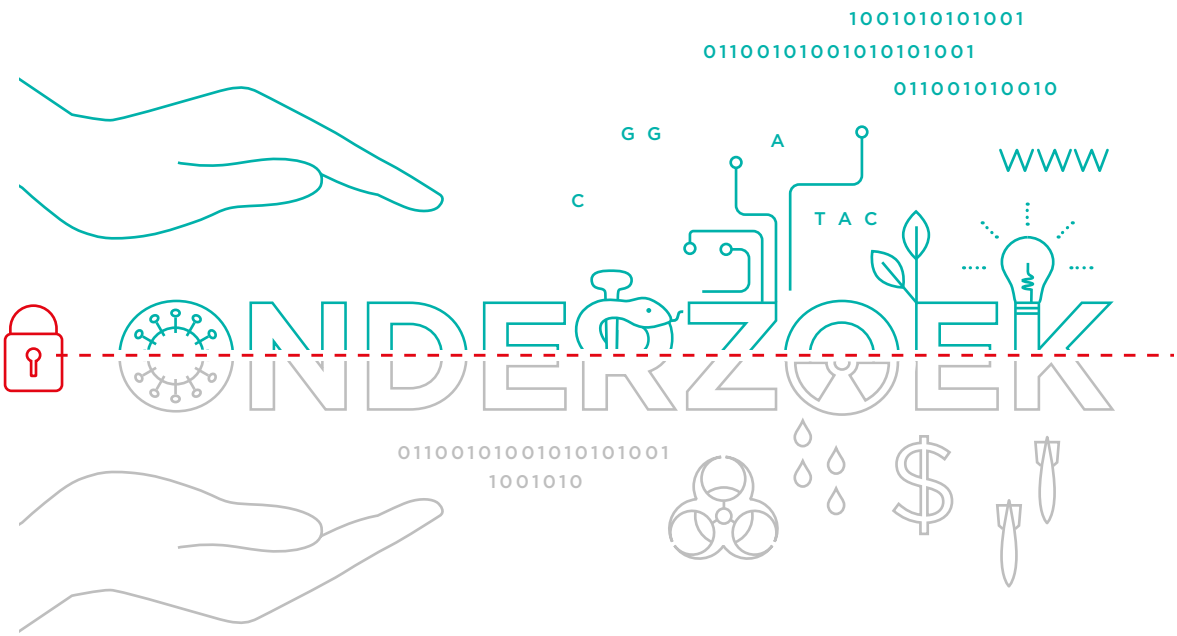
VLAAMSE INTERUNIVERSITAIRE RAAD

Richtlijnen voor onderzoekers over kennisveiligheid, dual use en misbruik van onderzoek



Deze Richtlijnen voor onderzoekers over kennisveiligheid, dual use en misbruik van onderzoek zijn ontwikkeld door de Vlaamse Interuniversitaire Raad (VLIR), meer bepaald door de leden van de VLIR Werkgroep Kennisveiligheid, Dual Use, Mensenrechten: Katleen Janssen, Inge Lerouge, Nynke Salverda (KU Leuven), Sarah Claes (UAntwerpen), Vincent Eechaudt (UGent), Stephanie Ruysschaert, Joke Kenens (UHasselt), Martyna Bajorinaite (VUB), en Filip Colson (VLIR).

Het is dus een product van de vijf Vlaamse universiteiten, maar waardevolle feedback op de sneuveltekst is gegeven door imec, VIB, het Instituut voor Tropische Geneeskunde, VITO en FlandersMake. De relevante contactpunten van die instellingen zijn ook opgenomen in deze Richtlijnen.

De illustratie op de cover is in opdracht van VLIR door Sisters of Design gemaakt. Het is gebaseerd op hun origineel werk voor Leopoldina, de Duitse Wetenschapsacademie. Van Leopoldina is toelating verkregen om een herwerkte versie voor VLIR te maken.

Verantwoordelijk uitgever:

Koen Verlaeckt, secretaris-generaal

Depotnummer: D/2025/2939/1

Vlaamse Interuniversitaire Raad | Flemish Interuniversity Council
Ravensteingalerij 27 bus 6, 1000 Brussel
+32 (0)2 790 67 20
administratie@vlir.be
www.vlir.be

Versie 1.0
Publicatiedatum: 29.09.2025

Richtlijnen voor onderzoekers over kennisveiligheid, dual use en misbruik van onderzoek

Ik wil een doctorandus die eerder werkte bij het leger van een land met een autoritair regime aannemen voor onderzoek over de detectie van stress en emoties via sensoren of hersenimplantaten. Waar moet ik rekening mee houden?

Ik zie een interessante oproep in het kader van het European Defence Fund. Kan ik hier zomaar op intekenen?

Ik wil samenwerken rond dronetechnologie met een universiteit in China. Kan dat?

Ik wil samenwerken rond het reduceren van geluid van vliegtuigmotoren met een bedrijf gevestigd in Malta. Er is weinig bekend over dit bedrijf, en er staat zeer weinig informatie op de website. Moet ik op mijn hoede zijn?

Ik ben gevraagd om onderzoek te doen naar diversiteit in opdracht van een buitenlandse overheidsinstelling, maar het is bekend dat de overheid een repressief beleid voert ten aanzien van het onderwerp. Kan ik dit onderzoek uitvoeren?

Deze richtlijnen beschrijven wat onderzoekers moeten doen wanneer er zorgen zijn over kennisveiligheid in hun onderzoek, met inbegrip van militair onderzoek, onderzoek naar dual use items, en wanneer er risico's op misbruik zijn, bijvoorbeeld op het gebied van mensenrechten of kwaadwillig gebruik.

Wat is kennisveiligheid?

Internationale samenwerking vormt de basis voor hoogstaand academisch onderzoek en onderwijs. De Vlaamse universiteiten streven naar een maximale samenwerking en open benadering van onderzoek, uitgevoerd binnen een context van academische vrijheid. Internationale samenwerking brengt echter ook risico's met zich mee. Deze uitdagingen kunnen worden gevat onder de term kennisveiligheid.

Kennisveiligheid is een verzamelterm voor het omgaan met risico's op:[1]

- **Ongewenste overdracht van gevoelige of kritieke kennis of technologie**[2] die de veiligheid van de Europese Unie of haar lidstaten kan bedreigen, bijvoorbeeld wanneer deze wordt gebruikt voor militaire of inlichtingendoeleinden in derde landen[3]. Denk bijvoorbeeld aan onderzoek naar dual use items samen met een partner die veel militair onderzoek doet of uit een land komt dat onder wapenembargo's of exportmaatregelen valt. Anno 2025 is dit bijvoorbeeld het geval voor Iran en (Wit-)Rusland.
- **Inmenging in onderzoek of onderwijs door of vanuit derde landen of externe partijen**. Dergelijke inmenging vormt een bedreiging voor de academische vrijheid, kan aanleiding geven tot zelfcensuur en tast de integriteit van onderzoekers aan. Dit risico kan ontstaan wanneer een onderzoeker financiering ontvangt uit een bepaald land of van een bepaalde externe partij, maar de onderzoeksresultaten nadelig zijn voor dat land/externe partij. In dat geval kan het land/externe partij proberen de onderzoeker onder druk te zetten om de resultaten aan te passen, niet transparant te communiceren, of de financiering in te perken.
- **Misbruik** (onethisch gebruik) **van onderzoeksresultaten en/of -data** (kennis of technologie) door derde partijen met als gevolg:
  - Het schenden of ondermijnen van mensenrechten of fundamentele Europese waarden.
  - Het ongewenst inzetten van onderzoek voor kwaadwillige doeleinden, zoals terroristische of criminele activiteiten.

