses en controles strikter en ligt de beslisbevoegdheid op een hoger, centraler niveau.
- Het begint met het aanwijzen van een **portefeuillehouder op bestuurlijk niveau** en het instellen van een **Adviesteam Kennisveiligheid** van enkele deskundigen met relevante expertises om de portefeuillehouder bij te staan. Als onderdeel van een open veiligheidscultuur dienen er **vertrouwenspersonen** te zijn waar medewerkers terecht kunnen met signalen over veiligheidsrisico's. Deze vertrouwenspersonen moeten zelf goed op de hoogte zijn van de risico's rond kennisveiligheid.
- Zorg op bestuursniveau voor een centraal en up-to-date **overzicht van veiligheidsgevoelige partnerschappen, financiering en buitenlandse promovendi en gastonderzoekers**. Dit 'dashboard' vormt de basis voor effectief risicomangement binnen uw instelling. Ook geeft het inzicht in het cumulatief effect van ontwikkelingen die los gezien onproblematisch lijken.
- Denk ook aan **fysieke en digitale beschermingsmaatregelen**: voor welke verdiepingen of ruimtes geldt een restrictief toegangsbeleid? Wie heeft toegang tot onderzoeksgegevens? Werkt u met zeer sensitieve gegevens, overweeg dan met rubricering van documenten te werken, zoals 'vertrouwelijk' of 'geheim'.
- Het creëren van een **open veiligheidscultuur** binnen uw instelling is essentieel. **Bewustwordingscampagnes** kunnen daar een nuttige bijdrage aan leveren. Sluit daarbij zo veel mogelijk aan op de belevingswereld van de doelgroepen via trainingsmodules, teamsessies en simulaties.

Internationale partnerschappen

- Samenwerkingsovereenkomsten vormen een goed aangrijpingspunt voor het afwegen van kansen en risico's. Voor samenwerkingen met een verhoogd risico volstaan de standaard sjablonen voor overeenkomsten mogelijk niet. Het is zaak **juridische en veiligheidsexpertise in te schakelen**.
- Eenmaal gesloten, is het raadzaam de samenwerking regelmatig te evalueren en eventuele knelpunten vroegtijdig te adresseren. **Verleng overeenkomsten met verhoogd risico nooit stilzwijgend**. Zorg er binnen uw organisatie voor dat u ruim voor het verlengmoment wordt gealerteerd zodat u de afspraken kritisch tegen het licht kunt houden.
- Ook bij **inkopen en aanbesteden** kan kennisveiligheid een rol spelen. Door risico's tijdig in kaart te brengen kunt u gepaste maatregelen nemen, zoals het opnemen van aanvullende contracteisen.

Personeelsbeleid

- De **werving en selectie** van nieuwe medewerkers is een cruciaal moment om veiligheidsrisico's in te schatten. Het is daarom van belang dat HR-medewerkers veiligheidsbewust zijn en signalen die wijzen op een verhoogd risico oppikken.
- Zorg ervoor dat nieuwe medewerkers **informatie en training** krijgen om hen veiligheidsbewust te maken. Daarnaast kan voorzien worden in opfrismodules en speciale trainingsprogramma's voor gastonderzoekers uit landen met een verhoogd risicoprofiel.
- U wordt geadviseerd een **bezoekersprotocol** uit te werken om risico's tijdens bezoeken aan sensitieve locaties te beperken. Omgekeerd vergt een **dienstreis** naar landen met een verhoogd risicoprofiel -bijvoorbeeld vanwege deelname aan een conferentie- de nodige voorbereiding en alertheid.

Cyberveiligheid

- **Digitale dreigingen nemen toe**. Ook de Nederlandse kennisinstellingen zijn regelmatig doelwit van cyberaanvallen. De grootste dreiging gaat uit van statelijke en criminele actoren.
- **Gecoördineerde cyberaanvallen** waarbij staten betrokken zijn, zijn volhardend en kunnen gedurende langere tijd onopgemerkt blijven. Statelijke actoren gebruiken cyberaanvallen ook om **desinformatie** te verspreiden. Bedenk dat ook digitale risico's van bedrijven of diensten (bijvoorbeeld cloud services) waar uw instelling mee werkt kunnen doorwerken naar uw organisatie.
- Om deze dreigingen het hoofd te bieden is het allereerst zaak in **bewustwording** te investeren: menselijk gedrag kan immers alle technische en procedurele maatregelen teniet doen. Het is belangrijk op bestuurlijk niveau aandacht te blijven geven aan cyberveiligheid en risicomanagement zó in te richten dat cyberaanvallen tijdig worden gedetecteerd en bestreden. Voor effectieve crisisafhandeling is **ketensamenwerking** cruciaal voor het herstellen van reguliere onderwijs- en onderzoeksprocessen.

Hoofdstuk 1

Introductie



Hoger onderwijs en wetenschap van wereldklasse kunnen niet zonder internationale samenwerking en wetenschappelijk talent van over de hele wereld. De vooraanstaande positie en goede academische reputatie van de Nederlandse kennisinstellingen hangen samen met de academische vrijheid die in Nederland gegarandeerd wordt en de openheid van onze kennisinstellingen naar de wereld. We hebben veel van onze welvaart te danken aan wetenschappelijke samenwerking. Tegelijkertijd vinden er geopolitieke machtsverschuivingen plaats, waarbij economie, geopolitiek en veiligheid met elkaar verweven zijn. Kennis en innovatie worden in deze context steeds meer gezien als strategisch machtsmiddel dat naast of in combinatie met klassieke middelen, zoals spionage, kan worden ingezet. Deze ontwikkelingen raken iedereen die in de Nederlandse kennissector actief is. Het is dan ook een gezamenlijke opgave om kennisveiligheid beter te borgen.

Waarom deze leidraad?

Voor u ligt de leidraad kennisveiligheid van de Nederlandse kennissector en de Rijksoverheid. De leidraad is een gids voor wie binnen kennisinstellingen te maken heeft met internationale samenwerking en daarbij kansen en (veiligheids) risico's tegen elkaar moet afwegen. Daarbij richten we ons primair op bestuurders van kennisinstellingen. Maar ook voor anderen, zoals veiligheidscoördinatoren, projectleiders en individuele onderzoekers bevat deze leidraad nuttige handvatten. Kan een internationaal samenwerkingsverband leiden tot ongewenste kennisoverdracht? Is er sprake van heimelijke beïnvloeding? Kleven er ethische kwesties aan de samenwerking, bijvoorbeeld doordat de onderzoeksresultaten in het land van de partner misbruikt kunnen worden?

Het doel is om ervoor te zorgen dat internationale wetenschappelijke samenwerking veilig kan plaatsvinden

De leidraad helpt u op weg bij dit soort vragen. Het doel is om ervoor te zorgen dat internationale wetenschappelijke samenwerking veilig kan plaatsvinden, met een goede balans tussen de kansen en risico's, én met respect voor en inachtneming van onze academische kernwaarden door alle betrokken partijen. Bij het nemen van beschermende maatregelen zijn proportionaliteit en maatwerk essentieel. Daarom geldt bij kennisveiligheid het motto 'open waar mogelijk, beschermen waar nodig'.

Wat is kennisveiligheid?

Met kennisveiligheid wordt in deze leidraad in de eerste plaats bedoeld: het voorkomen van ongewenste overdracht van sensitieve kennis en technologie met negatieve gevolgen voor onze nationale veiligheid en de Nederlandse innovatiekracht. Daarnaast gaat het om heimelijke beïnvloedings- en inmengingsactiviteiten van statelijke actoren in hoger onderwijs en wetenschap. Dergelijke beïnvloeding (*foreign interference*) kan leiden tot vormen van (zelf)censuur resulterend in aantasting van de academische vrijheid.

Tot slot draait het bij kennisveiligheid om ethische kwesties die samenhangen met de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd. Zo kunnen onderzoekers van uw instelling betrokken raken bij de ontwikkeling van technologie die in deze landen wordt ingezet bij de onderdrukking van de eigen burgers.

Dreigingen van statelijke actoren gericht tegen kennisinstellingen

Vanuit de intentie om de eigen militaire, technologische, politieke en economische macht te vergroten, zijn verschillende statelijke actoren ook in Nederland actief op zoek naar kennis en technologie.

Sommige van die toepassingen zijn niet verenigbaar met de Nederlandse belangen of druisen in tegen onze fundamentele waarden. Denk daarbij aan toepassingen in conventionele wapenprogramma's en programma's voor massavernietigingswapens (nucleaire, biologische of chemische wapens), inclusief de overbrengingsmiddelen daarvoor (zoals ballistische raketten en onbemande vliegtuigen). Daarnaast gaat het ook over kennis en technologie, die toepasbaar kan zijn binnen (massa)surveillanceprogramma's en voor digitale aanvallen, of over andere sensitieve en opkomende technologieën die een gevaar kunnen vormen voor de nationale veiligheid. Ook kunnen er onwenselijke afhankelijkheden ontstaan.

Ook verwerven statelijke actoren kennis en technologie op manieren die misbruik maken van de openheid van de Nederlandse kennisinstellingen en de in Nederland gegarandeerde academische vrijheid. Daarbij is sprake van een glijdende schaal, waarbij het onderscheid tussen illegale activiteiten, heimelijke intenties en legitieme samenwerking niet altijd eenvoudig te maken is. Soms worden middelen ingezet die illegaal en heimelijk zijn, zoals (digitale) spionage. Soms gaat het om legitieme activiteiten, zoals de internationale uitwisselingen van studenten, onderzoekers of medewerkers, waarbij echter wel sprake is van invloed van een statelijke actor met een heimelijke intentie. En 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. Naast de verwerving van kennis en technologie vinden er in relatie tot kennisinstellingen ook beïnvloedings- en inmengingsactiviteiten plaats door statelijke actoren. Daarbij probeert een actor bijvoorbeeld wetenschappelijk onderzoek te beïnvloeden en publicaties te censureren.

Zie hoofdstuk 3 [↗](#) voor een nadere uitwerking van het dreigingsbeeld.

Een gezamenlijke opgave

Het structureel verhogen van veiligheidsbewustzijn en de weerbaarheid tegen kennisveiligheidsrisico's van de Nederlandse universiteiten, hogescholen en onderzoeksinstituten is van groot belang. Bij de aanpak van kennisveiligheid speelt zelfregulering een centrale rol, uitgaande van de institutionele autonomie van de kennisinstellingen. Dat betekent dat de kennissector zelf -binnen de wettelijke kaders- veiligheidsrisico's monitort, een aanpak formuleert en instrumenten ontwikkelt en zo actief investeert in de weerbaarheid van de kennisinstellingen. Organisaties zoals VH, UNL, KNAW, NWO, NFU en de TO2-federatie, kunnen daarbij een initiërende en faciliterende rol spelen, o.a. door instellingen met elkaar in gesprek te brengen en *best practices* in beeld te brengen en uit te wisselen. Zo beschikken UNL, NWO en de TO2-federatie over eigen werkgroepen kennisveiligheid.

Echter, kennisveiligheid raakt óók aan de nationale veiligheid van ons land. Het beschermen van de nationale veiligheid is een kerntaak van de overheid. Daarom is er ook voor de Rijksoverheid een actieve rol weggelegd. De Rijksoverheid werkt samen met de kennissector om deze handelingsperspectief te bieden zodat kennisinstellingen invulling kunnen geven aan de verantwoordelijkheid die zij op grond van hun -in Nederland wettelijk geborgde- institutionele autonomie hebben. Daarbij gaat het om informeren, meedenken, faciliteren en adviseren. Maar ook om, waar dat vanwege de nationale veiligheid nodig is, kaders stellen en toezien op de naleving daarvan.

Zo is er een Rijksbreed Kennisveiligheidsloket geopend, waar kennisinstellingen terecht kunnen voor expertise en advies.

Rijksbreed Loket Kennisveiligheid

www.loketkennisveiligheid.nl

Om ervoor te zorgen dat kennisinstellingen terecht kunnen bij één centraal punt met vragen over kennisveiligheid is er een Rijksbreed loket kennisveiligheid opgezet. Hierop zijn alle relevante onderdelen van de Rijksoverheid aangesloten. Daardoor kan de brede expertise van de ministeries en diensten beter gedeeld worden met degenen die binnen kennisinstellingen te maken hebben met internationale samenwerking en daarbij tegen dilemma's aanlopen. Het loket kan informatie verstrekken en adviseren. Deze informatie kan de instelling gebruiken bij het maken van de afweging van kansen en risico's.

De basisfuncties van het loket zijn sinds januari 2022 operationeel, waarna in de loop van het jaar verdere doorontwikkeling volgt. Het loket wil het contact met de verschillende ministeries en diensten vereenvoudigen, door één toegangspunt te bieden. Het Kennisveiligheidsloket maakt deel uit van een samenhangend pakket aan maatregelen en initiatieven dat het kabinet eind 2020 aankondigde¹.

De leidraad is bedoeld als een levend document dat als basis kan dienen voor discussies met vakgenoten en experts

Ook deze leidraad is een voorbeeld van de samenwerking tussen de kennissector en de Rijksoverheid om het veiligheidsbewustzijn te versterken. Het is een gezamenlijk initiatief van de Nederlandse kennissector (KNAW, NWO, UNL, VH, NFU en de TO2-federatie) en verschillende onderdelen van de Rijksoverheid (OCW, EZK, NCTV, BZ, AIVD en MIVD). Deze brede samenwerking weerspiegelt dat kennisveiligheid een uitdaging is waarvoor we samen verantwoordelijkheid dragen.

Het dreigingsbeeld is dynamisch en er is toenemende aandacht voor de risico's die daarmee samenhangen. Zowel nationaal als internationaal wordt nieuw beleid ontwikkeld. De leidraad is nadrukkelijk bedoeld als een levend document dat als basis kan dienen voor discussies met vakgenoten en experts en dat op basis van nieuwe ervaringen en inzichten wordt bijgewerkt.

Leeswijzer

In deze leidraad komen alle relevante aspecten rond kennisveiligheid aan bod. We nemen u stap voor stap mee van de verschillende risico's en dreigingen tot het nemen van mitigerende maatregelen en van het uitonderhandelen van goede samenwerkingsovereenkomsten tot het verhogen van de weerbaarheid tegen cyberaanvallen van statelijke actoren.

De leidraad neemt de academische kernwaarden, waaronder academische vrijheid en wetenschappelijke integriteit, als vertrekpunt in hoofdstuk 2. Vervolgens gaat hoofdstuk 3 in op de verschillende risico's en dreigingen die zich kunnen voordoen. Hoofdstuk 4 beschrijft de wettelijke kaders die gelden en de gedragscodes die bedoeld zijn om kennisinstellingen op weg te helpen. In hoofdstuk 5 wordt ingegaan op en het uitvoeren van risicoanalyses, waarbij het identificeren van uw 'kroonjuwelen' en sensitieve kennisgebieden van belang is. Hoofdstuk 6 zet uiteen wat u binnen uw organisatie kunt doen om kennisveiligheid beter te borgen. Hoofdstuk 7 gaat in op het aangaan en beheren van partnerschappen met buitenlandse instellingen en bedrijven en hoofdstuk 8 op de rol die personeelsbeleid en bezoekersbeleid daarbij te spelen hebben. Hoofdstuk 9 gaat in op cyberveiligheid in relatie tot statelijke dreigingen.

