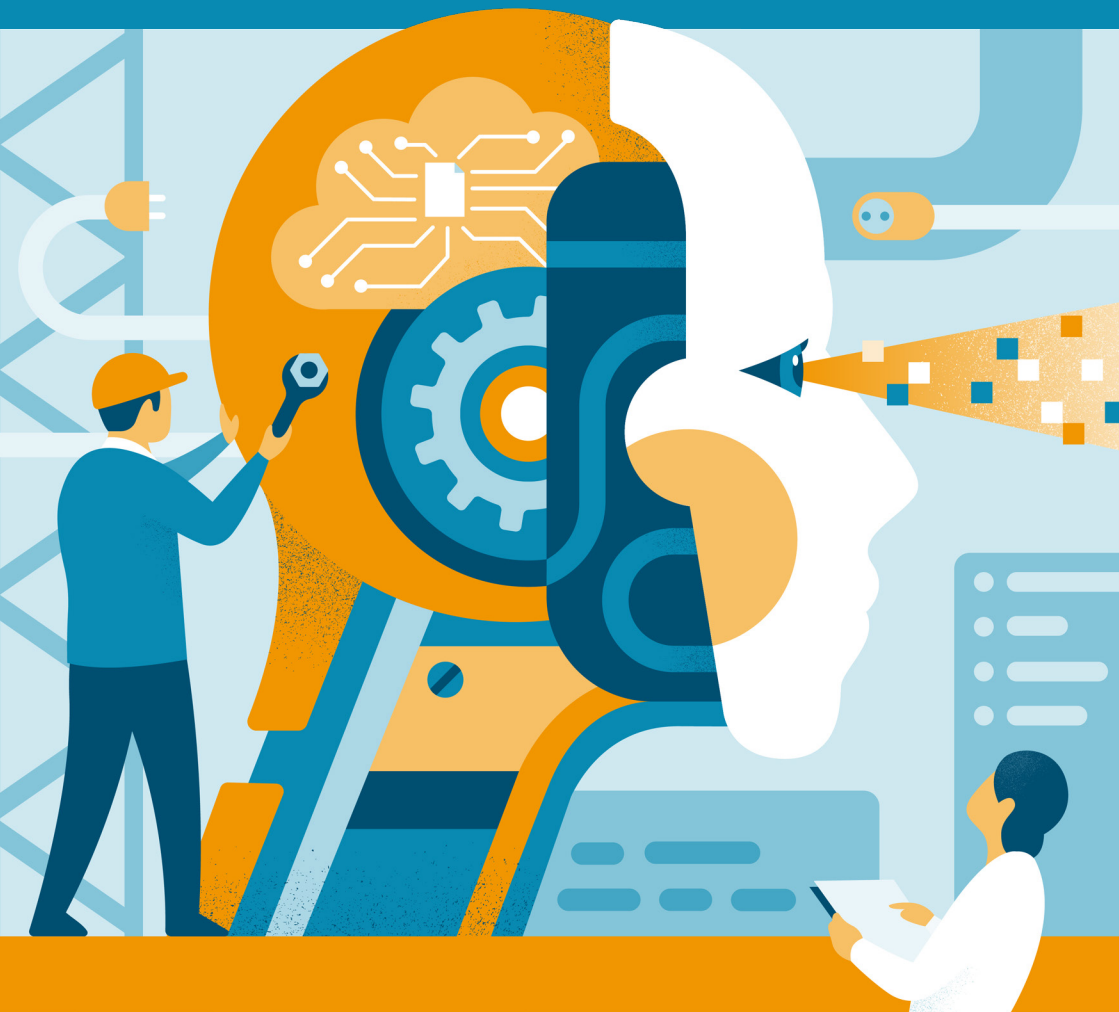
GEMEINSAMER AUSSCHUSS
ZUM UMGANG MIT
SICHERHEITSRELEVANTER
FORSCHUNG

The Handling of Security-Relevant Research in Germany — An Overview



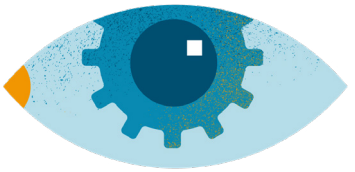
Should research be used to...

