



 Bundesministerium
Finanzen

AUSSCHREIBUNG 2026
EINREICHFRIST: 26.02.2027, 12:00 UHR

KIRAS/K-PASS AUSSCHREIBUNG 2026

AUSSCHREIBUNGSLEITFADEN



IMPRESSUM

Eigentümer, Herausgeber und Medieninhaber

Bundesministerium für Finanzen (BMF)
Johannesgasse 5, 1010 Wien

Programmverantwortung KIRAS/K-PASS

Bundesministerium für Finanzen (BMF)
Sektion VI - Bergbau
Stabsstelle für Sicherheitsforschung und Technologietransfer
Radetzkystraße 2, 1030 Wien

Programmabwicklung KIRAS/K-PASS

Österreichische Forschungsförderungsgesellschaft mbH (FFG)
Bereich Thematische Programme
Sensengasse 1, 1090 Wien

Wien, Oktober 2026

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS.....	6
1 DAS WICHTIGSTE IN KÜRZE	7
2 MOTIVATION	9
2.1 Hintergrund KIRAS	9
2.2 Hintergrund K-PASS.....	9
2.3 Zielgruppen und Förderwerber	10
2.4 Die Möglichkeit der Klassifizierung	11
3 AUSSCHREIBUNGSSCHWERPUNKTE	12
3.1 KIRAS. Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für kooperative F&E-Projekte	12
3.1.1 Verbesserung klimatischer Bedingungen in den österreichischen Justizgebäuden durch bauliche und technische Maßnahmen unter dem Aspekt der Nachhaltigkeit	12
3.1.2 Resilienz als Wirtschafts-, Innovations- und Standortfaktor.....	14
3.1.3 Risikowahrnehmung und wirksame Kommunikation in radiologischen Notfällen	15
3.1.4 Resilienz kritischer Binnenwasserstraßen-Infrastruktur entlang der österreichischen Donau	16
3.1.5 Entwicklung von non- bzw. mikro-invasiver Biomonitoring Sensorik zur Ermittlung der kognitiven und mentalen Belastung von Einsatzkräften.....	17
3.1.6 Pilotierung Datenraum Kulturgüterschutz.....	18
3.1.7 Detektion und Vorhersage von gefährlichen alpinen Massebewegungen mittels Glasfaserinfrastruktur.....	19
3.2 KIRAS. Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für F&E-Dienstleistungen.....	20
3.2.1 Kompetenzorientierte Beschäftigungsinitiativen in Justizanstalten	20
3.2.2 Frauen im Strafvollzug: Bedingungen der Resozialisierung in der Justizanstalt Schwarza.....	21
3.2.3 Prozessbegleitung und Strafverfahren in Österreich aus Sicht gewaltbetroffener Kinder und Jugendlicher.....	21
3.2.4 Relevanz Neuartige Kernenergiesysteme (SMR/AMR): für die internationale Sicherheit und die Nichtverbreitung (Proliferation)	22
3.2.5 Ernährungsvorsorge in Österreich.....	23
3.2.6 Einflussfaktoren für unterschiedliche Kriminalitätsformen	24
3.2.7 Gemeinsam.Sicher/Community Policing als dritte Säule moderner Polizeiarbeit. Von der Repression über die Prävention hin zu bürgernahem Informationsaustausch	25
3.2.8 Rechtsextremer Antifeminismus	26

3.2.9	Gewaltschutzkompetenzen von Gesundheitsberufen: Ist-Analyse	27
3.2.10	TEAM-SICHER – Sicheres Training für effektive Teamkommunikation in der Krise	28
3.2.11	Zunehmender Fachkräftemangel als Bedrohung für die Aufrechterhaltung der kritischen und sicherheitspolitisch relevanten Infrastruktur in der Akutpsychiatrie: Ursachen, Auswirkungen sowie Handlungsspielräume, mit Fokus auf unfreiwillige Unterbringungen gemäß Unterbringungsgesetz (UbG).....	29
3.2.12	Schulische Antisemitismusprävention als Beitrag zu Sicherheit und demokratischer Resilienz	30
3.2.13	Geistige Landesverteidigung – Analyse und Aufbereitung von Studien und Angeboten für die Lehrpersonenbildung und für Schulen im Bereich demokratischer Resilienz	31
3.2.14	Verwundbarkeitsanalyse zu Weltraumrisiken	33
3.2.15	Resiliente Verkehrsinfrastruktur durch KI-gestützte Steigerung der Datenqualität und Dienstrobustheit am Nationalen Zugangspunkt	34
3.2.16	Nihilistisch-gewaltextremistische Online-Netzwerke (NVE) als sicherheitspolitische Herausforderung	35
3.2.17	Ideologisch geprägte Gemeinschaften und Kindeswohlgefährdung: strukturelle Risiken und institutionelle Handlungssicherheit.....	36
3.2.18	Robotische Systeme zur Unterstützung von Einsatzkräften bei Vegetationsbränden.....	38
3.2.19	Untersuchung der Einsatzmöglichkeiten von Künstlicher Intelligenz zur Erkennung von Sozialleistungsbetrug in bestehenden Datensätzen	39
3.2.20	Anreize und Rahmenbedingungen für die Förderung der lokalen Produktion von Arzneimitteln zur Stärkung der Versorgungssicherheit in Österreich und Europa	40
3.3	K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für kooperative F&E-Projekte	41
3.3.1	Automatisierte KI-gestützte Erhebung von Waldbrandflächen und relevanten Parametern	41
3.3.2	Mixed Reality Trainings zur professionellen Reaktion auf verbales & nonverbales Verhalten im Justizvollzug	42
3.3.3	KI-gestützte Erschließung heterogener akustischer Datenbestände für sicherheitsrelevante Anwendungen	42
3.3.4	Aufbau eines agentenbasierten Lieferketten-Lagebilds zur Erkennung kritischer Abhängigkeiten und zur Ableitung staatlicher Handlungsoptionen in Echtzeit.....	43
3.3.5	Schutz vulnerabler Gruppen vor suchtfördernden digitalen Anwendungen und sozialer Zusammenhalt.....	44
3.3.6	KI- beschleunigte Cyberangriffe: Neue Anforderungen an Incident Handling, Krisenmanagement und Cyber-Übungen in kritischen Infrastrukturen.....	45

3.3.7	Gewährleistung der Einsatzfähigkeit von kritischer Infrastruktur und ad-hoc Betrieben während Cyberattacken und Firewall-Umgehung.....	46
3.3.8	KI-gestützte Auswertung von Einsatzdaten und Einsatznachbereitung zum Betrieb einer Führungsunterstützung bei Leitstellen und Einsatzleitungen im Krisen- und Katastrophenfall.....	48
3.3.9	Detektion von Deepfakes und medialen Manipulationen in Bildern und Videos für polizeiliche Ermittlungen und Erfordernisse.....	49
3.3.10	Weiterentwicklung und Erweiterung der KI-gestützten Schuhspurensammlung	50
3.3.11	KI-basierte Datenanalyse von Videodaten	51
3.4	K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für F&E-Dienstleistungen	52
3.4.1	Souveräne Legal AI für sicherheitspolitisch sensible Bereiche der österreichischen Justiz	52
3.4.2	Digitale Abhängigkeit als Sicherheitsrisiko für die europäische Land- und Ernährungswirtschaft	53
3.4.3	Anti-Phishing-Schutzschild für Österreich – Konzeptstudie nach internationalen Vorbildern.....	54
3.4.4	Analyse des Einsatzes und der Auswirkungen von KI-Agents im kriminalpolizeilichen Aufgabengebiet	54
3.4.5	E-Government-Schutz, Cyber Crime und Digitale Forensik.....	55
3.4.6	Befähigung der Verwaltung: Sicheres Low-Code/No-Code und Vibe-Coding zur KI-gestützten Prozessautomatisierung in Fachabteilungen.....	56
3.4.7	Nationales föderiertes Datenökosystem für das Krisen- und Katastrophenmanagement.....	57
3.4.8	Resilienz sektorgekoppelter Energiesysteme gegen Kaskadeneffekte.....	58
3.4.9	Demokratische Resilienz und Informationsintegrität	59
3.4.10	Digitale Souveränität kritischer Infrastruktursysteme zum Schutz öffentlicher Sicherheit durch resilienzorientierte, modulare IT-Architekturen	60
3.4.11	Erhebung technischer und inhaltlicher Rahmenbedingungen für eine Fact-Checking-Anwendung mit Fokus auf migrationsbezogene und -relevante Themen und Inhalte.....	61
3.4.12	CyberSecSenior	61
3.5	KIRAS/K-PASS KMU Initiative Innovation AKUT	63
3.6	AT-DE Bilaterale Ausschreibung.....	64
4	INSTRUMENTE UND ANFORDERUNGEN	65
4.1	Kooperatives F&E-Projekt.....	65
4.1.1	Konsortien.....	65
4.1.2	Forschungskategorien	65
4.1.3	Verwertung	66
4.2	F&E-Dienstleistung.....	66

4.2.1	Allgemein	66
4.2.2	Bietergemeinschaften	66
4.2.3	Auflagen und Bedingungen durch Jury	67
4.2.4	Weitere Anforderungen und Vorgaben zur Einreichung von F&E-Dienstleistungen	67
5	AUSSCHREIBUNGSDOKUMENTE	68
6	FÖRDERUNGS-/FINANZIERUNGSENTSCHEIDUNG UND RECHTSGRUNDLAGEN	69
7	WEITERE INFORMATIONEN	70
7.1	Hinweise zum Kostenplan.....	70
7.2	Service FFG Projektdatenbank	70
7.3	Open Access Publikationen.....	70
7.4	Umgang mit Projektdaten – Datenmanagementplan	71
7.5	Weitere Förderungsmöglichkeiten der FFG	71
8	ANHANG: CHECKLISTE FÜR DIE ANTRAGSEINREICHUNG.....	72

TABELLENVERZEICHNIS

Tabelle 1: Instrumente und Ausschreibungsschwerpunkte.....	7
Tabelle 2: Beratungsmöglichkeiten	8
Tabelle 3: Ausschreibungsdokumente.....	69
Tabelle 4: Formalprüfungcheckliste.....	72

1 DAS WICHTIGSTE IN KÜRZE

Im Rahmen von **KIRAS/K-PASS** stehen für die kommende [Ausschreibung](#) 11 Millionen Euro zur Verfügung. Projektanträge sind bei der Österreichischen Forschungsförderungsgesellschaft (FFG) bis spätestens 26.02.2027 (Innovation AKUT bis 29.01.2027) einzubringen. Die Einreichung ist ausschließlich via [eCall](#) möglich und hat vollständig und rechtzeitig bis zum Ende der Einreichfrist zu erfolgen. Eine spätere Einreichung (nach 12:00 Uhr des genannten Tages) wird nicht mehr angenommen und führt automatisch zum Ausschluss aus dem Auswahlverfahren.

Tabelle 1: Instrumente und Ausschreibungsschwerpunkte

Förderungs-/ Finanzierungsinstrument	Kooperatives F&E Projekt	F&E- Dienstleistung	F&E- Dienstleistung KMU Initiative Innovation AKUT
Kurzbeschreibung	Kooperatives F&E Projekt Industrielle Forschung (IF) oder Experimentelle Entwicklung (EE), je nach Ausschreibungs- schwerpunkt	Erfüllung eines vorgegebenen Ausschreibungs- inhaltes	Innovatives Projekt mit KMU- Beteiligung, TRL 6-8
Schutz kritischer Infrastruktur (KIRAS)	Ja Siehe Kapitel 3.1	Ja Siehe Kapitel 3.2	Ja Siehe Kapitel 3.5
Cybersicherheit (K-PASS)	Ja Siehe Kapitel 3.3	Ja Siehe Kapitel 3.4	Ja Siehe Kapitel 3.5
AT-DE Bilateral (KIRAS)	Ja Siehe Kapitel 3.6	Nein	Nein
Beantragte Förderung in Euro	min. 100.000 bis max. 2 Mio.	max. 200.000 inkl. ev. Ust	max. 100.000 inkl. ev. Ust
Finanzierungsquote	nicht anwendbar	100%	100%
Förderungsquote	max. 85%	nicht anwendbar	nicht anwendbar
Laufzeit in Monaten	max. 24 (und 12 Monate max. kostenneutrale Fristerstreckung)	max. 24 (und 12 Monate max. kostenneutrale Fristerstreckung)	max. 12 (und ggf. kostenneutrale Fristerstreckung in Ausnahmefällen)
Kooperationserfordernis	ja	nein	ja
Sprache	Deutsch	Deutsch	Deutsch
Einreichfrist	26.02.2027	26.02.2027	29.01.2027
Zum Einreichportal	eCall	eCall	eCall

Tabelle 2: Beratungsmöglichkeiten

Name	Kontaktdaten	Beratung zum Thema
Christian Brüggemann, MLS	Tel.: +43577555071 E-Mail: christian.brueggemann@ffg.at	Allgemeine Einreichberatung
Jozef Janco, MSc.	Tel.: +43577555073 E-Mail: jozef.janco@ffg.at	Allgemeine Einreichberatung
Dr. Polina Wilhelm	Tel.: +43577555072 E-Mail: polina.wilhelm@ffg.at	Allgemeine Einreichberatung
Mag. Gabriela Baluszynska	Tel.: +43577556092 E-Mail: gabriela.baluszynska@ffg.at	Kostenfragen
Mag. Martin Hudecek	Tel.: +43577556091 E-Mail: martin.hudecek@ffg.at	Kostenfragen

Inhaltliche Beratungsgespräche allgemeiner Natur können auf Wunsch eines potenziellen Antragstellers geführt werden. Terminvereinbarungen sind bis 05.02.2027 in schriftlicher Form an sicherheit@ffg.at zu stellen.

Weiterführende Informationen:

- https://www.ffg.at/kiras_k-pass/ausschreibung-2026
- www.ffg.at/kiras
- www.kiras.at
- www.ffg.at/k-pass
- www.ffg.at/sicherheitsforschung
- www.ffg.at/kiras-k-pass-innovation-akut

Bitte beachten Sie:

Sind die Formalvoraussetzungen für eine Projekteinreichung entsprechend den Konditionen und Kriterien des jeweiligen Förderungs-/Finanzierungsinstruments nicht erfüllt und handelt es sich um nicht-behebbarer Mängel, wird das Förderungsansuchen bei der Formalprüfung aufgrund der erforderlichen Gleichbehandlung aller Förderungsansuchen ausnahmslos aus dem weiteren Verfahren ausgeschieden und formal abgelehnt.

Diversität in der Teamzusammensetzung

Divers aufgestellte Teams können aufgrund der Vielfalt und unterschiedlicher Perspektiven innovativer und produktiver sein. Eine Teamzusammensetzung, die Gender- und Diversitätsdimensionen berücksichtigt, kann für eine höhere Qualität der Projekte sowie der daraus entstehenden Forschungsergebnisse, Produkte und Dienstleistungen sorgen. Die Auswirkungen der Projektergebnisse auf Menschen werden dadurch mitgedacht, z.B. durch die Berücksichtigung verschiedener Bedürfnisse in der Nutzung oder Herstellung von Produkten. Unterschiedliche Blickwinkel, Erfahrungen, Weltanschauungen und Fähigkeiten können dazu beitragen, überzeugende Lösungen für Gesellschaft und Wirtschaft zu entwickeln.

Die FFG unterstützt Sie dabei mit Förderungen! Informationen dazu finden Sie auf der Website: https://www.ffg.at/gleichstellung#Foerdermoeglichkeiten_Vielfalt.

2 MOTIVATION

2.1 Hintergrund KIRAS

Das unter der Programmverantwortung des Bundesministeriums für Finanzen (BMF) stehende österreichische Sicherheitsforschungsförderprogramm „KIRAS“ (KIRAS leitet sich aus dem Griechischen ab und setzt sich zusammen aus den Worten kirkos (Kreis) und asphaleia (Sicherheit)). „Kreis“ ist in diesem Fall als integrativ zu verstehen, da im Rahmen des KIRAS- Programms alle Disziplinen und Dimensionen miteingeschlossen werden) unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der Sicherheit Österreichs und seiner Bevölkerung. Das BMF hat die Österreichische Forschungsförderungsgesellschaft (FFG) mit dem Programm- und Schirmmanagement für das KIRAS- Programm beauftragt. Das KIRAS-Programm hat einen eindeutigen und klaren zivilen Programmfokus.

Schwerpunkt der Förderaktivitäten ist der Schutz kritischer Infrastrukturen. Die Sektoren, die als kritische Infrastrukturen gelten, sowie die strategischen Ziele sind in der [KIRAS-Sonderrichtlinie](#) beschrieben. Zusätzlich werden innerhalb dieses generellen Schwerpunkts für jede Ausschreibung spezifische Forschungsschwerpunkte durch die sicherheitspolitisch verantwortlichen Ressorts festgelegt. Diese Spezifizierung erlaubt es Einreichern, zielgerichtet den aktuellen Bedarf anzusprechen.

Im Thema Sicherheit (KIRAS) werden grundsätzlich solche sicherheitsforschungsrelevanten Vorhaben gefördert, die inhaltlich nicht effektiv durch andere bestehende Förderinitiativen abgedeckt werden können (z.B. in den Themenbereichen Energie, Mobilität und Verkehr, Informations- und Kommunikationstechnologien, Produktion und Raumfahrt). Im Sinne einer umfassenden Umsetzung des Themenmanagements erfolgt eine Abstimmung nicht nur mit Forschungsprogrammen innerhalb des BMF, sondern mit allen im Lenkungsausschuss vertretenen Stakeholdern (Ministerien, Interessensvertretungen, FORWIT, u.a.).

KIRAS weist folgende Alleinstellungsmerkmale auf:

- Definition von Sicherheit als nationale Sicherheit
- Beforschung sicherheitspolitisch relevanter Vorhaben im zivilen und dual-use-Bereich
- der integrative, umfassende Ansatz
- die Einbeziehung von Bedarfsträgern der Sicherheitspolitik
- ein klarer Österreichbezug
- die zwingende projektbezogene Integration von GSK- Aspekten
- die Möglichkeit der Klassifizierung von Projekten.

2.2 Hintergrund K-PASS

Im Rahmen der „Österreichischen Sicherheitsklammer“ bietet das Programm KIRAS/ „Kybernet-Pass“ (im folgenden K-PASS), unter der Programmverantwortung des Bundesministeriums für Finanzen (BMF), eine Unterstützung für nationale Forschungsvorhaben mit dem Ziel der Erhöhung der digitalen Sicherheit Österreichs und seiner Bevölkerung.

K-PASS unterstützt österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien und der Gewinnung des erforderlichen Wissens, um die digitale Sicherheit Österreichs zu erhöhen und Wertschöpfung zu generieren. Ziel ist die Schaffung marktnaher Forschungsergebnisse zu digitaler Sicherheit für Sicherheitsanwender.

Der Schwerpunkt der Förderaktivitäten in K-PASS wird in der ersten Phase (2023-2027, in Anlehnung an das Europäische Forschungsrahmenprogramm Horizont Europa) in den folgenden Bereichen liegen:

- Sicherheit von „security“-relevanter Software
- Sicherheit von „security“-relevanter Hardware
- Schutz für IoT-Anwendungen und Netze
- Cyber Crime und Digitale Forensik
- E-Government-Schutz (inkl. Aufrechterhaltung des Vertrauens in der Bevölkerung)
- Steganografie und digitale Datenanalyse (z.B. Post-Quantenverschlüsselung)
- Der User als Teil der digitalen Dimension (inkl. Datensicherheit, Cyber-Stalking, Cyber-Mobbing)
- Sicherheit und Künstliche Intelligenz
- Hybride Bedrohungen
- Schutz für IKT-Systeme als „smarte“ kritische Infrastruktursysteme (z.B. autonome Mobilität, smarte Strom- und sonstige Versorgungsnetze) inkl. Resilienz, Versorgungssicherheit und Vertrauensüberprüfung (vor allem Themen für Breitbandausbau und 5G/6G-Netze).

Zusätzlich werden innerhalb dieses generellen Schwerpunkts für jede Ausschreibung spezifische Forschungsschwerpunkte durch die sicherheitspolitisch verantwortlichen Ressorts festgelegt.

Detaillierte Information finden Sie in der [K-PASS Sonderrichtlinie](#).

2.3 Zielgruppen und Förderwerber

KIRAS/K-PASS richtet sich an folgende Zielgruppen:

- Industrie- und Dienstleistungsunternehmen mit Unternehmensstandort oder Forschungsstätte in Österreich, sowie
- Forschungseinrichtungen, Forschende aus dem universitären und außeruniversitären Bereich, Fachhochschulen
- Österreichische öffentliche und private Bedarfsträger: Bedarfsträger sind öffentliche oder private Institutionen, die (Mit-)Verantwortung für die Gewährleistung von Sicherheit (im Sinne von „security“) als öffentliches Gut tragen und Bedarf an Ergebnissen der Sicherheitsforschung (Technologien, Studien, etc.) haben bzw. diese anwenden. Dazu zählen insbesondere:
 - Sicherheitspolitisch verantwortliche Bundesministerien („Bedarfsträger der Sicherheitspolitik“)
 - weitere Bundesministerien
 - Bundesagenturen
 - Bundes- und Landesbehörden
 - Städte und Gemeinden
 - Infrastrukturbetreiber
 - Blaulichtorganisationen
 - Vereine und Nicht-Regierungsorganisationen.

KIRAS/K-PASS wendet sich inhaltlich auch an Einrichtungen der österreichischen Bundesverwaltung. Diese Einrichtungen können zwar nicht als Förderungswerber auftreten, sind jedoch ermutigt, sich im Rahmen von Konsortialbildungen an Vorhaben im Rahmen von KIRAS/K-PASS zu beteiligen.

Förderwerber:

- Förderbar sind außerhalb der Bundesverwaltung stehende juristische Personen, Personengesellschaften oder Einzelunternehmen
- Natürliche Personen sind als Einreicher nur für das Instrument „F&E-Dienstleistungen“ zulässig.

2.4 Die Möglichkeit der Klassifizierung

Es besteht die Möglichkeit, einen Antrag auf Klassifizierung des Projektes zu stellen, wenn abzusehen ist, dass im Projekt mit klassifizierten Informationen gearbeitet werden soll. Klassifizierte Informationen sind Informationen, Tatsachen, Gegenstände und Nachrichten, die unabhängig von Darstellungsform und Datenträger eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen (siehe Informationssicherheitsgesetz und –Verordnung).

Für den Fall, dass der Antragsteller einen Antrag auf Klassifizierung stellt, wird dieser Antrag nach positiv bestandener Formalprüfung durch die FFG von der FFG über das BMF an die Verbindungspersonen zum Nationalen Sicherheitsrat (NSR) weitergeleitet, welche ihrerseits prüfen, ob das Projekt mit bestehenden oder geplanten Systemen kompatibel ist und ob es wirklich als ein klassifiziertes Projekt durchgeführt werden muss. Wenn die Verbindungspersonen zum NSR feststellen, dass der Klassifizierungsantrag zu Recht gestellt wurde, erfolgt eine Prüfung durch den Kontrollbeauftragten, ob der Antragsteller die Schutzmaßnahmen laut Informationssicherheitsverordnung (bauliche und personelle Maßnahmen) ergriffen hat. Ist dies nicht der Fall, muss der (Projekt-)Antrag abgelehnt werden.

Wird der Antrag auf Klassifizierung von den Verbindungspersonen zum Nationalen Sicherheitsrat (NSR) negativ beschieden, wird das Projekt wieder der FFG zugeleitet und kann nach Rücksprache mit dem Antragsteller dem weiteren (normalen) Begutachtungsverfahren unterworfen werden.

Der Projektantrag darf keinesfalls klassifizierte Informationen enthalten.

Bitte lesen Sie die Rechtsgrundlagen, insbesondere die Anforderungen an Personal und bauliche Maßnahmen, wie sie in der Informationssicherheitsverordnung dargelegt sind, eingehend. Sollte der Antrag als „klassifiziert“ eingestuft werden, die baulichen und personellen Anforderungen aber nicht vorhanden sein, muss das Projekt abgelehnt werden. Die Informationssicherheitsverordnung kann von der [KIRAS-Homepage](#) heruntergeladen werden.

3 AUSSCHREIBUNGSSCHWERPUNKTE

Das Vorhaben muss sich prioritär auf einen der in Folge beschriebenen Ausschreibungsschwerpunkte beziehen, kann aber auch mehrere dieser Schwerpunkte ansprechen. Bitte beachten Sie, dass die F&E-Dienstleistungen bis max. 200.000 Euro inkl. Ust. finanzierbar sind.

Um die zukünftige Einsatzfähigkeit von angewandten Forschungsideen zu erhöhen, wird den Antragstellern empfohlen, in den Projektanträgen zu beschreiben, wie die geltenden rechtlichen Rahmenbedingungen im beforschten Themengebiet aussehen. Weiters sollte dargelegt werden, ob und welche Rechtsvorschriften einer praktischen Umsetzung der Forschungsergebnisse entgegenstehen könnten bzw. welche Anpassungen in den Rechtsgrundlagen dies ermöglichen / vereinfachen würden. Die dazu erforderliche rechtliche Expertise kann sowohl von den Konsortialmitgliedern direkt als auch im Subauftrag in die Forschungsprojekte eingebracht werden.

Folgend sind die Ausschreibungsschwerpunkte aus sicherheitspolitischer Sicht beschrieben.

