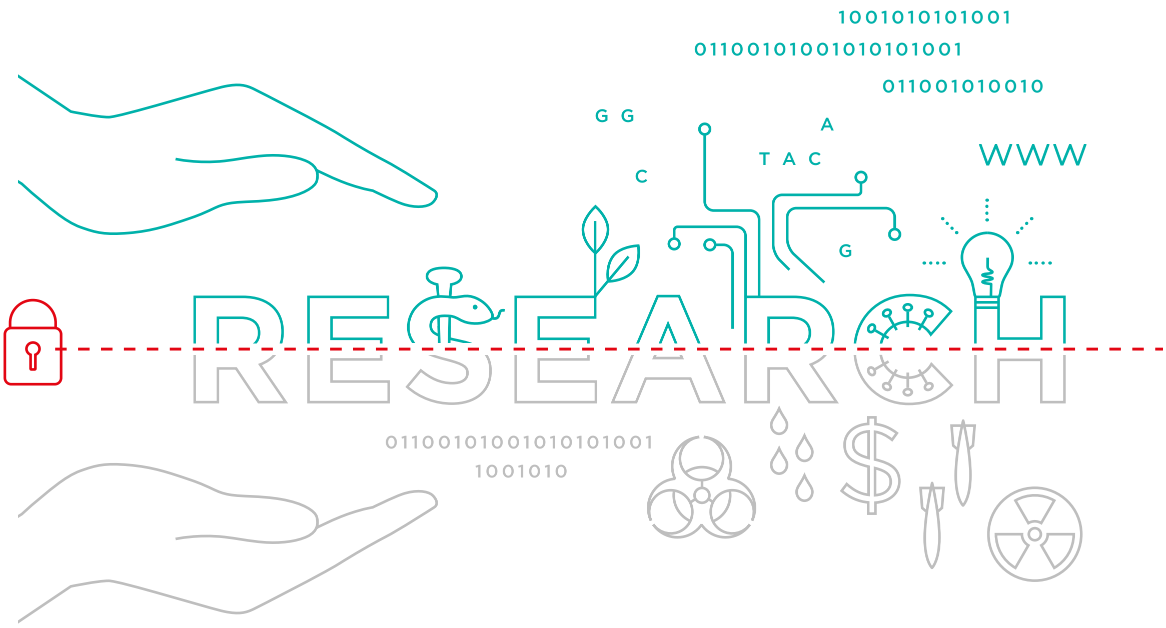
VLAAMSE
INTERUNIVERSITAIRE
RAAD

Guidelines for Researchers on Research Security, Dual Use and Misuse of Research



These Guidelines for researchers on research security, dual use and misuse of research were developed by the Flemish Interuniversity Council (VLIR), specifically by the members of the VLIR Working Group on Research Security, Dual Use, and Human Rights: Katleen Janssen, Inge Lerouge, Nynke Salverda (KU Leuven), Sarah Claes (UAntwerpen), Vincent Eechaudt (UGent), Stephanie Ruysschaert, Joke Kenens (UHasselt), Martyna Bajorinaite (VUB), and Filip Colson (VLIR).

It is therefore a product of the five Flemish universities, but valuable feedback on the draft text was provided by imec, VIB, the Institute of Tropical Medicine, VITO and FlandersMake. The relevant contact points of these institutions are also included in these Guidelines.

The cover illustration is commissioned by VLIR from Sisters of Design. It is based on their original work for Leopoldina, the German Academy of Sciences. Permission was obtained from Leopoldina to create a revised version for VLIR.

Responsible publisher:

Koen Verlaeckt, Secretary-General

Deposit number: D/2025/2939/1

Flemish Interuniversity Council | Vlaamse Interuniversitaire Raad
Ravensteingalerij 27 bus 6, 1000 Brussels
+32 (0)2 790 67 20

administratie@vlir.be
www.vlir.be

Version 1.0

Publication date: 29.09.2025

Guidelines for Researchers on Research Security, Dual Use and Misuse of Research

I want to hire a doctoral candidate who previously worked for the military of a country with an authoritarian regime for research on the detection of stress and emotions via sensors or brain implants. What should I consider?

I see an interesting call within the framework of the European Defence Fund. Can I simply apply for this?

I want to collaborate on drone technology with a university in China. Is that possible?

I want to collaborate on reducing aircraft engine noise with a company based in Malta. Little is known about this company, and there is very little information on the website. Should I be cautious?

I have been asked to conduct research on diversity commissioned by a foreign government agency, but it is known that the government pursues repressive policies regarding the subject. Can I conduct this research?

These guidelines describe what researchers must do when there are concerns about research security in their research, including military research, research on dual-use items, and when there are risks of misuse, for example in the area of human rights or malicious use.

What is Research security?

International cooperation forms the basis for high-quality academic research and education. The Flemish universities strive for maximum cooperation and an open approach to research, carried out within a context of academic freedom. However, international cooperation also brings risks. These challenges can be captured under the term research security.