... develop autonomous vehicles that could potentially be misused as weapons?

... develop methods for making communication secure and, at the same time, no longer able to be monitored?

... conduct experiments during which viruses are made more dangerous?

... develop artificial intelligence that can identify us, predict our behaviour and make decisions independently?



What is security-relevant research?

Research freedom as protected by the German constitution gives researchers the right to address scientific questions independently and to discuss their work freely among themselves.

Research freedom is fundamental to expanding human knowledge and ensuring social progress and prosperity. However, useful research findings and research methods can also be misused, for example for harmful military, political or criminal purposes. One example that illustrates this "dual-use dilemma" in research is the discovery of nuclear fission, which ultimately led to the development and use of nuclear weapons.

International debates on the benefits and potential risks (including the risk of misuse) of research and on the particular responsibilities of researchers currently focus on a wide range of areas, including research projects that make viruses more dangerous, research into algorithms that independently uncover security vulnerabilities in operating systems, the development of autonomous machines, the advancement of assistance systems for persons with physical disabilities that retrieve information directly from the brain or behavioural and social sciences research into the recruitment and radicalisation of terrorists.

In principal, security-relevant research is conducted in virtually all disciplines.

Based on the common understanding of *dual-use research of concern*, the Joint Committee of the DFG and the Leopoldina defines *security-relevant research projects of concern* as projects that have the potential to produce knowledge, products or technologies that could be misused directly by third parties and carry significant risks for the security of human dignity, life, health, freedom, property, the environment or peaceful coexistence.

When it comes to security-relevant research projects of concern in particular, the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) and the German National Academy of Sciences Leopoldina believe that action is needed to ensure that the benefits and potential risks are weighed up at any early stage in an interdisciplinary manner and that local committees for ethics in security-relevant research (KEFs – German acronym) are on hand to provide advice and conduct assessments. To enable such risks to be identified in good time, it is firstly important for awareness to be raised among researchers and within research institutions.

As a consequence of this advisory process, it is conceivable that projects could be replaced by less risky strategies, that publications could be amended or, as a last resort, that projects could be stopped or their results left unpublished. However, the failure to conduct or publish certain research can also be problematic from an ethical perspective if, for example, this hinders the development of treatments, vaccines or other protective measures or prevents important innovations that would contribute to the common good, for example by creating jobs or protecting the environment and the climate.

The Joint Committee on the Handling of Security-Relevant Research

The Joint Committee is a scientific advisory committee that keeps track of developments concerning security-relevant research, identifies areas where action is needed and advises the DFG and the Leopoldina accordingly.

It actively supports German research institutions with the implementation of the joint recommendations for handling security-relevant research[1] issued by the DFG and the Leopoldina, in particular by supporting KEFs to act as points of contact and by assisting with the sharing of experience.

The Joint Committee also helps to ensure that attention is paid to security-relevant aspects of research in the long term by organising regular events on the topic and forums for KEFs to share knowledge and by participating in relevant national and international discussions.

The Joint Committee's members comprise researchers from a range of disciplines as well as representatives appointed from the presidiums of the DFG and the Leopoldina. At least one member must be an expert on ethical issues and one on legal issues.

1 Available at www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/11/2022_Empfehlungen_Wissenschaftsfreiheit_Wissenschaftsverantwortung.pdf

Progress reports on the work of the Joint Committee, KEFs and the state of the discussions as well as the framework conditions for security-relevant research

▶ www.sicherheitsrelevante-forschung.org/en/tag/progress-reports

Model statutes for KEFs

▶ www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/11/2016_Modelstatutes-1.pdf

Events and KEF forums on the topic organised by the Joint Committee

▶ www.sicherheitsrelevante-forschung.org/en/events

Overview of the contact persons and committees responsible for ethics in security-relevant research

▶ www.sicherheitsrelevante-forschung.org/en/contactpersons

Slides and good practice examples for incorporating the topic into education and teaching