Bei den kooperativen F&E-Projekten ist am Ende eines jeden Schwerpunktes auf die Forschungskategorie (entweder „Industrielle Forschung“ oder „Experimentelle Entwicklung“) zu achten.

3.1 KIRAS. Schutz kritischer Infrastruktur.

Ausschreibungsschwerpunkte für kooperative F&E-Projekte

3.1.1 Verbesserung klimatischer Bedingungen in den österreichischen Justizgebäuden durch bauliche und technische Maßnahmen unter dem Aspekt der Nachhaltigkeit

Kontakt: Bundesministerium für Justiz (BMJ)

E-Mail: kiras@bmj.gv.at ; andreas.bednarek@bmj.gv.at

Die zunehmende sommerliche Überwärmung infolge des Klimawandels stellt österreichische Justizgebäude – insbesondere Gerichte und Justizanstalten – vor große Herausforderungen hinsichtlich Energieeffizienz, Aufenthaltsqualität, Gesundheitsschutz und Betriebssicherheit. Aufgrund ihrer architektonischen Vielfalt und ihren differenzierten Funktions- und Nutzungsbereichen – von denkmalgeschützten Altbauten bis zu funktionalen Neubauten, von öffentlich zugänglichen Räumen bis hin zu solchen der Sicherheitsverwahrung – fehlen bislang einheitliche, umsetzbare Lösungen für klimafitte Bestandsanpassung und nachhaltigen Neubau.

Das Projekt analysiert systematisch die typenspezifischen Anforderungen und Potenziale dieser Gebäude und ihre Funktions- und Nutzungsbereiche unter klimatischen, haustechnischen, sicherheitstechnischen und sozialen Gesichtspunkten. Neben Gebäudetypologien, Standortbewertungen und Nutzer:innenbefragungen wird ein technischer Versuchsaufbau in einem realen

Justizgebäude umgesetzt, der als „Laborumgebung im Feld“ fungiert. Dort werden bauliche, haustechnische und begrünende Maßnahmen unter kontrollierten Bedingungen auf Raumklima, Energieverbrauch und Nutzer:innenempfinden getestet. Monitoringdaten und begleitende soziologische Erhebungen liefern eine fundierte Evaluationsbasis.

Mittels typologischer Gebäudeanalysen, Standortbewertungen, Nutzerinnen- und Nutzer-Befragungen und interdisziplinärer Planungsworkshops werden konkrete Maßnahmen zur Reduktion sommerlicher Überwärmung entwickelt – etwa durch bauliche Anpassungen, passive Kühlstrategien, Begrünungen und haustechnische Lösungen. Besonderes Augenmerk gilt dabei den spezifischen Bedingungen des Strafvollzugs und der Resozialisierung, etwa durch die Integration von nutzbaren Begrünungssystemen durch Insassinnen und Insassen.

Ziel ist die Entwicklung eines evidenzbasierten, übertragbaren Maßnahmen- und Empfehlungskatalogs für klimafitte Justizgebäude. Dieser unterstützt das Bundesministerium für Justiz bei der strategischen Planung, Sanierung und dem zukunftsfähigen Betrieb seiner Liegenschaften – wirtschaftlich, ökologisch und sozial nachhaltig.

Darüber hinaus sind die Erkenntnisse auch auf andere sicherheitsrelevante Infrastrukturen wie Bildungseinrichtungen, Gesundheitseinrichtungen oder Bauten des BMLV übertragbar.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erarbeitung von Handlungsempfehlungen zur Implementierung
- Wie unterscheiden sich die architektonischen, haustechnischen und klimatischen Rahmenbedingungen österreichischer Justizgebäude in Bezug auf sommerliche Überwärmung und Energieeffizienz?
- Welche typenspezifischen Maßnahmen lassen sich zur klimafitten Sanierung und zum nachhaltigen Neubau unter Berücksichtigung von Sicherheit und Denkmalschutz entwickeln?
- Wie wirken sich bauliche, haustechnische und begrünende Maßnahmen auf das thermische Komfortempfinden sowie die physische und psychische Gesundheit von Bediensteten und Insassinnen und Insassen aus?
- Inwiefern kann die Gestaltung der Innen- und Außenbereiche zur Resozialisierung von Insassinnen und Insassen beitragen und gleichzeitig sicherheits- sowie betriebsorganisatorischen Anforderungen gerecht werden?
- Wie lassen sich technische, soziale und sicherheitspolitische Erkenntnisse in einem standardisierten, übertragbaren Empfehlungskatalog bündeln, um zukünftige Sanierungen und Neubauten strategisch zu unterstützen? Welche baulichen und haustechnischen Maßnahmen eignen sich zur Reduktion sommerlicher Überwärmung in österreichischen Justizgebäuden mit heterogener Bausubstanz?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.1.2 Resilienz als Wirtschafts-, Innovations- und Standortfaktor

Kontakt: Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET)

E-Mail: POST.III9a-25@bmwet.gv.at

**Kontakt: Bundesministerium für Land- und Forstwirtschaft, Klima- und
Umweltschutz, Regionen und Wasserwirtschaft (BMLUK)**

E-Mail: abt-28@bmluk.gv.at

Kontakt: Austrian Business Agency (ABA)

E-Mail: r.tritscher@aba.gv.at

Die Weltwirtschaft wandelt sich von einer relativ stabilen, regelbasierten Ordnung zu einer fragmentierten Landschaft mit zahlreichen geopolitischen Risiko-Hotspots. Für Österreich bedeutet dies, dass Sicherheit und die aktive Absicherung kritischer Ressourcen und Versorgungswege zur Grundvoraussetzung wirtschaftlicher Handlungsfähigkeit werden. In diesem Kontext wird Resilienz zu einem zentralen Wirtschafts-, Innovations- und Standortfaktor. Resilienz umfasst dabei mehr als klassische Absicherung, Risikomanagement, Versorgungssicherheit und Krisenmanagement. Gefordert ist die Fähigkeit von Unternehmen, Innovationsökosystemen und Standorten, Krisen und externe Schocks nicht nur zu überstehen, sondern sich aktiv anzupassen, zu erneuern und zu transformieren. Treiber des wachsenden Anpassungsdrucks sind multiple externe Schocks, geopolitische Spannungen und geoökonomische Fragmentierung, Lieferkettenrisiken, strategische Abhängigkeiten, stärkere Umwelteinflüsse, technologische Umbrüche (Digitalisierung, Automatisierung, KI) sowie Fachkräftemangel und demografischer Wandel.

Zentrale Quelle moderner Resilienz ist Innovationsfähigkeit: Sie erlaubt es, Technologien und Prozesse anzupassen, in verwandte Technologiefelder zu diversifizieren, neue Geschäftsmodelle und Märkte zu erschließen und Abhängigkeiten zu verringern. Ergänzend schaffen Rechtsstaatlichkeit, Rechtssicherheit, eine verlässliche Verwaltung, Klimaaspekte sowie weiche Standortfaktoren wie Kultur und Lebensqualität das notwendige Umfeld. Besonders wichtig ist Resilienz für kritische Infrastrukturbetreiber und alle systemrelevanten Unternehmen samt Zulieferern, da sie die Versorgungssicherheit der Bevölkerung gewährleisten.

Resilienz wird damit sowohl zu einem entscheidenden Argument für die Standortwahl internationaler Konzerne als auch zu einem operativen Vorteil österreichischer Unternehmen in Krisensituationen.

Daraus leitet sich ein umfangreicher Forschungsbedarf ab:

- zur optimalen Kombination von Standortbedingungen, zur empirischen Bestimmung wirksamer Resilienz- und Innovationsfaktoren, zur regionalen Differenzierung, zur Wirksamkeit und Stärkung dieser Faktoren, zur Wahrnehmung von EU-Resilienzansätzen in Unternehmen, zur Foresight-basierten Szenarienbildung, zur Entwicklung eines umfassenden Resilienzbildes (inkl. technologischer Souveränität und strategischer Autonomie) sowie zur Konzeption geeigneter Indikatoren und Monitoringsysteme für innovationsbasierte Resilienz.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.1.3 Risikowahrnehmung und wirksame Kommunikation in radiologischen Notfällen

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK), Abteilung V/8 - Strahlenschutz, AL DI Christina Raith

E-Mail: christina.raith@bmluk.gv.at

Radioaktivität wird in Österreich als besonders bedrohliches Risiko wahrgenommen, wobei diese Wahrnehmung nur begrenzt mit tatsächlichen Expositionen korreliert und stark durch Emotionen, Unsicherheit sowie Informations- und Kommunikationsprozesse geprägt ist. Diese spezifische Risikowahrnehmung beeinflusst maßgeblich den Umgang der Bevölkerung mit sicherheitsrelevanten Entscheidungen, sowohl in akuten Situationen als auch bei langfristigen Fragestellungen. Bestehende Leitlinien zur Risiko- und Krisenkommunikation formulieren grundlegende Prinzipien (Transparenz, Konsistenz und frühzeitige Information), liefern jedoch wenig empirische Evidenz zur Effektivität spezifischer Kommunikationskanäle. Insbesondere die Reichweite und Wirksamkeit digitaler Medien sowie die Dynamik von Fehlinformation („Infodemic“), aber auch nationale Besonderheiten, sind bisher unzureichend untersucht.

Der Schwerpunkt adressiert zwei Kernfragen: die Analyse der Reichweite und die Wirksamkeit unterschiedlicher Informationskanäle bei der Vermittlung von Handlungsanweisungen sowie die Untersuchung psychosozialer Auswirkungen radiologischer Bedrohungsszenarien.

Ziel ist die Entwicklung einer empirisch fundierten Grundlage für wirksame, zielgruppenspezifische und vertrauensbildende Risiko- und Krisenkommunikation zur Bewältigung des Ereignisses, zu Stärkung der gesellschaftlichen Resilienz und zur Reduktion psychosozialer Belastungen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse der Reichweite und Wirksamkeit unterschiedlicher Informationskanäle (z. B. Internet, Behördenwebsites, Social Media, klassische Medien, direkte Kommunikation) zur effektiven Verbreitung von Handlungsanweisungen auf Basis vorhandener empirischer Daten und vergleichbarer Anwendungsfälle mit dem Ziel einer evidenzbasierten Bewertung von Reichweite, Vertrauen, Verständlichkeit und Handlungseffektivität
- Analyse psychosozialer Auswirkungen radiologischer Freisetzungsszenarien unterschiedlicher Schweregrade, insbesondere in der Akutphase, unter Berücksichtigung von Wahrnehmung, Vertrauen und Verhalten verschiedener Bevölkerungsgruppen, wobei sozio-demografische Unterschiede und Informationsverhalten gezielt zu berücksichtigen sind
- Agentenbasierte Modellierung zur simulationsgestützten Untersuchung von Kommunikationsstrategien, Informationsdynamiken und deren Auswirkungen auf gesellschaftliches Verhalten und Entscheidungsprozesse.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung)

3.1.4 Resilienz kritischer Binnenwasserstraßen-Infrastruktur entlang der österreichischen Donau

Kontakt: Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)

Ing. Christian Stangl-Brachnik, BA MA; Mag. Nieves Kautny, MSc

E-Mail: Christian.Stangl-Brachnik@bmimi.gv.at ; nieves.kautny@bmimi.gv.at

Der Donau-Schwarzmeer-Korridor ist eine der strategisch bedeutendsten multimodalen Verkehrsachsen der EU. Er verbindet das TEN-T-Kernnetz Rhein-Donau mit ost- und südosteuropäischen Regionen sowie mit globalen Seehandelsrouten und führt dabei durch oder grenzt an zehn Länder – sowohl EU- als auch Nicht-EU-Staaten, die Ukraine befindet sich aktuell im Kriegszustand. Über den Korridor werden zu einem großen Teil Agrarprodukte (Getreide, Körner, Ölsaaten, etc.) aber auch Baustoffe (Erze) und metallurgische Produkte (Stahl) transportiert; der Containertransport hat in den letzten Jahren ebenfalls zugenommen. Dadurch ist der Donau-Schwarzmeer-Korridor signifikant für die Versorgung mit kritischen Gütern in Österreich, aber auch für die gesamte Europäische Union. Die Häfen und Schleusen sowie Logistikzentren und Verkehrsmanagement-Systeme entlang der österreichischen Donau zählen zu der kritischer Binnenwasserstraßen-Infrastruktur. Diese sind gleichzeitig vielfältigen Bedrohungen ausgesetzt, etwa:

- Technische Störungen und Unfälle (z.B. Fehlfunktionen, Havarien),
- Geplante oder ungeplante Ausfälle der Versorgung oder der Infrastruktur selbst (z.B. Strom, IKT, Wartungen, Niedrig- oder Hochwasser)
- Cyberangriffe (z.B. Ransomware)
- Hybride Bedrohungen (z.B. Sabotage oder Insider-Threats).

Mit dem Resilienz kritischer-Einrichtungen-Gesetz (RKEG), mit dem Österreich die CER-Richtlinie (2022/2557) in nationales Recht umsetzt, wurde ein Rahmen zur Stärkung der Resilienz dieser Infrastrukturen geschaffen. Allerdings fehlen bislang sektorspezifische und praxisnahe Ansätze, um die Anforderungen des RKEG auf die besonderen Rahmenbedingungen kritischer Binnenwasserstraßen-Infrastruktur anzuwenden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Infrastrukturelemente entlang der österreichischen Donau können als kritische Binnenwasserstraßen-Infrastruktur betrachtet werden?
- Welche dieser Infrastrukturelemente stellen verletzbare Knotenpunkte dar, deren Ausfall erhebliche Auswirkungen auf Schifffahrt, Logistik und Versorgungssicherheit hätte?
- Welche natürlichen, technischen und menschengemachten Bedrohungen können auf kritische Binnenwasserstraßen-Infrastruktur einwirken?
- Welche Lieferketten (Branchen, Produkte, Unternehmen) sind auf die Binnenwasser-Infrastruktur, bzw. Hafeninfrastruktur angewiesen?
- Wie können Abhängigkeiten zwischen den Infrastrukturen und anderen Sektoren identifiziert, skizziert und im Hinblick auf Kaskadeneffekte analysiert werden?
- Welche kompensierenden Maßnahmen helfen etwaige (Teil-)Ausfälle dieser Knotenpunkte zu begegnen?
- Wie ist der Umsetzungsstand des RKEG im Bereich der kritischen Binnenwasserstraßen-Infrastruktur entlang der österreichischen Donau zu bewerten?

- Welche Herausforderungen und Auswirkungen ergeben sich für die österreichischen Donauhäfen und die Binnenwasserstraßen-Infrastruktur durch das Resilienz-kritischer-Einrichtungen-Gesetz (RKEG)?
- Wie kann ein sektorspezifisches Bewertungs- und Methodenset zur Risiko- und Resilienzanalyse für Betreiber kritischer Binnenwasserstraßen-Infrastruktur konzipiert werden?
- Wie kann ein Risiko- und Resilienz-Framework aussehen, das die Anforderungen des RKEG für Betreiber kritischer Binnenwasserstraßen-Infrastruktur praxisnah umsetzt?
- Wie können geeignete Capacity-Building- und Trainingsformate entwickelt, pilotiert und evaluiert werden, um Betreiber und Behörden bei der Umsetzung des RKEG sowie bei der Stärkung der Resilienz kritischer Binnenwasserstraßen-Infrastruktur nachhaltig zu unterstützen?
- Welche Strategien und Handlungsoptionen für Unternehmen eignen sich, um Störungen durch z.B. Transportumleitungen, Verlagerung auf alternative Transportmittel (LKW, Bahn) zu umgehen? Wie können die Auswirkungen dieser Gegenstrategien im Sinne von Zeitverlusten, Kostendifferenzen quantifiziert werden?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung)

3.1.5 Entwicklung von non- bzw. mikro-invasiver Biomonitoring Sensorik zur Ermittlung der kognitiven und mentalen Belastung von Einsatzkräften

Kontakt: Bundesministerium für Landesverteidigung (BMLV)

E-Mail: sicherheitsforschung@bmlv.gv.at

Kontakt: Österreichische Bundesfeuerwehrverband (ÖBFV)

E-Mail: science@feuerwehr.or.at

Einsatzkräfte stehen regelmäßig unter enormer körperlicher und mentaler Belastung. Dabei sind nicht nur hohe Temperaturen und körperliche Anstrengungen von Interesse, sondern insbesondere die Belastung durch Stress, Wahrnehmungen und Überforderung. Aktuell werden hauptsächlich Eye-Tracking Methoden für die Feststellung der kognitiven/mental Belastung verwendet. Im gegenständlichen Schwerpunkt soll der Fokus auf die Entwicklung von Konzepten und Technologien gelegt werden, die einen effektiven, sofortigen und kontinuierlichen Vor-Ort-Nachweis von Biomarkern im Blut (zB Cortisol, Melatonin) ermöglichen. Der entsprechende Lösungsansatz muss im Einsatz unter der entsprechenden Schutzkleidung/Ausrüstung getragen werden können, ohne Einschränkungen für die überwachte Person zu bewirken. Die Ergebnisse müssen nicht in Echtzeit zur Verfügung stehen, aber lückenlose, engmaschige Daten liefern (mehrere Datenpunkte pro Minute).

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie kann eine mobile, engmaschige, mikroinvasive Datensammlung (idealerweise non-invasiv) der Biomarker von Personen unter Einsatzbedingungen umgesetzt werden.

- Welche Sensorgenauigkeit und -Stabilität ist erreichbar und sind die mobilen Messungen im Vergleich zu klassischen Messungen im Labor aussagekräftig genug?
- Welche Grundlagendaten (z.B. Ruhewerte, Basislinie) müssen bei den Probanden und Probandinnen verfügbar sein/erhoben werden, um die Nutzbarkeit der Blutparameter zu gewährleisten?
- Ergibt sich anhand der definierten Biomarker eine verbesserte Betrachtung des Belastungs- bzw. Gesundheitszustands?
- Können Korrelationen zwischen den Biomarkern und niederschwelliger zu messenden Körpervitaldaten hergestellt werden?
- Ist eine robuste und einfache Handhabung der Sensorik möglich bzw. werden durch die Ausrüstung oder durch die Einsatzszenarien bzw. definierten Arbeitsabläufe (intensive Bewegungen, etc.) die Messgenauigkeit in ihrer Qualität beeinträchtigt?
- Sind die Sensorsysteme in ihrer Anwendung sowohl organisatorisch als auch technisch in den Ablauf von Einsatzkräften integrierbar?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.1.6 Pilotierung Datenraum Kulturgüterschutz

Kontakt: Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport (BMWKMS), Mag.a Hannah Leodolter: Gruppe IV/B, Stabsstelle Kunstrückgabe und Gedenkkultur

E-Mail: hannah.leodolter@bmwkms.gv.at

Kontakt: Bundeskanzleramt (BKA), MinR Dr. Erich Albrechtowitz, Leitung Chief Digital Officer (CDO) (Gruppe I/C: Digitalisierung und Informationsmanagement)

E-Mail: erich.albrechtowitz@bka.gv.at

Aktuell werden sowohl national wie auch international große Anstrengungen unternommen, bestehende Kulturgüterinventare zu digitalisieren und somit in moderne Kulturgüterinventardatenbanken zu transformieren, da diese im Falle von Schadensereignissen (z.B. technische Defekte, Naturkatastrophen, Vandalismus, Terror und Krieg) von größter Bedeutung für die nachfolgende Krisen- und Katastrophenbewältigung sind. Ein schneller, sicherer und standardisierter internationaler Datenaustausch zu Kulturgütern zwischen den verschiedenen involvierten Akteuren (Kultureinrichtungen, Behörden, Einsatzorganisationen) ist daher von absoluter Wichtigkeit. Darüber hinaus ist eine Integration in das staatliche Krisen- und Katastrophenmanagement, eine Standardisierung digitaler Inventarisierungsansätze sowie sicheres, resilientes und souveränes Datenmanagement unerlässlich. Es besteht daher ein konkreter Bedarf an anwendungsorientierten Lösungen, um den Kulturgüterschutz wirksam in bestehende Sicherheitsstrukturen zu integrieren und die Nutzung digitaler Technologien im Einsatzfall zu ermöglichen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Konzept zur Integration des Schutzes von Kulturgütern in das staatliche Krisen- & Katastrophenmanagement als Teil der kritischen Infrastruktur zur Schaffung kultureller Schutzräume
- Erarbeitung eines Konzepts zur standardisierten, digitalen Inventarisierung betroffener Kulturgüter
- Erarbeitung eines Maßnahmenkatalogs zur Sicherstellung der Datensicherheit und Datensouveränität und Anforderungen an entsprechende digitale Schutzräume
- Prototypische Lösung und technische Umsetzung eines Datenraums für den Kulturgüterschutz
- Validierung der entwickelten Ansätze und Prototypen mit verantwortlichen Stakeholdern
- Konzeption von Schulungsmodulen für Kultureinrichtungen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.1.7 Detektion und Vorhersage von gefährlichen alpinen Massebewegungen mittels Glasfaserinfrastruktur

Kontakt: Amt der steiermärkischen Landesregierung

E-Mail: abteilung14@stmk.gv.at ; hans-peter.wind@stmk.gv.at

Kontakt: KELAG

E-Mail: Jennifer.Stippich@kelag.at

Mit steigender Erderwärmung steigen die Risiken von Massebewegungen, Fels- und Bergstürzen im alpinen Raum. Die Folgen können nicht nur in Siedlungsgebieten, sondern z.B. auch bei einem Bergsturz in einen Speichersee, katastrophal sein. In diesem Vorhaben soll die Möglichkeit mittels faseroptischer akustischer Sensorik (fibre optic acoustic sensing - FOAS) Massenbewegungen ohne Installation von zusätzlicher Sensorik im Feld über weite Entfernungen in Echtzeit zu detektieren und zu lokalisieren, erforscht werden. Die FOAS-Technologie bietet die Möglichkeit bestehende Glasfasernetze (d.h. Lichtwellenleiter LWL-Kabel) als weit verteiltes Sensornetzwerk für die empfindliche Detektion von Erschütterungen zu nutzen. Zunehmend im alpinen Raum vorhandene LWL-Kabel, in Tälern aber auch zu technischen Installationen am Berg, wie Seilbahnen oder Schneekanonen, könnten, unter Benutzung seismischer Algorithmen, als weit verzweigtes Netzwerk für die Überwachung von Massebewegungen auch in einiger Entfernung (Größenordnung Kilometer) von LWL-Kabeln benutzt werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie empfindlich ist die FOAS-Technologie in Bezug auf die Detektion von Felsstürzen in 1 bis 10 km Entfernung vom Kabel?
- Wie stark beeinflussen/stören andere, dem LWL-Kabel nahen Vibrationsquellen (üblicherweise Auto- oder Zugsverkehr) die Detektions- und Lokalisierungsqualität von weiter entfernten Massebewegungen?
- Welche seismischen Methoden existieren für Rekonstruktion der Richtung und Stärke von eintreffenden seismischen Erregungen, wie z.B. durch Felsstürze erzeugt, und wie lassen sich diese (von Signalen aus Geophonen) auf FOAS-Signale übertragen?

- Wie weit ist der Ausbau von LWL-Leitungen im alpinen Raum vorangeschritten und könnten diese Leitungen auch für ein FOAS-Überwachungssystem für die Detektion und Lokalisierung von Massebewegungen genutzt werden?
- Kann die Auswertung von zeitlich synchronisierten Signalen aus 2 oder mehreren LWL-Kabeln, die z.B. in zwei Nachbartälern verlegt sind, die Detektion und Lokalisierung verbessern?
- Welche technologischen Möglichkeiten existieren in der Zukunft, die derzeit noch teuren optoelektronischen FOAS-Interrogator-Geräte kostengünstiger für einen flächendeckenden Einsatz im alpinen Raum zu machen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.2 KIRAS. Schutz kritischer Infrastruktur.

Ausschreibungsschwerpunkte für F&E-Dienstleistungen

3.2.1 Kompetenzorientierte Beschäftigungsinitiativen in Justizanstalten

Kontakt: Bundesministerium für Justiz (BMJ)

E-Mail: kiras@bmj.gv.at ; andreas.bednarek@bmj.gv.at

Die Reintegration der Straftäterinnen und Straftäter in die Gesellschaft ist aus Sicht des BMJ das oberste Ziel des Strafvollzugs. Daher ist das Fördern von Fähigkeiten, die für ein selbstbestimmtes und straffreies Leben notwendig sind, ein wesentliches Vollzugsziel in österreichischen Justizanstalten. Hierzu zählen z. B. die Fähigkeiten zur Selbstkontrolle und Selbstorganisation, wie der Umgang mit Konflikten oder Geld. Eine systematische Aufarbeitung dieser Fähigkeiten und Fertigkeiten, die eine flexible und adäquate Umsetzung von Beschäftigungsmaßnahmen, wie Aus- und Weiterbildung sowie Freizeitgestaltung in österreichischen Justizanstalten ermöglicht, existiert bisher nicht.