Research security is an umbrella term for dealing with risks of:[1]

- **Unwanted transfer of sensitive or critical knowledge or technology**[2] that may threaten the security of the European Union or its member states, for example when used for military or intelligence purposes in third countries[3]. Consider, for example, research on dual-use items together with a partner that conducts extensive military research or comes from a country subject to arms embargoes or export measures. As of 2025, this is the case for Iran, Russia and Belarus, for example.
- **Interference in research or education by or from third countries or external parties**. Such interference poses a threat to academic freedom, can give rise to self-censorship, and undermines the integrity of researchers. This risk can arise when a researcher receives funding from a particular country or external party, but the research results are detrimental to that country/external party. In that case, the country/external party may try to pressure the researcher to adjust the results, not communicate transparently, or curtail funding.
- **Misuse** (unethical use) **of research results and/or data** (knowledge or technology) by third parties resulting in:
  - Violation or undermining of human rights or fundamental European values.
  - Unwanted deployment of research for malicious purposes, such as terrorist or criminal activities.

As a researcher, you must be alert to possible risks, know where to find relevant information, respect legal and institutional procedures and regulations, and avoid taking unacceptable risks consciously or unconsciously. How to do this is explained in these guidelines. The Research security Contact Point of your institution is also always available to support you in assessing and limiting risks.[4]

1 Council Recommendation of 23 May 2024 on improving research security, OJ C, C/2024/3510, 30.05.2024, ELI: http://data.europa.eu/eli/C/2024/3510/oj. The Recommendation uses the terms knowledge security and research security. These guidelines use the term Knowledge Security in Dutch ('kennisveiligheid'), because this has become generally accepted and corresponds with Dutch terminology.

2 Critical technology is 'knowledge and technology, including know-how, in emerging and disruptive areas and in areas important for economic competitiveness, social welfare and the security of the Union and its member states and where, as a result, excessive dependence on third countries is undesirable, taking into account the dynamic nature of research security and changing risks. This includes, but is not limited to, research and innovation with dual-use potential,' Council Recommendation of 23 May 2024 on improving research security, OJ C, C/2024/3510, 30.05.2024, ELI: http://data.europa.eu/eli/C/2024/3510/oj

3 Ibid.

4 For an overview of the contact points of all institutions, see 'Contact Points at Flemish Research Institutions Involved in These Guidelines'

The Flemish knowledge institutions assess their collaborations based on the following principles:

- **Openness of education and research**: We strive for maximum cooperation and open research, but limit collaborations if risks are too great ('as open as possible, as closed as necessary')

- **Proportionality**: restrictions are only possible if they are strictly necessary, can be clearly justified, and relate to specific entities (so not excluding an entire country, for example)

- **Institutional autonomy and academic freedom**: researchers have the right to conduct free and independent research with partners of their choice, within the limits of the human rights test

- **Country neutrality**: although risks in collaboration with some countries may be greater, not every collaboration with a risk country is by definition suspect. Research security risks can occur in collaborations with all countries.

What are the Risks?

A collaboration is risky if it threatens European security, if research results are later misused to violate human rights, if knowledge and results are appropriated in an unauthorized manner, or if third countries or external parties wish to censor or influence the results.

Whether a collaboration is risky depends on:

– How sensitive the technology or subject you are working on is;

– The partners you collaborate with, the funder or the client;

– The country in which the partners are located or the research takes place;

– The nature of the collaboration.

Research is not problematic *because* you are researching a sensitive subject, or because you are collaborating with a partner involved in the development of military technology. A risk usually only arises when various risk elements come together, e.g., when you conduct research on dual-use technology with a university that develops technology for the military in a non-democratic country.

Not every collaboration is problematic, but if there are risks, you must be able to justify why these do not apply to the collaboration you have in mind. Below we discuss how you can determine whether research is risky in terms of research security.

Examples of research security risks:

A researcher applying for a vacant position comes from a university directly involved in Iran's nuclear program. Is this researcher welcome at a Flemish university?

You are working with a company on genomic data. This company was in the news about genetic profiling of ethnic minorities. Can data still be sent for analysis?

You are asked to be co-supervisor of a PhD trajectory at a Russian university that appears on the European sanctions list. Is this still possible?

You are contacted by a top Chinese university to receive a visiting researcher and collaborate on autonomous ships. Is that allowed?

You want to collaborate with a researcher working in a hospital that has close ties to the military in an authoritarian regime. What should you consider?

You are asked by a European university to take measurements on a sample. In the publication process about these measurements, co-authors appear from universities known as Seven Sons of Defence. What should you do?

Research Topic

A research topic can be sensitive or risky for various reasons. Below we discuss:

– Topics sensitive to (foreign) interference

– Critical technologies (as defined by the European Commission)

– Dual-use items and research

– Technology maturity (TRL-level)

With increased sensitivity around theme, material or technology, both ethical and legal obligations may arise. As mentioned above, in most cases it is a highly sensitive topic *in combination with* a risky partner that can lead to research security risks.

Topics Sensitive to (Foreign) Interference

Certain topics may be politically sensitive or prohibited in the country that is the subject of research or in the country where the research takes place. Think of research on minorities, political beliefs, or social upheavals.

In other cases, research results may be sensitive to companies or research institutions because they pose a threat to the partner's activities. Think of research that demonstrates that a company's products or activities are harmful.

In such cases, there is a risk of interference or censorship by governments or the management of the partner institution. This may mean that you are pressured or misled to adjust the research topic, not to fully publish the results, or to adjust the research data. You are particularly vulnerable to pressure if you are too dependent on certain foreign funding sources.

