Institut für Neurowissenschaften und Medizin (INM)
Gehirn und Verhalten (INM-7)

Guideline on dual use and misuse of research for committees for ethics in security relevant research (KEFs)

Jan-Hendrik Heinrichs, Forschungszentrum Jülich
Serap Ergin Aslan, Forschungszentrum Jülich
Karla Alex, University of Heidelberg, Heidelberg University Hospital, NCT
Andreas Brenneis, Technical University of Darmstadt
Niel Henk Conradie, University of Aachen
Martin Hähnel, University of Bremen / University of Augsburg
Mario Kropf, University of Graz
Jochen Kuck, Forschungszentrum Jülich
Ori Lev, Sapir College
Martina Philippi, Paderborn University
Verena Risse, TU Dortmund University

Jül-4449

SPONSORED BY THE
Federal Ministry of Education and Research

JÜLICH
Forschungszentrum

Institut für Neurowissenschaften und Medizin (INM)

Guideline on dual use and misuse of research for committees for ethics in security relevant research (KEFs)

Jan-Hendrik Heinrichs, Forschungszentrum Jülich
Serap Ergin Aslan, Forschungszentrum Jülich
Karla Alex, University of Heidelberg, Heidelberg University Hospital, NCT
Andreas Brenneis, Technical University of Darmstadt
Niel Henk Conradie, University of Aachen
Martin Hähnel, University of Bremen / University of Augsburg
Mario Kropf, University of Graz
Jochen Kuck, Forschungszentrum Jülich
Ori Lev, Sapir College
Martina Philippi, Paderborn University
Verena Risse, TU Dortmund University

Berichte des Forschungszentrums Jülich
Jül-4449 · ISSN 0944-2952
Institut für Neurowissenschaften und Medizin (INM)

Vollständig frei verfügbar über das Publikationsportal des Forschungszentrums Jülich (JuSER)
unter www.fz-juelich.de/zb/openaccess

Forschungszentrum Jülich GmbH · 52425 Jülich
Zentralbibliothek, Verlag
Tel.: 02461 61-5220 · Fax: 02461 61-6103
zb-publikation@fz-juelich.de
www.fz-juelich.de/zb

Contents

Foreword

The following guideline emerged from the project DUMFE: Dual Use and Misuse of Research Results (“Dual use und Missbrauch von Forschungsergebnissen”), funded by the German Federal Ministry of Education and Research (BMBF, 01GP2187). In recent years, dual use has become a significant issue in research ethics for numerous reasons, garnering considerable attention not only within the ethical community but also in the broader scientific community and among political and security circles.

Among the reasons for this attention are the dissemination of scientific developments with high misuse potential, such as gain-of-function experiments (Imai et al. 2012; Herfst et al. 2012; Imperiale and Casadevall 2018); political factors, including recent shifts in the global security landscape (Nationale Akademie der Wissenschaften Leopoldina (Leopoldina) and Deutsche Forschungsgemeinschaft (DFG) 2024, 9ff.); and heightened awareness of historical misuses of science (De Block and Adriaens, 2013).

There is detailed advice on the handling of dual use research of concern provided by the Joint Committee (“Joint Committee on the Handling of Security-Relevant Research”) of the German National Academy of Science Leopoldina and the German Research Foundation (DFG) (2022). The Joint Committee also provides networking and exchange opportunities for Committees for Ethics in Security-Relevant Research (Kommissionen für Ethik sicherheitsrelevanter Forschung), so-called KEFs. Nevertheless, additional information and guidance on handling dual use research of concern is a regular request in particular from scientists, but also a request often heard in forums with policy experts, managers and administrators of institutions in research and education.

The present guideline provides such additional in-depth information on the definition, examples, legal as well as ethical issues and options for governance of dual use research. It has been written by ethicists and philosophers of technology, supported by lawyers and members of the commission for ethics in research of Forschungszentrum Jülich. It is intended to provide additional information supporting the design of and deliberation in institutional bodies dealing with ethics of security-relevant research. It aims to highlight decisions and options relevant to different institutions and refers to further sources of information throughout.

Acknowledgements

We would like to thank all the participants of the project DUMFE: Dual Use and Misuse of Research Result, its funder the German Federal Ministry of Education and Research (BMBF, 01GP2187) as well as the members of the Commission for Ethics in Research of Forschungszentrum Jülich.

Contributors

Karla Alex
University of Heidelberg, Heidelberg University Hospital, NCT

Andreas Brenneis
Technical University of Darmstadt

Niel Henk Conradie
University of Aachen

Serap Ergin Aslan
Forschungszentrum Jülich

Martin Hähnel
University of Bremen / University of Augsburg

Jan-Hendrik Heinrichs
Forschungszentrum Jülich

Mario Kropf
University of Graz

Jochen Kuck
Forschungszentrum Jülich

Ori Lev
Sapir College

Martina Philippi
Paderborn University

Verena Risse
TU Dortmund University

SUGGESTED CITATION

Heinrichs, J. H., Ergin Aslan, S., Alex, K., Brenneis, A., Conradie, N. H., Hähnel, M., Kropf, M., Kuck, J., Lev, O., Philippi, M. & Risse, V. (2025). Guideline on dual use and misuse of research for committees for ethics in security relevant research (KEFs). Verlag des Forschungszentrums Jülich.

1) Introduction

Dual use research can occur in widely different contexts. The most widely known – if not as such – forms of dual use research are technologies that have originally been designed for the military but have important civilian uses, from Teflon to the internet. This kind of dual use is not the focus of the present guideline and does not require specialized governance structures. We could probably imagine a weirdly militaristic research administrator that chides researchers for developing something that can be used for civilian purposes as well, but it does require quite a feat of imagination.

This example serves to point out that the mere fact of dual – or multiple – usability is not an ethical issue *per se* (Floridi 2023: 60). What constitutes a dual use in the normative sense and whether it requires ethical scrutiny rather depends on the purposes research results can be put to. And while there are common moral standards allowing us to evaluate most forms of dual use, there is an additional factor in the values and principles endorsed by the researchers and their institutions.

This guideline aims to provide ethics committees with a comprehensive framework for addressing dual use research. It covers key aspects such as the definition of dual use, legal and ethical considerations, potential governance strategies, and real-world examples. Understanding dual use is essential not only for mitigating potential threats but also for fostering a culture of responsibility and integrity in scientific research. As the global security environment evolves and new technologies emerge, the importance of effectively managing dual use research cannot be overstated. This guideline serves as a crucial resource for committees for ethics in security relevant research committed to promoting safe, ethical, and responsible scientific inquiry.

2) Definition of Dual Use and Misuse of Research Results

Lead author(s): Karla Alex

In recent years, research ethics has become increasingly concerned with the development of strategies for managing security-related research and its potential for misuse in and outside the sciences. This has led to calls for a clearer definition of the term "dual use", along with a more precise delineation of its scope (Hähnel 2024; Crowley and Dando 2022; Miller and Selgelid 2008). For this purpose, it is essential to elucidate the specific conditions under which research, its findings, or its products ought to be classified as dual use, or even as dual use of concern (see for example, Miller and Selgelid 2007; Shamoo and Resnik 2009; Forge 2010; Resnik 2009; Selgelid 2009). This chapter starts with an overview of different dual use concepts that are co-existing within research ethics and legislation.

Dual use Concepts

Definitions of dual use differ based on 1) the item with dual use (e.g., knowledge, technologies, or artefacts resulting from research), and 2) the areas of use referred to in the opposition of a dual *use* (e.g., civilian/military, benevolent/malevolent, peaceful/non-peaceful, or legitimate/illegitimate, as introduced below). For the current purpose, the key dual use item is *research itself*. Dual use is usually discussed particularly with respect to life sciences research (see for example NSABB 2007; RKI 2013; WHO 2022) but can also emerge in other disciplines, such as artificial intelligence (see ZEVEDI 2022). The existing definitions of dual use items in research extend to *knowledge* generated within research, *technologies* employed or emerging from research, and *artefacts* created by these technologies (Forge 2010). Several existing definitions of areas of dual use can be found in Rath et al. (2014), who delineates four dual use concepts present in international and national laws.

1) Civilian versus Military, is the opposition used in

a) *policies limiting the proliferation of civil technologies to a non-aligned military. It is based on considerations of* National Security. (Examples include the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual use Goods and Technologies, 1995; Article 2 of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual use items)

b) *policies limiting spin-in of civilian technologies for military applications*. *It is based on the underlying principle of* Human Security. (European Union Horizon restricts funding to research having an 'exclusive civil application focus' (cf. Rath et al. 2014: 780); Guidelines for Researchers on Dual Use and Misuse of Research published by the Flemish Interuniversity Council (Verlaeckt 2022))

c) *policies supporting spin-offs and spin-ins of military and civilian applications. These policies tend to be based on the underlying principles of* National Security, Civil Security, Economic Interests. (United States Congress, Office of Technology Assessment 1993; European Commission 2021)

2) Benevolent versus Malevolent

This opposition is used in policies that take Human Security (environmental, food, health, individual, community and political security) as their core principle. (European Parliament legislative resolution 23 October 2012 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items; Proposed Framework for the Oversight of Dual Use

Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information (NSABB 2007); Dual use potential of life sciences research. Code of conduct for risk assessment and risk mitigation (RKI 2013)).

3) Peaceful versus Non-Peaceful

This opposition is predominant in policies aimed at National Security and Human Security (individual and community security). In contrast to the opposition between civilian versus military use (see above), it highlights the possibly of misuse of research by non-state organizations. (Treaty on the Non-Proliferation of Nuclear Weapons; Global Guidance Framework for the Responsible Use of the Life Sciences (WHO 2022))

4) Legitimate versus Illegitimate

This opposition is usually found in National and International Legislation oriented towards a principle of Lawfulness. (cf. also: Global Guidance Framework for the Responsible Use of the Life Sciences (WHO 2022)).

The diversity of dual use definitions is owed to the different institutional purposes and enables Commissions for Ethics in Research to fall back on a version that suits its institutional context. At the same time, they reveal a current lack of consensus on the question of dual use within research ethics.

How to define dual use in your institution?

