vsnu
vereniging van universiteiten
association of universities
THE NETHERLANDS

Kader Kennisveiligheid Universiteiten

Inhoudsopgave

Voorwoord

Geachte lezer,

Voor u ligt het eerste Kader Kennisveiligheid Universiteiten. De Nederlandse Universiteiten koesteren de transparantie van de wetenschap én hebben oog voor de keerzijden daarvan. Met dit kader kunnen wetenschappers en universiteiten beter dan voorheen de afweging maken tussen enerzijds openheid van wetenschap en anderzijds het voorkomen van ongewenste kennisoverdracht.

Internationale samenwerking is cruciaal voor toponderzoek en het beste academisch onderwijs. Dat brengt kansen en risico's met zich mee. Kansen voor onderzoek, onderwijs en innovatie, voor open kennisdeling. Universiteiten zijn – door hun open, internationale karakter - een gewild doelwit voor spionageactiviteiten, voor het verkrijgen van sensitieve technologieën en om meningen te beïnvloeden. De risico's zijn dus diefstal van kennis door andere landen en beïnvloeding van medewerkers in het hoger onderwijs en wetenschap, wat kan leiden tot (zelf) censuur en de aantasting van academische vrijheid.

Dit kader is tot stand gekomen in de universitaire werkgroep kennisveiligheid, een inter-disciplinaire werkgroep met experts vanuit alle Nederlandse Universiteiten. Bovendien zijn er andere inhoudelijke experts geconsulteerd. We willen iedereen nadrukkelijk bedanken die betrokken is geweest bij het opstellen van het Kader Kennisveiligheid Universiteiten.

Wij zien dit Kader als een stap in het steeds meer bewust omgaan met risico's op het vlak van kennisveiligheid. De universiteiten zorgen voor:

1. compliant zijn met relevante wet- en regelgeving ("basis op orde")
2. vertalen risico-inventarisatie naar faculteiten, opleidingen en onderzoeksgroepen
3. doorontwikkelen kader en beslisboom
4. inrichten van een adviesteam kennisveiligheid per universiteit
5. training en awareness van alle medewerkers toegespitst op risicoprofiel
6. opnemen kennisveiligheid in risicomanagementsystematiek universiteit

Uiteindelijk heeft namelijk iedereen een rol in het beperken van de veiligheidsrisico's. Wij willen daarom afsluiten met een oproep aan alle academici om het kader welbewust te hanteren, weloverwogen beslissingen te nemen in het aangaan van samenwerkingsverbanden, en natuurlijk om door te gaan met het geven van geweldig goed academisch onderwijs en het doen van baanbrekend onderzoek.

Vriendelijke groet,

Pieter Duisenberg

Voorzitter Vereniging van Universiteiten

Hoofdstuk 1

Inleiding

Hoofdstuk 1
Inleiding

Het vrij kunnen kiezen van onderzoeks- en onderwijsonderwerpen en het vrij beschikbaar kunnen stellen van onderzoeksresultaten zijn academische verworvenheden. Tegelijkertijd willen universiteiten het gebruik van onderzoeksresultaten voor onethische, of anderszins onwenselijke doeleinden zo veel mogelijk tegengaan. Om instellingen te ondersteunen bij de besluit- en beleidsvorming rond kennisveiligheid hebben de Nederlandse universiteiten dit kader kennisveiligheid opgesteld.

Dit kader schetst waar de Nederlandse universiteiten zich aan committeren en waarbinnen zij zelf invulling geven aan het instellingsbeleid en biedt een richtsnoer om instellingen in staat te stellen goed geïnformeerde en onderbouwde beslissingen te nemen over internationale samenwerkingsverbanden. De doelgroep van dit kader is het bestuur van universiteiten, onderzoekers, de universitaire sector als geheel en betrokken ministeries. Hiermee wordt ook invulling gegeven aan de roep van overheid en samenleving om als sector verantwoordelijkheid te nemen voor het borgen van kennisveiligheid.[1]

Internationale samenwerking kent in toenemende mate uitdagingen. Universiteiten maken zich zorgen om de academische waarden en vrijheden, en andere ethische uitgangspunten in sommige partnerlanden. Statelijke actoren kunnen, ook in Nederland, middelen inzetten die de academische vrijheid van medewerkers aantasten. Bovendien zet dit de ambities van open science en open acces onder druk. Universiteiten zijn verantwoordelijk voor het borgen van de academische waarden. Academische vrijheid wordt wettelijk geborgd op nationaal (in de Grondwet en Wet op het hoger onderwijs en wetenschappelijk onderzoek) en internationaal niveau (in het EU-Handvest en het Europees Verdrag voor de Rechten van de Mens). Academische vrijheid is een grondrecht en mensenrecht.

Context: lokaal, regionaal, wereldwijd

Universiteiten werken op allerlei manieren samen met bedrijven, overheden en kennisinstellingen: in onderzoek, onderwijs en in het ontwikkelen van innovatieve oplossingen voor maatschappelijke problemen. Die samenwerking ontstaat vaak bottom-up: onderzoeksgroepen zoeken gelijkgestemden op aan de andere kant van de wereld of net over de grens; een onderwijsuitwisseling wordt op opleidingsniveau beklonken en een start-up kiest voor zijn

1 Van Engelshoven, I.; Grapperhaus, F.; Keijzer, M. (2020, 27 november), 'Kennisveiligheid hoger onderwijs en wetenschap' [Kamerbrief].

groeistrategie een internationaal bedrijf om mee samen te werken. Universiteiten kennen *checks and balances* om deze samenwerkingen te toetsen en te accorderen, en zetten in op het vergroten van de bewustwording dat deze samenwerkingen soms ook dreigingen met zich kunnen meebrengen.

De kwaliteiten van onze onderzoekers worden in Nederland[2] en daarbuiten[3] opgemerkt, waarmee wij op de radar komen van (goedwillende en) kwaadwillende individuen, groeperingen en landen. Zij kunnen een bedreiging vormen voor onze normen, waarden, veiligheid, mensen en economie. Deze bedreiging kan zich op verschillende manieren manifesteren, zoals door cyberaanvallen of spionage, maar ook door manipulatie of sabotage van wetenschappelijk onderzoek. Internationale relaties zijn bovendien aan verandering onderhevig waardoor de risico's kunnen veranderen. Door deze ontwikkelingen is de (cyber)veiligheid van de instellingen en van onze medewerkers en studenten in het geding.

Hoe gaan universiteiten om met de ingewikkelde balans waar zij zich dagelijks in bevinden, tussen kansen enerzijds en risico's anderzijds? De ministeries van OCW, JenV en EZK hebben met de Kamerbrief Kennisveiligheid[4] een startschot gegeven om hier landelijk en per universiteit aandacht aan te besteden. Om universiteiten te ondersteunen bij de besluit- en beleidsvorming rond kennisveiligheid, is dit kader vanuit de sector opgesteld. Toepassing van dit kader moet ervoor zorgen dat studenten en medewerkers in een veilige omgeving onderwijs kunnen genieten en onderzoek kunnen uitvoeren, vrij van ongewenste kennisoverdracht of nadelige beïnvloeding en met behoud van academische waarden.

Uitgangspunten en begrippen

Definitie Kamerbrief OCW d.d. 27 nov 2020:

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

2 Oproep President KNAW: 'Universiteiten bescherm je medewerkers'.
3 Samenwerking AIVD, MIVD en NCTV, 'Dreigingsbeeld Statelijke Actoren'.
4 Van Engelshoven, I.; Grapperhaus, F.; Keijzer, M. (2020, 27 november), 'Kennisveiligheid hoger onderwijs en wetenschap' [Kamerbrief].

Hierbij kan gedacht worden aan het 'weglekken' van gevoelige wetenschappelijke kennis en technologie naar landen en regimes die deze kennis inzetten om ons en onze partners te schaden. Of deze inzetten tegen (eigen) burgers op een manier die wij onethisch of maatschappelijk onverantwoord achten. Dat kan op vele manieren, zoals door cyberaanvallen of spionage, maar ook door manipulatie of sabotage van wetenschappelijk onderzoek. Ook kan gedacht worden aan kwesties rond (zelf)censuur, waardoor onderzoekers en studenten zich niet langer vrij voelen om zich uit te spreken, om zich kritisch uit te laten over bepaalde landen. Door deze ontwikkelingen is de (cyber)veiligheid van de instellingen en van medewerkers en studenten in het geding. Het waarborgen van de veiligheid van onze studenten en ons personeel is dan ook een belangrijke uitgangspositie voor dit kader.

Het vrij beschikbaar kunnen stellen van onderzoeksresultaten en het vrij kunnen kiezen van onderzoeksonderwerpen zijn en blijven de belangrijkste academische verworvenheden. De academische vrijheid is in het EU-Handvest en het Europees Verdrag voor de Rechten van de Mens expliciet vastgelegd als een grondrecht en mensenrecht. Tegelijkertijd willen universiteiten voldoen aan wetgeving (Europees en nationaal). Deze wetgeving is in hoofdstuk 3 verder uitgewerkt. Ook willen universiteiten het gebruik van onderzoeksresultaten voor onethische, of anderszins onwenselijke doeleinden zo veel mogelijk tegengaan. Het is cruciaal dat daarbij goed wordt gekeken naar de proportionaliteit van de mogelijke risico's en daaropvolgende maatregelen. Universitair onderzoek wordt gedaan over de volle breedte van disciplines, maar niet elk vakgebied is in gelijke mate een mogelijk doelwit voor ongewenste beïnvloeding of ongewenste kennisoverdracht. Sterker nog: bij de meerderheid van het onderzoek is het risico laag.