▶ www.sicherheitsrelevante-forschung.org/en/education-and-teaching

Information on selected security-relevant research topics and case studies

▶ www.sicherheitsrelevante-forschung.org/en/case-studies

Legal framework and funding of security-relevant research

▶ www.sicherheitsrelevante-forschung.org/en/legal-funding

Further publications by the DFG and the Leopoldina on the topic

▶ www.sicherheitsrelevante-forschung.org/en/thema/publications/internal

Members of the Joint Committee

▶ www.sicherheitsrelevante-forschung.org/en/board-members

Committees for ethics in security-relevant research (KEFs)

Around 100 German research institutions, research associations and professional societies have followed the recommendations of the DFG and the Leopoldina by establishing interdisciplinary committees that are available as and when required to advise researchers and provide recommendations on matters relating to security-relevant research projects. These committees also raise awareness of security-relevant aspects of research by organising events and providing information material. Examples include:

- **Committees for ethics in security-relevant research established primarily to deal with these matters** (e.g. the Committee for the Ethical Evaluation of Security-Relevant Research at the University of Greifswald and the Institutional Biorisk Committee at the Friedrich-Loeffler-Institut)
- **Long-standing committees** (e.g. clinical ethics committees or research committees) that also take on the role of a KEF (e.g. the Ethics Committee at the University of Mannheim)
- **Ad hoc committees that are only convened as and when required** (e.g. the Senate Board for Research and Young Academics at TU Dresden)
- **Commissioners responsible for ethics in security-relevant research** (e.g. at the Leibniz-Institute German Collection of Microorganisms and Cell Cultures)
- **KEFs jointly run by different institutions or research associations** (e.g. the KEF established by the Bernhard Nocht Institute, the Leibniz Institute of Virology and the Research Center Borstel or the Leibniz committee for ethics in research)

What can KEFs do for researchers and research institutions?

Create transparency and increase public trust in the freedom of scientific research

Assess the ethics of security-relevant research projects as a potential prerequisite for funding

Give researchers peace of mind by legitimising risky research projects

Raise awareness among researchers and provide them with support on ethical matters

Take additional disciplines into account when weighing up risks, such as disciplines in the fields of ethics, law and the humanities

Strengthen the independent handling of security-relevant research

Key questions for the ethical assessment of security-relevant research

1. Key questions for researchers indicating that they need to consult a KEF

1.1 Is it likely that your research project is security-relevant research according to the before-specified meaning and/or the before-mentioned contexts?

1.2 Is it possible that cooperation partners involved in your research project will cause security-relevant risks in the before-mentioned meaning?

1.3 Does the research project conflict with legal regulations[2] and thus need to be referred to compliance office alongside a KEF?

2. Key questions for processing the query by the KEF

2.1 What concrete objectives and purposes are the researchers and any sponsors involved pursuing with this research project?

2.2 Is the required expertise available to make an informed assessment of the research project in regard to its potential risks or does additional expertise need to be brought in?

2.3 Is it possible to adequately specify and weigh up the benefits and risks of the known and potential research findings with the information currently available?

2.4 Are the security-relevant outcomes and resulting risks of the research project new or could they also arise from previously published work?

2.5 How likely is it that the security-relevant findings will be disseminated and that this will lead to a direct[3] concrete misuse in the before-specified meaning of security-relevant research of concern?

2.6 In the event of an intentional harmful application of the findings through third parties, what would be the scale of the potential damage and are any suitable countermeasures[4] available?

2.7 What are the potential harmful consequences[5] of not carrying out the research project?

3. Key questions for the conclusive assessment and consultation by the KEF

3.1 Can the research project produce knowledge, products or technologies that could very likely be misused directly by third parties to cause significant damage of the before-specified legal interests?

3.2 Should the project be reassessed by the KEF at a more advanced stage when the security-relevant risks can be judged more easily?

3.3 Is the research project and its objectives and purposes compatible with the constitutional principles and the basic code or guidelines of the research institution?

3.4 Can the security-relevant risks be sufficiently reduced by imposing certain conditions on the project (e.g. usage agreement or alternative research strategy) or by adapting the publication?

3.5 How can the researchers involved in the research project be made aware of the ethical aspects of security-relevant research so that they consider the direct and future consequences of their work?

2 E.g. regular criminal law, export control legislation and export provisions of the German Federal Office of Economics and Export Control (BAFA), the Biological Weapons Convention and the Chemical Weapons Convention, the protection of human rights, humanitarian international law, rules of war, prohibition of torture and violence, Biodiversity Convention.