The way an institution defines dual use has direct repercussions on which stakeholders to involve in its governance of such research. Actors that can contribute to the governance of dual use research include, according to Rath et al. (2014):

- *National authorities* govern dual use research understood as *civilian versus military* research-use in the sense of *limiting non-aligned militaries' access to civil technologies* and dual use research understood as *peaceful versus non-peaceful* research-use, e.g., by enacting export control laws or embargos;
- *National authorities and national courts* govern dual use of research understood as *legitimate versus illegitimate* research-use by passing laws on the ways research-related items (knowledge, technologies, artefacts) are allowed to be used;
- *International authorities* also govern dual use research understood as *peaceful versus non-peaceful* research-use, e.g., by, again, enacting export control laws;
- *Civil society* governs dual use understood as *civilian versus military research-use* in the sense of *limiting spin-in of civilian technologies for military applications*, e.g., by promoting Peace/Civilian Clauses within research institutions, by self-assessing their research, or by serving as members of national research ethics committees such as KEFs (Committees for Ethics in Security-Relevant Research, Germany); and Civil society also governs dual use research understood as *benevolent versus malevolent* research-use, e.g., by serving as members of research ethics committees, or by self-assessing their own or – as a reviewer – others' research before publication with respect to the potential of misuse for malevolent purposes.

The present guideline is directed to and originates from civil society, in particular the scientific community. Specifically, it is directed to members of KEFs and individual researchers. We would therefore expect that most readers of this guideline will find the following concepts most useful:

- a concept of dual use research based on the civilian versus military distinction with the intention of limiting spin-in of civilian technologies for military applications grounded in the principle of Human Security,
- a concept of dual use research based on the benevolent versus malevolent distinction grounded in the principle of Human Security, specified as environmental, food, health, individual, community and political security,
- a concept of dual use research based on the peaceful versus non-peaceful distinction grounded in the principle of National Security and Human Security, specified as individual and community security,

or any combination of these three concepts.

3) Examples and Challenges from Different Fields

Lead author(s): Andreas Brenneis & Verena Risse

One of the main challenges for KEFs is to identify potential dual use research and technologies. This is often a challenge because much of the literature focuses on a few iconic examples from prominent fields. In the following we try to provide a slightly more inclusive list of examples drawing on a number of sources (Tucker 2012, Miller 2018, Verlaeckt 2022).

In addition, dual use risks are often discipline-specific, and hardly any discipline is free of dual use risks. As intuitive as this truth may be, it has not yet gained full attention. Some explanation for this lies in the historical development of the topic.

Sources differ as to what the first cases of dual use discussions were (some date them back as far as to Francis Bacon in the 1600s, cf. Oltmann 2015: 328), but it seems quite uncontroversial that the prevalent cases originate from physics or the life sciences. Nuclear energy research with its potential use in nuclear weapons research or research on (influenza) viruses that were prone to serve as biological weapons were among the most prominent cases triggering the modern debate in the 20th century (e.g. Bezuidenhout and Rappert 2012).

The following selection of examples are not only intended to illustrate that dual use concerns may be relevant for a much broader range of disciplines, but we will also discuss specific challenges confronting some of the disciplines.

Nuclear Technology

Nuclear technology encompasses various applications, including nuclear power generation, medical imaging and treatments, and military weaponry. While nuclear power provides ample energy, concerns arise from the proliferation of nuclear materials and the risk of nuclear accidents or terrorist attacks on nuclear facilities. Additionally, the same technology used for peaceful purposes can be diverted for the development of nuclear weapons, posing significant security threats and geopolitical risks. See also Miller and Taebi 2018; Colussi 2016.

Life Sciences

Advances in the biological sciences, such as genetic engineering and biotechnology, offer immense potential for improving healthcare, agriculture, and environmental sustainability. However, the manipulation of genetic material and the creation of synthetic organisms raise concerns about biosecurity and biosafety. Malicious actors could exploit biotechnological methods to engineer deadly pathogens, develop bioweapons, or cause ecological harm through the deliberate release of genetically modified organisms. The assessment of benefits and burdens as well as potential recipients and bearers of these must therefore be especially “fine-grained” (Miller and Selgelid 2007: 542). In addition, it seems advisable to consider relevant policy options that accompany certain kinds of research in this field (ibid.).

Dual use risks in biological and life sciences have been the object of specific concern for some time. The 2004 report “Biotechnology Research in an Age of Terrorism” emphasized the importance of a thorough assessment not only with regard to military use but also with regard to terrorism.

See also Tucker 2012; Miller 2018; Miller and Selgelid 2007.

Synthetic Biology

Synthetic biology enables the design and creation of novel organisms or biological agents with potentially harmful properties. Malicious applications of synthetic biology include the creation of bioweapons targeting specific populations or ecosystems, engineered pathogens resistant to existing treatments, or bioengineered pests capable of destroying crops or spreading disease. See also Kelle 2012; 2013; Marris, Jefferson and Lentzos 2014.

CRISPR-Cas9 Genetic/Epigenetic Editing Technology

CRISPR-Cas9 allows for precise modification of DNA, raising concerns about its potential for creating novel pathogens or genetically engineered bioweapons. Malicious actors could exploit this technology to develop highly virulent or drug-resistant strains of pathogens, leading to bioterrorism or biowarfare. Additionally, the accessibility of CRISPR-Cas9 technology raises concerns about DIY biohacking communities experimenting with potentially dangerous genetic modifications outside of regulated laboratory settings. Concerns about military applications of epigenetic editing have also recently gained attention. See also DiEuliis and Giordano 2018; Mir et al. 2022; Kropf 2024; Dalpé et al. 2023.

Chemical Engineering

Chemical engineering plays a critical role in the production of pharmaceuticals, fertilizers, and industrial chemicals essential for modern society. However, the same chemical processes and substances can be weaponized to produce toxic agents, nerve gases, or explosives. Chemical plants and storage facilities are vulnerable to sabotage or terrorist attacks, posing risks to public safety and environmental contamination. See also Miller 2018.

Information Technology (IT)

Information technology underpins modern infrastructure and communication systems, facilitating global connectivity and innovation. However, cybersecurity vulnerabilities in software, networks, and data storage systems can be exploited by cybercriminals, state-sponsored hackers, or terrorist organizations. Cyberattacks targeting critical infrastructure, financial institutions, or government agencies can disrupt services, steal sensitive information or cause widespread chaos. See also Riebe 2023; Weydner-Volkmann and Cassing 2023.

Cybersecurity

Cybersecurity measures are essential for protecting digital assets, networks, and personal information from cyber threats. However, the same tools and techniques used to defend against cyberattacks can be weaponized for offensive purposes. Malicious actors exploit vulnerabilities in software, hardware or human behavior to launch cyberattacks, steal sensitive data, or disrupt critical infrastructure systems. See also Riebe and Reuter 2019.

Artificial Intelligence (AI)

AI systems could be weaponized for various malicious purposes, including cyberattacks, surveillance, and autonomous weapons development. Malicious actors may deploy AI algorithms to amplify propaganda, manipulate public opinion, or conduct sophisticated phishing attacks. Furthermore, the development of autonomous weapons systems powered by AI raises ethical concerns about the lack of human oversight and the potential for accidental escalation in conflicts.

Research in the field of artificial intelligence faces a particular challenge. For AI researchers, explicability is a crucial ethical principle that guides their work. However, the more explicable AI is and the more accessible the underlying mechanisms are, the easier it is to misuse. It becomes even easier if open data is being practiced. (Hermann and Hermann 2022: 29) Therefore, AI research encounters a special need for weighing benefits and burdens not only with regard to its research question, but also with regard to how it is communicated and published.

See also Brundage et al. 2018; Urbina et al. 2022; Westerlund 2019; Koplin 2023; Carozza, Marshand and Reichberg 2022; Brenneis 2024.

Biometric Recognition Systems

Biometric data collected by recognition systems could be exploited for identity theft, surveillance or unauthorized access to sensitive information. Malicious actors may use stolen biometric data to impersonate individuals or bypass security measures, compromising privacy and personal security. Furthermore, the centralized storage of biometric databases poses risks of data breaches and unauthorized access by hackers. See also Smith and Miller 2021.

Blockchain Technology

While blockchain technology offers enhanced security and transparency for transactions, it can also be used for illicit activities such as money laundering, drug trafficking or terrorist financing. Malicious actors exploit the pseudonymous nature of blockchain transactions to conceal their identities and evade law enforcement detection. Additionally, blockchain-based smart contracts may contain vulnerabilities that could be ill-used for fraud or exploitation (Kirchschläger 2021). Thus, what is specific to the case of blockchain technology is that it appears to be both a dual-use good in itself, but also a mechanism that can be used to maliciously exploit other dual-use goods.

The following examples are more closely related to mechanical engineering (including aerospace engineering) and illustrate particular dual use issues. This concerns research on certain materials with a potential use for military equipment as much as research on improved vehicles or aeronautics. Moreover, mechanical engineering has a more targeted focus on industrial exploitation of the research results than in other disciplines. Therefore, additional dual use precautions include export controls depending on the countries for which the innovations and products are intended.

Aerospace and Defense

Aerospace and defense technologies encompass a wide range of applications, from commercial aviation to military weaponry and space exploration. While these technologies enhance national security and scientific progress, they also pose risks of proliferation and misuse. Advanced aircraft components or satellite technology can be repurposed for military and offensive purposes, including surveillance, reconnaissance, and combat. See also Farinella, Anselmo and Bertotti 2000; Finocchio, Prasad and Ruggieri 2008; Pražák 2021.

Advanced Materials

Advanced materials, such as nanomaterials, metamaterials, and smart textiles, offer unique properties and applications in various industries. However, concerns arise from the potential environmental and health impacts of nanomaterials, as well as their dual use potential in military and surveillance technologies. Nanomaterials could be engineered for stealth coatings, lightweight armor, or sensors capable of detecting chemical or biological agents (Panina et al. 2023).

Nanotechnology

Nanomaterials and nanodevices could pose health and environmental risks if released into the environment or used in consumer products without adequate safety measures. Malicious applications of nanotechnology include the development of nanoweapons, such as toxic nanoparticles or self-replicating nanorobots, capable of causing harm to living organisms or disrupting critical infrastructure systems (Whitman 2013).

3D Printing (Additive Manufacturing)

3D printing technology can be used to produce illegal firearms, explosives or counterfeit goods. Malicious actors could use 3D printers to manufacture untraceable weapons or components, bypassing traditional regulatory controls. Additionally, the proliferation of 3D-printed objects poses challenges for law enforcement in identifying and tracing illicit activities. See also Hoffman and Volpe 2018 and Volpe 2019.

Robotics and Autonomous Systems

Robotics and autonomous systems are revolutionizing industries such as manufacturing, transportation, and healthcare. However, concerns about the ethical and societal implications of autonomous weapons, drones, and robots arise from their potential for indiscriminate use, lack of human oversight, and lack of accountability. Autonomous systems could be deployed for surveillance, targeted killings, or suppressing dissent, raising questions about both their legality and ethical implications. See also Horowitz 2021; Sharkey and Sharkey 2012.