Als onderzoeker moet je alert zijn voor mogelijke risico's, weten waar je relevante informatie kunt vinden, de wettelijke en instellingseigen procedures en voorschriften respecteren, en vermijden dat je bewust of onbewust onaanvaardbare risico's neemt. Hoe je dit doet, lees je in deze richtlijnen. Het Contactpunt Kennisveiligheid van je instelling is er ook steeds om je te ondersteunen bij het beoordelen en inperken van de risico's.[4]

1 Aanbeveling van de Raad van 23 mei 2024 betreffende verbetering van de onderzoeksveiligheid, OJ C, C/2024/3510, 30.05.2024, ELI: http://data.europa.eu/eli/C/2024/3510/oj. De Aanbeveling gebruikt de termen onderzoeksveiligheid en research security. Deze richtlijnen gebruiken in het Nederlands de term Kennisveiligheid, omdat deze ondertussen reeds algemeen gangbaar is en overeenstemt met de Nederlandse terminologie

2 Kritieke technologie is 'kennis en technologie, met inbegrip van knowhow, in opkomende en disruptieve gebieden en op gebieden die belangrijk zijn voor economisch concurrentievermogen, sociaal welzijn en de veiligheid van de Unie en haar lidstaten en waar, als gevolg daarvan, te grote afhankelijkheid van derde landen niet wenselijk is, rekening houdend met de dynamische aard van onderzoeksveiligheid en veranderende risico's. Dit omvat, maar is niet beperkt tot, onderzoek en innovatie met potentieel voor tweeërlei gebruik', Aanbeveling van de Raad van 23 mei 2024 betreffende verbetering van de onderzoeksveiligheid, OJ C, C/2024/3510, 30.05.2024, ELI: http://data.europa.eu/eli/C/2024/3510/oj

3 Ibid.

4 Voor een overzicht van de contactpunten van alle instellingen, zie verder.

De Vlaamse kennisinstellingen beoordelen hun samenwerkingen aan de hand van de volgende principes:

Openheid van onderwijs en onderzoek: We streven naar maximale samenwerking en open onderzoek, maar beperken de samenwerkingen indien de risico's te groot zijn ('as open as possible, as closed as necessary').

Proportionaliteit: beperkingen kunnen enkel indien ze strikt noodzakelijk zijn, duidelijk gerechtvaardigd kunnen worden, en betrekking hebben op specifieke entiteiten (dus vb. geen volledig land uitsluiten).

Institutionele autonomie en academische vrijheid: onderzoekers hebben het recht om vrij en ongebonden onderzoek uit te voeren met partners naar keuze, binnen de grenzen van de mensenrechtentoets.

Landenneutraliteit: hoewel de risico's bij samenwerking met sommige landen groter kunnen zijn, is niet elke samenwerking met een risicoland per definitie verdacht. Kennisveiligheidsrisico's kunnen zich voordoen bij samenwerkingen met alle landen.

Wat zijn de risico's?

Een samenwerking is risicovol indien deze samenwerking de Europese veiligheid bedreigt, indien de onderzoeksresultaten later worden misbruikt om mensenrechten te schenden, indien kennis en resultaten op een niet toegelaten manier worden ontvreemd, of indien derde landen of externe partijen de resultaten wensen te censureren of beïnvloeden.

Of een samenwerking risicovol is hangt af van:

– Hoe gevoelig de technologie of het onderwerp is waarrond je werkt;

– De partners waarmee je samenwerkt, de financier of de opdrachtgever;

– Het land waarin de partners zich bevinden of het onderzoek plaatsvindt;

– De aard van de samenwerking.

Een onderzoek is niet problematisch *omdat* je onderzoek doet naar een gevoelig onderwerp, of omdat je samenwerkt met een partner betrokken bij de ontwikkeling van militaire technologie. Een risico stelt zich doorgaans pas wanneer verschillende risico-elementen samenkomen, bv. wanneer je onderzoek doet naar dual use technologie met een universiteit die technologie ontwikkelt voor het leger in een niet-democratisch land.

Niet elke samenwerking is problematisch, maar als er risico's zijn, moet je wel kunnen verantwoorden waarom deze niet gelden voor de samenwerking die je voor ogen hebt. Hieronder wordt ingegaan hoe je kan nagaan of het onderzoek risicovol is op het vlak van kennisveiligheid.

Voorbeelden van kennisveiligheidsrisico's:

Een onderzoeker die solliciteert op een openstaande vacature is afkomstig van een universiteit die direct betrokken is bij het nucleaire programma van Iran. Is deze onderzoeker welkom aan een Vlaamse universiteit?

Je werkt samen met een bedrijf rond genomische data. Dit bedrijf was in het nieuws over genetische profiling van etnische minderheden. Mag je data nog steeds opgestuurd worden voor analyse?

Je wordt gevraagd als co-promotor van een PhD-traject aan een Russische universiteit die op de Europese sanctielijst voorkomt. Is dit nog mogelijk?

Je wordt gecontacteerd door een Chinese topuniversiteit om een gastonderzoeker te ontvangen en samen te werken rond autonome schepen. Mag dat?

Je wil samenwerken met een onderzoeker werkzaam in een ziekenhuis dat nauwe banden heeft met het leger in een autoritair regime. Waar moet je aan denken?

Je wordt gevraagd door een Europese universiteit om metingen te doen op een staal. In het publicatieproces over deze metingen verschijnen coauteurs van universiteiten die gekend staan als Seven Sons of Defence. Wat moet je doen?

Onderzoeksonderwerp

Een onderzoeksonderwerp kan om verschillende redenen gevoelig of risicovol zijn. Hieronder gaan we in op:

– Onderwerpen die gevoelig zijn voor (buitenlandse) inmenging
– Kritieke technologieën (zoals gedefinieerd door de Europese Commissie)
– Dual use items en onderzoek
– Maturiteit van de technologie (TRL-level)

Bij een verhoogde gevoeligheid rond thema, materiaal of technologie kunnen er zowel ethische als wettelijke verplichtingen optreden. Zoals hierboven reeds vermeld is het in de meeste gevallen een hoger gevoelig onderwerp in combinatie met een risicovolle partner die tot kennisveiligheidsrisico's kunnen leiden.

Onderwerpen gevoelig voor (buitenlandse) inmenging

Bepaalde onderwerpen kunnen politiek gevoelig liggen of verboden zijn in het land dat onderwerp is van onderzoek of in het land waar het onderzoek plaatsvindt. Denk aan onderzoek naar minderheden, naar politieke overtuigingen, of maatschappelijke omwentelingen.

In andere gevallen kunnen onderzoeksresultaten gevoelig liggen voor bedrijven of onderzoeksinstellingen, omdat ze een bedreiging vormen voor de activiteiten van de partner. Denk aan onderzoek dat aantoont dat de producten of activiteiten van een bedrijf schadelijk zijn.

In dergelijke gevallen bestaat er een risico op inmenging of censuur door overheden of het bestuur van de partnerinstelling. Dit kan betekenen dat je onder druk wordt gezet of misleid wordt om

het onderzoeksonderwerp aan te passen, om de resultaten niet volledig te publiceren, of om de onderzoeksdata aan te passen. Je bent in het bijzonder vatbaar voor druk als je te afhankelijk bent van bepaalde buitenlandse financieringsbronnen.

Kritieke technologieën

De Europese Commissie identificeerde 10 kritieke technologiedomeinen waar de risico's het grootst zijn bij internationale samenwerking. In elk van deze domeinen is er een verhoogd risico:

- Op civil-military fusion, met name dat defensiebedrijven en militaire overheden zeer nauw samenwerken met universiteiten en onderzoeksinstellingen zodat innovaties snel doorstromen naar de militaire sector;
- Op misbruik, met name dat de technologie later wordt ingezet voor het schenden of beperken van mensenrechten (bv. surveillance, interne repressie);
- Dat de technologie van transformatieve aard is zodat de prestaties en efficiëntie aanzienlijk verbeteren en/of een radicale verandering kan betekenen voor bepaalde sectoren.

In elk van deze domeinen vraagt de Europese Commissie een risicobeoordeling van de samenwerking. Dat betekent dat er mogelijks beperkingen moeten ingevoerd worden zodat cruciale onderzoeksresultaten niet weglekken uit de EU, omdat dit de Europese veiligheid en economie bedreigt.

In elk van deze 10 domeinen moeten maatregelen genomen worden om te verzekeren dat de EU minder afhankelijk wordt van niet-EU lidstaten in de toeleveringsketen; dat de kritieke infrastructuur beter beveiligd wordt (fysiek en digitaal) en dat hoogtechnologische kennis niet naar derde landen weglekt.