Daher sollen in einem entsprechenden Projekt die benötigten Fähigkeiten und Fertigkeiten der Insassinnen und Insassen mittels sozialwissenschaftlicher Methodik erhoben und in einem themenspezifischen Überblick, der didaktische sowie institutionelle regionale und nationale Umsetzungsmöglichkeiten beinhaltet, gegeben werden. Die gewonnenen Erkenntnisse sollen den Justizanstalten eine effizientere und effektivere Identifikation und passende Umsetzung von Initiativen ermöglichen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation von Fähigkeiten und Fertigkeiten, die Insassinnen und Insassen benötigen, um ein selbstbestimmtes und straffreies Leben führen zu können
- Analyse passender Umsetzungsmöglichkeiten, um diese Fähigkeiten und Fertigkeiten innerhalb von Justizanstalten weiterzuentwickeln
- Erhebung relevanter regionaler und nationaler Ansprechpartnerinnen und Ansprechpartner, die Justizanstalten bei der Förderung entsprechender Kompetenzen unterstützen können.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.2 Frauen im Strafvollzug: Bedingungen der Resozialisierung in der Justizanstalt Schwarzau

Kontakt: Bundesministerium für Justiz (BMJ)

E-Mail: kiras@bmj.gv.at ; andreas.bednarek@bmj.gv.at

Straffällig gewordene Frauen führen in der Kriminal- und Justizforschung ein Schattendasein. Die Situation der Frauen wird in der Justizforschung zwar manchmal mitberücksichtigt und mit Männern verglichen, jedoch wurde in der Vergangenheit die Forschung speziell zu Frauen im Strafvollzug stark vernachlässigt. Wenn Frauen ins Zentrum der Justizforschung gerückt werden sollen, dann vor allem mit der Begründung, dass sie aufgrund besonderer Erlebnisse auch andere Bedürfnisse in den Strafvollzug mitbringen. Dazu zählen Substanzabhängigkeiten (Drogen, Alkohol) und mentale Folgeschäden, die aus unterschiedlichen Marginalisierungs- und Misshandlungserfahrungen resultieren. Den Besonderheiten weiblicher Strafgefangener wird jedoch bei der Ausgestaltung des Vollzugs in Justizanstalten und in der Arbeit zur Resozialisierung mit Hilfs- und Behandlungsangeboten nur wenig Rechnung getragen. Diesen Mangel will das Projekt beheben.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie unterscheiden sich straffällige Frauen von straffälligen Männern hinsichtlich der begangenen Delikte, in der justiziellen Verfahrenserledigung und in der Sanktionierung von Straftaten?
- Wie können Vollzugauftrag und gesetzliche Vollzugsziele unter den betrieblichen – organisatorischen und personellen - Bedingungen in der Justizanstalt Schwarzau bestmöglich erfüllt werden?
- Welche Anstrengungen gibt es in der Justizanstalt Schwarzau, Frauen auf ein Leben ohne Kriminalität in Freiheit bereits während der Haft vorzubereiten? Wie gut gelingt das? Und welche Hindernisse treten bei der Umsetzung auf?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.3 Prozessbegleitung und Strafverfahren in Österreich aus Sicht gewaltbetroffener Kinder und Jugendlicher

Kontakt: Bundesministerium für Justiz (BMJ)

E-Mail: kiras@bmj.gv.at ; andreas.bednarek@bmj.gv.at

In Österreich haben Opfer vorsätzlicher Gewalttaten Anspruch auf kostenlose psychosoziale und juristische Prozessbegleitung. Psychosoziale Prozessbegleitung soll stabilisieren, informieren und durch das Verfahren begleiten; juristische Prozessbegleitung soll beraten, Opferrechte wahren und Ansprüche geltend machen. Für Kinder und Jugendliche – als besonders schutzbedürftige Gruppe – ist eine altersgerechte, geschlechtersensible und partizipative Begleitung entscheidend, die Sicherheit, Orientierung und Verfahrensverständnis schafft sowie Sekundärviktimisierung vorbeugt. Österreich verfügt über ein etabliertes Prozessbegleitungssystem mit klarer Rechtsgrundlage und bundesweiten Qualitätsstandards. Trotz dieser guten Voraussetzungen fehlt im deutschsprachigen Raum bislang eine systematische sozialwissenschaftliche Untersuchung der Sicht und Erlebnisweisen minderjähriger Gewaltopfer, die ein Strafverfahren durchliefen und Prozessbegleitung in Anspruch nahmen. Damit bleibt unklar, wie Kinder und

Jugendliche Verfahren und Prozessbegleitung tatsächlich erleben, welche Bedürfnisse sie formulieren und wo konkrete Verbesserungsbedarfe liegen. Das Projekt adressiert diese Forschungslücke und richtet den Blick explizit auf die Perspektiven der Betroffenen; es folgt den Ansätzen der Neuen Kindheitsforschung, Kinder und Jugendliche als Expert*innen ihrer Lebenswelt ernst zu nehmen.

- Wie erleben Kinder und Jugendliche die psychosoziale und juristische Prozessbegleitung und das Strafverfahren?
- Welche Unterstützungsangebote waren besonders hilfreich, welche Gespräche/Interventionen verunsichernd – und was wäre besser gewesen?
- Wie ordnen sie ihre Gerichtserfahrungen rückblickend ein, welches Verständnis von Recht/Unrecht beschreiben sie?
- Welche Wünsche und Bedürfnisse zur Stabilisierung und Stärkung ihres Sicherheitsgefühls äußern sie?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.4 Relevanz Neuartige Kernenergiesysteme (SMR/AMR): für die internationale Sicherheit und die Nichtverbreitung (Proliferation)

Kontakt: Bundesministerium für Frauen, Wissenschaft und Forschung (BMFWF)

E-Mail: stefan.hanslik@bmfwf.gv.at

Ausgangssituation/Motivation: Im europäischen forschungs-, energie- und industriepolitischen Kontext werden Small Modular Reactors (SMR) und Advanced Modular Reactors (AMR) verstärkt als Weiterentwicklungen der Kernenergie diskutiert. Einzelne Konzepte sind mit neuartigen Brennstoffen, höheren Anreicherungsgraden oder fortgeschrittenen Brennstoffkreisläufen verbunden und daher auch im Hinblick auf Proliferationsresistenz und latente militärische Fähigkeiten gesondert zu bewerten.

Aus österreichischer Sicht besteht daher Bedarf an einer unabhängigen, wissenschaftlich fundierten Bewertung der sicherheitsrelevanten Auswirkungen dieser Technologien auf die Weiterverbreitung und die internationale Sicherheit.

Zugleich wird ihre Entwicklung auch durch europäische Forschungs-, Ausbildungs- und Vernetzungsstrukturen geprägt. Insbesondere Maßnahmen im Rahmen von Euratom können zur Etablierung entsprechender Technologiepfade in Europa beitragen. Daraus ergeben sich aus österreichischer Sicht Fragen hinsichtlich unabhängiger Bewertungskompetenz, der Beobachtung technologischer Entwicklungen und der wissenschaftsbasierten Politikberatung.

Zielsetzung: Ziel des Vorhabens ist die Erarbeitung einer evidenzbasierten, interdisziplinären Bewertungsgrundlage zu den Auswirkungen neuartiger Kernenergiesysteme (SMR/AMR) auf die Weiterverbreitung und die internationale Sicherheit. Es soll die nationale Bewertungs- und Handlungsfähigkeit im europäischen Kontext stärken und eine Grundlage schaffen, um auch mittel- und langfristige Entwicklungen im europäischen Forschungs- und Kompetenzaufbau aus österreichischer Sicht sicherheitspolitisch und wissenschaftsstrategisch bewerten zu können.

Anwendungsbezug / Bedarfsträger: Die Ergebnisse sollen österreichische Behörden bei der evidenzbasierten Beurteilung neuartiger Kernenergiotechnologien unterstützen. Ein besonderer Anwendungsbezug besteht für das BMFWF im Bereich

wissenschaftsbasierter Politikberatung und Wissensaufbau für die Mitwirkungen in internationalen und europäischen, Gremien, sowie für das BMLUK in den Bereichen Umwelt-, Strahlen-, Krisen- und Vorsorgepolitik.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

Derzeit fehlt eine systematische, interdisziplinäre und auf die Anforderungen österreichischer Bedarfsträger zugeschnittene Gesamteinschätzung der sicherheitsrelevanten Auswirkungen von SMR- und AMR-Technologien.

Forschungsbedarf besteht insbesondere hinsichtlich:

- Einer vergleichenden Bewertung im europäischen Kontext relevanter SMR-/AMR-Konzepte im Hinblick auf Sicherheitsmerkmale, Brennstoffkreisläufe, Materialströme, technologischen Reifegrad sowie mögliche Missbrauchs- und Abzweigungsrisiken
- Einer Analyse möglicher Brennstoffkreisläufe, der dabei entstehenden Stoffströme und des technologischen Reifegrads verschiedener Abtrenntechnologien, insbesondere im Zusammenhang mit abzutrennenden Isotopengemischen
- Der Bewertung abgetrennter Stoffgemische im Hinblick auf ihre Eignung für den militärischen Einsatz sowie der Einordnung von Fragestellungen der Sicherung nuklearer Materialien, der Proliferationsresistenz und potenzieller Missbrauchs- und Abzweigungsrisiken der Identifikation von Wissenslücken, Unsicherheiten und regulatorischen Herausforderungen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.5 Ernährungsvorsorge in Österreich

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK), Abteilung II/8 – Lebensmittel- und Ernährungssysteme

E-Mail: abt-28@bmluk.gv.at

Kontakt: Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET)

E-Mail: POST.III9a-25@bmwet.gv.at

Die Versorgung mit landwirtschaftlichen Erzeugnissen und insbesondere die Ernährungsvorsorge ist eine zentrale Herausforderung, die im Rahmen von Klimawandel, Extremwetterereignissen, Bevölkerungswachstum, Ressourcenknappheit und globalen Krisen betrachtet werden muss. Die letzte umfassende Studie in diesem Zusammenhang wurde 2015 veröffentlicht. Unter diesem Scherpunkt soll ein Überblick über den Status im Bereich der privaten Vorsorge und hinsichtlich der derzeitigen Situation in den Unternehmen entlang der Lebensmittelversorgungskette sowie der Versorgung landwirtschaftlichen Erzeugnissen geben. Ebenso wurde bislang noch keine spezifische Risikomatrix für die Lebensmittelversorgung in Österreich erstellt. Die Vorgaben der RKE-Richtlinie betrifft unter anderem auch Unternehmen aus dem Sektor landwirtschaftliche Erzeugnisse und Lebensmittel und verlangt auch hier weitreichende Anpassungen. Dieser Schwerpunkt soll an das KIRAS Projekt „Risiko und Krisenmanagement für die

Ernährungsvorsorge in Österreich (EV-A)“ aus 2015 anknüpfen, die dort gewonnenen Erkenntnisse berücksichtigen und in Beziehung zur aktuellen Situation setzen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation und Beschreibung jener Krisen- und Katastrophenszenarien, von denen eine wesentliche Gefährdung der Lebensmittelversorgungssicherheit, der Versorgung mit agrarischen Rohstoffen für die Industrie bzw. der Versorgungssicherheit von Waren gem. Lebensmittelbewirtschaftungsgesetz (LMBG) ausgeht
- Erstellung einer Risikomatrix für landwirtschaftliche Erzeugnisse und Lebensmittel inklusive Inputs und Vorleistungen
- Wesentliche Versorgungsströme für Lebensmittel in Österreich und Identifikation von Schlüsselunternehmen der gesamten Wertschöpfungskette von Futter- und Düngemittelerzeugung über Lebensmittelproduktion, -verarbeitung und -industrie, Lebensmittellogistik bis hin zu Verpackungen für Lebensmittel und Handel
- Identifikation von kritischer Infrastruktur im Bereich der Lebensmittelwertschöpfungskette
- Erhebung und Beschreibung der Ausprägung des vorhandenen betrieblichen Risiko- und Krisenmanagements in diesen Unternehmen
- Empfehlungen für die Erstellung von Kommunikationsplänen zwischen den wesentlichen Akteuren der kritischen Infrastruktur im Bereich lw. Erzeugnisse und Lebensmittelwirtschaft
- Erhebung und Darstellung der Bevorratungssituation in privaten Haushalten, im öffentlichen Bereich sowie bei Produktions-, Verarbeitungs- und Handelsunternehmen
- Erarbeitung von Empfehlungen und Konzepten zur Risikokommunikation für die Zielgruppen der Landwirt:innen, Unternehmen der Wertschöpfungskette sowie der breiten Öffentlichkeit.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.6 Einflussfaktoren für unterschiedliche Kriminalitätsformen

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Die Kriminalitätsforschung steht vor der Herausforderung, die vielschichtigen Ursachen und Muster kriminellen Verhaltens zu entschlüsseln. Das Verknüpfen von Daten aus verschiedenen gesellschaftlichen Bereichen ermöglicht es, Kriminalität als ein vielschichtiges Phänomen besser zu verstehen.

Mit 1. Juli 2022 nahm das Austrian Micro Data Center (AMDC) bei der Statistik Austria seinen Betrieb auf. Dadurch ergeben sich neue Möglichkeiten für die Register- und die Kriminalitätsforschung. Die Sammlung von Mikrodaten aus verschiedenen Quellen des AMDC ermöglicht, kriminelle Handlungen in Beziehung zu sozialen, ökonomischen und geographischen Faktoren zu setzen und so zu untersuchen, wie bestimmte Lebensbedingungen mit verschiedenen Kriminalitätsformen zusammenhängen.

Neue und umfassendere Erkenntnisse zu den Einflussfaktoren verschiedener Kriminalitätsformen können dazu beitragen, bestehende präventive und repressive Maßnahmen weiterzuentwickeln und neue Maßnahmen vorzuschlagen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Studie zu den rechtlichen Rahmenbedingungen (insbes. Zusammenwirken von DSGVO, FOG, Statistik Gesetz) für Registerforschung aus Perspektive der Ressortforschung (Nutzung von Registerdaten und AMDC unter Miteinbeziehung der Perspektive der inneren Sicherheit).
- Einschätzung der entsprechenden methodischen Möglichkeiten (bspw. synthetische Datensätze)
- Basierend auf den rechtlichen und methodischen Möglichkeiten sollen im Anschluss folgende Fragen betrachtet werden:
- Welche neuen Erkenntnisse über bekannte Faktoren und welche neuen Faktoren zu Kriminalität lassen sich durch die Verknüpfung von verschiedenen Datenquellen identifizieren?
- Inwiefern beeinflussen diese Faktoren verschiedene Kriminalitätsformen (z. B. Eigentumsdelikte, Gewaltverbrechen)?
- Wie stehen verschiedene identifizierte Einflussfaktoren auf das Risiko, Opfer oder Täterin und Täter einer kriminellen Handlung zu werden, in Bezug zueinander?
- Welche Handlungsoptionen können basierend auf den Erkenntnissen für bestehende präventive und repressive Maßnahmen, für neue Maßnahmen sowie zur Weiterentwicklung von Opferschutz und Strafverfolgung vorgeschlagen werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.7 Gemeinsam.Sicher/Community Policing als dritte Säule moderner Polizeiarbeit. Von der Repression über die Prävention hin zu bürgernahem Informationsaustausch

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

„GEMEINSAM.SICHER mit unserer Polizei“ blickt im Jahr 2026 auf eine zehnjährige Entwicklungsgeschichte zurück. Die Initiative folgt dem international bereits seit Jahrzehnten etablierten Ansatz des Community Policing und ist seit 2017 österreichweit in der polizeilichen Arbeit verankert. Community Policing ist als wesentlicher Bestandteil einer modernen, wirkungsorientierten und bürgernahen sicherheitspolizeilichen Grundaufgabe zu verstehen. Neben der Verhinderung und Aufklärung von Straftaten bildet es eine dritte Säule zeitgemäßer Polizeiarbeit in Form von bürgernaher Polizeiarbeit.

Dabei geht es nicht nur um einzelne lokale Aktivitäten, sondern um einen gesamtstaatlich bedeutsamen Ansatz: Sicherheitsrelevante Entwicklungen sollen durch proaktiven Kontakt zur Bevölkerung, Behörden, Institutionen, etc. bundesweit frühzeitig wahrgenommen, strukturiert bewertet und gemeinsam mit zuständigen Stakeholdern bearbeitet werden.

Durch den proaktiven Kontakt mit der Bevölkerung und den Aufbau regionaler Netzwerke können sich abzeichnende Problemfelder, Konflikte und negative

Entwicklungen bereits frühzeitig erkannt werden, bevor daraus konkrete Straftaten, dauerhafte Kriminalitätsvorkommen oder wiederkehrende polizeiliche Einsätze entstehen. Wahrnehmungen aus der Bevölkerung, Erkenntnisse der Polizei und Informationen der beteiligten Institutionen werden zusammengeführt und ermöglichen dadurch ein umfassenderes Bild der jeweiligen Sicherheitslage.

Aus diesen Kontakten entstehen Sicherheitspartnerschaften, die einen kontinuierlichen Informations- und Erfahrungsaustausch gewährleisten. Regionalforen bieten darüber hinaus eine freiwillige und transparente Plattform, um unterschiedliche Stakeholder zusammenzubringen, konkrete Herausforderungen gemeinsam zu analysieren und abgestimmte Maßnahmen zu entwickeln. Ein mögliches Beispiel ist die Bearbeitung einer Suchtmittelproblematik im Umfeld eines Bahnhofs unter Einbindung der Polizei, der Gemeinde, des Verkehrsunternehmens, sozialer Einrichtungen, der Jugendarbeit und weiterer zuständiger Stellen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Herausforderungen gibt es in der Zusammenarbeit mit Sicherheitspartnern?
- An welchen internationalen Erkenntnissen und Erfahrungen kann sich die Initiative Gemeinsam.Sicher orientieren?
- Inwiefern trägt die sichtbare Präsenz des einzelnen Beamten in der Öffentlichkeit zum subjektiven Sicherheitsgefühl der Bevölkerung bei?
- Wie kann der Bekanntheitsgrad von Gemeinsam.Sicher erhöht werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.8 Rechtsextremer Antifeminismus

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Kontakt: Bundesministerium für Frauen, Wissenschaft und Forschung (BMFWF)

E-Mail: strategie.frauen@bmfwf.gv.at , catharina.haller-wank@bmfwf.gv.at

Rechtsextremer Antifeminismus verbindet klassische rechtsextreme Vorstellungen von Ungleichwertigkeit, ethnonationaler Homogenität und kultureller Bedrohung mit Feminismus, LGBTQI+-Rechte und sexueller Selbstbestimmung, die als Teil eines angeblichen Angriffs auf Familie, Nation, Männlichkeit, Tradition und „natürliche Ordnung“ konstruiert werden. Im rechtsextremen Spektrum dient Antifeminismus häufig als Brückenideologie. Er erleichtert den Anschluss an breitere Milieus, wie der sog. Manosphere, Tradwives und christlich-extremistische Subkulturen, die sich nicht zwingend selbst als rechtsextrem verstehen, aber für autoritäre, patriarchale, rassistische oder verschwörungsideologische Deutungen empfänglich sind.

Der Schwerpunkt fokussiert auf antifeministische und misogynie Erscheinungsformen, die rechtsextreme Ideologeelemente enthalten oder rechtsextremen Mobilisierungen Vorschub leisten. Ein besonderer Fokus liegt auf Frauen, sowohl als Opfer als auch als Akteurinnen, Influencerinnen, Aktivistinnen und Täterinnen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche antifeministischen Narrative, Feindbilder und Argumentationsmuster sind in rechtsextremen deutschsprachigen Online-Milieus besonders verbreitet?

- Wie werden Feminismus, Gleichstellung, LGBTQI+-Rechte, Migration, Familie, Mutterschaft, Männlichkeit und Nation in rechtsextrem-antifeministischen Diskursen im deutschsprachigen Raum miteinander verknüpft?
- Welche Akteurinnen, Plattformen, Kanäle, Influencerinnen und Netzwerke prägen die Verbreitung rechtsextremen Antifeminismus in Österreich und im deutschsprachigen Raum? Welche Rolle spielen weibliche deutschsprachige Influencerinnen und Aktivistinnen bei der Normalisierung, Übersetzung und Popularisierung rechtsextrem-antifeministischer Inhalte?
- Wie werden Frauen in diesen Milieus als Opfer, Feindbilder, Zielgruppen, Symbolfiguren und Täterinnen konstruiert?
- Welche Bedeutung haben Manosphere, Incels, Red-Pill-Milieus, Tradwife-Formate, Anti-Gender-Kampagnen und religiös-traditionalistische Submilieus für rechtsextreme Radikalisierung?
- Welche Strategien und Taktiken nutzen rechtsextreme Akteurinnen und Akteure, um antifeministische Inhalte online anschlussfähig zu machen, etwa über Humor, Memes, Popkultur, Gaming, Lifestyle oder persönliche Krisenerzählungen? Welche Rolle spielt generative KI dabei?
- Welche Schlussfolgerungen ergeben sich für Prävention, Verfassungsschutz und politische Bildung?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.9 Gewaltschutzkompetenzen von Gesundheitsberufen: Ist-Analyse

Kontakt: Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK), Abteilung VII/1

E-Mail: christina.dietscher@gesundheitsministerium.gv.at

Kontakt: Bundesministerium für Frauen, Wissenschaft und Forschung (BMFWF), Abteilung III/4

E-Mail: marie-theres.prantner@bmfwf.gv.at

Kontakt: Gesundheit Österreich GmbH (GÖG)

E-Mail: alexander.eggerth@goeg.at

Jede dritte Frau in Österreich erlebt im Erwachsenenalter körperliche und/oder sexuelle Gewalt, 16 % innerhalb einer intimen Partnerschaft. Im Gesundheitswesen tätigen Personen kommt beim Erkennen und bei der interdisziplinären Zusammenarbeit im Gewaltschutz eine Schlüsselrolle zu, da Gesundheitseinrichtungen häufig die erste Anlaufstelle für Betroffene von Gewalt sind. Wenn sichergestellt wird, dass sie hier die richtigen Fragen gestellt bekommen, adäquat versorgt und an die richtigen Stellen weiterverwiesen werden, kann dies dazu beitragen, eine weitere Gewalteskalation mit schwerwiegenden Folgen zu verhindern. Österreich hat sich durch die Ratifizierung der Istanbul Konvention dazu verpflichtet, Angehörige von Gesundheitsberufen entsprechend zu schulen, auch im Nationalen Aktionsplan zur Bekämpfung von Gewalt an Frauen und Mädchen 2025-2029 ist dem Gesundheitsbereich ein Kapitel gewidmet. Aktuell wird ein Standard für die zielführende Integration des Themas in die Ausbildungscurricula von Gesundheitsberufen erarbeitet. Um eine zukünftige Implementierung des Standards zu stärken, besteht ergänzend Bedarf für eine Ist-Analyse. Es braucht Informationen darüber, in welchem Ausmaß das Thema Gewalt bereits in Ausbildungscurricula

verankert ist, welche Kompetenzen in Bezug auf Gewaltschutz und Gewaltprävention Angehörige von Gesundheitsberufen mit in die Praxis bringen und wo etwaige Lücken bestehen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung zentraler Anforderungen in Bezug auf Gewaltschutz und Gewaltprävention in der Praxis
- Identifikation themenrelevanter Inhalte in bestehenden Ausbildungscurricula von Gesundheitsberufen
- Erhebung von im Rahmen der Ausbildungen erworbenen Gewaltschutzkompetenzen aus Sicht von Berufseinsteiger:innen
- Identifikation von etwaigem Anpassungsbedarf in Ausbildungscurricula zur Erreichung anforderungsspezifischer Kompetenzen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.10 TEAM-SICHER – Sicheres Training für effektive Teamkommunikation in der Krise

Kontakt: Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK), Sektion X/A/5

E-Mail: patrizia.theurer@gesundheitsministerium.at

Kontakt: Gesundheit Österreich GmbH (GÖG)

E-Mail: eva.potura@goeg.at

Eine leistungsfähige Gesundheitsversorgung in Krisen- und Katastrophensituationen hängt maßgeblich von Teamarbeit, Kommunikation und von Entscheidungen ab – insbesondere in dynamischen Lagen, an Schnittstellen und bei Übergaben unter Zeit- und Systemdruck. Sicherheitskritische Ereignisse entstehen dabei häufig nicht primär durch mangelndes Fachwissen, sondern durch unklare Rollen und Verantwortlichkeiten, Hierarchiedynamiken sowie eingeschränktes Situationsbewusstsein. Hier setzen Crisis Resource Management (CRM) und Threat and Error Management (TEM) an: Sie bieten konkrete Werkzeuge, um unter Druck strukturierte Entscheidungsprozesse, effektive Kommunikation und ein geteiltes Lageverständnis zu fördern. Simulationszentren schaffen die Infrastruktur, um diese sicherheitsrelevanten Kompetenzen in realitätsnahen Settings zu trainieren. In Österreich existiert bereits eine wachsende Simulationslandschaft (u. a. MedUni Wien, WIGEV, OÖ-Gesundheitsholding, LGA NÖ – Hohegg, Medizinische Universität Graz). Die Integration von CRM- und TEM-Prinzipien in Trainingsdesign, Instruktion und Debriefing erfolgt jedoch bislang heterogen und ohne systematische Evaluation. Es fehlen damit belastbare evidenzbasierte Grundlagen für Qualitätsstandards, strukturierte Train-the-Trainer-Programme und eine nachhaltige, skalierbare Implementierung.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Ausgangspunkt ist die strukturierte Evaluierung ausgewählter Simulationszentren als sicherheitsrelevante Ausbildungsinfrastruktur, inkl. Strukturen, Curricula, Instruktor:innen-Qualifikationen mit Fokus auf CRM und TEM Inhalten

- Konzeption eines standardisierten, interprofessionellen CRM/TEM Train-the-Trainer-Lehrgangs.