Unmanned Aerial Vehicles (UAVs or Drones)

Drones have been used by terrorist organizations for reconnaissance, surveillance, and targeted attacks. Their ability to carry payloads, including explosives or chemical agents, poses significant security risks. Malicious actors could use drones to conduct aerial surveillance of sensitive locations, deliver payloads to inaccessible areas, or carry out targeted assassinations with minimal risk of detection (WHO 2021). Furthermore, drones have to be considered as a special case of semi-autonomous or even autonomous systems, due to their long range and enhancement of human sight. They have long been the subject of dual use debates, which focus on their civilian (e.g. humanitarian) and military use and the possible transfer of technology and expertise between these different sectors (see also Meunier and Bellais 2018).

4) Legal Situation – Regulation

Lead author(s): Jochen Kuck

For the overview on the legal situation and regulation of dual use items in this section, we primarily refer to items that are usually used for civilian purposes but can also be used for military activities (see chapter 2 for an overview of alternative definitions of dual use). These items are, together with military items, one of the central targets of export control law.[1] Export control is to protect Germany and its partners from threats posed by the proliferation of conventional weapons, weapons of mass destruction (WMD), and the underlying technologies. It aims to prevent malign actors, such as terrorist groups, from accessing critical goods and technologies, deter states from using them for internal repression and human rights violations, and avoid further destabilization of conflict areas. Effective export control requires collaboration among authorities, industry, and research institutions. Export control is also crucial for research security.

From the German perspective, export control mostly applies to activities that pertain to foreign countries, especially countries outside the EU. However, even domestic activities, e.g. the knowledge transfer towards a guest researcher in Germany, may be legally relevant under export control law with regards to the concept of technical assistance. Furthermore, export control law comprises sanctions against individuals and entities, such as corporations, universities, or research institutes. These sanctions apply regardless of where these individuals are located at any moment. Moreover, there are certain countries which are sanctioned by embargo regulations.

Legal principle and exceptions

In Germany and the EU, trade and technology transfer with foreign countries is, in principle, free, i.e. it is not subject to any legal restrictions, such as for instance export license requirement. However, there are certain countries or certain individuals or entities to which the export of items or technology, or the provision of economic resources may be strictly prohibited, e.g. under an embargo regulation. Furthermore, the export of dual use goods or transfer of dual use technology requires an export license irrespective of the purpose of research. In legal terms, export means that the destination of the item or technology is located outside the EU.

Scientific freedom and civilian clauses

Art. 5 (3) of the Basic Law for the Federal Republic of Germany, i.e. the German constitution, says:

“Arts and sciences, research and teaching shall be free. The freedom of teaching shall not release any person from allegiance to the constitution.”

It is important to note that even this basic right of freedom of research does not release any research institution or researcher from his or her legal duty to comply with export control law. The underlying rationale of export control is to prevent misuse but not to restrict research. This is challenging when it comes to the publication of dual use relevant results since publication is part of good scientific practice (see paragraph on values below).

[1] There are also the aspects of sanctions against persons and countries. In general, it is distinguished between person based, country based and goods based export control.

Importance of export control in academia

The importance of export control in academia has increased over the last few years for several reasons, such as rising geopolitical tensions and the German authorities having increased their controls at universities and research institutions. To help academic institutions comply with the applicable rules and regulations, the EU has published the *Commission Recommendation (EU) 2021/1700 on internal compliance programs for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*. The German authorities, the Federal Office for Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle, BAFA) has also released a specific manual on export control and academia and has undertaken several outreach activities to academia (BAFA 2023).

Export control is especially important for academic institutions due to specific risk factors, such as their commitment to the free exchange of ideas, involvement in cutting-edge technologies, complex organizational structures, and the international nature of scientific exchanges. Additionally, regulating emerging technologies like for instance artificial intelligence presents new challenges for policymakers in export control, particularly due to the broad applications of these technologies. Quantum computing and related electronic hardware infrastructure has recently been added to the German export control list.

Legal sources

The most important legal sources in export control are:

- War Weapons Control Act (KrWaffKontrG)
- German Foreign Trade and Payments Act (AWG)
- Foreign Trade and Payments Ordinance (AWV), including Export List (AL)
- EU Dual-use Regulation (EU) 2021/821, including Annex I listing dual use items
- Embargo-Regulations, e.g. Iran (EU) Nr. 267/2012 or Russia (EU) 822/2014
- Anti-Terrorlists Al-Qaida, VO (EU) Nr. 881/2002; Afghanistan/Taliban, VO (EU) Nr. 753/201

Definitions, listed items and not-listed items

A core term in export control is “items” (Güter), which comprises three subcategories, such as goods, technology and software. The key term “dual use” is not defined in export control law but the EU Dual-use Regulation (EU) 2021/821 defines ‘dual use items’, which means *“items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of, including all items which can be used for both non-explosive uses and assisting in any nuclear, chemical or biological weapons or their means of delivery in the manufacture of nuclear weapons or other nuclear explosive devices”.*

These items, including technology and software are listed in Annex I to the EU Dual-use Regulation.

If any of these items is going to be exported to a recipient outside of the EU, the exporter needs to obtain a license from BAFA before exporting the item (Art. 3). In principle, items listed on Annex IV of the EU Dual use regulation even require a license when being transferred to a recipient inside the EU (Art. 11). Export means, simply put, making an item available in a country outside the EU, including via mail or via electronic means or even in carry-on luggage.

To better understand which kind of items fall into the regime of the Dual-use Regulation, it is helpful to take a glance at the categories according to which Annex I is structured, which are the following:

- Category 0: Nuclear materials, facilities and equipment
- Category 1: Special materials and related equipment
- Category 2: Materials processing
- Category 3: Electronics
- Category 4: Computers
- Category 5. Telecommunications and "information security"
- Category 6: Sensors and lasers
- Category 7: Navigation and avionics
- Category 8: Marine
- Category 9: Aerospace and propulsion

Even non-listed items may be subject to a license requirement if they are, or may be intended to be, used, in their entirety or in part, in connection with

- weapons of mass destruction or missiles suitable for this purpose (Art. 4 para. 1 lit. a of the EU Dual-use Regulation (EU) 2021/821)
- or as components of military items listed in the national military list that have been exported from the EU without authorization (Art. 4 para. 1 lit. c of the EU Dual-use Regulation (EU) 2021/821),
- a military end-use in the country of arms embargo (Art. 4 para. 1 lit. b of the EU Dual-use Regulation (EU) 2021/821),
- or for the construction or the operation of a facility for nuclear purposes within the meaning of Category 0 of Annex I of the EU Dual-use Regulation (EU) 2021/821 or for installation in such a facility if the facility is located in Algeria, Iraq, Iran, Israel, Jordan, Libya, North Korea, Pakistan or Syria (Section 9 AWV).

Technology

Export control law defines “technology” as a specific technical information required for the development, production, or use of a listed dual use item. Examples of technologies could be formulas, construction plans, descriptions, written instructions, and diagrams both as paper and electronic files. Technology must be either indispensable to achieve technical parameters of a listed dual use item or a key technology, which is indispensable because it is responsible for the fundamental functions of a dual use item. Technology transfer also includes a transfer via email or access to a server or a cloud from a country outside the EU or a server that is located in a country outside the EU.

Technical assistance

Technical assistance means “*any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including by electronic means as well as by telephone or any other verbal forms of assistance”* (Art. 2 (9) of the EU Dual-use Regulation (EU) 2021/821)). Technical assistance essentially means the verbal transfer of knowledge or know-how.

This legal concept is crucial for international projects, especially when hosting guest researchers or hiring personnel from outside the EU. Thus, technical assistance can occur as an export on campus in

Germany. Technical assistance to individuals from certain countries, such as the USA, the United Kingdom, Canada, Australia, New Zealand, Japan, Norway and Switzerland, are exempt from the legal concept of technical assistance.

Pursuant to Art. 8 in connection with Art. 4 para. 2 of the EU Dual-use Regulation, knowledge-transfer requires a notification to BAFA, which will then decide whether an export license is required if either BAFA has informed the exporter that the items in question are or may be intended, in their entirety or in part, for any of the uses referred to in Article 4 (1) (see above), such as for example:

- the development of WMD or
- military end use in a country with arms embargo or
- for the construction or operation of a nuclear facility if the facility is located in Algeria, Iraq, Iran, Israel, Jordan, Libya, North Korea, Pakistan or Syria (Section 9 AWV).

Additionally and more importantly in practice, exporters providing technical assistance must notify BAFA if they become aware that dual use items are intended, in their entirety or in part, for any of the uses mentioned above. Therefore, institutions must diligently check for any red flags regarding the recipient and the end use for whom and for which they intend to provide technical assistance, ensuring no obvious indications are overlooked. While using a listed item is an indicator, it alone does not mandate a notification requirement.

Publications

The first publication of research results is considered an export. Thus, a publication which can be of dual use and meets the technology threshold, which is rather high, requires an export license (Butler 2012).

Legal exceptions

There are several legal exceptions as far as the export of technology and technical assistance is concerned (BAFA 2023: 36). The first is basic research, i.e. any technology transfer or technical assistance that remains within technical readiness level one to three (BAFA 2023: 79-80). This exception is, in principle, not applicable to embargos and the export of goods. A strong indicator that a research project is not a case of basic research is if research funding is provided by industry or private corporations or if they are involved in a research collaboration. The second exception is publicly available knowledge. Any knowledge that is already published or available in any university library, and thus in the public domain, is not export-controlled. Third, content that is necessary to file a patent is also not export-controlled unless it refers to nuclear technology.

Personal liability and responsibility

The violations of export control laws and regulations are sanctioned as either criminal actions by fines or prison sentence, or as administrative offensives, which entails fines. In most cases, the risk is that rules are violated negligently. Every employee is responsible for his or her actions within his or her area of responsibility. If management representatives of a research organization violate their duties of selection, control and organization, they can also be fined under § 130 of the Act on Regulatory Offences (OWiG). The authorities also have the option to fine the research organization as such under § 30 OWiG. The management of any research institution has the legal duty to organize its institution in a way that violations of export control law are precluded and to supervise the personnel to which export control compliance has been delegated.