Om de toegang tot kritieke technologieën te beperken, worden niet EU-entiteiten en door het buitenland gecontroleerde EU-entiteiten geweerd uit bepaalde Horizon Europe onderzoeksprojecten (bv. naar quantum technologies, critical raw materials, space)[5]. Om diezelfde reden kunnen bepaalde Chinese entiteiten (met name Huawei en ZTE) niet deelnemen aan Horizon Europe Innovation Actions.[6]

De volgende kritieke technologieën worden vermeld in de Annex bij de Europese Aanbeveling over Kritieke Technologiedomeinen.[7]

- Geavanceerde halfgeleidertechnologieën
  - Micro-elektronica, met inbegrip van processoren

5 Art. 22(5) Regulation 2021/695.

6 MEDEDELING VAN DE COMMISSIE, Uitvoering van de toolbox inzake 5G-cyberbeveiliging , https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

7 AANBEVELING (EU) 2023/2113 VAN DE COMMISSIE van 3 oktober 2023 over technologiegebieden die kritiek zijn voor de economische veiligheid van de EU met het oog op nadere risicobeoordeling met de lidstaten, https://eur-lex.europa.eu/eli/reco/2023/2113/oj.

- Fotonicatechnologieën (met inbegrip van high-energy lasertechnologieën)
- Hogefrequentiechips
- Apparatuur voor de fabricage van halfgeleiders met zeer geavanceerde knooppuntgrootten

– AI-technologieën

- High Performance Computing
- Cloud enedge computing
- Technologieën voor gegevensanalyse
- Beeldherkenning, taalverwerking, objectherkenning

– Kwantumtechnologieën

- Kwantumcomputing
- Kwantumcryptografie
- Kwantumcommunicatie
- Kwantumdetectie en -radar

– Biotechnologieën

- Genmodificatietechnieken
- Nieuwe genomische technieken
- Gendruk (Gene-drive)
- Synthetische biologie

– Geavanceerde connectiviteits-, navigatie- en digitale technologieën

- Beveiligde digitale communicatie en connectiviteit, zoals RAN & Open RAN (radiotoegangsnetwerk) en 6G
- Cyberbeveiligingstechnologieën, met inbegrip van cyberbewakings-, beveiligings- en inbraaksystemen, digitaal forensisch onderzoek
- Internet der dingen en virtuele realiteit
- Distributed ledger- en digitale-identiteitstechnologieën
- Begeleidings-, navigatie- en controletechnologieën, met inbegrip van avionica en mariene lokalisering

– Geavanceerde detectietechnologieën

- Elektro-optische, radar-, chemische, biologische, stralingsdetectietechnologieën en

'distributed sensing'

- Magnetometers, magnetische gradiëntmeters
- Sensoren voor het meten van elektrische velden onder water
- Zwaartekrachtmeters en -gradiëntmeters

– Ruimtevaart- en voortstuwingstechnologieën

- Technologieën die speciaal op de ruimtevaart zijn gericht, variërend van component- tot systeemniveau
- Technologieën voor bewaking vanuit de ruimte en aardobservatie
- Plaatsbepaling, navigatie en tijdsbepaling (PNT)
- Beveiligde communicatie, met inbegrip van LEO-connectiviteit (LEO: Low Earth Orbit — lage omloopbaan)
- Voortstuwingstechnologieën, met inbegrip van hypersonica en onderdelen voor militair gebruik

– Energietechnologieën

- Kernfusietechnologieën en -reactoren en elektriciteitsopwekking met kernfusie, radiologische conversie-/verrijkings-/recyclingtechnologieën
- Waterstof en nieuwe brandstoffen
- Nettonultechnologieën, met inbegrip van fotovoltaïsche energie
- Slimme netwerken en energieopslag, batterijen

– Robotica and autonome systemen

- Drones, (land)voertuigen en vaartuigen (in de lucht en op en onder water)
- Robots en robotgestuurde precisiesystemen
- Exoskeletten
- Op AI gebaseerde systemin

– Geavanceerde materialen, geavanceerde fabricage- en recyclingtechnologieën

- Technologieën voor nanomaterialen, slimme materialen, geavanceerde keramische materialen, 'stealth'-materialen, veilige en inherent duurzame materialen
- Additieve productie, ook in het veld
- Digitale gestuurde microprecisieproductie en kleinschalige laserbewerking/lassen
- Technologieën voor de extractie, verwerking en recycling van kritieke grondstoffen

(met inbegrip van hydrometallurgische extractie, biouitloging, filtratie op basis van nanotechnologie, elektrochemische verwerking en zwarte massa's)

Dual use items (inclusief exportcontrolewetgeving)

Dual use items zijn goederen, materialen, technologie, software en technische kennis die aan specifieke technische parameters beantwoorden en die omwille van hun eigenschappen nuttig kunnen zijn voor civiele, maar ook voor militaire toepassingen.

Hoewel dual use items ook onderzocht worden in onderzoeksprojecten met een militaire finaliteit (samenwerking met defensiebedrijven of Defensie of o.b.v. EDF of DEFRA-financiering), gebeurt onderzoek naar dual use items meestal in het kader van reguliere onderzoeksprojecten met een civiele finaliteit (FWO, Horizon, etc.). Niettegenstaande de civiele finaliteit van het onderzoek, zijn de materialen, onderzoeksdata en -resultaten ook nuttig in een militaire context, voor bijvoorbeeld de ontwikkeling van wapens, radars, geleidingstechnologie, raketgeleiding, nachtkijkers, communicatiemiddelen, beschermende uitrusting, observatie, navigatie, drones, etc.

Bij dual use onderzoek zijn de risico's inherent groter. Zeker wanneer je samenwerkt met partners actief in een autoritair regime of conflictgebieden, nemen de risico's op onethisch gebruik van je onderzoeksresultaten toe. De data en resultaten kunnen in deze landen namelijk gebruikt worden om de militaire capaciteiten van dat land te versterken, bijvoorbeeld omdat de partner waarmee je samenwerkt (ook universiteiten!) in het thuisland ook betrokken is bij militair onderzoek.

Dual use items worden vermeld in Annex I van de Europese Dual Use Verordening (EU) nr. 2021/821. Deze items zijn per definitie gevoelig, omwille van mogelijk militair eindgebruik, gebruik voor massavernietigingswapens, of gebruik voor schendingen van mensenrechten, interne repressie of terroristische toepassingen. Hoe je zo efficiënt mogelijk kan bepalen of jouw onderzoek betrekking heeft op deze dual use items, vind je terug in de Annex of op de website van je onderzoeksinstelling. De wet beperkt samenwerkingen met niet-EU lidstaten rond dual use items.

Dual use exportcontrolewetgeving

Werk je met dual use items vermeld in de Dual Use Verordening én wil je deze items delen met partijen buiten de EU? Dan heb je een dual use exportvergunning nodig.[8]

Een exportvergunning heb je niet enkel nodig voor de fysieke verzending van materiële goederen. Ook het delen van immateriële zaken (software, technische kennis) wordt beschouwd als export.

8 Voor bepaalde gevoelige technologie heb je ook een vergunning nodig voor intra-EU transfers. Het gaat onder meer over nucleaire technologie, materialen voor het absorberen van elektromagnetische straling, of cryptoanalyse.

Deel je dual use goederen, software, technologie of technische kennis buiten de EU? Dan vraagt het contactpunt aan je universiteit een exportvergunning aan. Elke onderzoeker is binnen de instelling verplicht te melden wanneer dual use items buiten de EU worden gedeeld zodat een wettelijk verplichte vergunning kan aangevraagd worden. Zowel de instelling als de onderzoeker zijn strafrechtelijk aansprakelijk indien de items gedeeld worden zonder exportvergunning.

Twijfel je of de items die je wil delen vermeld staan op de EU dual use controlelijst? Neem contact op met het contactpunt aan je instelling.