Der Forschungsbedarf adressiert sicherheitskritische Situationen in Krisen und Katastrophen mit besonderem Fokus auf effektive Kommunikation in der Simulation.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.11 Zunehmender Fachkräftemangel als Bedrohung für die Aufrechterhaltung der kritischen und sicherheitspolitisch relevanten Infrastruktur in der Akutpsychiatrie: Ursachen, Auswirkungen sowie Handlungsspielräume, mit Fokus auf unfreiwillige Unterbringungen gemäß Unterbringungsgesetz (UbG)

Kontakt: Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK), Abteilungsleitung VI/4, Rechtsangelegenheiten Arzneimittel, Medizinprodukte, Apotheken, Krankenanstalten, übertragbare Krankheiten

E-Mail: claudia.steinboeck@gesundheitsministerium.gv.at

Kontakt: Bundesministerium für Justiz (BMJ), Abteilung I 1 Familien-, Personen- und Erbrecht

E-Mail: Ulrike.Toyooka@bmj.gv.at

Die Akutpsychiatrie ist integraler Bestandteil der kritischen Infrastruktur von Krankenanstalten. Sie gewährleistet die fachgerechte Behandlung psychisch kranker Menschen, die aufgrund ernstlicher und erheblicher Selbst- oder Fremdgefährdung nach dem UbG angehalten werden müssen. Bei der Reduktion von Gefährdungspotenzial kommt ihr eine bedeutende präventive Wirkung zu. Sie trägt dadurch zum Schutz der Patient:innen, des Personals und der Bevölkerung bei.

Aktuelle Krisen und Katastrophen erhöhen psychische Belastungen in der Bevölkerung und damit den Bedarf an psychiatrischer Akutversorgung, der zunehmende Personalmangel verschärft der die Situation. Bereits jetzt führen Nachbesetzungsschwierigkeiten, Einschränkungen der Regelversorgung sowie Betten- und Stationssperren zu Versorgungsengpässen. Dies kann höhere Krankenstände beim Personal, Qualitätsverluste in der Versorgung sowie eine Zunahme von Aggression, Gewalt und Zwangsmaßnahmen in einem menschenrechtlich und sicherheitspolitisch sensiblen Bereich nach sich ziehen. Das UbG regelt eine zentrale Schnittstelle zwischen Gesundheitswesen und öffentlicher Sicherheit. Die Funktionsfähigkeit der Akutpsychiatrie ist für angrenzende Systeme wie die extramurale Versorgung, Gerichte, den Maßnahmen- und Strafvollzug sowie Sicherheitskräfte elementar. Eine Überlastung kann verfrühte Entlassungen und damit sicherheitsrelevante Auswirkungen auf die Bevölkerung zur Folge haben. Trotz hoher Relevanz fehlen vertiefende Erkenntnisse zu den Ursachen personeller Engpässe, deren Auswirkungen auf die psychiatrische Akutversorgung sowie zu wirksamen Strategien zur Aufrechterhaltung einer fachgerechten, interdisziplinären und menschenrechtsorientierten Versorgung unter herausfordernden Personalbedingungen. Solche Erkenntnisse leisten einen zentralen Beitrag zum Schutz kritischer Versorgungsstrukturen sowie zur Sicherheit von Personal, Patient:innen, Angehörigen und Bevölkerung.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Untersuchung der Ursachen von Personalengpässen und Fachkräftemangel in der Akutpsychiatrie sowie deren multiperspektivische Auswirkungen auf die psychiatrische Akutversorgung insbesondere auf Unterbringungen und die Anwendung von Zwangsmaßnahmen gemäß UbG.
- Erhebung und Aufbereitung von Beispielen guter Praxis zur Gewährleistung einer fachgerechten Versorgung im Kontext von Personalengpässen in der (Akut)Psychiatrie inkl. Use Cases
- Ableiten von Umsetzungsempfehlungen zur Aufrechterhaltung und zum Schutz einer qualitativ hochwertigen Akutversorgung sowie zur Prävention und Reduktion von Eskalationen, Aggressionen und Zwangsmaßnahmen - in Situationen anhaltender oder temporärer Personalengpässe.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.12 Schulische Antisemitismusprävention als Beitrag zu Sicherheit und demokratischer Resilienz

Kontakt: Bundesministerium für Bildung (BMB), Mag. Barbara Schrotter, Abt. III/8
E-Mail: barbara.schrotter@bmb.gv.at

Die Nationale Strategie gegen Antisemitismus – NAS 2.0 bildet einen klaren Regierungsauftrag Maßnahmen zur Prävention von Antisemitismus zu setzen. Im Kapitel „Bildung. Resilienz“, Maßnahme 9, sind Forschungsprojekte zur schulischen Unterrichtspraxis vorgesehen. In Österreich gibt es bisher nur wenige qualitative Forschungen zu Holocaust Education und Antisemitismusprävention im Unterricht.

Das zweijährige Projekt „Antisemitismus in der Schule – Perspektiven von Betroffenen und Case Management Strategien“ wurde 2025 erfolgreich abgeschlossen und hat erstmals die Sichtweise jüdischer Schülerinnen und Schüler an öffentlichen Schulen in Österreich auf antisemitische Erlebnisse und Erfahrungen sowie auf den „alltäglichen“ Antisemitismus im Schulalltag erhoben. Die Ergebnisse zeigen eine Zunahme des Israelbezogenen Antisemitismus, insbesondere nach dem Hamas-Anschlag im Oktober 2023, sowie die anhaltende Präsenz des „traditionellen“ Antisemitismus. Auf Basis der Projektergebnisse wurden Handlungsstrategien für Schulen in Form einer Handreichung erarbeitet, die Case Management Strategien für die reaktive Intervention im Klassenzimmer und im Schulkontext bereitstellt.

Die Projektergebnisse und die daraus resultierenden Empfehlungen wurden mehrfach in unterschiedlichen bildungsrelevanten Kontexten verschiedenen Gruppen von Stakeholdern (Lehrende, Vertreter und Vertreterinnen diverser Schulen/Schultypen, der PHs und des Schulqualitätsmanagements, etc.) präsentiert und mit diesen diskutiert. Dabei wurde seitens verschiedener Gruppen von Stakeholdern mehrmals darauf hingewiesen, dass diese reaktiven Strategien zwar sehr hilfreich wären, aber weitere empirische Forschung nötig sei, um Antisemitismusprävention und Holocaust Education im Schulalltag zu unterstützen.

Angesichts steigender antisemitischer Vorfälle (siehe auch Jahresbericht 2025 der Antisemitismus Meldestelle der IKG), die auch den Bildungsbereich betreffen und eine besondere Sicherheitsgefahr insbes. für jüdische Schüler:innen darstellen, rückt die tatsächliche Behandlung des Themas im Unterricht daher verstärkt in den Fokus.

Dabei ist in Hinblick auf Sicherheit und demokratische Resilienz die Wirkung der Unterrichtsqualität auf Prävention und Schutz zu diskutieren. Ein neues Forschungsprojekt würde diese Lücke schließen und könnte nachhaltig zur Verbesserung der Unterrichtsqualität sowie zur Sicherheit jüdischer Schüler:innen beitragen. Methodologische Überlegungen und Erfahrungen ähnlicher Studien in Deutschland sprechen für eine getrennte Betrachtung von Antisemitismus und Rassismus. Entsprechend trennt auch die Fundamental Rights Agency der EU (FRA) ihre empirischen Studien nach Diskriminierungsformen; eigene Studien zu Antiziganismus, Rassismus, Antisemitismus.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung wie Lehrpersonen Unterricht zu aktuellen Formen des Antisemitismus gestalten; Analyse wie diese Ansätze in Lehrpläne integriert werden können
- Untersuchung der Rolle von Lehr- und Lernmaterialien, sowie Fort- und Weiterbildungen; Erforschung, wie Ansätze der Prävention und Intervention im schulischen Kontext sinnvoll ineinandergreifen
- Untersuchung welche didaktischen Konzepte in welchen Unterrichtsfächern und thematischen Kontexten (historisch, aktuelle Konflikte, ethische Fragestellungen, gruppenbezogene Menschenfeindlichkeit) Antisemitismus thematisieren
- Auswertung von Best-practise-Beispielen aus Ländern mit ausgebauter qualitativer Unterrichtsforschung (z.B. Schweiz).

Neben Beantwortung der Forschungsfragen sollen anwendungsorientierte Empfehlungen für Lehrpersonen erarbeitet werden, die für die schulische Praxis zur Verfügung stehen und zur Stärkung der Sicherheit und gesellschaftlichen Resilienz beitragen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.13 Geistige Landesverteidigung – Analyse und Aufbereitung von Studien und Angeboten für die Lehrpersonenbildung und für Schulen im Bereich demokratischer Resilienz

Kontakt: Bundesministerium für Bildung (BMB), AL Anna Katharina Obenhuber

E-Mail: anna.obenhuber@bmb.gv.at

Kontakt: Bundesministerium für Landesverteidigung (BMLV)

E-Mail: sicherheitsforschung@bmlv.gv.at

Die Geistige Landesverteidigung (GLV) ist neben der militärischen, der wirtschaftlichen und der zivilen Landesverteidigung Teil der Umfassenden Landesverteidigung (Bundesverfassung Art. 9a). Damit unterstützt die GLV im Rahmen der Politischen Bildung und Demokratiebildung die Vermittlung demokratischer Werthaltungen und eines umfassenden Bewusstseins für die Sicherstellung von staatlicher Souveränität, der in der Bundesverfassung verankerten Bürger- und Menschenrechte und einer bewussten Wahrnehmung der österreichischen Neutralität. Im Lichte der aktuellen globalen Krisen und kriegsähnlichen Auseinandersetzungen sowie der zunehmenden Gefährdung des Rechtsstaats durch die Verbreitung von Desinformation durch soziale Medien und KI leistet die GLV einen Beitrag zum Verständnis der umfassenden nationalen Sicherheitspolitik und den Bedingungen einer demokratischen und resilienten Gesellschaft.

Im österreichischen Bildungssystem ist die GLV im Fachlehrplan „Geschichte und Politische Bildung“ der 8. Schulstufe ("Umfassende Landesverteidigung und Bundesheer") verankert. Zudem finden sich auch in anderen Unterrichtsfächern und in anderen Schulstufen Anknüpfungspunkte.

Die Zielsetzungen des Regierungsprogramms 2025-2029 im Bereich der GLV stellen den Schutz der „wehrhaften Demokratie“ und die „Stärkung des Rechtsstaates“ in den Vordergrund. Wesentliche Forderungen umfassen die Sicherung der liberalen Demokratie, die Förderung von Medienkompetenz, die Bekämpfung von Extremismus, Rassismus und Antisemitismus sowie die Stärkung demokratischer Grundwerte im gesamten Bildungssystem. Die Stärkung der Demokratiebildung und GLV an Österreichs Schulen ist daher Teil der aktuellen Maßnahmen im Bildungsbereich.

Im Rahmen dessen bestehen bereits mehrere Kooperationen mit dem BMLV und anderen Ministerien sowie auf Ebene der Bildungsdirektionen, der Pädagogischen Hochschulen (PH) und Universitäten sowie der Einsatz von Informationsoffizieren an Schulen. Weitere wichtige Impulse werden durch die Einführung neuer Unterrichtsfächer zur Stärkung der demokratischen Kompetenzen von Kindern und Jugendlichen sowohl in der Sekundarstufe I („Demokratie, Kommunikation und Konfliktlösung“ SJ 2029/2030) als auch der Sekundarstufe II („Medien und Demokratie“ in der AHS-Oberstufe sowie weitere Fächer in der Berufsbildung SJ 2027/2028) in den kommenden Jahren gesetzt.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

Das Verständnis und Vorwissen von Schülerinnen und Schülern und Lehrkräften im Bereich der GLV wurden in den letzten beiden Jahren im "SEEDS - Security Education by Empowering Democratic Strength"-Projekt beforscht. Die Ableitungen aus diesem KIRAS-Projekt und die genannten aktuellen Entwicklungen sollen berücksichtigt werden:

- Nutzung und Aufbereitung von bestehenden bzw. zukünftiger nationaler und europäischer/internationaler Studien zu Politischer Bildung und Demokratiebildung in Hinblick auf Erkenntnisse betreffend die GLV/ULV sowie Ableitung von Empfehlungen
- Evaluierung und Weiterentwicklung der im Rahmen des SEEDS-Projektes erstellten Praxismodule und der Online-Ressourcensammlung im Bereich GLV und Identifikation von Anknüpfungspunkten zu weiteren Webseiten, Plattformen mit Angeboten zu Politischer Bildung/Demokratiebildung.
- Beforschung und Evaluierung der Bildungsangebote von PH und Universitäten im Bereich der Lehrpersonenbildung zur GLV bzw. zu GLV-relevanten Themen
- Beforschung und Evaluierung der weiteren Angebote zur GLV, die sich an Schulen und Lehrpersonen richten
- Erstellung einer Gesamtstrategie zur erfolgreichen Implementierung der GLV/ULV im Bildungssystem inkl. Erfassung der europäischen Dimension und Anknüpfungsmöglichkeiten an Initiativen europäischer Institutionen
- Identifizierung der möglichen Beiträge der GLV zur Nationalen Strategie gegen Antisemitismus (NAS 2.0) und dem Nationalen Aktionsplan gegen Rechtsextremismus (NAP-REX)
- Identifikation relevanter Stakeholder im Bereich der GLV und Erarbeitung eines Kommunikationskonzepts

- Berücksichtigung der Heterogenität schulischer Realitäten in einer von Migration und weiteren demografischen Disparitäten (Stadt/Land) geprägten Gesellschaft und Ableitung von Empfehlungen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.14 Verwundbarkeitsanalyse zu Weltraumrisiken

Kontakt: Bundesministerium für Landesverteidigung (BMLV)

E-Mail: sicherheitsforschung@bmlv.gv.at

Kontakt: Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)

E-Mail: nieves.kautny@bmimi.gv.at

Die gesellschaftliche wie staatliche Abhängigkeit von Weltraumservices wächst sowohl im zivilen als auch im militärischen Sektor kontinuierlich an. Parallel dazu vervielfältigen sich die Bedrohungsszenarien im Weltraum hinsichtlich Quantität und Qualität. Durch den technologischen Fortschritt stehen diese Kapazitäten zudem zunehmend auch nicht-staatlichen Akteuren zur Verfügung. Diese Kombination aussteigender systemischer Abhängigkeit und wachsenden Bedrohungen erhöht das Risiko für die gesamtstaatliche Resilienz im Weltraumbereich maßgeblich.

Die ressortübergreifende Analyse umfasst sowohl aktuelle als auch zukünftige Abhängigkeiten staatlicher Funktionen und kritischer Infrastrukturen von Weltraumsystemen. Insbesondere zu untersuchen sind die spezifischen Verwundbarkeiten, die durch den potenziellen Ausfall oder die Einschränkung von Diensten wie Satellitenkommunikation, Positionierung, Navigation, Zeitdiensten sowie Erdbeobachtung entstehen. Ziel ist die Schaffung eines Lagebildes hinsichtlich spezifischer gesamtstaatlicher Verwundbarkeiten gegen Weltraumbedrohungen und die Identifikation konkreter Handlungsempfehlungen für die Risikomitigierung, um ein präventives Krisenmanagement sowie eine risikoadaptierte Planung zu gewährleisten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche kritischen staatlichen Funktionen und kritische Infrastruktur ist besonders von Weltraumservices abhängig?
- Welche Weltraumbedrohungen und Weltraumrisiken sind besonders hervorzuheben?
- Wie würden sich unterschiedliche Ausfallszenarien von Weltraumservices auf kritische staatliche Funktionen und kritische Infrastruktur auswirken?
- Welche Souveränitätsanforderungen können zivil/gesamtstaatlich sowie militärisch identifiziert werden?
- Welche strukturellen und prozessualen Empfehlungen könnten kurz-, mittel- und langfristig die größten Risiken mitigieren?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.15 Resiliente Verkehrsinfrastruktur durch KI-gestützte Steigerung der Datenqualität und Dienstrobustheit am Nationalen Zugangspunkt

Kontakt: AustriaTech – Gesellschaft des Bundes für technologiepolitische Maßnahmen GmbH

E-Mail: damaris.gruber@austriatech.at

Kontakt: Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)

E-Mail: krima@bmimi.gv.at

Hintergrund: Österreichische Umsetzung der IVS-Richtlinie

Die EU-IVS-Richtlinie (2010/40/EU) und die zugehörigen Delegierten Verordnungen (z. B. SSTP, SRTI, RTTI und MMTIS) bilden den rechtlichen Rahmen für die Bereitstellung von Verkehrsdaten. In Österreich erfolgt die Umsetzung gemäß dem novellierten IVS-Gesetz über den Nationalen Zugangspunkt (NAP, www.mobilitaetsdaten.gv.at) sowie über die nationale Stelle. Während **NAPCORE** auf EU-Ebene Regelwerke und Verfahren standardisiert, liegt die operative Prüfung der Datenqualität und Einhaltung der Delegierten Verordnungen bei den nationalen Stellen. Diese müssen sicherstellen, dass Datenanbieter die regulatorischen Vorgaben einhalten, was derzeit einen hohen manuellen Aufwand bedeutet.

Herausforderung: Grenzen bestehender Validatoren und Sicherheitsanforderungen

Der aktuelle Ansatz zur automatisierten Prüfung stützt sich oft auf statische Validatoren, die Datenformate gegen Schemata prüfen. Erfahrungsgemäß sind solche Tools jedoch schnell veraltet, wartungsintensiv und erfassen nicht die inhaltliche Qualität oder Konsistenz der Daten. Zudem gibt es derzeit keine strukturierte Übersicht über existierende KI-Tools, die für diese spezifischen Fragestellungen nutzbar wären. Eine zentrale Herausforderung für den KI-Einsatz ist darüber hinaus die **Datensicherheit**: Da es sich bei den zu prüfenden Daten um sensible Unternehmensdaten handelt, ist die Nutzung von „Public Cloud“-KI-Lösungen ausgeschlossen. Es bedarf einer isolierten, sicheren Umgebung. Es ist davon auszugehen, dass es keine fertigen „Off-the-Shelf“-KI-Lösungen gibt; vielmehr ist eine enge Zusammenarbeit mit KI-Entwickler:innen erforderlich.

Zielsetzung: Sichere KI-Analyseumgebung für resiliente IVS-Dienste

Der Schwerpunkt zielt auf die Entwicklung einer maßgeschneiderten, sicheren KI-Analyseumgebung am österreichischen nationalen Zugangspunkt (NAP) ab. Über die reine regulatorische Compliance hinaus steht die **Erhöhung der Resilienz und Robustheit der kritischen Verkehrsinfrastruktur** im Fokus. Die KI-Systeme sollen nicht nur technische Formate validieren, sondern die inhaltliche Konsistenz, Datenredundanz und Verfügbarkeit der Datenströme prüfen. Ziel ist es, durch eine automatisierte Analyse die Effektivität und Nutzbarkeit der Daten für Verkehrsmanagement-Dienste zu steigern, Datenlücken frühzeitig zu identifizieren und die Robustheit der Dienste selbst zu gewährleisten.

Erwarteter Nutzen

Durch den Einsatz einer sicheren, KI-basierten Analyseumgebung soll der administrative Aufwand für Behörden und Anbieter reduziert, die Datenqualität am NAP nachhaltig verbessert und eine skalierbare, zukunftsichere Alternative zu veralteten Validatoren geschaffen werden. Im Kontext Resilienz/Krisenfestigkeit des Mobilitätssystems (Services, Steuerung, Information im Krisenfall, ...) ist es besonders wichtig, korrekte und qualitätsgesicherte Daten zugänglich zu haben und

auch alternative Datenbestände im Sinne der notwendigen Redundanz nutzen zu können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- **Analyse der NAP-Datensätze:** Untersuchung von Erfassungs-, Auswertungs- und Bereitstellungsprozessen am NAP, um die Datenbasis für die KI-Analyse zu strukturieren
- **Unterstützung des Compliance Assessments der nationalen Stelle:** Entwicklung von KI-Methoden, um Inhalte aus unterschiedlichen Dokumenten, Webseiten und Datensätzen semantisch zu verknüpfen und auf Konformität zu prüfen
- **Datenqualität und Matching:** Automatisierte nachvollziehbare Analyse der Datenqualität durch Abgleich mit vorgegebenen Maßzahlen (KPIs) und Metriken
- **Identifikation von Datenlücken:** KI-gestützte Erkennung von fehlenden Informationen oder Lücken in den Datenströmen, die für die Vollständigkeit der Dienste relevant sind
- **Sichere Architektur (On-Premise/Private):** Implementierung der KI-Modelle in einer geschützten Umgebung, die den Schutz sensibler Unternehmensdaten gewährleistet (keine Datenabflüsse in Public Cloud).

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.16 Nihilistisch-gewaltextremistische Online-Netzwerke (NVE) als sicherheitspolitische Herausforderung

Kontakt: Bundesstelle für Sektenfragen

E-Mail: p.pflegerl@sektenfragen.at

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Kontakt: Bundeskanzleramt (BKA)

E-Mail: robert.lender@bka.gv.at

Nihilistisch-gewaltextremistische Online-Netzwerke (NVE) wie „764“ und das übergeordnete „COM“-Ökosystem, sind in den letzten Jahren zunehmend in den sicherheitspolitischen Blick geraten. Diese Netzwerke nötigen Minderjährige systematisch zur Produktion von Missbrauchs-, Selbstverletzungs- und Gewaltinhalten. Dafür setzen sie Methoden wie Online-Sextortion ein, mit der Jugendlichen über intime oder mittels KI erzeugte Aufnahmen unter Druck gesetzt und schrittweise zu immer extremeren Handlungen gezwungen werden. Kanada hat „764“ im Dezember 2025 als Terrororganisation gelistet. Der europäische und österreichische Sicherheitsdiskurs steht vor der Aufgabe, diese hybride Bedrohung zwischen Kinderschutz, organisierter Kriminalität und Extremismus einzuordnen.

Für Österreich fehlt bislang ein belastbares Lagebild, eine als wirksam evaluierte Präventionspraxis sowie die Verknüpfung dieser Netzwerke mit der etablierten Expertise zu sektenartigen Manipulationsmustern. NVE-Netzwerke weisen strukturelle Parallelen zu Rekrutierungs- und Bindungsmechanismen von Gruppen auf, wie sie in der Sektenforschung beschrieben sind – dazu zählen Isolation, schamgesteuerte Geheimhaltung, eskalierende Loyalitätsproben und Statusgewinn durch Tabubruch. Eine systematische Anwendung dieser Konzepte auf NVE-Netzwerke ist im deutschsprachigen Raum nach derzeitigem Kenntnisstand noch nicht erfolgt, ist jedoch zentral für die Ausarbeitung neuer Präventionsansätze.

Denn klassische Präventionsbotschaften zu sicherem Online-Verhalten verlieren zunehmend an Schutzwirkung. Dazu zählt etwa der Hinweis, skeptisch gegenüber fremden Kontakten zu sein, insbesondere wenn es um das Versenden intimer Aufnahmen geht. NVE-Netzwerke setzen aber nicht auf plumpe Erstkontakte durch Fremde, sondern bauen über längere Zeit Beziehungen in vulnerablen Online-Communities auf, etwa auf Gaming-Plattformen wie Roblox oder in Discord-Servern rund um psychische Probleme und Selbstverletzung. Aus diesen öffentlichen Räumen ziehen sie ihre Opfer in private Discord- oder Telegram-Server, in denen Grooming und Erpressung stattfinden. Täter, die Jugendliche unter Druck setzen, sind zu diesem Zeitpunkt längst keine Fremde mehr. Generative KI könnte die Lage zusätzlich verschärfen, weil sich kompromittierende Aufnahmen als Mittel für Online-Sextortion auch aus harmlosen Profilfotos erzeugen lassen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Phänomenologische Einordnung: Welche Erscheinungsformen, Dynamiken und Wirkungsweisen von NVE-Netzwerken sind im deutschsprachigen Raum erkennbar, und wie verhalten sie sich zu vergleichbaren Strukturen im internationalen Kontext?
- Verbreitung in Österreich: In welchem Umfang sind österreichische Jugendliche von Kontaktaufnahmen oder Viktimisierung durch NVE-Netzwerke und Online-Sextortion betroffen? Welche vorhandenen Datenquellen aus Strafverfolgung, Meldestellen, Beratungsstellen und Helplines lassen sich für eine erste Einschätzung zusammenführen?
- Manipulations- und Bindungsmechanismen: Welche Parallelen bestehen zwischen den in NVE-Netzwerken beobachteten Rekrutierungs-, Bindungs- und Statusdynamiken und Mustern, wie sie in der Forschung zu destruktiven Gruppen beschrieben werden? Welche Erkenntnisse aus der Sekten- und Ausstiegssforschung sind übertragbar?
- Präventionsbedarf: Welche Präventionsangebote bestehen aktuell in Österreich, an welchen Stellen verlieren sie ihre Wirkung und wo bestehen Lücken? Welche Zielgruppen (Jugendliche, Eltern, Lehrkräfte, Beratungsstellen, Sicherheitsbehörden) sind bislang unzureichend adressiert?
- Präventionsstrategien: Welche Ansätze versprechen unter den veränderten Bedingungen Wirksamkeit? Exemplarisch denkbar sind Schulworkshops, Beratungsleitfäden für die Bundesstelle für Sektenfragen und kooperierende Stellen, Reaktionshilfen für Betroffene und Bezugspersonen sowie Empfehlungen für Sicherheits- und Strafverfolgungsbehörden.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

**3.2.17 Ideologisch geprägte Gemeinschaften und Kindeswohlgefährdung:
strukturelle Risiken und institutionelle Handlungssicherheit**

Kontakt: Bundesstelle für Sektenfragen

E-Mail: p.pflegerl@sektenfragen.at

In Österreich bestehen historisch wie gegenwärtig soziale Kontexte, in denen Kinder und Jugendliche in ideologisch oder weltanschaulich stark normierten Gemeinschaften aufwachsen. Diese können religiöser, politisch-ideologischer oder sonst weltanschaulicher Natur sein. Häufig sind sie durch geschlossene Binnenlogiken, charismatische oder autoritäre Führungsstrukturen sowie

Abschottungsmechanismen geprägt, die externe Kontrolle, behördliche Kooperation und institutionelle Aufsicht erschweren.