Compliance processes

To comply with export control laws, research institutions must establish specific processes, including one for exporting physical goods, one for vetting non-EU personnel, one for managing collaborations, and one for publications. The entire set of processes, including documentation, clearly defined responsibilities within an institution and awareness raising are the most important elements of what is referred to as the Internal Compliance Programme (ICP) in export control. It is the duty of the management of any research institution to establish an ICP, which needs to be risk adequate, to fulfill its legal duty to organize the institution in a way to be compliant with all applicable laws and regulations.

Conclusion

A key takeaway from examining export control laws in academia is that exporting certain listed items, technology, software, and even know-how to a destination outside the EU may require a license. Technical assistance, including educating researchers, might also need a license under certain conditions, even when the whole process is happening within German borders. Moreover, specific research activities may be prohibited when involving embargoed countries or researchers from those nations.

Due to the intricate nature of export control law, it is crucial for research institutions to develop expertise in this area to effectively evaluate cases. This expertise should be leveraged in KEF proceedings when applicable. Achieving compliance with export control law requires raising awareness among researchers and administrators, establishing and enhancing an Internal Compliance Programme (ICP) on export control, and securing support from top management. Additionally, academic institutions can benefit from exchanging ideas, experiences, and best practices with peers to address the unique challenges of navigating the legal framework of export control in academia.

5) Ethics

Lead author(s): Niël Conradie; Mario Kropf & Martina Philippi

Responsibilities

Not all instances of dual use give rise to demands for moral responsibility. It is when the dual use involves a moral transgression, or raises a concern of such a transgression, that the assignment of responsibility is called for. This means that when we consider the matter of dual use and responsibility, we are focused more narrowly on so-called research of concern (DURC), i.e. research that could be directly misapplied to cause damage to public health and safety, the environment or to other important legal interests and where the risk of misapplication is sufficiently likely and imminent. There are two broad questions to be answered in these cases: *who* is responsible? (Lev and Keren 2024) And *what* are they responsible for? (Heinrichs and Ergin Aslan 2024) In this section, we focus on moral responsibility, distinct from legal responsibility (see previous chapter). Moral responsibility involves justifying actions to others and legitimizing responses to them based on their moral quality. Blame may result from harmful actions lacking adequate justification, while morally commendable actions may warrant praise (Shoemaker 2017; Menges 2020). Only moral agents, not all individuals, are subject to blame or praise, and the actions under consideration must stem from their moral agency (Strawson 1962; Fischer and Ravizza 1998; Vargas 2013; Shoemaker 2015). The structure of responsibility typically (but not universally) involves A being responsible for x toward B by reference to y, with A representing a moral agent (individuals, groups, or institutions), x referring to actions or decisions, B representing the recipient of responsibility (which we keep intentionally underspecified here), and y encompassing reasons, social conventions, laws, or moral norms (Werner 2002).

As to who is responsible in cases of DURC, there are many possibilities: developers (e.g. funders, scientists, researchers, engineers), purveyors (e.g. journal editors, corporate officers), users, and regulators (including legislative but much more so executive regulators).[2] All of these parties can fall short of justified normative expectations in cases of DURC, and thus can be morally responsible. However, since such cases challenge our responsibility practices, we believe the focus should be on developers, purveyors, and regulators. In contrast, attributing responsibility to users is in general straightforward: if an user employs a tool for a maliciously or harmfully dual use, they are usually accountable – barring the usual excuses and exemptions that can apply.

As to the question of what responsibility needs to be attributed for, it is important to note that there are types of cases that are unproblematically dealt with by established practices: if, for example, a developer or purveyor intentionally produces or distributes a research contribution or item with a possible DURC with the *active intent* that the concerning dual use scenario occurs, then they are clearly responsible for this.

The more paradigmatic, and problematic, cases of DURC occur when the output (research or product) has a beneficial primary use, and the developer, purveyor, or regulator are considering either the risk or uncertainty of foreseen and reasonably foreseeable dual uses. In cases like these, any dual use is unintended. These can be divided into, on the one hand, cases where the dual use is foreseen, and on

[2] To clarify this last group, our primary targets here are Research Ethics Committees, University Ethics Committees, DURC Committees, and similar bodies. [Questions of legal regulation have been discussed in the previous section.]

the other hand, cases where the dual use is foreseeable but unforeseen. If the dual use case in question is foreseen, a developer or purveyor would be negligent or reckless in permitting its dissemination, reflecting a deficit in quality of will, or a "violation of some standard" (Herstein 2019: 11). The developer or purveyor has control over whether the dual use occurs, so awareness alone is insufficient—judgment and action are required. As Small and Lew (2021: 112) put it, "[A] person who is mindful, and therefore acts with awareness, and remains observant, non-reactive, describing and non-judging in situations that require moral reasoning will also be morally responsible."

Clearly, there are limits to responsibility in the cases described above. We don't hold developers, purveyors, or regulators of hammers accountable for murders committed with them, yet we do blame gain-of-function researchers if their work is used for virological terrorism. This indicates that we hold individuals responsible for some (reasonably) foreseen dual use cases (including DURC) but not others, and the criteria for this distinction aren't immediately clear. Factors such as potential harm, likelihood of harm, and the scale of benefit—often analyzed through a risk/benefit lens (Taddeo and Blanchard 2022: 19)—inform our judgments (see Chapter 6). However, there is significant variation in balancing these considerations. For example, research shows experts accept risk if benefits outweigh harms, considering population-level impacts, while laypeople are more likely to also weigh factors like voluntariness and fair distribution of risks and benefits (Nihlén Fahlquist 2021: 816).

Even more, or at least differently, challenging are those cases where the dual use was foreseeable, but the developers, purveyors, and regulators failed to foresee it. Such cases are still instances of negligence if the failure to foresee it is explained by a deficit of conscientiousness and/or failure to spend sufficient resources to assess the potential for misuse (Björnsson 2011: 185-186). A developer, purveyor, or regulator of research or technology has the prospective responsibility to diligently attempt to foresee the potential DURC of their outputs. However, given that research is often characterised by the uncertainty of its outcomes, that our technologies become increasingly complex and opaque, and that we frequently have to trust other experts contributing to our projects without the ability to scrutinise their work ourselves, it can become extraordinarily difficult to identify where the appropriate level of conscientiousness lies. Still, scientists ought to reflect on their studies and alert those in charge if there is potential for misuse.

Taken altogether this allows us to identify three vital, interrelated challenges: (i) the difficulty of weighing risk and benefit, (ii) the role of uncertainty, and (iii) the problem of determining reasonable conscientiousness. As regards (i) and (ii), it is largely uncontroversial that in cases where *sufficient possibility of DURC* is foreseen, a risk/benefit analysis should be undertaken (see Chapter 6). We can say that developers and regulators are under prospective responsibility to undertake such measures as demanded by both their roles and wider normative expectations of their quality of will. But how should this work be divided? In favour of the developers – including researchers –, it can be plausibly pointed out that they are both 'closest to the coalface' and likely to have the highest level of technical expertise vis-a-vis the output. On the other hand, they might lack expertise in undertaking risk/benefit analyses or lack the perspective from which to properly evaluate the scope of possible impacts – to mix metaphors, being close to the coalface can prevent you from seeing the forest for the trees. In terms of these considerations, it seems that properly trained and informed regulators should be preferred. Of course, these need not be mutually exclusive. One could require both developer and regulator to undertake a risk/benefit analysis (see Chapter 6), but in doing so risk wasting time and resources by doubling work and drawing experts away from their domains of expertise. Also, depending on the uncertainties involved, it can be unclear when there is or is not sufficient possibility of DURC. This ties us to (iii), and the question of what degree of conscientiousness is it morally acceptable to demand of those trying to handle DURC, which demands of us a better understanding of both decision-making under uncertainty and the nature of uncertainty in DURC cases. What can be said is that establishing the required level of conscientiousness cannot be done wholly theoretically but requires deliberative engagement with stakeholders and their representatives to negotiate reasonable expectations.

Values

Values are central to ethical considerations, providing orientation for weighing benefits and risks—such as the dual use risk—in research and technology development. Applied ethics identify specific values relevant to particular contexts, such as transparency, fairness, reliability, and accountability, as noted in the High-Level Expert Group on AI's Ethics Guidelines for Trustworthy AI (2019). These values guide decision-making and legitimize choices in research and technology governance.

Conflicts predominantly arise not between values themselves but from the consequences of actions motivated by different values. To illustrate, the value of reliability can motivate agents to take actions to increase the ability of an algorithmic system designed for triage to accurately identify patients most likely to benefit from treatment, and the value of fairness can simultaneously motivate actions to remove variables from consideration that could engender unfairness. These consequences can conflict if the consideration of some variables might increase reliability but also engender unfairness, as can be the case with so-called protected classes (race, sex, etc.). This is similar to conflicts of interest.

While values can align with different stakeholders' perspectives (cf. Friedman and Hendry 2019), ethical considerations rather focus on generalized, desirable needs or interests than on situational interests. In dual use research, transparency is crucial, emphasizing conducting and disclosing research to support the freedom and democratization of research.

Transparency, accessibility, and collaboration in research are promoted under the principle of *open science*, which promotes making scientific knowledge, data, and methods openly available to everyone. In the context of dual use risks, open science presents a complex challenge: it encourages the free exchange of ideas and accelerates innovation, which, as described above, raises concerns about the potential misuse of sensitive information for harmful purposes.

The value that conflicts with the transparency requirement of open science is not economic competitive advantages, but resilience against possible attacks also referred to as security (Jore 2019). Security in this context refers to handling risks arising from the use of a well-functioning technology that is motivated by malicious interests.

This creates a fundamental conflict: open science advocates for complete transparency in research processes, data, and findings to foster innovation and trust, while security requirements necessitate secrecy or restricted access to prevent misuse or protect privacy rights. Open science encourages unrestricted collaboration across borders and disciplines to accelerate progress, but security measures require controlling collaborations, particularly with entities or individuals from countries with challenging conditions of cooperation. This can hinder the free exchange of ideas and slow down scientific advancements. Similarly, while open science aims to make knowledge universally accessible, security concerns involve restricting access to certain types of information to prevent dual use applications, limiting who can access and benefit from scientific research.

Balancing these conflicting demands involves implementing stringent risk assessments to identify dual use potential in research projects and establishing oversight committees to monitor and guide such research. Developing policies for selective openness, where only certain parts of the research are shared openly while sensitive data is kept restricted, can help. Controlled access repositories where researchers can access data after meeting specific security criteria also offer a solution. Additionally, educating researchers about dual use risks and responsible conduct, promoting awareness of the ethical implications of their work, and enforcing regulations that balance open science with security concerns are essential. Creating clear guidelines on what constitutes dual use research (see Chapter 2) and the procedures for handling such research (see Chapter 6) is crucial.