Maturiteit van de technologie

Toegepast onderzoek naar technologieën is risicovoller dan fundamenteel onderzoek. Fundamenteel onderzoek focust namelijk op de fundamentele beginselen van verschijnselen of waarneembare feiten en is niet gericht op een bepaald praktisch doel of oogmerk. Toegepast onderzoek waarbij bepaalde technologieën ontwikkeld worden is een pak gevoeliger, gelet dat de technische kennis en onderzoeksresultaten sneller gebruikt of misbruikt kunnen worden in bepaalde toepassingen (en dus ook in een militaire context).

Om te bepalen of je aan fundamenteel onderzoek doet, kan je gebruik maken van de Technology Readiness Level (TRL) schaal. Dat is een schaal van 1 t/m 9 die economische toepasbaarheid van de technologie uitdrukt en die ook binnen Horizon Europe wordt gebruikt.[9]

Betreft het technologie met een TRL van 1 of 2, dan wordt er uitgegaan van fundamenteel wetenschappelijk onderzoek. Onderzoek naar technologie met een TRL van 3 of hoger is in principe toegepast onderzoek.[10] In dergelijke onderzoeksprojecten ontwikkel je een experimentele 'proof of concept' en is het gangbaar om samen te werken met partners uit de bedrijfswereld of het maatschappelijk middenveld.

Partner

Instelling (inclusief sancties)

Het risico bestaat dat de onderzoeksdata of -resultaten van je project doorstromen naar militaire diensten of veiligheidsdiensten, gebruikt worden voor de ontwikkeling van militaire technologie

9 Op het Horizon Europe NCP portal vind je een TRL assessment tool om het TRL niveau van je onderzoek te bepalen (zie https://horizoneuropencpportal.eu/store/trl-assessment). Ook de Canadese overheid biedt een eenvoudige checklist aan (zie : https://ised-isde.canada.ca/site/clean-growth-hub/sites/default/files/attachments/TRL-e.pdf.

10 Voor meer informatie, zie Aanbeveling (EU) 2021/1700 van de Commissie van 15 september 2021 inzake interne nalevingsprogramma's voor controles op onderzoek met betrekking tot producten voor tweeërlei gebruik uit hoofde van Verordening (EU) 2021/821 van het Europees Parlement en de Raad 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik, OJ L 338, 23.9.2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H1700.

of later misbruikt worden voor schendingen van mensenrechten (bijvoorbeeld interne repressie) of criminele activiteiten. Het is daarom belangrijk dat je nagaat of de partner waarmee je samenwerkt:

- Nauw verbonden is aan het leger of nationale veiligheidsdiensten (bijv. door samenwerking met het leger of defensiebedrijven of de ontwikkeling van defensietechnologie);
- Nauw samenwerkt met defensiebedrijven of bedrijven die veiligheidstechnologie ontwikkelen;
- Betrokken is bij de ontwikkeling van militaire of veiligheidstechnologie;
- Betrokken is bij discriminatie of bij schendingen of beperkingen van de academische vrijheid, de vrijheid van meningsuiting of andere mensenrechten.

Bedenk of critici de samenwerking kunnen gebruiken om je bevindingen in diskrediet te brengen, ongeacht de kwaliteit van het onderzoek zelf, of jij en/of je gastinstelling reputatieschade kunnen oplopen door de samenwerking met deze instelling, en of jij zelf in een moreel moeilijke situatie kunt terechtkomen.

Hoe beoordeel je de partnerinstelling?

- Bepaalde landen en organisaties zijn het voorwerp van sancties omdat ze een bedreiging vormen voor de veiligheid en/of de internationale vrede. De sancties tegen Rusland, Wit-Rusland en Iran springen hierbij het meest in het oog, maar er zijn nog andere entiteiten onderhevig aan sancties. Dergelijke sancties en maatregelen worden onder andere opgelegd door (internationale) instanties zoals de Verenigde Naties, de Europese Unie, de Vlaamse overheid, of door andere landen. Zo hebben de Verenigde Staten en Japan bijvoorbeeld uitgebreide sanctielijsten. Via www.opensanctions.org kan je controleren of jouw partner onderhevig is aan dergelijke sancties.
- Heel wat onderzoeksinstellingen zijn betrokken bij de ontwikkeling van defensietechnologie. Voor China en Iran zijn er specifieke websites beschikbaar:
  - The China Defence Universities Tracker: https://unitracker.aspi.org.au. (Deze staat sinds augustus 2025 achter een paywall, eind 2026 wordt een Europese alternatieve bron verwacht).
  - Iran Watch : https://www.iranwatch.org/iranian-entities.
- Bepaalde academische instellingen zijn betrokken bij mensenrechtenschendingen.
  - Scholars at Risk rapporteert over incidenten wereldwijd: https://www.scholarsatrisk.org/academic-freedom-monitoring-project-index.
  - Middle East Studies Association over incidenten in het Midden-Oosten: https://mesana.org/advocacy (gebruik de zoekfunctie).
- Bepaalde bedrijven zijn betrokken bij mensenrechtenschendingen of zware milieuschade.

- Het Noors Pensioenfonds rapporteert over een selectie beursgenoteerde bedrijven: https://www.nbim.no/en/responsible-investment/ethical-exclusions/exclusion-of-companies.
- Het Australian Strategic Policy Institute rapporteert over de verwevenheid van Chinese technologiebedrijven met de overheid en de activiteiten in Xinjiang: https://chinatechmap.aspi.org.au
- Business & Human Rights Resource Centre beheert een databank waarin het nieuws en aantijgingen rond mensenrechtenschendingen wordt bijgehouden voor meer dan 20 000 bedrijven: https://www.business-humanrights.org.
- Zoeken op de website van Human Right Watch kan inzichten bieden in een aantal grote bedrijven: www.hrw.org.

– Je kan uiteraard ook je partner rechtstreeks bevragen, de website van de kandidaat-partner raadplegen (bij voorkeur in de taal van regio waar de instelling zich bevindt, met een vertaalmiddel) of gebruik maken van zoekmachines of AI chatbots. Aan de chatbot kan je bijvoorbeeld vragen of je partner betrokken is bij mensenrechtenschendingen, bij militaire activiteiten, of bij controverses. Uiteraard geeft dit enkel een indicatie, en zal verder onderzoek nog steeds nodig zijn.

Indien de activiteiten of de doelstellingen van je partner onduidelijk zijn of moeilijk te achterhalen, kan de samenwerking ongewenst zijn. Het is namelijk belangrijk dat je weet wie je partner is en dat je kan verantwoorden waarom je samenwerkt, ongeacht de kwaliteit van het onderzoek zelf. Het contactpunt van je instelling kan je helpen met een screening van de partnerinstelling.[11]

> De Vlaamse universiteiten besloten in 2019 een **mensenrechtentoets** in te voeren. Die bepaalt dat we als instelling zelf geen mensenrechten wensen te schenden, maar ook dat we vermijden dat de onderzoeksresultaten later misbruikt worden voor mensenrechtenschendingen, én dat we samenwerkingen vermijden met partners betrokken bij ernstige mensenrechtenschendingen. Zelfs als het onderzoek geen verband houdt met de schendingen, is het partnerschap problematisch. A Als de samenwerking leidt tot meer positieve dan negatieve gevolgen voor de mensenrechtensituatie, kan die worden verdergezet mits monitoring.

Onderzoeker

Er is een groeiende bezorgdheid dat bepaalde landen via academische samenwerking en het uitsturen van studenten gespecialiseerde kennis opdoen, om die later in te zetten voor de ontwikkeling van militaire technologie. Dit betekent dat visumaanvragen voor onderzoekers uit deze landen langer kunnen duren en dat de kans groter is dat de visumaanvraag geweigerd wordt. Houd dit in het achterhoofd indien je werkt met gevoelige of strategische kennis en een onderzoeker wenst aan te werven van buiten de EU.

Bij inkomende onderzoekers (PhD students, exchange students, visiting researchers, …) is een

11 Voor de contactgegevens van jouw instelling, zie verder.

samenwerking risicovoller wanneer de inkomende onderzoeker slechts tijdelijk aan een Vlaamse instelling verblijft. In tegenstelling tot het uitvoeren van een volledig onderzoeksproject aan een Vlaamse instelling, worden er bij Joint PhD's, exchange students en visiting researchers, onderzoeksdata en -resultaten gedeeld met onderzoekers en instellingen in het buitenland en worden deze resultaten dus ook gebruikt voor (onderzoeks)activiteiten aan de buitenlandse instelling.