Fallkonstellationen zeigen, dass in solchen Milieus Kindeswohlgefährdungen über längere Zeiträume bestehen können, ohne frühzeitig erkannt oder wirksam unterbunden zu werden. Neben den gravierenden Folgen für betroffene Kinder und Jugendliche besitzen solche Kontexte auch eine **sicherheitsrelevante Dimension**: Sie verweisen auf Schwächen institutioneller Früherkennung, erschweren koordiniertes staatliches Handeln und können das Vertrauen in Schutz-, Kontroll- und Rechtsdurchsetzungsmechanismen beeinträchtigen. Hinzu kommt, dass radikalisierte Eltern ideologische Deutungsmuster, Feindbilder und antidemokratische Loyalitätsanforderungen an ihre Kinder weitergeben können.

Kinder und Jugendliche können dadurch selbst in Radikalisierungsprozesse eingebunden werden; im Extremfall können solche Sozialisationskontexte Anschlussfähigkeit an extremistische Milieus, Gewaltlegitimationen oder terroristische Handlungsoptionen begünstigen. In einzelnen Fällen entstehen normative Parallelordnungen, in denen demokratische Grundprinzipien infrage gestellt oder Loyalitätsanforderungen gegenüber der Gemeinschaft über rechtliche und gesellschaftliche Normen gestellt werden. Dadurch können externe Kontrolle weiter erschwert und Gewalt, Zwang oder systematische Grenzverletzungen innerhalb der Gemeinschaft legitimiert oder begünstigt werden.

Ziel ist die Entwicklung evidenzbasierter Orientierungsgrundlagen für Behörden, Aufsichtsinstitutionen und Fachpraxis. Gefährdungslagen in ideologisch abgeschlossenen Erziehungs- und Betreuungskontexten sollen dadurch früher erkannt, institutionelle Reaktionsfähigkeit gestärkt und Schutz-, Kontroll- und Interventionsmechanismen verbessert werden

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- **Systematische Rekonstruktion von Gefährdungsdynamiken:** Analyse historischer und gegenwärtiger Fallkonstellationen zur Identifikation zentraler Strukturmerkmale
- **Analyse ideologischer und organisatorischer Mechanismen:** Untersuchung, wie Deutungsmuster, Loyalitätsanforderungen und Abschottungsstrategien zur Normalisierung von Gewalt, Vernachlässigung oder Grenzverletzungen beitragen
- **Ableitung beobachtbarer Frühwarnsignale:** Entwicklung übertragbarer Indikatoren für Fachkräfte in Kinder- und Jugendhilfe, Bildung, Gesundheitswesen und Aufsicht
- **Analyse institutioneller Schnittstellen und Kontrollversäumnisse:** Untersuchung von Informationsbrüchen, Zuständigkeitsdiffusion und strukturellen Blindstellen zwischen beteiligten Institutionen
- **Erhebung von Unterstützungs- und Nachsorgelücken:** Einbeziehung der Erfahrungen ehemals betroffener Personen mit fehlenden oder unzureichenden Hilfsangeboten
- **Grundlagen für Prävention und Intervention:** Aufbereitung der Ergebnisse in Form handhabbarer Leitprinzipien für Prävention, Früherkennung, Intervention und Nachsorge.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.18 Robotische Systeme zur Unterstützung von Einsatzkräften bei Vegetationsbränden

Kontakt: Österreichischer Bundesfeuerwehrverband

E-Mail: science@feuerwehr.or.at , gerald.czech@feuerwehr.or.at

Waldbrände im schwierigen Gelände zählen zu den herausforderndsten Lagen für Einsatzkräfte. Eine der wichtigsten Brandbekämpfungsmaßnahmen ist das Anlegen von Wundstreifen, um die Ausbreitung des Brandes zu stoppen. Diese Tätigkeit wird vorwiegend manuell und in großer Truppenstärke durchgeführt, bindet viele Ressourcen und ist körperlich anstrengend. In solchen Lagen sind diese Tätigkeiten wegen sich ständig ändernder Bedingungen (Wind, Brandintensität der Vegetation) auch äußerst gefährlich.

Daher soll im Rahmen dieses Forschungsprojekts erforscht werden, wie solche Tätigkeiten mittels robotischer Systeme unterstützt oder gänzlich automatisiert werden können. Es ist primär zu untersuchen, wie sich die aktuell verwendeten manuellen Werkzeuge (z.B. Pulaski, Patschen, Äxte) effizient durch auf einem robotischen Trägerplattform montierte mechanisierte Werkzeuge ergänzt oder ersetzt werden können. Bei der Entwicklung von Werkzeugen für die automatisierte Bearbeitung müssen auch Sicherheitsaspekte berücksichtigt werden, sodass durch Funkenflug oder Materialtransport die Lage nicht verschlimmert wird. Spezielle Fragen wie der langfristige Betrieb und die Energieversorgung der schweren Werkzeuge sind zu berücksichtigen. Für den Einsatz der robotischen Fähigkeiten sollen Konzepte sowohl für Teleoperation wie auch Semi- und Vollautonomie untersucht werden. Für Letztere ist zu erforschen, welche Lageinformationen für eine effiziente Planung und robuste Ausführung der automatisierten Interventionen nötig sind und wie diese im Feld gewonnen werden können. Ferner ist zu untersuchen, wie diese neuen robotischen Fähigkeiten in beliebige Lage- und Führungsunterstützungssysteme abgebildet werden können. Gefordert ist ebenfalls eine systematische Betrachtung, wie diese Fähigkeiten in den Einsatzalltag integriert werden können.

Um entsprechende Entwicklungsfortschritte zu machen und den robotischen Nutzen für die Feuerwehren zu demonstrieren ist auf Wissen aus Vorgängerprojekt, wie z.B. Spürroboter, RoboNav und Robo-Mole aufzubauen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung von Konzepten zur Automatisierung von Interventionen das Anlegen von Wundstreifen oder Ausgraben von Glutnestern
- Erforschung von Konzepten für Energieversorgung und Batterien für den Betrieb von schweren Werkzeugen
- Entwicklung von Methoden zur automatischen Planung von Interventionen anhand verschiedener Informationen wie Lagebildern, Geländemodellen, Landbedeckung
- Weiterentwicklung von bestehenden Methoden zur automatischen Navigation im steilen und schwierigen Gelände
- Entwicklung von Methoden zur Einbindung in Lage- und Führungsunterstützungssoftware, ohne diese an einen bestimmten Hersteller zu binden
- Taktikentwicklung zur Integration der robotischen Fähigkeiten in die Vegetationsbrandbekämpfung.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.19 Untersuchung der Einsatzmöglichkeiten von Künstlicher Intelligenz zur Erkennung von Sozialleistungsbetrug in bestehenden Datensätzen**Kontakt: Bundesministerium für Inneres (BMI)**E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Beim Sozialleistungsbetrug handelt es sich um die unrechtmäßige Erschleichung von sozialen Leistungen aus dem Sozialsystem (z.B. Mindestsicherung, Notstandshilfe Grundversorgung, Arbeitslosengeld, Krankenkassenleistungen, Familienbeihilfe usw.).

Die Erkennung von solchen Betrugshandlungen in bestehenden Datenbeständen erfolgt bislang anlassbezogen, etwa durch gezielte Abfragen von Strafverfolgungsbehörden zu konkreten Sachverhalten. Dadurch können insbesondere solche Betrugsmuster unentdeckt bleiben, die nicht Gegenstand einer konkreten Anfrage sind oder deren Merkmale zum Zeitpunkt der Abfrage noch nicht bekannt sind. Es soll untersucht werden, inwieweit moderne KI-Verfahren strukturierte und unstrukturierte Datenbestände automatisiert auf Auffälligkeiten, Zusammenhänge und bislang nicht bekannte Muster mit möglichem Betrugsbezug analysieren können. Damit soll ein Beitrag geleistet werden, verbesserte Möglichkeiten der Betrugsermittlung unter Wahrung des bestehenden Grundrechts- und Datenschutzniveaus zu schaffen und die zusätzlichen Potenziale von KI mit rechtsstaatlichen Anforderungen in Einklang zu bringen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Untersuchung der Einsatzmöglichkeiten von KI zur Erkennung von Sozialleistungsbetrug
- Prüfung der Anforderungen an menschliche Kontrolle, Transparenz, Verhältnismäßigkeit und die Begrenzung der automatisierten Analyse
- Prüfung, inwieweit KI selbst zur Unterstützung einer grundrechts- und datenschutzkonformen Verarbeitung beitragen kann, etwa durch die gezielte Auswahl und Reduktion relevanter Daten, die Erkennung und Vermeidung unnötiger Datenverarbeitungen oder den Einsatz datenschutzfreundlicher Analyseverfahren
- Entwicklung von Grundlagen für einen technisch leistungsfähigen und zugleich grundrechts- und datenschutzkonformen Ansatz zur verbesserten Sozialbetrugsermittlung.
- Untersuchung, wie die zusätzlichen Ermittlungsmöglichkeiten moderner KI genutzt und zugleich die mit ihrer Anwendung verbundenen Risiken beherrschbar gemacht werden können.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.20 Anreize und Rahmenbedingungen für die Förderung der lokalen Produktion von Arzneimitteln zur Stärkung der Versorgungssicherheit in Österreich und Europa

Kontakt: Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK), Abteilung VII/6

E-Mail: martin.renhardt@gesundheitsministerium.gv.at

Kontakt: Gesundheit Österreich GmbH (GÖG)

E-Mail: sabine.vogler@goeg.at

Kontakt: Bundesministerium für Landesverteidigung (BMLV)

E-Mail: sicherheitsforschung@bmlv.gv.at

Die kontinuierliche Versorgung mit wirksamen und sicheren Arzneimitteln ist wesentlich für die Gesundheit der österreichischen Bevölkerung. Die Versorgungssicherheit mit Arzneimitteln hängt von komplexen Faktoren ab. Eine zentrale Herausforderung liegt in der starken Konzentration der Produktion (v.a. von Arzneimittelwirkstoffen) in asiatischen Ländern, weswegen eine erhebliche Importabhängigkeit von diesen Ländern besteht. Insbesondere die COVID-19-Pandemie hat gezeigt, dass Lieferkettenunterbrechungen zu teils gravierenden Arzneimittelengpässen und damit zu Versorgungsschwierigkeiten, auch in Österreich, führen können. Auf nationaler wie europäischer Ebene werden verschiedene Maßnahmen zur Stärkung der Versorgungssicherheit diskutiert, mit unterschiedlichen, teils auch gegensätzlichen Wirkungen. Auf EU-Ebene spiegelt sich dieses Bewusstsein in Initiativen wie dem Critical Medicines Act oder der Optimierung öffentlicher Beschaffungspraktiken wider. Besondere Aufmerksamkeit erhält dabei auch die Rückverlagerung von Produktionskapazitäten für Wirkstoffe und Fertigarzneimittel aus Asien nach Europa (Reshoring) und die Stärkung lokaler Produktion, vor allem auch in Krisensituationen (Notfallproduktion). Wie diese Maßnahmen ausgestaltet werden sollen, für welche Arzneimittel diese priorisiert verwendet werden sollen, und welchen tatsächlichen Einfluss die Maßnahmen haben könnten, ist unklar.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung von technischen und organisatorischen Rahmenbedingungen für eine lokale (Notfall-)Produktion von Arzneimitteln in Österreich
- Mapping von bereits implementierten und weiteren potenziellen Maßnahmen im Zusammenhang mit lokaler Produktion von Arzneimitteln bzw. Wirkstoffen in Österreich und Europa
- Analyse der Lieferketten von kritischen Arzneimitteln in Österreich hinsichtlich ihrer Struktur, Produktionskomplexität und Versorgungsrelevanz, sowie hinsichtlich möglicher Ansatzpunkte für Fördermaßnahmen und Umsetzungsstrategien
- Bewertung des Beitrags von Maßnahmen zur Förderung lokaler Produktion auf die Versorgungssicherheit von kritischen Arzneimitteln in Österreich und Europa.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.3 K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für kooperative F&E-Projekte

3.3.1 Automatisierte KI-gestützte Erhebung von Waldbrandflächen und relevanten Parametern

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK)

E-Mail: kilian.heil@bmluk.gv.at

Ziel der Ausschreibung ist die Entwicklung eines praxisorientierten und weitgehend automatisierten Systems zur Erfassung, Analyse und Bereitstellung von Waldbrandflächendaten nach Ereignissen, das als österreichweit einheitliche und interoperable Informationsbasis dient.

Das geplante System soll sämtliche relevanten Informationen nach Waldbrandereignissen standardisiert erfassen und direkt in die österreichische Waldbrand-Datenbank einspeisen. Die erhobenen Daten sollen sowohl operative Zwecke – etwa Einsatzplanung, Lagebeurteilung und Risikomanagement – als auch rechtliche, wissenschaftliche und administrative Anforderungen unterstützen. Insbesondere sollen sie zur Erfüllung forstgesetzlicher Aufgaben, beispielsweise bei der Dokumentation und Abgeltung von Waldbrandbekämpfungskosten, genutzt werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Automatisierte Erhebung: Analyse der wesentlichen Anforderungen und Akteur:innen, und Entwicklung eines Systems zur automatisierten Erfassung der relevanten Parameter aller Waldbrände in Österreich mit direkter Einspeisung in die österreichische Waldbrand-Datenbank
- Standardisierung: Einheitliche Datenstruktur und relevante Parameter (Lagekoordinaten, Brandart, Brandfläche, Fotos, Einsatzkräfte, etc.) in Abstimmung mit Landesfeuerwehrverbänden; automatisierte Datenweiterleitung
- Technische Schnittstellen: Integration weiterer Tools (Apps wie z.B. SpotFIRE, oder Sensoren) zur interoperablen Erfassung
- KI-gestützte Analyse und empirische Validierung: Einsatz von KI zur Auswertung von Satelliten- und Drohnenbildern zur schnellen und präzisen Erkennung von Brandflächen nach den Waldbrandereignissen; Validierung an Fallbeispielen vor Ort
- Verwertungskonzept: Darstellung der Nutzung der Daten für forstgesetzliche Zwecke, Kostenabgeltung, Forschung, Behörden und Einsatzplanung.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.2 Mixed Reality Trainings zur professionellen Reaktion auf verbales & nonverbales Verhalten im Justizvollzug

Kontakt: Bundesministerium für Justiz (BMJ)

E-Mail: kiras@bmj.gv.at ; andreas.bednarek@bmj.gv.at

Verbale und nonverbale Kommunikations- bzw. Einsatztrainings sind in Justizanstalten von entscheidender Bedeutung. Sie helfen Justizbeamtinnen und Justizbeamten dabei deeskalierend, vertrauensaufbauend, stressreduzierend und professionell aufkeimenden Konflikten mit einer hohen Reaktionsfähigkeit entgegenzutreten und somit die Sicherheit im Betrieb zu gewährleisten. Mixed Reality (MR) Lösungen können dabei ein effizientes, Zeit- und (teilweise) ortsunabhängiges Training ermöglichen. Die Möglichkeit faktisch jedes Einsatzszenario nachzustellen und gefahrlos zu trainieren und im Nachgang in einem gemeinsamen Debriefing zu besprechen, ermöglichen so eine innovative Ausbildung in Kombination mit den klassischen Einsatztrainings. Dabei ist gerade in der aktuellen Forschung die nonverbale & verbale Kommunikation in Verknüpfung MR-Simulationen in einem vergleichweisen frühen Versuchsstadium (Aburumman et al. 2022).

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welches Potenzial haben Mixed Reality Lösungen für Einsatztrainings zur Reaktionsschulung für verbale und nonverbale Kommunikation?
- Wie kann sich solch eine MR-Lösungen entlang der gesamten Ausbildungsschiene eines Justizwachebeamten ergänzend und effizienzsteigernd integrieren?
- Entwicklung eines MR-Prototypen für verbale & nonverbale Einsatztrainings
- Erarbeitung von Handlungsempfehlungen zur Integration in den Regelbetrieb.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.3 KI-gestützte Erschließung heterogener akustischer Datenbestände für sicherheitsrelevante Anwendungen

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SIFO@bmi.gv.at

Kontakt: Bundesministerium für Landesverteidigung (BMLV)

E-Mail: sicherheitsforschung@bmlv.gv.at

Behörden und Einsatzorganisationen verfügen zunehmend über umfangreiche Bestände digitaler Audioaufzeichnungen aus unterschiedlichen technischen Quellen. Diese Daten weisen stark variierende Formate, Aufnahmebedingungen und Qualitätsniveaus auf und können sprachliche, nicht-sprachliche sowie situative Informationen enthalten. Bestehende automatisierte Verfahren sind häufig auf einzelne Analyseaufgaben und günstige Aufnahmebedingungen beschränkt. Bei realen Datenbeständen können relevante Inhalte daher unentdeckt bleiben oder Ergebnisse entstehen, deren Verlässlichkeit nur schwer beurteilt werden kann.

Ziel des Ausschreibungsschwerpunktes ist die Erforschung und Erprobung eines modularen, vertrauenswürdigen und skalierbaren Ansatzes zur automatisierten inhaltlichen Erschließung heterogener akustischer Datenbestände. Relevante Eigenschaften, Inhalte und zeitliche Strukturen sollen erkannt, in standardisierte und

durchsuchbare Informationen überführt und für operative sowie analytische Arbeitsprozesse bereitgestellt werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung relevanter Anwendungsszenarien, Nutzeranforderungen, Datenarten und Qualitätsmerkmale
- Erforschung robuster Verfahren zur automatisierten Qualitätsbewertung, zeitlichen Strukturierung und inhaltlichen Erschließung heterogener Audio-Aufzeichnungen
- Untersuchung geeigneter Methoden zur Kombination komplementärer Analyseverfahren und zur Überführung der Ergebnisse in ein einheitliches Datenmodell
- Entwicklung von Verfahren zur Erkennung, Quantifizierung und transparenten Darstellung von Unsicherheiten und widersprüchlichen Ergebnissen.
- Erforschung geeigneter Human-in-the-Loop-Ansätze für Prüfung, Korrektur und Qualitätssicherung
- Entwicklung skalierbarer und ressourceneffizienter Architekturen sowie geeigneter Such-, Filter-, Visualisierungs- und Schnittstellenkonzepte
- Erarbeitung und Validierung von Testmethoden und Bewertungskriterien für Robustheit, Fehlerraten, Nachvollziehbarkeit und Übertragbarkeit
- Analyse rechtlicher, datenschutzrechtlicher, ethischer und gesellschaftlicher Anforderungen sowie Umsetzung und Evaluierung eines Demonstrators.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.4 Aufbau eines agentenbasierten Lieferketten-Lagebilds zur Erkennung kritischer Abhängigkeiten und zur Ableitung staatlicher Handlungsoptionen in Echtzeit

Kontakt: Bundesministerium für Wirtschaft, Energie und Tourismus (BMWET)

E-Mail: POST.III9a-25@bmwet.gv.at

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK)

E-Mail: abt-28@bmluk.gv.at

Kontakt: Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI)

E-Mail: nieves.kautny@bmimi.gv.at

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SIFO@bmi.gv.at

Österreichs Versorgung und staatliche Sicherheitsvorsorge hängen an global verflochtenen Lieferketten. Kritische Rohstoffe, Vorprodukte für die verarbeitende Industrie und für die Lebensmittelwirtschaft sowie medizinische Güter, verteidigungsrelevante Vorprodukte und Single-Points-of-Failure liegen überwiegend in tieferen Lieferkettenebenen (Tier-N), die staatlichen Stellen heute nicht zugänglich sind. Die Krisen der vergangenen Jahre haben gezeigt, dass sektorale und reaktive Ansätze nicht ausreichen, um Abhängigkeiten frühzeitig zu erkennen und ihre Bedeutung für kritische Staatsfunktionen zu bewerten.

Für eine wirksame staatliche Vorsorge fehlt eine rechenbare, gesamtstaatliche Sicht auf die Kritikalität nationaler Lieferketten, die Risiken in Echtzeit sichtbar macht und

fundierte Handlungsoptionen ableitet. Ziel der Forschung ist die Entwicklung und Validierung geeigneter Methoden und eines souverän betreibbaren Referenzprototyps. Das Vorhaben baut auf bisherigen Forschungsprojekten auf.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie lässt sich Kritikalität aus staatlicher Sicht quantifizieren? (z.B. Substituierbarkeit, Risiko)
- Welche Datenquellen sind für eine Inferenz tieferer Lieferkettenebenen geeignet, und welche rechtlichen Rahmenbedingungen regeln ihre Nutzung?
- Wie kann ein digitaler Zwilling nationaler Lieferketten aufgebaut werden, der fehlende Verbindungen mit ausgewiesener Unsicherheit inferiert?
- Wie lassen sich aus erkannten Risiken staatliche Handlungsoptionen ableiten, über die Ebenen Unternehmen, Mitgliedsstaat und EU systematisieren und durch KI-Agenten umsetzen?
- Wie können erfolgreiche Stresstests und Szenario-Analysen aufzeigen, wann ein unternehmerisches Lieferkettenproblem zu einem Versorgungsengpass im Sinne der Lenkungsgesetze wird?
- Wie können Methodik und Ergebnisse validiert, aktuell gehalten und institutionell verankert werden?
- Wie kann ein dauerhaftes Lieferketten-Monitoring für staatliche Anwendungen aufgebaut werden?

Strategischer Beitrag

Relevante EU-Richtlinien: CRMA, CER, IMERA, EDIP, CHIPS ACT 2, NZIA

Beitrag zur Industriestrategie Österreich 2035

Das Vorhaben schließt die Lücke bei der Sichtbarkeit von Tier-N-Netzwerken für strategische Güter. Es ermöglicht den Ressorts, proaktive Maßnahmen zu simulieren sowie bei Lieferkettenblockaden Handlungsoptionen abzuleiten, zu bewerten und damit Österreichs operative Souveränität zu stärken.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.5 Schutz vulnerabler Gruppen vor suchtfördernden digitalen Anwendungen und sozialer Zusammenhalt

Kontakt: Bundeskanzleramt, Sektion VII, Abteilung 1 (BKA)

E-Mail: post.kiras@bka.gv.at

Die österreichische Sicherheitsstrategie beschreibt folgende Prioritäten (S. 18):

- Sicherstellung des sozialen Friedens und des Zusammenhalts, insb. Gleichstellung, Kampf gegen steigende Ungleichheiten und Diskriminierung sowie Armutsbekämpfung und Schutz vulnerabler Gruppen
- Förderung von (Zugang zu) Innovation und technologischer Entwicklung bei verantwortungsvoller Nutzung ggü Mensch und Umwelt
- Unterstützung und Förderung eines breiten Sicherheitsbewusstseins der Bevölkerung und Stärkung der gemeinsamen Sicherheitsverantwortung.

Suchtfördernde Designelemente, welche durch Soziale Medien und andere Anwendungen wie insb. Spiele oder AI Companions eingesetzt werden, um eine

Abhängigkeit der Nutzenden von profitorientierten Anwendungen zu schaffen, können negative Effekte insb. für vulnerable Gruppen (auch Kinder und Jugendliche) aufweisen. Zudem können damit im Zusammenhang stehende langfristige negative Folgen in Bezug auf sozialen Zusammenhalt, Gleichstellung und Diskriminierung Bedrohungslagen für die öffentliche Sicherheit begünstigen. Laut einer [Studie des IHS](#) im Auftrag der Arbeiterkammer können suchtfördernde Designelemente identifiziert und in einer Taxonomie klassifiziert werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Ziel des Forschungsvorhabens ist es, diese Methodologie auf ihre Übertragbarkeit auf weitere Arten von Apps zu prüfen (insb. Spiele, AI Companions und Chatbots) und ggf. weiterzuentwickeln sowie eine Toolbox bereitzustellen, um ggf. basierend auf individuellen Einstellungen das Suchtrisiko einzelner Anwendungen bewerten zu können. Diese Toolbox soll Erziehungsberechtigten, Schulen, Gemeinden und ähnlichen lokalen Partnerorganisationen bereitgestellt werden, um Bewusstseinsbildung für Suchtrisiken auszubauen, den Schutz vulnerabler Gruppen zu stärken und auf diese Weise sozialen Zusammenhalt stärken.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.6 KI- beschleunigte Cyberangriffe: Neue Anforderungen an Incident Handling, Krisenmanagement und Cyber-Übungen in kritischen Infrastrukturen

Kontakt: Wirtschaftskammer Österreich (WKO)

E-Mail: martina.lassl@wko.at

Die rasante Entwicklung generativer künstlicher Intelligenz (KI) und spezialisierter Modelle mit offensiven Cyber-Fähigkeiten verändert die Cyber-Bedrohungslage für Unternehmen und Betreiber kritischer Infrastrukturen grundlegend. Es ist absehbar, dass Schwachstellen künftig schneller identifiziert, bewertet und potenziell auch effektiver ausgenutzt werden können. Dadurch verkürzen sich die Zeitfenster zwischen Schwachstellenentdeckung, Angriffsvorbereitung, Angriffsdurchführung und wirksamer Verteidigung erheblich. Für Organisationen mit hoher Versorgungsrelevanz entsteht damit ein neues Risikoprofil, das nicht nur technische Schutzmaßnahmen betrifft, sondern auch die organisatorische und personelle Reaktionsfähigkeit.