3 To be considered here are e.g. the necessary capabilities, specialist knowledge and technical equipment for misuse.

4 E.g. measures of recovery and traceability and damage limitation.

5 Can the absence of certain innovations result in additional damage, for example, in the course of ongoing military conflicts, in the course of climate change, in naturally emerging waves of infection?

The legal framework and research funding

In Germany, security-relevant research is subject to a series of legal regulations. These include:

- regular criminal law
- the German Biological Agents Ordinance (Biostoffverordnung)
- the German Genetic Engineering Act (Gentechnikgesetz)
- the German Infectious Diseases Protection Act (Infektionsschutz-gesetz)
- the German War Weapons Control Act (Kriegswaffenkontrollgesetz)
- the export regulations of the German Federal Office for Economic Affairs and Export Control (BAFA)

The relevant international laws include:

- the EU regulation on the control of exports of dual-use items and technology
- the Biological Weapons Convention
- the Chemical Weapons Convention
- the Treaty on the Prohibition of Nuclear Weapons

The EU's Framework Programme for Research and Innovation (Horizon Europe) requires funding proposals to include an ethics self-assessment of the risks of misuse; ethics approvals are required for some funding proposals and the guidelines also recommend establishing advisory boards for dealing with ethical issues.

The German Research Foundation (DFG) asks funding applicants to assess their projects for security-relevant risks and, if necessary, to submit statements on the risk-benefit ratio and possible measures to minimise such risks. If applicants have questions about security-relevant aspects or risk assessments, the DFG advises that they seek advice from ethics committees like KEFs. Guideline 10 in the DFG's Guidelines for Safeguarding Good Research Practice also states the following:

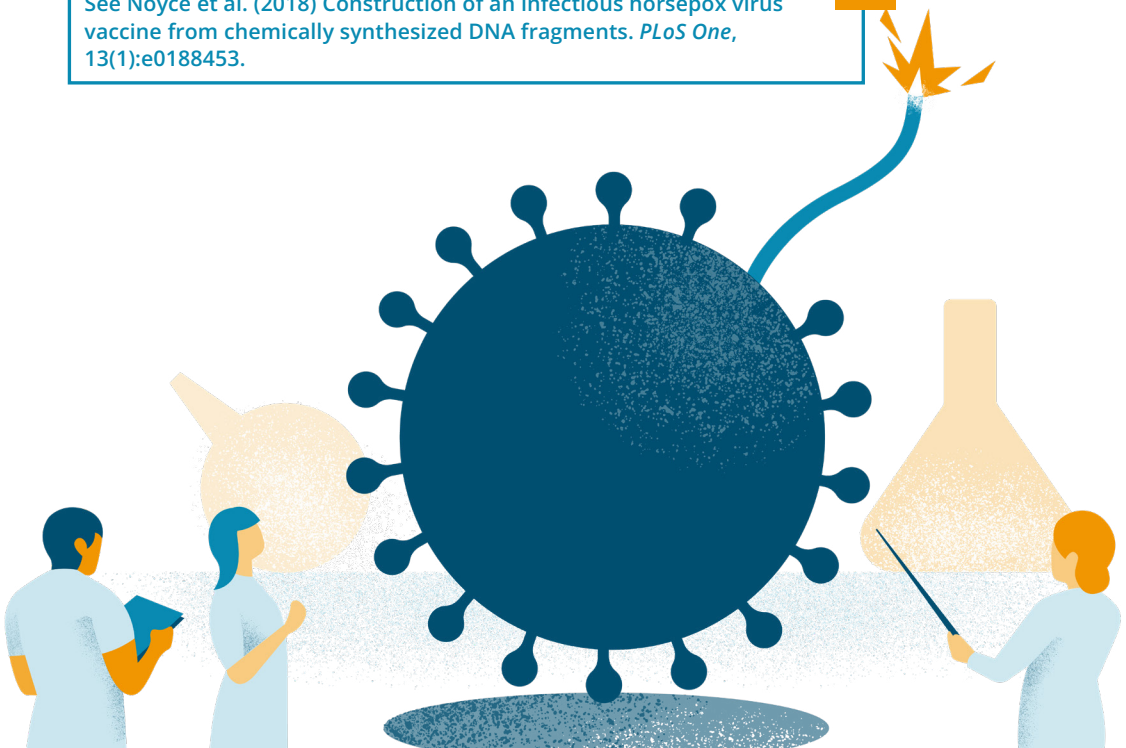
> **"Researchers adopt a responsible approach to the constitutionally guaranteed freedom of research. They comply with rights and obligations, particularly those arising from legal requirements and contracts with third parties, and where necessary seek approvals and ethics statements and present these when required. With regard to research projects, the potential consequences of the research should be evaluated in detail and the ethical aspects should be assessed [...]. They pay particular attention to the aspects associated with security-relevant research (dual use). HEIs [higher education institutions] and non-HEI research institutions are responsible for ensuring that their members' and employees' actions comply with regulations and promote this through suitable organisational structures [...]."**