Afhankelijk van de eerdere werkervaringen en affiliaties van een inkomende onderzoeker, kan ook het risico in kaart worden gebracht of de opgedane kennis later gebruikt kan worden voor ongewenste doeleinden, en of de onderzoeker mogelijk onderhevig zal zijn aan externe druk (vanuit zijn overheid of thuisinstelling) om resultaten, data of materiaal te delen.

Het contactpunt van je instelling kan je helpen bij de risicoanalyses van inkomende onderzoekers.

Financier

Overheden, bedrijven of donateurs hebben bepaalde motieven om een onderzoek te financieren. In bepaalde gevallen kunnen onderzoeksresultaten gevoelig liggen voor financiers, omdat de resultaten een negatieve impact kunnen hebben op de bedrijfsvoering of politiek gevoelig kunnen zijn.

In dat geval bestaat er een risico op inmenging of censuur door overheden of het bestuur van de partnerinstelling. Dit kan betekenen dat je onder druk wordt gezet of misleid wordt om het onderzoeksonderwerp aan te passen, om de resultaten niet volledig te publiceren, of om de onderzoeksdata aan te passen. Hou er ook rekening mee dat deze druk groter kan worden wanneer je in een positie van financiële afhankelijkheid terecht komt van één financier.

Daarnaast kan een financier, net zoals een projectpartner, ook kwaadwillige intenties hebben met de resultaten van je onderzoek, of zijn echte intenties verborgen houden. Mogelijke signalen hiervoor zijn: de financier geeft bijzonder gunstige financieringsvoorwaarden, wil uitzonderlijk hoge bedragen betalen, of eist zeer ongewone technische specificaties die niet gangbaar zijn voor het betrokken onderzoek. Ook als er weinig tot geen informatie over de financier te vinden is (vb. geen website, geen corporate e-mailadres, geen Linkedin profiel), zijn er mogelijk redenen tot bezorgdheid.

Ook hier kan het contactpunt van je instelling je helpen met een risicoanalyse.

Land

Sommige landen vormen een bedreiging voor de Europese veiligheid. Het is dan risicovoller om samen te werken met organisaties of onderzoekers in die landen, in het bijzonder wanneer de partneruniversiteit of -bedrijf samenwerkt met defensiebedrijven of militaire overheden.

Bovendien komen in bepaalde landen en regio's mensenrechtenschendingen frequent voor. Dit risico verhoogt wanneer er een oorlog of gewapend conflict woedt in die regio.

Omwille van bovenstaande vaststellingen, vormen samenwerkingen met onderzoekers en organisaties in specifieke landen steeds een risico op het vlak van kennisveiligheid. Het gaat dan specifiek om **China, Iran, Israël, Noord-Korea, Pakistan, Rusland, Saoedi-Arabië, Syrië, Turkije, Verenigde Arabische Emiraten en Wit-Rusland**.[12]

Wanneer je samenwerkt met een partner in één van deze landen, is het extra belangrijk dat je informatie inwint over je partner en je de risico's van je samenwerking grondig evalueert. Wens je daar hulp bij, dan kan je het contactpunt van je instelling contacteren.

Internationale rankings tonen hoe verschillende landen scoren op het vlak van de rechtstaat, mensenrechten, democratie, en corruptie:

- Rule of Law Index
- Academic Freedom Index
- Democracy Index
- Corruption Index
- Freedom Index

Beleid van financiers en specifieke institutionele beperkingen

Omwille van kennisveiligheidsrisico's nemen financiers en onderzoeksinstellingen bepaalde maatregelen om deze risico's te beperken. Die kunnen inhouden dat samenwerkingen met bepaalde landen en/of instellingen uitgesloten worden en dat bepaalde onderzoeken alleen mogelijk zijn met risicobeperkende maatregelen. Hieronder volgt een niet-exhaustief overzicht.[13]

FWO kennisveiligheidsbeleid

FWO heeft in 2024 een eigen kennisveiligheidsbeleid gelanceerd, gebaseerd op vier pijlers: 1) risico-analyse van de eigen partnerschappen in het buitenland; 2) sensibilisering van de FWO-aanvragers via het toevoegen van een 'Research Security Appraisal' aan alle aanvragen; 3) monitoring in de rapportering; en 4) een beleid rond cyberveiligheid.

De Research Security Appraisal peilt naar de kennisveiligheidsrisico's van een onderzoeksproject in drie domeinen: het topic van het projectvoorstel, het land dat betrokken is bij het onderzoek, en de partner waarmee je samenwerkt. Wanneer een project op basis van de vragenlijst als 'hoog risico' wordt geclassificeerd, is een goedkeuring inzake kennisveiligheid van je instelling nodig. Voor meer informatie hierover en over de interne procedure kan je terecht bij het contactpunt van je instelling.

12 Lijst o.b.v. internationale sancties en Vlaamse exportmaatregelen.

13 De ethische self-assessment van Horizon Europe bevat onder meer een beoordeling van het mogelijke misbruik dat gemaakt kan worden van de onderzoeksresultaten (https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf).

Seven Sons of National Defence (China)

De Seven Sons of National Defence zijn een groep van 7 Chinese universiteiten die tot 2008 ondergeschikt waren aan het Ministerie van Defensie. De Seven Sons universiteiten besteden ongeveer de helft van hun onderzoeksbudget aan defensieonderzoek.[14] Ze hebben allemaal veiligheidsmachtigingen voor toegang tot de informatie die geclassificeerd wordt als 'zeer geheim'. Tot één op drie van de afgestudeerden van deze universiteiten vindt werk in de defensiesector.

Omwille van de risico's op civil-military fusion financiert het FWO geen samenwerkingen meer met deze universiteiten. Ook tekenen de Vlaamse universiteiten geen nieuwe institutionele samenwerkingsovereenkomsten met de Seven Sons of National Defence universiteiten.

Het gaat om Harbin Institute of Technology, Harbin Engineering University, Beijing Institute of Technology, Beihang University, Northwestern Polytechnical University, Nanjing University of Science and Technology en Nanjing University of Aeronautics and Astronautics.

In diezelfde zin worden er ook geen institutionele samenwerkingen aangegaan met Chinese militaire onderzoeksinstellingen.

Iran

Omwille van gevangenneming van dr. Ahmadreza Djalali, gastprofessor aan de VUB, door de Iraanse overheden, besloot de Vlaamse Interuniversitaire Raad dat institutionele samenwerkingen met Iraanse kennisinstellingen uitgesloten zijn.[15]

Rusland

In 2022 heeft de Russische rectorenconferentie een verklaring gepubliceerd ter ondersteuning van de Russische oorlog in Oekraïne, in navolging van het standpunt van Vladimir Poetin als zou de invasie in Oekraïne een noodzakelijke 'speciale militaire operatie' zijn met als doel 'de demilitarisering en denazificatie van Oekraïne te bewerkstelligen', een einde te maken aan het conflict in de Donbass en Rusland te beschermen tegen 'toenemende militaire dreigingen'. Daarom hebben de rectoren van de Belgische universiteiten beslist om geen institutionele samenwerkingen aan te gaan met de universiteiten die deze verklaring hebben ondertekend.[16]

De Europese Commissie besloot in maart 2022 om binnen het Horizon Europe onderzoeksprogramma geen nieuwe samenwerkingen met Russische organisaties meer aan te gaan en, in april 2022 via het vijfde sanctiepakket, om ook de lopende deelnames binnen Horizon 2020 te stoppen[17]. Ook het FWO financiert geen enkele samenwerking meer met (Wit-)Russische entiteiten.[18]

14 https://unitracker.aspi.org.au/glossary
15 https://vlir.be/nieuws/academische-samenwerking-met-iran-onmogelijk
16 https://vlir.be/nieuws/opschorting-samenwerking-rusland
17 https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/bilateral-cooperation-science-and-technology-agreements-non-eu-countries/russia_en
18 https://www.fwo.be/nl/over-fwo/onderzoeksbeleid/institutionele-beperkingen/

Militaire onderzoeksfinanciering

De Vlaamse universiteiten doen in eerste instantie onderzoek gericht op civiele toepassingen. Niettemin kan ook onderzoek plaatsvinden dat ook militair nuttig is (dual use) of een militaire focus heeft. Denk hierbij bijvoorbeeld aan samenwerkingen met de Koninklijke Militaire School of projecten in het kader van de Defence Research Action (DEFRA, gefinancierd door Defensie) en het European Defence Fund (EDF, gefinancierd door de Europese Unie).