Bestaande praktijken

Bij universiteiten is er altijd sprake geweest van diverse *checks and balances* om samenwerkingen op het gebied van onderzoek, onderwijs en valorisatie te toetsen. Zo zijn er binnen de universiteiten richtlijnen voor goed bestuur, publiek-private samenwerking, intellectueel eigendom en wetenschappelijke integriteit. Deze documenten zijn en blijven relevant in het kader van kennisveiligheid en bieden universiteiten en medewerkers handelingsperspectief.

Toepassing van dit kader

Het doel van dit kader is een raamwerk te bieden voor het beoordelen van kansen en risico's van internationale samenwerkingen. Dit kader biedt universitaire bestuurders een landen-neutraal afwegingskader voor beleids- en besluitvorming rond kennisveiligheid.
Dit kader is zo opgesteld dat deze op alle universiteiten kan worden toegepast, ongeacht onderzoeksfocus, schaal of aanwezige expertise. Dit kader kent een toepassing voor individuele medewerkers van universiteiten, hun CvB's, de universitaire sector als geheel en de betrokken ministeries (OCW, BZK, EZK, Defensie, JenV en SZW). We onderscheiden daarbij vier doelgroepen en toepassingsmogelijkheden.

Voor ***individuele medewerkers:*** vergroten van bewustwording van kansen en risico's alsmede kennis van hun eigen handelingsperspectief en de besluitvormingsstructuur bij landen en programma's die door de overheid als risicovol zijn bestempeld.

- voor onderzoekers;
- voor de verantwoordelijken voor de instroom van internationale studenten en voor uitwisselingsprogramma's voor studenten en medewerkers;
- voor de verantwoordelijken in het HR-proces bij het aanstellen van internationale medewerkers;
- voor de verantwoordelijken voor het vorm en inhoud geven aan samenwerkingsprojecten/ programma's;
- ondersteuners zoals juristen en contract officers.

Voor het ***bestuur*** van universiteiten:

- ontwikkelingskader dat per onderdeel van de universiteit schetst wat de kansen en risico's zijn, wat de Europese en nationale kaders zijn en hoe en waar dit integraal bezien moeten worden;
- een raamwerk dat dient om te identificeren op welke fronten medewerkers en studenten en kennis beschermd dienen te worden;
- voorzet voor een proces en een structuur om kennisveiligheid een vaste plek te geven in bedrijfsvoering, besluitvorming en primaire processen van de universiteiten, inclusief een gerichte aanpak voor training en communicatie;
- aanpassing/gebruikmaking van applicaties voor registratie van researchprojecten, archivering, communicatie en auditbehoefte;
- delen van dilemma's en casuïstiek met andere universiteiten;
- een dergelijke benadering leidt tot een betere reactie en sterkere voorbereiding op het moment dat er zich nieuwe casuïstiek voordoet op dit thema.

Voor de ***universitaire sector*** als geheel:

- inventarisatie van kansen en risico's van internationale samenwerking, waarbij de risico's worden beheerst in het licht van verhoogde internationale, strategische concurrentie en groeiende politieke polarisatie;
- een ontwerp voor een gestructureerd proces en een indicatie van de middelen die nodig zijn om de kansen en bedreigingen van internationale samenwerking te identificeren, adresseren en behandelen, in samenwerking met andere spelers in de hogeronderwijssector.

Voor de ***betrokken ministeries*** bij kennisveiligheid (naast OCW, JenV en EZK ook BZ, SZW en Defensie):

- welomschreven behoefte: wat universiteiten nodig hebben vanuit de ministeries (institutionele inbedding, middelen, kennis) zodat studenten en medewerkers in een veilige omgeving onderwijs kunnen genieten en onderzoek kunnen uitvoeren;
- ontwikkeling van nationaal en Europees beleid rondom *technology sovereignty* om te voorkomen dat er binnen Europa onvoldoende alternatieven voorhanden zijn, wanneer strategische samenwerking met bepaalde regio's vanuit kennisveiligheidsrisico's wordt uitgesloten.

Leeswijzer kader

Deze inleiding beschrijft de aanleiding tot en context van dit kader. Vervolgens behandelen we in hoofdstuk 2 de kansen en risico's van onderzoek en onderwijs op wereldniveau. Het in balans houden van die kansen en risico's is en blijft een complex vraagstuk. In hoofdstuk 3 schetsen we de governance-inrichting internationaal, bij rijksoverheid en universiteiten om dat vraagstuk te beheersen. Hoofdstuk 4 beschrijft hoe dat aan de hand van een beslisboom binnen universiteiten gestalte kan krijgen in de vorm van betrokkenen, verantwoordelijkheden en risicomanagementprocessen. Hierbij wordt aandacht besteed aan due diligence, informatievoorziening/voorlichting/communicatie, kennisdeling en veiligheid.

Hoofdstuk 2

Kansen en risico's van internationale samenwerking

Hoofdstuk 2

Kansen en risico's van internationale samenwerking

Kansen voor universiteiten door internationalisering

Nederlandse universiteiten zoeken samenwerking met andere universiteiten, bedrijven of overheden die aanvullende kennis of onderzoeksfaciliteiten hebben om in consortia samen aan de oplossing van maatschappelijke problemen te werken. Universiteiten werken daarbij op allerlei manieren samen: in onderzoek en onderwijs en in het ontwikkelen van innovatieve oplossingen en valorisatie. Die samenwerking ontstaat vaak bottom-up: onderzoeksgroepen zoeken gelijkgestemden op aan de andere kant van de wereld, net over de grens of binnen de grenzen van Nederland; een onderwijsuitwisseling wordt op opleidingsniveau beklonken en een start-up kiest voor zijn groeistrategie een internationaal bedrijf om mee samen te werken.

Internationale samenwerkingen bieden Nederlandse universiteiten toegang tot mensen en middelen waardoor Nederland zijn toppositie in de wetenschap kan behouden. Bovendien bieden dergelijke samenwerkingen een frisse blik op onderzoekersonderwerpen, culturen en gebruiken van andere landen. Verder bieden internationale samenwerkingen Nederland ook de kans om onze (academische) normen, waarden en gebruiken over de wereld te verspreiden. Zo zetten Nederlandse universiteiten al jaren succesvol in op open access en open science. Kortom, zonder internationale samenwerking is het voor een klein land als Nederland onmogelijk om op wereldniveau onderzoek te verrichten en onderwijs te faciliteren.

Het proces van globalisering en de daarmee gepaard gaande toename van wereldwijde interactie en het gebruik van (digitale) netwerken tussen personen en organisaties, heeft een grote impact op de maatschappij en het dagelijks leven van velen. Niet eerder hebben we in zo'n grote mate in contact gestaan met internationaal georiënteerde organisaties en personen met zo veel uiteenlopende culturele achtergronden als in de hedendaagse mondiale arbeidsmarkt, in alle sectoren, binnen en buiten de academie, in de publieke en private sector. Globalisering en internationalisering bieden dan ook legio kansen voor onderzoek en onderwijs en zijn niet meer weg te denken op de campus. Het zijn integrale onderdelen van de moderne universiteit.

Onderzoek

Een groeiend aantal vraagstukken in het hedendaags wetenschappelijk onderzoek is complex, interdisciplinair en maatschappelijk relevant. Vraagstukken rondom thema's als duurzaamheid, publieke gezondheid, energietransitie en migratie zijn bovendien per definitie grensoverschrijdend en afhankelijk van samenwerking tussen disciplines en over landsgrenzen heen. Door kennis te delen in mondiale allianties binnen grotere ecosystemen van bedrijven, (semi) overheid, ngo's, onderwijs- en onderzoeksinstellingen, wordt gewerkt aan oplossingen voor een betere wereld. Dergelijke partnerschappen zijn cruciaal voor het verbeteren van de toegang tot

talent, kennis, complementaire onderzoeksomgevingen, ultramoderne onderzoeksfaciliteiten en financiering. Uiteindelijk leidt dit tot een positieve impact.

Onderwijs

Universiteiten streven er voortdurend naar om de internationale oriëntatie van de bachelor- en mastercurricula te verbeteren, versterken en verrijken door middel van onderwijs- en onderzoekssamenwerking met vooraanstaande (academische) partners wereldwijd. Deze partnerschappen stellen studenten in staat competenties te ontwikkelen, zoals intercultureel begrip, diversiteit in contexten en integratie door interactie met leeftijdsgenoten in uitwisselingsprogramma's voor studenten en gezamenlijke projecten. Dat betekent dat naast het benutten van internationale inzichten en kennis uit het curriculum, studenten al tijdens de studie moeten leren omgaan met diversiteit en interculturele vaardigheden opdoen. Het leerproces moet zo worden gefaciliteerd dat studenten een wereldwijze blik en een breed bewustzijn van de wereld om hen heen ontwikkelen.

Het vraagstuk wordt op korte termijn pregnanter door de ontwikkelingen rondom leven lang ontwikkelen (LLO). Veel professionals gaan de komende jaren op zoek naar opleidingen in binnen- en buitenland. Door de groei in microcredentials kunnen de Nederlandse universiteiten ook een digitale toestroom van internationaal talent verwachten.

