FAQ: SICHERHEITSRELEVANTE FORSCHUNG

Leitfaden zu Themenfeldern, Fördermechanismen und Akteuren für Universitäten

cyberagentur

VDI Technologiezentrum

GERMAN U15

Impressum

Herausgeber

German U15 e.V.
Markgrafenstr. 57
10117 Berlin

Agentur für Innovation in der Cybersicherheit GmbH
Große Steinstraße 19
06108 Halle (Saale)

VDI Technologiezentrum GmbH
VDI-Platz 1
40468 Düsseldorf

Inhaltliche Verantwortung und Redaktion
Yannick Bauer (German U15)
Peter Paulitsch (Cyberagentur)
Linus Piesch (VDI Technologiezentrum)
Dr. Christine Prokopf (VDI Technologiezentrum)
Dr. Friederike Schröder (German U15)

Kontakt
geschaeftsstelle@german-u15.de

Titelbild
Unsplash/Hiroyuki Sen

August 2026

© 2026 German U15 e. V., Agentur für Innovation in der Cybersicherheit GmbH und VDI Technologiezentrum GmbH

Die Erstellung und Nutzung der FAQ stehen in keinem Zusammenhang mit der Vergabe von Fördermitteln oder öffentlichen Aufträgen, deren Möglichkeiten oder den entsprechenden (Vergabe-) Verfahren. Die Zusammenarbeit im Rahmen dieser FAQ hat keinen Einfluss auf die Fördermittelvergabe, Auftragsvergabe oder das Vergabeverfahren durch die Agentur für Innovation in der Cybersicherheit GmbH oder die VDI Technologiezentrum GmbH. Es ergeben sich daraus keine Vorteile oder Begünstigungen für die Kooperationspartner, deren Mitglieder oder mit ihnen verbundene Personen.

Inhalt

1. Einordnung 4
2. Akteure und Strukturen 5
3. Themen, Bedarfe und strategische Orientierung 7
4. Zugang zu Förderung und Projekten 9
5. Vorbereitung auf Projekte 11
6. Sicherheits- und Geheimschutzanforderungen in Projekten 13
7. EU-spezifische Sicherheitsprozesse 17
8. Ergebnisse, Intellectual Property und Publikationen 19

Worum geht es?

Die folgenden *Frequently Asked Questions* (FAQ) und Antworten darauf sind in einer Kooperation der German U15 mit der Agentur für Innovation in der Cybersicherheit (Cyberagentur) und dem Projektträger VDI Technologiezentrum GmbH (als Nationale Kontaktstelle für den Europäischen Verteidigungsfonds (EVF) sowie als Nationale Kontaktstelle Sicherheitsforschung) entstanden. Ausgangspunkt waren aus Sicht von German U15 drängende Fragen aus Hochschulleitungen und Hochschulforschung. Die in den Bereichen Sicherheit und Verteidigung einschlägigen Projektträger Cyberagentur und VDI Technologiezentrum haben hierzu konkrete Antworten formuliert. Die FAQ bieten eine strukturierte Orientierung für Universitäten, die sich mit dem Feld der sicherheitsrelevanten Forschung auseinandersetzen. Sie stellen keine Positionierung der Universitäten hinsichtlich dieses Forschungsbereichs dar.

Von Themenfeldern bis zu Fördermechanismen, Sicherheitsanforderungen bis zu Fragen des geistigen Eigentums (*Intellectual Property/IP*) – der Leitfaden bündelt zentrale Fragen und leistet einen Beitrag, häufige Fragestellungen systematisch in Diskussionen und Entscheidungsprozesse einzubringen und eine fundierte Orientierung im Vorfeld potenzieller Antragstellungen zu ermöglichen. Er richtet sichdabei sowohl an Hochschulleitungen als auch an Forschungsabteilungen und Wissenschaftlerinnen und Wissenschaftler, die sich mit entsprechenden Fragestellungen befassen oder eine vertiefte Auseinandersetzung planen.

Die hier vorliegenden FAQ verstehen wir als wachsendes Dokument, das im weiteren Verlauf durch ergänzende Fragen und Themen erweitert werden kann. Wenn Ihnen Fragen fehlen oder Sie Anmerkungen und Anregungen zu bestimmten Themen haben, nehmen wir diese gerne auf.

Diese FAQ bieten eine erste Orientierung und erheben keinen Anspruch auf Vollständigkeit oder rechtliche Verbindlichkeit. Insbesondere die Ausführungen zu Geheimschutz, Sicherheitsüberprüfungen, Exportkontrolle und projektspezifischen Sicherheitsanforderungen können eine Prüfung des Einzelfalls nicht ersetzen. Maßgeblich sind stets die einschlägigen gesetzlichen Vorgaben, Verwaltungsvorschriften, Förderbedingungen, Vertragsregelungen sowie die Anforderungen der jeweils zuständigen Behörden oder Auftraggeber. Universitäten sollten daher bei konkreten Vorhaben frühzeitig die zuständigen internen Stellen und gegebenenfalls externe Beratungs- oder Behördenkontakte einbeziehen.

1. EINORDNUNG

Was ist sicherheitsrelevante Forschung?

Sicherheitsrelevante Forschung umfasst – einen weiten Sicherheitsbegriff annehmend – nicht nur militärische bzw. Verteidigungsforschung, sondern alle Forschung, die *„zur Aufrechterhaltung der inneren und äußeren Sicherheit sowie zum Aufbau der Resilienz und Erhaltung der natürlichen Lebensgrundlagen des Gemeinwesens beiträgt und beitragen soll oder diese gefährden kann“* (Definition des Wissenschaftsrats, 2025).

Für einen breiten Einblick in die Vielfalt sicherheitsrelevanter Technologien kann die Liste der Güter mit doppeltem Verwendungszweck gemäß der einschlägigen EU Verordnung herangezogen werden.

In welchen Themenfeldern und Technologiebereichen bestehen relevante Schnittstellen zwischen ziviler und militärischer Forschung?

Grundsätzlich können alle Technologien und Forschungsbereiche relevant sein, die auch für sicherheits- und verteidigungsbezogene Anwendungen eine Rolle spielen. Dies kann von Bereichen wie Radartechnologie, Kryptologie oder Luft- und Raumfahrtingenieurswissenschaften bis hin zur Notfallmedizin (Zivilschutz), Klima- und Nachhaltigkeitsforschung (Bevölkerungsschutz) reichen.

Schnittstellen können sowohl technologischer Natur sein (bspw. in den Bereichen Cybersicherheit, Künstliche Intelligenz, Sensorik oder autonome Systeme) als auch sozial- und geisteswissenschaftliche Fragestellungen betreffen, etwa im Hinblick auf zivil-militärische Zusammenarbeit, Resilienz oder ethische und rechtliche Aspekte neuer Technologien.

Sicherheitsrelevante Forschung erfordert in der Regel keine grundlegende Neuorientierung, sondern erweitert den Fokus um Anwendungsfelder für Technologien, Szenarien mit Sicherheitsbezug oder neue Zielgruppen für den Transfer. Es ist daher empfehlenswert, die Publikations- und Konferenzlandschaft aktiv zu verfolgen, um sicherheits- und verteidigungsrelevante wissenschaftliche und technologische Entwicklungen frühzeitig zu erkennen, sofern eine Einrichtung eine strategische Ausweitung ihrer Aktivitäten in diesen Bereich in Erwägung zieht.

2. AKTEURE UND STRUKTUREN

Wie ist sicherheitsrelevante Forschung auf deutscher und europäischer Ebene strukturiert?

Sicherheitsrelevante Forschung wird entweder durch Zuwendungen oder im Rahmen von Auftragsforschung finanziert. Dabei sind insbesondere zu unterscheiden:

Sicherheitsrelevante Forschung mit militärischem Fokus wird in Deutschland überwiegend im Rahmen von Auftragsforschung vergeben. Dies bedeutet, dass Forschungsaufträge direkt von Bedarfsträgern, wie dem Geschäftsbereich des Bundesministeriums für Verteidigung (BMVg einschließlich seiner nachgeordneten Behörden), oder durch Innovationsagenturen wie der Cyberagentur vergeben werden.

Darüber hinaus kann sicherheitsrelevante Forschung durch Zuwendungen in allen zivilen Förderprogrammen der üblichen nationalen und europäischen Fördergeber adressiert werden (v. a. Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR), Bundesministerium für Wirtschaft und Energie (BMWE), Deutsche Forschungsgesellschaft (DFG) und EU-Kommission), unter anderem Forschung für die zivile Sicherheit (BMFTR), maritimes Forschungsprogramm (BMWE) und Horizont Europa (EU).