Critical Technologies

The European Commission identified 10 critical technology domains where risks are greatest in international cooperation. In each of these domains there is an increased risk:

– Of civil-military fusion, particularly that defense companies and military governments cooperate very closely with universities and research institutions so that innovations quickly flow to the military sector;

– Of misuse, particularly that the technology is later deployed to violate or restrict human rights (e.g., surveillance, internal repression);

– That the technology is transformative in nature so that performance and efficiency improve significantly and/or can mean a radical change for certain sectors.

In each of these domains, the European Commission requests a risk assessment of the collaboration. This means that restrictions may need to be imposed so that crucial research results do not leak out of the EU, as this threatens European security and economy.

In each of these 10 domains, measures must be taken to ensure that the EU becomes less dependent on non-EU member states in the supply chain; that critical infrastructure is better secured (physically and digitally); and that high-tech knowledge does not leak to third countries.

To restrict access to critical technologies, non-EU entities and foreign-controlled EU entities are excluded from certain Horizon Europe research projects (e.g., on quantum technologies, critical raw materials, space).[5] For the same reason, certain Chinese entities (namely Huawei and ZTE) cannot participate in Horizon Europe Innovation Actions.[6]

The following critical technologies are mentioned in the Annex to the European Recommendation on Critical Technology Domains:[7]

– Advanced semiconductor technologies

- Micro-electronics, including processors
- Photonics technologies (including high-energy laser technologies)
- High-frequency chips
- Semiconductor manufacturing equipment for very advanced node sizes

– AI technologies

- High Performance Computing
- Cloud and edge computing
- Data analysis technologies
- Image recognition, language processing, object recognition

– Quantum technologies

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

6 COMMUNICATION FROM THE COMMISSION, Implementation of the 5G Cybersecurity Toolbox, https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox.

7 COMMISSION RECOMMENDATION (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States, https://eur-lex.europa.eu/eli/reco/2023/2113/oj.

- Quantum computing
- Quantum cryptography
- Quantum communication
- Quantum sensing and radar

– Biotechnologies

- Gene modification techniques
- New genomic techniques
- Gene drive
- Synthetic biology

– Advanced connectivity, navigation and digital technologies

- Secure digital communication and connectivity, such as RAN & Open RAN (radio access network) and 6G
- Cybersecurity technologies, including cyber monitoring, security and intrusion systems, digital forensics
- Internet of Things and virtual reality
- Distributed ledger and digital identity technologies
- Guidance, navigation and control technologies, including avionics and marine localization

– Advanced detection technologies

- Electro-optical, radar, chemical, biological, radiation detection technologies and 'distributed sensing'
- Magnetometers, magnetic gradient meters
- Sensors for measuring electric fields underwater
- Gravity meters and gradient meters

– Space and propulsion technologies

- Technologies specifically focused on space, ranging from component to system level
- Technologies for space monitoring and earth observation
- Positioning, navigation and timing (PNT)
- Secure communication, including LEO connectivity (LEO: Low Earth Orbit)
- Propulsion technologies, including hypersonics and components for military use

– Energy technologies

- Nuclear fusion technologies and reactors and electricity generation with nuclear fusion, radiological conversion/enrichment/recycling technologies
- Hydrogen and new fuels
- Net-zero technologies, including photovoltaic energy
- Smart grids and energy storage, batteries

– Robotics and autonomous systems

- Drones, (land) vehicles and vessels (in air and on and under water)
- Robots and robot-controlled precision systems
- Exoskeletons
- AI-based systems

– Advanced materials, advanced manufacturing and recycling technologies

- Technologies for nanomaterials, smart materials, advanced ceramic materials, 'stealth' materials, safe and inherently sustainable materials
- Additive manufacturing, including in the field
- Digitally controlled micro-precision production and small-scale laser processing/welding
- Technologies for extraction, processing and recycling of critical raw materials (including hydrometallurgical extraction, bioleaching, nanotechnology-based filtration, electrochemical processing and black masses)

Dual-Use Items (Including Export Control Legislation)

Dual-use items are goods, materials, technology, software and technical knowledge that meet specific technical parameters and whose properties can be useful for civilian as well as military applications.

Although dual-use items are also researched in research projects with a military purpose (collaboration with defence companies or Defence or based on EDF or DEFRA funding), research on dual-use items usually takes place in the context of regular research projects with a civilian purpose (FWO, Horizon, etc.). Despite the civilian purpose of the research, the materials, research data and results are also useful in a military context, for example for the development of weapons, radars, guidance technology, missile guidance, night vision devices, communication equipment, protective equipment, observation, navigation, drones, etc.

With dual-use research, the risks are inherently greater. Especially when you collaborate with partners active in an authoritarian regime or conflict zones, the risks of unethical use of your research results increase. The data and results can be used in these countries to strengthen that country's military capabilities, for example because the partner you are working with (including universities!) is also involved in military research in the home country.

Dual-use items are listed in Annex I of the European Dual Use Regulation (EU) No. 2021/821. These items are sensitive by definition, due to possible military end use, use for weapons of mass destruction, or use for human rights violations, internal repression or terrorist applications. How you can most efficiently determine whether your research relates to these dual-use items can be found in the Annex or on your research institution's website. The law restricts collaborations with non-EU member states on dual-use items.