Risico's van onderzoek en onderwijs op wereldniveau

Naast kansen op basis van ons niveau van onderzoek en onderwijs, zijn er uiteraard ook risico's voor Nederland en de academische wereld. Het is expliciet niet het doel van dit kader om alle mogelijke risico's uit de weg te gaan. Het is echter wel essentieel om een goed begrip te hebben van de risico's (door middel van risicomanagement), en een effectieve manier om die te beheersen (door middel van goede afspraken in een governancestructuur). Diverse rapporten beschrijven de risico's die Nederland, Europa en de academische wereld lopen (o.a. Rathenau, Clingendael, NCTV).

In de volgende vier paragrafen beschrijven we de belangrijkste categorieën van die risico's, in dezelfde volgorde als de vier verschijningsvormen van kennisveiligheid in hoofdstuk 1. Als laatste beschrijven we het risico van een te rigide aanpak van kennisveiligheidscasuïstiek.

Risico voor de (inter)nationale veiligheid

Het meest in het oog springende kennisveiligheidsrisico is die voor de (inter)nationale veiligheid. Voor sommige van deze risico's is al bestaande (internationale) wetgeving, zoals exportbeperkingen voor *dual use technologies* middels het Wassenaar Arrangement, rakettechnologie via het multilateraal *Missile Technology Control Regime (MCTR)* en EU-verordeningen voor het tegengaan van de verspreiding van biologische en chemische wapens. Deze verdragen en wetgeving zijn echter niet sluitend voor onderwerpen die een risico vormen

voor de (inter)nationale veiligheid en lopen per definitie achter op de stand van de wetenschap, zo blijkt ook uit recente conferentie-inzichten over *omni-use technology* en de toepassing van de verdragen en wetgeving op zogenaamde *emerging technologies*. Het is de verantwoordelijkheid van individuele onderzoekers, vakgroepen en universiteiten om zich breed te informeren over de mogelijke gevolgen van hun onderzoek. Dat is complex, maar absoluut noodzakelijk. Enkele voorbeelden tonen de complexiteit van dit risico:

- onderzoekers uit risicolanden die solliciteren naar een onderzoekersplek bij een vakgroep die onderzoek verricht naar dual use technologies;
- cyberincidenten rondom toegang tot onderzoekersdata die onder het Missile Technology Control Regime vallen;
- publicatie van onderzoek naar virusmutaties die in de handen van kwaadwillenden tot ontwikkeling van biologische wapens kan leiden;
- publicatie van kwetsbaarheden in software die kan leiden tot grootschalige cyberincidenten.

Risico voor de economische veiligheid

Er is een inherente spanning tussen enerzijds het academisch ondernemerschap (o.a. vrije verspreiding van kennis en zo veel mogelijk vruchtbare samenwerking) en anderzijds de nationale bescherming van de (relatieve) innovatiekracht (t.o.v. andere landen). Die spanning komt met name tot uiting naarmate het onderzoek betreft dat dichter tegen economische, instrumentele bruikbaarheid aan zit. Een manier om die spanning te identificeren en belangen te taxeren, is gebruik te maken van het zogeheten *Technology Readiness Level* (TRL) van het betreffende onderzoek. De EU heeft dat uiteengezet in negen bruikbare niveaus, van fundamenteel onderzoek tot economisch rendabel voor productie.[5] De exacte toepassing van de EU TRL's behoeft wel wat vingeroefening, maar is bruikbaar om spanningen tussen academisch ondernemerschap en bescherming van economische veiligheid te bespreken en te wegen. Bovendien kan deze indeling ook gebruikt worden bij de risicoafweging voor (inter)nationale veiligheid, waarvoor wetgeving meestal geen eenduidige vereisten geeft. Enkele voorbeelden tonen de complexiteit van dit risico:

- samenwerkingsverband met buitenlandse landbouwindustrie voor de efficiëntere groenteteelt;
- gebruik van buitenlandse computersystemen voor onderzoek naar nanotechnologie.

Risico van (heimelijke) beïnvloeding van onderzoekers of docenten

Beïnvloeding kent vele verschijningsvormen, oorsprongen, richtingen en uitwerkingen. Zo kan beïnvloeding plaatsvinden door 'positieve' factoren (bv. financieel, ideologisch, middelen, toegang, functies, erkenning) of 'negatieve' factoren (bv. opspraak, chantage, dwang, politieke druk, bureaucratie, ontzegging van toegang of visa, boetes). De oorsprongen kunnen individuen, organisaties of overheden zijn in binnen- en buitenland. De richting van beïnvloeding kan zijn aan instellingen, faculteiten, vakgroepen of individuele medewerkers. De uitwerkingen kunnen zich bijvoorbeeld bevinden in (zelf)censuur, aantasting academische

5 De EU beschrijft 9 niveaus: van "*basis principles observed*" in level 1, via "*technology validated in lab*" in level 4 tot aan "*actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)*" in level 9.

vrijheden, keuzes van onderzoeksonderwerpen, aantasting van de integriteit van onderzoek, het moeten stoppen met onderzoek of reputatieschade voor de instelling, vakgroep of individuele onderzoekers. Uit de recente oproep van de president van de KNAW aan universiteiten om hun medewerkers te beschermen[6], blijkt dat dit risico zeer serieus moet worden genomen. Enkele voorbeelden tonen de complexiteit van dit risico:

- beïnvloeding van onderzoekers uit de diaspora van risicolanden;
- ontzegging van toegang of visa voor onderzoekers naar risicolanden;
- nuance-aanpassing van onderzoeksresultaten op basis van verzoek van onderzoeksponsor;
- uitsluiting van deelname aan het publieke debat voor onderzoekers in verband met bedreiging;
- dreiging van studentenuitwisselingsstop naar aanleiding van incidenten in de samenwerking met een buitenlandse universiteit.

Risico van onethisch of ongewenst gebruik van onderzoeksresultaten of onderwijs

Er bestaat het risico dat de kennis, kunde of technologie die voortvloeit uit onderzoeksresultaten of onderwijs onethisch of anderszins ongewenst gebruikt wordt. Het is in de regel complex om die risico's vooraf in te schatten, mede doordat onethisch of ongewenst gebruik aan interpretatie onderhevig is. Bovendien is de relatie tussen de theoretische onderzoeksresultaten of onderwijs en het praktische onethische of ongewenste gebruik niet altijd even sterk. Enkele voorbeelden tonen de complexiteit van dit risico:

- Onderzoek op het gebied van artificiële intelligentie kan gebruikt worden om geautomatiseerd cameratoezicht efficiënter te maken, en daarmee bruikbaar te maken voor statelijke onderdrukking.
- Onderzoek naar zaadveredeling kan gebruikt worden om heroïneteelt efficiënter te maken, en daarmee de straatprijs van heroïne te laten zakken.
- Studenten informatica, die middels onderwijs hebben geleerd hoe de beveiliging van informatiesystemen werkt, kunnen worden gerekruteerd door (statelijke) actoren om in te breken bij bedrijven en overheden.

Risico van een te rigide aanpak van kennisveiligheid

Een laatste – maar belangrijk om te onderkennen – risico betreft een te rigide, eendimensionale aanpak van kennisveiligheid. Oorzaken kunnen onder andere een langdurig, bureaucratisch of ontransparant proces zijn. De gevolgen ervan kunnen groot zijn: de concurrentiepositie van de instelling binnen Nederland of Europa wordt aangetast; belangrijke onderzochte thema/problematiek loopt vertraging op; individuele onderzoekers of vakgroepen raken gedemotiveerd of gaan om de ingerichte processen heen werken; de kwaliteit en toepassing van onderzoek worden geraakt en de instelling wordt aansprakelijk gesteld voor vroegtijdig stopgezet onderzoek of bijdrage aan een consortium.

6 https://www.scienceguide.nl/2021/03/president-knaw-universiteiten-bescherm-je-medewerkers/

Om deze risico's te ondervangen is een wendbare en transparante aanpak nodig. De inrichting moet dicht op het primaire onderzoeksproces staan, een overzichtelijk proces en termijn hebben en bovenal een 'ja tenzij'-instelling kennen. Bovendien is het belangrijk om periodiek het gehele systeem van checks and balances van kennisveiligheid op de universiteit aan de hand van (landelijke) casuïstiek te evalueren en zo nodig bij te stellen.