Wer sind die zentralen nationalen, europäischen und internationalen Akteure im Bereich sicherheitsrelevanter Forschung und welche Vernetzungs- und Informationsplattformen gibt es?

Rolle und Anknüpfungspunkte für Universitäten

Universitäten nehmen innerhalb und im Umfeld dieser Strukturen bisher insbesondere eine komplementäre Rolle ein. Zum einen bilden sie die Schnittstelle zwischen grundlagenorientierter und anwendungsorientierter Forschung und tragen durch ihre wissenschaftliche Breite (stärker ausgeprägt als bei außeruniversitären Forschungseinrichtungen) und methodische Expertise wesentlich zur Weiterentwicklung der Wissensbasis sicherheitsrelevanter Technologien bei. Zum anderen wirken sich die Forschungsaktivitäten der Universitäten auf den wirtschaftlichen Bereich aus, insbesondere durch Ausgründungen aus dem universitären Umfeld sowie durch die Ausbildung zukünftiger Fachkräfte im Bereich Sicherheit und Verteidigung.

Nationale Akteure, Netzwerke und Foren

Das Zusammenbringen relevanter Akteure der sicherheits- und verteidigungsrelevanten Forschung findet vor allem über fachspezifische Netzwerke (Konferenzen und Tagungen) statt. Solche Formate bieten die Möglichkeit, wissenschaftliche, industrielle und behördliche Perspektiven zusammenzuführen und gemeinsame Forschungsinteressen zu identifizieren. Zudem gibt es für Universitäten ein hohes Potenzial für Industriekooperationen mit spezialisierten Unternehmen der Sicherheits- und Verteidigungsindustrie.

Knotenpunkte für die verteidigungsrelevante Forschung und Innovation sind auf Bundesebene bspw. die Einrichtungen und Institute des Geschäftsbereiches BMVg. Durchgeführt wird diese zum Beispiel in den Wehrtechnischen Dienststellen der Bundeswehr (WTD 41, WTD 52, WTD 61, WTD 71, WTD 81, WTD 91), im Cyber Innovation Hub oder dem Sanitätsdienst der Bundeswehr etc.

Das BMVg eröffnete im Februar 2026 außerdem das Innovationszentrum der Bundeswehr in Erding (Bayern). Allerdings ist noch unklar, wie Universitäten sich hier konkret einbringen können.

Auf zivile Forschung ausgerichtete Forschung findet im und mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), dem Bundeskriminalamt (BKA), dem Technischen Hilfswerk (THW), dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der deutschen Raumfahrtagentur und in anderen Bundesbehörden mit Sicherheitsbezug statt. Auch auf Länderebene gibt es forschungsaffine Akteure des Sicherheitsbereichs, zum Beispiel in den Landeskriminalämtern (LKA). Ein Kontakt zu öffentlichen, zivilgesellschaftlichen und privaten Anwendern in der zivilen Sicherheitsforschung ist über das BMFTR-geförderte Netzwerk ForAn± möglich.

In der sicherheits- und verteidigungsrelevanten Forschung bestehen zahlreiche etablierte Netzwerke. Dazu zählen insbesondere die Fraunhofer Institute, die dem Fraunhofer VVS-Verbund (Verteidigung, Vorbeugung, Sicherheit) angehören. Darüber hinaus sind derzeit zahlreiche regionale Clusternetzwerke im Aufbau (z. B. Innovationscampus Sicherheit und Verteidigung Baden-Württemberg, TechHub SVI von

Bayern Innovativ, TechHub SVI Nord für maritime Technologien, Defence.NRW für Nordrhein-Westfalen).

Weitere wichtige Foren sind die Deutsche Gesellschaft für Wehrtechnik (DWT) mit ihren Fachveranstaltungen, insbesondere der Konferenz „Forschung für Sicherheit und Verteidigung", sowie das Forschungsforum Öffentliche Sicherheit.

Die Cyberagentur finanziert Forschungsprogramme zu Cybersicherheit und damit verwandter Schlüsseltechnologien. In diesem Rahmen veranstaltet sie regelmäßig sogenannte *„Partnering Events"*, die dem Austausch zwischen Wissenschaft, Wirtschaft und öffentlichen Bedarfsträgern dienen und die Anbahnung neuer Kooperationen im Bereich innovativer und sicherheitsrelevanter Technologien unterstützen. Darüber hinaus veröffentlicht sie einen Großteil ihrer laufenden Forschungsprogramme und -projekte auf ihrer Website und bietet damit einen Überblick über aktuelle thematische Schwerpunkte und Förderaktivitäten.

Europäische und internationale Strukturen

Auf europäischer Ebene ist die *European Defence Agency* (EDA) ein zentraler Akteur, der Fähigkeitsentwicklungen steuert und Forschungsprioritäten setzt. Außerdem veröffentlicht sie technologische Foresightstudien, die ebenfalls dabei behilflich sein können, künftige Forschungsbedarfe zu antizipieren. Zudem ermöglicht die *Community for European Research and Innovation for Security* (CERIS) einen Austausch unter Forschenden im Bereich der zivilen Sicherheit.

Außerdem sind die *Capability Technology Groups* (CapTechs) der EDA eine wichtige Vernetzungs- und Informationsplattform, in die Universitäten Fachexpertise einbringen können. In den CapTechs kommen Vertreterinnen und Vertreter der EDA-Mitgliedstaaten sowie Industrie, Hochschulen und Forschungseinrichtungen zusammen, um Fähigkeitslücken zu identifizieren. Auf Basis dieser Fähigkeitslücken können dann Forschungsprojekte entweder über das gemeinsame EDA-Budget als EDA-weite Projekte (Kategorie A) oder von mindestens zwei interessierten EDA-Mitgliedstaaten über nationale Budgets (Kategorie B) initiiert werden, wobei Kategorie-B-Projekte deutlich häufiger sind.

Auf europäischer Ebene verfügen insbesondere Horizont Europa und der Europäische Verteidigungsfonds (EVF) über eigene Vernetzungsformate, die durch die Europäische Kommission, Projektträger bzw. Nationale Kontaktstellen unterstützt werden. Für sicherheitsrelevante Forschung sind vor allem die Nationale Kontaktstelle Sicherheitsforschung (NKS Sifo) im Rahmen von Horizont Europa sowie die Nationale Kontaktstelle für den Europäischen Verteidigungsfonds (NKS EVF) einschlägig. Die NKS EVF informiert unter anderem über Ausschreibungen, nationale und europäische Veranstaltungen sowie über Konsortien aus anderen Mitgliedstaaten, die spezifische Partner suchen. Je nach thematischer Ausrichtung können ergänzend weitere Nationale Kontaktstellen, etwa in den Bereichen Digitalisierung, Industrie oder Energie, relevant sein.

Schließlich gibt es die *Science and Technology Organization der NATO* (NATO STO). Sie ist die zentrale wissenschaftlich-technologische Organisation der NATO, die Forschung und Wissensaustausch im Bündnis koordiniert. Sie bietet die Möglichkeit, Teil ihrer internationalen Forschungscommunity zu werden, und veranstaltet regelmäßig Konferenzen, Workshops und Fachgremien. Darüber hinaus existiert ein Arbeitsprogramm kooperativer Forschungsaktivitäten, das sich mit zentralen sicherheits- und verteidigungsrelevanten Fragestellungen befasst und den Austausch zwischen Wissenschaft, Militär und Industrie fördert.

Allgemeiner Hinweis:
Vertrauen ist im Sicherheitsbereich ein sehr wichtiger Wert. Hier werden persönliche Kontakte hochgeschätzt und dienen der Vertrauensbildung. Es ist daher unabdingbar, sich ein Netzwerk aufzubauen. Zudem muss Vertrauen dafür geschaffen werden, dass Fragen der Forschungssicherheit in der Institution ernst genommen und umgesetzt werden (vgl. auch Geheimschutz unten).

3. THEMEN, BEDARFE UND STRATEGISCHE ORIENTIERUNG

Welche prioritären Forschungsthemen von Cyberagentur und EVF bieten konkrete Anknüpfungspunkte für forschungsintensive Universitäten?