Tot slot treft u een bronnenoverzicht en contactenlijst aan, met verwijzingen naar waar u meer informatie kunt vinden over relevante (deel)onderwerpen.

Hoofdstuk 2

Het beschermen van academische kernwaarden



Binnen de kennisector vormen academische kernwaarden zoals academische vrijheid en wetenschappelijke integriteit de toetsstenen van ons handelen. Statelijke dreigingen kunnen ertoe leiden dat deze kernwaarden onder druk komen te staan.

In dit hoofdstuk gaat het om academische vrijheid, wetenschappelijke integriteit en openheid en hoe deze in de knel kunnen komen bij internationale samenwerking. Ook wordt ingegaan op de ethische kant van kennisveiligheid. Tegelijkertijd mag het nemen van maatregelen rond kennisveiligheid nooit tot discriminatie of willekeurige uitsluiting leiden.

2.1 Academische vrijheid en wetenschappelijke integriteit

Onderzoek in Nederland moet worden uitgevoerd in overeenstemming met de nationaal en internationaal aanvaarde normen van wetenschappelijk handelen

Academische kernwaarden zoals academische vrijheid en wetenschappelijke integriteit vormen het fundament voor hoger onderwijs en wetenschap in Nederland.

Onderzoek in Nederland moet worden uitgevoerd in overeenstemming met de nationaal en internationaal aanvaarde normen van wetenschappelijk handelen.

Het respecteren van deze kernwaarden is een voorwaarde om volwaardig mee te draaien in de academische gemeenschap.

Academische vrijheid is essentieel voor goede wetenschapsbeoefening en daarom ook wettelijk geborgd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Wat houdt academische vrijheid in?

Academische vrijheid definieert de KNAW als het beginsel dat medewerkers aan wetenschappelijke instellingen in vrijheid hun wetenschappelijk onderzoek kunnen doen, hun bevindingen naar buiten kunnen brengen en onderwijs kunnen geven. Deze vrijheid geldt onder meer voor:

- de keuze van te onderzoeken thema's,
- de keuze en toepassing van de eigen onderzoeksvragen en -methoden,
- de toegang tot informatiebronnen,
- het publiceren en delen van informatie via conferenties, lezingen en lidmaatschap van wetenschappelijke groepen,
- de keuze om samenwerking met wetenschappelijke partners aan te gaan, en
- de invulling van het wetenschappelijk onderwijs.

De grenzen van academische vrijheid worden bepaald door de mate waarin vijf basisprincipes worden nageleefd: eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid. Verantwoordelijkheid verdient hier bijzondere aandacht. Verantwoordelijkheid betekent onder andere dat onderzoekers zich rekenschap geven van het feit dat zij niet in isolement opereren en daarom, binnen de grenzen van het redelijke, rekening houden met belangen van bij onderzoek betrokken personen, opdrachtgevers en financiers en van de context waarbinnen het onderzoek plaatsvindt. De kennisector verbindt zich eraan ook kennisveiligheid mee te wegen bij internationale wetenschappelijke samenwerking.

De Nederlandse kennissector heeft zich verbonden aan nationale en internationale gedragscodes met betrekking tot wetenschappelijke integriteit. Deze codes zijn daardoor richtinggevend voor onderwijs en wetenschapsbeoefening in Nederland, óók als het gaat om activiteiten met buitenlandse partijen.

Daarmee bieden zij houvast bij het aangaan van internationale partnerschappen of onderzoeksprojecten, bijvoorbeeld bij het opstellen van een samenwerkingscontract met een internationale partner ([zie hoofdstuk 7](#)). Ook betekent het dat buitenlandse (gast)docenten en onderzoekers, wanneer zij in Nederland werken, deze codes zullen moeten onderschrijven en naleven.

Gedragscodes Wetenschappelijke Integriteit

Om duidelijk te maken wat we verstaan onder wetenschappelijke integriteit, heeft het gezamenlijke Nederlandse kennisveld (KNAW, NFU, NWO, TO2-federatie, VH en UNL) een Nederlandse Gedragscode Wetenschappelijke Integriteit vastgesteld². In deze code zijn de vijf principes die de grondslag vormen van integer onderzoek (eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid) uitgewerkt in 61 normen voor goede onderzoekspraktijken. Ook bevat de code richtlijnen voor de manier waarop moet worden omgegaan met veronderstelde schendingen van de wetenschappelijke integriteit.

Daarnaast is er een Europese gedragscode: European Code of Conduct for Research Integrity, uitgewerkt door ALLEA, de Europese Federatie van Wetenschapsacademies waar vanuit Nederland de KNAW bij is aangesloten³. De Europese Commissie erkent deze Code als het referentiedocument voor wetenschappelijke integriteit voor alle door de EU gefinancierde onderzoeksprojecten en als een model voor organisaties en onderzoekers in heel Europa.

Diverse kennisinstellingen beschikken over eigen gedragscodes waarin de interne regels rond wetenschappelijke integriteit en/of veiligheid nader worden uitgewerkt. Zo hebben de Universitaire Medisch Centra zgn. research codes.

Het is belangrijk om niet alleen zuiver wetenschappelijke overwegingen maar ook overwegingen rond kennisveiligheid te betrekken bij het aangaan van internationale samenwerking

Activiteiten van statelijke actoren kunnen ertoe leiden dat academische vrijheid en wetenschappelijke integriteit worden aangetast. De manieren waarop dit zich manifesteert worden beschreven in [hoofdstuk 3](#). Het niet respecteren van academische kernwaarden kan vergaande gevolgen hebben voor de kwaliteit van onderwijs en onderzoek, maar ook voor de wetenschappelijke reputatie en het internationale aanzien van de betrokken onderzoekers en de instelling waarvoor zij werken.

Ook kan heimelijke beïnvloeding van hoger onderwijs en wetenschap door statelijke actoren resulteren in vormen van (zelf)censuur bij studenten en onderzoekers die zich niet meer vrij voelen om mee te praten over bepaalde onderwerpen en daarmee aantasting van de sociale veiligheid.

De gedragscode wetenschappelijke integriteit geeft invulling aan wat integriteit vanuit wetenschappelijk oogpunt inhoudt. Met deze leidraad willen wij u erop attent maken dat het belangrijk is niet alleen zuiver wetenschappelijke overwegingen maar ook overwegingen rond kennisveiligheid te betrekken bij uw afweging over het aangaan van internationale samenwerking.

2.2 Open science

Nederland onderschrijft het Europese streven om met publieke middelen gefinancierde onderzoeksresultaten voor iedereen toegankelijk te maken. Denk aan het open access maken van publicaties en het 'FAIR' (*Findable, Accessible, Interoperable, Reusable*) maken van onderzoeksdata. Het vrijelijk delen van wetenschappelijke inzichten is een belangrijk uitgangspunt van wetenschapsbeoefening en een belangrijke aanjager voor de ontwikkeling van nieuwe kennis en innovaties.

Binnen de Europese Unie is afgesproken dat *open science* de norm wordt in wetenschappelijk onderzoek en deze praktijk wordt al steeds meer gangbaar binnen de kennissector. Dat wil echter niet zeggen dat ook alle internationale partners open science praktiseren. Bovendien kunnen er legitieme redenen zijn om sommige onderzoeksresultaten te beschermen en niet of slechts ten dele openbaar te maken. Denk daarbij aan privacy, nationale veiligheid, intellectueel eigendom en commerciële redenen.

Het is belangrijk om stil te staan bij de vraag of aan onderzoek binnen uw instelling dergelijke aspecten verbonden zijn en, zo ja, welke afspraken daarover gemaakt kunnen worden met uw internationale partners. Zo kunnen er afspraken worden gemaakt in hoeverre data worden gedeeld of alleen kunnen worden ingezien (*data visiting*). Door hierover vooraf goede afspraken te maken kunt u voorkomen dat er later in het proces spanning ontstaat tussen het streven naar maximale openheid enerzijds en de legitieme redenen om beschermende maatregelen te treffen anderzijds.

Er kunnen legitieme redenen zijn om sommige onderzoeksresultaten te beschermen en niet of slechts ten dele openbaar te maken

2.3 Ethiek in de wetenschap

Bij internationale samenwerking kunnen ook ethische dilemma's een rol spelen. Dat kan bijvoorbeeld het geval zijn in de samenwerking met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd. Denk hierbij aan de grondrechten zoals vastgelegd in de Universele Verklaring van de Rechten van de Mens en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

Hoe gaat u om met onderzoek in opdracht van een buitenlandse partij waarvan vermoed kan worden dat deze de technologie zal inzetten om in eigen land minderheden te surveilleren? Ook kan het voorkomen dat onderzoekers uit landen die de grondrechten niet respecteren tijdens hun onderzoek of bij terugkeer in eigen land gedwongen worden om opgedane kennis in te zetten voor doeleinden die indruisen tegen fundamentele normen en waarden.

Het is van belang om daar op alle lagen binnen uw instelling alert op te zijn en te blijven, zowel bij het aangaan van contacten als het verdere verloop van de samenwerking. Veel kennisinstellingen beschikken al over ethische commissies. Denk bijvoorbeeld aan ethische kwesties die kunnen spelen binnen een Universitair Medisch Centrum (UMCs) rond medisch-wetenschappelijk onderzoek

Het is raadzaam om een ethische commissie te hebben waar internationale samenwerkingskwesties waar ethische dilemma's aan kleven kunnen worden gemeld en besproken

met mensen. Een ethische commissie kan daarover adviseren. Het is raadzaam om binnen uw instelling een ethische commissie te hebben waar onderzoekers ook internationale samenwerkingskwesties waar ethische dilemma's aan kleven kunnen melden en bespreken. Een ethische commissie dus die zich niet alleen richt op de wijze van onderzoeksuitoefening, maar ook op de mogelijk onethische toepassing van onderzoeksresultaten.

2.4 Inclusiviteit en non-discriminatie

Nederlandse instellingen voor hoger onderwijs bieden hun studenten een veilige leeromgeving. Kennisinstellingen bieden hun medewerkers, ongeacht hun functie, een veilige werkomgeving. Kennisinstellingen hebben in op het vlak van sociale veiligheid een zorgplicht jegens hun medewerkers en studenten. Voor discriminatie is geen plaats aan Nederlandse kennisinstellingen.

Zorgplicht kennisinstellingen

De zorgplicht voor onderzoekers wordt in de Nederlandse gedragscode wetenschappelijke integriteit als volgt weergegeven: "De instelling zorgt voor een werkomgeving waarbinnen goede onderzoekspraktijken worden bevorderd en gewaarborgd. De instelling zorgt ervoor dat onderzoekers kunnen werken in een veilige, inclusieve en open omgeving, waarin zij zich verantwoordelijk en aanspreekbaar voelen, dilemma's kunnen delen en gemaakte fouten kunnen bespreken zonder bang te hoeven zijn voor de consequenties (blame-free reporting) ... De zorgplichten hebben betrekking op training en supervisie, onderzoekscultuur, databeheer, openbaarmaking en verspreiding en ethische normstelling en procedures."

Veiligheidsmaatregelen moeten altijd objectieverbaar en proportioneel zijn en gerelateerd worden aan een reëel gevaar

Zeker bij een onderwerp als kennisveiligheid, waarbij dreigingsanalyses en risicoprofielen een belangrijke rol spelen, ligt het gevaar op de loer dat de aanpak 'doorslaat' en leidt tot vormen van willekeurige uitsluiting, verdachtmaking en discriminatie. Dat moet te allen tijde voorkomen worden. Getroffen maatregelen moeten altijd objectieverbaar en proportioneel zijn en gerelateerd worden aan een reëel gevaar. Voer hier een open gesprek over binnen uw instelling en neem signalen hierover altijd serieus. Zie ook Nationaal Actieplan voor meer diversiteit en inclusie⁴.

Hoofdstuk 3

Dreigingsbeeld



Om wat voor dreigingen gaat het bij kennisveiligheid? Wat zijn de motieven en de werkwijzen van statelijke actoren? Hoe kunnen academische kernwaarden onder druk komen te staan? In dit hoofdstuk gaan we dieper in op de aard van de dreigingen en hoe deze zich kunnen manifesteren.

3.1 Om welke dreigingen gaat het?

Verschillende statelijke actoren zijn -ook in Nederland- actief op zoek naar kennis en technologie vanuit de intentie om de eigen militaire, politieke en economische macht te vergroten. Nederland loopt het risico dat overgedragen kennis later wordt ingezet voor doeleinden die direct onze nationale veiligheid raken, bijvoorbeeld in de vorm van militaire middelen, of dat deze kennis gebruikt wordt voor doeleinden die indruisen tegen onze fundamentele waarden, zoals voor (massa)surveillancemiddelen.

Nederland loopt het risico dat overgedragen kennis later wordt ingezet voor doeleinden die onze nationale veiligheid raken

Naast de verwerving van kennis en technologie vinden er in relatie tot kennisinstellingen ook beïnvloedings- en inmengingsactiviteiten plaats door statelijke actoren. Daarbij probeert een actor bijvoorbeeld meningen en publicaties te beïnvloeden en wetenschappelijk onderzoek en onderzoeksresultaten te censureren. Een actor kan hiervoor gebruikmaken van een financiële afhankelijkheid. Ook houden sommige actoren hun landgenoten in de gaten om te voorkomen dat zij bijvoorbeeld tijdens colleges of congressen onwelgevallige meningen over het thuisland verkondigen.

De druk van deze activiteiten kan leiden tot zelfcensuur, waarbij individuen en groepen zich niet altijd openlijk kritisch uit durven te laten of academici worden gehinderd om onderzoeksresultaten te publiceren wanneer deze onwelgevallig zijn voor een bepaalde statelijke actor. Dit is een bedreiging van fundamentele vrijheden zoals de vrijheid van meningsuiting en voor academische kernwaarden zoals academische vrijheid en wetenschappelijke integriteit. Hieronder worden de belangrijkste dreigingen nader uitgewerkt.

3.2 Verwerving van kennis en technologie

Overdracht via personen

Statale actoren sturen doelgericht studenten, onderzoekers en medewerkers naar buitenlandse kennisinstellingen, om kennis op te doen waar de statale actor naar op zoek is. Dit gebeurt ook bij Nederlandse kennisinstellingen. Dit kan bijvoorbeeld als onderdeel van een gecentraliseerd aangestuurd talentenprogramma zijn. Maar het kan ook zijn dat de actor voor de financiering van een buitenlandse stageplaats, opleidingsplaats of (tijdelijke) baan een tegenprestatie verlangt in de vorm van terugmelding van de onderzoeksbevindingen, of door het opeisen van het eigenaarschap van de onderzoeksbevindingen. Studenten en onderzoekers maken niet altijd kenbaar dat zij nog nevenactiviteiten of verplichtingen naar andere kennisinstellingen hebben, bijvoorbeeld als onderdeel van eerdergenoemde talentenprogramma's.

Van diverse statelijke actoren is bekend dat zij bereid zijn om hun geëmigreerde (ex-) landgenoten te dwingen mee te werken aan de belangen van die staat

Van diverse statelijke actoren is bekend dat zij bereid zijn om hun geëmigreerde (ex-) landgenoten te dwingen mee te werken aan de belangen van die staat. Buitenlandse studenten, onderzoekers en medewerkers van een Nederlandse instelling kunnen in zo'n geval ongewild gebruikt of misbruikt worden door statelijke actoren voor de overdracht van kennis. In die gevallen wordt druk uitgeoefend op de student, onderzoeker of medewerker in kwestie. Die druk kan verder vergroot worden als naasten, zoals familie en vrienden en collega's, onder druk worden gezet door die statelijke actor.

Individueel op strategische posities binnen de kennisinstelling kunnen vanwege hun eigen kennis, dan wel hun toegang tot kennis, technologie of laboratoria, een interessant doelwit voor statelijke actoren vormen. Statelijke actoren zetten in op de rekrutering van deze personen, waarbij werkwijzen als *social engineering*, omkoping, chantage en intimidatie gehanteerd worden. Afhankelijk van de werkwijze die wordt gehanteerd, is het belangrijk om te beseffen dat een gerekruteerde niet zonder meer uit vrije wil mee werkt met de statelijke actor. In sommige gevallen is de scheidslijn tussen bewust en onbewust meewerken zelfs erg dun; niet altijd is een student, onderzoeker of medewerker zich er van bewust dat hij of zij eigenlijk met een partij samenwerkt die banden heeft met een buitenlandse overheid. Bepaalde vormen van rekrutering, zoals *social engineering*, vinden zeer geleidelijk plaats. Het doelwit wordt langzaam 'binnengehaald', over een soms langere periode, tot een moment dat de gerekruteerde geen weg meer terug heeft.

Statale actoren werven en faciliteren (praktisch en financieel) actief talentvolle studenten en wetenschappers om in hun land te komen studeren of te werken. Dit kan bijvoorbeeld aantrekkelijk worden gemaakt door het verstrekken van beurzen en het creëren van gunstige onderzoeksfaciliteiten met bijvoorbeeld gespecialiseerde grote innovatiecentra. Niet zelden doet een statelijke actor dit in nauwe en afgestemde samenwerking met onderzoeksinstituten uit eigen land, die met behulp van door de actor geleverde staatssteun een wetenschapper goede arbeidsvoorwaarden en hoogwaardige onderzoeksfaciliteiten kan bieden. Daarbij bestaat er een risico dat onderzoeksresultaten of –gegevens, afkomstig uit onderzoek dat door de Nederlandse kennisinstelling is opgezet en/of gefinancierd, door een statelijke actor worden gekopieerd.

Studenten, onderzoekers en medewerkers van kennisinstellingen kunnen, net als elk ander potentieel doelwit dat beschikt over waardevolle gedigitaliseerde kennis en informatie, doelwit worden van digitale spionageactiviteiten van een statelijke actor. Van diverse statelijke actoren is door de inlichtingen- en veiligheidsdiensten onderkend dat zij een offensief cyberprogramma hebben dat ook gericht is tegen Nederlandse belangen. Deze landen bevinden zich ook in de voorhoede als het gaat om (economische) spionage. Sommige statelijke actoren voeren omvangrijke en structurele spionagecampagnes, gericht op het verkrijgen van hoogwaardige kennis en technologie. Wanneer deze kennis en technologie te vinden is bij specifieke personen, zoals onderzoekers en medewerkers van een kennisinstelling, zullen spionageactiviteiten op hen worden gericht. Met (*spear*)*phishing*-aanvallen gericht op een concreet doelwit kan dan bijvoorbeeld getracht worden toegang tot systemen en bestanden te krijgen.

Van diverse statelijke actoren is onderkend dat zij een offensief cyberprogramma hebben dat ook gericht is tegen Nederlandse belangen

Overdracht via samenwerkingsverbanden

In verschillende landen werken statelijke actoren nauw samen met onderzoeksinstellingen. Soms behoren kennisinstellingen, zoals universiteiten, zelfs direct tot de overheid. Dat betekent dat de statelijke actor, in ruil voor financiële steun of vanwege officiële zeggenschap, ook een bepalende stem heeft welke (internationale) samenwerkingsverbanden de instelling aangaat. Dergelijke samenwerkingen kunnen ingezet worden als verlengstuk van het eigen overheidsbeleid, bijvoorbeeld ten behoeve van de ontwikkeling van het militaire apparaat, de verbetering van digitale aanvallen en voor gebruik in massasurveillance.

Het kan zijn dat de band tussen kennisinstelling en statelijke actor niet duidelijk is, wat voor een Nederlandse kennisinstelling in de praktijk kan betekenen dat een ogenschijnlijk academische samenwerking een dubbele agenda heeft. De connectie met een kennisinstelling, via financiering of via zeggenschap, geeft de statelijke actor de mogelijkheid een claim te leggen op onderzoeksresultaten of intellectueel eigendom.

Het kan zijn dat de band tussen kennisinstelling en statelijke actor niet duidelijk is, wat kan betekenen dat een ogenschijnlijk academische samenwerking een dubbele agenda heeft

3.3 Beïnvloedings- en inmengingsactiviteiten

Sommige statelijke actoren zetten middelen in om invloed uit te kunnen oefenen op de wijze waarop zij internationaal gezien en begrepen worden, of worden geportretteerd. Ook doen bepaalde statelijke actoren pogingen om mondiale legitimatie te zoeken voor hun beleid. Vanuit deze optiek kunnen studenten, onderzoekers en medewerkers in de Nederlandse wetenschap (hoger en academisch onderwijs), denktanks en kennisinstellingen doelwit zijn van statelijke actoren, ter beïnvloeding van meningen en publicaties en het censureren van wetenschappelijk onderzoek en onderzoeksresultaten. Het gaat dan bijvoorbeeld om (studenten, onderzoekers en medewerkers van) instituten waar onderzoek wordt gedaan naar voor een statelijke actor onwelgevallige onderwerpen (zoals mensenrechtenschendingen), of onderwerpen waarvan de statelijke actor bang is dat er onwelgevallige bevindingen over worden gepubliceerd. Bij deze activiteiten kan het voorkomen dat een actor gebruik maakt van financiële middelen die worden ingezet als stimulans of juist als drukmiddel.

Daarnaast zijn er statelijke actoren die er baat bij hebben om zicht en greep te houden op hun landgenoten, bijvoorbeeld om te voorkomen dat zij 'dissidente' of onwelgevallige geluiden laten horen over het herkomstland. Vanuit deze optiek kunnen ook studenten, onderzoekers en medewerkers van kennisinstellingen een doelwit van statelijke actoren vormen, bijvoorbeeld wanneer zij een studie volgen of les geven over potentieel onwelgevallige onderwerpen.

Tot slot kunnen wetenschappelijke experts aantrekkelijk zijn voor statelijke actoren om te dienen als geloofwaardige spreekbuis, wanneer zij, uit hoofde van hun expertise, standpunten kunnen uitdragen die in lijn zijn met de belangen van de actor. Zij worden bijvoorbeeld uitgenodigd om in bepaalde buitenlandse media een stuk te schrijven of om op symposia te spreken.

Wetenschappelijke experts kunnen aantrekkelijk zijn als geloofwaardige spreekbuis wanneer zij standpunten uitdragen die in lijn zijn met de belangen van de actor

Hoofdstuk 4

Juridische kaders en gedragscodes



Er zijn zowel nationaal als internationaal juridische kaders en gedragscodes die bijdragen aan de veiligheid van Nederland. Voor de wet- en regelgeving geldt dat compliance een verplichting is voor uw instelling. Het zijn de 'harde' kaders waarbinnen samenwerking met internationale partners dient plaats te vinden. We gaan in op exportcontrole en sanctieregimes maar ook op wetgeving die in voorbereiding is. Daarnaast is er aandacht voor de verschillende gedragscodes die er binnen de kennisector zijn uitgewerkt en die richtinggevend zijn en u kunnen helpen bij het maken van afwegingen.

4.1 Exportregels voor dual-use producten en technologie

Bij het aangaan van een internationale samenwerking zijn Europese exportregels met betrekking tot *dual-use* producten en technologie relevant. Daarbij gaat het om goederen, software en technologie die worden gebruikt voor civiele doeleinden, maar die militaire toepassingen kunnen hebben of kunnen bijdragen aan de productie of verspreiding van massavernietigingswapens zoals kernwapens, chemische strijdgassen of biologische wapens, of overbrengingsmiddelen daarvoor.

Er gelden op grond van de EU *dual-use* verordening⁵ strenge regels voor de uit- en doorvoer van deze producten en technologie. Een vergunning is verplicht voor uitvoer naar landen buiten de Europese Unie en in sommige gevallen voor de overdracht binnen Europa. Soms vallen ook producten en technologie waar u het in eerste instantie niet van verwacht onder de *dual-use* regels (bijvoorbeeld bepaalde frequentieomzetter), omdat ze gebruikt kunnen worden in de proliferatie van bijvoorbeeld massavernietigingswapens. Ook is het begrip 'export' zeer veelomvattend: in feite gaat het om alle vormen van overdracht, ongeacht het middel. Dus ook via e-mail of een clouddienst⁶.

Bij 'export' gaat het om alle vormen van overdracht, ongeacht het middel. Dus ook via e-mail of een clouddienst

Het is daarom belangrijk dat u alert blijft op potentieel ongewenst gebruik van uw onderzoek, kennis of technologie en het delen hiervan. Instellingen zijn zelf verantwoordelijk voor de naleving van deze EU-regels en overtreding kan -nog los van de veiligheidsrisico's die dat met zich meebrengt- leiden tot vervolging van de betrokkenen.

De exportcontroleregels gelden niet voor *basic scientific research*, oftewel: fundamenteel wetenschappelijk onderzoek. Maar waar eindigt fundamenteel onderzoek en begint toegepast onderzoek? Een hulpmiddel dat u daarbij kunt gebruiken is de *Technology Readiness Level* (TRL) methodiek. Dat is een schaal van 1 t/m 9 die economische toepasbaarheid van de technologie uitdrukt en die ook binnen Horizon Europe wordt gebruikt. Niveaus 1 en 2 gelden als fundamenteel wetenschappelijk onderzoek, niveaus 3 en 4 moeten van geval tot geval bekeken worden en niveaus 5 en hoger zijn toepassingsgericht en vallen dus mogelijk onder exportcontrole. Er zijn diverse hulpmiddelen om het TRL-niveau van onderzoek te bepalen, zie bijvoorbeeld de 'TRL Assessment Tool' van de Canadese overheid die ook goed toepasbaar is voor de Europese situatie⁷.

Een andere factor om te bepalen of er sprake is van fundamentele wetenschap is de financieringsbron van het onderzoeksproject: als er sprake is van (volledige) financiering door een bedrijf dan bestaat de kans dat het onderzoek gericht is op commerciële ontwikkeling van technologie. Het kan een indicatie zijn dat de onderzoeksresultaten die zo'n onderzoeksproject oplevert niet vallen binnen de definitie van fundamenteel wetenschappelijk onderzoek en dat exportcontrole er dus mogelijk op van toepassing is.

Een tweede voor de wetenschap relevante uitzonderingsgrond op de regels voor exportcontrole is of het om technologie gaat die zich al 'in het publieke domein' bevindt. Dat houdt in dat de technologie toegankelijk is voor iedereen die dat wil, ongeacht of er kosten in rekening worden gebracht of dat een registratie verplicht is. Denk hierbij aan klassieke regeltechniek of aerodynamica.

Voor de exportcontroles gebruikt de Nederlandse overheid de Europese lijst voor dual-use producten en technologie. De verantwoordelijkheid om op de hoogte te zijn van eventuele dual-use classificatie ligt bij uw instelling. Als u iets wilt exporteren dat op deze lijst staat, moet daarvoor een vergunning worden aangevraagd. Er is een praktische EU-aanbeveling voor kennisinstellingen beschikbaar over het inrichten van interne compliance procedures⁸.

Om welke technologie gaat het?

De EU-regelgeving rond exportcontrole is zeer gedetailleerd en daarmee niet eenvoudig te doorgronden voor leken. Om toch een indruk te geven van de kennisvelden die eronder kunnen vallen hieronder de 10 categorieën waarin dual-use producten en technologie zijn onderverdeeld:

- Nucleaire goederen
- Speciale materialen en aanverwante apparatuur
- Materiaalverwerking
- Elektronica
- Computers
- Telecommunicatie en "informatiebeveiliging"
- Sensoren en lasers
- Navigatie en vliegtuigelektronica
- Zeewezen en schepen
- Ruimtevaart en voortstuwing

Bij het maken van een risico-inschatting is de eindgebruiker een belangrijke factor

Bij het maken van een risico-inschatting is de eindgebruiker een belangrijke factor. In voorkomende gevallen kan er om een eindgebruikersverklaring gevraagd worden. Dit is een door de eindgebruiker ondertekend document waarin hij verklaart dat hij de goederen niet anders dan voor civiele doeleinden zal gebruiken. De eindgebruikersverklaring wordt ook wel een End User Statement (EUS) genoemd.

Bij twijfel of vragen kunt u contact opnemen met de Centrale Dienst voor In- en Uitvoer (CDIU)⁹. Ook kunt u hier een indelingsverzoek indienen als u niet zeker weet of de goederen, software, technologie of diensten die u voornemens bent te exporteren onder de dual-use wetgeving vallen. De CDIU en het ministerie van Buitenlandse Zaken maken een risico-inschatting van iedere vergunningaanvraag.

Ook organiseert het ministerie van Buitenlandse Zaken tweemaal per jaar een seminar over exportcontrole voor bedrijven en kennisinstellingen die hier meer over willen weten.

Voor de levenswetenschappen is *biosecurity* relevant. Wetenschappelijk onderzoek naar risicovolle ziekteverwekkers is essentieel voor het ontwikkelen van diagnostiek, vaccins en therapieën. Maar de onderzoeksresultaten kunnen ook worden misbruikt. Om kennisinstellingen te helpen om deze vorm van dual-use tegen te gaan is bij het RIVM Bureau Biosecurity¹⁰ ingesteld als kennis- en informatiepunt van de overheid over biosecurity. Een deel van de site richt zich specifiek op onderzoekers. Hier zijn o.a. een online tool om potentiële dual-use aspecten van onderzoek te identificeren en de *biosecurity* gedragscode van de KNAW te vinden.

4.2 Internationale sanctieregimes

Als er dreiging is voor de internationale vrede en veiligheid, bijvoorbeeld als gevolg van schending van het internationale recht of van mensenrechten, kunnen de Verenigde Naties (VN) en de Europese Unie (EU) sancties opleggen tegen landen, organisaties, bedrijven en individuele personen die nodig zijn om de internationale veiligheid te handhaven of te herstellen. Sancties kunnen gericht zijn op het tegengaan van verspreiding van kernwapens, maar ook tegen landen, personen en organisaties die mensenrechten schenden of tegen personen die betrokken zijn bij terroristische activiteiten. Sanctiemaatregelen zijn dwingend: overtreding van een sanctieregeling is een strafbaar feit. Actuele informatie over de geldende sanctieregimes is te vinden op de website www.sanctionsmap.eu.

Bijzondere aandacht in dit verband verdienen de VN- en EU-sancties tegen Noord-Korea en Iran, die de overdracht van bepaalde technologie en kennis naar deze landen verbieden.

Sanctiemaatregelen zijn dwingend: overtreding van een sanctieregeling is een strafbaar feit

Sancties tegen Noord-Korea en Iran

*In het geval van **Noord-Korea** hebben de sancties betrekking op o.a. de overdracht van kennis die kan bijdragen aan proliferatiegevoelige activiteiten van Noord-Korea of aan de ontwikkeling van systemen voor de overbrenging van kernwapens. In dit kader besluit de overheid op grond van de Sanctieregeling Noord-Korea 2017 of een ontheffing verleend kan worden om een persoon toegang te verlenen tot gespecialiseerde kennis.*

*In het geval van **Iran** is er een verbod op de overdracht van goederen en technologie die kan bijdragen aan de ontwikkeling van onder meer het ballistische raketprogramma en het verlenen van technische bijstand met betrekking tot deze goederen en technologie voor gebruik in Iran. Denk bijvoorbeeld aan gasturbinemotoren, keramische poeders, composieten met bepaalde eigenschappen en oxidatoren geschikt voor raketmotoren. Ook is er tegen een aantal kennisinstellingen sancties ingesteld omwille van hun bijdragen aan proliferatiegevoelige activiteiten. Samenwerken met deze kennisinstellingen is niet toegestaan. Samenwerking met personen die indirect, of in het verleden hebben gewerkt bij gesanctioneerde instelling moeten op individuele basis beoordeeld worden. De lijst vindt u terug in bijlagen VIII, IX, XIII en XIV van de Iran-verordening¹¹.*

Op grond van deze sancties geldt op een aantal vakgebieden aan Nederlandse kennisinstellingen ‘verscherpt toezicht’, wat inhoudt dat iedereen die er toegang toe wil door de overheid wordt getoetst. Deze toetsing geldt ongeacht de nationaliteit, dus ook voor Nederlanders, en zo lang als de internationale sancties van kracht zijn. Er wordt uitsluitend getoetst bij onderwijs- en onderzoeksgebieden waar een risico bestaat op overtreding. U vindt de lijst met vakgebieden waarop verscherpt toezicht van toepassing is hier op de website van de Rijksoverheid¹².

In geval van twijfel of vragen over geldende sanctieregimes, kunt u contact opnemen met de Centrale Dienst In- en Uitvoer (CDIU) van de Douane.

Beleid in ontwikkeling

De beleidsontwikkeling op het terrein van kennisveiligheid is volop in beweging. Om het handelingsperspectief en de weerbaarheid van Nederlandse kennisinstellingen, bedrijven en overheden te vergroten zijn diverse maatregelen in voorbereiding. Hierna worden twee relevante initiatieven vanuit het kabinet kort toegelicht. Daarbij dient benadrukt te worden dat de het gaat om voorstellen die nog door de Kamer behandeld moeten worden.

Toetsingskader ongewenste kennis- en technologieoverdracht

Om het veiligheidsbewustzijn en de weerbaarheid van de Nederlandse kennissector verder te verhogen heeft het kabinet eind 2020 een samenhangend pakket aan maatregelen en initiatieven aangekondigd¹³. Daarbij ligt er veel nadruk op zelfregulering binnen de sector, in lijn met de autonomie van de kennisinstellingen.

Op vakgebieden waar de risico's voor de nationale veiligheid het grootst zijn, acht het kabinet zelfregulering niet afdoende. Daarom werkt het kabinet aan een toetsingskader voor personen die toegang willen tot deze specifieke vakgebieden. De vormgeving en reikwijdte van het toetsingskader zijn nog onderwerp van overleg, waarbij het kabinet ook het kennisveld betreft. Het kabinet streeft ernaar dat dit toetsingskader in de loop van 2023 van kracht zal worden en dan in de plaats komt van het bestaande verscherpt toezicht (zie hiervoor).

Wet veiligheidstoets investeringen, fusies en overnames

Ook via buitenlandse investeringen in, overnames van, of fusies met Nederlandse bedrijven kan een statelijke actor sensitieve kennis bemachtigen. Om te voorkomen dat dergelijke verwervingsactiviteiten een risico vormen voor de nationale veiligheid, is de Wet veiligheidstoets investeringen, fusies en overnames (Wet Vifo) in voorbereiding. Deze wet zal zich richten op vitale aanbieders en bedrijven die beschikken over sensitieve technologie. Dit wetsvoorstel is in juni 2021 ter behandeling aangeboden aan de Tweede Kamer.

Het is niet waarschijnlijk dat kennisinstellingen bij de uitoefening van hun onderzoeks- en onderwijstaken met deze wet te maken krijgen. Niettemin hebben kennisinstellingen soms een aandelenbelang in bijvoorbeeld startups van (oud-)studenten of medewerkers. Verwervingsactiviteiten in deze bedrijven kunnen binnen de reikwijdte van de investeringstoets vallen.

4.3 Gedragscodes kennisveiligheid

**Gedragscodes
zijn niet-bindend,
maar wel
richtinggevend**

Gedragscodes zijn in de regel niet-bindend, maar wel richtinggevend. Het is een passend instrument voor de kennissector, die zich kenmerkt door een hoge mate van autonomie en zelfregulering.

UNL kennisveiligheidskader

Om universiteiten te ondersteunen bij de besluit- en beleidsvorming rond kennisveiligheid heeft UNL een kader kennisveiligheid voor universiteiten opgesteld¹⁴. De tekst vormt een kader waar de Nederlandse universiteiten zich aan committeren en waarbinnen zij zelf invulling geven aan hun instellingsbeleid.

Het kader gaat in op kansen en risico's van internationale samenwerking, op governance en beleidskaders en doet concrete aanbevelingen rond risicomanagement. Daarmee stelt het universiteiten in staat goed geïnformeerde en onderbouwde beslissingen te nemen over internationale samenwerkingen.

EU guidelines on tackling R&I foreign interference

De Europese Commissie heeft richtsnoeren uitgewerkt gericht op het tegengaan van buitenlandse inmenging binnen de Europese kennissector¹⁵. Ze zijn geschreven voor een brede doelgroep: nationale autoriteiten, onderzoeksinstellingen en -organisaties, instellingen voor hoger onderwijs en individuele onderzoekers en ander personeel van kennisinstellingen. De Europese richtsnoeren zijn nadrukkelijk bedoeld als basis en inspiratiebron voor veiligheidsbeleid van lidstaten, veldorganisaties en instellingen.

De richtsnoeren omvatten vier thema's: waarden, governance, partnerschappen en cyberveiligheid. Per thema wordt een integrale aanpak gepresenteerd, met daarbij voorbeelden van mogelijke maatregelen die genomen kunnen worden.

Kennisveiligheid in andere landen

Ook andere landen nemen maatregelen om kennisveiligheid te verhogen. In diverse landen worden er richtsnoeren en checklists ontwikkeld. Deze initiatieven dienen hetzelfde doel als de Nederlandse leidraad kennisveiligheid, namelijk om inzichtelijk te maken waar op gelet moet worden bij internationale samenwerking en een beeld te krijgen van de eigen weerbaarheid en handelingsperspectieven. Voorbeelden hiervan zijn: Australië¹⁶, Duitsland¹⁷, het Verenigd Koninkrijk¹⁸, Zweden¹⁹ en Canada²⁰.

Het feit dat zowel de EU als individuele partnerlanden dergelijke teksten kennen, maakt het bij samenwerking makkelijker om het gesprek erover te voeren: ook onze partners zijn op zoek naar manieren om binnen het hoger onderwijs en de wetenschap alertheid en weerbaarheid tegen statelijke dreigingen te vergroten.

Hoofdstuk 5

Het inschatten van risico's



Dit hoofdstuk biedt een aantal handvatten om risico's voor ongewenste kennisoverdracht in kaart te brengen. Hierbij spelen de volgende drie factoren een belangrijke rol: de inhoud van het onderzoek, het land waar de betrokken samenwerkingspartner gevestigd is en de samenwerkingspartner zelf. Deze factoren hangen met elkaar samen en dienen integraal bekeken te worden bij het inventariseren van risico's.

5.1 Welke kennisgebieden binnen uw instelling hebben een verhoogd risico?

Bij een effectieve risicobeperking is het van belang om sensitieve kennisgebieden nauwkeurig te identificeren. Voor deze kennisgebieden geldt dat er risico's voor de nationale veiligheid samenhangen met ongewenste kennisoverdracht.

Te denken valt aan kennis die specifiek voor militaire toepassingen ontwikkeld wordt of aan dual-use technologieën (zie paragraaf 4.1 [↗](#)). De lijst met dual-use technologieën biedt goede handvatten, maar is niet uitputtend: ook kennisgebieden die buiten de reikwijdte van de exportcontrole vallen, kunnen sensitief zijn. Denk bijvoorbeeld aan (deelterreinen binnen) kunstmatige intelligentie, geavanceerde robotica en kwantumtechnologie. Daarbij kan meespelen dat er sprake is van een verhoogd risico op onethische toepassing van onderzoeksresultaten, zoals rond (massa)surveillanceprogramma's.

Deze risico's zijn nog groter op gebieden waarop Nederland een unieke kennispositie heeft of omdat de technologie raakt aan de continuïteit van vitale processen in Nederland en/of Nederland ervan afhankelijk is doordat er geen bruikbaar alternatief voorhanden is. In deze context wordt wel gesproken van 'kroonjuwelen': de sensitieve kennisgebieden waarop uw instelling een reputatie heeft opgebouwd en waar onderzoek wordt verricht dat internationaal geldt als excellent.

U kunt per sensitief kennisgebied een korte risicoanalyse uitvoeren, niet alleen vanwege de nationale veiligheid, maar ook vanwege de veiligheid van uw medewerkers en waarborging van de academische kernwaarden en de reputatie van uw instelling. Stel uzelf daarbij de vraag of het (voorgenomen) onderzoek potentieel ongewenst of onethisch kan worden ingezet en/of onze nationale veiligheid kan raken, bijvoorbeeld vanwege militaire of onethische toepassing van de onderzoeksresultaten.

Ga voor uzelf na waar binnen uw instelling de gevoelige kennis zich bevindt, welke dreigingen er spelen en welke maatregelen u hiertegen kunt nemen

Ga voor uzelf na waar binnen uw instelling de unieke, gevoelige kennis zich bevindt, welke dreigingen er spelen en welke maatregelen u hiertegen kunt nemen om deze dreigingen af te wenden. Bedenk daarbij dat een technologie door technologische ontwikkelingen in de loop van de tijd meer of minder sensitief kan worden. Het is daarom raadzaam om te werken met een dynamische lijst met sensitieve kennisgebieden die periodiek wordt herzien.

Bij het uitvoeren van risicoanalyses binnen uw instelling kan de accountmanager van de AIVD met u meedenken.

5.2 Welke landen hebben een verhoogd risico?

Bij welke landen moet u extra opletten en misschien wel extra maatregelen treffen als u gaat samenwerken met een daar gevestigde partner? Wat kunt u zelf doen om een inschatting te maken van de risico's?

Het is verstandig uit te gaan van een risicomanagementbeleid dat gericht is op dreigingen, ongeacht uit welk land ze komen. Indien u zou besluiten uw beleid uitsluitend op enkele 'risicolanden' te richten, dan heeft dat belangrijke nadelen. Niet alleen ziet u dan dreigingen over het hoofd vanuit andere landen waardoor u alsnog risico loopt, maar ook kan het ertoe leiden dat alles wat aan de gekozen 'risicolanden' verbonden is op voorhand verdacht wordt gemaakt. Dat laatste is slecht voor de wetenschap en in strijd met het non-discriminatie beginsel.

Als u een inschatting wilt maken van het risicoprofiel van een land, kunt u gebruikmaken van openbaar beschikbare dreigingsinformatie. Zo hebben NCTV, AIVD en MIVD begin 2021 een gezamenlijk 'Dreigingsbeeld Statelijke Actoren' gepubliceerd²¹. Ook de jaarverslagen van AIVD²² en MIVD²³ bevatten actuele dreigingsinformatie. En kijk bijvoorbeeld op www.sanctionsmap.eu om te zien tegen welke landen er sancties gelden (zie ook paragraaf 4.2 ↗).

Daarnaast kunt u relevante internationale ranglijsten en indices van NGO's, onderzoeksinstituten en internationale organisaties raadplegen. Een slechte score op dergelijke overzichten moet alarmbellen doen afgaan. Kijk bijvoorbeeld naar hoe het gesteld is met de academische vrijheid, vrijheid in het algemeen, democratie en respect voor de rechtsstaat. De hier genoemde overzichten zijn illustratief; waar het om gaat is dat u uw risico-oordeel staft en onderbouwt.

Voorbeelden van internationale ranglijsten en indices

- *Academic Freedom Index*: <https://www.gppi.net/2021/03/11/free-universities>
- *Freedom in the World Report* van Freedom House: <https://freedomhouse.org/report/freedom-world>
- *Democracy Index* van The Economist Intelligence Unit: <https://www.eiu.com/n/campaigns/democracy-index-2020/>
- *World Justice Project Rule of Law Index* van World Justice Project: <https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2020>

Scoort een land slecht op dergelijke ranglijsten, dan betekent dat niet per se dat u niet kunt samenwerken met instellingen uit dit land. Ook met onderzoekers uit dergelijke landen kan in principe worden samengewerkt, mits u de juiste voorzorgsmaatregelen treft en u zich rekenschap geeft van de context waarbinnen de beoogde partner opereert.

U kunt contact opnemen met het [loket kennisveiligheid](#) van de Rijksoverheid als u meer wilt weten over het risicoprofiel van specifieke landen. Dit loket staat in verbinding met alle relevante onderdelen van ministeries en diensten, waaronder de landenexperts van Buitenlandse Zaken en RVO.

5.3 Ken uw samenwerkingspartners, opdrachtgevers en financiers

Bij het aangaan of verlengen van een overeenkomst is het van belang dat de betrokken onderzoeker of projectleider zich verdiept in de achtergrond van de buitenlandse partnerorganisatie of opdrachtgever. *Due diligence* is de term die daar internationaal voor gebruikt wordt. Wat is de wetenschappelijke reputatie van de instelling? Wie zijn er precies bij het project betrokken? Hoe zit het met de kosten? Het is van belang dat u daarbij óók stilstaat bij kennisveiligheid.

Goed beschouwd is het altijd goed om daar op te letten, maar het is pure noodzaak bij instellingen of bedrijven afkomstig uit landen met een hoog risicoprofiel (zie paragraaf 5.2 ↗) en bij samenwerkingen op sensitieve kennisgebieden (zie paragraaf 5.1 ↗). Ook hier geldt overigens dat het er niet om gaat op voorhand instellingen of bedrijven categorisch uit te sluiten. Het betekent dat de betrokken medewerkers zich bewust zijn van de risico's en dreigingen en bewust maatregelen treffen om deze te voorkomen.

Daarvoor hoeft hij of zij geen veiligheidsexpert te zijn: met alertheid en open bronnen kan men al een eind komen. Het gaat erom scherp te letten op signalen die erop kunnen wijzen dat er iets niet in de haak is. Denk bijvoorbeeld aan een partner waarover amper informatie is te vinden op internet en die bij niemand bekend is. Als de beoogde partner al wel bekend is binnen uw organisatie of bij collega's van andere instellingen kan navraag gedaan worden. Welke ervaringen hebben zij? Zijn er incidenten geweest? De veiligheidscoördinator van uw instelling kan helpen bij het op tafel krijgen van dit soort informatie. Enkele voorbeelden van factoren waar u op kunt letten:

- Is de partner verbonden aan de overheid? Denk bijvoorbeeld aan staatsgeleide bedrijven of instellingen.
- Is de partner verbonden aan het leger of de defensie-industrie?
- Zijn er sancties op de partner van toepassing?
- Heeft de instelling een aantoonbare reputatie op het vakgebied waar het om gaat? Als expertise ontbreekt of onduidelijk is hoe de beoogde samenwerking aansluit op de normale activiteiten van de partner dan is dat een reden tot alertheid.
- Wat voor onderzoek doen de bij de samenwerking betrokken onderzoekers nog meer? Zijn zij verbonden aan meerdere instellingen/organisaties?
- Het contact verloopt met een andere entiteit (andere naam, ander adres) dan de partnerorganisatie zelf, of wordt gaande het proces veranderd.
- De partner geeft geen duidelijke antwoorden op vragen over de beoogde toepassing van de onderzoeksuitkomsten of maakt om onduidelijke redenen bezwaar tegen bepalingen die standaard zijn in overeenkomsten of stelt excessieve geheimhoudingsbepalingen voor.

Ook zijn er gespecialiseerde onderzoeksbureaus actief, die veiligheidsgerelateerde analyses maken die nuttig kunnen zijn. Denk bijvoorbeeld aan de *China Defense Universities Tracker* van het Australische ASPI²⁴.

Bij opdrachtgevers en onderzoeksfinanciers geldt iets vergelijkbaars als bij onderzoekspartners. Daarbij maakt het in beginsel niet uit om wat voor soort financier het gaat, het kan bijvoorbeeld ook gaan om schenkingen van donateurs. Het begint met basale vragen als: waar komt het geld dat de partner wil investeren vandaan en wat zouden de motieven van de partner kunnen zijn om het onderzoek te financieren? Heeft de financier economische of politieke belangen bij een bepaalde uitkomst van het onderzoek? Enkele voorbeelden van factoren waar u op kunt letten:

- Er is weinig tot geen informatie te vinden over de opdrachtgever of financier (geen website etc.).
- Er wordt gebruik gemaakt van een entiteit die atypisch is voor dit soort onderzoeksfinanciering.
- De opdrachtgever of financier stelt uitzonderlijk grote bedragen beschikbaar of stelt bijzonder gunstige financieringsvoorwaarden voor en vraagt daar amper iets voor terug.
- De opdrachtgever of financier wil niet dat resultaten worden gepubliceerd, stelt uitzonderlijk strenge intellectuele eigendomseisen of bedingt geheimhouding t.a.v. eindgebruikers en specificaties.

Bedenk dat u ook stap voor stap in een situatie van (financiële) afhankelijkheid terecht kunt komen

Bedenk daarbij dat u ook stap voor stap in een situatie van (financiële) afhankelijkheid terecht kunt komen. Met de projecten en activiteiten afzonderlijk is dan weinig mis, maar bij elkaar opgeteld geven ze de financier een positie die hem in staat stelt de samenwerking en de inhoud ervan te sturen. De financier kan uw instelling en/of de betrokken onderzoekers persoonlijk onder druk zetten zowel via positieve prikkels (in het vooruitzicht stellen van beloningen) als via negatieve prikkels (bedreigingen).

Als u inschat dat aan de beoogde samenwerkingspartner, opdrachtgever of financier veiligheidsrisico's verbonden zijn, is het van belang dat de veiligheidscoördinator van uw organisatie wordt betrokken. Samen met hem/haar kunnen vervolgstappen worden overwogen. De uiteindelijke beslissing over het aangaan van de samenwerking, valt onder de verantwoordelijkheid van het centrale gezag van uw organisatie (bij universiteit: College van Bestuur). Bij dat besluit worden veiligheidsrisico's expliciet meegewogen, als onderdeel van het partneracceptatiebeleid van de instelling.

Wij raden u aan contact op te nemen met het loket kennisveiligheid van de Rijksoverheid. Het loket kan informatie en expertise die binnen de ministeries en diensten van de Rijksoverheid aanwezig is delen en meedenken over mogelijke mitigerende maatregelen die u kunt treffen. [Paragraaf 7.1](#) [↗](#) gaat verder in op waar u op zou moeten letten bij het aangaan van internationale samenwerkingsverbanden.

Hoofdstuk 6

Risicomanagement



Kennisveiligheid doet een groot beroep op de verantwoordelijkheid die kennisinstellingen op grond van hun institutionele autonomie hebben. Binnen de instelling is risicomangement een gezamenlijke opgave, waar de hele organisatie zich verantwoordelijk voor moet voelen. Het doel is steeds ervoor te zorgen dat het kennisveiligheidsbewustzijn tot in de haarvaten van uw instelling doordringt. In dit hoofdstuk komen verschillende aspecten aan de orde die bijdragen aan een veiligheidscultuur en daarmee aan de weerbaarheid van uw organisatie.

Binnen een kennisinstelling is het bestuur eindverantwoordelijk voor risicomangement. Dat geldt ook voor de risico's samenhangend met kennisveiligheid. Kennisinstellingen dienen daarom interne procedures en protocollen te hebben, zodat zij risico's tijdig signaleren en adresseren.

Het is van belang te onderstrepen dat deze leidraad nadrukkelijk niet gelezen moet worden als oproep om alle risico's uit de weg te gaan. Het is echter wel essentieel om een goed begrip te hebben van de bestaande dreigingen en risico's en om deze op een effectieve manier te beheersen. Dit hoofdstuk biedt hiervoor een aantal handvatten gerelateerd aan governance en interne procedures.

6.1 Organiseer risicomangement binnen uw organisatie

Kennisinstellingen, en zeker universiteiten, kenmerken zich door een gelaagde bestuursstructuur. Zowel op centraal instellingsniveau als op decentraal niveau (d.w.z. faculteiten, vakgroepen, onderzoeksgroepen en de individuele onderzoekers) is actie nodig. Daarom is het belangrijk dat duidelijk wordt afgesproken wie waarvoor verantwoordelijk is. Vanuit het uitgangspunt dat het bestuur van de kennisinstelling eindverantwoordelijkheid draagt, betekent dit dat het bestuur beslisbevoegdheden mandateert. Het is aan te raden om dergelijke mandatering formeel vast te leggen. Dat maakt ook dat in geval van incidenten of onregelmatigheden snel kan worden geschakeld.

Net zoals bij andere vormen van veiligheid (denk aan cyberveiligheid en sociale veiligheid) is het belangrijk om centraal een aantal standaard processen in te regelen. Dat kunt u doen aan de hand van hetgeen er in de vorige hoofdstukken is beschreven. Heeft u alle dreigingen in beeld ([hoofdstuk 3](#))? Hoe zit het met de compliance binnen uw organisatie (geldende wet- en regelgeving en gedragscodes, [hoofdstuk 4](#))? Weet u wat de sensitieve kennisgebieden van uw organisatie zijn en op welke landen u (extra) alert moet zijn als het gaat om statelijke dreigingen ([hoofdstuk 5](#))?

Het is zaak al deze factoren en overwegingen om te zetten in stappenplannen die rekening houden met de specifieke kenmerken van uw organisatie. Risicomangement is maatwerk. Afhankelijk van het risiconiveau zijn de benodigde risicoanalyses en controles strikter en ligt de beslissingsbevoegdheid op een hoger, centraler niveau binnen de organisatie.

Afhankelijk van het risiconiveau zijn de benodigde risicoanalyses en controles strikter en ligt de beslissingsbevoegdheid op een hoger, centraler niveau binnen de organisatie

Bij dit alles zijn twee belangrijke kanttekeningen te maken. Allereerst: bij het uitwerken van kennisveiligheidsmaatregelen is proportionaliteit essentieel: er moet een gezonde verhouding zijn tussen de dreiging en risico's enerzijds en de getroffen maatregelen anderzijds. Dat het nemen van te weinig maatregelen onwenselijk is, spreekt voor zich. Maar ook het treffen van te veel en/of te ingrijpende maatregelen kan nadelig uitpakken. Denk aan bureaucratie door een overdaad aan controle en wantrouwen. Maar denk ook aan aantasting van uw academische reputatie als openheid en toegankelijkheid al te zeer worden beperkt. Het adagium 'open waar mogelijk, beschermen waar nodig' vat het belang van proportionaliteit goed samen.

Een tweede kanttekening betreft het risico op onterechte bejegening en discriminatie van studenten en medewerkers uit bepaalde landen. Geborgd moet worden dat bewustwording over de risico's niet doorslaat in vijandsbeelden of in willekeurige uitsluiting van bepaalde groepen studenten en medewerkers. Academische waarden van vrijheid, respect en het open academisch gesprek moeten uitgedragen en voorgeleefd worden, zeker ook in de opleiding van onderzoekers en het onderwijs in den brede.

6.2 Organisatorische maatregelen

Uiteindelijk is het doel te komen tot een integraal veiligheidsbeleid op instelling-niveau; een veiligheidsbeleid waarin de verschillende vormen van veiligheid (sociale veiligheid, cyberveiligheid en kennisveiligheid) samenkomen. Maar om daar te komen, is het als eerste stap nodig bewustzijn over kennisveiligheid te creëren en het thema bestuurlijk te verankeren.

Concreet begint dit met het aanwijzen van een bestuurlijk trekker of portefeuillehouder voor het thema kennisveiligheid. Gelet op het strategische en geopolitieke karakter ervan, zou het een vergissing zijn kennisveiligheid puur als een bedrijfsvoeringskwestie te beleggen. Het vergt aandacht van het bestuursniveau.

Vervolgens is het aan te raden dat de portefeuillehouder kennisveiligheid wordt bijgestaan en geadviseerd door een intern Adviesteam Kennisveiligheid, d.w.z. een team van enkele deskundigen met uiteenlopende expertises. In de kern kan gedacht worden aan: (1) de veiligheidscoördinator of adviseur integrale veiligheid; (2) een expert op het gebied van informatiebeveiliging, bijvoorbeeld de Chief Information Security Officer (CISO); en (3) een deskundige op het gebied van internationalisering/ internationale samenwerking. Afhankelijk van de casuïstiek kan daar andere expertise aan worden toegevoegd, zoals een HR-adviseur. Dit adviesteam heeft bij voorkeur een formeel mandaat om het bestuur gevraagd en ongevraagd te informeren en adviseren over kennisveiligheidsissues. Met name voor kleinere kennisinstellingen kan het interessant zijn om bepaalde expertise, bijvoorbeeld met betrekking tot bepaalde landen of kennisvelden, te bundelen en te werken met een *shared service*.

Het is van belang te werken met vertrouwenspersonen of ombudsfunctionarissen en over een goede klokkenluidersregeling te beschikken

In algemene zin is het van belang dat er binnen uw organisatie een open veiligheidscultuur bestaat (zie hierna, paragraaf 6.5 ↗). In aanvulling daarop is het van belang te werken met vertrouwenspersonen of ombudsfunctionarissen en over een goede klokkenluidersregeling te beschikken. Dit zorgt ervoor dat medewerkers vermoedens van illegale of onethische praktijken binnen de instelling (anoniem en in vertrouwen) kunnen melden. Medewerkers die zorgen hebben over kennisveiligheid, bijvoorbeeld bij een te optimistisch beoordeelde samenwerkingsovereenkomst, moeten weten dat zij bij een vertrouwenspersoon terecht kunnen om die zorgen te bespreken. De vertrouwenspersonen en ombudsfunctionarissen zelf moeten goed op de hoogte zijn van risico's rond kennisveiligheid en hun kennis hierover periodiek bijspijkeren.

Zoals hiervoor al beschreven (zie paragraaf 2.3 ↗) is het raadzaam binnen uw instelling een ethische commissie te hebben die kan adviseren over kwesties die samenhangen met een mogelijke toepassing van onderzoeksresultaten in andere landen die indruist tegen fundamentele normen en waarden, zoals mensenrechten.

NB: wanneer de onderzoeksuitkomsten waarschijnlijk een militaire toepassing krijgen in het land van de partner waarmee u samenwerkt, dan gaat het niet alleen om ethische overwegingen, maar ook om de juridische verplichtingen die voortvloeien uit Europese exportregelgeving (zie paragraaf 4.1 ↗) of internationale sanctieregimes (zie paragraaf 4.2 ↗). Overtreding van deze regels is een strafbaar feit.

6.3 Zorg voor een accurate feitenbasis voor besluitvorming

Het is belangrijk dat er centrale overzichten beschikbaar zijn van samenwerkingen met partners en opdrachtgevers van buiten de EU

In het kader van internationaliseringsbeleid worden al cijfers bijgehouden over o.a. studentenmobiliteit en internationale promovendi. Het is belangrijk dat dergelijke centrale overzichten ook beschikbaar zijn van samenwerkingen met partners en opdrachtgevers van buiten de EU. Een dergelijk up-to-date overzicht vormt de basis voor effectief risicomanagement. Een bestuur (voor een universiteit of hogeschool: College van Bestuur) hoort te allen tijde inzicht te hebben in de significante samenwerkingen die de organisatie aangaat, zonder daarvoor de betrokken partijen binnen de organisatie nog te moeten consulteren.

Op het bestuursniveau ontstaat er hiermee een dashboard, een centraal overzicht van veiligheidsgevoelige partnerschappen, financiering en buitenlandse promovendi en gastonderzoekers. Bijkomstig voordeel van zo'n centraal overzicht, is dat u ook zicht heeft op het cumulatief effect waardoor -alles bij elkaar opgeteld- een onwenselijke afhankelijkheid kan ontstaan. Bijvoorbeeld wanneer vooral met één instelling wordt samengewerkt of wanneer financiering hoofdzakelijk van één opdrachtgever of financierer komt. Wanneer u een dergelijke onwenselijke ontwikkeling signaleert kunt u, waar nodig, tijdig bijsturen.

Ook kunnen de geregistreerde gegevens op geaggregeerd niveau gebruikt worden als feitenbasis voor jaarlijkse rapportages, bijvoorbeeld via het jaarverslag, over kennisveiligheid.

6.4 Fysieke en digitale beschermingsmaatregelen

Naast organisatorische en administratieve maatregelen kunnen ook tamelijk eenvoudige maatregelen in de fysieke omgeving effectief zijn. Welke gebouwen zijn vrij toegankelijk en voor welke verdiepingen of ruimtes geldt een restrictief toegangsbeleid? Zorg dat op plekken, zoals labs, waar sensitief onderzoek wordt gedaan alleen diegenen toegang hebben die bij het onderzoek betrokken zijn.

Zorg dat op plekken waar sensitief onderzoek wordt gedaan alleen diegenen toegang hebben die bij het onderzoek betrokken zijn

Dat geldt evenzeer voor onderzoeksgegevens. Wie heeft er binnen het systeem toegang toe? Welke gegevens en resultaten moeten ook voor niet bij het onderzoek betrokken vakgenoten en collega's worden afgeschermd? Het (digitaal) afschermen van gegevens en deze alleen toegankelijk maken voor personen die geautoriseerd zijn is een effectieve en relatief eenvoudige manier om ongewenst weglekken ervan te voorkomen.

Heeft u binnen uw instelling te maken met zeer sensitieve onderzoeksdata of -resultaten dan valt te overwegen om te werken met rubricering van documenten. Dat betekent dat documenten worden ingedeeld in een gevoeligheidsklasse, zoals 'vertrouwelijk' of 'geheim'. Door het aanbrengen van rubriceringen op documenten weet iedere medewerker de gevoeligheid van de informatie en de daaraan gekoppelde maatregelen. Het draagt eraan bij dat iedereen binnen de organisatie dezelfde 'taal' spreekt als het gaat om vertrouwelijkheid van informatie en verkleint daarmee de kans dat gevoelige kennis weglekt.

ABDO: Algemene Beveiligingseisen voor Defensieopdrachten

Defensie werkt samen met bedrijven en enkele instellingen voor toegepast onderzoek. Wanneer zij omgaan met gevoelige informatie, moeten zij voldoen aan de veiligheidseisen van Defensie. Deze staan in de Algemene Beveiligingseisen voor Defensieopdrachten 2019, ABDO 2019²⁵. De MIVD controleert of een bedrijf of instelling zich houdt aan de ABDO en medewerkers die toegang hebben tot staatsgeheime informatie, dienen in het bezit te zijn van een geldige Verklaring van Geen Bezwaar. Een bedrijf of instelling kan alleen een ABDO-autorisatie krijgen als het een staatsgerubriceerd contract aangaat met Defensie.

De kennisinstellingen die met ABDO te maken hebben, beschikken over zeer robuuste risicomangementprocessen. Daardoor kunnen zij een inspiratiebron vormen voor kennisinstellingen die weliswaar geen defensieopdrachten uitvoeren maar wel hun interne procedures en processen willen verstevigen.

6.5 Veiligheidscultuur: bewustwording en alertheid

Het creëren van een open veiligheidscultuur binnen uw organisatie is essentieel als het gaat om bewustzijn (incident- en risicodetectie) en weerbaarheid. Mensen moeten open en in vertrouwen met elkaar over mogelijke risico's kunnen spreken en ervan doordrongen zijn dat interne veiligheidsprocedures er niet voor niks zijn. Bied ruimte voor het uiten van zorgen en denk actief mee over wat er kan worden verbeterd. Het mag niet iets zijn waar alleen de bestuurders en de veiligheidscoördinator het over hebben.

Zeker in de initiële fase, waarin het bewustzijn nog beperkt is, kunnen campagnes een nuttige bijdragen leveren. Zo kunt u ervoor zorgen dat de boodschap van deze leidraad wordt overgebracht op een manier die aansluit bij de behoeften van uw organisatie.

Bewustwording is echter nooit een eenmalige exercitie: doorlopende aandacht is nodig om iedereen scherp te houden en ook nieuwe medewerkers mee te krijgen. Ook is kennisveiligheid -en het denken daarover- volop in beweging waardoor het belangrijk is kennis up-to-date te houden.

Daarbij kunt u gebruikmaken van input en expertise die binnen de rijksoverheid en organisaties als UNL en de TO2-federatie voorhanden is. Zij kunnen bijvoorbeeld een platform bieden waar u van ervaringen binnen andere kennisinstellingen kunt leren en wellicht nuttige instrumenten en checklists kunt overnemen.

**Bewustwording
is nooit een
eenmalige
exercitie:
doorlopende
aandacht is nodig
om iedereen
scherp te houden
en ook nieuwe
medewerkers mee
te krijgen**

Zorg er bij een bewustwordingscampagne altijd voor dat deze is toegesneden op de beoogde doelen en doelgroepen (onderzoekers, projectleiders, ondersteunende diensten, ...). Sluit zo veel mogelijk aan bij hun belewingswereld. Een effectieve campagne gebruikt meerdere kanalen en ingangen. Denk bijvoorbeeld aan informeren via posts op intranet, e-mails en e-learning modules en interactieve bijeenkomsten en teamsessies. Ook simulaties, waar (fictieve) casuïstiek wordt doorlopen, zijn zeer geschikt om houdings- en gedragsaspecten te trainen.

Denk ook na over wie de boodschap binnen de organisatie overbrengt. Essentieel is dat het management het goede voorbeeld geeft en uitstraalt kennisveiligheid belangrijk te vinden. In aanvulling daarop kunnen bijvoorbeeld 'ambassadeurs' binnen de organisatie worden aangewezen die de boodschap actief verder verspreiden. Tot slot kunnen er vanuit de Rijksoverheid briefings verzorgd worden. Afhankelijk van de insteek kan gedacht worden aan experts van OCW, EZK, BZ, NCTV, AIVD of MIVD. Voor meer informatie kunt u contact opnemen met het loket kennisveiligheid van de Rijksoverheid.

Hoofdstuk 7

Internationale partnerschappen, inkopen en aanbesteden



Binnen het risicomanagement van uw kennisinstelling verdienen overeenkomsten met buitenlandse partners bijzondere aandacht. Door ‘aan de voorkant’ duidelijke afspraken te maken kunt u bepaalde risico’s mitigeren én heeft u iets om op terug te vallen in gevallen dat het toch mis dreigt te gaan. Ook aan inkopen en aanbesteden kunnen risico’s rond kennisveiligheid kleven. Risico’s waar u -mits u ze tijdig signaleert- maatregelen tegen kunt nemen.

7.1 Waar u op moet letten bij het aangaan van een samenwerking

Samenwerking met buitenlandse instellingen of bedrijven kan op allerlei manieren ontstaan, soms heel informeel en vrijblijvend via persoonlijke contacten van onderzoekers. Echter, op het moment dat er inhoudelijke of financiële toezeggingen worden gedaan, is het belangrijk de afspraken ergens vast te leggen. Een gangbare vorm om een partnerschap te sluiten is via een Memorandum of Understanding (MoU). Een samenwerking kan ook de vorm aannemen van een onderzoeksopdracht die door een buitenlandse opdrachtgever aan een kennisinstelling wordt gegund.

We hebben het hier over alle vormen van samenwerking, van formeel tot informeel, van breed tot specifiek. Samenwerkingsovereenkomsten vormen een goed aangrijpingspunt voor het afwegen van kansen en risico’s. Het sluiten of verlengen van een overeenkomst of het aanvaarden van een opdracht is bij uitstek een geschikt moment om een risicoanalyse uit te voeren en eventuele risico’s te mitigeren.

Het sluiten of verlengen van een overeenkomst is bij uitstek een geschikt moment om een risicoanalyse uit te voeren en risico’s te mitigeren

Wanneer uw instelling of een onderdeel daarvan een samenwerking aangaat met een buitenlandse kennisinstelling of een buitenlands bedrijf, dan is het allereerst van belang grondig te onderzoeken met wie u precies in zee gaat (zie paragraaf 5.3 [↗](#)). Vervolgens is het zaak duidelijke afspraken te maken, afspraken die risico’s rond kennisveiligheid, academische kernwaarden en onethisch gebruik van onderzoeksresultaten zo veel mogelijk voorkomen. Op die manier heeft u gedurende de looptijd van de samenwerking altijd iets om op terug te vallen als zich onwenselijke ontwikkelingen voordoen. U kunt dan uw samenwerkingspartner erop aanspreken en, als de risico’s blijven voortbestaan, de samenwerking vroegtijdig beëindigen (exit strategie).

Er zijn talloze formats en standaardovereenkomsten in omloop. Uw organisatie hanteert vast ook dergelijke sjablonen. Die bieden een zekere basisbescherming tegen de meest voorkomende juridische en financiële risico’s. Echter, heeft de samenwerking betrekking op een sensitief kennisgebied met een partner uit een land met een verhoogd risicoprofiel, dan volstaan dergelijke standaardbepalingen waarschijnlijk niet. Maatwerk is in deze gevallen aangewezen en u wordt aangeraden juridische en veiligheidsexpertise in te schakelen. Het zou goed zijn als uw organisatie in dergelijke gevallen een specifieke procedure kent (zie ook hoofdstuk 6 [↗](#)). In sommige gevallen kan de conclusie zijn dat samenwerking niet mogelijk is, ook niet met een goed contract. Dat is het geval wanneer de restrisico’s niet acceptabel zijn voor de verantwoordelijke risico-eigenaar (veelal het college van bestuur).

In sommige gevallen kan de conclusie zijn dat samenwerking niet mogelijk is, ook niet met een goed contract

Zaken waar u in elk geval scherp op moet zijn:

- Is duidelijk omschreven wie de partners precies zijn? Worden er geen entiteiten opgevoerd die u niet kent of waarvan de betrokkenheid onduidelijk is?
- Zijn de gebieden waarop de samenwerking betrekking heeft goed afgebakend? Daarmee kunt u voorkomen dat gedurende het project de aandacht van de partner verschuift naar een terrein dat sensitief is.
- Wie draagt welke kosten? Bedenk daarbij dat als de buitenlandse partij bijvoorbeeld alle kosten voor personeel en onderzoeksfaciliteiten voor zijn rekening neemt, er daarmee een afhankelijkheid wordt gecreëerd. U verliest zeggenschap ('wie betaalt, bepaalt') en het wordt lastiger om de overeenkomst op te zeggen, vanwege de grote implicaties.
- Gaat de overeenkomst uit van wederkerigheid (reciprociteit)? Denk met name aan de toegankelijkheid en gebruik van onderzoeksdata. Maar denk ook aan vertrouwelijkheids- en geheimhoudingsbepalingen en bepalingen over disseminatie en publicatie.
- Is Nederlands recht van toepassing op de samenwerking? Bedenk bijvoorbeeld dat academische kernwaarden, zoals academische vrijheid en institutionele autonomie, in Nederland wettelijk zijn geborgd in de Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW).
- Beding dat het onderzoek wordt uitgevoerd in overeenstemming met internationaal aanvaarde normen van wetenschappelijk handelen, zoals neergelegd in (inter)nationale gedragscodes, zoals de Nederlandse Gedragscode Wetenschappelijke Integriteit ([zie paragraaf 2.1 ↗](#)).
- Bevat de overeenkomst eenduidig geformuleerde ontbindende voorwaarden? Deze bepalingen geven u het recht de samenwerking vroegtijdig te beëindigen als zich zaken voordoen die voor u niet door de beugel kunnen. Ook een bepaling over geschillenbeslechting (*dispute settlement*), is wenselijk.
- Ga na welk niveau van toegang wenselijk is voor de partner. Tot welke gebouwen, informatie of intern netwerk krijgt de partner toegang? Wat wordt met de partner gedeeld? Wordt toegang gegeven tot een volledig product of tot een 'light' versie zonder gevoeligheden.
- Ga na of de samenwerking betrekking heeft op *dual use*-technologie ([zie paragraaf 4.1 ↗](#)). Is dat het geval, dan is een eindgebruikersverklaring wenselijk. Dit is een door de eindgebruiker ondertekend document waarin hij verklaart dat hij de goederen niet anders dan voor civiele doeleinden zal gebruiken. De eindgebruikersverklaring wordt ook wel een *End User Statement (EUS)* genoemd.

Is de overeenkomst eenmaal gesloten, dan komt het erop aan de gemaakte afspraken leidend te laten zijn. Dat vergt regelmatig overleg met de samenwerkingspartner waarbij er niet alleen aandacht is voor de inhoudelijke voortgang, maar ook voor de *manier waarop* de samenwerking vorm krijgt. Knelpunten en incidenten moeten daarbij vroegtijdig worden aangekaart en geadresseerd. Het verdient aanbeveling om periodieke evaluaties van de samenwerking in te bouwen en daarbij de onderwerpen voor evaluatie vooraf te identificeren.

Samenwerkingsovereenkomsten lopen vaak stilzwijgend door na de initiële looptijd. Wanneer de samenwerking zonder grote problemen heeft plaatsgevonden, is de neiging om geen aandacht te besteden aan zo'n verlengingsmoment. Bij samenwerkingen met een verhoogd risico (vanwege het kennisveld, de samenwerkingspartner en/of het land waar deze partner gevestigd is) is dat onverstandig en wordt u geadviseerd uw interne organisatie zó in te richten dat u ruim voor het verlengmoment wordt gealerteerd en de samenwerking nog eens kritisch tegen het licht kunt houden. Mogelijk hebben zich sinds het afsluiten van de overeenkomst ontwikkelingen voorgedaan die extra mitigerende maatregelen of scherpere afbakeningen nodig maken.

7.2 Kennisveiligheid bij inkopen en aanbesteden

Aan sommige aanbestedingen zijn veiligheidsrisico's verbonden. Dit hangt af van het type product of dienst dat wordt geleverd, de opdrachtgever en het bedrijf dat de opdracht wordt gegund. Afhankelijk hiervan kan er bijvoorbeeld het risico ontstaan dat hoogwaardige of gevoelige kennis en informatie weglekt, vitale bedrijfsprocessen worden verstoord en strategische afhankelijkheden ontstaan. Denk bijvoorbeeld aan de aanbesteding van uw digitale infrastructuur, clouddiensten en software of de vervanging van systemen waar veel persoonsgegevens op staan. Daarnaast is voor sommige inkoopopdrachten fysieke toegang tot gevoelige locaties nodig, waarbij het goed is om beschermende maatregelen te treffen.

Bij een aanbesteding is het daarom zaak om eerst in kaart te brengen of dit soort risico's aanwezig zijn. Risico's kunnen gesignaleerd worden met behulp van de quickscan nationale veiligheid bij inkoop en aanbesteden²⁶. Dit instrument is ontwikkeld voor de Rijksoverheid en de vitale sector maar dient ook ter inspiratie voor andere sectoren. De quickscan bestaat uit een aantal vragen om snel te kunnen bepalen of er met de opdracht risico's worden gevormd voor de nationale veiligheid of dat er eventueel nader onderzoek nodig is om dit te bepalen. Als uit de quickscan blijkt dat er mogelijk risico's zijn, wordt een risicoanalyse uitgevoerd. In een risicoanalyse wordt precies vastgesteld welke risico's er zijn en hoe kan worden gehandeld om deze risico's te mitigeren. Hierbij dient zowel inhoudelijke expertise ten aanzien van de opdracht als juridische (aanbestedingsrechtelijke) expertise betrokken te worden. Vervolgens kunnen er aanbestedingsrechtelijke maatregelen worden getroffen of kunnen er in de opdracht (product/dienstverlening) zelf maatregelen worden genomen.

Te denken valt aan de volgende vragen:

- Is de te contracteren opdrachtnemer ingericht op de informatie waar ze mee moeten werken?
- Weet de opdrachtnemer wat ze moeten doen als beveiligingsincidenten zich voordoen en voldoen ook de onderaannemers aan de beveiligingseisen voor de opdracht?
- Kan er met de samenwerking of overeenkomst met een dergelijk bedrijf een strategische afhankelijkheid ontstaan?

- Kan er gevoelige informatie (zoals persoonsgegevens) weglekken?
- Kan de continuïteit van de levering in gevaar komen en wat zou dit voor gevolgen hebben?
- Komt personeel in aanraking met gevoelige informatie?
- Wat gebeurt er met de informatie na beëindiging van het contract?

Wanneer er een beeld is geschetst van de potentiële risico's van een opdracht kunnen er maatregelen worden getroffen. Te denken valt aan het stellen van aanvullende contracteisen of andere maatregelen gericht op risicomanagement (zie [hoofdstuk 6](#) ↗) en het verhogen van de digitale weerbaarheid ([hoofdstuk 9](#) ↗).

Hoofdstuk 8

De rol van personeelsbeleid



Het is belangrijk om veiligheidsbewustzijn onderdeel te maken van uw personeelsbeleid. Daarnaast is er aandacht nodig voor houdings- en gedragsaspecten: het veiligheidsbewustzijn moet gaan leven op de werkvloer. Het management en de projectleiders zijn verantwoordelijk voor de begeleiding en hebben een voorbeeldfunctie.

8.1 Veiligheidscheck bij werving en selectie

Voor uw instelling is het belangrijk dat op het gebied van personeelsbeleid een goede samenwerking en communicatie bestaat tussen de vacaturehouder op decentraal niveau (bijvoorbeeld bij een faculteit) en de HR-afdelingen op decentraal (facultair) en op centraal niveau. De vacaturehouder is verantwoordelijk voor de vakinhoudelijke match, maar dient ook op de hoogte te zijn van bestaande kennisveiligheidsrisico's en hier tijdens de sollicitatieprocedure, inclusief mogelijke interviews, rekening mee te houden.

Bij werving en selectie van nieuwe medewerkers is het belangrijk dat de HR-afdeling de academische kernwaarden zoals beschreven in gedragscode wetenschappelijke integriteit onderstreept. Immers, er zijn landen waar kennisinstellingen onder direct bewind van de autoriteiten vallen en waar principes als eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid niet worden nageleefd.

Het is van belang dat HR-medewerkers veiligheidsbewust zijn. Zij zijn het eerste aanspreekpunt voor nieuwe medewerkers en kunnen signalen opmerken in cv's of netwerken van nieuwe medewerkers. Hebben ze bijvoorbeeld gewerkt aan instellingen in landen met een verhoogd risico? Of zijn er andere onverklaarbare gaten in cv's die verklaard dienen te worden tijdens een sollicitatiegesprek, waar de HR-adviseur de personen die dit gesprek voeren op kan wijzen? Heeft de kandidaat een gastaanstelling in het buitenland bij een instelling waar twijfels over zijn of opvallende nevenfuncties?

Afhankelijk van de aard van de risico's kan bij bepaalde functies een VOG worden vereist. Bij het aanvragen van een VOG kan op specifieke functieaspecten worden getoetst die relevant zijn voor het werk dat de nieuwe medewerker uit gaat voeren. Houd er rekening mee dat een VOG alleen terugkijkt over een periode van 4 jaar en dat voor een VOG alleen Nederlandse systemen worden geraadpleegd. Dat zegt dus weinig over buitenlandse onderzoekers die nog maar net in Nederland zijn. In sommige gevallen kan een met een VOG vergelijkbare verklaring vanuit het buitenland uitkomst bieden.

Ook kan bij werving gebruik gemaakt worden van een integriteitstest die meet of:

1. gedrag van de kandidaat in lijn is met regels en algemeen geldende waarden, ook wanneer er druk uitgeoefend wordt of regels onduidelijk zijn;
2. de kandidaat zich niet door oneigenlijke motieven laat leiden, maar door het algemeen belang. En dat hij of zij zich niet laat verleiden regels niet toe te passen of te ruim te interpreteren;
3. de kandidaat consistent is in zijn of haar gedrag en daarvoor verantwoordelijkheid neemt.

Het is van belang dat HR-medewerkers veiligheidsbewust zijn

Overigens is het raadzaam ook bij uitdiensttreding van personeel dat met sensitieve kennis of technologie werkt te voorzien in een vorm van 'nazorg'. Dit kan bestaan uit het onderhouden van contact met de betrokkene. Ook kunnen de geheimhoudingsbepalingen in de arbeidsovereenkomst zodanig geformuleerd worden dat deze ook na uitdiensttreding van kracht blijven.

8.2 Opleiding en training

Zorg ervoor dat iedereen adequate training en/of informatie krijgt om veiligheidgerelateerde uitdagingen te herkennen en de juiste actie te ondernemen. U kunt hierbij denken aan:

- Standaard relevante informatie en regelingen opnemen in het welkomspakket en een (verplichte) module of briefing over kennisveiligheid aanbieden aan nieuwe medewerkers en evt. ook studenten die met gevoelige kennis/technologie gaan werken;
- Het aanbieden van opfrimodules die worden gegeven aan het begin van een nieuw onderzoeksproject om te zorgen dat het bewustzijn van de projectleden op peil is;
- Het inrichten van een platform op het intranet waar medewerkers informatie kunnen vinden en waar zij hun kennis en alertheid kunnen testen (*self assessment*);
- Het opzetten van een speciaal trainingsprogramma voor gastonderzoekers en -studenten uit landen met een verhoogd risicoprofiel gericht op de academische kernwaarden.

8.3 Buitenlandse bezoekers en dienstreizen naar het buitenland

Ongewenste kennisoverdracht kan plaatsvinden in het kader van een meerjarig onderzoeksproject, waarbij de buitenlandse onderzoekers gedurende langere tijd in Nederland werken. Het is ook mogelijk dat deze juist plaatsvindt bij kortstondige contacten. Dan hebben we het over buitenlandse bezoekers in Nederland, zoals deelnemers aan een conferentie of gastdocenten of -onderzoekers. Omdat er in deze gevallen geen arbeidsrelatie is, is screening vooraf geen optie en gaat het erom de risico's tijdens het bezoek aan sensitieve locaties te beperken.

Het is raadzaam een bezoekersprotocol uit te werken, waarin wordt beschreven hoe om te gaan met buitenlandse bezoekers in het algemeen en die vanuit landen met een verhoogd risicoprofiel in het bijzonder. Daarbij kan het gaan om onderzoekers, maar denk ook aan vertegenwoordigers van bedrijven of overheden. Bezoekersbeleid heeft alleen nut als er daarnaast ook fysieke en digitale maatregelen worden getroffen om de locaties te beschermen.

Het is raadzaam een bezoekersprotocol uit te werken

Bouwstenen voor een bezoekersprotocol

- *Laat bezoekers en delegaties uit het buitenland zich altijd vooraf aanmelden door de medewerkers die deze bezoekers willen ontvangen. Zonder aanmelding vooraf geen toegang. Zorg er daarnaast voor dat alle bezoekers zich bij binnenkomst identificeren en registreren en bij de receptie worden opgehaald.*
- *Weet waar bepaalde bezoekers wel mogen rondlopen en waar niet zodat van tevoren kan worden beoordeeld of een bezoek op een bepaalde plek kan doorgaan.*
- *Kondig bezoek in gevoelige ruimtes vooraf aan bij collega's, zodat zij hier rekening mee kunnen houden.*
- *Laat uw bezoekers nooit alleen (vooral niet op sensitieve plekken). Begeleid hen te allen tijde op uw locaties.*
- *Maak duidelijk dat het niet is toegestaan om foto's of video's te maken op locatie zonder uw toestemming of zorg dat alle apparatuur op sensitieve locaties opgeborgen is (bijvoorbeeld in een kluis).*
- *Stel van te voren vast wat u wel en niet met de bezoeker gaat (en mag) delen en blijf tijdens het bezoek en het bespreken van informatie weg van onderwerpen die met beveiliging van informatie of locaties te maken hebben.*
- *Voor zeer gevoelige onderzoeken/plekken/locaties is het beter om geen bezoekers te ontvangen, of om bezoekers van landen met een verhoogd risicoprofiel uit te sluiten.*

Daarnaast is het verstandig om een protocol te hebben voor het omgekeerde scenario, waarbij u vanwege uw werk een ander land bezoekt. Zeker indien dat een land is met een verhoogd risicoprofiel vanuit het oogpunt van kennisveiligheid en de onderzoeker in kwestie onderzoek doet op een terrein dat binnen uw instelling als kroonjuweel (zie [paragraaf 5.1 ↗](#)) geldt en daarmee voor dit land interessant is, vergt dat de nodige voorbereiding en alertheid.

Dat geldt in allerlei gevallen, denkt u bijvoorbeeld aan een scenario waarbij u wordt uitgenodigd als keynote spreker en u daarbij flink wordt gefêteerd (luke hotel, diners, ...). Dat kan oprechte gastvrijheid zijn. Maar helaas kan het in bepaalde landen ook een doelbewuste poging zijn van actoren -die u misschien niet eens te zien krijgt- om iets van u gedaan te krijgen.

Bouwstenen voor een protocol bij dienstreizen naar landen met een verhoogd risicoprofiel

Voordat u vertrekt

- *Zorg dat u een minimale hoeveelheid (vertrouwelijke) gegevens bij u heeft.*
- *Bedenk vooraf wat er op de gegevensdragers staat die u meeneemt. Bevat uw laptop bestanden met gevoelige informatie, terwijl u deze niet nodig heeft tijdens uw reis? Verplaats deze bestanden dan naar een andere computer voor u vertrekt of neem een andere (reis)laptop mee.*
- *Idem voor uw mobiele telefoon. Wis de belgeschiedenis van uw telefoon voor vertrek of neem een andere (reis)telefoon mee op reis.*
- *Gebruik wachtwoorden en/of toegangscode voor uw devices en schakel ze waar mogelijk uit: wanneer ze aanstaan, bent u extra kwetsbaar.*

Als u onderweg bent

- Schakel de bluetooth functie van uw telefoon en laptop altijd uit.
- Neem vertrouwelijke informatie en gegevensdragers altijd mee in uw handbagage en niet in uw koffer (denk aan usb-sticks, telefoons).
- Wees voorzichtig met vertrouwelijke gesprekken aan boord van een vliegtuig, trein of andere publieke ruimten. Sommige (vliegtuig)maatschappijen hebben bijvoorbeeld nauwe banden met inlichtingen- en veiligheidsdiensten maar denk ook aan de medepassagiers.

Op de plek van bestemming

- Bescherm vertrouwelijke informatie. Laat geen vertrouwelijke gegevens achter op een plaats waar anderen ze kunnen inzien. Dit geldt ook voor uw hotelkamer of hotelkluis.
- Geef uw laptop of telefoon niet zomaar af en zorg ervoor dat u altijd kunt controleren of iemand uw informatie heeft ingekeken.
- Verstrek selectief informatie. Ga bij contacten uit van het need-to-know-principe: vertel uw gesprekspartner niet meer dan noodzakelijk. Dit geldt ook voor congressen of bijeenkomsten waar u voor uitgenodigd wordt om te spreken.
- Wees voorzichtig met verkregen (gratis) USB's op congressen of evenementen. Dit is een makkelijke manier om malware te installeren op uw laptop.

Zie ook de AIVD-brochure 'Op reis naar het buitenland – Veiligheidsrisico's onderweg'²⁷

Voor degenen die werkzaam zijn op een kennisgebied dat zeer sensitief is en/of regelmatig in landen met een verhoogd risicoprofiel zijn, kan het verstandig zijn een HEAT-training ("Hostile Environment Awareness Training") te volgen of een reisbriefing van de AIVD aan te vragen. Dit kan via het loket kennisveiligheid van de Rijksoverheid.

Hoofdstuk 9

Cyberveiligheid in relatie tot statelijke dreigingen



De digitale dreigingen nemen toe, door onder meer (statelijke) actoren en (beroeps) criminelen. Dit is een nationaal probleem waarbij ook de Nederlandse kennisinstellingen doelwit zijn van cyberaanvallen met aanvalsmethoden die uiteenlopen van pogingen om informatie openbaar te maken en phishing e-mails tot DDos (Denial-of-service-) en ransomware aanvallen. Omdat kennisinstellingen veelal diensten afnemen bij een aantal grote techbedrijven, kan er bij cyberaanvallen op deze dienstverleners grootschalige uitval plaatsvinden. Dit hoofdstuk is bedoeld om instellingen te ondersteunen bij het vergroten van bewustzijn over cyberveiligheid en aandacht voor (keten-)samenwerking, de maatregelen die instellingen kunnen treffen om de digitale weerbaarheid te verhogen en hoe het veiligheidsbeleid binnen instellingen verder kan worden verankerd voor het optimaal presteren van de organisatie, continuïteit van onderwijs, onderzoek en kennisdeling en voor het waarborgen van de integriteit en vertrouwelijkheid van de data waarover de sector beschikt.

9.1 Dreigingen en risico's

Ransomware aanvallen claimen het merendeel van de gemelde cyberaanvallen in kennisinstellingen en zijn merkbaar vanwege hun specifieke werkwijze waarbij het doelwit wordt gedwongen het gevraagde losgeld te betalen. Dit is anders bij sabotage of spionage, waarbij de kwaadwillende partij actief probeert detectie te ontwijken om zijn doel te bereiken. Het Cyberdreigingsbeeld van SURF geeft een goed beeld van welke dreigingen zich in het hoger onderwijs en onderzoek manifesteren en de impact hiervan.

De grootste dreiging gaat uit van statelijke en criminele actoren

Daders kunnen uiteenlopende achtergronden en motieven hebben. De grootste dreiging voor de meeste organisaties in Nederland gaat uit van statelijke en criminele actoren. Dat geldt zeker ook voor kennisinstellingen. Door te spioneren kunnen landen op relatief laagdrempelige wijze aan kennis komen, waarbij het motief politiek, militair en/of economisch van aard is. Gecoördineerde cyberaanvallen op kennisinstellingen worden vaak uitgevoerd door bekende Advanced Persistent Threat (APT)-groepen van een staat of die door een staat worden gesponsord. Ze zijn geavanceerd in het inzetten van een reeks tactieken en technieken om toegang te krijgen tot gerichte digitale infrastructuur en intellectueel eigendom. Ze zijn volhardend in het uitvoeren van operaties die heimelijk kunnen zijn of gedurende langere perioden onopgemerkt blijven om hun doelstellingen te bereiken. Ze vormen een bedreiging omdat ze het vermogen en de intentie hebben om de kwetsbaarheden van hun doelwit te misbruiken. Het kan hierbij gaan om (on)bekende kwetsbaarheden in technische en ondersteunende infrastructuur van kennisinstellingen. Ook kunnen mensen die de kennisinstellingen bezoeken, daar studeren en/of werken een doelwit zijn.

Cyberaanvallen dienen voor staten ook als middel voor het verspreiden van desinformatie. Door bonafide informatie te vermengen met desinformatie of die te manipuleren, kunnen twijfels worden gezaaid over bepaalde vraagstukken.

Naast cyberactoren waar een dreiging van kan uitgaan, kunnen ook andere oorzaken resulteren in digitale risico's. U kunt hierbij denken aan storingen in hardware, technisch falen van componenten in de infrastructuur, uitval van elektriciteit, overstromingen, brand e.d. Het is belangrijk om ook hiermee rekening te houden.

Digitale risico's van organisaties waarmee wordt samengewerkt of waar diensten, hardware of software van worden afgenomen, kunnen doorwerken naar kennisinstellingen. Talrijke voorbeelden hebben zich voorgedaan waarbij bijvoorbeeld diensten van andere, veelal mondiaal opererende bedrijven, waren gemanipuleerd waardoor actoren ook toegang konden krijgen tot de infrastructuur van andere organisaties. Ook maken actoren veelvuldig gebruik van (on)bekende kwetsbaarheden in veel gebruikte producten. Bijvoorbeeld het misbruik van kwetsbaarheden in cloud services en mailservers voor het e-mailverkeer. Omgekeerd zouden digitale processen/ systemen aantrekkelijk kunnen zijn als opstap naar andere 'doelwitten'. Denk aan inzage in oppositieleden of dissidenten uit bepaalde landen die studeren of promoveren aan de universiteit en mogelijk voor die landen gevoelig onderzoek doen. Via bijvoorbeeld studenteninformatie zouden die landen hun digitale pijlen kunnen richten op die personen.

De NCTV onderkent in het 'Cybersecuritybeeld Nederland 2021' vier risico's voor de nationale veiligheid:

1. Ongeautoriseerde inzage in informatie (en eventueel publicatie daarvan), in het bijzonder door spionage of datalekken.
2. Ontoegankelijkheid van processen, als gevolg van (voorbereidingen voor) sabotage, de inzet van ransomware.
3. Schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leveranciersketens.
4. Grootschalige uitval: een situatie waarin één of meer processen zijn verstoord als gevolg van natuurlijke of technische oorzaken, of als gevolg van niet-moedwillig menselijk handelen.

In het Cybersecuritybeeld Nederland wordt tevens aandacht gevraagd voor de Handreiking Cybersecuritymaatregelen²⁸. Hierin worden basismaatregelen genoemd die op orde moeten zijn voor een minimumniveau van digitale veiligheid. Deze basismaatregelen komen overeen met verbeterpunten die uit diverse evaluaties van incidenten naar voren zijn gekomen en met de investeringen die door een deel van de instellingen al is gedaan of is voorgenomen. Het gaat hierbij om acht basismaatregelen die volgens het Nationaal Cyber Security Centrum (NCSC) minimaal noodzakelijk zijn om u te beschermen tegen actuele digitale dreigingen. Het is daarom belangrijk dat uw instelling deze basisregels zoveel mogelijk toepast en dat u hierover in uw jaarverslag rapporteert. Hoe deze basismaatregelen door uw instelling zorgvuldig kunnen worden toegepast kunt u in het kader van risicomanagement inrichting in overleg doen met organisaties zoals VH, UNL, KNAW, NWO, NFU en de TO2-federatie. Het is hierbij belangrijk dat rekening wordt gehouden met de diversiteit en verschillen in risicoprofielen tussen instellingen.

Basismaatregelen cyberveiligheid

1. *Zorg dat elke applicatie en elk systeem voldoende loginformatie genereert*
2. *Pas multifactor authenticatie toe waar nodig*
3. *Bepaal wie toegang heeft tot uw data en diensten*
4. *Segmenteer netwerken*
5. *Versleutel opslagmedia met gevoelige bedrijfsinformatie*
6. *Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze*
7. *Maak regelmatig back-ups van uw systemen en test deze*
8. *Installeer software-updates*

9.2 Handelingsperspectief: wat kunt u doen?

Wat moet u op instellingsniveau op orde hebben? Welke processen en procedures moeten er bestaan? Hoe zorgt u ervoor dat iedereen ermee bekend is? Hoe kan iedereen zelf bijdragen? Hoe zorgt u voor voldoende 'digitale hygiëne'? Waar is vooral behoefte aan samenwerking en kennis- en informatiedeling?

a. Vergroten bewustzijn

Menselijk gedrag kan technische en procedurele maatregelen tenietdoen. De grootste primaire oorzaak van de gemelde veiligheidsincidenten is onwetendheid en onjuist handelen van mensen. Daarmee vormen mensen ook een belangrijke factor voor cybersecurity. Om de kans op een cyberaanval te verkleinen is het van belang dat studenten en medewerkers gefaciliteerd worden om veilig gedrag te ontwikkelen en dat instellingen daartoe de nodige maatregelen treffen.

Voorbeelden van maatregelen die uw instelling kan nemen om bewustzijn zowel op instellingsniveau als op het niveau van studenten en medewerkers te vergroten:

- Zet diverse communicatiekanalen in zoals nieuwsbrieven, speciale intranetpagina's, infographics en vlogs van experts en bestuurders. Publiceer regelmatig nieuws over best practices die cyberbeveiligingsincidenten beschrijven, inclusief verhalen met suggesties voor gedrag en acties.
- Ontwikkel opleidingen, trainingen en terugkerende voorlichtingssessies voor onderzoekers, studenten en administratief en ondersteunend personeel in cyberhygiëne, het identificeren van de risico's en kennis over het vermijden of aanpakken van. Dit kan ook met behulp van fysieke en digitale campagneactiviteiten zoals Cybersave Yourself van SURF²⁹.
- Implementeer e-learning tools voor studenten en medewerkers zoals het Digitaal-Brevet van SURF.
- Doe mee aan cybercrisisoefeningen (zoals OZON van SURF).

b. Risicomanagement en bestuurlijke en strategische aandacht

Welke afspraken maakt u binnen uw instelling en met externe stakeholders voor het optimaal presteren van de organisatie, continuïteit van onderwijs, onderzoek en kennisdeling en voor het waarborgen van de integriteit en vertrouwelijkheid van de data waarover de sector beschikt.

Om de kans op een cyberaanval te verkleinen is het van belang dat studenten en medewerkers gefaciliteerd worden om veilig gedrag te ontwikkelen

**Cybercriminelen
verdiepen zich
steeds beter in de
organisaties die zij
willen aanvallen**

Het is cruciaal om als kennisinstelling zo goed mogelijk voorbereid te zijn op een cyberaanval. Cybercriminelen verdiepen zich steeds beter in de organisaties die zij willen aanvallen en benaderen doelgericht specifieke functionarissen binnen de organisatie. Het is daarom belangrijk dat instellingen op bestuurlijk en strategisch niveau aandacht blijven geven aan veiligheid en maatregelen implementeren om, naast bewustwording, mogelijke aanvallen te detecteren en te monitoren. Het zorgvuldig inrichten van risicomanagement is nodig om inzicht te krijgen in de risico's en passende maatregelen te kunnen nemen om deze risico's op kosteneffectieve wijze te mitigeren. Dit vraagt om een gedegen governance en strategische positionering van het veiligheidsrisicomanagement in uw instelling. Opnemen van veiligheidsbeleid in de jaarverslagen, meerjarenvisie en strategische plannen van uw instelling en het structureel bespreken van dit onderwerp binnen de Raden van Toezicht zijn concrete maatregelen waar u aan kan denken.

Technische en organisatorische maatregelen waar uw instelling, naast de basismaatregelen van het Nationaal Cyber Security Centrum, aan kan denken om risico's beter te borgen zijn:

- Aansluiten op een CERT (Emergency Response Team), zoals SURFcert, waarbij aangesloten instellingen 24/7 ondersteuning krijgen wanneer er zich een beveiligingsincident voordoet. SURFcert staat in direct contact met het Nationaal Cyber Security Centrum (NCSC), als onderdeel van het Landelijk Dekkend Stelsel (LDS). Dit is een stelsel waarin publieke en private partijen kennis en informatie met elkaar uitwisselen. Aangesloten zijn bijvoorbeeld de CERTs, sectorale en regionale samenwerkingsverbanden, het NCSC en het Digital Trust Center (DTC). Het NCSC fungeert in het Landelijk Dekkend Stelsel als centraal informatieknooppunt.
- Aansluiten bij een Security Operations Center (SOC) oplossing, zoals het SURFsoc, zorgt voor 24/7 monitoring van uw netwerken en signalering van dreigingen. De continue monitoring zal uw instelling enorm helpen met het versterken van de informatiebeveiliging, omdat er constant informatie wordt verzameld die bij mogelijke dreigingen snel sectorbreed wordt gedeeld.
- Een gedeeld normenkader naast een adequaat systeem van preventie en respons is noodzakelijk om risicomanagement binnen uw organisatie goed in te richten. Zo maken een groot deel van de hoger onderwijsinstellingen gebruik van de normenkader informatiebeveiliging hoger onderwijs. Met een toetsingskader dat het normenkader aanvult, wordt vervolgens beschreven wat de vereisten zijn om aan een bepaald volwassenheidsniveau te voldoen.
- Uitvoeren van structurele interne en/of externe audits waarmee meer inzicht wordt verkregen in de mate waarmee instellingen informatiebeveiliging onder controle hebben en waar de prioriteiten liggen voor verbetering.
- Om inzicht te krijgen in de dreiging van cyberaanvallen en praktische tips om een aanval te herkennen en te voorkomen kunt u de publicatie van de AIVD en MIVD 'Cyberaanvallen door statelijke actoren'³⁰ over de zeven momenten waarop u een cyberaanval door een statelijke actor kan stoppen raadplegen.

c. Aandacht voor ketensamenwerking

Er zijn tal van internationale samenwerkingsverbanden tussen academische en kennisinstellingen, waarbinnen legitieme kennisoverdracht plaatsvindt. Kennis kan echter ook ongewenst wegvloeien door cyberaanvallen en toegang tot systemen en bestanden.

Omdat academische en kennisinstellingen unieke en hoogwaardige kennis genereren en er persoonsgegevens worden verwerkt zijn dit gewilde doelwitten voor kwaadwillende actoren. Daarom is bij een effectieve bestrijding van cyberrisico's samenwerking en continue kennis-en informatiedeling over risico's cruciaal om. Zo vormen de SURF beveiligingscommunity's SURFnet Community of Incident Response Teams (SCIRT) en de SURF Community voor Informatiebeveiliging en Privacy (SCIPR) een goed platform voor operationele security experts van kennisinstellingen om bij te leren en kennis met vakgenoten te delen. Hiermee leveren zij een bijdrage aan de professionalisering van de informatiebeveiliging binnen deze instellingen.

SURF is tevens namens de sector onderwijs en onderzoek aangesloten op het Landelijk Dekkend Stelsel (LDS). Het LDS is een stelsel waarin publieke en private partijen kennis en informatie met elkaar uitwisselen en waarmee het NCSC kwetsbaarheden en dreigingsinformatie kan delen. Aangesloten zijn bijvoorbeeld CERTs, OKKTs (sectorale en regionale samenwerkingsverbanden) en het Digitaal Trust Center (DTC).

Overzicht contactgegevens en bronnen

Loket Kennisveiligheid

Telefoon: 088-0424242
E-mail: info@loketkennisveiligheid.nl
Website: www.loketkennisveiligheid.nl

Exportcontrole - Centrale Dienst voor In- en Uitvoer (CDIU)

Telefoon: 088 - 151 21 22
Informatie: https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/douane_voor_bedrijven/veiligheid_gezondheid_economie_en_milieu_vgem/cdiu/cdiu_algemeen/cdiu

Aanvragen en meldingen indienen:

https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/programmas_en_formulieren/aanvraag_indelingsverzoek

Bronnen

H1: Introductie

- 1 Kamerbrief Kennisveiligheid Hoger Onderwijs en Onderzoek (2020): <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/27/kennisveiligheid-hoger-onderwijs-en-wetenschap>

H2: Het beschermen van academische kernwaarden

- 2 Nederlandse gedragscode wetenschappelijke integriteit: <https://www.nwo.nl/nederlandse-gedragscode-wetenschappelijke-integriteit>
- 3 The European Code of Conduct for Research Integrity: <https://allea.org/code-of-conduct>
- 4 Nationaal Actieplan voor meer Diversiteit en Inclusie (2020): <https://www.rijksoverheid.nl/actueel/nieuws/2020/09/01/nieuw-nationaal-actieplan-voor-diversiteit-en-inclusie>

H4: Juridische kaders en gedragscodes

- 5 EU dual-use verordening (2021): <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32021R0821&qid=1632830707418>
- 6 Rijksoverheid factsheet export via de cloud (2018): <https://www.rijksoverheid.nl/documenten/brochures/2018/10/23/factsheet-export-via-de-cloud>
- 7 Technology Readiness Level (TRL) Assessment Tool: [https://www.ic.gc.ca/eic/site/099.nsf/vwapj/TRL-e.pdf/\\$file/TRL-e.pdf](https://www.ic.gc.ca/eic/site/099.nsf/vwapj/TRL-e.pdf/$file/TRL-e.pdf)
- 8 EU-aanbeveling voor kennisinstellingen over het inrichten van interne compliance procedures voor dual-use exportcontrole (2021): <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32021H1700>
- 9 CDIU Aanvraagformulier indelingsverzoek: https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/programmas_en_formulieren/aanvraag_indelingsverzoek
- 10 RIVM Bureau Biosecurity: <https://www.bureaubiosecurity.nl>
- 11 EU-verordening betreffende beperkende maatregelen ten aanzien van Iran: <https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:02012R0267-20210731&from=EN#M39-1>
- 12 Rijksoverheid lijst vakgebieden verscherpt toezicht: <https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies>

- 13 Kamerbrief Kennisveiligheid Hoger Onderwijs en Onderzoek (2020): <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/27/kennisveiligheid-hoger-onderwijs-en-wetenschap>
- 14 UNL Kader Kennisveiligheid Universiteiten: https://www.universiteitenvannederland.nl/nl_NL/nieuwsbericht/nieuwsbericht/766-universiteiten-presenteren-kader-kennisveiligheid.html
- 15 EU guidelines on Tackling R&I foreign interference (2022): <https://ec.europa.eu/info/files/tackling-ri-foreign-interference>
- 16 Guidelines Australië: <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector>
- 17 Guidelines Duitsland: <https://www.hrk.de/positionen/beschluss/detail/leitlinien-und-standards-in-der-internationalen-hochschulkooperation>
- 18 Guidelines Verenigd Koninkrijk: <https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation>
- 19 Guidelines Zweden: https://www.stint.se/wp-content/uploads/2020/02/STINT_Responsable_Internationalisation
- 20 Guidelines Canada: https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html

H5: Het inschatten van risico's

- 21 NCTV/AIVD/MIVD Dreigingsbeeld Statelijke Actoren 2021: <https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren>
- 22 AIVD Jaarverslagen: <https://www.aivd.nl/onderwerpen/jaarverslagen>
- 23 MIVD Jaarverslagen: <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/downloads>
- 24 ASPI China Defense Universities Tracker: <https://unitracker.aspi.org.au>

H6: Risicomanagement

- 25 MIVD Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) 2019: <https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019>

H7: Internationale partnerschappen, inkopen en aanbesteden

- 26 Quickscan nationale veiligheid bij inkoop en aanbesteden: <https://www.pianoo.nl/nl/document/16908/quickscan-nationale-veiligheid-bij-inkoop-en-aanbesteden>

H8: De rol van personeelsbeleid

- 27 AIVD-brochure 'Op reis naar het buitenland – Veiligheidsrisico's onderweg' (2017): <https://www.aivd.nl/documenten/publicaties/2017/12/20/op-reis-naar-het-buitenland>

H9: Cyberveiligheid in relatie tot statelijke dreigingen

- 28 Nationaal Cyber Security Centrum, Handreiking Cybersecuritymaatregelen (2021): <https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen>
- 29 SURF Toolkit bewustzijn cyberveiligheid "Cybersave Yourself": <https://www.surf.nl/cybersave-yourself-maak-medewerkers-en-studenten-bewust-van-internetgevaaren>
- 30 AIVD/MIVD Cyberaanvallen door statelijke actoren (2021): <https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen>

Universiteiten
van Nederland }