Thus, while the principle of open science promotes progress and inclusivity, it also increases the risk of misuse of sensitive information. A nuanced approach that includes robust risk assessments, selective openness, and stringent regulatory frameworks is essential to balance the benefits of open science with the imperative to ensure security.

Where research institutions subscribe to additional ethical values—such as a peace or civilian clause—this adds an additional layer of ethical and operational complexity. Such institutions must ensure that their research output is aligned with their commitment to peaceful and civilian applications. This often involves stringent internal policies and oversight mechanisms to prevent any deviation from their stated goals. However, in case of dual use it is research projects with benign intentions that can be repurposed for harmful uses. This inherent risk requires these institutions to implement rigorous risk assessment and management procedures, often more stringent than those at institutions without such clauses.

In addition, the commitment to a civilian clause can limit the scope of collaboration with other research entities, particularly those engaged in defense or security-related projects. While open science thrives on collaboration and the free exchange of ideas, institutions with a civilian clause must carefully vet potential collaborators to ensure that their partnerships do not inadvertently contribute to military or non-peaceful applications. This can slow down research progress and limit access to a broader pool of knowledge and resources.

Moreover, these institutions need to develop policies that allow for the dissemination of research findings in a way that aligns with open science principles while simultaneously ensuring that sensitive information that could be misused for non-civilian purposes is adequately protected. This might for example involve creating controlled access repositories and implementing selective openness strategies where only non-sensitive parts of the research are openly shared.

6) Handling Dual Use Risks

Lead author(s): Karla Alex; Andreas Brenneis; Martin Hähnel

It is common to refer to dual use—where it is not explicitly desired—as a risk for researchers and research institutions. Dual use is viewed through the lens of risk to emphasize the need for careful assessment, management, and mitigation strategies to prevent unintended harmful consequences while enabling beneficial advancements. In the following, we first describe the concepts risks, risk assessment and risk management, and thereafter present a decisional flowchart (framework for addressing dual use concerns).

What Are Risks and How Can They Be Managed?

What are risks?

With the term 'risk' we refer to the statistical expectation value of the occurrence of an unwanted event, understood as a product of severity of the event and likelihood of its occurrence.

An additional element of risk, alongside probability and severity, is responsibility (cf. Kermisch 2012). Different cultures, depending on insularity, individualism, egalitarianism, and hierarchy (cf. Douglas 1979; quoted from Kermisch 2012: 95), define risks differently. Risks can therefore not be described in a vacuum but are determined by societies:

> "Risks are […] constructed according to a social process in which individuals are involved as active subjects: a risk does not only characterise an element of the external world – a danger – but results from the interaction between social processes and, possibly, the external world" (Kermisch 2012: 96).

One example for this is the decision of an institution or a specific scientific community to define military use of civilian research (e.g., in institutions with so-called civilian clauses) *per se* as a risk. What constitutes a risk from the perspective of a given research institution thus depends not only on the possible trajectories of a research project, its dissemination and uptake, but also on institutional goals and values. For a research institution with a civilian clause, military use of their projects is a risk, for other institutions it need not be.

How can risks be managed?

a) Risk assessment

Risks are so widespread that it is impossible to accurately assess risks associated with each action and event. But some actions, such as conducting human-subjects research (cf., for a summary, Rudra and Lenk 2021), practicing medicine (cf. Spielthenner 2012), marketing specific products, such as chemicals (cf., for a summary, Jahnel 2015), and conducting security-relevant research (cf. Chapter 2 of this guideline on the definition of dual use and misuse of research and Chapter 4 on legal regulatory requirements) are regularly subject to risk assessments. This is based on the general understanding that these actions can be associated with risks so severe that they should be minimized or prevented because their imposition is impermissible (cf. Hayenhjelm 2018; Steigleder 2018).

To assess risks, it is important to determine

- the likelihood of an unwanted (harmful) event,
- its severity,
- as well as associated uncertainties (with respect to likelihood, severity and responsibilities).

Risk assessments should furthermore put specific emphasis on identifying the cause for the envisioned unintended outcome. This can not only help to reduce (uncertain) black swan events—rare, unpredictable events with severe consequences—but is also part of assessing causal responsibility for unintended outcomes of risky events. In addition to assessing an action's risks, it is important to compare its risks to potential benefits as well as to compare its risk/benefit ratio to that of alternative actions (cf. Spielthenner 2012). Risk assessments for research projects pose challenges in identifying their future trajectory and thus the risks they pose, as well as in identifying alternatives, which explains the high demand for expertise in the relevant fields.

b) Risk prevention and mitigation

Risk assessments are an important first step towards identifying impermissible risks, preventing, mitigating, and otherwise managing them. There are multiple means of risk mitigation, typically starting with the decision of how to approach risk in general. One general approach consists in following the Precautionary Principle (cf. Kuhlau et al. 2011). The Precautionary Principle states that

- in cases of uncertainty about the likelihood or severity of unwanted outcomes, precautionary measures should be applied to prevent them.

Decisions based on the Precautionary Principle are generally risk averse and—because risky courses of action are not taken—do not always require risk/benefit assessments and comparison with alternatives. Alternatively, decisions can be based not only on risk assessments, but the richer information of risk/benefit assessments and comparison with alternatives, which better informs risk neutral decision making.

Precautionary measures to prevent risks – while sometimes introducing risks of their own—can include safety barriers or safety factors. To increase safety, multiple different safety barriers are required. In cases of managing dual use and misuse of research results, safety barriers can include civilian clauses at research institutions, best practice guidelines by publishers and other stakeholders, in addition to pre-publication reviews, export control laws, and further measures. An additional risk management strategy is to compensate those who are exposed to risk or have been affected by past exposure for their losses (cf. Haines 2018). This strategy is compatible with and can follow precautionary measures.

In summary, risk management requires the identification and assessment of risks, and the avoidance or mitigation of risks the imposition of which is impermissible. Risk assessment consists of determining the likelihood, severity, and responsibility (with particular emphasis on the cause) of a risk and the associated uncertainties. Preventing or mitigating risk requires the introduction of safety barriers and safety factors.

Decisional Flowchart

Framework for Addressing Dual use Concerns

The framework presented herein represents a revised iteration of the most comprehensive framework concerning decisions regarding dual use technologies to date, as initially formulated by Tucker (2012: 67 ff.). While Tucker's framework primarily focuses on emerging technologies within the life sciences domain, our approach endeavors to encompass a broader spectrum of emerging technologies. Moreover, monitoring research processes is of equal, if not greater, importance compared to scrutinizing research outcomes, as the processes themselves can harbor potential for harm or misuse.[3]

Another notable distinction lies in the intended recipients of the framework: whereas Tucker's framework targets policy makers at local or federal governmental levels, our framework adopts a more inclusive stance. It serves as a decision-making tool applicable to various stakeholders, predominantly encompassing research ethics committees, policymakers across different tiers of governance, research institutions, funding bodies, research groups, and individual researchers.

Our framework comprises two principal components: the first component furnishes a structural overview of the process for ethically monitoring and assessing potential misuses of research outcomes, while the second component delineates a process for the ethical governance of such misuses.

(1) Ethical Monitoring and Assessment of Potential Misuses of Research Results (RMA)

The framework starts with the completion of a questionnaire about the research project or outcome in question and a subsequent *Risk of Misuse Assessment* (RMA).[4] Five parameters have to be assessed and ranked with a value.

These parameters encompass the *real or possible accessibility*, *ease of misuse*, *magnitude of potential harm*, *imminence of potential misuse* of the technology or research process/outcome and the likelihood that the person identified as the perpetrator of misuse can be discharged from responsibility. Each parameter is assigned a value (low/medium/high) based on questionnaire outcomes.

The *real or possible accessibility* indicates the ease of generating and spreading research result (acquire the necessary equipment, software, and further information that would enable someone to misuse a given invention). The *ease of misuse* evaluates what kind of expertise and knowledge a potential bad actor would need to make effective use of an innovation or technology. The *magnitude of potential*

[3] Particularly, the pivotal role of research ethics committees lies in evaluating research proposals that have the potential to yield unethical or injurious outcomes. It is imperative that these committees not only assess the proposed research's ethical implications but also consider the possibility that certain research endeavors may be fundamentally detrimental, warranting a critical examination of whether they should be pursued at all. When it comes to addressing dual use aspects of research, it is preferable to conduct assessments early in the research development phase rather than postponing them until the project's conclusion.

[4] The entity responsible for conducting the Risk of Misuse Assessment (RMA) and overseeing the formulation of the questionnaire as well as evaluating its outcomes has yet to be explicitly determined. Research ethics committees situated within research institutions emerge as a compelling choice for this role. Their proximity to ongoing research endeavors within their respective institutions coupled with their established expertise in navigating ethical challenges inherent to scientific research processes positions them as well-suited candidates. Should research ethics committees be designated as the institutional bodies tasked with monitoring dual use research, they must be adequately equipped to fulfill this responsibility. Beyond providing guidelines, this may necessitate a redistribution of authority in favor of these committees, empowering them with the mandate to assess relevant research projects comprehensively.

harm resulting from misuse depends on both the technology itself and the susceptibility of the probable targets. The *imminence* of potential misuse refers to the speed with which a research result can be exploited for malicious intention. It strongly depends on a technology's maturity.

Depending on the aggregated risk score derived from the Risk of Misuse Assessment, the decisional framework offers two courses of action. In instances where the risk of misuse is deemed low, continued monitoring of the research process is advised to detect any developments necessitating the formulation of a governance strategy. Upon detecting substantial changes, a reassessment via RMA is recommended. Conversely, if the risk of misuse is moderate or high, the second component of the decision-making framework becomes pertinent.

(2) Ethical Governance of Misuses of Research Results (EGA)

Should the RMA yield a moderate or high-risk score, an *Ethical Governability Assessment* (EGA) is warranted.[5] This assessment aims to evaluate options for governing the dual use research or outcome in question through five parameters: *Embodiment*, *maturity*, *convergence*, *rate of advance*, and *international diffusion*.

Embodiment refers to the degree to which a technology exists as hardware or as intangible information. *Maturity* refers to the position in the research and development process and can be approximated with technology readiness levels. *Convergence*—as in 'convergent technologies'—indicates how many different disciplines contribute to a new device or technology. *Rate of advance* refers to the acceleration of a technology's effectiveness as measured in e.g. reliability, speed, throughput, accuracy, or cost. *International diffusion* indicates the availability across national markets or other local distribution channels.

Analogous to RMA, each parameter in EGA is assigned a value (low, medium, or high).

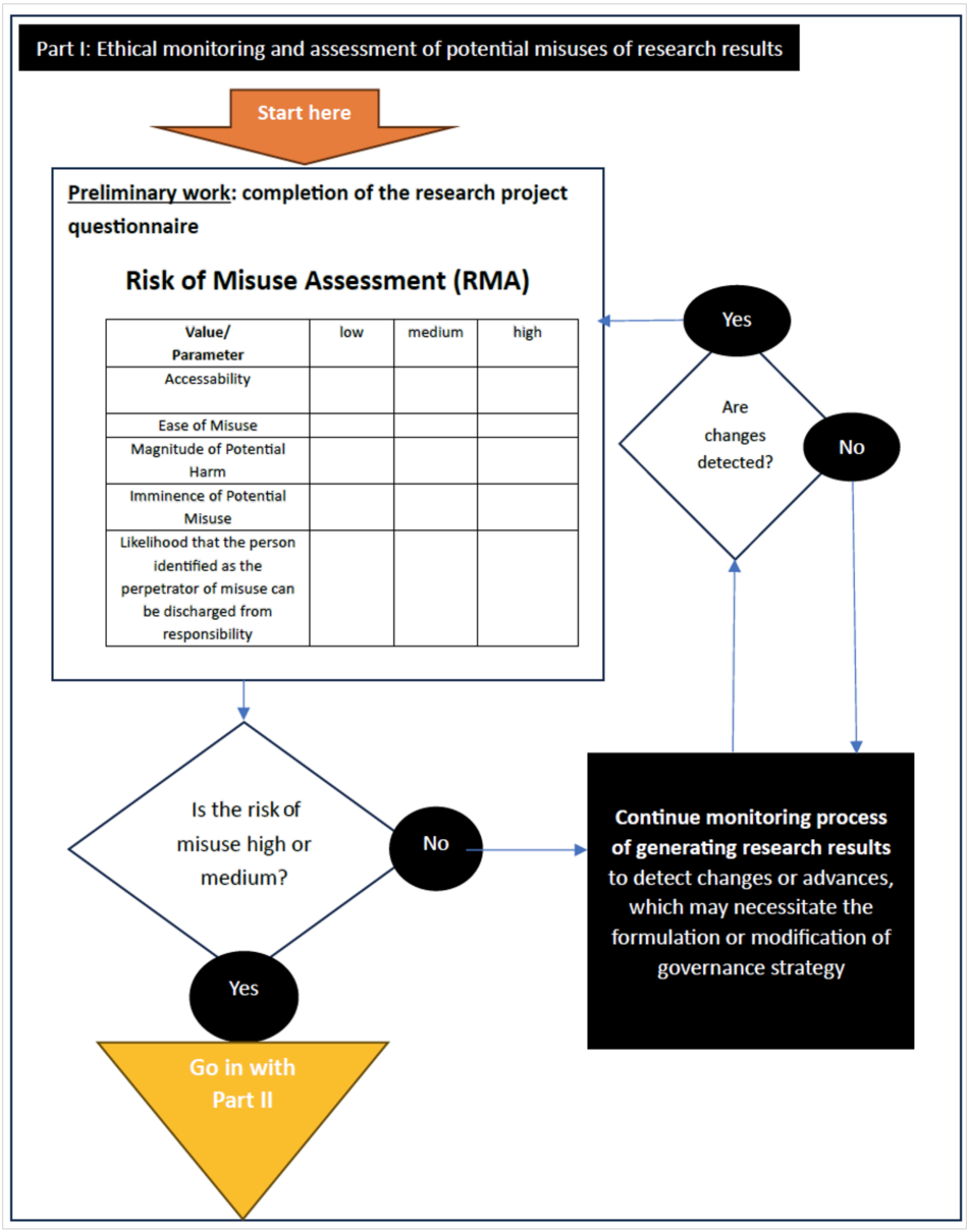
Based on the overall governability score derived from the EGA, the decision-making framework offers two paths. In instances where governability is deemed low, informal measures should be devised to implement at least some degree of governance, which may include ethical codes of conduct or awareness-raising programs. Conversely, if a research process or outcome exhibits a moderate or high level of governability, a combination of soft-law[6] and hard-law[7] measures should be contemplated and elaborated. Various trade-off scenarios must be carefully considered to strike a balance between implementing governance measures and preserving the freedom of scientific research, alongside other pertinent factors.[8] Drawing upon these deliberations, a customized set of governance measures can be crafted to suit the specific research process or outcome under scrutiny.

[5] The Risk of Misuse Assessment (RMA) stands out as a pivotal component for research institutions such as universities and other organizations engaged in potential dual use research. Consequently, within our framework, the RMA assumes a central role. However, the suitability of these institutions to assess ethical governability remains somewhat ambiguous. While the parameters informing the Ethical Governability Assessment (EGA) hold relevance for assessments conducted by research ethics committees, their placement within these institutions may not be definitive. Scholarly societies or specialized bodies overseeing the governability of specific scientific and technological advancements might offer more appropriate avenues. This is because the question of governability necessitates consideration of a broader spectrum of factors beyond scientific progress alone.

[6] Like prepublication reviews, security screenings, best practices etc.

[7] Like multilateral treaties, accreditations, certifications, or onsite inspections.

[8] Trade-offs to be considered are at least the following: benefits vs. risks, well-being vs. harm, freedom of research vs. public security.



Part I: Ethical monitoring and assessment of potential misuses of research results

Start here

Preliminary work: completion of the research project questionnaire

Risk of Misuse Assessment (RMA)

Value/ Parameter	low	medium	high
Accessability			
Ease of Misuse			
Magnitude of Potential Harm			
Imminence of Potential Misuse			
Likelihood that the person identified as the perpetrator of misuse can be discharged from responsibility			

Is the risk of misuse high or medium?

Yes

Go in with Part II

No

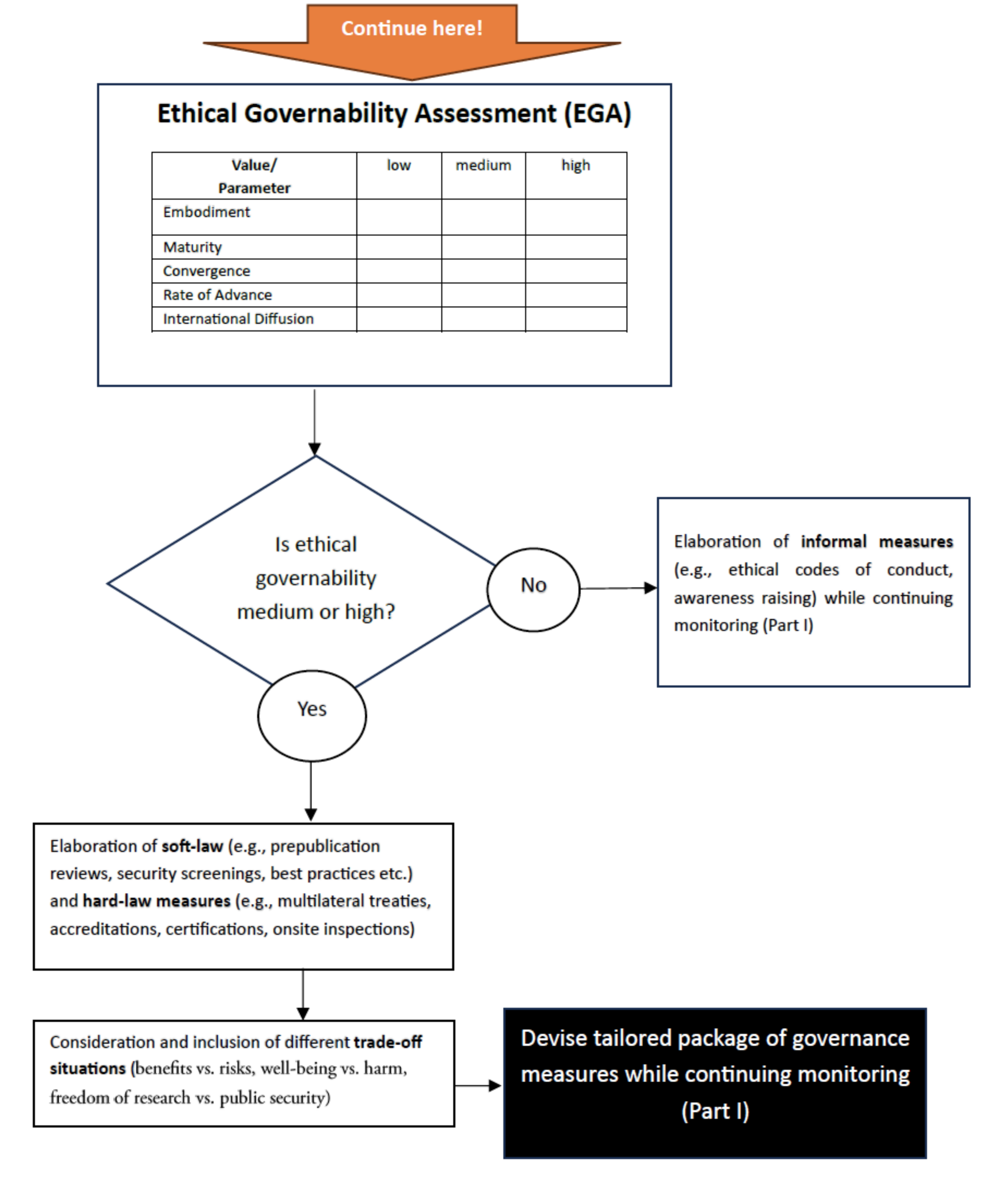
Continue monitoring process of generating research results to detect changes or advances, which may necessitate the formulation or modification of governance strategy

Are changes detected?

Yes

No

Part II: Ethical governance of misuses of research results



Ethical Governability Assessment (EGA)

Value/ Parameter	low	medium	high
Embodiment			
Maturity			
Convergence			
Rate of Advance			
International Diffusion			

Is ethical governability medium or high?