Das Themenspektrum entsprechender Forschung ist breit und interdisziplinär und reicht von Grundlagenforschung bis hin zu anwendungsnahen technologischen Entwicklungen. Die folgenden Beispiele ausgewählter Förderprojekte verdeutlichen die thematische Bandbreite und mögliche Anknüpfungspunkte für universitäre Forschung:

Beispiele aus der nationalen Sicherheitsforschung:

- Das Projekt MOTRA (und das Nachfolgeprojekt MOTRA II) ist ein über das BMFTR, das Bundesministerium des Innern (BMI) und das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend (BMBFSFJ) geförderter Forschungsverbund im Kontext der zivilen Sicherheitsforschung. Beteiligt sind die Universität Hamburg und Ludwig-Maximilians-Universität München (und weitere). MOTRA dient unter anderem dem Aufbau und der Weiterentwicklung einer Monitoringplattform zur Früherkennung, Prävention und Bekämpfung von Extremismus.
- Das Forschungsprojekt RESILIA entwickelt einen Innovationshub, um durch bessere Zusammenarbeit und neue Trainingsformate die Krisen- und Widerstandsfähigkeit der Gesellschaft zu stärken. In diesem Vorhaben arbeitet unter anderem die Freie Universität Berlin mit den Universitäten der Bundeswehr zusammen. Das Projekt wird vom BMFTR gefördert.
- Die Humboldt Universität Berlin, die Martin-Luther-Universität Halle-Wittenberg, die Technische Universität Berlin sowie Fraunhofer SIT und Deloitte GmbH WPG entwickeln im Projekt MaLeFiz ein KI-basiertes Verfahren, mit dem auffällige Finanzströme automatisiert erkannt werden können. Das Projekt wird vom BMFTR gefördert.

Beispiele aus dem Portfolio der Cyberagentur:

- Im Rahmen des Programms „Existenzbedrohende Risiken aus dem Cyber- und Informationsraum für Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien (HSK)“ sind sowohl Forschende der Universität Hamburg gemeinsam mit ihren Projektpartnern im Projekt SOVEREIGN als auch Forschende der Otto-von-Guericke-Universität Magdeburg im Projekt ATTRIBUT beteiligt.
- Im Rahmen der SPECTRA-Challenge der Cyberagentur, die sich mit dem Schutz unbemannter Systeme vor elektronischer Kampfführung befasst, hat ein Team von Forschenden der Technischen Universität Clausthal den ersten Platz in der Kategorie „Moonshot-Track“ erreicht.

Beispiele aus dem Europäischen Verteidigungsfonds (EVF):

- Im Rahmen des Projekts SQORPION forscht die Johannes Gutenberg-Universität Mainz mit anderen Konsortialpartnern an spin-basierten Quantensystemen mit dem Ziel, robuste Quantensensorik für zukünftige verteidigungsrelevante Anwendungen zu entwickeln.
- Die Technische Universität München entwickelt im Rahmen von iMEDCAP eine robotische Lösung, die während eines (autonomen) Evakuierungsflugs telemedizinisch bedient werden kann.
- An der Universität Stuttgart beschäftigen sich Forschende des Fachbereichs Physik im Projekt ADEQUADE damit, neue Phänomene in wechselwirkenden Quantensystemen zu entwickeln, zu steuern und zu verstehen.
- Forschende der Universität Ulm sowie der Universität der Bundeswehr München arbeiten im Projekt GENIUS zu Gefahrenminimierung und Gefahrenabwehr bei Sprengstoffen und Kampfmitteln.

Beispiele aus der europäischen Sicherheitsforschung (Horizont Europa):

- Im Rahmen des europäischen Verbundprojekts VIGILANT wurde in Zusammenarbeit mit Polizeibehörden eine Plattform mit integrierten Tools entwickelt, um Desinformationen aus allen wichtigen Online-Quellen und in verschiedenen Sprachen zu erkennen. Die Albert-Ludwigs-Universität Freiburg (*Centre for Security and Society*) war in diesem Projekt für ethische Fragestellungen verantwortlich.
- Klimatologinnen und Klimatologen der Justus-Liebig-Universität Gießen forschen im Rahmen des MedEWSa an der frühzeitigen Erkennung von Extremwetter, Hitzewellen, Dürren, Überschwemmungen, Erdrutschen und Waldbränden.
- Die Technische Hochschule Köln betreut im Rahmen von NBSINFRA die Kölner Fallstudie, in der naturbasierte Lösungen technisch und sozialverträglich für den Schutz kritischer Infrastrukturen vor Gefahren realisiert werden können.

Wie werden die Prioritäten für die Programme der Sicherheits- und Verteidigungsforschung festgelegt?

› Die Festlegung der Prioritäten unterscheidet sich je nach Zuwendungs- bzw. Auftraggeber. Unter anderem:

Zivile Sicherheitsforschung der Bundesregierung/BMFTR:
Die Prioritäten für die Projektförderung ergeben sich aus dem Programm der Bundesregierung „Forschung für die zivile Sicherheit – gemeinsam für ein sicheres Leben in einer resilienten Gesellschaft“ und orientieren sich stark an den Anwenderinnen und Anwendern sowie Behörden und Organisationen mit Sicherheitsaufgaben.

Die Forschungsprogramme der Cyberagentur orientieren sich maßgeblich an den Bedarfen ihrer zivilen wie militärischen Bedarfsträger. Deren Anforderungen leiten sich aus aktuellen und absehbaren Bedrohungslagen im Cyber- und Informationsraum ab und prägen die thematischen Schwerpunkte der geförderten Forschungsaktivitäten.

Auftragsforschung des Bundes:
Die Prioritäten orientieren sich zum einen an den Bedarfen der Behörden und Organisationen mit Sicherheitsaufgaben, also insbesondere der Polizeien, des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, des Bundesamts für Sicherheit in der Informationstechnik und der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). Zum anderen richten sie sich nach den Bedarfen der Bundeswehr, die insbesondere im Ressortforschungsplan des BMVg konkretisiert werden. Die Bedarfe dieser Behörden und Organisationen ergeben sich aus ihren jeweiligen Aufträgen in Wechselwirkung mit aktuellen und absehbaren Entwicklungen, die ihre Aufgabenerfüllung betreffen.

Europäischer Verteidigungsfonds (EVF):
Das BMVg bringt über den Programmausschuss EVF Themen ein, wenn diese dem Fähigkeitsinteresse der Bundeswehr entsprechen.

Zivile Sicherheitsforschung in Horizont Europa:
Die Prioritäten ergeben sich aus den Bedarfen der deutschen Anwenderinnen und Anwender sowie der Bundesressorts. Zudem besteht eine Beteiligungsmöglichkeit der Fachöffentlichkeit.

4. ZUGANG ZU FÖRDERUNG UND PROJEKTEN

Welche Förder- und Auftragsforschungsprogramme existieren im Bereich Sicherheits- und Verteidigungsforschung und wo erhalten Interessierte Beratung sowie weiterführende Informationen?

Folgende Institutionen vergeben Forschungsaufträge und Forschungsförderung mit Sicherheits- und Verteidigungsbezug (kein Anspruch auf Vollständigkeit):

- **Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR):**
  Förderlinie „Forschung für die zivile Sicherheit“. Beratung erfolgt durch den zuständigen Projektträger VDI Technologiezentrum. Weiterführende Informationen und aktuelle Ausschreibungen sind über die Programmwebsite und einschlägige Förderportale abrufbar. Weitere Förderprogramme unter anderem im Bereich Cybersicherheit sowie fach- oder domänenspezifisch (z. B. Geistes- und Sozialwissenschaften, Extremwetter, Künstliche Intelligenz).

- **Horizont Europa (HEU):**
  Europäisches Rahmenprogramm für Forschung und Innovation mit sicherheitsrelevanten Themen insbesondere im Cluster 3 „Civil Security for Society“. Beratung erfolgt über die jeweiligen Nationalen Kontaktstellen (NKS), insbesondere die NKS Sicherheitsforschung. Eine Übersicht über Programme, Ausschreibungen und Ansprechpersonen bietet das *Funding & Tenders Portal* sowie das Netzwerk der Nationalen Kontaktstellen.

- **Europäischer Verteidigungsfonds (EVF):**
  Förderung von verteidigungsbezogener Forschung und Entwicklung auf EU-Ebene. Beratung erfolgt durch die Nationale Kontaktstelle EVF (NKS EVF). Informationen zu Ausschreibungen und Programminhalten sind ebenfalls über das *Funding & Tenders Portal* sowie die NKS EVF verfügbar.

- **Agentur für Innovation in der Cybersicherheit (Cyberagentur):**
  Vergibt Forschungsaufträge insbesondere im Bereich disruptiver Cyber- und Schlüsseltechnologien. Beratung erfolgt in der Regel direkt über die Cyberagentur. Informationen zu Programmen, thematischen Schwerpunkten und laufenden Projekten werden über die Website der Cyberagentur sowie über Ausschreibungen auf der Plattform eVergabe bereitgestellt.