Bestaande maatregelen

Zoals de Kamerbrief ook beschrijft, hebben universiteiten, de VSNU, ministeries, de internationale gemeenschap en tal van andere instituties de afgelopen jaren niet op hun handen gezeten. Er zijn tal van (functionerende) maatregelen, procedures, handreikingen, richtlijnen en checklists om risico's rondom kennisveiligheid te identificeren en te beheersen. Bij het opstellen van dit kader willen we niet voorbijgaan aan deze documenten, en adviseren we om bij de inrichting van dit kader zo veel mogelijk aansluiting te zoeken bij bestaande governance, processen, procedures, maatregelen, checklists enz. Echter blijkt alleen al uit het initiatief voor dit kader, dat die op dit moment onvoldoende zijn om de risico's van kennisveiligheid voldoende te beheersen. Enerzijds wordt dat veroorzaakt doordat niet alle documenten en processen bekend zijn bij betrokkenen, anderzijds is het algemene bewustzijn voor kennisveiligheidsrisico's laag. Het zal daarom noodzakelijk zijn om niet alleen aan te sluiten bij bestaand materiaal, maar ook wijzigingen, aanvullingen of complete vernieuwingen door te voeren en betrokkenen te wijzen op deze materialen. Zonder tot doel te hebben om een uitputtende lijst bestaande documenten op te nemen, sommen we de belangrijkste op om direct gebruik van te kunnen maken:

Wetgeving

- EU export control regimes voor dual use technologies op basis van Wassenaar Arrangements, Missile Technology Control Regime en EU-verordeningen voor het tegengaan van de verspreiding van biologische en chemische wapens;

Sectorale regelgeving, richtlijnen en codes

- Code goed bestuur universiteiten;
- Nederlandse gedragscode wetenschappelijke integriteit;
- KNAW-brochure over uitdagingen en dilemma's bij internationale wetenschappelijke samenwerking uit 2014[7];
- VSNU-overzicht van richtlijnen voor publiek-private samenwerking en intellectueel eigendom;
- Internationale voorbeelden van richtsnoeren, waar onder Australië, Duitsland, het Verenigd Koninkrijk, Zweden en Canada[8];

7 KNAW "International Scientific Cooperation: challenges and predicaments", 2014

8 Australië; 'Guidelines to counter foreign interference in the Australian university sector', Duitsland; 'Leitlinien und Standards für internationale Hochschulkooperationen' en 'Leitfragenzur Hochschulkooperationen mit der Volksrepublik China', Verenigd Koninkrijk; 'Managing risks in Internationalisation: Security related issues', Zweden; 'Responsible internationalisation: Guidelines for reflection on international academic collaboration' en Canada; 'Safeguarding your research'

- Specifieke checklists voor samenwerking met China van The Hague Centre for Strategic Studies (HCSS)[9] en het Leiden Asia Center (LAC);
- Aandachtspunten voor samenwerking met China uit beleidsstuk "Nederland – China: een nieuwe balans".
- Lokale initiatieven voor checklists, procedures of risicoprocessen voor het aangaan van internationale samenwerkingen.

In hoofdstuk 3 wordt beschreven hoe de governance van kennisveiligheid binnen Nederland geborgd dient te worden. Hoofdstuk 4 schetst vervolgens hoe risicomanagement-processen op universiteiten kunnen worden ingezet om te beoordelen waar bovengenoemde stukken effectief kunnen worden gebruikt, en waar aanvullende maatregelen en processen nodig zijn. Bovendien sluit dit nauw aan bij de recente investeringen op universiteiten om veiligheidszaken integraal te benaderen. Kennisveiligheid is een multidisciplinair domein en leent zich daarom bij uitstek voor een integrale benadering.

9 HCSS, 'Checklist for Collaboration with Chinese Universities and Other Research Institutions'

Hoofdstuk 3

Governance en beleidskaders

Hoofdstuk 3
Governance en beleidskaders

De Nederlandse universiteiten handelen in hun optreden op basis van de Nederlandse grondwet, het Europees Verdrag voor de Rechten van de Mens en het Handvest van de grondrechten van de Europese Unie. Zoals in de 'Magna Charta Universitatum' is vastgelegd, is de vrijheid van onderzoek en onderwijs een essentiële voorwaarde voor het succes van universiteiten.

Eindverantwoordelijkheid voor zowel bewustwording van als een zelfregulerings-systeem voor het thema kennisveiligheid ligt bij het College van Bestuur (CvB). De universiteit wordt echter gekenmerkt door de decentrale organisatie van de wetenschap met grote autonomie voor wetenschappers en faculteiten. De uitvoering van de primaire taken van de universiteit - wetenschappelijk onderzoek en onderwijs en valorisatie van onderzoek, zoals beschreven in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) - is belegd bij faculteiten. Universiteiten zijn bovendien open netwerkorganisaties. De academische staf is verbonden met mondiale wetenschappelijke netwerken en daarmee ook met de mondiale maatschappelijke en economische omgeving. Door deze complexe netwerken zijn sturings- en besluitvormingsprocessen binnen de universiteit ingewikkeld.

Er is een nadrukkelijk belang om samen op te trekken en te komen tot een gezamenlijke aanpak op het gebied van kennisveiligheid, voor OCW, voor veiligheidsdiensten, maar ook voor instellingen en de betrokken onderzoekers en medewerkers. Een aanpak die proportionaliteit als leidend principe heeft, want openheid en toegankelijkheid van onderwijs en wetenschap mogen nooit in het geding zijn. Academische vrijheid, wetenschappelijke integriteit en institutionele autonomie evenmin.

Het kabinet op zijn beurt werkt langs verschillende sporen aan het vergroten van kennisveiligheid. Zo is er een aanpak gericht op statelijke dreigingen[10] en wordt ook in de Chinanotitie van het kabinet uitgebreid ingegaan op kennisgerelateerde aspecten.[11] Daarnaast is er verscherpt toezicht op studenten en onderzoekers die een link kunnen hebben met de Noord-Koreaanse of Iraanse ballistische raketprogramma's.[12]

10 Link Brief Statelijke Dreigingen
11 Nederland-China: een nieuwe balans
12 Link Kamerbrief Verscherpen toezicht op studenten en onderzoekers uit risicolanden

Universiteiten hebben behoefte aan heldere richtlijnen vanuit de rijksoverheid. Regering en parlement verschaffen publieke kennisinstellingen kaders ten aanzien van:

a. Welke verantwoordelijkheid ze verwachten dat kennisinstellingen nemen voor nationale veiligheid;
b. Hoe ze veiligheidsbelangen dienen af te wegen tegen andere belangen, zoals die van vrije wetenschap, economische ontwikkeling, innovatievermogen en concurrentiekracht, bijdragen aan global public goods, aantrekken van toptalent, en goede bilaterale relaties. De kamerbrief bevestigde immers dat de institutionele autonomie van de instellingen belangrijk is en blijft;
c. Aan welke standaarden kennisinstellingen zich dienen te houden om een gelijk speelveld te garanderen.

Bij internationale samenwerking en bij sommige activiteiten kan specifieke wet- en regelgeving van toepassing zijn waaraan voldaan moet worden.

Europees en internationaal

Internationale sancties

De Verenigde Naties (VN) en de Europese Unie (EU) leggen internationale sancties op, aan landen, organisaties, bedrijven en individuele personen. Bijvoorbeeld bij een dreiging voor de internationale vrede en veiligheid. De EU kan ook sancties opleggen om op te komen voor vrede, internationale veiligheid, mensenrechten, de naleving van het internationaal recht, de democratie en de rechtsstaat. Zo zijn er bijvoorbeeld sancties om verspreiding van kernwapens tegen te gaan. Maar ook tegen landen, personen en organisaties die mensenrechten schenden. Of tegen personen die betrokken zijn bij terroristische activiteiten.

Sancties zijn dwingende maatregelen. Hierbij is geen sprake van militaire middelen. Het doel van sancties is om:

- ongewenst gedrag van personen, bedrijven, organisaties of landen te doen veranderen;
- het moeilijker te maken om dit ongewenste gedrag te vertonen;
- andere partijen af te schrikken om datzelfde ongewenste gedrag te vertonen.

Op dit moment gelden er maatregelen voor ongeveer 30 landen.[13] Het is dus van belang dat bij het aangaan van internationale samenwerkingsverbanden wordt gecontroleerd of er sancties aanwezig zijn tegen bepaalde landen, universiteiten of bedrijven.[14]

13 Zie uitleg over de Sanctiewet in Nederland en de nationale sanctielijst terrorisme 'personen en organisaties'
14 Zie sanctielijst www.sanctionsmap.eu

Voor studenten en onderzoekers vormt het gestudeerd hebben aan een gesanctioneerde universiteit feitelijk geen probleem, mits:
- hij/zij daar geen formele aanstelling heeft;
- hij/zij er geen banden meer mee heeft;
- hij/zij er geen afhankelijkheidsrelatie mee heeft;
- de universiteit zelf een afweging maakt in termen van (spionage)risico's en cyberrisico's.

Het niet naleven van de sanctieregels levert een strafbaar feit op. Overtreding kan tevens reputatierisico's met zich meebrengen voor universiteiten of individuele onderzoekers. Een goede beoordeling van de sanctiewetgeving is daarom van groot belang.

Exportwet en dual use guidelines

Exportcontroles zijn bedoeld om de uitvoer en communicatie van gevoelige technologie of strategische goederen te beperken. Soms is onderzoek of een product interessant voor zowel burgerlijke als militaire toepassingen. Dit heet dan 'dual use'. Denk aan onderzoek naar carbon, dat wordt gebruikt voor windturbinebladen en fiets(en)(helmen), maar ook voor militaire drones. Encryptiesoftware is nuttig om diefstal van gegevens te voorkomen, maar kan ook gebruikt worden in een militaire context.

Om het proliferatierisico te beperken, worden dual use goederen, software of technische kennis niet uitgevoerd naar bepaalde landen, entiteiten of individuen, conform de verplichtingen die de overheid oplegt. Export control regulation is bindend, ook voor onze sector. Overtredingen worden gesanctioneerd onder de wet economische delicten. Voor uitvoer van dual use goederen, software of technische kennis naar andere landen, is het nodig om een exportvergunning aan te vragen.[15] In mei 2021 is de nieuwe 'EU Regulation for Export Controls of Dual Use Goods' aangenomen door de Raad van de Europese Unie. Hierin is onder andere meer aandacht voor cyber- en surveillancetechnologieën die gebruikt kunnen worden voor mensenrechtenschendingen buiten de EU.

Uit inventarisatie blijkt dat enkele universiteiten momenteel monitoren hoe deze nieuwe wetgeving de academische vrijheid raakt en welke impact dit heeft op onderwijs en onderzoek.