Elaboration of **informal measures** (e.g., ethical codes of conduct, awareness raising) while continuing monitoring (Part I)

Elaboration of **soft-law** (e.g., prepublication reviews, security screenings, best practices etc.) and **hard-law measures** (e.g., multilateral treaties, accreditations, certifications, onsite inspections)

Consideration and inclusion of different **trade-off situations** (benefits vs. risks, well-being vs. harm, freedom of research vs. public security)

Devise tailored package of governance measures while continuing monitoring (Part I)

7) Limitations

While this guide provides a comprehensive approach to the ethical assessment of dual use and misuse of research issues, there are clear limitations to its scope. It cannot replace formal legal regulations or institutional self-certification measures but should instead be seen as a complementary tool to inspire reflection. Legal frameworks and structural mechanisms remain essential in addressing dual use concerns, particularly given the complexity and ever-changing nature of research.

Ethical evaluations, especially in the context of disruptive and rapidly evolving technologies, face inherent challenges. Many emerging fields, such as artificial intelligence, synthetic biology, or quantum computing, develop at a pace that can outstrip existing regulatory or ethical frameworks. These technologies often carry unpredictable consequences, making it difficult to anticipate their potential dual use risks fully. In such cases, more careful and ongoing scrutiny is necessary to account for emerging risks that may not be immediately evident.

Additionally, the rapid shifts in the global political and security landscape further complicate the ethical evaluation of dual use technologies. Geopolitical tensions, emerging conflicts, and changing security priorities can dramatically alter the context in which technologies are developed and deployed. What may initially be seen as a benign research endeavor could quickly become sensitive or dangerous in a volatile political environment. This underscores the need for an adaptive and proactive approach, ensuring that dual use risks are continually reassessed in light of evolving global threats and political dynamics.

Given the fluid nature of scientific, technological, and political progress, this guide itself must be continuously updated. Without regular revisions, its relevance may diminish as new innovations, shifting security concerns, and unforeseen ethical dilemmas arise. Therefore, it is crucial to maintain a vigilant and adaptable approach to dual use issues, recognizing that no single framework can account for all eventualities.

In conclusion, while this guide offers valuable insights, it is not a definitive solution. It should be used in conjunction with broader ethical, legal, and institutional practices, with the recognition that a more holistic and dynamic engagement is required to address the evolving challenges of dual use research.

References

Bezuidenhout, L., and Rappert, B. (2012). The ethical issues of dual-use and the life sciences. CORE Issues in Professional and Research Ethics 1 (Paper 1).

Björnsson, G. (2011). Joint Responsibility Without Individual Control: Applying the Explanation Hypothesis. In: Vincent, N., van de Poel, I., and van den Hoven, J. (eds.), Moral Responsibility. Library of Ethics and Applied Philosophy, vol 27. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-1878-4_11

Brenneis, A. (2024). Assessing dual use risks in AI research: necessity, challenges and mitigation strategies. Research Ethics 0(0). https://doi.org/10.1177/17470161241267782

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Apollo – University of Cambridge Repository. https://doi.org/10.17863/CAM.22520

Butler, D. (2012). Mutant-flu researcher backs down on plan to publish without permission. Nature. https://doi.org/10.1038/nature.2012.10514

Carozza, I., Marsh, N., and Reichberg, G. (2022). Dual use AI Technology in China, the US and the EU. Strategic Implications for the Balance of Power. PRIO Paper. Oslo: PRIO. www.prio.org/publications/13150

Colussi, I.A. (2016). Mitigating the Nuclear 'Dual-Use Dilemma': Suggestions for the Enhancement of the Culture of Responsibility. In: Black-Branch, J., and Fleck, D. (eds.), Nuclear Non-Proliferation in International Law, Volume III. The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-138-8_5

Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (OJ L 338 23.09.2021, p. 1, ELI: http://data.europa.eu/eli/reco/2021/1700/oj)

Crowley, M., and Dando, M. (2022). Toxin and bioregulator weapons: Preventing the misuse of the chemical and life sciences. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-10164-9

Dalpé, G., Huerne, K., Dupras, C., Cheung, K., Palmour, N., Winkler, E., Alex, K., Mehlman, M., Holloway, J. W., Bunnik, E., König, H., Mansuy, I. M., Rots, M. G., Erwin, C., Erler, A., Libertini, E., and Joly, Y. (2023). Defusing the legal and ethical minefield of epigenetic applications in the military, defense, and security context. Journal of law and the biosciences 10(2), lsad034. https://doi.org/10.1093/jlb/lsad034

De Block, A., and Adriaens, P.R. (2013) Pathologizing sexual deviance: A history. Journal of Sex Research 50(3-4), 276–298.

DiEuliis, D., and Giordano, J. (2018). Gene editing using CRISPR/Cas9: implications for dual use and biosecurity. Protein & Cell 9(3), 239240. https://doi.org/10.1007/s13238-017-0493-4

Douglas, M. (1979). Cultural Bias. London. Royal Anthropological Institute, Occasional paper No. 35.

European Commission (2021). Communication from the Commission to the European Parliamant, the European Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan on synergies between civil, defence and space industries, COM(2021) 70 final. https://commission.europa.eu/document/download/2353ded9-0e39-4d35-a46c-67c62779afe1_en?filename=action_plan_on_synergies_en.pdf (accessed March 10, 2024).

Farinella, P., Anselmo, L., and Bertotti, B. (2000). Nuclear Power in Space: A Dual-use Conflict. In: Schroeer, D., and Elena, M. (eds.): Technology Transfer. London and New York: Routledge, 91–104.

Federal Office for Economic Affairs and Export Control (BAFA) (2023). Manual Export Control and Academia. https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.pdf?__blob=publicationFile&v=5 (accessed October 10, 2024).

Finocchio, P., Prasad, R., and Ruggieri, M. (eds.) (2008). Aerospace Technologies and Applications for Dual Use: A New World of Defense and Commercial in 21st Century Security. Aalborg: River Publishers.

Fischer, J. M., and Ravizza, M. (1998). Responsibility and Control: A Theory of Moral Responsibility. Cambridge: Cambridge University Press.

Floridi, L. (2023). On Good and Evil, the Mistaken Idea That Technology Is Ever Neutral, and the Importance of the Double-Charge Thesis. Philosophy & Technology 36, 60. https://doi.org/10.1007/s13347-023-00661-4

Forge, J. (2010). A Note on the Definition of “Dual Use”. Science and Engineering Ethics 16, 111–118. https://doi.org/10.1007/s11948-009-9159-9

Friedman, B., and Hendry, D. G. (2019). Value Sensitive Design. Shaping Technology with Moral Imagination. Cambridge, Mass.: MIT Press.

Hähnel, M. (2024). Conceptualizing Dual Use: A Multidimensional Approach. Research Ethics, https://doi.org/10.1177/17470161241261466

Haines, J. (2018). Risk and the libertarian case for redistribution. Ethical Perspectives 25(3): 497–516.

Hayenhjelm, M. (2018). Risk impositions, genuine losses, and reparability as a moral constraint. Ethical Perspectives 25(3): 419–446.

Heinrichs, J.-H., and Ergin Aslan, S. (2024). Agent regret and the moral responsibility for the misuse of research results. Research Ethics 0(0). https://doi.org/10.1177/17470161241272760

Herfst, S., Schrauwen, E. J., Linster, M., et al. (2012). Airborne transmission of influenza A/H5N1 virus between ferrets. Science 336(6088), 1534–1541

Hermann, E., and Hermann, G. (2022). Artificial intelligence in research and development for sustainability: the centrality of explicability and research data management. AI and Ethics 2, 29–33. https://doi.org/10.1007/s43681-021-00114-8

Herstein, O. (2019). Nobody's Perfect: Moral Responsibility in Negligence. Canadian Journal of Law and Jurisprudence 31(1): 109–125.

High-Level Expert Group on AI (2019). Ethics Guidelines for Trustworthy Artificial Intelligence. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (accessed October 15, 2024).

Hoffman, W., and Volpe, T.A. (2018). Internet of nuclear things: Managing the proliferation risks of 3-D printing technology. Bulletin of the Atomic Scientists 74(2), 102–113. https://doi.org/10.1080/00963402.2018.1436811

Horowitz, M. (2021). When speed kills: Lethal autonomous weapon systems, deterrence and stability. In: Sechser, T. (ed.), Emerging Technologies and International Stability. London: Routledge, 144–168.

Imai, M., Watanabe, T., Hatta, M., et al. (2012). Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. Nature 486, 420–428. https://doi.org/10.1038/nature10831

Imperiale, M. J., and Casadevall, A. (2018). A New Approach to Evaluating the Risk–Benefit Equation for Dual use and Gain-of-Function Research of Concern. Frontiers in Bioengineering and Biotechnology 6: 21. https://doi.org/10.3389/fbioe.2018.00021

Jahnel, J. (2015). Conceptual Questions and Challenges Associated with the Traditional Risk Assessment Paradigm for Nanomaterials. Nanoethics 9, 261–276. https://doi.org/10.1007/s11569-015-0235-0

Jore, S.H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. European Journal for Security Research 4, 157–174. https://doi.org/10.1007/s41125-017-0021-9

Kelle, A. (2012). Synthetic biology with standardized parts. In: Tucker, J.B. (ed.), Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies. Cambridge, Mass.: MIT Press, 147–159.

Kelle, A. (2013). Beyond patchwork precaution in the dual use governance of synthetic biology. Science and Engineering Ethics 19: 1121–1139. https://doi.org/10.1007/s11948-012-9365-8

Kermisch, C. (2012). Risk and Responsibility: A Complex and Evolving Relationship. Science and Engineering Ethics 18, 91–102. https://doi.org/10.1007/s11948-010-9246-y

Kirchschläger, P. G. (2021). Ethics of blockchain technology. In: Ulshöfer, G., Kirchschläger, P. G., and Huppenbauer, M. (ed.), Digitalisierung aus theologischer und ethischer Perspektive. Baden-Baden: Nomos, 185–210.

Koplin, J. (2023). Dual use implications of AI text generation. In: Ethics and Information Technology 25(2), 1–11. https://doi.org/10.1007/s10676-023-09703-z

Kropf, M. (2024). The ethically significant difference between dual use and slippery slope arguments, in relation to CRISPR-Cas9: philosophical considerations and ethical challenges. Research Ethics 0(0). https://doi.org/10.1177/17470161241240587

Kuhlau, F., Höglund, A. T., Evers, K., and Eriksson, S. (2011). A precautionary principle for dual use research in the life sciences. Bioethics 25(1), 1–8. https://doi.org/10.1111/j.1467-8519.2009.01740.x

Lev, O., and Keren, A. (2024). Addressing the risks of dual use research: who is responsible? Research Ethics 0(0). https://doi.org/10.1177/17470161241268685

Marris, C., Jefferson, C., and Lentzos, F. (2014). Negotiating the dynamics of uncomfortable knowledge: The case of dual use and synthetic biology. BioSocieties 9, 393–420. https://doi.org/10.1057/biosoc.2014.32

Menges, L. (2020). Responsibility and appropriate blame: The no difference view. European Journal of Philosophy 29(2), 1–17. https://doi.org/10.1111/ejop.12571

Meunier, F. X., and Bellais, R. (2018). Technical systems and cross-sector knowledge diffusion: an illustration with drones. Technology Analysis & Strategic Management 31(4), 433–446. https://doi.org/10.1080/09537325.2018.1518522

Miller, S. (2018). Dual Use Science and Technology, Ethics and Weapons of Mass Destruction. SpringerBriefs in Ethics. Cham: Springer. https://doi.org/10.1007/978-3-319-92606-3

Miller, S., and Selgelid, M. J. (2007). Ethical and philosophical consideration of the dual use dilemma in the biological sciences. Science and Engineering Ethics 13(4), 523–580. https://doi.org/10.1007/s11948-007-9043-4

Miller, S., and Selgelid, M. J. (2008). Ethical and Philosophical Consideration of the Dual use Dilemma in the Biological Sciences. Dordrecht: Springer. https://doi.org/10.1007/978-1-4020-8312-9

Miller, S., and Taebi, B. (2018). Nuclear Industry. In: Miller, S. (ed.), Dual Use Science and Technology, Ethics and Weapons of Mass Destruction (SpringerBriefs in Ethics). Cham: Springer, 73–90 https://doi.org/10.1007/978-3-319-92606-3_6

Mir, T. U. G., Wani, A. K., Akhtar, N., and Shukla, S. (2022). CRISPR/Cas9: Regulations and challenges for law enforcement to combat its dual-use. Forensic science international 334, 111274. https://doi.org/10.1016/j.forsciint.2022.111274

National Science Advisory Board for Biosecurity (NSABB) (2007). Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information. A Report of the National Science Advisory Board for Biosecurity (NSABB). https://biosecuritycentral.org/static/a222b882183ec4317ef06c234b21758e/Proposed-Oversight-Framework-for-Dual use-Research.pdf (accessed March 10, 2024).

Nationale Akademie der Wissenschaften Leopoldina (Leopoldina) and Deutsche Forschungsgemeinschaft (DFG) (2022). Wissenschaftsfreiheit und Wissenschaftsverantwortung: Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung / Scientific Freedom and Scientific Responsibility: Recommendations for Handling of Security-Relevant Research, second edition, Halle (Saale). https://www.leopoldina.org/fileadmin/redaktion/Publikationen/Nationale_Empfehlungen/2022_DFG-Leopoldina_Empfehlungen_Wissenschaftsfreiheit_web.pdf (accessed March 10, 2024).

Nationale Akademie der Wissenschaften Leopoldina (Leopoldina) and Deutsche Forschungsgemeinschaft (DFG) (2024). Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung. Tätigkeits- und Sachstandsbericht November 2024, Berlin.

Nihlén Fahlquist, J. (2021). The moral responsibility of governments and individuals in the context of the coronavirus pandemic. Scandinavian journal of public health 49(7), 815–820. https://doi.org/10.1177/1403494821990250

Oltmann, S. (2015). Dual Use Research: Investigation Across Multiple Science Disciplines. Science and Engineering Ethics 21, 327–341. https://doi.org/10.1007/s11948-014-9535-y

Panina, L.V., Thakur, A., and Thakur, P. (2023). Nano/Mesoporous Materials as State-of-the-Art Military Applications. In: Suhag, D., Thakur, A., and Thakur, P. (eds.), Integrated Nanomaterials and their Applications. Singapore: Springer. https://doi.org/10.1007/978-981-99-6105-4_19

Pražák, J. (2021). Dual use conundrum: Towards the weaponization of outer space? In: Acta Astronautica 187, 397–405. https://doi.org/10.1016/j.actaastro.2020.12.051

Rath, J., Ischi, M., and Perkins, D. (2014). Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. Science and engineering ethics 20(3), 769–790. https://doi.org/10.1007/s11948-014-9519-y

Rayner, S. (1992). Cultural theory and risk analysis. In: Krimsky, S., and Golding, D. (eds.), Social theories of risk. Westport: Praeger, 1992, 83–115.

Resnik, D. B. (2009). What is "dual use" research? A response to Miller and Selgelid. Science and engineering ethics 15(1), 3–5. https://doi.org/10.1007/s11948-008-9104-3

Riebe, T. (2023). Technology assessment of dual use ICTs: How to assess diffusion, governance and design. Springer Nature. https://doi.org/10.1007/978-3-658-41667-6

Riebe, T., and Reuter, C. (2019). Dual use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In: Reuter, C. (ed.), Information Technology for Peace and Security. Wiesbaden: Springer Vieweg, 165–183. https://doi.org/10.1007/978-3-658-25652-4_8

Robert Koch Institut (RKI) (2013). Dual use potential of life sciences research. Code of conduct for risk assessment and risk mitigation. https://www.rki.de/EN/Content/infections/Dual_Use/code_of_conduct.html (accessed March 10, 2024).

Rudra, P., und Lenk, C. (2021). Process of risk assessment by research ethics committees: foundations, shortcomings and open questions. Journal of Medical Ethics (47), 343–349. Advance online publication. https://doi.org/10.1136/medethics-2019-105595

Selgelid, M. J. (2009). Dual use Research Codes of Conduct: Lessons from the Life Sciences. NanoEthics 3(3), 175–183. https://doi.org/10.1007/s11569-009-0074-y

Shamoo, A. E., and Resnik, D. B. (2009). Responsible Conduct of Research. Oxford and New York: Oxford University Press.

Sharkey, A., and Sharkey, N. (2012). Granny and the robots: ethical issues in robot care for the elderly. Ethics and Information Technology 14, 27–40. https://doi.org/10.1007/s10676-010-9234-6

Shoemaker, D. (2017). Response-Dependent Responsibility; or, A Funny Thing Happened on the Way to Blame. The Philosophical Review, 126(4), 481–527. https://www.jstor.org/stable/27130954

Shoemaker, D. (ed.) (2015). Oxford Studies in Agency and Responsibility: Volume 3. Oxford: Oxford University Press.

Small C., and Lew C. (2021). Mindfulness, Moral Reasoning and Responsibility: Towards Virtue in Ethical Decision-Making. Journal of Business Ethics 169(1), 103–117. https://doi.org/10.1007/s10551-019-04272-y

Smith, M., and Miller, S. (2021). Biometric Identification, Law and Ethics (SpringerBriefs in Ethics). Cham: Springer. https://doi.org/10.1007/978-3-030-90256-8

Spielthenner, G. (2012). Risk-benefit analysis: from a logical point of view. Journal of bioethical inquiry 9(2), 161–170. https://doi.org/10.1007/s11673-012-9366-y

Steigleder, K. (2018). On the Criteria of the Rightful Imposition of Otherwise Impermissible Risks. Ethical perspectives 25(3), 471–495. doi:10.2143/EP.25.3.3285426

Strawson, P. (1962). Freedom and Resentment. Proceedings of the British Academy 48, 187–211.

Taddeo, M., and Blanchard, A. (2022). Accepting Moral Responsibility for the Actions of Autonomous Weapons Systems—a Moral Gambit. Philosophy & Technology 35, 78. https://doi.org/10.1007/s13347-022-00571-x

Tucker, J.B. (2012). Innovation, Dual Use, and Security. Managing the Risks of Emerging Biological and Chemical Technologies. Cambridge, Mass.: MIT Press.

Urbina, F., Lentzos, F., Invernizzi, C., and Ekins, J. (2022). Dual use of artificial-intelligence-powered drug discovery. Nature Machine Intelligence 4, 189–191. https://doi.org/10.1038/s42256-022-00465-9

U.S. Congress, Office of Technology Assessment (1993). Defense Conversion: Redirecting R&D, OTA-ITE-552. Washington, DC: U.S. Government Printing Office, May. https://ota.fas.org/reports/9318.pdf (accessed March 09, 2024).

Vargas, M. (2013). Building better beings: A theory of moral responsibility. Oxford: Oxford University Press.

Verlaeckt, K. (ed.) (2022). Guidelines for Researchers on Dual Use and Misuse of Research. Flemish Interuniversity Council. Available from https://vlir.be/wp-content/uploads/2022/10/VLIR-Dual use-2022-EN.pdf (accessed March 09, 2024).

Volpe, T.A. (2019). Dual use distinguishability: How 3D-printing shapes the security dilemma for nuclear programs. Journal of Strategic Studies 42(6), 814–840. https://doi.org/10.1080/01402390.2019.1627210

Werner, M.H. (2002). Verantwortung. In: Düwell, M., Hübenthal, C., and Werner, M.H. (eds.), Handbuch Ethik. Stuttgart and Weimar: Metzler, 521–527.

Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. In: Technology Innovation Management Review 9 (11), 39–52.

Weydner-Volkmann, S., and Cassing, K. (2023). Forschende in der Angriffsrolle: Zum besonderen forschungsethischen Bedarf in der IT-Sicherheit. Zeitschrift für Praktische Philosophie 10(1). https://doi.org/10.22613/zfpp/10.1.3

Whitman, J. (2013). Nanotechnology and Dual-Use Dilemmas. In: Rappert, B., and Selgelid, M.J. (eds.), On the Dual Uses of Science and Ethics. Canberra: ANU E Press, 13–28.

World Health Organization (WHO) (2021). Emerging technologies and dual-use concerns: a horizon scan for global public health. World Health Organization. https://iris.who.int/handle/10665/346862 (accessed March 09, 2024).

World Health Organization (WHO) (2022). Global guidance framework for the responsible use of the life sciences: mitigating biorisks and governing dual use research, Geneva, World Health Organization. https://iris.who.int/bitstream/handle/10665/362313/9789240056107-eng.pdf?sequence=1 (accessed March 10, 2024).

Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI) (2022). Zur forschungsethischen Begutachtung von KI-Forschungsprojekten: Handreichung zur Unterstützung der Arbeit von Ethikkommissionen an Hochschulen. Darmstadt. https://zevedi.de/wp-content/uploads/2022/11/ZEVEDI_Handreichung-KI-Forschungsethik_2022.pdf (accessed March 10, 2024).

Jül-4449 • März 2025
ISSN 0944-2952

Mitglied der Helmholtz-Gemeinschaft

JÜLICH
Forschungszentrum