- **Bundesministerium der Verteidigung (BMVg):**
  Vergibt Forschungsaufträge im Rahmen der Ressortforschung. Hier bestehen in der Regel keine öffentlichen Ausschreibungen und es gibt keine offizielle Beratungsstelle. Informationen zu thematischen Schwerpunkten ergeben sich vor allem aus einschlägigen Veröffentlichungen wie dem Ressortforschungsplan sowie aus dem Austausch mit relevanten Bedarfsträgern.

- **Forschungsausschreibungen anderer Ministerien und Behörden:**
  Jeweils aktuell über die Förderberatung des Bundes suchbar.

Wie unterscheiden sich Auftragsforschung und Forschungsförderung (Zuwendungen) in ihrer Förderlogik?

Sicherheitsrelevante Forschung in Deutschland erfolgt einerseits durch Auftragsforschung (z. B. BMVg, Cyberagentur). Sie wird vollständig durch den Auftraggeber finanziert. Der Auftragnehmer nennt hierfür einen Festpreis, zu dem die Forschungs- und Entwicklungsleistung erbracht wird. Dieser enthält typischerweise 100 % der Kosten inklusive indirekter Kosten und einer Gewinnmarge. In der Regel erhält der Auftraggeber teilweise oder vollständige Nutzungs- oder Verwertungsrechte an den Forschungsergebnissen. Da im Rahmen der Auftragsforschung individuelle zivilrechtliche Verträge für jeden Auftrag geschlossen werden, kann es zu abweichenden vertraglichen Regelungen kommen.

Andererseits kann sicherheitsrelevante Forschung im Rahmen von Zuwendungen erfolgen. Gewinnmargen sind in diesem Fall nicht enthalten. Die Förderquoten sind hier vom konkreten Programm abhängig. Beim Europäischen Verteidigungsfonds (EVF) ist bei bestimmten Projekten – insbesondere im Entwicklungsbereich – eine Kofinanzierung durch das BMVg im Rahmen nationaler Auftragsvergaben möglich. Voraussetzung hierfür ist in der Regel ein entsprechendes nationales Fähigkeitsinteresse, das durch das BMVg bestätigt wird. Die Kofinanzierung dient dazu, den nationalen Anteil an europäischen Entwicklungsprojekten abzudecken

und eine Beteiligung deutscher Akteure an diesen Vorhaben zu ermöglichen bzw. zu stärken.

Die Verwertungsrechte bei durch Zuwendungen finanzierten Projekten verbleiben grundsätzlich bei den Zuwendungsempfängern. Diese werden jedoch durch spezifische Regelungen, etwa zu Zugriffsrechten, Geheimschutz oder Exportkontrolle, ergänzt.

Für weitere Informationen zu IP- und Verwertungsrechten siehe Kapitel 8: Wie werden IP-Rechte im Rahmen sicherheitsrelevanter Forschung geregelt?

Welche Förderquoten und Overheads gelten in nationalen und europäischen Forschungsprogrammen (Zuwendungen)?

› Die Förderquoten variieren je nach Programm und Projektart. Für nationale Förderprogramme des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) gelten die jeweiligen Förderrichtlinien. Die Förderquoten und Overheads orientieren sich dabei an den üblichen Regelungen der Projektförderung im nationalen Kontext.

Im Rahmen von Horizont Europa werden Universitäten in der Regel mit bis zu 100 % der förderfähigen direkten Kosten gefördert, während für industrielle Akteure – insbesondere bei Innovationsmaßnahmen – geringere Förderquoten gelten können. Im Europäischen Verteidigungsfonds (EVF) sind die Förderquoten aktivitätsspezifisch ausgestaltet und liegen je nach Projektphase zwischen etwa 20 % und 100 %; im Forschungsbereich beträgt die Förderung in der Regel bis zu 100 % für alle Beteiligten.

Die Overheads (indirekte Kosten) in EU-Programmen werden üblicherweise pauschal mit 25 % der direkten Kosten angesetzt. Im Europäischen Verteidigungsfond (EVF) besteht darüber hinaus teilweise die Möglichkeit, die tatsächlich angefallenen indirekten Kosten geltend zu machen, was jedoch mit erhöhtem administrativem Aufwand verbunden ist.

Wo können Forschende einsehen, welche Forschungsbedarfe derzeit durch die öffentliche Hand ausgeschrieben werden?

› Ausschreibungen im Bereich der sicherheits- und verteidigungsrelevanten Forschung werden über eine Vielzahl nationaler und europäischer Plattformen veröffentlicht, die einen zentralen Zugang zu aktuellen Förder- und Vergabeverfahren bieten.

Auf nationaler Ebene werden sicherheitsrelevante Ausschreibungen regelmäßig im Bundesanzeiger, über die Plattform eVergabe und über die Ausschreibungsplattform service.bund.de veröffentlicht. Förderprogramme werden darüber hinaus in der Förderdatenbank der Förderberatung des Bundes zusammengefasst.

Die Ausschreibungen der Cyberagentur erfolgen über die Plattform eVergabe; ergänzend bietet ihre Website einen Überblick über aktuelle Programme, Projekte und thematische Schwerpunkte. Diese umfassen insbesondere die Absicherung komplexer IT- und Infrastruktursysteme, innovative Ansätze der Cyberabwehr, den Einsatz von Künstlicher Intelligenz für Sicherheitsanwendungen sowie Schlüssel- und Zukunftstechnologien mit Relevanz für die innere und äußere Sicherheit.

Ausschreibungen zu EU-Programmen (z. B. Horizont Europa, EVF) werden im *Funding & Tenders Portal (Calls for proposal)* veröffentlicht. Hier können ebenfalls vergangene Ausschreibungen und bereits geförderte Projekte eingesehen werden.

Im Rahmen der *NATO Science and Technology Organization* (STO) bieten sich Beteiligungsmöglichkeiten weniger über klassische Ausschreibungen als über thematisch definierte Forschungsprogramme, Grants (z. B. im *NATO Chief Scientist Grants Programme*) sowie die Mitarbeit in kooperativen Forschungsnetzwerken und Projektgruppen zu zentralen sicherheitsrelevanten Fragestellungen.

5. VORBEREITUNG AUF PROJEKTE

Was sollte vor Antragstellung beachtet bzw. auf universitärer Ebene geklärt sein?

Sicherheitsrelevante Forschung, die auf den zivilen Bereich zielt, ist in der Regel ohne vorbereitende Maßnahmen möglich, profitiert jedoch gegebenenfalls von den unten genannten Schritten.

Falls es eine Zivilklausel gibt: Wie wird diese gehandhabt, wie groß ist der Spielraum für Forschende? Sinnvoll ist auch eine Position zur Verteidigungsforschung, die ermöglichend mindestens auf die Freiheit von Forschung und Wissenschaft verweist, die nach Artikel 5 Absatz 3 Grundgesetz garantiert ist.

Grundsätzlich ist zu klären, ob die Hochschule, das betreffende Institut oder die jeweilige Forschungsgruppe aus individuellen Überzeugungen heraus Forschung mit militärischem Bezug ablehnt bzw. kritisch sieht. Idealerweise hat ein Dialog an der Institution stattgefunden oder es gibt ein permanentes Dialogangebot.

Empfehlenswert ist die Bestellung eines Geheimschutzbeauftragten, der auch für Anliegen rund um die Sicherheitsanforderungen ansprechbar ist. Diese Funktion kann beispielsweise durch die für Informationssicherheit beauftragte Person der Hochschule wahrgenommen werden. Es gibt spezielle Lehrgänge, durch die das benötigte Fachwissen aufgebaut werden kann. Ergänzend sollte – insbesondere bei Forschung mit Bezug zu Dual-Use-Gütern und entsprechenden exportkontrollrechtlichen Anforderungen – eine Exportkontrollbeauftragte bzw. ein Exportkontrollbeauftragter benannt sein. Bei grundlegenden Fragen zum Exportkontrollrecht in Verbindung mit Forschungsvorhaben bietet die Seite des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA) Orientierung.

Hinweis:
Für hochschulinterne Diskussionen gilt zudem zu beachten, dass Forschungsprojekte mit militärischem Bezug mit sich bringen können, dass im Rahmen der Projektarbeit auch uniformierte Angehörige der Bundeswehr Zugang zum Campus der Hochschule erhalten.