Nationaal

Missile Technology Control Regime (MTCR)

Het kabinet maakt zich in toenemende mate zorgen over het ballistische raketprogramma van Iran en heeft om die reden het toezicht op studenten en onderzoekers die een link kunnen hebben met het Iraanse ballistische raketprogramma verscherpt. EU Iran-sanctieverordening 267/2012 vormt daarvoor de juridische basis. Hiervoor is een toetsingskader opgesteld dat

15 Meer informatie is te vinden: EU compliance guidance for research involving dual-use items

voorziet in de screening van alle studenten en onderzoekers die op dit moment studeren of onderzoek verrichten binnen specifieke onderwijs- en onderzoeksgebieden, waarin kennis kan worden opgedaan die relevant is voor het Iraanse ballistische raketprogramma. Deze lijst met onderwijs- en onderzoeksgebieden is in samenwerking met betrokken universiteiten vastgesteld.

Expertise- en adviesloket Kennisveiligheid

In de Kamerbrief is de precieze invulling van dit nationale loket nog niet nader uitgewerkt, dit zal later in 2021 gebeuren. Gezien de naamgeving verwachten wij voornamelijk een adviserende en ondersteunende rol, eventueel signalerend of handhavend in acute situaties.

Universiteiten

Colleges van bestuur ontwikkelen richtlijnen ten aanzien van kennisveiligheid, implementeren procedures en gedragscodes en zien toe op nakoming. Onderzoekers en vakgroepen houden zich aan gedrags- en integriteitscodes, signaleren kwesties rond kennisveiligheid en kaarten die aan. Dit kader bouwt dan ook voort op de Nederlandse gedragscode wetenschappelijke integriteit en de Code goed bestuur universiteiten, specifiek de volgende passages:

Nederlandse gedragscode wetenschappelijk integriteit:

- "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'). Deze verplichtingen van de instelling zijn zorgplichten."
- "Zorg ervoor dat alle relevante wettelijke voorschriften, gedragscodes, instructies en protocollen worden nageleefd."

Code goed bestuur universiteiten:

- "Aan de universiteit worden waarden gehanteerd die passen bij haar maatschappelijke opdracht. De universiteit bevordert een open cultuur waarin ieder onderwerp ter sprake kan komen en waarin bestuurders, medewerkers en studenten zich vrij voelen om elkaar aan te spreken. Die cultuur wordt uitgedragen binnen en buiten de organisatie."
- "De universiteit bevordert het realiseren van een veilige omgeving waar studenten en medewerkers zich kunnen ontplooien en zich professioneel kunnen ontwikkelen."

Er zijn onvrije landen waar de kennisinstellingen onder direct bewind van de autoriteiten vallen. Als een samenwerkingspartner een openbare instelling is of nauwe banden heeft met de overheid, kan dit van invloed zijn op de inhoud van de samenwerking en op alle eventuele toekomstige geschillenprocedures. In een dergelijk geval moet altijd gekeken worden of alle academische waarden, zoals beschreven in de gedragscode wetenschappelijke integriteit, geborgd kunnen worden.

Voor het inrichten van een solide structuur van *checks and balances* op universiteiten is het volgende nodig:

Rijksoverheid	Universiteit
– in continuïteit beschikbaar stellen van inventarisatie van landen, bedrijven en opleidingen die door de overheid als risicovol zijn bestempeld; – inrichten van het advies- en expertiseloket kennisveiligheid voor informatie over bedrijven of landen en voor delen van dilemma's over samenwerkingsvormen; – functioneren als informatiepunt voor HR-medewerkers over risico's bij aanstelling van medewerkers of instroom van studenten ; – bepalen heldere taakverdeling en rolopvatting van betrokken diensten, zoals AIVD en MIVD, inzake het screenen van projecten, bedrijven/organisaties, personen en consortia.	– vertalen van die (risico)inventarisatie naar faculteiten, opleidingen en onderzoeksgroepen; – bepalen van kader/beslisboom met impactgebieden en bijbehorend risico-analyseproces. Hierin is aangegeven welke analyse nodig is voor welk type samenwerkingsvorm; – vormgeven governance/besluitvormings-structuur voor welke soort samenwerking en/of kennisveiligheidsrisico op welk niveau advies of akkoord nodig is; – maken van afspraken over periodieke toetsing: door wie, wanneer en met welke rapportage- en escalatielijnen.

Zowel de rijksoverheid als de universiteiten hebben een relatie met de EU en met andere landen daarbinnen en daarbuiten. Wat betreft de EU gaat het niet alleen om onderwijs, onderzoek en export- en handelsbeleid, maar is ook digitaal (cyber security) beleid steeds relevanter voor onze sector. In al deze domeinen worden maatregelen getroffen die kennisveiligheid raken, zoals blijkt uit de recente aanscherping van Horizon-2020-deelname voor China en de VS.

In het volgende hoofdstuk over risicomanagement zijn bovenstaand proces en kader richtinggevend uitgewerkt.

Hoofdstuk 4

Risicomanagement

Hoofdstuk 4
Risicomanagement

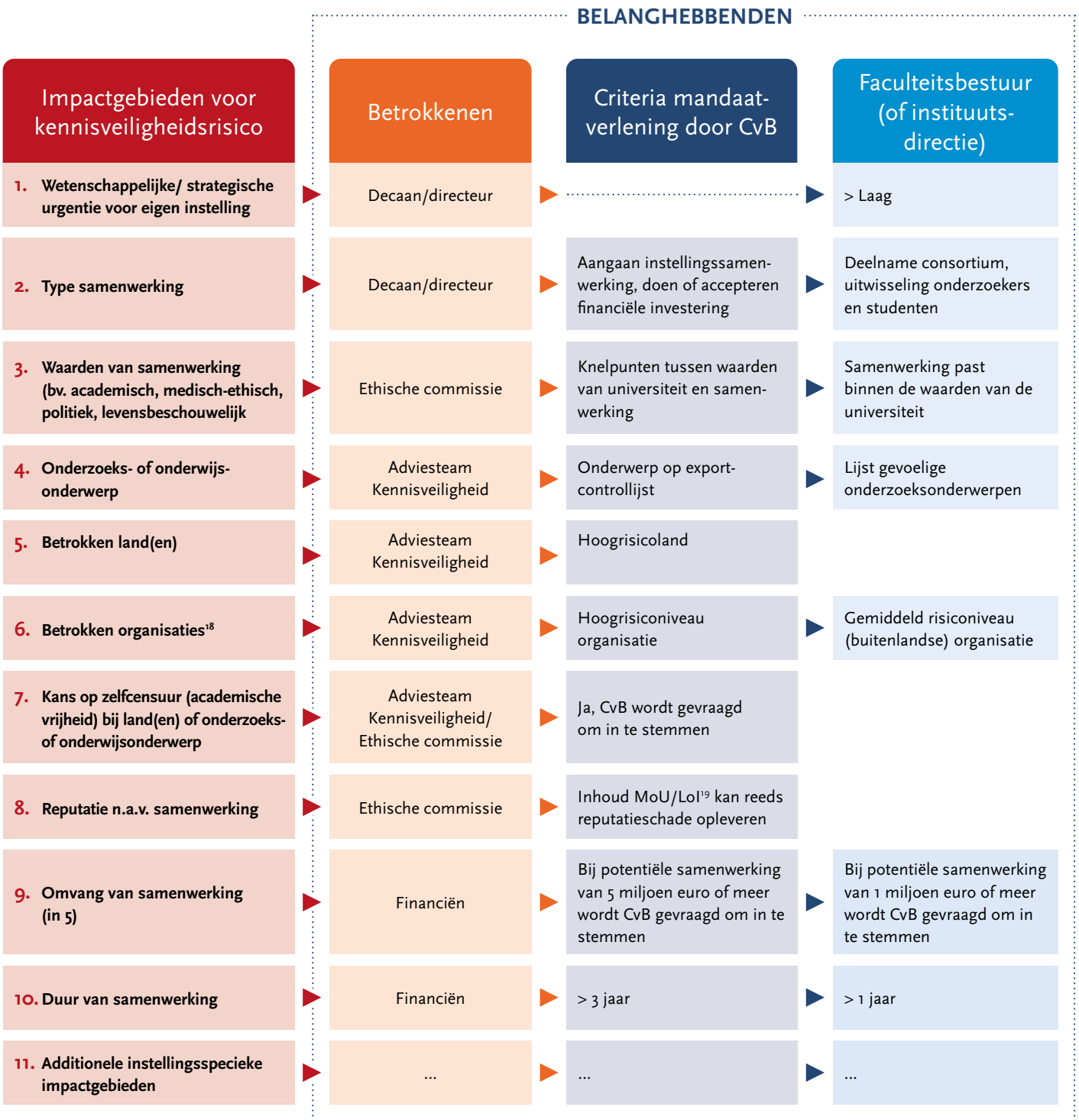
Lokale inbedding

Zoals eerder uitvoerig besproken, rust de eindverantwoordelijkheid voor kennisveiligheid in een instelling bij het CvB en de RvT. Het CvB zal vervolgens besluiten dat het een of meerdere organen binnen zijn instelling mandateert met beslissingsbevoegdheid tot een bepaald risiconiveau. In zoverre sluit kennisveiligheid aan bij de risicobeheersing op andere veiligheidsdomeinen. Elke instelling (en elk CvB) heeft andere kenmerken, profielen en gebruiken die meewegen in het bepalen van het te mandateren risiconiveau en de plaats waar dat mandaat wordt belegd.

Om CvB's te ondersteunen in die beslissing, zijn hieronder voorbeeld-impactgebieden en -criteria opgenomen die een plek zouden kunnen vinden in een beslisboom voor mandaat. Voor elk van de te kiezen impactgebieden kan het CvB bepalen wie bij welk criterium het mandaat heeft te besluiten. Nadat het mandaat is bepaald, volgt het gekozen gremium een gedetailleerder risicoproces (zie verderop). Voor elk van de voorbeeld-impactgebieden zijn typische belanghebbenden opgenomen die betrokken kunnen worden in het scoren van het impactgebied.[16]

16 Het scoren van het impactgebied zal voor de meerderheid van de casussen geen uitgebreide (feitelijke) analyse behoeven. Voor het betrekken van de genoemde belanghebbenden geldt ook dat in voorkomende gevallen die belanghebbenden niet betrokken zullen zijn.

Beslisproces impactgebieden en mandatering kennisveiligheid



17 Bij het beoordelen van de betrokken organisaties is het van belang ook de entiteitsstructuur van de organisatie in de beschouwingen te betrekken. Zo zou een te beoordelen kennisinstelling als organisatie in de laagste categorie kunnen vallen, maar wel dochter zijn van een buitenlandse organisatie die gelieerd is aan de overheid van een risicoland in een hogere categorie. Bovendien kunnen commerciële activiteiten van een universiteit (bv. spin-offs) ook betrokken zijn in onvrije landen.

18 Memorandum of Understanding / Letter of Intent.

Per casus kunnen alle impactgebieden worden 'ingevuld', en daar blijkt of het nodig zal zijn om de casus tot het CvB te brengen. In dit voorbeeld is ervoor gekozen om onderscheid te maken in twee niveaus: mandaat bij het CvB of bij het faculteitsbestuur. Het staat het CvB vrij om zelf invulling te geven aan het aantal niveaus, de impactgebieden en de bijbehorende criteria.

Adviesteam Kennisveiligheid

Het mandaat van het CvB om te beslissen (tot een bepaald niveau) over kennisveiligheidskwesties bevindt zich centraal en/of decentraal in de universiteit. Om die beslissingen te ondersteunen raden wij aan een Adviesteam Kennisveiligheid als virtueel team in te richten. Een dergelijk Adviesteam Kennisveiligheid moet zijn uitgerust met relevante deskundigen om over casuïstiek te adviseren. Uit een inventarisatie van besproken casuïstiek bij reeds bestaande Adviesteams, komen de volgende deskundigheden veelvuldig voor:

- deskundigen op het gebied van veiligheidsrisicomanagement (bv. adviseur integrale veiligheid of veiligheidscoördinator);
- deskundigen op het gebied van informatiebeveiliging (bv. informatiebeveiligingsmanager of (C)ISO, (Chief) Information Security Officer);
- deskundigen op het gebied van internationale samenwerking (bv. (senior) policy advisor).

Daarnaast blijkt per casus of additionele deskundigen of experts geraadpleegd dienen te worden. Te denken valt aan (onafhankelijke) deskundigen op het gebied van:

- onderzoeksonderwerp;
- betrokken landen of regio's;
- onderzoeksmethodiek;
- HR;
- valorisatie;
- data (bv. Research Data Officer);
- privacy & ethiek;
- inlichtingen & veiligheid;
- contractering (juridische zaken/inkoop);
- contactpersoon voor het (nog op te richten) nationale expertise- en adviesloket kennisveiligheid.

Uit de inventarisatie blijkt bovendien dat het expliciet oormerken van die additionele deskundigen bijdraagt aan hun betrokkenheid en inzet. Als laatste valt te overdenken, met name voor kleinere instellingen, of deskundigheid kan worden opgezet in een verband met meerdere universiteiten. Zo kan bepaalde landenexpertise, of expertise op onderzoeksonderwerpen bij de ene universiteit uitgeleend worden aan een Adviesteam Kennisveiligheid van een andere universiteit. Ook kan een shared service voor kleine instellingen worden ingericht via platform IV-HO om een proces te organiseren waar adviesteams van instellingen van elkaar kunnen leren.

De senioriteit van de betrokken deskundigen (met name het basisteam) is cruciaal voor de complexiteit van kennisveiligheidscasuïstiek. De belangen van betrokkenen zijn groot, en per definitie multidisciplinair. Het heeft de dringende aanbeveling om de inrichting van het Adviesteam Kennisveiligheid formeel te besluiten, en het Adviesteam directe escalatiebevoegdheid tot het CvB te geven (gevraagd en ongevraagd). Wanneer een universiteit ervoor kiest om meer dan één Adviesteam Kennisveiligheid in te richten (bv. om tegemoet te komen aan de decentrale inrichting van de universiteit), is het aan te raden één contactpersoon kennisveiligheid aan te stellen voor dit loket.

Ondersteunende processen

Om de risicomanagementprocessen van het gemandateerde gremium van de lijnorganisatie te ondersteunen bij kennisveiligheidscasuïstiek, zijn enkele ondersteunende processen onontbeerlijk: een doorlopende bewustwordingscampagne op de universiteit; het onder de aandacht brengen van de klokkenluidersregeling in relatie tot kennisveiligheid; en een centrale vastlegging van samenwerkingen met partners van buiten de EU.

Bewustwordingscampagne

De Kamerbrief Kennisveiligheid beschrijft dat het bewustzijn van kennisinstellingen over kennisveiligheid nog onvoldoende is. Een bewustwordingscampagne moet worden ingericht om het bewustzijn te verhogen op alle niveaus en functies, van CvB tot individuele onderzoekers en van faculteiten tot ondersteunende diensten. Bewustwording is echter geen eenmalige exercitie: aandacht voor de risico's verslapt over tijd, het dreigingslandschap verandert continu en de instroom van nieuwe medewerkers (en daarmee cultuur) is hoog. Het doel van de bewustwording is om zowel de individuele verantwoordelijkheid van onderzoekers en vakgroepen, als de eindverantwoordelijkheid van het CvB te ondersteunen met concrete kennis over kennisveiligheid. Bescherming van de universiteit en haar medewerkers start met bewustwording van de aanwezige risico's.

De opzet en inhoud van bewustwordingscampagnes zullen in de regel sterk beïnvloed worden door de onderzoeks- en onderwijsonderwerpen, lopende en toekomstige samenwerkingen, de besturingsfilosofie, heersende cultuur en talloze andere criteria. Bij de opzet van de campagne raden wij aan om bij de inzet van media/vorm rekening te houden met het beoogde doel, zoals:

- Statische vormen als e-mail, posters en e-learnings lenen zich goed om medewerkers te informeren.
- Interactieve vormen als dilemmasessies en dialoogsessies lenen zich goed om medewerkers te overtuigen.
- Spelvormen als het nabootsen van een incident of het doorlopen van een fictieve casus lenen zich goed om gedrag bij medewerkers te borgen.

Voor de inhoud raden wij aan rekening te houden met de positie waar medewerkers zich in bevinden:

- Voor CvB-leden past complexe multidisciplinaire casuïstiek (bv. inclusief contact met pers of nationale overheid).
- Onderzoekers zijn meer gebaat bij het herkennen van verschijningsvormen van kennisveiligheidscasuïstiek in hun eigen onderzoeksgebied (bv. rondom zelfcensuur).
- Ondersteunende diensten zijn meer gebaat bij het herkennen van verschijningsvormen bij collega's (bv. beïnvloeding) of diensten (bv. cyberincidenten) waar zij mee werken.

Bij bewustwording over kennisveiligheid is flankerend aandacht nodig voor houdings- en gedragsaspecten. Er is een reëel risico op onterechte bejegening, uitsluiting en discriminatie van studenten en medewerkers uit hoogrisicolanden. Door te borgen dat bewustwording van de risico's niet doorslaat in vijandsbeelden, en studenten en medewerkers worden uitgesloten of onheus bejegend, houden we de academische waarden van vrijheid, respect en het open academisch gesprek hoog. Deze academische waarden moeten voorgeleefd worden, in het onderzoek, en vooral ook in de opleiding van jonge onderzoekers en het onderwijs in den brede.

Klokkenluidersregeling

Alle universiteiten beschikken al over een klokkenluidersregeling voor het (anoniem) melden van vermoedens van illegale of immorele praktijken binnen de universiteit. Daaronder vallen ook de beschreven kennisveiligheidsrisico's. Bij het vergroten van bewustzijn voor die risico's, dient ook het bestaan en de reikwijdte van de klokkenluidersregeling onder de aandacht te komen. Individuele medewerkers die zorgen hebben over kennisveiligheid, bijvoorbeeld bij een te optimistisch beoordeelde samenwerkingsovereenkomst, moeten weten dat zij bij een vertrouwenspersoon terechtkunnen om die zorgen te bespreken.

Samenwerkingsregister partners (van buiten de EU)

Uit het onderzoek van het Rathenau Instituut[19] blijkt dat niet alle universiteiten een eenduidig en overzichtelijk beeld hebben van de samenwerkingen die zij aangaan met partners van buiten de EU. Een dergelijk overzicht vormt de basis voor effectief risicomanagement, met name voor het kunnen toezien op en herzien van bekende risico's. Adviesteams Kennisveiligheid zullen betrokken moeten zijn bij de totstandkoming en het onderhouden van dergelijke vastleggingen. Bij voorkeur vindt die vastlegging centraal plaats: het CvB mandateert weliswaar mogelijk naar decentrale teams, maar dat ontslaat het CvB niet van de eindverantwoordelijkheid voor dit veiligheidsdomein. Een CvB hoort te allen tijde inzicht te kunnen hebben in de significante samenwerkingen die het aangaat, zonder daarvoor betrokken partijen nog te moeten consulteren. Bovendien draagt het centraal bijhouden van een dergelijk register bij aan de snelheid waarmee op eventuele WOB-verzoeken kan worden gereageerd.

19 Rathenau Instituut – Kennisveiligheid in hoger onderwijs en wetenschap: een gedeelde verantwoordelijkheid. 2021, 11 januari. Geraadpleegd via https://www.rathenau.nl/nl/berichten-aan-het-parlement/kennisveiligheid-hoger-onderwijs-en-wetenschap

Hierbij moet worden opgemerkt dat samenwerking vele verschijningsvormen kent en ruim kan worden geïnterpreteerd. Als een onderzoeker geregeld e-mailcontact heeft met een collega aan de andere kant van de wereld over een gezamenlijke interesse, kan dat gezien worden als samenwerking. Veel van dit soort samenwerkingen ontstaan bottom-up en komen en gaan voordat deze uitkristalliseren.

Introductie risicomanagement

De afgelopen jaren hebben universiteiten geïnvesteerd in het volwassener maken van hun risicomanagementprocessen. De VSNU, de Vereniging Hogescholen en het ministerie van OCW onderschrijven integrale veiligheid als methode om van regelgestuurd naar risicogestuurd veiligheidsbeleid te gaan.[20] Bij sommige universiteiten heeft dat inmiddels geleid tot harmonisering van de processen, wat in gereguleerde sectoren *enterprise risk management* wordt genoemd: een organisatiebrede, gestandaardiseerde inrichting van risicomanagement waarop veelal wordt toegezien door een onafhankelijk orgaan (bv. een risicocommissie). Voor universiteiten betekent dat in de regel dat risicomanagement plaatsvindt in zowel de haarvaten van de organisatie (bij de faculteiten en diensten), als op centraal niveau. Decentrale risico's rollen op naar centraal, waardoor daar een geïntegreerd risicobeeld ontstaat. Daarmee richt risicomanagement zich op zowel strategische, tactische als operationele risico's (wat belet ons om onze visie, strategie en beleidsplannen te realiseren?), waarbij er ook aandacht wordt besteed aan zogenaamde *upside risks* (wat is het risico van iets *niet* doen?). Het CvB en de RvT zijn zo beter in staat om de universiteit, haar belangen, haar medewerkers en de samenleving te beschermen. Een goed functionerend risicomanagementproces onderbouwt en legitimeert de keuzes van het CvB.

Kennisveiligheid zal een plek moeten krijgen binnen de bestaande risicomanagement-processen. Zij kan daardoor meeliften op de volwassenheid van de bestaande processen. Bovendien is kennisveiligheid een dermate multidisciplinair risicogebied, dat integraal georganiseerd veiligheidsrisicomanagement een cruciale voorwaarde is voor een succesvolle implementatie van dit kader. Voorbeeld zijn (mede gebaseerd op de Kamerbrief):

- toegang tot fysieke ruimtes met gevoelige technologie;
- pre-employment screening van medewerkers voor hoogrisico-onderwerpen;
- inkoop van geavanceerde computersystemen uit hoogrisicolanden;
- toetsen van externe financiering;
- aanpak van *insider threat*-risico's van medewerkers;
- reageren op een melding middels de klokkenluidersregeling.

20 Platform Integrale Veiligheid Hoger Onderwijs – Integraal veiligheidsbeleid in het hoger onderwijs. Een intentieverklaring voor de sector en overheden

Uit de voorbeelden wordt duidelijk dat risicomanagement twee sporen kent: een continu risicomanagementproces en ad-hocactiviteiten (risicoanalyses). Voor beide sporen kan in de regel hetzelfde proces worden gevolgd van risico-identificatie, risicoschatting, risicoreactie en risicomonitoring. Om die processen effectief te ondersteunen is er een inrichtings- en onderhoudsproces (de 'Plan-Do-Check-Act'-cyclus van Deming) nodig. Dat proces is de smeerolie van de losse activiteiten en sporen, en bevat doorgaans:

- een beschrijving van het risicomanagementproces en -stappen, inclusief rollen en verantwoordelijkheden;
- een afgesproken risicotaal, bijvoorbeeld in de vorm van een risicotabel of een *business impact reference table*;
- risicocategorieën inclusief de bijbehorende risicobereidheid;
- een link naar bewustwordingsprocessen van medewerkers voor de verschillende risicogebieden;
- een gestandaardiseerde aanpak en template om risico's te identificeren, inclusief 'triggerlijsten;
- een gestandaardiseerde aanpak en template om risico's te schatten op basis van impact en kans;
- een gestandaardiseerde aanpak om een risicoreactie te kiezen;
- een risicoregister[21] om restrisico's en maatregelen in bij te houden en te monitoren;
- een evaluatiesysteem om de effectiviteit van het gehele risicomanagementproces te beoordelen en tot verbeteringen te komen.

Due diligence/vooronderzoek

Een van de ad-hocprocessen als onderdeel van risicomanagement is het uitvoeren van *due diligence* of zorgvuldig vooronderzoek naar samenwerkingsverbanden. Er zijn twee natuurlijke momenten waarop zo'n proces kan worden gestart: voorafgaand aan een nieuwe samenwerking en bij de verlenging van een samenwerking. Om dit risicomanagementproces ook op lopende samenwerkingen toe te passen is, zeker bij grote universiteiten, een grote investering nodig. Het is daarom verstandig om lopende samenwerkingen enkel op basis van een hoog kennisveiligheidsrisico tegen het licht te houden. Bijvoorbeeld bij samenwerkingen met hoogrisicolanden elke twee jaar een verkorte due diligence.

Kennisveiligheid is een van de onderwerpen die bij een due diligence van belang zijn, naast vele andere onderwerpen (bv. reputatie, wetenschappelijke integriteit, financiën, governance). De te beoordelen risico's kunnen worden geïdentificeerd, gewogen en beoordeeld aan de hand van het generieke risicomanagementproces voor kennisveiligheid. Het Adviesteam Kennisveiligheid kan hierbij worden geconsulteerd. De beslissing om een samenwerking aan te gaan (al dan niet na het treffen van aanvullende maatregelen), ligt bij de lijnorganisatie en moet een afgewogen besluit zijn op basis van, maar niet uitsluitend, kennisveiligheid.

21 Let op: het betreft hier een instellingsbreed risicoregister, en niet enkel dat van Kennisveiligheid.

Risico-identificatie

Als onderdeel van het reguliere risico-identificatieproces dient kennisveiligheid te worden meegenomen. De complexiteit van deze risico's vraagt om naast reguliere risicomanagers ook expertise van kennisveiligheid expliciet te betrekken (bv. het Adviesteam Kennisveiligheid). Tijdens risico-identificatie kan vervolgens effectief gewerkt worden door het gebruik van zogenaamde 'triggerlijsten' voor aspecten van kennisveiligheid. Die lijsten kunnen gebruikt worden om individuen betrokken bij het proces te herinneren aan ontwikkelingen die spelen, of casuïstiek die belangrijk kan zijn.

Voorbeelden van triggerlijsten om het proces te ondersteunen zijn een lijst met:
- hoogrisicolanden of anderszins onvrije landen;
- onderzoeks- en onderwijsonderwerpen die gevoelig zijn, of op exportcontrollijsten voorkomen;
- incidenten op de eigen universiteit of breder verkregen via bijvoorbeeld het nationaal loket, van de inlichtingen- en veiligheidsdiensten, koepels of uit de media;
- vakgroepen om periodiek ontwikkelen van die vakgroep naar boven te halen in het proces;
- recente geopolitieke en technologische ontwikkelingen relevant voor de universiteit.

Als invoer voor risico-identificatie kunnen bovendien ook worden meegenomen:
- meldingen uit de klokkenluidersregeling;
- meldingen vanuit het nationaal loket, het Adviesteam Kennisveiligheid of andere relevante meldingen;
- incidenten uit het verleden;
- nieuwe samenwerkingsverbanden;
- volledige lijst samenwerkingsverbanden.

Risicoschatting

Voor het inschatten van risico's kan gebruik worden gemaakt van de begrippen *kans* en *impact* om te bepalen hoe groot een risico voor de instelling is. Veel universiteiten werken met gestandaardiseerde impactcategorieën en risicotaal, dit vergemakkelijkt het schatten van risico's aanzienlijk. Bovendien kan het helpen om scenario-gebaseerd te werken voor geïdentificeerde risico's die lastig te schatten zijn. Het kan echter zo zijn dat de huidige impactcategorieën nog onvoldoende zijn uitgerust om impact van kennisveiligheid te vatten.
Ter overweging volgt een aantal (gedetailleerde) voorbeelden van impact dat een plek zou kunnen verdienen tussen de huidige impactcategorieën, dit betreft de impact op:
- academische vrijheid (het mogen publiceren of woordvoering over mogen voeren);
- de waarden van medewerkers (gelijke behandeling ongeacht geslacht, seksualiteit of levensovertuiging);
- de fysieke of intellectuele vrijheid van medewerkers;
- de innovatiekracht van Nederland.