Case studies providing examples of security-relevant research

Could the production of synthetic, infectious smallpox viruses be an instruction manual for constructing biological weapons?

A research group intends to produce infectious horsepox viruses by introducing a synthetically constructed horsepox genome into cells infected with an innocuous rabbit virus. The innovative value of this project is primarily the realisation of a complex technical process of synthesis, as the theoretical feasibility of this kind of experiment has long been accepted. The researchers argue that new vaccines could then be developed using this procedure. The main risk of the project is that the technology can be used for the production of human pathogenic smallpox viruses. As the smallpox virus has been eradicated since the 1980s and good vaccines have long been developed, the viability of the researchers' argumentation is questionable.
On the other hand, as the project requires an extremely high level of expertise and technology, the experiment cannot be readily copied.

See Noyce et al. (2018) Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. *PLoS One*, 13(1):e0188453.



Could research into radicalisation methods help terrorist groups with recruitment?

The study investigates the link between the consumption of extremist (Islamist) material online by adolescents and how this is associated with radicalisation. Earlier research projects have already demonstrated how the internet plays a significant role in the distribution of radicalising material. This study takes this a step further by exploring which character traits make individuals especially susceptible to being radicalised and which channels and media are particularly effective. Although beheading videos are found to be the material consumed the most by adolescents, they have a low potential to cause radicalisation. In contrast, the results show that online magazines published by the so-called Islamic State and Al-Qaeda are only searched for by a small group of people but have the greatest cognitive effect.
The research findings are intended to help identify deradicalisation strategies. At the same time, extremist and terrorist groups could use the results to develop more effective methods of recruitment.

See Frissen (2021) Internet, the great radicalizer? Exploring relationships between seeking for online extremist materials and cognitive radicalization in young adults. *Computers in Human Behavior*, 114, 106549.

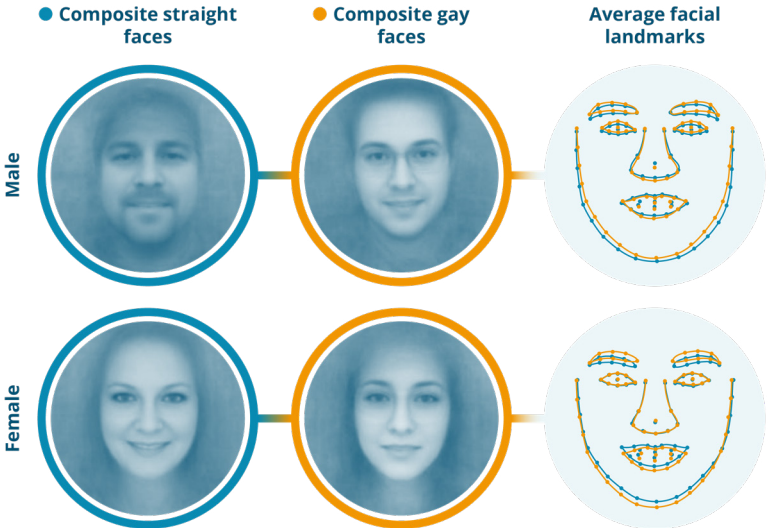
Could the advancement of brain-computer interfaces lead to passwords being extracted?