Ein interessantes **Beispiel** für den Umgang mit sicherheitsrelevanter, insbesondere verteidigungsrelevanter, Forschung zeigt die **University of Manchester**. Sie stellt auf ihrer Website Informationen zum Engagement der Universität im Bereich Verteidigung und Sicherheit öffentlich zur Verfügung, um Transparenz und Klarheit zu schaffen. Sie informiert über die Grundsätze der Zusammenarbeit mit Verteidigungsorganisationen (unter Wahrung akademischer Freiheit und gesetzlicher Vorgaben), die Arten von Forschungsprojekten (militärisch, *dual-use*, zivil) und deren ethische sowie rechtliche Prüfung, die Investitionsrichtlinien (Ausschluss umstrittener Waffenhersteller), die Berufsorientierung für Studierende (neutrale Darstellung von Karrieremöglichkeiten im Verteidigungssektor, inklusive Protestmöglichkeiten). Die Seite ist hier abrufbar.

Ergeben sich aus sicherheitsrelevanter Forschung besondere Anforderungen an die technische Ausstattung (insbes. IT) und deren Beschaffung?

Die Sicherheitsrelevanz eines Forschungsvorhabens führt grundsätzlich nicht automatisch zu spezifischen Anforderungen an die technische Ausstattung und deren Beschaffung. In der Auftragsforschung können jedoch projektbezogene Anforderungen durch den Auftraggeber festgelegt werden.

Dies betrifft insbesondere sicherheitsrelevante, aber nicht amtlich eingestufte Vorhaben, bei denen etwa bestimmte technische Standards, organisatorische Maßnahmen oder Zertifizierungen (z. B. nach BSI-Grundschutz oder einschlägigen ISO-Normen) vertraglich vorgegeben werden.

In der Forschungsförderung (Zuwendungen) ist es möglich, dass einzelne Förderprogramme spezifische Vorgaben beinhalten, insbesondere vor dem Hintergrund zunehmender Anforderungen an die Forschungssicherheit.

Sofern im Projekt mit als amtliche Verschlusssache eingestuften Informationen gearbeitet wird, gelten darüber hinaus besondere sicherheitsrechtliche Anforderungen, die gesondert zu beachten sind (vgl. Kapitel 6).

Welche Anforderungen sind bei der Auswahl von Konsortialpartnern in sicherheitsrelevanten Forschungsprojekten zu beachten?

Die Auswahl von Konsortialpartnern ist zunächst im Rahmen allgemeiner Erwägungen zur Forschungssicherheit zu bewerten. Hierzu zählen insbesondere die Vertrauenswürdigkeit der Partner, der Umgang mit sensiblen Informationen, mögliche Interessenkonflikte sowie rechtliche Rahmenbedingungen, etwa im Bereich Exportkontrolle oder Datenschutz. Die Beteiligung von Organisationen bzw. Personen aus einem der Staaten der Staatenliste im Sinne von § 13 Abs. 1 Nr. 17 Sicherheitsüberprüfungsgesetz (SÜG) ist kritisch zu prüfen.

Darüber hinaus können sich programmspezifische Anforderungen ergeben. Im Europäischen Verteidigungsfonds (EVF) müssen Konsortialpartner grundsätzlich aus EU-Mitgliedstaaten oder Norwegen stammen. Zudem ist nachzuweisen, dass beteiligte Einrichtungen unter effektiver Kontrolle von EU-Mitgliedstaaten bzw. Norwegen stehen. In begründeten Ausnahmefällen kann ein Mitgliedstaat bzw. Norwegen entsprechende Garantien übernehmen.

Die konkrete Ausgestaltung und Bewertung der Zulässigkeit von Konsortialpartnern sollte frühzeitig geprüft und – insbesondere bei komplexeren Konstellationen – mit den zuständigen Beratungsstellen, wie der Nationalen Kontaktstelle für den Europäischen Verteidigungsfonds (NKS EVF), abgestimmt werden.

Welche exportkontrollrechtlichen Anforderungen sind bei grenzüberschreitenden Forschungsprojekten zu beachten?

Bei grenzüberschreitenden Forschungsprojekten sind die Vorgaben des Exportkontrollrechts zu beachten, insbesondere bei der Weitergabe von Gütern, Technologien oder Informationen mit potenzieller Dual-Use-Relevanz. In der Regel gilt bereits die Übermittlung von Forschungsergebnissen – etwa in Form von Berichten, Daten oder Software (z. B. *Deliverables*) – an Projektpartner im Ausland als Ausfuhr bzw. Verbringung im rechtlichen Sinne und ist somit genehmigungspflichtig.

In vielen Fällen ist daher die Beantragung einer entsprechenden Genehmigung beim BAFA erforderlich. Häufig wird hierfür eine sogenannte Sammelausfuhrgenehmigung (SAG) genutzt. Sie muss je Konsortialpartner beim BAFA beantragt werden, die Ausfuhr bzw. Verbringung an mehrere Empfänger und in verschiedene Länder abdecken und wird in der Regel für einen begrenzten Zeitraum (typischerweise bis zu zwei Jahre) erteilt. Weitere Informationen bietet das BAFA auf seiner Website (Exportkontrolle und Wissenschaft (Academia).

Welche Sicherheitsprozesse und -maßnahmen müssen über die Exportkontrolle hinaus an Universitäten implementiert sein?

Neben der Exportkontrolle sollten Forschungseinrichtungen weitergehende Maßnahmen zur Herstellung von Forschungssicherheit ergreifen, insbesondere Due-Diligence-Maßnahmen, IT-Anforderungen und -Sicherheitsstandards, Schulungen von Forschenden sowie die Etablierung von Verfahren bei Sicherheitsvorfällen. Darüber hinaus bietet es sich an, frühzeitig eine verantwortliche Person für Forschungssicherheit zu bestimmen und mit entsprechenden Kompetenzen auszustatten.

Sofern eine Hochschule oder Forschungseinrichtung beabsichtigt, amtlich als Verschlusssache (VS) eingestufte Projekte durchzuführen, sind weitreichender Maßnahmen zur personellen und materiellen Ertüchtigung notwendig (siehe Kapitel 6).

6. SICHERHEITS- UND GEHEIMSCHUTZ-ANFORDERUNGEN IN PROJEKTEN

6.1 Grundlagen

Welche Geheimhaltungsgrade gibt es und woran entscheidet sich, wie ein Projekt eingestuft wird?

Bei Forschungsprojekten können einzelne Projektbestandteile – etwa Arbeitspakete oder konkrete Ergebnisse (sog. *Deliverables*) – durch zuständige Behörden sicherheitsrechtlich eingestuft werden[1]. Die Bandbreite dieser Einstufungen reicht von **VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)** (entspricht etwa EU RESTRICTED) über **VS-VERTRAULICH (VS-Vertr.)** (EU CONFIDENTIAL) und **GEHEIM** (EU SECRET) bis hin zu **STRENG GEHEIM** (EU TOP SECRET). Es gilt der Grundsatz, dass die Informationen nur einem begrenzten Personenkreis zugänglich gemacht werden dürfen (Kenntnis nur wenn nötig/Need-to-know-Prinzip). Die Entscheidung einer Einstufung hängt vom Inhalt und von der Kritikalität der Informationen ab.

Neben den amtlichen Einstufungen gibt es noch die Einstufung **„EU sensitive“**, die nicht behördlich klassifizierte, aber schützenswerte Informationen kennzeichnet.

VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)/EU RESTRICTED
Informationen dieser Einstufung sind schutzbedürftig, da ihre unbefugte Weitergabe nachteilige Auswirkungen haben kann. In der deutschen Hochschulforschungspraxis ist der Geheimhaltungsgrad VS-NfD (EU RESTRICTED) der mit Abstand am häufigste vorkommende Geheimhaltungsgrad.

VS-VERTRAULICH (VS-Vertr.)/EU CONFIDENTIAL
Die unbefugte Offenlegung kann den Interessen der Bundesrepublik Deutschland oder der EU schaden. Entsprechend gelten erhöhte Anforderungen an Zugriff, Verarbeitung und Speicherung der Informationen. In der deutschen Hochschulforschungspraxis kommt der Geheimhaltungsgrad VS-Vert. (EU CONFIDENTIAL) gelegentlich vor.

GEHEIM/EU SECRET
Eine unbefugte Weitergabe kann schwerwiegende Schäden für staatliche Sicherheitsinteressen verursachen. Der Zugang ist stark eingeschränkt und unterliegt strengen Sicherheitsvorkehrungen. In der deutschen Hochschulforschungspraxis kommt der Geheimhaltungsgrad GEHEIM (EU SECRET) sehr selten vor und wird hier nur im Sinne der Vollständigkeit aufgeführt.