Risicoreactie

In lijn met de standaardrisicomanagementprocessen, volgt er een reactie op geschatte risico's. De reactie is veelal gebaseerd op een risicobereidheid van de universiteit. Standaardreacties betreffen:

- Risicoacceptatie. Cruciaal is vastlegging in een risicoregister, inclusief risico-eigenaar en einddatum voor de huidige risicoacceptatie.
- Nemen van maatregelen. Cruciaal is vastlegging in een risicoregister, inclusief genomen maatregelen en hoe die de transitie van een inherent risico naar een restrisico ondersteunen.
- Uit de weg gaan van het risico. De keuze voor het uit de weg gaan van het risico kan toekomstig risicomanagement beïnvloeden, daar kan vastlegging toe bijdragen.
- Delen van het risico. Relatief ongebruikelijk, maar universiteiten zouden het risico kunnen delen met andere (onderwijs/research)instellingen, overheid of zelfs een verzekeraar.

Risicomonitoring

Een solide risicomanagementproces monitort of restrisico's na de risicoreactie op de geïdentificeerde en geschatte risico's veranderen. Verandering van restrisico kan plaatsvinden door een verandering in het onderliggende risico (dus een verandering van kans en impact) of doordat de effectiviteit van de risicoreactie verandert (bv. doordat de maatregelen niet effectief blijken, of de risicoacceptatie over datum gaat). Risicomonitoring maakt voor dit proces gebruik van het risicoregister, waarin minimaal het inherente risico, de risicoreactie, het restrisico en de risico-eigenaar zijn opgenomen. Periodiek wordt geëvalueerd of er relevante veranderingen hebben plaatsgevonden, waarna risico-identificatie, -schatting en -reactie worden heroverwogen.

Overgangssituatie

Voor universiteiten die het risicogebied kennisveiligheid nog niet integraal hebben opgenomen in hun risicomanagementprocessen is een overgangssituatie van toepassing. De overgangssituatie bestaat uit een aantal fases, waarvan enkele parallel zouden kunnen worden doorlopen.

1. ***Inrichting Adviesteam Kennisveiligheid***: cruciale eerste stap is de inrichting van het Adviesteam. Zodra andere fases starten, zal het Adviesteam naast coördinerende activiteiten ook direct om advies worden gevraagd in lopende vraagstukken.
2. ***Instellen beslisboom impactgebieden en mandatering kennisveiligheid***: als het Adviesteam is opgericht, raden wij aan de buitenste vangrails voor kennisveiligheid aan te leggen via de Beslisboom impactgebieden en mandatering. Die vangrails geven richting aan de vervolgfases en brengt het Adviesteam in positie.
3. ***Bewustwordingscampagne kennisveiligheid voor CvB, decanen en directeuren***: als de vangrails en het Adviesteam zijn ingericht, kunnen de eerste casussen worden aangedragen. Vermoedelijk gaat dit in eerste instantie enkel om nieuwe, of te verlengen, internationale samenwerkingsverbanden of reeds bestaande andere situaties die van belang zijn voor de kennisveiligheid.

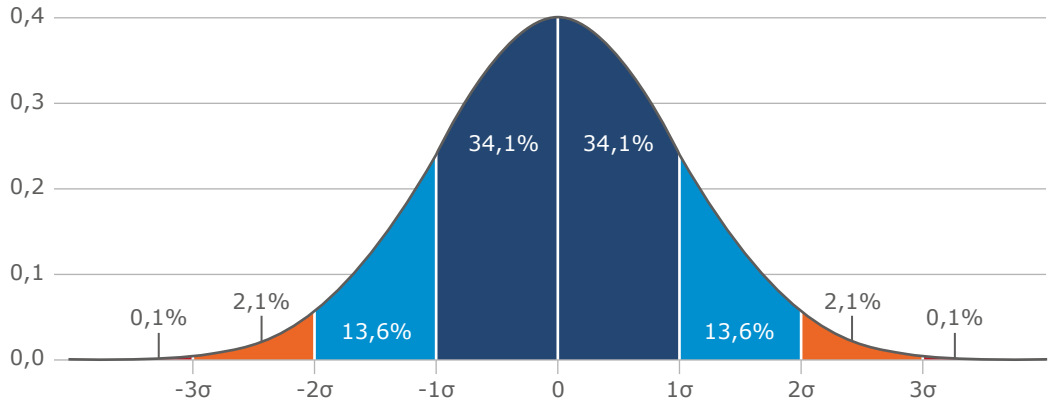
4. ***Inbedding kennisveiligheid in bestaande risicomanagementprocessen***: als het Adviesteam heeft proefgedraaid op internationale samenwerkingsverbanden, kan het risicogebied kennisveiligheid breder worden ingebed in bestaande risicomanagementprocessen.
5. ***Bewustwordingscampagne voor vakgroepen, onderzoekers en diensten***: parallel aan de inbedding van kennisveiligheid in bestaande risicomanagementprocessen, kan de aandacht voor dit risicogebied onder vakgroepen, onderzoekers en diensten verder onder de aandacht worden gebracht aan de hand van een bredere bewustwordingscampagne.
   Die bewustwordingscampagne kan putten uit behandelde casuïstiek van de vorige fases.
6. ***Inbedding in integrale veiligheid***: als laatste vindt kennisveiligheid geleidelijk haar inbedding binnen integrale veiligheid. De raakvlakken van kennisveiligheid zijn even divers als die van integrale veiligheid. Succesvol kennisveiligheidsbeleid in de geest van dit kader dekt uiteindelijk alle beleidsterreinen. Het versterken ervan maakt alle schakels van de ketting sterker.

Uit analyse van universiteiten die al zijn begonnen met het risicogebied kennisveiligheid, volgt dat het multidisciplinaire belang van het risicogebied vraagt om daar géén specifieke kennisveiligheidsadviseur voor aan te stellen, maar om te werken met een (virtueel) team met verschillende expertisegebieden daarin verenigd. Effectieve behandeling van het risicogebied kennisveiligheid vraagt om capaciteit. De benodigde capaciteit zal per universiteit voor elke fase van de overgang wisselend zijn. Om met die onzekerheid om te gaan, kan het verstandig zijn om aanvankelijk te werken met projectcapaciteit. Wanneer de benodigde capaciteit beter te schatten is, kan permanente inrichting volgen.

Bijlagen

Schatting tijdsbesteding

Als voorbeeld kan de capaciteitsschatting van het Adviesteam worden berekend aan de hand van het aantal te beoordelen casussen. Ter illustratie maken we hieronder gebruik van een standaardnormaalverdeling om daarmee te rekenen, waarbij we specifiek kijken naar de verdeling van te beoordelen samenwerkingen naar risico voor kennisveiligheid.[22] De verwachting is dat veel van de samenwerkingen niet worden voorgelegd aan het Adviesteam na het doorlopen van de beslisboom (alles tot μ+σ: 84.1%). Van de samenwerkingen ter beoordeling (15.9% van totaal), verwachten wij dat de eerste 13.6 procentpunt consultaties van ongeveer één uur zijn. De volgende 2.1 procentpunt betreft relatief eenvoudige casuïstiek van 2½ uur per adviseur (samen één mandag) en de laatste 0.1 procentpunt diepere analyse van 2 dagen per adviseur (samen zes mandagen). Dat zou betekenen dat er per 5.000 samenwerkingen ongeveer 1 fte nodig is voor het Adviesteam Kennisveiligheid.



Figuur 1. Standaardnormaalverdeling Kennisveiligheidscasussen naar risico

Onderdeel verdeling	Percentage samen-werkingen	Tijdsbesteding Adviesteam KV per casus	Dagen per 5.000 samen-werkingen	Betrokkenheidsvorm
Tot μ+σ	84.1%	-	-	Adviesteam Kennisveiligheid niet betrokken
σ tot 2σ	13.6%	1 uur	680 uur	Consultatie (één uur)
2σ tot 3σ	2.1%	1 dag	840 uur	Analyse & advies
3σ en verder	0.1%	6 dagen	240 uur	Uitgebreide analyse
Totaal			**1,760 uur**	

Tabel 2. Voorbeeld tijdsbesteding Adviesteam Kennisveiligheid per 5.000 samenwerkingen

22 Er is geen wetenschappelijke basis om aan te nemen dat Kennisveiligheidscasuïstiek zich normaal gaat verdelen naar risico. Dit voorbeeld is enkel ter illustratie.

Deelnemers werkgroep

Naam	Rol	Universiteit
Floor van der Heijden	Voorzitter	TU/e
Anouk Tso	UPI	UvA
Daria Ratsiborinskaya	UPI	EUR
Rogier Ragetlie	IV	EUR
Leo Harskamp	IV	LEI
Yoni Shem Tov	IV	VU
Mireille van Emmerik	IV	UM
Raoul Vernede	UCISO	UU
Niek Brunsveld	AOV	UvA
Willem-Rutger van Dijk	AOV	TuD
Marieke Wagenaar	AOV	RUG
Mark Kas	AOV	RUG
Irna van der Molen	AOV	UT
Frans Pingen	AOV	WUR
Harry Steinbusch	China Netwerk	X
Lisa Gorter	Secretaris	VSNU
Anno Bunnik	Adviseur	VSNU
Jascha van Hoorn	Adviseur	VSNU
Willemijn Lamet	Adviseur	VSNU
Martijn Verwegen	Domeinleider	VSNU