Als onderzoeker ben je in principe vrij om al dan niet mee te werken aan projecten waarvan de onderzoeksresultaten ook militair nuttig kunnen zijn, binnen het ethisch kader van de onderzoeksinstelling. Deelname aan dergelijke projecten vraagt dus een persoonlijke ethische reflectie o.b.v. de eigen waarden en normen. Daarnaast moet je ook rekening houden met het beleid van de eigen instelling en de voorwaarden van de onderzoeksfinancier.

Het is belangrijk om voorzichtiger te zijn wanneer de financiering niet afkomstig is van de eigen overheid, EU/NAVO-programma's of bondgenoten en partnerlanden (inclusief private bedrijven), aangezien defensie en nationale veiligheid altijd in het belang van de nationale soevereiniteit staan.

Bij bepaalde onderzoeksprojecten wordt gewerkt met geclassificeerde informatie. Wanneer deze informatie geclassificeerd wordt als 'vertrouwelijk', 'geheim' of 'zeer geheim', dan kan je enkel werken met deze informatie indien je als onderzoeker over een individuele veiligheidsmachtiging beschikt. In het geval de informatie geclassificeerd wordt als 'beperkt' heb je geen individuele veiligheidsmachtiging nodig, maar zal je wel verschillende fysieke en digitale veiligheidsmaatregelen moeten nemen.

Om een individuele veiligheidsmachtiging te verkrijgen dien je aan strenge voorwaarden te voldoen. Meer info vind je op de website van de Veiligheid van de Staat: https://www.nvoans.be/nl/veiligheidsmachtigingen/individuele-veiligheidsmachtigingen. Een aanvraag voor een individuele veiligheidsmachtiging wordt aangevraagd door de veiligheidsofficier van je onderzoeksinstelling. Contacteer het contactpunt voor de aanvraag van veiligheidsmachtigingen en het invoeren van de nodige fysieke en digitale veiligheidsmaatregelen.

Financiers van militair onderzoek leggen ook andere beperkingen op aan onderzoekers. Zo bepalen de DEFRA-projectoproepen dat de betrokken onderzoekers de EU-nationaliteit moeten hebben, dan wel onderdaan moeten zijn van een land van de Europese Vrijhandelsassociatie of een NAVO-lidstaat. Bovendien kunnen de betrokken onderzoekers onderworpen worden aan een 'veiligheidsverificatie'.

Hoe kan je de risico's beperken?

Verantwoordelijkheid van de onderzoeker

Het is in eerste instantie aan jou om na te gaan of je onderzoek één of meerdere van de hierboven beschreven risico's met zich meebrengt. Wanneer dit het geval is, moet je overwegen of de mogelijke risico's te beheersen zijn door het nemen van mitigerende maatregelen.

Daarnaast moet je ook de toepasselijke wetgeving naleven. Je moet ook de interne procedures van je instelling naleven en je onderzoek aanmelden bij de ethische commissie of bevoegde dienst. In uitzonderlijke gevallen zal het onderzoek niet mogelijk zijn.

Mitigerende maatregelen

Als je kennisveiligheidsrisico's identificeert in je geplande onderzoek, tracht je maatregelen te nemen om die risico's te beperken. Die maatregelen kunnen betrekking hebben op het onderwerp of onderzoeksdesign; fysieke, organisatorische of cyberveiligheid; of de partner(s) waarmee je samenwerkt. Het contactpunt van je instelling kan je helpen met het maken van de risicoanalyse van je onderzoek, en het implementeren van de mogelijke mitigerende maatregelen.

Voorbeelden van mitigerende maatregelen die je kan nemen zijn:

- Het installeren van fysieke veiligheidsmaatregelen zodat gevoelige data en technologie enkel toegankelijk is voor de onderzoekers betrokken bij het project (bijvoorbeeld toegangsbeperkingen, het gebruik van een kluis).
- Het zorgen voor voldoende cyberbeveiliging: aparte netwerkschijven, anti-virus software, two factor authentication, de toegang beperken tot de onderzoekers betrokken bij het project, etc.
- Het nemen van voorzorgen bij internationale reizen (vb. het meenemen van een 'schone' laptop of GSM);
- Het volgen van een protocol voor bezoekers (vb. bezoekers steeds begeleiden, geen toegang geven tot ruimtes met strategische apparatuur);
- Het afsluiten van vertrouwelijkheidsovereenkomsten, het beschermen van intellectuele eigendom of het invoegen van clausules rond toegelaten eindgebruik in samenwerkingsovereenkomsten;
- Het voorzien van een publicatieclausule die voldoende garanties biedt dat vrij gepubliceerd kan worden over de resultaten;
- Het voorzien van verplichte 'veiligheidsopleidingen' (safety training) voor het onderzoekspersoneel;
- Het aanduiden van een onafhankelijke ethische adviseur of ethische board verbonden aan het

onderzoeksproject (los van de interne bevoegde commissie van je universiteit);

- Het aanpassen van het onderzoeksdesign, door bijvoorbeeld dummy gegevens te gebruiken, of de toegang tot onderzoeksdata te beperken op niveau van de deelnemers aan een werkpakket;
- Het als geheim aanmerken van bepaalde onderzoeksresultaten of de verspreiding van onderzoeksresultaten beperken, bijvoorbeeld door slechts een deel van de onderzoeksresultaten te publiceren.

Juridische verplichtingen of beperkingen

Je zal mogelijk ook onderworpen zijn aan juridische verplichtingen of beperkingen in het kader van je onderzoek. Wanneer je partner bijvoorbeeld onderhevig is aan internationale sancties, moet je nagaan wat je niet met hen mag delen, en of dit een impact heeft op je onderzoek.

Wanneer je onderzoek betrekking heeft op dual use items zoals vermeld in de Europese Dual Use Verordening nr. 821/2021, heb je mogelijk een exportvergunning nodig om materialen, software, of onderzoeksresultaten te delen met je partner buiten de Europese Unie. Dit kan ook het geval zijn wanneer je een lezing of workshop geeft buiten de EU óf online met deelname van buiten de EU. Die vergunning moet worden aangevraagd bij de Vlaamse of Brusselse overheid vóór de dual use items worden gedeeld. Contacteer voor ondersteuning hierbij het Contacpunt of de dienst bevoegd voor het aanvragen van vergunningen binnen je instelling.

Meldingsplicht

Wanneer er dual use of militair gebruik mogelijk is of een reëel risico op misbruik van onderzoek bestaat, dan geldt er voor iedere onderzoeker een meldingsplicht bij het Contactpunt. Dit geldt ook voor aanvragen (onderzoeksactiviteiten en/of partners) die mogelijk problematisch blijken op het gebied van mensenrechten (VLIR Mensenrechtentoets). In samenwerking met het Contactpunt worden maatregelen genomen om het risico op misbruik te beperken.

Het project niet opstarten of beëindigen

In uitzonderlijke gevallen zijn de risico's te groot om te mitigeren, of leent het onderzoek zich niet tot het nemen van mitigerende maatregelen. Dat kan ertoe leiden dat het onderzoek niet kan worden uitgevoerd. Het contactpunt binnen je instelling kan je ondersteunen bij deze beoordeling.

Wanneer de situatie tijdens een lopend project verandert en de kennisveiligheidsrisico's te groot worden om nog verder te werken, neem je contact op met het Contactpunt om te bekijken of en onder welke voorwaarden de samenwerking kan worden beëindigd.

Contactpunten aan de Vlaamse onderzoeksinstellingen betrokken bij deze richtlijnen

UAntwerpen

- Contactpunt Kennisveiligheid: researchsecurity@uantwerpen.be
- Ethische Commissie voor Misuse, Human Rights & Security | Universiteit Antwerpen (Ethische Commissie voor Misuse, Human Rights & Security (MiHRS))
- +32 3 265 90 63
- https://www.uantwerpen.be/nl/onderzoek/beleid/ethiek-integriteit/dual-use-misuse-military-use/
- https://www.uantwerpen.be/nl/onderzoek/beleid/ethiek-integriteit/kennisveiligheid/
- https://www.uantwerpen.be/nl/onderzoek/beleid/ethiek-integriteit/mensenrechten/

UGent

- Contactpunt Kennisveiligheid: researchsecurity@ugent.be
- https://ugentbe.sharepoint.com/sites/intranet-onderzoek/SitePages/Kennisveiligheid.aspx
- Informatie over onderzoek met militair onderzoek, dual use items en exportcontrole: https://ugentbe.sharepoint.com/sites/intranet-onderzoek/SitePages/Onderzoek-naar-dual-use-items.aspx
- Informatie over het UGent Mensenrechtenbeleid: https://ugentbe.sharepoint.com/sites/intranet-onderzoek/SitePages/Mensenrechten.aspx

KU Leuven

- Kennisveiligheid: kennisveiligheid@kuleuven.be
- Ethische aspecten van dual use en misuse: ecdmm@kuleuven.be
- Exportcontrole: kennisveiligheid@kuleuven.be of lrd.export@kuleuven.be (LRD)
- Mensenrechten: humanrights@kuleuven.be
- Informatie over kennisveiligheid aan KU Leuven: https://www.kuleuven.be/knowledgesecurity

UHasselt

- rri@uhasselt.be
- Beleid rond integriteit en ethische aspecten: https://www.uhasselt.be/en/research/responsible-research-and-innovation

VUB

- ecdmm@vub.be Secretaris Ethische Commissie Dual Use, Militair Onderzoek en Misbruik | Vrije Universiteit Brussel
- Mensenrechten, ethiek en internationale samenwerking: Ethische commissies & Data Protection Office | Vrije Universiteit Brussel

imec

- ExportControl@imec.be
- Export control compliance | homepage (sharepoint.com)

Vlaams Instituut voor Biotechnologie (VIB)

- dualuse@vib.be
- +32 9 244 66 11

Instituut voor Tropische Geneeskunde

- dualuse@itg.be

VITO

- dualuse@vito.be

FlandersMake

- info@flandersmake.be
- +32 11 790 590

Casussen

Je wil een doctorandus met een achtergrond bij het Iraanse leger aannemen voor onderzoek over de detectie van stress en emoties via sensoren of hersenimplantaten.

Onderzoek over stress en emoties, en over de interface tussen de hersenen en computers of AI, is mogelijk in te zetten voor militaire doeleinden, repressie of criminele activiteiten, bijvoorbeeld voor het uitschakelen of juist verhogen van stress, het voelen van pijn, het gehoorzamen van bevelen, e.d. Voor je start met het onderzoek, neem je de volgende stappen:

- Bekijk samen met je contactpunt of de onderzoeker op de sanctielijst staat, en of die persoon wel op het project mag werken.
- Doe kritisch onderzoek naar het CV van de kandidaat: wat heeft deze gedaan bij het leger (vb. standaard legerdienst of specifiek onderzoek rond dit topic), is de persoon nog verbonden aan het leger, welke vooropleiding heeft de kandidaat, zijn er gaten in het CV van de onderzoeker, etc.
- Denk na over mitigerende maatregelen voor zover die mogelijk zijn. Je kan hier zeker ook contact voor opnemen met het contactpunt van je instelling.

Indien de vorige vragen op een risico wijzen, dien je een aanvraag in bij de bevoegde commissie in je instelling.

Je wil samenwerken rond het reduceren van geluid van vliegtuigmotoren met een bedrijf gevestigd in Malta. Er is weinig bekend over dit bedrijf, en er staat zeer weinig informatie op de website.

Malta stond voor de inval van Rusland in Oekraïne bekend als één van de landen waar zeer veel Russische bedrijven werden opgericht. Het is dus niet onmogelijk dat het bedrijf waarmee je wil samenwerken in handen is van Russische aandeelhouders. Het gebrek aan informatie over het bedrijf is daarvoor een aanwijzing. Onderzoek rond vliegtuigmotoren zal dan ook mogelijk risicovol zijn. Voor je start met je onderzoek, neem je de volgende stappen:

- Zoek meer informatie over het bedrijf, en ga na wie de eigenaars zijn van het bedrijf. Uiteraard kan het contactpunt van je instelling daarbij helpen. Indien het bedrijf Russische eigenaars zou hebben, bekijk je met je contactpunt of je samenwerking wettelijk mogelijk is onder de toepasselijke Rusland-sancties.
- Indien samenwerking wettelijk mogelijk is en je instelling samenwerking met een Russische partner toelaat, bekijk je de achtergrond van de Russische aandeelhouders: zijn deze betrokken

bij militaire activiteiten, of zijn ze in handen van de overheid?

– Denk na over mitigerende maatregelen, voor zover die mogelijk zijn. Je kan hier zeker ook contact voor opnemen met het contactpunt van je instelling.

Indien de vorige vragen op een risico wijzen, dien je een aanvraag in bij de bevoegde commissie in je instelling.

Je wil samenwerken rond dronetechnologie met een universiteit in China.

Dronetechnologie is een gevoelige technologie, die vrijwel altijd een dual use toepassing heeft, soms een exportvergunning nodig heeft en een zeer hoog risico op misbruik heeft. Naast vreedzame toepassingen kunnen drones immers gebruikt worden voor massa-surveillantie, maar ook in wapentechnologie. Partners in het buitenland kunnen kwaadwillige redenen voor hun interesse in deze technologie hebben. Voor je start met het onderzoek, neem je de volgende stappen:

– Ga na of je onderzoek betrekking heeft op drone technologie die op de dual use lijst van Verordening 821/2021 staat, en waarvoor een exportvergunning nodig is om het onderzoek te delen met je partner. Je kan hiervoor ook contact opnemen met je contactpunt.

– Ga na of de partner op een sanctielijst staat in de EU of elders, vb. via https://opensanctions.org. Je kan hiervoor ook contact opnemen met je contactpunt. Buitenlandse sancties (vb. Amerikaanse of Japanse) brengen niet noodzakelijk wettelijke beperkingen met zich mee, maar geven wel een indicatie over de mogelijke bezorgdheden rond militaire activiteiten en proliferatie, mensenrechtenschendingen, spionage, etc.

– Ga na of de partner wordt beschouwd als een risicovolle partner, vb. op de ASPI-lijst en de Canadese 'Named Research Organisations' lijst. Dit betekent niet noodzakelijk dat je het onderzoek niet kan uitvoeren, maar wel dat de risico's goed moeten overwogen worden.

– Ga na of je partner bekend staat om zijn militaire activiteiten, zijn band met de overheid of schendingen van de mensenrechten.

– Denk na over mogelijke mitigerende maatregelen voor zover die mogelijk zijn. Je kan hier zeker ook contact voor opnemen met je contactpunt.

Indien de vorige vragen op een risico wijzen, dien je een aanvraag in bij de bevoegde commissie in je instelling.

Je bent gevraagd om onderzoek te doen naar diversiteit in opdracht van een buitenlandse overheidsinstelling, maar het is bekend dat de overheid repressief beleid heeft ten aanzien van het onderwerp.

Voor je start met het onderzoek, neem je de volgende stappen:

– Ga na of de opdrachtgever op een sanctielijst staat in de EU of elders, vb. via https://

opensanctions.org. Je kan hiervoor ook contact opnemen met je contactpunt. Buitenlandse sancties (vb. Amerikaanse of Japanse) brengen niet noodzakelijk wettelijke beperkingen met zich mee, maar geven wel een indicatie over de mogelijke bezorgdheden rond militaire activiteiten en proliferatie, mensenrechtenschendingen, spionage, etc.

- Ga na of de overheidsinstelling mensenrechtenschendingen heeft begaan, of dat er mogelijke controverse bestaat over de houding van de instellingen tegenover fundamentele rechten en waarden.
- Bekijk de financieringsvoorwaarden aandachtig: mag je de resultaten publiceren, heeft de opdrachtgever een recht op review, ben je vrij om je respondenten te kiezen? De ondersteunende diensten van je instelling kunnen je hier bij helpen. Als de voorwaarden in orde lijken, zorg ook dat deze contractueel worden vastgelegd en dat je de mogelijkheid hebt om het onderzoek te beëindigen in geval van niet-naleving.
- Ga na of het onderzoek praktisch uit te voeren valt: komt de veiligheid van je respondenten in gevaar? Is je eigen veiligheid gegarandeerd?
- Denk na over mitigerende maatregelen, voor zover die mogelijk zijn. Je kan hier zeker ook contact voor opnemen met je contactpunt.

Indien de vorige vragen op een risico wijzen, dien je een aanvraag in bij de bevoegde commissie in je instelling.

Je Belgische doctoraatsstudent wil onderzoek doen naar het gebruik van minderheidstalen in de publieke sfeer in China. De jonge onderzoeker zal hiervoor ter plaatse foto- en videomateriaal verzamelen en interviews afnemen met individuen binnen minderheidsgroepen. De interviews zullen peilen naar de ervaringen en meningen van de individuen die tot de minderheidsgroep behoren. Als promotor ben je bezorgd over de veiligheid van de onderzoeker zelf en over de veiligheid van eventueel geïnterviewden. Daarnaast rijst ook de vraag of verzamelde data (ook foto- en videomateriaal) zonder problemen mee getransporteerd kan worden buiten de grenzen van het thuisland.

- Bekijk kritisch je onderzoeksdesign: heb je al het geplande foto- of videomateriaal nodig? Hoe kan je het aantal respondenten zo klein mogelijk maken?
- Ga na hoe je optimale anonimiteit van je deelnemers kan garanderen. Breng geen herkenbare personen in beeld en anonimiseer of pseudonimiseer de interviews. Informeer deelnemers voldoende om eventuele bezorgdheden tegemoet te komen. Wees je ervan bewust dat in een autoritaire staat er altijd risico's zullen zijn voor deelnemers aan dit soort onderzoek, en blijf voorzichtig.
- Tracht zoveel mogelijk, in lijn met richtlijnen van de Veiligheid van de Staat, burner phones/laptops te gebruiken bij het afreizen ter plaatse. Indien niet mogelijk kan data meteen geëncrypteerd overgemaakt worden via VPN, om mogelijk onderschepping of inmenging in de data bij het uitreizen te vermijden.

– Besteed bijzondere aandacht aan adviezen van Staatsveiligheid of Diplomatie België ('Politie en veiligheidspersoneel en hun installaties mogen niet worden gefotografeerd. Het filmen of fotograferen van demonstraties of samenscholingen is strikt afgeraden.') en ga na of er reisrestricties gelden voor de bestemming.

Neem contact op met het contactpunt van je instelling voor ondersteuning.

Een doctorandus met een CSC-beurs wil graag een jaar als gastonderzoeker in je onderzoeksgroep doorbrengen en onderzoek doen naar de efficiëntie van netwerken voor elektriciteitstransport, in het kader van het doctoraat waar zij in China aan bezig is.

– In principe wordt een CSC-beurs toegekend aan een individuele kandidaat los van de instelling waaraan deze verbonden is. In dit geval zal de kandidaat echter onderzoek doen in het kader van een lopend doctoraat, dus moet je ervan uitgaan dat zij de resultaten gegenereerd tijdens haar verblijf verder zal gebruiken voor haar doctoraat aan haar thuisinstelling. Het kan dus nodig zijn om IP-afspraken te maken met de doctorandus en met de thuisinstelling.

– Ga na aan welke thuisinstelling de gastonderzoeker verbonden is. Indien deze deel uitmaakt van de seven sons, op de sanctielijst staat, of banden heeft met het Chinese regime, kan een overeenkomst mogelijk problematisch zijn. Indien dit het geval is, bekijk je met je contactpunt wat er mogelijk is.

– Ga na of de gastonderzoeker zelf op de sanctielijst staat. Ook hier contacteer je je contactpunt indien dit het geval is.

– Doe kritisch onderzoek naar het CV van de kandidaat: zijn er indicaties van militair onderzoek in haar onderzoeksgroep, etc.?

– Denk na over het onderwerp van het onderzoek en over de toegang die de onderzoeker krijgt tot de informatie in jouw onderzoeksgroep. Zijn er strategische onderzoeksprojecten die afgeschermd moeten worden?

– Denk na over mitigerende maatregelen voor zover die mogelijk zijn. Je kan hier zeker ook contact voor opnemen met je contactpunt.

Indien de vorige vragen op een risico wijzen, dien je een aanvraag in bij de bevoegde commissie in je instelling.

Links

Vlaamse en Belgische bronnen

- Website Vlaamse overheid bevoegd voor exportcontrole: http://www.fdfa.be/csg
- Vlaams Exportcontrole beleid: https://www.fdfa.be/nl/vlaams-exportcontrolebeleid
- Website Brusselse overheid bevoegd voor exportcontrole: https://international.brussels/wie-zijn-we/permits-unit-old/?lang=nl#permits-unit
- Website Belgische overheid over exportcontrole: https://diplomatie.belgium.be/nl/beleid/beleidsthemas/vrede-en-veiligheid/ontwapening-en-non-proliferatie/exportcontrole-strategische-goederen

Europese bronnen

- Verordening 821/2021
- Richtlijnen voor compliance in het kader van onderzoek met dual use items, https://eur-lex.europa.eu/eli/reco/2021/1700/oj/eng
- Richtlijnen over onderzoek en misbruik: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf
- Richtlijnen over onderzoek met louter civiele finaliteit: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-research-focusing-exclusively-on-civil-applications_he_en.pdf
- Tool voor Europese sancties https://www.sanctionsmap.eu/
- Tool voor internationale sancties: www.opensactions.org
- Aanbevelingen Europese Raad rond Kennisveiligheid: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510
- Tackling R&I foreign interference: https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en

Buitenlandse bronnen

- Richtlijnen van de Duitse overheid bevoegd voor exportcontrole (BAFA): https://www.bafa.de/EN/Foreign_Trade/Export_Control/export_control_node.htmlFWO kennisveiligheidsbeleid: https://www.fwo.be/nl/over-fwo/onderzoeksbeleid/kennisveiligheid/

- Nederlands loket kennisveiligheid: https://www.loketkennisveiligheid.nl/
- Nederlandse leidraad kennisveiligheid: https://www.loketkennisveiligheid.nl/documenten/2022/01/14/nationale-leidraad-kennisveiligheid
- US EAR (Export Administration Regulation): https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear
- US ITAR (International Traffic in Arms Regulations) https://www.pmddtc.state.gov/ddtc
- US Office of Foreign Assets Controls: https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx
- US Research Security at the National Science Foundation: https://www.nsf.gov/research-security
- CANADA Safeguarding your research: https://science.gc.ca/site/science/en/safeguarding-your-research
- CANADA Named Research Organisations list: https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/named-research-organizations

Academische bronnen en andere tools met uitleg

- King's College London, Centre for Science & Security Studies: https://www.kcl.ac.uk/csss/research/strategic-trade/controls
- Leopoldina – Nationale Akademie der Wissenschaften, The Handling of Security-Relevant Research in Germany — An Overview https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information_The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf
- http://www.fas.org/biosecurity/education/dualuse/index.html: Case Studies in Dual-use Biological Research, an 8-module resource that has been developed by the Federation of American Scientists.
- TIM Dual use https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en
- ASPI (Australian Strategy Policy Institute) China Defence Universities tracker: https://unitracker.aspi.org.au/
- ASPI Mapping China's Tech Giants: https://chinatechmap.aspi.org.au
- Iran Watch: https://www.iranwatch.org/iranian-entities