VS-STRENG GEHEIM/EU TOP SECRET
Die höchste Einstufung: Eine Offenlegung würde außergewöhnlich schweren Schaden für zentrale staatliche Interessen bedeuten. Entsprechend gelten sehr hohe Sicherheitsanforderungen und strengste Zugangsbeschränkungen.
In der deutschen Hochschulforschungspraxis kommt der Geheimhaltungsgrad STRENG GEHEIM (EU TOP SECRET) sehr selten vor und wird hier nur im Sinne der Vollständigkeit aufgeführt.

Woran kann man Sicherheitsanforderungen festmachen und kann der Blick auf das Technology Readiness Level (TRL) helfen?

Sicherheitsanforderungen hängen nicht vom TRL ab. Sie können sich daraus ergeben, dass mit einer *Background-IP* gearbeitet wird oder mit sensiblen Daten ohne Einstufung (z. B. Daten zu Schwachstellen in der kritischen Infrastruktur), oder dass die Forschungsergebnisse ein Missbrauchspotenzial haben. Sicherheitsanforderungen ergeben sich aus dem Zusammenspiel technologiespezifischer Sicherheitskriterien, regulatorischer Vorgaben sowie weiterer Faktoren wie ethischer Fragestellungen und potenzieller Reputationsrisiken. Zur Gewährleistung angemessener Sicherheitsmaßnahmen innerhalb einer Einrichtung ist eine strukturierte Risikobewertung bzw. Chancen-Risiken-Abwägung notwendig, die in etablierte Strukturen der Forschungssicherheit eingebettet sein sollte.

[1] siehe auch Überblick des Deutschen Bundestages.

6.2 Technische und organisatorische Anforderungen

Welche Sicherheitsanforderungen gelten für amtlich eingestufte Forschungsprojekte?

Die konkreten Sicherheitsanforderungen richten sich nach der jeweiligen Einstufung der Projektinhalte und nehmen mit zunehmendem Geheimhaltungsgrad deutlich zu.

Bereits bei der Einstufung **VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD/EU RESTRICTED)** sind grundlegende Maßnahmen umzusetzen. Sie finden sich in der Verschlusssachenanweisung (VSA) des Bundes (Bundeseinrichtungen) bzw. in der VSA ihres Bundeslandes (Landeseinrichtungen).[2] Hervorzuheben sind hier vor allem die Regelungen des VS-NfD-Merkblatts (Anhang der VSA). Zu den umzusetzenden technischen und organisatorischen Maßnahmen zählt insbesondere der Einsatz geeigneter IT-Systeme (VS-IT), etwa Rechner ohne Drahtlosschnittstellen und mit klar geregelten Benutzerprofilen. Die Verarbeitung und Weitergabe entsprechender Informationen darf nur unter Einhaltung geeigneter Schutzmaßnahmen erfolgen, vor allem durch Verschlüsselung. Maßgeblich sind hierbei in erster Linie die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Darüber hinaus sind Aufbewahrungsorte für entsprechende Unterlagen oder Datenträger physisch zu sichern und vor unbefugtem Zugriff zu schützen.

Mit höheren Geheimhaltungsgraden (**VS-VERTRAULICH** und darüber hinaus) steigen die Anforderungen deutlich an. Dies betrifft insbesondere strengere Zugangsbeschränkungen auf einen klar definierten und sicherheitsüberprüften Personenkreis. Zudem ist die Nutzung speziell zugelassener und entsprechend abgesicherter IT-Systeme (VS-IT) erforderlich, und zwar einschließlich erhöhter Anforderungen an Verschlüsselung, Nutzerverwaltung und die konsequente Trennung von IT-Systemen, die nicht amtlich eingestufte Dokumenten verarbeiten. Darüber hinaus sind geeignete, kontrollierte Räumlichkeiten für die Verarbeitung und Aufbewahrung vorzusehen. Ergänzend bestehen erweiterte organisatorische Vorgaben, vor allem hinsichtlich der eindeutigen Kennzeichnung von Verschlusssachen, der lückenlosen Dokumentation von Zugriff, Weitergabe und Aufbewahrung sowie der kontrollierten Weitergabe und des gesicherten Transports von Informationen.

Wie müssen in sicherheitsrelevanten Projekten erhobene Forschungsdaten gespeichert werden und welche Anforderungen kommen dabei auf Universitäten zu?

Die Anforderungen an die Speicherung von Forschungsdaten ergeben sich nicht aus der Sicherheitsrelevanz eines Projekts als solcher, sondern maßgeblich aus einer etwaigen amtlichen Einstufung der verarbeiteten Informationen. Bei nicht amtlich eingestuften Projekten gelten grundsätzlich die üblichen Anforderungen an Datenschutz, IT-Sicherheit und gute wissenschaftliche Praxis.

Bereits bei der Einstufung **VS-NfD (EU RESTRICTED)** sind jedoch spezifische Schutzmaßnahmen umzusetzen. Dazu zählen insbesondere die Verarbeitung und Speicherung der Daten in geeigneten, abgesicherten IT-Umgebungen (VS-IT), der Verzicht auf Drahtlosschnittstellen, die Nutzung von Verschlüsselungsverfahren sowie klare Zugriffsregelungen. Darüber hinaus müssen entsprechende Systeme und Datenbestände vor unbefugtem Zugriff geschützt und organisatorisch abgesichert werden. Maßgeblich sind hierbei in erster Linie die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Mit höheren Geheimhaltungsgraden (**VS-VERTRAULICH** und darüber hinaus) (EU CONFIDENTIAL und höher) steigen die Anforderungen weiter an. Dies betrifft insbesondere die Nutzung speziell zugelassener IT-Infrastrukturen, streng kontrollierte Zugriffs- und Berechtigungskonzepte, die Einbindung sicherheitsüberprüften Personals sowie weitergehende Anforderungen an Dokumentation, Protokollierung und physische Sicherung der Systeme (Anforderungen des materiellen Geheimschutzes).

Für Rechenzentren an Universitäten bedeutet dies, dass je nach Einstufung entsprechende technische und organisatorische Voraussetzungen geschaffen werden müssen. Dies kann den Aufbau separater, besonders gesicherter IT-Umgebungen, die Anpassung bestehender Sicherheitskonzepte sowie die Abstimmung mit den zuständigen Sicherheits- und Geheimschutzstellen erfordern.

[2] Hier finden Sie exemplarisch die VSA Bund: https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_13032023_SII554001405.htm.

Für jedes Bundesland gibt es eine eigene VSA, die sich aber nur marginal unterscheiden.

6.3 Personal

Welche Anforderungen gelten für Sicherheitsüberprüfungen von Projektmitarbeitenden und wie sollten Universitäten organisatorisch damit umgehen?

Sicherheitsüberprüfungen (SÜ) von Projektmitarbeitenden sind erst ab der Einstufung **VS-VERTRAULICH (EU CONFIDENTIAL)** und höher erforderlich und richten sich nach den Vorgaben des Sicherheitsüberprüfungsgesetzes (SÜG). Hierfür muss die Universität eine bzw. einen Geheimschutzbeauftragte(n) benennen. Er gibt dann die SÜ der Projektmitarbeitenden mit Zugriff zu VS-VERTRAULICH bei den zuständigen Verfassungsschutzbehörden in Auftrag. In der Regel ist jeweils das Landesamt für Verfassungsschutz zuständig, aber in bestimmten Fällen kann auch das Bundesamt für Verfassungsschutz eingebunden sein.

Je nach Projekt und Zugang zu Verschlusssachen können unterschiedliche Stufen der Sicherheitsüberprüfung (z. B. einfache oder erweiterte SÜ) erforderlich sein. Es sollte genug Zeit eingeplant werden (Dauer der SÜ 3-24 Monate je nach Komplexität des Falles und Auslastung der Behörden). Es entstehen für die SÜ keine direkten Kosten. Grundlage für die SÜ ist die Sicherheitserklärung der zu überprüfenden Person (Selbstauskunft) mit Angaben zur Person, gegebenenfalls Lebenspartner, Wohnorte sowie Anfragen bei Verfassungsschutzbehörden und dem Bundeszentralregister (Führungszeugnis).

Wie unterscheiden sich die einfache Sicherheitsüberprüfung (Ü1) und die erweiterte Sicherheitsüberprüfung (Ü2)?

Die einfache Sicherheitsüberprüfung **(Ü1)** umfasst die Prüfung grundlegender personenbezogener Angaben sowie behördliche Abfragen, insbesondere bei Verfassungsschutzbehörden und dem Bundeszentralregister.