The aim of the research project is to use an electroencephalogram to investigate and extract information from regions of the brain that are responsible for motor commands as well as the retention and retrieval of numbers, images and locations. This technology could be used to help persons with physical disabilities to interact more effectively with machines, to perform banking transactions without having to input information manually or to communicate with others. The reliability of the extracted data continued to improve as the experiments progressed. However, this technology could also be used to extract sensitive information, such as passwords and bank details, without the user's knowledge by means of seemingly harmless stimuli.

See Martinovic et al. (2012) On the feasibility of side-channel attacks with brain-computer interfaces. In 21st {USENIX} Security Symposium ({USENIX} Security 12) (pp. 143-158).

Could the detection of the sexual orientation of humans from facial images using deep learning algorithms be a tool for illegal invasions of privacy?

This research project wants to further develop a deep learning algorithm to identify patterns in facial images. The project plans to train the algorithm using photos of open homosexuals and heterosexuals so that it can analyse other portrait photos to predict sexual orientation. The benefit of the project according to researchers is to find out how deep learning algorithms connect data and what reference points it selects to make predictions. Purported additional benefits are furthering our understanding of the physiological origin of human sexual orientation and the limits of human perception. The risk of malicious application lies in the possible illegal acquisition of sensitive personal data using the biometrics of individuals, for example in countries in which homosexuality is criminalised. Highly developed deep learning algorithms of this kind could also be used to group people according to their consumer or voting behaviour or their criminal history.



See Wang and Kosinski (2018) Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of personality and social psychology*, 114(2), 246.

Education and teaching

To raise awareness of security-relevant aspects of research at an early stage, universities and other higher education institutions should, wherever possible, incorporate the topic into their teaching and into the curricula of all relevant degree courses and make it part of their researchers' everyday work. This can be achieved using a three-stage process:

1. **Bachelor's degree courses** should cover interdisciplinary security-relevant aspects of research in general lectures on "good research practice" and basic issues of ethics in science.

2. **Master's degree courses** should then include seminars on the specific ethical and security-relevant aspects of the subject being studied, both on a theoretical level and using case studies.

3. **Doctoral students**, in particular, as well as **postdocs** and other staff involved in research should additionally be instructed on the specific risks of their research in group seminars, further training courses, summer schools or graduate schools.

Examples of courses on security-relevant research

Technical University of Munich, "Ethics for Nerds" seminar organised by the Department of Informatics in the 2019/20 winter semester

The aim of the seminar was to encourage students to think about the consequences of their (future) research for individuals and society by examining matters from an ethical perspective. Several topic areas were explored and used to shed light on different socio-political fields significantly affected by information technology.

Hamburg University of Technology "Ethics and Science" seminar in the 2020 summer semester

The seminar presented examples of ethical problems in natural sciences and engineering, including in the fields of medicine, life sciences and physics. It covered topics such as organ donation, the future of energy consumption and dual-use research in biology. The participants had the opportunity to discuss their own areas of interest and problems as well as the careers of famous scientists so that they could identify examples of ethical and non-ethical conduct.

University of Tübingen, "Ethics in the Life Sciences" seminar in the 2021/22 winter semester

The seminar used examples to address key ethical topics, theory and the history of the life sciences. It examined cross-cutting issues, such as research ethics, the risks associated with research and potential areas of misuse within the life sciences. The students had the chance to discuss a range of topics with different teaching staff.

Deutsche Forschungsgemeinschaft

Leopoldina
Nationale Akademie
der Wissenschaften

Office of the Joint Committee on the Handling of Security-Relevant Research:
Dr Johannes Fritsch, Head of Office
Dr Anita Krätzner-Ebert, Scientific Officer
Lena Diekmann, Project Coordinator

Contact:
Mail: gemeinsamer-ausschuss@leopoldina.org
Postal address: Reinhardtstr. 14, 10117 Berlin
Tel.: +49 160 9121 2676
Website: www.security-relevant-research.org

Contact at the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation):
Dr Ingrid Ohlert
Dr Christian Bamann
Mail: dual-use@dfg.de

IN COOPERATION WITH

MAX PLANCK GESELLSCHAFT

Fraunhofer

HELMHOLTZ

Leibniz Gemeinschaft

Design: Studio Grau, 2022