Bisher wird diese Entwicklung überwiegend technisch betrachtet, etwa im Hinblick auf automatisierte Schwachstellenanalyse, schnellere Exploit-Entwicklung oder KI-gestützte Erkennung. Weniger untersucht ist hingegen, wie verantwortliche Akteure in Unternehmen und kritischen Infrastrukturen auf diese neue Lage reagieren können und sollen. Insbesondere ist unklar, ob bestehende Best Practices im Incident Handling, in Eskalations- und Entscheidungsprozessen, in internen und externen Meldewegen sowie in der Zusammenarbeit zwischen Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT) / Security Operations Center(SOC), Management, Recht und Kommunikation weiterhin ausreichen oder unter den veränderten Rahmenbedingungen neu bewertet werden müssen.

Ziel des vorgeschlagenen Vorhabens ist es daher, die Auswirkungen KI-beschleunigter Cyberangriffe auf organisatorische Abläufe, Rollenmodelle und Entscheidungsprozesse systematisch zu untersuchen und daraus praxistaugliche Handlungs-, Trainings- und Übungskonzepte für österreichische Bedarfsträger abzuleiten. Dazu sollen realitätsnahe Simulations-Szenarien entwickelt und unter möglichst realistischen Bedingungen, etwa mit Hilfe einer Cyber Range, mit relevanten Akteuren aus kritischen Infrastrukturen und der öffentlichen Verwaltung erprobt und validiert werden. Das Projekt soll einen Beitrag dazu leisten, die Resilienz österreichischer Organisationen gegenüber einer neuen, dynamischen und schwer vorhersehbaren Cyber-Bedrohungslage zu erhöhen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse, wie KI-gestützte offensive Cyber-Fähigkeiten bestehende Annahmen zu Vorwarnzeit, Angriffsdynamik und Reaktionsfenstern verändern
- Entwicklung und Validierung realitätsnaher Simulations- und Übungsszenarien für Management-, Krisenstabs- und operative Ebenen, insbesondere unter Nutzung von Cyber-Range-Umgebungen
- Untersuchung, welche Incident-Handling-, Eskalations- und Krisenmanagementprozesse unter einer KI-beschleunigten Bedrohungslage an ihre Grenzen stoßen
- Identifikation von Anpassungsbedarf bei Rollen, Zuständigkeiten und Schnittstellen zwischen CISO, CSIRT/SOC, Management, Recht, Kommunikation und operativen Einheiten
- Bewertung, ob bestehende interne und externe Meldewege, Berichtspflichten und Entscheidungsprozesse unter den veränderten Rahmenbedingungen weiterhin zweckmäßig sind
- Aufzeigen und Analyse möglicher (veränderter) Handlungsoptionen und Verbesserung des Reaktionsportfolios bei KI-gestützten Angriffsvektoren
- Ableitung von sektorübergreifenden und sektorspezifischen Handlungsleitfäden für Betreiber kritischer Infrastrukturen und öffentliche Stellen in Österreich.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.7 Gewährleistung der Einsatzfähigkeit von kritischer Infrastruktur und ad-hoc Betrieben während Cyberattacken und Firewall-Umgehung

Kontakt: Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH

E-Mail: georg.aumayr@johanniter.at

Kontakt: Samariterbund Wien Rettung und Soziale Dienste gemeinnützige GmbH

E-Mail: Robert.lorenz@samariterbund.net

Ziel ist die Stärkung der digitalen Souveränität auf europäischer Ebene sowie die Weiterentwicklung von Sicherheitssystemen für kritische Infrastrukturen. Untersucht werden soll, wie die Sicherheit erhöht werden kann, ohne die notwendige Erreichbarkeit und Einsatzfähigkeit der Infrastruktur wesentlich einzuschränken.

Abgeschottete Systeme für die Lage- und Einsatzführung sind heute ohne Internetanbindung nur noch eingeschränkt funktionsfähig. Datenübertragung,

Analyseverfahren und der Einsatz neuer Technologien erfordern zunehmend den Zugriff auf dezentrale Rechenressourcen sowie eine laufende Verbindung zu externen Rechenzentren.

Diese systemimmanente Abhängigkeit stellt eine zentrale Schwachstelle dar und muss gezielt abgesichert werden. Durch Zero-Day-Exploits und die KI-gestützte, stark beschleunigte Identifikation von Sicherheitslücken in Firewalls ist diese Infrastruktur heute stärker gefährdet als je zuvor.

Hierzu gehört die Detektion von Angriffen auf diese Kommunikationsflüsse und -systeme sowie die schnelle und Sichere Absicherung des Betriebes der kritischen Infrastruktur, bis der Angriff vorbei ist und die Schäden behoben wurden.

Ein weiterer kritischer Punkt ist dabei die Identifikation der geeigneten Stellen, um eine Schadensminimierung zu erreichen und die bestmögliche Einsatzbereitschaft zu halten. Hierfür soll mit Wissensmodellen und Simulationen eine Stütze für die Beurteilung entstehen. Diese Wissensmodelle sollen zudem im Sinne von GraphRAGs der verbesserten Nutzung von KI-Systemen dienen und sowohl die Früherkennung von Angriffen als auch potenzielle Ausfallkaskaden als Simulation vorbereiten, um Abschottungen und -schaltungen auf einer begründeten Datenbasis befehlen zu können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Automatische Detektion von Cyberangriffen/Früherkennung von Angriffen und Störungen
- Welche Angriffs-, Störungs- und Ausfallmuster treten bei einsatzkritischer Kommunikationsinfrastruktur in Krisenlagen auf?
- Welche technischen und organisatorischen Indikatoren eignen sich zur frühen Erkennung von Angriffen oder Fehlkonfigurationen?
- Wie können Einsatzszenarien mit Daten wie Latenz, Verfügbarkeit, Netzlast oder Sensordatenströme zu einem belastbaren Risikobild verbunden werden?
- Welche Funktionalitäten von Systemen kritischer Infrastruktur können reduziert angeboten werden und wie kann die Funktionalität mit möglichst höher Resilienz gegen Cyberangriffe gehalten werden?
- Welche technischen Lösungen für die (physikalische) Abschottung von Systemen und deren Auswirkung auf die Einsatzführung gibt es und wie können sie weiterentwickelt werden?
- Kann durch temporäres Airgapping gewisser Bereiche die negative Auswirkung einer Hacking Attacke gemildert oder verhindert werden?
- Wie funktioniert „Cybersecurity“ in Zeiten von FABLE und Claude und wie kann sich kritische Infrastruktur davor schützen?
- Worin bestehen die Limitationen bisheriger Technologien in der aktuellen neuen Gefahrenlage und wie können sie überwunden werden?
- Netzwerkanalysen und Systemarchitektur zur effizienten Implementierung solcher Technologien – Adaptive Systemarchitektur
- Wie können Wissensmodelle, Prozessmodelle und Infrastrukturmodelle genutzt werden, um technische Abhängigkeiten und kritische Pfade explizit strukturiert abzubilden und somit die Vertrauenswürdigkeit der KI-Unterstützung und AI Governance zu verbessern?
- Wie können Wissensgraphen evidenzbasierte Antworten zu benötigter Infrastruktur, Schnittstellen, Risiken und Integrationsoptionen liefern?

- Welche Kompatibilitätskriterien müssen erfüllt sein, bevor neue KI-Services, Sensoren, Drohnen-, Funk- oder Netzwerk-Komponenten in Einsatzprozesse integriert werden?
- Wie können Logs, Quellenverlinkung und reproduzierbare Auswertung genutzt werden, um Entscheidungen nachträglich zu prüfen und Lessons Learned abzuleiten?
- Welche organisatorischen, rechtlichen und ethischen Voraussetzungen müssen Einsatzorganisationen schaffen, um KI für kritische Infrastruktur verantwortungsvoll einzusetzen?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.8 KI-gestützte Auswertung von Einsatzdaten und Einsatznachbereitung zum Betrieb einer Führungsunterstützung bei Leitstellen und Einsatzleitungen im Krisen- und Katastrophenfall

Kontakt: Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH

E-Mail: georg.aumayr@johanniter.at

Kontakt: Samariterbund Wien Rettung und Soziale Dienste gemeinnützige GmbH

E-Mail: Robert.lorenz@samariterbund.net

Der Einsatz von künstlicher Intelligenz ist die Einführung in ein neues Zeitalter des Arbeitens und der Verschiebung von Kompetenz und Leistung von Menschen zu Maschine. Im Einsatzkritischen Bereich werden beide Seiten vor besondere Herausforderungen gestellt. Immer mehr Daten werden für die Einsatzführung potenziell möglich und gleichzeitig bleibt das Verarbeitungspensum weiterhin limitiert und eine Überinformation kann zu Fehlentscheidungen führen. Mit der Nutzung von künstlicher Intelligenz wurde bereits eine Fokussierung und Kanalisierung von Daten in Vorprojekten wie AIFER oder MOSAIK getestet. In Projekten wie GigaResponse und AI4Emergency wurden die Leistungsparameter und Netzwerke von 5G für KI erforscht und die Anforderungen für die Nutzung datenintensiver Dienste definiert. Im Nachfolgeschritt ist die Integration solcher KI-gestützten Systeme in den Betrieb einer Leitstelle und Einsatzführung zu erforschen. Dies soll auf die technischen und einsatztaktischen Aspekte konzentriert sein.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Skalierbare und verteilte Test- & Messmethoden zur Bestimmung von Zuverlässigkeit und Resilienz der AI-basierten Services mit Verwendung von typischen Kommunikations- und Lastmodellen.
- Untersuchung der Netz-Applikations-Kopplung für adaptives Verhalten einsatzkritischer Netze und Anwendungen
- Optimale Platzierung von Analysediensten für den Einsatz von Federated Learning zur datenschutzgerechten KI-Modell-Erstellung
- 5G für Mission Critical Communication: Testen von 5G-Features wie QoS Identifiers (5QI), Slicing, Network Exposure Functions (NEFs)
- Automatisierte Transkription und semantische Analyse von Sprach- und Audioaufzeichnungen (Notrufe, Funkverkehr), inkl. Erkennung kritischer Muster wie Häufungen bestimmter Merkmale.

- Bild- und Videoanalyse in Echtzeit oder retrospektiv, um relevante Ereignisse und Objekte zu identifizieren.
- Multimodale Datenfusion: Zusammenführung von Audio-, Video-, Text- und Sensordaten zu einem konsistenten Lagebild mit integrierter Qualitätssicherung.
- Lernfähige Systeme: Einsatz von Reinforcement Learning und Human-in-the-Loop-Ansätzen zur kontinuierlichen Verbesserung und Erkennung neuer Einsatzmuster.
- Datenschutz und Ethik: Entwicklung von Mechanismen zur Wahrung rechtlicher und ethischer Standards bei KI-gestützter Auswertung.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.9 Detektion von Deepfakes und medialen Manipulationen in Bildern und Videos für polizeiliche Ermittlungen und Erfordernisse

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Gerade im polizeilichen Kontext ist es wichtig gesichert festzustellen, ob Bilder und Videos echt oder gefälscht sind. Digitale Medien werden heute oft als Beweise bei Ermittlungen verwendet. Fotos von Tatorten, Überwachungsvideos oder Aufnahmen von Handys können helfen, Straftaten aufzuklären und Täterinnen und Täter zu identifizieren. Wenn solche Bilder oder Videos jedoch manipuliert oder gefälscht sind, kann das zu falschen Verdächtigungen und ungerechten Entscheidungen führen. Deshalb müssen Polizeibehörden prüfen können, ob digitale Inhalte authentisch sind.

Besonders durch moderne Technologien wie Deepfakes wird diese Aufgabe immer schwieriger. Mit künstlicher Intelligenz können täuschend echte Fotos oder Videos erstellt werden, in denen Personen Dinge sagen oder tun, die niemals passiert sind.

Außerdem ist die Überprüfung der Echtheit wichtig, um das Vertrauen der Bevölkerung in die Polizei und das Rechtssystem zu schützen.

Das bereits abgeschlossene F&E-Projekt defalsif-AI hat sich das Erkennen von Deepfakes und medialen Manipulationen in digitalen Bild- und Videoinhalten zum Ziel gesetzt, um dadurch die technologischen Fähigkeiten zur Verifikation von Bild- und Videomaterial zu stärken.

Aufgrund laufender Weiterentwicklungen im technischen Bereich auch die Fakes von Bildern und Videos betreffend sowie erweiterter Anforderungen, um (Ver-)Fälschungen erkennen zu können, bedarf es einer Weiterentwicklung des Bestehenden. Elementar ist dabei die einfache Nutzbarkeit für die Bedarfstragenden im polizeilich forensischen Bereich, darüber hinaus aber auch im generalpräventiven Sinn zum Schutz der Gesellschaft vor Irreführung und anderen Schäden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Beschreibung des Status Quo über die Anwendbarkeit der Erkenntnisse und Ergebnisse des KIRAS-Projektes defalsif-AI für polizeiliche Ermittlungen
- Einholung von Erkenntnissen und Lösungsstrategien vergleichbarer Bedarfsträger anderer europäischer Strafverfolgungseinheiten

- Betrachtung der Entwicklung von Deepfake- und Manipulationsverfahren und Adaptierung bestehender Analyse-Tools bzw. Generierung zeitgemäßer Lösungsansätze für aktuelle Fragestellungen
- Entwicklung eines Tools, das insbesondere in der Lage ist, bei Live-Videokonferenzen in Echtzeit zu verifizieren, ob eine Person real ist.
- Sicherstellung der Praktikabilität und Umsetzung der generierten Tools.
- Abwägung der weiteren Entwicklung im betreffenden Sektor, um möglichst zukunftswirksam Lösungen zur Verfügung stellen zu können.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.10 Weiterentwicklung und Erweiterung der KI-gestützten Schuhspurensammlung

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at Mit dem KIRAS-Projekt IMPRESS wurde eine österreichweite Schuhspurensammlung entwickelt, die seit 2025 operativ im Einsatz ist und nun weiterentwickelt werden soll. Konkret betrifft dies den Abgleich fotografisch gesicherter Schuhspuren bzw. Laufflächen oder Schuhabdrücke in folgenden Varianten:

- Schuhspuren mit Schuhspuren zur Erkennung möglicher Tatzusammenhänge,
- Schuhspuren mit Referenzmaterial (z. B. Laufflächen von Schuhen am Markt), um beispielsweise bestimmte Marken oder Modelle eingrenzen zu können
- Schuhspuren mit Schuhabdrücken sichergestellter Schuhe möglicher Tatverdächtiger.

Ziel ist eine im Vergleich zum Ist-Stand deutlich verbesserte automatisierte, KI-basierte Vorselektion bzw. Reihung potenzieller Übereinstimmungen, die als fachliche Entscheidungsgrundlage für Expertinnen und Experten bei Vergleichsuntersuchungen dienen und den derzeit noch zeitintensiven Vergleichsprozess wesentlich beschleunigen kann.

Darüber hinaus besteht Interesse an komplett neuen mobilen Lösungen (idealerweise mittels dienstlicher Smartphones) zur digitalen Erfassung von Schuhspuren direkt am Tatort, einschließlich dreidimensionaler Schuhspuren, mit anschließender unmittelbarer Übertragung in bestehende Vergleichs- und Datenbanksysteme. Derartige mobile Erfassungsmöglichkeiten existieren derzeit nicht.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Nutzung bestehender Datenbestände und Expertinnen-/Expertenklassifizierungen zur Weiterentwicklung und Erweiterung der Tatortschuhspurensammlung durch moderne KI-gestützte Bildverarbeitung und Mustererkennung
- Verbesserung der automatisierten Vorselektion und Reihung potenzieller Übereinstimmungen zwischen Tatortspuren untereinander sowie zwischen Tatortspuren und Referenzmaterial
- Verbesserte Auswertung fragmentarischer, qualitativ eingeschränkter und störungsbehafteter Schuhspuren

- Entwicklung mobiler Lösungen zur digitalen Erfassung von Schuhspuren direkt am Tatort
- Direkte digitale Übertragung und Integration mobil erfasster Spuren in bestehende bzw. in Rahmen des Projekts weiterentwickelte Vergleichssysteme.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.3.11 KI-basierte Datenanalyse von Videodaten

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Im Rahmen der Informationsgewinnung fallen zunehmend Mengen an videobasierten Daten an, die aus diversen Quellen stammen. Die manuelle Sichtung und Analyse dieser Datenströme ist aufgrund ihrer schieren Quantität und Heterogenität nicht mehr effizient manuell bewältigbar. Dies führt zu einer erheblichen Lücke in der zeitnahen Auswertung, wodurch wertvolle Erkenntnisse über Bedrohungslagen oft erst mit Verzögerung identifiziert werden.

Der Einsatz von KI-gestützter Computer Vision kann die automatisierte Aufbereitung dieser Daten revolutionieren. Ziel ist es, die Transformation von unstrukturierten Videodaten in verwertbare Erkenntnisse zu beschleunigen, um ein präziseres und aktuelleres Lagebild zu erstellen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse und Evaluation moderner Deep-Learning-Architekturen hinsichtlich ihrer Robustheit und Präzision bei der automatisierten Detektion sowie Kategorisierung von Zielobjekten und komplexen Verhaltensmustern innerhalb hochheterogener Videoströme
- Konzeption und Validierung von Methoden zur Multi-Source-Korrelation, um die konsistente Identifizierung und den Bewegungsfluss von Personen und Objekten über zeitlich und räumlich disjunkte Quellen hinweg wissenschaftlich zu untersuchen
- Systematische Untersuchung der Modellzuverlässigkeit und potenzieller Fehlerquellen (z. B. Bias, Fehlidentifikationen) zur Entwicklung eines Bewertungs-Frameworks, welches die technische Integrität und die Einhaltung rechtsstaatlicher Anforderungen an die Informationsgewinnung garantiert
- Als zentrales Ergebnis der Forschung ist die Konzeption und Implementierung eines interaktiven Demonstrators vorgesehen. Dieser Demonstrator fungiert als Proof-of-Concept und Forschungswerkzeug, nicht als fertiges Produkt. Er dient als essenzielle Umgebung, um die entwickelten Analysealgorithmen in simulierten, praxisnahen Szenarien zu testen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Experimentelle Entwicklung)

3.4 K-PASS. Cybersicherheit. Ausschreibungsschwerpunkte für F&E-Dienstleistungen

3.4.1 Souveräne Legal AI für sicherheitspolitisch sensible Bereiche der österreichischen Justiz

Kontakt: Bundesministerium für Justiz (BMJ)

E-Mail: kiras@bmj.gv.at ; andreas.bednarek@bmj.gv.at

In sicherheitspolitisch sensiblen Verfahren der österreichischen Justiz, wie z.B. In Fällen von Cybercrime, Terrorismusfinanzierung, organisierte Kriminalität, Verfassungsschutzdelikte, Wirtschaftsspionage oder bei hybride Bedrohungslagen, wachsen die digital sicherzustellenden und auszuwertenden Datenmengen (Datenträger, Chatprotokolle, Telekommunikationsüberwachung, Krypto-Forensik, offene Quellen) exponentiell, während spezialisierte Personalressourcen in den Schwerpunkt- und Sonderzuständigkeiten knapp bleiben. Bestehende generische KI-Tools sind in diesen Verfahren strukturell ungeeignet: Sie laufen entweder in US-basierten Rechenzentren/Clouds (Konflikt mit dem US CLOUD Act, Amtsgeheimnis, Berufsgeheimnissen, Ermittlungsgeheimnis), erzeugen Halluzinationen, die in der Strafrechtspflege existenzbedrohend sind, oder lassen sich nicht in die heterogene Justiz-IKT integrieren.

- Es soll erhoben werden, wie souveräne Legal LLM, durch einen quantensicheren Cybersecurity-Stack auf der Justiz-IKT als kritischer Infrastruktur eingesetzt werden könnte, um konkrete sicherheitspolitisch sensible BMJ-Workflows zu beschleunigen, qualitativ zu verbessern und gegen heutige und vor allem zukünftige quantenbasierte Angriffe abzusichern. Des Weiteren sollen die Anforderungen an souveräne Rechenzentren in Österreich und der EU erarbeitet werden, so dass eine Verwendung durch öffentliche Stellen, insbesondere Ministerien, möglich und wünschenswert wird (inklusive Verarbeitung klassifizierter Daten). Auch die Möglichkeit von verteilten Rechenzentren zur Steigerung der Resilienz kann in Betracht gezogen werden. Das Ergebnis ist ein in sich geschlossenes Implementierungskonzept als Entscheidungsgrundlage für das BMJ – inklusive priorisierter Anwendungsfälle, konzeptioneller Referenzarchitektur, Risiko- und Bedrohungsmodell sowie nachvollziehbarer Roadmap für ein etwaiges Folgevorhaben (Prototyping/Pilotierung).
- Welche konkreten Workflows in sicherheitspolitisch sensiblen Verfahren des BMJ lassen sich durch ein souveränes Legal LLM substantiell entlasten – und welche Anforderungen an Nachvollziehbarkeit, Beweiswert und EU-AI-Act-Hochrisiko-Konformität sind dabei zu erfüllen?
- Welche sicherheitspolitischen Risiken entstehen durch den heutigen Einsatz US-basierter generativer KI in justiziellen Verfahren – und wie sind diese zu quantifizieren?
- Welche Vorteile bietet ein souveränes österreichisches Rechenzentrum und welchen Anforderungen muss es für den Betrieb von Legal LLMs genügen, um von öffentlichen Stellen mit sensiblen Daten bedenkenlos genutzt werden zu können?
- Welche Referenzarchitektur erfüllt die Anforderungen der Justiz-IKT als kritische Infrastruktur und ist mit der bestehenden Justiz-Aktenlandschaft integrierbar?
- Wie sieht ein evidenzbasierter Migrationspfad zu einer „Justiz-AI by Design“ aus (TRL-Roadmap, Pilotumfeld, Betriebsmodell, Personalentwicklung)?