Die erweiterte Sicherheitsüberprüfung **(Ü2)** geht darüber hinaus und bezieht zusätzliche Aspekte ein, etwa Angaben zu Lebenspartnern bzw. Ehepartnern sowie längere Auslandsaufenthalte. Sie wird insbesondere dann erforderlich, wenn der Zugang zu GEHEIM (EU SECRET) oder zu einer hohen Anzahl von VS-VERTRAULICH (EU CONFIDENTIAL) bestehen wird.

Darüber hinaus gibt es noch die erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen **(Ü3)**, die für die deutsche Hochschulforschungspraxis allerdings wenig relevant ist.

Die Entscheidung darüber, welche Art der Sicherheitsüberprüfung durchgeführt wird, treffen die zuständigen Behörden für Verfassungsschutz, sie kann nicht durch die Hochschule selbst bestimmt werden.

Welche sicherheitsbezogenen Rollen und Zuständigkeiten sind in Forschungsprojekten vorzusehen?

Die konkreten Rollen und Zuständigkeiten im Bereich Sicherheit hängen maßgeblich von der Art des Projekts sowie von dessen sicherheitsbezogenen Anforderungen ab.

In EU-geförderten Projekten, in denen mit amtlich eingestuften Informationen gearbeitet wird, ist in der Regel die Benennung eines **Project Security Officers (PSO)** erforderlich. Diese bzw. dieser ist für die Umsetzung und Überwachung der projektspezifischen Sicherheitsanforderungen verantwortlich und fungiert als zentrale Ansprechperson gegenüber den zuständigen Stellen. Voraussetzung für die Ausübung dieser Funktion ist in der Regel eine entsprechende Sicherheitsüberprüfung.

Darüber hinaus können, je nach Projekt und Sensibilität der Inhalte, weitere Strukturen vorgesehen werden, etwa beratende Gremien im Bereich Sicherheit (z. B. ein *Security Advisory Board*). Solche Gremien sind jedoch nicht grundsätzlich verpflichtend, sondern werden bei Bedarf eingerichtet, insbesondere, wenn mit sensiblen oder potenziell amtlich einzustufenden Informationen gearbeitet wird. Unabhängig von formalen Rollen ist sicherzustellen, dass die Zuständigkeiten für Sicherheitsfragen im Projekt klar geregelt und institutionell verankert sind.

Weitere Informationen finden sich im EU-Leitfaden für den Umgang mit sicherheitsrelevanten Projekten und in den Allgemeine Sicherheitsvorgaben für Programme des Europäischen Verteidigungsfonds (EVF).

Gibt es besondere Vorgaben für Dienst- und Privatreisen, die an sicherheitsrelevanten Projekten beteiligte Personen unternehmen?

Die Sicherheitsrelevanz eines Projektes an sich begründet keine besonderen Vorgaben für Dienst- und Privatreisen. Für Projektmitarbeitende, die Zugang zu Informationen des

Geheimhaltungsgrades VS-NfD (EU RESTRICTED) haben, gilt keine Anzeige- oder Genehmigungspflicht von Dienst- oder Privatreisen. Für Projektmitarbeitende, die mit amtlich eingestuften Informationen des Geheimhaltungsgrades VS-Vertr. oder höher (EU CONFIDENTIAL oder höher) arbeiten, gelten die Regelungen des Sicherheitsüberprüfungsgesetzes (SÜG) des entsprechenden Bundeslandes. Als allgemeine Orientierung kann hier § 32 SÜG des Bundes dienen, da sich die SÜG der Bundesländer nur marginal unterscheiden. Genehmigungspflichtig sind in diesem Fall Dienst- und Privatreisen in Staaten mit erhöhtem Sicherheitsrisiko gemäß der Staatenliste des BMI (derzeit u. a. China, Hongkong, Macau, Russland). Für das EU-Ausland gibt es keinerlei einschränkende Vorgaben. Es wird nicht zwischen Dienst- und Privatreisen unterschieden.

Bei nicht amtlich eingestuften EU-Forschungsprojekten und Forschungsprojekten mit Klassifzierung „EU sensitive“ gibt es keine gesetzlichen Reisebeschränkungen. Möglicherweise sind aber im *Security Framework* (*Programme Security Instruction, Security Aspects Letter*, Zuwendungsvertrag) Regelungen vereinbart (z. B. Anzeigepflicht für Dienstreisen innerhalb der EU, Genehmigungspflicht für Dienstreise außerhalb der EU).

7. EU-SPEZIFISCHE SICHERHEITS-PROZESSE

Welche Projekte im Rahmen von Horizont Europa werden auf Sicherheitsaspekte geprüft (Security Appraisal)?

Ziel des Security Appraisal ist es, sicherzustellen, dass Projekte die EU-Sicherheitsregeln einhalten und keine Sicherheitsrisiken für EU, Mitgliedstaaten, Partner, Daten oder Infrastrukturen verursachen. Es gibt eine zusätzliche Prüfung für ausgewählte Horizon-Europe-Vorhaben. Folgende Projektanträge werden dort aufgenommen:

- Anträge im Cluster 3: Civil Security for Society
- Anträge mit Beteiligung von Drittstaaten mit erhöhtem Sicherheitsrisiko
- Anträge mit sensiblen Technologien, Dual-Use-Potenzial, kritischen Infrastrukturen
- Anträge, die mit vertraulichen Daten, potenziell klassifizierbaren Informationen oder sicherheitsrelevanten Anlagen arbeiten

Wie läuft das Security Appraisal ab?

1. Schritt: Selbsteinschätzung der Antragstellenden

Im Rahmen der Antragstellung sind zunächst standardisierte Fragen zu sicherheitsrelevanten Aspekten zu beantworten. Die Fragen sind im Ja-Nein-Fragen-Format formuliert. Sobald eine Frage mit Ja beantwortet wurde, müssen weitergehende Angaben gemacht werden, wie das Projekt die Sicherheitsrisiken mitigieren möchte. Dies kann beispielsweise Maßnahmen wie die Einstufung von Projektergebnissen mit entsprechend eingeschränkter Verbreitung, die Benennung eines *Project Security Officers* (PSO) oder die Einrichtung eines *Security Advisory Boards* umfassen. Ergänzende Informationen können dabei sowohl im Antragsformular selbst als auch in Form zusätzlicher Anhänge eingereicht werden. Für bestimmte, als sicherheitsrelevant gekennzeichnete Ausschreibungsthemen stellt das *Funding & Tenders Portal* hierfür bereits spezifische Vorlagen zur Verfügung, die verpflichtend auszufüllen sind.

Eine kurze Einführung findet sich hier. Generell gilt: Schätzen Sie Ihre Projektinhalte möglichst realistisch ein.

Eine Hilfe findet sich in diesem Dokument: *How to handle security-sensitive projects*

2. Schritt: Das eigentliche Security Appraisal

Alle Anträge, bei denen die Antragstellenden eine der Fragen zur Sicherheit mit JA angekreuzt haben, werden durch die Europäische Kommission geprüft. Die Europäische Kommission kann Informationen nachfordern. Es werden sowohl das Projekt als auch die vorgeschlagenen Sicherheitsmaßnahmen geprüft. Wird die Selbsteinschätzung bestätigt, wird der Antrag in die *Security Scrutiny* aufgenommen. Projektanträge aus Cluster 3 gehen direkt in die *Security Scrutiny*.

3. Schritt: Security Scrutiny

Ziel der *Security Scrutiny* ist die Prüfung des Geheimschutzbedarfes und in der Konsequenz die Formulierung von Auflagen für das Projekt sowie Einschränkungen oder Änderungen am Projekt. Die Prüfung wird durch die Sicherheitsbehörden der am möglichen Projekt beteiligten Mitgliedstaaten durchgeführt. Sie erfolgt auf Grundlage der von den Antragstellenden eingereichten Unterlagen, und zwar einschließlich des gegebenenfalls verpflichtend auszufüllenden Anhangs „Sicherheit“. Das Ergebnis bildet sich im jeweils projektspezifischen *Security Framework* ab, das die Gesamtheit der Sicherheitsanforderungen beschreibt. Es sind folgende Ergebnisse möglich:

- Genehmigung ohne Auflagen
- Genehmigung mit Auflagen (z. B. Vorgabe von Klassifizierung/Restriktionen für Ergebnisse und Zugriffe)
- Keine Genehmigung, da die Inhalte zu sicherheitskritisch für eine Förderung sind
- Der letzte Fall tritt sehr selten ein. Auflagen müssen entweder vor der Unterschrift des *Grant Agreements* oder während der Projektlaufzeit erfüllt werden.