Dual-Use Export Control Legislation

Are you working with dual-use items listed in the Dual Use Regulation and do you want to share these items with parties outside the EU? Then you need a dual-use export licence.[8]

You don't only need an export licence for the physical shipment of material goods. Sharing intangible items (software, technical knowledge) is also considered export.

Are you sharing dual-use goods, software, technology or technical knowledge outside the EU? Then the contact point at your university applies for an export licence. Every researcher within the institution is obliged to report when dual-use items are shared outside the EU so that a legally required licence can be applied for. Both the institution and the researcher are criminally liable if items are shared without an export licence.

Are you unsure whether the items you want to share are listed on the EU dual-use control list? Contact the contact point at your institution.

Technology Maturity

Applied research on technologies is riskier than fundamental research. Fundamental research focuses on the fundamental principles of phenomena or observable facts and is not aimed at a specific practical goal or purpose. Applied research in which certain technologies are developed is much more sensitive, given that the technical knowledge and research results can be used or misused more quickly in certain applications (and therefore also in a military context).

To determine whether you are conducting fundamental research, you can use the Technology Readiness Level (TRL) scale. This is a scale from 1 to 9 that expresses the economic applicability of the tech-

8 For certain sensitive technologies you also need a licence for intra-EU transfers. This includes nuclear technology, materials for absorbing electromagnetic radiation, or cryptanalysis.

nology and is also used within Horizon Europe.[9]

If the technology has a TRL of 1 or 2, it is assumed to be fundamental scientific research. Research on technology with a TRL of 3 or higher is in principle applied research.[10] In such research projects, you develop an experimental 'proof of concept' and it is common to collaborate with partners from the business world or civil society.

Partner

Institution (including Sanctions)

There is a risk that the research data or results of your project flow to military services or security services, are used for the development of military technology, or are later misused for human rights violations (such as internal repression) or criminal activities. It is therefore important that you determine whether the partner you are collaborating with:

- Is closely connected to the military or national security services (e.g., through collaboration with the military or defence companies or the development of defence technology);
- Cooperates closely with defence companies or companies that develop security technology;
- Is involved in the development of military or security technology;
- Is involved in discrimination or in violations or restrictions of academic freedom, freedom of expression or other human rights.

Consider whether critics could use the collaboration to discredit your findings, regardless of the quality of the research itself, or whether you and/or your host institution could suffer reputational damage from the collaboration with this institution, and whether you yourself could end up in a morally difficult situation.

How Do You Assess the Partner Institution?

- Certain countries and organisations are subject to sanctions because they pose a threat to security and/or international peace. The sanctions against Russia, Belarus and Iran are most prominent, but there are other entities subject to sanctions. Such sanctions and measures are imposed by (international) bodies such as the United Nations, the European Union, the Flemish government, or other countries. For example, the United States and Japan have extensive sanctions lists. Via www.opensanctions.org you can check whether your partner is subject to such

9 On the Horizon Europe NCP portal you will find a TRL assessment tool to determine the TRL level of your research (see https://horizoneuropencpportal.eu/store/trl-assessment). The Canadian government also offers a simple checklist (see: https://ised-isde.canada.ca/site/clean-growth-hub/sites/default/files/attachments/TRL-e.pdf.

10 For more information, see Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programs for research-related controls on dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council 2021 establishing a Union regime for export, brokering, technical assistance, transit and transfer controls on dual-use items, OJ L 338, 23.9.2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H1700.

sanctions.

– Many research institutions are involved in the development of defence technology. For China and Iran, specific websites are available:

  • The China Defence Universities Tracker: https://unitracker.aspi.org.au. (This has been behind a paywall since August 2025; an alternative European source is expected at the end of 2026).

  • Iran Watch: https://www.iranwatch.org/iranian-entities.

– Certain academic institutions are involved in human rights violations.

  • Scholars at Risk reports on incidents worldwide: https://www.scholarsatrisk.org/academic-freedom-monitoring-project-index.

  • Middle East Studies Association on incidents in the Middle East: https://mesana.org/advocacy (use the search function).

– Certain companies are involved in human rights violations or serious environmental damage.

  • The Norwegian Pension Fund reports on a selection of listed companies: https://www.nbim.no/en/responsible-investment/ethical-exclusions/exclusion-of-companies.

  • The Australian Strategic Policy Institute reports on the intertwining of Chinese technology companies with the government and activities in Xinjiang: https://chinatechmap.aspi.org.au

  • Business & Human Rights Resource Centre maintains a database tracking news and allegations of human rights violations for more than 20,000 companies: https://www.business-humanrights.org.

  • Searching the Human Rights Watch website can provide insights into a number of large companies: www.hrw.org.

– You can of course also question your partner directly, consult the candidate partner's website (preferably in the language of the region where the institution is located, with a translation tool), or use search engines or AI chatbots. For example, you can ask the chatbot whether your partner is involved in human rights violations, military activities, or controversies. Of course, this only gives an indication, and further research will still be necessary.