- Welche operativen, prozessualen und rechtlichen Maßnahmen sind erforderlich, um KI-gestützte Auswertungen rechtssicher in das Strafverfahren einzubringen (StPO, Dokumentations- und Auditpflichten, EU-AI-Act-Konformität)?
- Welche besonders langlebigen Justizdaten (Strafakten, TKÜ-Ergebnisse, Zeugenschutz-Daten) sind dem ‚Store-now, decrypt-later‘-Risiko durch Quantencomputer ausgesetzt – und wie sieht ein priorisierter, kryptoagiler Migrationspfad der Justiz-IKT hin zu PQC, QRNG-basiertem Secret Sharing und optional QKD aus?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.2 Digitale Abhängigkeit als Sicherheitsrisiko für die europäische Land- und Ernährungswirtschaft

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft (BMLUK), Digitalisierung

E-Mail: johann.doppelbauer@bmluk.gv.at

Digitale Abhängigkeiten im Agrar- und Ernährungssektor sind nicht nur wirtschaftliche Risiken, sie sind sicherheitspolitische Verwundbarkeiten. Die zunehmende Durchdringung landwirtschaftlicher Prozesse durch vernetzte Systeme schafft Angriffsflächen, die im Kontext hybrider Bedrohungslagen strategisch genutzt werden (können). Gezielte Störungen oder Manipulationen digitaler Infrastrukturen können Produktionsprozesse, Lieferketten und Versorgungsflüsse in kurzer Zeit und in großem Maßstab beeinträchtigen – ohne dass physische Einwirkung erforderlich wäre. Aktuelle geo- und handelspolitische Spannungen, darunter Exportbeschränkungen für Halbleiter, Technologiekomponenten bis hin zu Sprachmodellen, extraterritoriale Datenanforderungen und die wachsende Instrumentalisierung digitaler Infrastrukturen und Services im Kontext hybrider Bedrohungslagen, unterstreichen die Dringlichkeit einer strategischen Auseinandersetzung mit der digitalen Souveränität im Agrar- und Ernährungssektor. Es fehlt an einer systematischen, empirisch fundierten Analyse der tatsächlichen Abhängigkeitsstrukturen sowie an konkreten, praxistauglichen Gegenmaßnahmen für den Agrar und Nahrungsmittelsektor.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Systematische Kartierung und Quantifizierung digitaler Abhängigkeiten im Agrarbereich
- Internationale Vergleichsforschung: Ziel ist es, bewährte Ansätze für mehr digitale Souveränität zu identifizieren.
- Identifikation technischer und organisatorischer Maßnahmen zur Stärkung digitaler Souveränität
- Verhaltens- und Akzeptanzforschung: warum nutzen landwirtschaftliche Betriebe souveräne Technologien nicht oder nur zögerlich
- Governance-Analyse und Regulierungslücken.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.3 Anti-Phishing-Schutzschild für Österreich – Konzeptstudie nach internationalen Vorbildern

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Phishing zählt zu den häufigsten Einfallstoren für Internetbetrug und verursacht in Österreich jährlich steigende Schäden. Bestehende Präventions- und Meldestrukturen erreichen Betroffene häufig erst, nachdem der Schaden bereits eingetreten ist; eine zeitnahe, netzseitige Unterbrechung der Angriffskette fehlt in Österreich bislang. > International gibt es dafür bereits erprobte Vorbilder. Vorreiter ist Belgien: Das Belgian Anti-Phishing Shield (BAPS) des Centre for Cyber Security Belgium lässt Bürgerinnen und Bürger verdächtige Nachrichten an eine zentrale Meldeadresse weiter-leiten, analysiert die enthaltenen Links und verteilt bestätigte Schaddomains als Sperrliste an die Internet-Service-Provider. Auf DNS-Ebene werden Nutzerinnen und Nutzer beim Aufruf einer gesperrten Seite auf eine Warnseite umgeleitet. Die Niederlande haben 2025 ein an BAPS angelehntes, DNS-basiertes Schutzschild pilotiert und dessen Weiterentwicklung beschlossen. Das Vereinigte Königreich verfolgt mit dem Suspicious E-Mail Reporting Service einen ergänzenden Ansatz. > Für Österreich stellt sich die Frage, wie ein vergleichbarer Schutzmechanismus organisatorisch tragfähig und technisch wirksam ausgestaltet werden kann. Ziel einer dementsprechenden F&E-Dienstleistung ist es, hierfür eine fundierte Entscheidungsgrundlage samt Umsetzungskonzept zu erarbeiten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Vergleichende Analyse internationaler Vorbilder (u. a. BAPS in Belgien, das niederländische NCSC-Schutzschild, der britische Melde- und Takedown-Ansatz) und Bewertung ihrer Übertragbarkeit auf den österreichischen Kontext
- Klärung der rechtlichen Rahmenbedingungen für netz- bzw. DNS-seitige Warnungen und Sperren (u. a. Datenschutz, Fernmelderecht, Grundrechte und Netzneutralität)
- Entwicklung eines Betreiber- und Governance-Modells unter Einbindung bestehender Strukturen sowie eines „Trusted-Partner“-Ansatzes
- Konzeption der technischen Architektur und Abwägung von Eingriffsvarianten
- Bewertung von Wirksamkeit, Wirtschaftlichkeit und Skalierbarkeit sowie von Maßnahmen zur Vermeidung von Fehlklassifikationen (Overblocking)
- Ausarbeitung konkreter Handlungsempfehlungen für einen nationalen Anti-Phishing-Schutzschild.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.4 Analyse des Einsatzes und der Auswirkungen von KI-Agents im kriminalpolizeilichen Aufgabengebiet

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

KI-Agents gewinnen zunehmend an Bedeutung, da sie in der Lage sind, eigenständig Aufgaben zu analysieren, Entscheidungen zu treffen und Prozesse automatisiert auszuführen. Dies birgt nicht nur großes Potential, sondern auch erhebliche

Gefahren. Es besteht das Risiko von Fehlentscheidungen, insbesondere wenn die zugrunde liegenden Daten fehlerhaft oder voreingenommen sind.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie kann man KI-Agents identifizieren/unterscheiden (im Sinne der Zuordenbarkeit von Artefakten)?
- Wie können Strafverfolgungsbehörden KI-generierte Inhalte zuverlässig von menschlich erstellten Inhalten unterscheiden?
- Welche Methoden eignen sich zur Erkennung von autonomen KI-Agents bei Cyberkriminalität?
- Inwiefern können KI-Agents zur automatisierten Verbreitung von Desinformation und Fake News genutzt werden?
- Welche technischen Möglichkeiten besitzt die Polizei, um missbräuchlich eingesetzte KI-Systeme zu identifizieren?
- Wie verändert der Einsatz von KI-Agents die digitale Ermittlungsarbeit der Polizei?
- Welche Gefahren entstehen durch KI-gestützte Angriffe für die öffentliche Sicherheit?
- Welche rechtlichen Herausforderungen entstehen bei der Strafverfolgung von KI-basierten Straftaten auf Basis des österreichischen Strafrechts?
- Welche Rolle spielt KI selbst bei der Erkennung krimineller KI-Agents?
- Wie können internationale Polizeibehörden bei der Bekämpfung von KI-gestützter Kriminalität zusammenarbeiten?
- Wie können digitale Forensik und KI kombiniert werden, um automatisierte Angriffe schneller aufzudecken?
- Welche Auswirkungen haben KI-Agents auf Betrugsdelikte wie Identitätsdiebstahl oder Online-Scams?
- Welche Ausbildungs- und Weiterbildungsmaßnahmen benötigen Polizeibehörden im Umgang mit KI-gestützter Kriminalität?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.5 E-Government-Schutz, Cyber Crime und Digitale Forensik

Kontakt: Bundeskanzleramt (BKA) VII/1

E-Mail: post.kiras@bka.gv.at

Mit dem dadeX und den daran angeknüpften Registern verfügt die österreichische Verwaltung über Zugriff auf eine enorme Menge strukturierter und semistrukturierter Daten, deren Nutzung im Sinne eines Datenraums der öffentlichen Verwaltung einen wesentlichen Beitrag zur Stärkung der staatlichen Handlungsfähigkeit sowie zur Erhöhung der inneren Sicherheit und Krisenresilienz leisten könnte. Als digitale Repräsentation von Informationen könnten bei entsprechender Qualität und gezielten Verarbeitungsmethoden Erkenntnisse aus den angebundenen Datenregistern abgeleitet werden, die – insbesondere mit der künftigen Anbindung an das AMDC der Statistik Austria – sicherheitspolitisch relevante Hinweise enthalten und als evidenzbasierte Entscheidungshilfe für die Politik und die Verwaltung dienen können („Registerforschung kann kausale Zusammenhänge erklären, die für die Politik entscheidend sind“, so Dr. Michael

Strassni,(WWTF), Kurier, abrufbar unter <Registerdatenforschung: Kein Schubladendenken mehr | Kurier> (Stand 29.6.2026). So könnten in den bestehenden Registern etwa Informationen zu missbräuchlicher Nutzung digitaler Identitäten, Mehrfachanbringen, betrugsnahen Mustern oder Anomalien in digitalen Verwaltungsprozessen enthalten sein. Vor einer möglichen Nutzung dieser Daten gilt es jedoch fundiert zu klären, welche bestehende Datenregister – insbesondere der an den dadeX angebotenen Register – für solche Ableitungen technisch tatsächlich geeignet sind (insb. hinsichtlich Datenqualität, Schnittstellenproblemen), welche belastbaren und für die Verwaltung nützlich Ableitungen daraus getroffen werden können und welche Analysen rechtskonform und ethisch vertretbar sind.

Vor obigem Hintergrund sollen somit die folgenden Forschungsfragen beantwortet werden:

- Aus welchen über den dadeX abrufbaren Daten können sicherheitsrelevante Informationen welcher Art abgeleitet werden?
- Welche technischen Anforderungen stellen sich dabei (insb. hinsichtlich Datenqualität, Interpretierbarkeit, mögliche Schnittstellenprobleme)?
- Welche Schlussfolgerungen dürfen bei rechtskonformer, verhältnismäßiger und ethisch vertretbarer Nutzung gezogen werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.6 Befähigung der Verwaltung: Sicheres Low-Code/No-Code und Vibe-Coding zur KI-gestützten Prozessautomatisierung in Fachabteilungen

Kontakt: Bundeskanzleramt (BKA), Sektion VII/A/1

E-Mail: post.kiras@bka.gv.at

Zur Stärkung der staatlichen Handlungsfähigkeit sowie zur Erhöhung der inneren Sicherheit und Krisenresilienz ist eine effiziente, reaktionsschnelle öffentliche Verwaltung unerlässlich. Bedienstete in den Fachabteilungen verfügen über tiefgreifendes Domänenwissen zu den Verwaltungsprozessen, sind bei der digitalen Umsetzung jedoch oft auf knappe zentrale IT-Ressourcen angewiesen oder in der Entwicklung nicht eingebunden. Der Einsatz von Low-Code/No-Code (LC/NC) Plattformen sowie modernen KI-Tools zum sogenannten „Vibe-Coding“ (bei dem Softwaretools und Arbeitsprozesse durch natürliche Sprache mithilfe von KI generiert werden) bietet enormes Potenzial. Öffentlich Bedienstete können damit eigenständig Prozesse automatisieren, kleinere Anwendungen bauen und Routineaufgaben beschleunigen. Die Förderung von Innovation und technologischer Entwicklung muss jedoch bei verantwortungsvoller Nutzung erfolgen. Die dezentrale Erstellung von automatisierten Prozessen durch Nicht-Programmierer birgt Risiken für die IT-Sicherheit, wie etwa die Entstehung von unkontrollierter Schatten-IT, den fehlerhaften Umgang mit sensiblen Daten oder Cybersicherheitsrisiken. Um die Resilienz des E-Governments aufrechtzuerhalten, gilt es fundiert zu klären, wie diese Werkzeuge sicher in die bestehende IT-Infrastruktur (und an bestehende Register) der österreichischen Verwaltung integriert werden können. Es bedarf strategischer Governance-Ansätze, um die Innovationskraft der Fachabteilungen zu nutzen, ohne die Cybersicherheit und den Datenschutz zu gefährden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche technischen Anforderungen stellen sich dabei (insb. hinsichtlich Datenqualität, IT-Sicherheit, Vermeidung von Schatten-IT und mögliche Schnittstellenprobleme)?
- Welche Governance-Regeln und Leitplanken müssen implementiert werden, um eine rechtskonforme, verhältnismäßige und ethisch vertretbare Nutzung von KI-generiertem Code und automatisierten Workflows zu garantieren?
- Welche Verwaltungsprozesse in Fachabteilungen eignen sich fachlich und sicherheitstechnisch für die Automatisierung durch LC/NC und Vibe-Coding?
- Welche Auswirkungen ergeben sich auf Informationssicherheit und Datenschutz
- Wie können bestehende Register und E-Government-Komponenten sicher angebunden werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.7 Nationales föderiertes Datenökosystem für das Krisen- und Katastrophenmanagement

Kontakt: Gerald Czech, Österreichischer Bundesfeuerwehrverband

E-Mail: science@feuerwehr.or.at , gerald.czech@feuerwehr.or.at

Kontakt: Elmar Rizzoli, Amt der Tiroler Landesregierung

E-Mail: krisenmanagement@tirol.gv.at

Die Verfügbarkeit, Qualität und sichere Austauschbarkeit von Daten zwischen allen BOS und Betreibern kritischer Infrastruktur ist eine wesentliche Voraussetzung für ein wirksames Krisen- und Katastrophenmanagement. Österreich verfügt über ein bewährtes subsidiäres System mit geteilten Zuständigkeiten von Gemeinden über Länder bis zum Bund. Gleichzeitig erschweren fragmentierte Datenbestände, proprietäre Systeme und bilaterale Austauschprozesse die Erstellung eines organisationsübergreifenden Lagebildes. Mit dem datahub.tirol verfügt Österreich bereits über Europas ersten EU-konformen regionalen Data Space und damit über ein zukunftsweisendes Beispiel für den sicheren und souveränen Datenaustausch. Aufbauend auf diesem Ansatz sowie den Konzepten von Gaia-X, der International Data Spaces Association (IDSA) und den Rahmenbedingungen des EU Data Act soll untersucht werden, wie ein föderiertes Datenökosystem für das Staatliche Krisen- und Katastrophenmanagement sowie die Strukturen gemäß Bundes-Krisensicherheitsgesetz konzipiert und evaluiert werden kann. Ziel ist ein organisationsübergreifendes Lagebild, das eine schnellere, effizientere und datensouveräne Krisenbewältigung ermöglicht.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- **Föderierte Datenarchitektur:** Entwicklung einer Architektur für einen sicheren, organisationsübergreifenden Datenaustausch unter Wahrung der Datenhoheit aller beteiligten Akteure
- **Interoperabilität:** Identifikation und Weiterentwicklung gemeinsamer Datenmodelle und Standards zur organisationsübergreifenden Nutzung von Lageinformationen sowie Analyse bestehender Standardisierungslücken

- **Resilienz:** Konzeption einer robusten Dateninfrastruktur mit gestuften Betriebsmodi und dynamischen Zugriffsrechten, die auch bei Ausfällen von Kommunikations- oder IT-Infrastrukturen funktionsfähig bleibt
- **Recht und Governance:** Analyse der rechtlichen Rahmenbedingungen sowie Entwicklung eines föderalen Governance-Modells für den nachhaltigen Betrieb und die Zusammenarbeit zwischen Bund, Ländern, Einsatzorganisationen und Betreibern kritischer Infrastruktur
- **Europäische Integration:** Untersuchung der Anbindung an europäische Datenräume und Krisenmanagementsysteme, insbesondere im Hinblick auf Interoperabilität und grenzüberschreitende Zusammenarbeit.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.8 Resilienz sektorgekoppelter Energiesysteme gegen Kaskadeneffekte

Kontakt: Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI);

Ing. DI (FH) Florian Moritz, MBA; Mag. Nieves Kautny, MSc

E-Mail: florian.moritz@bmimi.gv.at ; nieves.kautny@bmimi.gv.at

Die österreichische Energiewende führt zu einer zunehmenden Kopplung der Sektoren Strom, Wärme, Gas, Mobilität und Industrie sowie zum verstärkten Einsatz digitaler Steuerungs- und Aggregationsplattformen. Dadurch entstehen neue Interdependenzen zwischen kritischen Infrastrukturen. Störungen können sich sektorenübergreifend ausbreiten und Kaskadeneffekte auslösen. Gleichzeitig erhöhen klimabedingte Extremereignisse die Verwundbarkeit der Energieinfrastruktur und können im Zusammenwirken mit Cyberangriffen oder technischen Ausfällen sogenannte Compound-Risiken verursachen. Für diese neuen Verwundbarkeiten fehlen bislang integrierte Bewertungsansätze, die physische, digitale und klimabedingte Risiken gemeinsam betrachten.

Ziel der F&E-Dienstleistung ist die Entwicklung eines integrierten Resilienzmodells für sektorgekoppelte Energiesysteme. Dieses soll kritische Kopplungspunkte identifizieren, Kaskadeneffekte infolge technischer Ausfälle, Cyberangriffe und Klimaextreme modellieren sowie Resilienzprinzipien ("Resilience by Design"), insbesondere Redundanz, Entkoppelbarkeit und resiliente Steuerungsarchitekturen, ableiten. Darüber hinaus ist eine priorisierte FTI-Roadmap zu entwickeln, welche die wesentlichsten Forschungs-, Technologie- und Innovationsbedarfe zur Stärkung der Resilienz sektorgekoppelter Energiesysteme identifiziert. Die Ergebnisse dienen der sicherheitspolitischen Bewertung sowie der Priorisierung zukünftiger FTI-Förderschwerpunkte im Bereich Energiewende.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Kopplungspunkte zwischen den Sektoren Strom, Wärme, Gas, Mobilität und Industrie weisen die größten Resilienzdefizite auf und wie lassen sich diese systematisch priorisieren?
- Wie lassen sich Kaskadeneffekte infolge technischer Ausfälle, Cyberangriffe und klimabedingter Belastungen modellieren und welche Resilienzprinzipien sind für Kopplungstechnologien und digitale Steuerungsarchitekturen abzuleiten?

- Welche Compound-Risiken entstehen durch das Zusammenwirken klimabedingter Infrastrukturbelastungen mit technischen oder digitalen Störungen und welche Schutz- bzw. Resilienzmaßnahmen ergeben sich daraus?
- Wie können die identifizierten Resilienzkriterien und Schwachstellen in einen Bewertungsrahmen für zukünftige FTI-Förderschwerpunkte überführt werden?
- Welche Forschungs-, Technologie- und Innovationsbedarfe ergeben sich daraus und welche Schlüsseltechnologien, Systemlösungen und Demonstrationsvorhaben sollten künftig prioritär adressiert werden?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.9 Demokratische Resilienz und Informationsintegrität

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Für die Integrität demokratischer Prozesse stellen Informationsmanipulation (z. B. Desinformation, Foreign Information Manipulation and Interference) sowie Meinungsbildungsprozesse in sozialen Medien und mit Hilfe von künstlicher Intelligenz (z. B. Modellkollaps) wachsende Herausforderungen und Bedrohungen dar. Ziel ist daher die Entwicklung neuer Forschungsansätze zur Stärkung von Informationsintegrität, elektoraler Resilienz und epistemischer Souveränität.

Der Mehrwert eines solchen Forschungsansatzes liegt in der konsequenten Erweiterung des Begriffs der kritischen Infrastruktur um demokratische Prozesse, die Stärkung vorausschauender Sicherheitspolitik sowie die Sicherung von Informationsintegrität und demokratischer Resilienz.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie beeinflusst Informationsmanipulation die elektorale Integrität? Analyse von Desinformation sowie der Verwendung von KI-Inhalten als Informationsquelle im Kontext von Wahlen und demokratischen Entscheidungsprozessen; Identifikation von Risiken für institutionelles Vertrauen und öffentliche Meinungsbildung
- Was sind gesellschaftliche Verwundbarkeiten und Resilienzfaktoren? Untersuchung von Polarisierung, Vertrauensverlust und Fragmentierung als Angriffspunkte; Entwicklung von Indikatoren für kognitive und demokratische Resilienz
- Welche Möglichkeiten der Governance digitaler Kommunikationsräume gibt es? Analyse von Plattformlogiken und algorithmischer Kuratierung
- Was sind mögliche Szenarien und Policy-Entwicklungen? Entwicklung von Szenarien zu Informationsangriffen, Durchführung partizipativer Formate.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.10 Digitale Souveränität kritischer Infrastruktursysteme zum Schutz öffentlicher Sicherheit durch resilienzorientierte, modulare IT-Architekturen

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Derzeit ist eine zunehmende Marktverschiebung von On-Premise-Systemen hin zu Cloud-basierten Lösungen festzustellen, die durch Kosten-, Skalierungs- und Innovationsdruck getrieben wird. Diese Entwicklung führt zu steigenden Abhängigkeiten von externen Anbietern und Infrastrukturen und birgt insbesondere für sicherheitskritische Systeme Risiken hinsichtlich Konnektivität, Verfügbarkeit, Kontrolle und strategischer Handlungsfähigkeit.

Es soll daher untersucht werden, wie ein Rahmenwerk zur Stärkung der digitalen Souveränität kritischer Infrastrukturen ausgestaltet sein soll, das staatliche und infrastrukturelle Akteure dabei unterstützt, resiliente, unabhängige und zukunftssichere IT-Architekturen zu gestalten und zu bewerten.

Im Fokus steht ein systemischer Ansatz, der

- Anforderungen an Konnektivität, Verfügbarkeit und Ausfallsicherheit,
- Cloud- und On-Premise-Architekturen sowie hybride Betriebsmodelle,
- Anbieterabhängigkeiten (Vendor Lock-in) und technologische Souveränität,
- sowie modulare, interoperable und standardbasierte IT-Architekturprinzipien
- integriert, um IT-Architekturen hinsichtlich ihrer Souveränität und Resilienz zu analysieren, zu evaluieren und zu gestalten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse der Auswirkungen der zunehmenden Verlagerung von On-Premise- zu Cloud-basierten IT-Architekturen auf die digitale Souveränität kritischer Infrastrukturen
- Erhebung und Systematisierung von Anforderungen an Konnektivität, Ausfallsicherheit und Betriebsstabilität im Kontext kritischer Infrastruktursysteme
- Vergleich und Bewertung von Cloud-, On-Premise- und hybriden IT-Architekturen hinsichtlich ihrer Eignung zur Gewährleistung von Souveränität und Resilienz
- Entwicklung eines systemischen Bewertungsmodells zur Evaluierung von IT-Architekturen unter Berücksichtigung von Souveränitäts- und Resilienzkriterien
- Identifikation und Ausarbeitung modularer, interoperabler und standardbasierter Architekturprinzipien zur Reduktion von Abhängigkeiten und zur Erhöhung der technologischen Souveränität.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.11 Erhebung technischer und inhaltlicher Rahmenbedingungen für eine Fact-Checking-Anwendung mit Fokus auf migrationsbezogene und -relevante Themen und Inhalte

Kontakt: Bundesministerium für Inneres (BMI)

E-Mail: BMI-I-S-3-SiFo@bmi.gv.at

Falschinformationen und gezielt verbreitete Desinformationen spielen im Kontext von Migration eine zunehmend bedeutende Rolle. Insbesondere Personen, die Migration erwägen oder sich bereits auf dem Weg befinden, sind häufig mit irreführenden Informationen über Einreisebestimmungen, Arbeitsmöglichkeiten, und realistischen Perspektiven in Zielländern konfrontiert. Reale Gefahren und wahre Kosten von illegaler Migration werden von den Schleppern verschwiegen.

Ziel einer F&E Dienstleistung zu diesem Schwerpunkt ist die wissenschaftlich fundierte Erarbeitung der technischen, organisatorischen, rechtlichen und inhaltlichen Rahmenbedingungen für eine potenzielle Fact-Checking-App zum Themenfeld Migration. Im Mittelpunkt steht die Frage, wie eine solche Anwendung ausgestaltet werden müsste, um Falschinformationen und gezielt verbreitete Desinformation wirksam identifizieren, aufbereiten und zielgruppengerecht kommunizieren zu können. Die betreffende F&E Dienstleistung umfasst ausdrücklich keine Entwicklung oder Implementierung einer Anwendung, sondern dient als vorbereitende Forschungs- und Konzeptionsphase.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse der Informationsbedürfnisse und Mediennutzung der definierten Zielgruppen in Herkunftsländern sowie entlang ausgewählter Migrationsrouten
- Identifikation typischer Falschinformationen, irreführender Narrative und Desinformationskampagnen im Migrationskontext sowie legaler Alternativen
- Technischer und funktionaler Anforderungskatalog für eine mögliche App
- Empfehlungen zu Inhaltsstrategie, Qualitätssicherung und Fact-Checking-Prozessen
- Bewertung rechtlicher, datenschutzrechtlicher und ethischer Anforderungen.
- Empfehlungen zu Governance, Betrieb und organisatorischer Einbettung
- Konzept für eine mögliche spätere Pilotierung und Weiterentwicklung.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.12 CyberSecSenior

Kontakt: Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK)

Abteilung V/A/6: Seniorenpolitische Grundsatzfragen und Freiwilligenangelegenheiten; Mag. Anton Hörting

E-Mail: va6@sozialministerium.gv.at

Insbesondere ältere Menschen (60 Jahre und älter) mit geringen digitalen Kompetenzen sind stark gefährdet, Opfer von Cyber Angriffen (Social Engineering, Phishing, KI-gestützte Täuschungen, Deepfakes, Malware und Identitätsdiebstahl) zu werden. Gründe sind physiologische (z.B. kognitiver Abbau) und psychologische Faktoren (z.B. erhöhte Angst vor Cyberkriminalität), familiäre Risiken (z.B. Betrug im

eigenen Umfeld) und soziokulturelle Aspekte (z.B. Isolation). Senior:innen melden Cyberangriffe allerdings seltener als andere Altersgruppen. Die rasante Entwicklung von Künstlicher Intelligenz verschärft diese Lage weiter: Fake-Bilder bzw. Videos, Sprachnachrichten, Anrufe oder Profile können heute schnell und realistisch erzeugt werden. Ziel bei CyberSecSenior ist es, das Kompetenzlevel der Senior:innen zu Digitalisierung/KI und Cybersecurity zu heben, altersadäquate Ausbildungsangebote und eine Roadmap zur Umsetzung zu entwickeln und die digitale Kluft zu verringern.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung von Anforderungen bzw. Status-Quo-Analyse unter Einbindung von Stakeholdern und Senior:innen
- Identifikation und Analyse zu Methoden und Themeninhalten bestehender Schulungsangeboten zu Digitalisierung und Cybersicherheit für Senior:innen
- Identifikation von Best Practice Beispielen zur Vermittlung von digitalen Kompetenzen mit Fokus auf Cyber Security Skills bei älteren Menschen (inkl. Gamification etc.)
- Erarbeitung einer senior:innenspezifischen Methodensammlung bzw. eines Toolkits für eine effektive und niederschwellige kompetenzangepasste Wissensvermittlung zu Cybersecurity
- Erarbeitung spezifischer Handlungsempfehlungen und einer Roadmap zur Erreichung eines einheitlichen Bildungsgrads zu Digitalisierung und Cybersecurity für Senior:innen und zum Aufbau geeigneter Schutzmaßnahmen für ältere Menschen sowie barrierefreier Anlaufstellen im Fall von Vorfällen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.5 KIRAS/K-PASS KMU Initiative Innovation AKUT

Im Rahmen der KIRAS/K-PASS KMU Initiative Innovation AKUT wird ausschließlich des Instrumentes „F&E-Dienstleistung“ verwendet. Die allgemeinen Informationen über F&E-Dienstleistungen finden Sie im Leitfaden für Forschungs- und Entwicklungsdienstleistungen. Die KIRAS/K-PASS Innovation AKUT ist eine Sonderform der F&E-Dienstleistung, deswegen sind die im Folgenden erwähnten speziellen Regelungen ausschlaggebend und beschränken die allgemeineren Regelungen des Leitfadens für Forschungs- und Entwicklungsdienstleistungen.

F&E-Dienstleistungen sind definiert durch die Erfüllung eines Ausschreibungsinhaltes in einem bestimmten Zeitraum. Die Leistungserbringung erfolgt durch F&E-Tätigkeiten. Die Leistung steht im öffentlichen Interesse und ist in geteilten Rechten durch den Auftragnehmer und durch den Auftraggeber zu verwerten. Allgemein gelten Dienstleistungen als F&E-Dienstleistungen, wenn sie darauf ausgerichtet sind, neue Erkenntnisse zu gewinnen, ab TRL 6 – 7 in Ausnahmefällen TRL 8, sofern es sich nicht nur um Zertifizierungsmaßnahmen handelt.