Wichtig:
Der Prüfprozess hat keinen Einfluss auf die wissenschaftliche Evaluation der Projekte.

Was ist unter einem Security Framework im Kontext sicherheitsrelevanter Forschungsprojekte zu verstehen?

Das *Security Framework* bezeichnet den konzeptionellen Rahmen aller sicherheitsrelevanten Anforderungen. Es ist somit kein einheitliches oder standardisiertes Dokument. Vielmehr hängen die im Rahmen des *Security Frameworks* erforderlichen Dokumente vom Förderprogramm ab. In EU-Projekten (Horizont Europa und EVF) ist für gewöhnlich eine Übersicht aller eingestuften *Deliverables*, ein *Programme Security Instruction* (PSI) (ab VS-NfD/EU RESTRICTED) sowie ein *Security Aspects Letter* (SAL) als Zusammenfassung aller Sicherheitsanforderungen für die Unterzeichnung des Zuwendungsvertrags erforderlich. Alle Maßnahmen, die gefordert werden, müssen im Projekt umgesetzt werden.

8. ERGEBNISSE, INTELLECTUAL PROPERTY UND PUBLIKATIONEN

Wie werden IP-Rechte im Rahmen sicherheitsrelevanter Forschung geregelt?

Das hängt davon ab, ob es sich um Auftragsforschung (Cyberagentur, Ressortforschung BMVg) oder Forschungsförderung per Zuwendung (BMFTR, Horizont Europa, EVF) handelt. Bei Forschungsförderung (Zuwendungen) verbleiben die IP-Rechte bei den Geförderten, die sie erschaffen. Der Konsortialvertrag regelt Näheres.

Bei Auftragsforschung werden die Regelungen zum Verbleib der IP-Rechte individuell im Vertrag zwischen Auftraggeber und Auftragnehmer festgelegt. Dabei kann der Auftraggeber einerseits die Inhaberschaft bzw. die ausschließlichen Nutzungsrechte am geistigen Eigentum erwerben.
Andererseits können auch offenere Vereinbarungen mit einer Inhaberschaft an Schutzrechten für den Auftragnehmer und unbeschränkten, nicht ausschließlichen Nutzungsrechten für den Auftraggeber festgelegt werden; möglich ist auch eine gemeinsame Inhaberschaft an gewerblichen Schutzrechten. Bei diesen offeneren Regelungen verbleiben dem Auftragnehmer Möglichkeiten zur eigenen Nutzung, Verwertung und Weiterentwicklung der IP-Rechte. Darüber hinaus können vertraglich weitergehende Nutzungsbeschränkungen vereinbart werden, etwa dass die Verwertung durch den Auftragnehmer auf den EWR-Raum oder auf NATO-Staaten beschränkt ist.

Im Rahmen sogenannter *Pre-Commercial Procurement* Verfahren (PCP-Verfahren), wie sie beispielsweise von der Cyberagentur oder im Rahmen von Horizont Europa eingesetzt werden, ist der Erwerb von Inhaberschaft oder ausschließlicher Nutzungsrechte an IP durch den öffentlichen Auftraggeber nicht möglich. Daher wird in diesen Fällen auf die genannten offeneren Regelungsmodelle zurückgegriffen.

Im Falle einer Einstufung von Ergebnissen gelten unabhängig von der Zuordnung der daran bestehenden IP-Rechte die Regelungen des Geheimschutzes weiter und schränken so die tatsächlichen Nutzungs- und Verwertungsmöglichkeiten des Auftragnehmers ein. Beispielsweise steht dann die Weitergabe von Ergebnissen an Dritte unter dem Zustimmungsvorbehalt des VS-Herausgebers, auch wenn sie IP-rechtlich gestattet wäre (z. B. bei Inhaberschaft des Auftragnehmers an den Schutzrechten).

Werden Erfindungen aus sicherheitsrelevanter Forschung als Patente oder Gebrauchsmuster angemeldet, kann es außerdem zu einer Geheimhaltungsanordnung nach §§ 50 ff. Patentgesetz durch das Deutsche Patent- und Markenamt (DPMA) kommen (dies ist ein sehr seltener Fall). Voraussetzung ist, dass es sich um ein Staatsgeheimnis nach § 93 Strafgesetzbuch handelt. Dabei handelt es sich nicht um den Regelfall. Die Anforderungen für das Vorliegen eines solchen Staatsgeheimnisses entsprechen weitgehend denen der Einstufung GEHEIM oder höher (EU SECRET oder höher). Die Einstufung selbst ist formal ein unabhängiges Verfahren, wird aber im Regelfall parallel laufen. In diesem Fall ist eine Weiterverfolgung von Patent- oder Gebrauchsmusteranmeldungen außerhalb Deutschlands nicht oder nur unter Auflagen möglich.

Welche Auswirkungen hat sicherheitsrelevante Forschung auf die Veröffentlichung von Forschungsergebnissen und welche Regelungen sind dabei zu beachten?

Bei der Förderung durch Zuwendungen hängen die Regelungen vom Fördergeber ab. Bei Horizont Europa gibt es häufig keinerlei Beschränkungen, während beim EVF zumeist die Zustimmung des Fördergebers (durch den *Project Officer*) nötig ist (häufigster Fall).

Sofern es sich bei sicherheitsrelevanter Forschung um *Deliverables* oder Projektbestandteile handelt, die als Verschlusssache eingestuft sind, ist eine Veröffentlichung der Ergebnisse grundsätzlich ausgeschlossen und strafbewehrt (seltener Fall). Im Falle einer Geheimhaltungsanordnung durch das DPMA (siehe vorherige Frage) unterbleibt die sonst gesetzlich vorgeschriebene Veröffentlichung einer Patentanmeldung durch das DPMA.

Im Rahmen sicherheitsrelevanter Auftragsforschung, die nicht als Verschlusssache eingestuft ist, hängt die Möglichkeit einer Veröffentlichung vom jeweiligen Einzelfall ab. Bei der Beauftragung von Forschung durch die Cyberagentur muss jede Veröffentlichung individuell beantragt und durch die Cyberagentur genehmigt werden. Dabei ist zu beachten, dass das Verfahren regelmäßig eine gewisse Zeit in Anspruch nimmt, sodass besonders kurzfristige Veröffentlichungen (z. B. innerhalb von 2-3 Tagen), etwa die Einreichung eines Abstracts für eine Konferenz, nicht immer möglich sind.

Diese Genehmigungspflicht ist darüber hinaus im Besonderen zu beachten, wenn die Publikation der Ergebnisse eine Voraussetzung für die wissenschaftliche Qualifikation der Forschenden, etwa im Rahmen einer Promotion, ist. Die Cyberagentur genehmigt die deutliche Mehrheit der Publikationsanfragen. Es kann aber dazu kommen, dass einzelne Anfragen aus sicherheitsrelevanten Gründen abgelehnt werden.

Es lässt sich also sagen: Die Möglichkeiten zur Veröffentlichung von Forschungsergebnissen hängen maßgeblich von der Art des Projekts sowie von sicherheitsbezogenen Vorgaben und vertraglichen Regelungen ab. Grundsätzlich lassen sich **drei Konstellationen** unterscheiden:

Erstens können Forschungsergebnisse ohne Einschränkungen veröffentlicht werden, sofern keine sicherheitsrelevante Einstufung oder vertragliche Beschränkung vorliegt. Dies ist bei der Mehrzahl der Projekte der Fall.

Zweitens können Veröffentlichungen genehmigungspflichtig sein, etwa, wenn Projekte oder einzelne Ergebnisse sicherheitsrelevant sind oder entsprechenden vertraglichen Auflagen unterliegen. In diesen Fällen ist eine Veröffentlichung häufig möglich, bedarf jedoch der vorherigen Prüfung und Freigabe durch den Fördergeber oder Auftraggeber. Dabei kann es auch vorkommen, dass einzelne Ergebnisse veröffentlicht werden dürfen, während andere Projektbestandteile amtlich eingestuft bleiben.

Drittens kann eine Veröffentlichung in Einzelfällen vollständig ausgeschlossen sein, insbesondere bei Auftragsforschung mit entsprechenden vertraglichen Vorgaben oder bei als Verschlusssache eingestuften Inhalten. Während ein vollständiger Veröffentlichungsausschluss bei öffentlich geförderten Projekten in der Regel nicht vorgesehen ist, kann er im Rahmen von Auftragsforschung vorkommen.