If your partner's activities or objectives are unclear or difficult to trace, the collaboration may be undesirable. It is important that you know who your partner is and that you can justify why you are collaborating, regardless of the quality of the research itself. Your institution's contact point can help you screen the partner institution.[11]

11 For an overview of the contact points of all institutions, see 'Contact Points at Flemish Research Institutions Involved in These Guidelines'

The Flemish universities decided in 2019 to introduce a human rights test. This determines that as an institution we do not wish to violate human rights ourselves, but also that we avoid research results being misused later for human rights violations, and that we avoid collaborations with partners involved in serious human rights violations. Even if the research is unrelated to the violations, the partnership is problematic. If the collaboration leads to more positive than negative consequences for the human rights situation, it can be continued with monitoring.

Researcher

There is growing concern that certain countries gain specialized knowledge through academic collaboration and sending out students, to later deploy it for the development of military technology. This means that visa applications for researchers from these countries may take longer and the chance of visa refusal is greater. Keep this in mind if you work with sensitive or strategic knowledge and wish to recruit a researcher from outside the EU.

For incoming researchers (PhD students, exchange students, visiting researchers, ...) a collaboration is riskier when the incoming researcher only stays temporarily at a Flemish institution. Unlike conducting a complete research project at a Flemish institution, with Joint PhDs, exchange students and visiting researchers, research data and results are shared with researchers and institutions abroad and these results are therefore also used for (research) activities at the foreign institution.

Depending on the previous work experience and affiliations of an incoming researcher, the risk can also be mapped whether the acquired knowledge can later be used for unwanted purposes, and whether the researcher may be subject to external pressure (from their government or home institution) to share results, data or material.

Your institution's contact point can help you with risk analyses of incoming researchers.

Funder

Governments, companies or donors have certain motives for funding research. In certain cases, research results may be sensitive to funders because the results may have a negative impact on business operations or be politically sensitive.

In that case, there is a risk of interference or censorship by governments or the management of the partner institution. This may mean that you are pressured or misled to adjust the research topic, not to fully publish the results, or to adjust the research data. Also keep in mind that this pressure can increase when you end up in a position of financial dependence on one funder.

In addition, a funder, like a project partner, may also have malicious intentions with the results of your research, or keep their true intentions hidden. Possible signals for this are: the funder offers particularly favorable funding conditions, wants to pay exceptionally high amounts, or demands very unusual technical specifications that are not common for the research involved. Also, if little to no information can be found about the funder (e.g., no website, no corporate email address, no LinkedIn profile), there may be reasons for concern.

Here too, your institution's contact point can help you with a risk analysis.

Country

Some countries pose a threat to European security. It is then riskier to collaborate with organisations or researchers in those countries, especially when the partner university or company cooperates with defense companies or military governments.

Moreover, in certain countries and regions, human rights violations occur frequently. This risk increases when there is a war or armed conflict in that region.

Due to the above findings, collaborations with researchers and organisations in specific countries always pose a risk in terms of research security. This specifically concerns **China, Iran, Israel, North Korea, Pakistan, Russia, Saudi Arabia, Syria, Turkey, United Arab Emirates and Belarus**.[12]

When you collaborate with a partner in one of these countries, it is especially important that you gather information about your partner and thoroughly evaluate the risks of your collaboration. If you want help with this, you can contact your institution's contact point.

International rankings show how different countries score in terms of rule of law, human rights, democracy, and corruption:

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

Funder Policy and Specific Institutional Restrictions

Due to research security risks, funders and research institutions take certain measures to limit these risks. These may mean that collaborations with certain countries and/or institutions are excluded and that certain research is only possible with risk-mitigating measures. Below is a non-exhaustive overview.[13]

12 List based on international sanctions and Flemish export measures.
13 The Horizon Europe ethics self-assessment includes an assessment of possible misuse of research results (https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf).

FWO Research security Policy

FWO launched its own research security policy in 2024, based on four pillars: 1) risk analysis of its own partnerships abroad; 2) awareness-raising of FWO applicants through the addition of a 'Research Security Appraisal' to all applications; 3) monitoring in reporting; and 4) a cybersecurity policy.

The Research Security Appraisal surveys research security risks of a research project in three domains: the topic of the project proposal, the country involved in the research, and the partner you are collaborating with. When a project is classified as 'high risk' based on the questionnaire, approval regarding research security from your institution is required. For more information about this and about the internal procedure, you can contact your institution's contact point.

Seven Sons of National Defence (China)

The Seven Sons of National Defence are a group of 7 Chinese universities that were subordinate to the Ministry of Defence until 2008. The Seven Sons universities spend about half of their research budget on defence research.[14] They all have security clearances for access to information classified as 'top secret.' Up to one in three graduates from these universities find work in the defence sector.

Due to the risks of civil-military fusion, FWO no longer funds collaborations with these universities. The Flemish universities also do not sign new institutional cooperation agreements with the Seven Sons of National Defence universities.

These are Harbin Institute of Technology, Harbin Engineering University, Beijing Institute of Technology, Beihang University, Northwestern Polytechnical University, Nanjing University of Science and Technology and Nanjing University of Aeronautics and Astronautics.

In the same vein, no institutional collaborations are entered into with Chinese military research institutions.

Iran

Due to the imprisonment of Dr. Ahmadreza Djalali, visiting professor at VUB, by the Iranian authorities, the Flemish Interuniversity Council decided that institutional collaborations with Iranian knowledge institutions are excluded.[15]

Rusland

In 2022, the Russian rectors' conference published a statement in support of the Russian war in Ukraine, following Vladimir Putin's position that the invasion of Ukraine was a necessary 'special military operation' aimed at 'achieving the demilitarization and denazification of Ukraine,' ending the conflict in Donbass and protecting Russia against 'increasing military threats.' Therefore, the rectors of Belgian universities decided not to enter into institutional collaborations with universities that signed this

14 https://unitracker.aspi.org.au/glossary
15 https://vlir.be/nieuws/academische-samenwerking-met-iran-onmogelijk

statement.[16]

The European Commission decided in March 2022 not to enter into new collaborations with Russian organisations within the Horizon Europe research program and, in April 2022 via the fifth sanctions package, to also stop ongoing participations within Horizon 2020.[17] FWO also no longer finances any collaboration with Russian/Belarusian entities.[18]

Military Research Funding

The Flemish universities primarily conduct research focused on civilian applications. However, research may also be conducted that has military utility (dual-use) or a military focus. Examples include collaborations with the Royal Military Academy or projects under the Defence Research Action (DEFRA, a cooperation between the Belgian Science Policy Office (BELSPO) and the Royal Higher Institute for Defence (RHID), funded by the Ministry of Defence) and the European Defence Fund (EDF, funded by the European Union).

As a researcher, you are generally free to participate in projects whose results may have military applications, provided you comply with your institution's ethical framework. Participation in such projects requires personal ethical reflection based on your own values and standards. You must also comply with your institution's policies and the conditions set by research funders.

Exercise greater caution when funding does not originate from your own government, EU/NATO programmes, or allied and partner countries (including private companies), as defence and national security are inherently tied to national sovereignty.

Some research projects involve classified information. When information is classified as 'confidential,' 'secret,' or 'top secret,' you may only access it if you hold an individual security clearance. If information is classified as 'restricted,' no individual clearance is required, but various physical and digital security measures must be implemented.

Obtaining an individual security clearance requires meeting strict conditions. Further information is available on the State Security website: https://www.nvoans.be/nl/veiligheidsmachtigingen/individuele-veiligheidsmachtigingen. Applications for security clearances are submitted by your institution's security officer. Contact your institutional contact point for guidance on applying for clearances and implementing required security measures.

Funders of military research may impose additional restrictions. For instance, DEFRA project calls require that participating researchers hold EU nationality or be nationals of a European Free Trade Association country or NATO member state. Researchers may also be subject to security verification.

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/

How Can You Limit the Risks?

Researcher's Responsibility

It is primarily up to you to determine whether your research entails one or more of the risks described above. When this is the case, you must consider whether the possible risks can be managed by taking mitigating measures.

In addition, you must also comply with applicable legislation. You must also comply with your institution's internal procedures and report your research to the ethics committee or competent service. In exceptional cases, the research will not be possible.

Mitigating Measures

If you identify research security risks in your planned research, you try to take measures to limit those risks. Those measures may relate to the topic or research design; physical, organisational or cybersecurity; or the partner(s) you collaborate with. Your institution's contact point can help you with the risk analysis of your research and implementing possible mitigating measures.

Examples of mitigating measures you can take are:

- Installing physical security measures so that sensitive data and technology are only accessible to researchers involved in the project (for example, access restrictions, use of a safe).
- Ensuring sufficient cybersecurity: separate network drives, anti-virus software, two-factor authentication, restricting access to researchers involved in the project, etc.
- Taking precautions during international travel (e.g., bringing a 'clean' laptop or phone);
- Following a protocol for visitors (e.g., always accompanying visitors, not giving access to spaces with strategic equipment);
- Entering into confidentiality agreements, protecting intellectual property or inserting clauses about permitted end use in collaboration agreements;
- Providing a publication clause that offers sufficient guarantees that results can be freely published;
- Providing mandatory 'security training' for research staff;
- Appointing an independent ethical adviser or ethical board linked to the research project (separate from the internal competent committee of your university);
- Adjusting the research design, for example by using dummy data, or limiting access to research data at the level of participants in a work package;

– Marking certain research results as secret or restricting the dissemination of research results, for example by publishing only part of the research results.

Legal Obligations or Restrictions

You may also be subject to legal obligations or restrictions in the context of your research. For example, when your partner is subject to international sanctions, you must determine what you may not share with them, and whether this has an impact on your research.

When your research relates to dual-use items as listed in the European Dual Use Regulation No. 821/2021, you may need an export licence to share materials, software, or research results with your partner outside the European Union. This may also be the case when you give a lecture or workshop outside the EU or online with participation from outside the EU. That licence must be applied for with the Flemish or Brussels government before dual-use items are shared. Contact the Contact Point or the service responsible for applying for licences within your institution for support with this.

Reporting Obligation

When dual-use or military use is possible or there is a real risk of misuse of research, every researcher has a reporting obligation to the Contact Point. This also applies to applications (research activities and/or partners) that prove to be potentially problematic in the field of human rights (VLIR Human Rights Test). In collaboration with the Contact Point, measures are taken to limit the risk of misuse.

Not Starting or Terminating the Project

In exceptional cases, the risks are too great to mitigate, or the research does not lend itself to taking mitigating measures. This can result in the research not being able to be carried out. The contact point within your institution can support you with this assessment.

When the situation changes during an ongoing project and research security risks become too great to continue working, you contact the Contact Point to see whether and under what conditions the collaboration can be terminated.

Contact Points at Flemish Research Institutions Involved in These Guidelines

UAntwerpen

- Research security Contact Point: researchsecurity@uantwerpen.be
- Ethics Committee for 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

- Research security Contact Point: researchsecurity@ugent.be
- https://ugentbe.sharepoint.com/sites/intranet-onderzoek/SitePages/Kennisveiligheid.aspx
- Information about research with military research, dual-use items and export control: https://ugentbe.sharepoint.com/sites/intranet-onderzoek/SitePages/Onderzoek-naar-dual-use-items.aspx
- Information about UGent Human Rights Policy: https://ugentbe.sharepoint.com/sites/intranet-onderzoek/SitePages/Mensenrechten.aspx

KU Leuven

- Research security Contact Point: kennisveiligheid@kuleuven.be
- Ethical aspects of dual-use and misuse: ecdmm@kuleuven.be
- Export control: kennisveiligheid@kuleuven.be or lrd.export@kuleuven.be (LRD)
- Human Rights: humanrights@kuleuven.be
- Information about research security at KU Leuven: https://www.kuleuven.be/knowledgesecurity

UHasselt

- Research security Contact Point: rri@uhasselt.be
- Policy on integrity and ethical aspects: https://www.uhasselt.be/en/research/responsible-research-and-innovation

VUB

- Research security Contact Point: ecdmm@vub.be
- Ethics Committee Dual Technologies, Military Research & Misuse
- Human Rights, ethics and international cooperation: Ethics Committees, Data Protection and International Collaboration Policy

imec

- ExportControl@imec.be
- Export control compliance

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

Cases

You want to hire a doctoral candidate with a background in the Iranian military for research on the detection of stress and emotions via sensors or brain implants.

Research on stress and emotions, and on the interface between the brain and computers or AI, can potentially be deployed for military purposes, repression or criminal activities, for example for disabling or increasing stress, feeling pain, obeying commands, etc. Before you start the research, you take the following steps:

– Check with your contact point whether the researcher is on the sanctions list, and whether that person may work on the project.

– Do critical research on the candidate's CV: what did they do in the military (e.g., standard military service or specific research on this topic), is the person still connected to the military, what education does the candidate have, are there gaps in the researcher's CV, etc.

– Think about mitigating measures insofar as they are possible. You can certainly also contact your institution's contact point for this.

If the previous questions point to a risk, you submit an application to the competent committee in your institution.

You want to collaborate on reducing aircraft engine noise with a company based in Malta. Little is known about this company, and there is very little information on the website.

Before Russia's full-scale invasion of Ukraine, Malta was known as one of the countries where very many Russian companies were established. It is therefore not impossible that the company you want to collaborate with is in the hands of Russian shareholders. The lack of information about the company is an indication of this. Research on aircraft engines may therefore be potentially risky. Before you start your research, you take the following steps:

– Find more information about the company, and determine who the owners of the company are. Of course, your institution's contact point can help with this. If the company were to have Russian owners, you check with your contact point whether your collaboration is legally possible under the applicable Russia sanctions.

– If collaboration is legally possible and your institution allows collaboration with a Russian partner, you examine the background of the Russian shareholders: are they involved in military activities, or are they owned by the government?

– Think about mitigating measures, insofar as they are possible. You can certainly also contact your institution's contact point for this.

If the previous questions point to a risk, you submit an application to the competent committee in your institution.

You want to collaborate on drone technology with a university in China.

Drone technology is a sensitive technology that almost always has a dual-use application, sometimes requires an export license, and has a very high risk of misuse. In addition to peaceful applications, drones can be used for mass surveillance, but also in weapons technology. Partners abroad may have malicious reasons for their interest in this technology. Before you start the research, you take the following steps:

– Determine whether your research relates to drone technology listed on the dual-use list of Regulation 821/2021, and for which an export licence is needed to share the research with your partner. You can also contact your contact point for this.

– Determine whether the partner is on a sanctions list in the EU or elsewhere, e.g., via [https://opensanctions.org.](https://opensanctions.org) You can also contact your contact point for this. Foreign sanctions (e.g., American or Japanese) do not necessarily entail legal restrictions, but do give an indication of possible concerns about military activities and proliferation, human rights violations, espionage, etc.

– Determine whether the partner is considered a risky partner, e.g., on the ASPI list and the Canadian 'Named Research Organisations' list. This does not necessarily mean that you cannot conduct the research, but that the risks must be carefully considered.

– Determine whether your partner is known for their military activities, their ties to the government, or human rights violations.

– Think about possible mitigating measures insofar as they are possible. You can certainly also contact your contact point for this.

If the previous questions point to a risk, you submit an application to the competent committee in your institution.

You have been asked to conduct research on diversity commissioned by a foreign government agency, but it is known that the government has repressive policies regarding the subject.

Before you start the research, you take the following steps:

– Determine whether the client is on a sanctions list in the EU or elsewhere, e.g., via [https://opensanctions.org.](https://opensanctions.org) You can also contact your contact point for this. Foreign sanctions (e.g., American or Japanese) do not necessarily entail legal restrictions, but do give an indication of possible concerns about military activities and proliferation, human rights violations, espionage, etc.

– Determine whether the government agency has committed human rights violations, or whether there is possible controversy about the institution's attitude toward fundamental rights and values.

– Review the funding conditions carefully: may you publish the results, does the client have a right to review, are you free to choose your respondents? Your institution's support services can help you with this. If the conditions seem in order, also ensure they are contractually established and that you have the option to terminate the research in case of non-compliance.

– Determine whether the research is practically feasible: is the safety of your respondents at risk? Is your own safety guaranteed?

– Think about mitigating measures, insofar as they are possible. You can certainly also contact your contact point for this.

If the previous questions point to a risk, you submit an application to the competent committee in your institution.

Your Belgian doctoral student wants to conduct research on the use of minority languages in the public sphere in China. The young researcher will collect photo and video material on site and conduct interviews with individuals within minority groups. The interviews will survey the experiences and opinions of individuals belonging to the minority group. As a supervisor, you are concerned about the safety of the researcher themselves and about the safety of possible interviewees. In addition, the question arises whether collected data (including photo and video material) can be transported without problems outside the borders of the home country.

– Critically review your research design: do you need all the planned photo or video material? How can you minimize the number of respondents?

– Determine how you can guarantee optimal anonymity of your participants. Do not show recognizable people and anonymize or pseudonymize the interviews. Inform participants sufficiently to address any concerns. Be aware that in an authoritarian state there will always be risks for participants in this type of research, and remain cautious.

– Try as much as possible, in line with State Security guidelines, to use burner phones/laptops when traveling on site. If not possible, data can be immediately encrypted and transferred via VPN, to avoid possible interception or interference in the data when exiting.

– Pay special attention to advice from State Security or Diplomacy Belgium ('Police and security personnel and their installations may not be photographed. Filming or photographing demonstrations or gatherings is strongly discouraged.') and determine whether travel restrictions apply to the destination.

Contact your institution's contact point for support.

A doctoral candidate with a CSC scholarship wants to spend a year as a visiting researcher in your research group and conduct research on the efficiency of networks for electricity transmission, as part of the doctorate they are working on in China.

- In principle, a CSC scholarship is awarded to an individual candidate separate from the institution to which they are affiliated. However, in this case the candidate will conduct research as part of an ongoing doctorate, so you must assume that they will continue to use the results generated during their stay for their doctorate at their home institution. It may therefore be necessary to make IP agreements with the doctoral candidate and with the home institution.
- Determine which home institution the visiting researcher is affiliated with. If it is part of the seven sons, on the sanctions list, or has ties to the Chinese regime, an agreement may be problematic. If this is the case, you check with your contact point what is possible.
- Determine whether the visiting researcher themselves is on the sanctions list. Here too, you contact your contact point if this is the case.
- Do critical research on the candidate's CV: are there indications of military research in their research group, etc.?
- Think about the subject of the research and about the access the researcher gets to the information in your research group. Are there strategic research projects that need to be shielded?
- Think about mitigating measures insofar as they are possible. You can certainly also contact your contact point for this.

If the previous questions point to a risk, you submit an application to the competent committee in your institution.

Links

Flemish and Belgian Sources

- Flemish government website responsible for export control: http://www.fdfa.be/csg
- Flemish Export Control Policy: https://www.fdfa.be/nl/vlaams-exportcontrolebeleid
- Brussels government website responsible for export control: https://international.brussels/wie-zijn-we/permits-unit-old/?lang=nl#permits-unit
- Belgian government website on export control: https://diplomatie.belgium.be/nl/beleid/beleidsthemas/vrede-en-veiligheid/ontwapening-en-non-proliferatie/exportcontrole-strategische-goederen

European Sources

- Regulation 821/2021
- Guidelines for compliance in the context of research with dual-use items: https://eur-lex.europa.eu/eli/reco/2021/1700/oj/eng
- Guidelines on research and misuse: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf
- Guidelines on research focusing exclusively on civil applications: 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 for European sanctions: https://www.sanctionsmap.eu/
- Tool for international sanctions: www.opensanctions.org
- European Council Recommendations on Knowledge Security: 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

Foreign Sources

- Guidelines of the German authority responsible for export control (BAFA): https://www.bafa.de/EN/Foreign_Trade/Export_Control/export_control_node.html

- FWO research security policy: https://www.fwo.be/nl/over-fwo/onderzoeksbeleid/kennis-veiligheid/
- Dutch research security desk: https://www.loketkennisveiligheid.nl/
- Dutch research security guideline: https://www.loketkennisveiligheid.nl/documen-ten/2022/01/14/nationale-leidraad-kennisveiligheid
- US EAR (Export Administration Regulation): https://www.bis.doc.gov/index.php/regulati-ons/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-se-curity
- CANADA Safeguarding your research: https://science.gc.ca/site/science/en/safeguar-ding-your-research
- CANADA Named Research Organisations list: https://science.gc.ca/site/science/en/safe-guarding-your-research/guidelines-and-tools-implement-research-security/sensitive-tech-nology-research-and-affiliations-concern/named-research-organizations

Academic Sources and Other Tools

- 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/Ue-ber_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