Verwendet wird das FFG-Instrument „F&E-Dienstleistung“ mit folgenden Einschränkungen:

- Maximale Vertragssumme 100.000.- Euro inkl. ev. Ust. Eine höhere Einreichung führt daher zu einer Formalablehnung
- Laufzeit max. 12 Monate, eine Verlängerung der Laufzeit kann in begründeten Ausnahmefällen gewährt werden
- TRL Bereich 6 – 7, in Ausnahmefällen TRL 8 (ohne Zertifizierungsmaßnahmen)
- Konsortialvorschrift: Die BIEGE/ARGE muss aus mindestens einem österreichischen KMU und mindestens einem Bedarfsträger bestehen
- Ausländische Partner können teilnehmen, allerdings keine Finanzierung erhalten
- Die Finanzierung wird unter der Voraussetzung gewährt, dass das entwickelte Produkt/Verfahren bis zum Ende der Projektlaufzeit in geeigneter Form präsentiert/demonstriert wird; dies ist mit FFG und BMF abzustimmen
- Eine vorhergehende Förderung oder Finanzierung in KIRAS/K-PASS ist von Vorteil, aber keine verpflichtende Voraussetzung für eine Teilnahme
- Zur Erreichung der Wirkungsoptimierung des Instruments ist ein Finanzierungsanteil des/r beteiligten KMU von zumindest 50% in der Bietergemeinschaft anzustreben.

Für die KIRAS/K-PASS KMU Innovation AKUT Ausschreibung stehen max. 1.000.000 Euro zur Verfügung. Mehrere Ausschreibungen pro Jahr sind geplant.

Die Ausschreibungsschwerpunkte sind im Kapitel 3.2 (für KIRAS. Schutz kritischer Infrastruktur) und Kapitel 3.4 (für K-PASS. Cybersicherheit) angeführt.

Es können alle F&E-Dienstleistungen eingereicht werden, welche die Themen Schutz kritischer Infrastruktur allgemein und Cybersicherheit allgemein treffen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.6 AT-DE Bilaterale Ausschreibung

Hinweise zur Antragsstellung für österreichisch-deutsche Konsortien

Seit April 2013 besteht eine Vereinbarung zur Kooperation auf dem Gebiet der "Forschung für die zivile Sicherheit". Mit der bilateralen Zusammenarbeit wollen Österreich und Deutschland die Sicherheit in ihren Ländern und in Europa stärken.

Im Zuge dieser KIRAS Ausschreibung 2026 können Projekte, die sich dem allgemeinen Schwerpunkt „Schutz kritischer Infrastruktur“ des Instruments „KIRAS Kooperative F&E Projekte“ widmen, als österreichisch-deutsches Konsortium eingereicht werden. Unter einem österreichisch-deutschen Konsortium wird ein gemeinsamer Verbund aus österreichischen und deutschen Partnern mit sich ergänzenden Kompetenzen verstanden, die in einem gemeinsamen Projekt zusammenarbeiten und gemeinsame Ergebnisse erzeugen.

Die Antragsteller nutzen zur Antragstellung ihre jeweiligen nationalen Formulare für den fachlichen und administrativen Teil - wie in den jeweiligen nationalen Ausschreibungen dargestellt. Weiterhin erstellen die österreichischen und deutschen Antragsteller eines bilateralen Konsortiums gemeinsam ein Exposé zur bilateralen Zusammenarbeit. Die Anträge sind bei beiden Agenturen bzw. Projektträgern, bis zur nationalen Abgabefrist, einzureichen.

Der österreichische Teil des Konsortiums muss seinen Vollantrag bei der österreichischen Forschungsförderungsgesellschaft vorlegen. Deutsche Antragsteller müssen ihre Projektskizze beim VDI Technologiezentrum einreichen.

Weitere Informationen zur Ausgestaltung des [Exposés](#), sowie die [Hinweise zur Antragstellung](#) für österreichisch-deutsche Konsortien finden Sie auf der [Webseite der Ausschreibung](#).

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

4 INSTRUMENTE UND ANFORDERUNGEN

4.1 Kooperatives F&E-Projekt

4.1.1 Konsortien

Konsortien für kooperative F&E-Projekte müssen aus mindestens zwei Partnern bestehen. Die Anzahl der Projektteilnehmer ist nach oben formal nicht begrenzt.

Über diese standardisierte Auflage hinausgehend müssen sich bei allen kooperativen F&E-Projekten im Rahmen von KIRAS/K-PASS:

- mindestens ein Bedarfsträger aus dem öffentlichen oder privaten Bereich als Konsortialteilnehmer
- mit mindestens einem Partner aus der Wissenschaft (universitäre oder außeruniversitäre Forschungseinrichtung) als Konsortialteilnehmer und
- einem Partner aus der Wirtschaft als Konsortialteilnehmer sowie
- einem Vertreter der Geistes-, Sozial- und Kulturwissenschaften (GSK) als Konsortialteilnehmer oder Subauftragnehmer des Konsortiums,

zusammenschließen (mindestens 1+1+1(+1) Partner).

Für das Konsortium kann nur ein Projektpartner (Unternehmen, Forschungseinrichtung) mit Standort in Österreich gegenüber der FFG als Konsortialführer auftreten.

Die Ausschreibung wendet sich inhaltlich auch an Organisationen des Bundes. Mit dem Bund idente Bedarfsträger können zwar als Projektpartner einreichen, jedoch erhalten keine Förderung.

Der GSK-Partner soll all jene Probleme oder Hindernisse adressieren, die mit dem Gebrauch der technischen Lösung im Realbetrieb einhergehen. Der GSK-Partner muss eigenständig und unabhängig sein.

Die Förderung der ausländischen Beteiligten beträgt maximal 20 % der Gesamtförderung.

Die Grenze für Drittkosten liegt bei 20 % der Gesamtkosten je Partner. Liegen sie darüber, muss die Überschreitung in der Projektbeschreibung begründet werden. Insgesamt dürfen die Drittkosten 20 % der Gesamtprojektkosten nicht überschreiten.

Beachten Sie den Leitfaden für Kooperative F&E-Projekte.

4.1.2 Forschungskategorien

Forschungs- und Entwicklungsprojekte können als kooperative Projekte eingereicht werden. Von der Projektart sind Industrielle Forschung und Experimentelle Entwicklung mit unterschiedlichen Maximalfördersätzen vorgesehen.

Details zu den Forschungskategorien, sowie Fragen die eine Einstufung in die Projektkategorie erleichtern, finden Sie in dem Leitfaden für Kooperative F&E-Projekte.

4.1.3 Verwertung

Bei Einreichung von Kooperativen F&E-Projekten müssen folgende Voraussetzungen zwingend beachtet werden: ein zentrales Ziel angewandter Forschung ist die wirtschaftliche Verwertung von Ergebnissen, planen sie daher verpflichtend entsprechende weiterführende Maßnahmen wie ein Beratungsgespräch bei einer öffentlichen Wirtschaftsförderungsagentur im Projektverlauf oder die Nutzung der KIRAS/K-PASS KMU Initiative Innovation AKUT nach Projektende ein.

4.2 F&E-Dienstleistung

4.2.1 Allgemein

Es werden Studien und studienähnliche Vorhaben im Rahmen des aktuellen Schwerpunktes finanziert. Zielgruppe sind Nutzer im weiteren Sinne. Die beauftragten Maßnahmen können eigenständige Vorhaben darstellen oder in direktem Zusammenhang mit anderen Projekten aus KIRAS/K-PASS stehen.

Aufgrund der Breite des Themas können grundsätzlich all jene Studien bzw. studienähnlichen Vorhaben beauftragt werden, die dazu beitragen, das Gemeinwesen in Österreich sicherer und stabiler zu gestalten (z.B. Studien zur Perzeption von Sicherheit und Sicherheitstechnologien, Machbarkeitsstudien, etc.). Diese Maßnahmen können auch einen Beitrag dazu leisten, dass oben genannter umfassender Sicherheitsbegriff in Berücksichtigung der KIRAS/K-PASS Ziele weiterentwickelt und für Teilbereiche näher definiert wird.

Beachten Sie den Leitfaden für Forschungs- und Entwicklungsdienstleistungen. Zu den speziellen Anforderungen des F&E-Dienstleistungsfokus KIRAS/K-PASS KMU Innovation AKUT siehe Kapitel 3.5.

4.2.2 Bietergemeinschaften

Das Instrument richtet sich an Partner aus den Bereichen Wirtschaft und Wissenschaft sowie an Bedarfsträger. Für eine BIEGE/ARGE kann nur ein Unternehmen oder Forschungseinrichtung mit Standort in Österreich gegenüber der FFG als Einzelbieter bzw. BIEGE/ARGE- Leiter auftreten.

Die Ausschreibung wendet sich inhaltlich auch an Organisationen des Bundes. Mit dem Bund idente Bedarfsträger können zwar nicht als BIEGE/ARGE- Leiter auftreten, sind jedoch ermutigt sich an der Ausschreibung zu beteiligen.

Im Falle einer BIEGE/ARGE können ausländische Partner teilnehmen, allerdings dürfen diese nicht mehr als 20 % der Finanzierung bekommen.

Die Grenze für Drittkosten liegt bei 20 % der Gesamtkosten je Partner. Liegen sie darüber, muss die Überschreitung in der Projektbeschreibung begründet werden. Insgesamt dürfen die Drittkosten 20 % der Gesamtprojektkosten des Projekts nicht überschreiten.

4.2.3 Auflagen und Bedingungen durch Jury

Im Rahmen des Bewertungsverfahrens für „Forschungs- und Entwicklungsdienstleistungen“ können von der Jury zusätzliche Auflagen unter den im folgenden Abschnitt angeführten Rahmenbedingungen definiert werden, welche in weiterer Folge Vertragsbestandteil werden. Hierbei handelt es sich um eine abschließende Aufstellung aller durch die Jury gegebenenfalls dem einzelnen Bieter/der einzelnen Bieterin vorzuschreibenden Auflagen und Bedingungen.

Das Anbot muss eine detaillierte Personalkostenplanung sowie ausreichende Belege (Lebensläufe) für den Nachweis der korrekten Einstufung aller am Projekt beteiligten Personen beinhalten. Während des Begutachtungsprozesses können die Personalkosten um bis zu 50 % gekürzt werden, wenn:

- Der für die F&E-Dienstleistung beantragte Personalaufwand in seiner Höhe im Anbot nicht detailliert und nachvollziehbar begründet wurde oder
- die Angemessenheit der Kosten nicht gegeben ist (z.B. der Inhalt eines Lebenslaufs die für das Projekt getätigte Einstufung der Funktion des entsprechenden Mitarbeiters nicht ausreichend belegt).

Bei für das Projekt vorgesehener Reisetätigkeit muss das Anbot eine detaillierte Reiseplanung sowie eine realistische Reisekostenschätzung (Preis) beinhalten. Der Jury ist es vorbehalten, die beantragten Reisetätigkeiten gesamt oder nur in Teilen anzuerkennen. Während des Begutachtungsprozesses können die Reisekosten um bis zu 50 % gekürzt werden, wenn:

- der Aufwand an Reisetätigkeit im Anbot nicht detailliert und nachvollziehbar begründet wurde, oder
- die Angemessenheit der Kosten nicht gegeben ist.

Arbeitspakete können ganz oder zum Teil gestrichen werden. Die Projektgesamtkosten sind in diesem Fall anteilmäßig zu reduzieren. Ein überarbeiteter Kostenplan ist in diesem Fall vom Bieter/der Bieterin im eCall der FFG vorzulegen. Arbeitspakete oder Teile davon können durch die Jury gemäß den nachfolgenden Parametern gekürzt werden, wenn:

- eine angebotene Leistung enthalten ist, welche für die Zielerreichung des Projekts nicht notwendig erscheint oder
- eine angebotene Leistung, welche bereits durch ein nationales bzw. EU-Projekt hinreichend abgedeckt ist.

4.2.4 Weitere Anforderungen und Vorgaben zur Einreichung von F&E- Dienstleistungen

Folgende Nachweise sind als Anhang im eCall hochgeladen:

- Auszug aus dem Gewerberegister oder beglaubigte Abschrift des Berufsregisters oder des Handelsregisters des Herkunftslandes des:der Bietenden oder die dort vorgesehene Bescheinigung oder – falls im Herkunftsland keine Nachweismöglichkeit besteht – eine eidesstattliche Erklärung des Bewerbers, jeweils nicht älter als 12 Monate
- Bietende, die im Gebiet einer anderen Vertragspartei des EWR-Abkommens oder in der Schweiz ansässig sind und die für die Ausübung einer Tätigkeit in Österreich eine behördliche Entscheidung betreffend ihre Berufsqualifikation

einholen müssen, haben ein darauf gerichtetes Verfahren möglichst umgehend, jedenfalls aber vor Ablauf der Angebotsfrist einzuleiten. Gleiches gilt für Subunternehmende, an die der:die Bietende Leistungen vergeben will. Der:die Bietende hat den Nachweis seiner:ihrer Befugnis durch die Vorlage der entsprechenden Gewerbeberechtigung grundsätzlich in seinem:ihrer Angebot zu führen. Die Auftraggeberin behält sich vor, die Befugnis von allfälligen Subunternehmern gesondert zu prüfen

- Aktueller Firmenbuchauszug (max. 6 Monate alt)
- Der:die Bietende hat auch einen Nachweis über den Gesamtumsatz und die Umsatzentwicklung für die letzten drei Jahre bzw. für den seit Unternehmensgründung bestehenden Zeitraum bei Newcomer:innen (darunter sind Unternehmen zu verstehen, die vor weniger als drei Jahren gegründet wurden) vorzulegen.

5 AUSSCHREIBUNGSDOKUMENTE

Reichen Sie das Projekt ausschließlich elektronisch via [eCall](#) ein.

Die Einreichung beinhaltet folgende **online** Elemente, die im [eCall](#) unter folgenden Menüpunkten zu erfassen sind:

- **Inhaltliche Beschreibung** umfasst die Darstellung der Projektinhalte
- **Arbeitsplan** beinhaltet die Darstellung der Arbeitspakete und Elemente des Projektmanagements wie Zeit-Managementplan (GANTT-Diagramm), Aufgaben, Meilensteine, Ergebnisse
- **Konsortium** beschreibt die Expertise der einzelnen Konsortiumsmitglieder
- **Kosten und Finanzierung** beschreibt alle Kostenkategorien pro Konsortiumsmitglied. Die Summen je Arbeitspaket werden automatisch im online Arbeitsplan angezeigt
- Die Risikomatrix ist als Grundlage zur Beurteilung des Risikos und des Risikomanagements im Projekt als Anhang zum inhaltlichen Antrag im eCall hochzuladen
- Als Teil des elektronischen Antrags können etwaige Anhänge (wie bspw. LOIs) über die eCall Upload-Funktion hochgeladen werden
- Sämtliche relevante Dokumente für die Ausschreibung finden Sie auf der [Webseite der Ausschreibung](#).

Die nachfolgende Übersicht zeigt für die jeweiligen Instrumente die relevanten Dokumente. Weitere Hinweise finden Sie im [Tutorial](#) und unter den [FAQs](#).

Tabelle 3: Ausschreibungsdokumente

Förderungs- /Finanzierungsinstrument bzw. sonstige Information	Verfügbare Ausschreibungsdokumente
Kooperative F&E-Projekte	– Leitfaden für Kooperative F&E-Projekte (v5.2) Als Anhang zum inhaltlichen Antrag - Upload als PDF im eCall : – Risiko Management Tabelle – MOU für Kooperative F&E Projekte – Antrag auf Klassifizierung – Angaben zur Einordnung des Vorhabens – Angabe zu Arbeitsplätzen – Eidesstattliche Erklärung zum KMU-Status (bei Bedarf)
F&E-Dienstleistungen	– Leitfaden für Forschungs- und Entwicklungsdienstleistungen (v5.1) Als Anhang zum inhaltlichen Antrag - Upload als PDF im eCall : – Risiko Management Tabelle – MOU für F&E-Dienstleistungen – Antrag auf Klassifizierung – Angaben zur Einordnung des Vorhabens – Angabe zu Arbeitsplätzen – Mustervertrag
Allgemeine Regelungen zu Kosten	– Kostenleitfaden (v3.2)

Hinweis: Die eidesstattliche Erklärung zum KMU-Status ist für unternehmerisch tätige Vereine, Einzelunternehmen und ausländische Unternehmen notwendig. In der zur Verfügung gestellten Vorlage muss – sofern möglich – eine Einstufung der letzten 3 Jahre lt. KMU-Definition vorgenommen werden

6 FÖRDERUNGS-/FINANZIERUNGSENTSCHEIDUNG UND RECHTSGRUNDLAGEN

Das Bundesministerium für Finanzen (BMF) trifft die **Förderungs- bzw. Finanzierungsentscheidung** auf Basis der Förderungs- bzw. Finanzierungsempfehlung des Bewertungsgremiums.

Die Ausschreibung basiert auf der [Sonderrichtlinie KIRAS](#) und [Sonderrichtlinie K-PASS](#) für die Österreichische Forschungsförderungsgesellschaft mbH zur Förderung von Sicherheitsforschung.

Bezüglich der Unternehmensgröße ist die jeweils geltende KMU-Definition gemäß EU-Wettbewerbsrecht ausschlaggebend. Hilfestellung zur Einstufung finden sie auf der [KMU-Seite der FFG](#).

Sämtliche EU-Vorschriften sind in der jeweils geltenden Fassung anzuwenden.

Als **Rechtsgrundlage für „Forschungs- und Entwicklungsdienstleistungen“** wird der Ausnahmetatbestand § 9 Z 12 Bundesvergabegesetz 2018 angewendet.

7 WEITERE INFORMATIONEN

In diesem Abschnitt finden Sie Informationen über weitere Förderungsmöglichkeiten und Services, die im Zusammenhang mit Förderungsansuchen bzw. geförderten Projekten für Sie hilfreich sein können.

7.1 Hinweise zum Kostenplan

Der Konsortialführung obliegt das Projektmanagement sowie die Kommunikation mit der Förderungsstelle und den Projektpartner:innen. Dazu gehören die Prüfung der Kostenpläne aller Partner:innen im Hinblick auf Projektrelevanz, genehmigungskonforme Kostenhöhe, genehmigungskonforme Projektentwicklung und vorgabengetreue (Förderungsrichtlinien, Leitfaden) Förderungsansuchen der Partner:innen anhand der – von den Partner:innen bekannt gegebenen – Daten und Angaben. Beim Feststellen von Mängeln (lt. Checkliste) bei den Förderungsansuchen der Partner:innen sind diese im Kostenplan vom/von der jeweilige/n Partner:in zu korrigieren und die korrekte Version der Konsortialführung zu übermitteln.

7.2 Service FFG Projektdatenbank

Die FFG bietet als Service die Veröffentlichung von kurzen Informationen zu geförderten Projekten und eine Übersicht der Projektbeteiligten in einer öffentlich zugänglichen [FFG Projektdatenbank](#) an. Somit können Sie Ihr Projekt und Ihre Projektpartner besser für die interessierte Öffentlichkeit positionieren. Darüber hinaus kann die Datenbank zur Suche nach Kooperationspartnern genutzt werden.

Nach positiver Förderungsentscheidung werden die Antragstellenden im eCall System über die Möglichkeit der Veröffentlichung von kurzen definierten Informationen zu ihrem Projekt in der FFG Projektdatenbank informiert. Eine Veröffentlichung erfolgt ausschließlich nach aktiver Zustimmung im eCall System.

Nähere Informationen finden Sie auf der [FFG-Seite zur Projektdatenbank](#).

7.3 Open Access Publikationen

Die Sichtbarkeit und Verfügbarkeit von Projektergebnissen hat sich in Programmen des BMF bereits bestens bewährt. Auch die Europäische Kommission setzt mit ihrer Empfehlung (2012/417/EU) zu Open Access auf den verbesserten Zugang zu wissenschaftlichen Publikationen, um eine wissens- und innovationsgestützte Wirtschaft zu erleichtern.

Daher sollen Projektergebnisse des Programms über geeignete Plattformen wie die KIRAS-Portal oder eine Projektdatenbank der FFG publiziert und frei zugänglich gemacht werden. Bei dieser Ausschreibung werden die geförderten Projekte und deren Ergebnisse (z.B. in Form publizierbarer Kurzfassungen) auf den oben erwähnten Plattformen der Öffentlichkeit zur Verfügung gestellt. Davon ausgenommen sind vertrauliche Inhalte (z. B. Projekte mit Patentanmeldungen, anderen Schutzstrategien wie Geheimhaltung, oder personenbezogene Daten). Um die Projektergebnisse übersichtlich und verständlich aufzubereiten, werden Hinweise für die Berichtslegung zu Projekten, die im Rahmen von KIRAS/K-PASS gefördert und durchgeführt werden, sowie korrespondierende Veranstaltungen mit entsprechenden Vorgaben zum Berichtswesen geregelt.

Die mit öffentlicher Förderung erzielten Forschungsergebnisse sind einer bestmöglichen Verwertung für Wissenschaft, Wirtschaft und Gesellschaft zuzuführen. In diesem Sinne ist bei referierten Publikationen, die mit Unterstützung der durch die FFG vergebenen Förderung entstehen, Open Access soweit wie möglich anzustreben. Als Prinzip gilt „as open as possible, as closed as necessary“, wie es auch für die Europäischen Förderungen angeführt wird.

Publikationskosten zählen zu den förderbaren Projektkosten.

7.4 Umgang mit Projektdaten – Datenmanagementplan

Ein Datenmanagementplan (DMP) ist ein Managementtool, das dabei unterstützt, effizient und systematisch mit in den Projekten generierten Daten umzugehen.

Für die Erstellung des DMP kann z.B. das kostenlose Tool [DMP Online](#) verwendet werden. Auch die Europäische Kommission bietet über ihre „[Guidelines on FAIR Data Management](#)“ Hilfestellung an.

Ein Datenmanagement-Plan beschreibt:

- welche Daten im Projekt gesammelt, erarbeitet oder generiert werden
- wie mit diesen Daten im Projekt umgegangen wird
- welche Methoden und Standards dabei angewendet werden
- wie die Daten langfristig gesichert und gepflegt werden und
- ob es geplant ist, Datensätze Dritten zugänglich zu machen und ihnen die Nachnutzung der Daten zu ermöglichen (sogenannter „Open Access zu Forschungsdaten“).

Es ist sinnvoll, Forschungsdaten, die referierten Publikationen zugrunde liegen und deren Veröffentlichung zur Reproduzierbarkeit und Überprüfbarkeit der publizierten Ergebnisse notwendig ist, offen verfügbar zu machen.

Werden Daten veröffentlicht, sollen die Grundsätze „auffindbar, zugänglich, interoperabel und wiederverwertbar“ berücksichtigt werden. Für eine optimale Auffindbarkeit empfiehlt es sich, die Daten in etablierten und international anerkannten Repositorien zu speichern.

7.5 Weitere Förderungsmöglichkeiten der FFG

Sie interessieren sich für andere Förderungsmöglichkeiten der FFG?

Das **Förderservice** ist die zentrale Anlaufstelle für Ihre Anfragen zu den Förderungen und Beratungsangeboten der FFG. Kontaktieren Sie uns, wir beraten Sie gerne!

Kontakt: FFG-Förderservice, T: +43 (0) 57755-0, E: foerderservice@ffg.at

Web: <https://www.ffg.at/foerderservice>

Weitere Förderungsmöglichkeiten der FFG finden Sie weiters [hier](#).

8 ANHANG: CHECKLISTE FÜR DIE ANTRAGSEINREICHUNG

Bei der Formalprüfung wird das Förderungs- bzw. Finanzierungsansuchen auf formale Richtigkeit und Vollständigkeit geprüft. Bitte beachten Sie: **Sind die Formalvoraussetzungen nicht erfüllt und handelt es sich um nicht-behebbarer Mängel, wird das Förderungs- bzw. Finanzierungsansuchen bei der Formalprüfung aufgrund der erforderlichen Gleichbehandlung aller Förderungs- bzw. Finanzierungsansuchen ausnahmslos aus dem weiteren Verfahren ausgeschieden und formal abgelehnt.**

Tabelle 4: Formalprüfungsscheckliste

Kriterium	Prüfinhalt	Mangel behebbar	Konsequenz
Die Projektbeschreibung ist ausreichend befüllt vorhanden und es wurde die richtige Sprache verwendet.	Die Online-Projektbeschreibung ist vollständig auszufüllen. Sprache: Deutsch	Nein	Ablehnung aus formalen Gründen
Die verpflichtenden Anhänge gem. Ausschreibung liegen vor. [behebbar]	Zum Beispiel: Interessensbekundungen, Absichtserklärungen (Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Ja	Korrektur per eCall nach Einreichung
Der/Die Förderungswerbende ist berechtigt, einen Antrag einzureichen.	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Bei Konsortien: Die Projektbeteiligten sind teilnahmeberechtigt.	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Mindestanforderungen an das Konsortium	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Projektlaufzeit	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Höhe der Förderung/Finanzierung	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen
Die im Ausschreibungsleitfaden angegebene Forschungskategorie, je nach Ausschreibungsschwerpunkt ist einzuhalten	(Angaben lt. Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen