



FFG
Forschung wirkt.



Bundesministerium
Finanzen

AUSSCHREIBUNG 2022
EINREICHFRIST: 17.03.2023



KIRAS

DAS ÖSTERREICHISCHE FÖRDERUNGSPROGRAMM FÜR SICHERHEITSFORSCHUNG

AUSSCHREIBUNGSLEITFADEN



IMPRESSUM

Eigentümer, Herausgeber und Medieninhaber

Bundesministerium für Finanzen (BMF)
Radetzkystraße 2, 1030 Wien

Programmverantwortung KIRAS

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

Programmabwicklung

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

Wien, Dezember 2022

INHALTSVERZEICHNIS

TABELLENVERZEICHNIS.....	7
1 DAS WICHTIGSTE IN KÜRZE	8
2 MOTIVATION	10
2.1 Hintergrund.....	10
2.2 Zielgruppen und Förderwerber.....	11
2.3 Die Möglichkeit der Klassifizierung	12
3 AUSSCHREIBUNGSSCHWERPUNKTE	13
3.1 Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für kooperative F&E-Projekte	13
3.1.1 Datengetriebener Mangelradar für die wirtschaftliche Krisenvorsorge	13
3.1.2 FMCG-Monitoring zur Sicherstellung einer resilienten Daseinsvorsorge der österreichischen Bevölkerung.....	15
3.1.3 Wissenschaftliche Analyse einer breiten Teststellung von E-Fahrzeugen im praxisnahen Polizeieinsatz.....	16
3.1.4 Sicherstellung der Kommunikation in krisenhaften Situationen.	17
3.1.5 Entwicklung eines Verfahrens und eines IT-gestützten Demonstrators zur Beobachtung und Analyse von Rücküberweisungen in relevante Herkunftsländer von irregulärer Migration	19
3.1.6 Erkennungsdienstliche Behandlung.....	20
3.1.7 Mobile digitale Aufnahmetechnologie für Schuhspurenerfassung	21
3.1.8 UAV-UGV-Teaming zur kooperativen Raumüberwachung von sicherheitsrelevanten Gebieten	22
3.1.9 Erhöhung der Sicherheit und Effizienz im Strafvollzug durch digitalisierte und automatisierte Prozesse.....	23
3.1.10 Kombination einer Notstromversorgung basierend auf erneuerbarer Energieerzeugung und innovativen Speichersystemen mit Energiegemeinschaften.....	25
3.1.11 Krisenbevorratung von Lebensmitteln und landwirtschaftlichen Produktionsmitteln	26
3.1.12 Erhebung und Berechnung von geologischen sowie geographischen Daten mittels der Kombination von Feldmethoden und der Geoanalyse von Satellitenbildern.....	28
3.1.13 Kontaminationsmonitor - Feststellung von Kontaminationsrückständen mit optischen Detektionsmethoden	30
3.1.14 Assistenzsystem zur Einsatzführung im urbanen Umfeld	31
3.1.15 Alternative Technologien zur Detektion, Klassifizierung und Identifikation von Micro- und Mini-Drohnen	32

3.1.16	Mobilitätsdaten als Instrument des Krisen- und Pandemienmanagements.....	33
3.1.17	Abwassermonitoring als Instrument der Krisenprävention, sowie des Krisen- und Pandemienmanagements.....	34
3.1.18	Schutz kritischer Infrastruktur im Bereich AMR und Sicherstellung einer antimikrobiellen Therapie	35
3.1.19	Surveillance und Gewährleistung von Trinkwasser-Sicherheit und Wasser-Qualität	37
3.1.20	Neue Gefahren für die Gesundheit in Österreich durch klimawandel-bedingte, neu oder wieder auftretende Infektionskrankheiten und allergieauslösende Neobiota (Vektorübertragene Infektionskrankheiten,...).....	38
3.1.21	Resiliente Dateninfrastrukturen für Gesundheitskrisen	39
3.1.22	Mixed Reality Trainingsframework für das Trainieren von zivilen Expert:innen für den Einsatz bei Krisensituationen.....	40
3.1.23	Einbindung informeller Hilfsangebote in das Krisen- und Katastrophenmanagement.....	41
3.1.24	Digitaler Kompetenzausweis	42
3.1.25	Entwicklung eines Wissensmanagementsystems im Österreichische Feuerwehrewesen	43
3.1.26	Aufbau und Entwicklung einer innovativen Gebäudedatenbank zur Unterstützung der Analyse der physischen Verwundbarkeit von Gebäuden gegenüber Naturgefahren	44
3.1.27	Registerdatenbasierte Netzwerkanalysen zur Identifizierung krimineller Muster und strukturellen Risikos wie Steuerhinterziehung, Schattenwirtschaft, Geldwäsche und Strohmänner (PACC im BFF)	45
3.1.28	Drohnen in der Landwirtschaft.....	46
3.2	Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für F&E-Dienstleistungen	48
3.2.1	Vorurteils kriminalität in Österreich	48
3.2.2	Wirkungsweisen der Bewährungshilfe.....	49
3.2.3	Fremdenrecht und Strafrecht – Schnittpunkte und wechselseitige Abhängigkeiten	50
3.2.4	Modernes Haftmanagement durch Monitoring des sozialen Klimas in Justizanstalten	51
3.2.5	Zusammenhänge zwischen Partnergewalt, Geschlechterrollenbildern und psychischer Gesundheit / psychischen Erkrankungen	52
3.2.6	Psychosoziale Resilienz von Beschäftigten in kritischen Infrastrukturen	54
3.2.7	Prävention antisemitischer Gewalt im schulischen Umfeld – Antisemitismus als Herausforderung für die Schule.....	56
3.3	Cybersicherheit. Ausschreibungsschwerpunkte für kooperative F&E-Projekte	57
3.3.1	Erkennung von Deepfakes und medialen Manipulationen in großen Sammlungen digitaler Bild- und Videoinhalte.....	57

3.3.2	Früherkennung von Fake News und Desinformationskampagnen in sozialen Netzwerken	59
3.3.3	Resilienz von Supply Chains gegenüber Kaskadeneffekten aus dem digitalen Raum	61
3.3.4	Erhöhung der Cybersicherheit für Universitäten durch proaktiven Hackerschutz im ACOnet	62
3.3.5	Nachverfolgung von Virtual Assets im Decentralized Finance (DeFi)-Ökosystem, Blockchains von Stablecoins und anderen Cross-Chain-Modellen	63
3.3.6	Testen und Validieren moderner Systeme zur Erkennung von Cyber-Angriffen.....	64
3.3.7	Sichere Kommunikationsinfrastruktur für GSVP Missionen.....	65
3.3.8	Erhöhte Cybersicherheit für Österreichs Trinkwasserversorgung und Abwasserentsorgung.....	66
3.4	Cybersicherheit. Ausschreibungsschwerpunkte für F&E-Dienstleistungen	68
3.4.1	Anforderungen von KMU zur Cybersicherheit.....	68
3.4.2	Digitalisierungspotential von Services in der öffentlichen Sicherheit.....	69
3.4.3	Cybermobbing als Herausforderung für Pädagoginnen und Pädagogen	70
3.4.4	Cybersecurity-Literacy in der Wissensvermittlung der Sekundarstufe in Österreich.....	71
4	INSTRUMENTE UND ANFORDERUNGEN	73
4.1	Kooperatives F&E-Projekt	73
4.1.1	Konsortien	73
4.1.2	Forschungskategorien	74
4.2	F&E-Dienstleistung.....	74
4.2.1	Allgemein.....	74
4.2.2	Bietergemeinschaften	75
4.2.3	Auflagen und Bedingungen durch Jury	75
4.2.4	Weitere Anforderungen und Vorgaben zur Einreichung von F&E-Dienstleistungen	76
5	AUSSCHREIBUNGSDOKUMENTE.....	77
6	RECHTSGRUNDLAGEN	79
7	WEITERE INFORMATIONEN	79
7.1	Hinweise zum Kostenplan	79
7.2	Service FFG Projektdatenbank.....	80
7.3	Open Access Publikationen	80
7.4	Umgang mit Projektdaten - Datenmanagementplan	81
7.5	Weitere Förderungsmöglichkeiten der FFG.....	81

8 ANHANG: CHECKLISTE FÜR DIE ANTRAGSEINREICHUNG 82

TABELLENVERZEICHNIS

Tabelle 1: Instrumente und Ausschreibungsschwerpunkte	8
Tabelle 2: Beratungsmöglichkeiten.....	9
Tabelle 3: Ausschreibungsdokumente	78
Tabelle 4: Formalprüfungcheckliste	82

1 DAS WICHTIGSTE IN KÜRZE

Einreichung

Projektanträge sind bei der Österreichischen Forschungsförderungsgesellschaft (FFG) bis spätestens 17.03.2023, 12:00 Uhr 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.

Tabella 1: Instrumente und Ausschreibungsschwerpunkte

Förderungs-/ Finanzierungsinstrument	Kooperatives F&E Projekt	F&E-Dienstleistung
Kurzbeschreibung	Kooperatives F&E Projekt Industrielle Forschung (IF) oder Experimentelle Entwicklung (EE)	Erfüllung eines vorgegebenen Ausschreibungsinhaltes
Schwerpunkt 1	Schutz kritischer Infrastruktur Siehe Kapitel 3.1	Schutz kritischer Infrastruktur Siehe Kapitel 3.2
Schwerpunkt 2	Cybersicherheit Siehe Kapitel 3.3	Cybersicherheit Siehe Kapitel 3.4
Beantragte Förderung in €	min. 100.000 bis max. 2 Mio. €	keine Vorgabe
Finanzierungsquote	nicht anwendbar	100%
Förderungsquote	max. 85%	nicht anwendbar
Laufzeit in Monaten	max. 24 (und 12 Monate max. kostenneutrale Fristerstreckung)	max. 24 (und 12 Monate max. kostenneutrale Fristerstreckung)
Kooperationserfordernis	ja	nein
Sprache	Deutsch	Deutsch

Tabelle 2: Beratungsmöglichkeiten

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

Inhaltliche Beratungsgespräche allgemeiner Natur (siehe dazu im Detail Pkt. 2.2) können auf Wunsch eines potenziellen Antragstellers bis 03.03.2023 geführt werden. Terminvereinbarungen sind bis spätestens 24.02.2023 in schriftlicher Form an Herrn Christian Brüggemann (christian.brueggemann@ffg.at) zu stellen.

Formal- und Vertragsfragen sind ausschließlich schriftlich per E-Mail an Herrn Christian Brüggemann (christian.brueggemann@ffg.at) bis 03.03.2023 zu stellen.

Weiterführende Informationen / Links:

www.ffg.at/kiras und www.kiras.at

Information zur Einstufung in die Forschungskategorie:

Im Rahmen der Antragstellung wird das Vorhaben in die Forschungskategorie Industrielle Forschung oder Experimentelle Entwicklung eingestuft. Die Einstufung wird im Rahmen der Begutachtung geprüft und kann gegebenenfalls vom Bewertungsgremium geändert werden.

Beachten Sie im Rahmen der Antragstellung die näheren Erläuterungen zu den Forschungskategorien „Industrielle Forschung“ und „Experimentelle Entwicklung“, sowie die ergänzenden Angaben zu den TRLs (Technology Readiness Levels) im Anhang des [Instrumentenleitfadens Kooperative F&E Projekte \(v4.2\)](#).

Bitte beachten Sie:

Sind die Formalvoraussetzungen für eine Projekteinreichung entsprechend den Konditionen und Kriterien des jeweiligen Förderungsinstrumentes 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.

2 MOTIVATION

2.1 Hintergrund

Das nunmehr 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.

Die Gewährleistung von „Sicherheit“ ist eine staatliche und daher ressortübergreifende Kernaufgabe. Vor dem Hintergrund vielfältiger, sich in stetem Wandel befindlicher Bedrohungslagen für unsere Gesellschaft gilt es, innovative Ansätze für die Begegnung dieser Bedrohungen zu entwickeln. Darin manifestiert sich die unbedingte Notwendigkeit eines Beitrages von Forschung und Innovation bei der Begegnung der Herausforderung „Gewährleistung von Sicherheit“.

In KIRAS erfolgt die thematische Konzentration auf F&E-Projekte der Sicherheitsforschung, die den Schutz von kritischen Infrastrukturen behandeln.

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.

Die Sektoren, die als kritische Infrastrukturen gelten, sowie die strategischen Ziele sind in der [KIRAS-Sonderrichtlinie](#) beschrieben.

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, RFTE, u.a.).

Die enge Verzahnung mit der Sicherheitspolitik (Schwerpunktsetzung, Auswahlverfahren, etc.), die in KIRAS wie in keiner anderen Förderinitiative gegeben

ist, erlaubt in einem technologieoffenen Ansatz die ausschließliche Fokussierung auf sicherheitsrelevante Themen (i.S.v. „security“).

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 Integrierung von GSK-Aspekten
- die Möglichkeit der Klassifizierung von Projekten.

Selbstverständlich wird KIRAS keine Rüstungsforschung betreiben und sich klar von Rüstungsforschung abgrenzen. Das KIRAS-Programm hat einen eindeutigen und klaren zivilen Programmfokus, da Sicherheitsforschung hinsichtlich seiner verteidigungspolitischen Anforderungen keine wehrtechnisch orientierte Materie ist. Die Abgrenzung zwischen Rüstungs- und Verteidigungsforschung einerseits und Sicherheitsforschung andererseits erfolgt im Rahmen des Nationalen Sicherheitsforschungsprogramms in Übereinstimmung mit der diesbezüglichen Abgrenzung der EU im Rahmen des Europäischen Sicherheitsforschungsprogramms.

Das Verteidigungsforschungsprogramm FORTE ist ausschließlich auf den militärischen Kernbereich ausgerichtet und deckt all jene sicherheitspolitisch relevanten Forschungsthemen ab, die beim nationalen Sicherheitsforschungsprogramm KIRAS keine Berücksichtigung finden können. FORTE ist somit komplementär zu KIRAS zu sehen und umzusetzen, da:

- diese Themenmaterie gem. [KIRAS-Sonderrichtlinie](#) entweder dezidiert ausgeschlossen ist (KIRAS hat einen zivilen Programmfokus mit klarer Abgrenzung zur Rüstungs- und Verteidigungsforschung - d.h. keine Rüstungsforschung) oder
- das ÖBH, als Bedarfsträger, ein thematisches Alleinstellungsmerkmal hat, welches nicht im prioritären Interesse anderer sicherheitsrelevanter Bedarfsträger liegt, vom ÖBH aber dennoch zur Erfüllung ihrer Aufgaben unbedingt benötigt wird.

2.2 Zielgruppen und Förderwerber

KIRAS 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 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 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.

2.3 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. Die folgenden Ausschreibungsschwerpunkte sind allerdings nicht ausschließlich zu begreifen. Es können auch weiterhin alle kooperativen Projekte, beziehungsweise F&E-Dienstleistungen eingereicht werden, welche dem Schutz kritischer Infrastruktur gelten.

Folgend sind die Ausschreibungsschwerpunkte aus sicherheitspolitischer Sicht beschrieben.

3.1 Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für kooperative F&E-Projekte

3.1.1 Datengetriebener Mangelradar für die wirtschaftliche Krisenvorsorge

Kontakt: Bundesministerium für Arbeit und Wirtschaft

E-Mail: michael.stern@bmaw.gv.at

Die Covid-19-Pandemie hat die evidente Datenlücke verdeutlicht, mit der die Bundesministerien mit Wirtschaftslenkungs-kompetenz (BMDW, BML, BMK) in einer wirtschaftlichen Krisensituation konfrontiert sind. Es sind einerseits zu wenig Marktinformationen tatsächlich verfügb- oder verarbeitbar, andererseits fehlen übergeordnete und akzeptierte Konzepte über die system- oder versorgungsrelevante Güter, Services oder Rohstoffe und ihre Zusammensetzungen.

Erste konkrete Projekte (z.B. KIRAS ReagtSion, SyRi) haben die Problematik der Datenlücken anhand von spezifischen Beispielen aufgezeigt. Der Aufbau eines Datenpools für einen Mangelradar kann helfen, die fehlende Steuerbarkeit der marktbestimmenden Einflüsse zu minimieren. Dabei ist primäres Ziel, Mangelsituationen mittels neuartiger technologischer Möglichkeiten anhand der Daten schon im Entstehen zu erkennen, rasch mögliche risikominimierenden Maßnahmen zu setzen und – sollte es zu einer wirtschaftlichen Krisenlage kommen – bereits ein mögliches Arsenal an stimulierenden Maßnahmen durch die öffentlichen Bedarfsträger an der Hand zu haben, das zeitnahe effektiv eingesetzt werden kann.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erstellung einer umfassenden und methodisch strukturierten Auflistung der system- oder versorgungsrelevante Güter, Services oder Rohstoffe auf Basis von vorangegangenen Arbeiten
- Die system- oder versorgungsrelevante Güter, Services oder Rohstoffe und ihre Zusammensetzungen sollen einer strukturierten Analyse unterzogen werden, die mögliche Abhängigkeiten, Vorbedingungen, Alternativen und Kaskadeneffekte ex ante bewerten kann
- Es soll eruiert werden, welche erforderlichen beschreibende Wirtschaftsdaten auf Datenkategorie-Basis notwendig sind, um etwaige Mangelsituationen frühzeitig erkennen zu können. Dabei sind die Aspekte bezüglich Qualitätskriterien, Aktualisierungsfrequenz, Datenkonsistenz, Einheiten zu diskutieren. Ziel ist es, einen umfassenden offenen Datenpool zu generieren, der in Krisen- und Mangellagen den Bundesministerien mit Wirtschaftslenkungscompetenz, den Bundesländern und ggf. Gemeinden zur Verfügung steht. Dies stellt die Realisierung eines datengetriebenen Mangelradars dar
- Für das Begriffskonzept „resilientes Unternehmen“ sollen allgemeine Kriterien und eine Guideline für ein Self-Assessment durch das Unternehmen erarbeitet werden, um möglichst effizient feststellen zu können, ob das Unternehmen einerseits systemrelevant ist und ob hinreichende Resilienzmaßnahmen implementiert wurden. Dabei ist auf eine sinnvolle Skalierung Bedacht zu nehmen, um später in die Breite gehen zu können und um den Mangelradar-Datenpool bewirtschaften zu können
- Aus den verfügbaren Wirtschaftsdaten sollen allgemeine Methoden entwickelt werden, über Künstliche Intelligenz mögliche Mangelsituationen für spezifische Güter, Services oder Rohstoffe vorab zu erkennen und zu visualisieren. Dies soll eine datengetriebene Basis für verwaltungstechnische und politische Entscheidungsfindung sein. Etwaige kritische Erfolgsfaktoren (z.B. Fehlerquellen in vorgelagerten Wertschöpfungsketten) sollen systemisch erkannt und über das vorangegangene Self-Assessment aufgedeckt werden, um diese später kontinuierlich beobachten zu können
- Der Mangelradar-Datenpool soll möglichst offen gestaltet sein, um dabei sowohl Datenbewirtschaftungssysteme auf Mikroebene als auch Wirtschaftsinformationssysteme auf der Makroebene integrieren respektive anbinden zu können.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.2 FMCG-Monitoring zur Sicherstellung einer resilienten Daseinsvorsorge der österreichischen Bevölkerung

Kontakt: Bundesministerium für Arbeit und Wirtschaft

E-Mail: michael.stern@bmaw.gv.at

Ausgangssituation

In Österreich sowie in Zentraleuropa sind die Bürgerinnen und Bürger an einen hohen Standard an Versorgungssicherheit und Produktvielfalt gewohnt. Dies betrifft nicht nur die komfortable Wohnsituation, sondern auch die selbstverständliche Annahme, dass alle gewünschten Güter in jeder Größe und Ausführung, zu jeder Zeit vorhanden sind. Behörden empfehlen den Bürgerinnen und Bürgern für den Fall einer Krise, Vorräte von Fast Moving Consumer Goods (FMCG) (z.B. Hygieneprodukte, Haushaltsprodukte, Kosmetikartikel, Nahrungsmittel) für mindestens 2-4 Wochen einzulagern. Viele Menschen befassen sich dennoch nicht (ausreichend) mit diesen Themen, weswegen im Falle einer tatsächlichen Krise erhebliche Teile der Bevölkerung in AT unterversorgt wäre und innerhalb von wenigen Wochen ernsthafte Ernährungs- und Versorgungsprobleme auftreten. Die Weltwirtschaftskrise 2008, die Migrationswelle 2015, die Covid-19-Pandemie seit 2020 sowie die aktuelle Situation in der Ukraine zeigen deutlich, dass es durch Grenzsicherungen, Rohstoffmangel und Produktionsengpässe zu Versorgungsschwierigkeiten kommen kann. Auf diese potenziellen Gefährdungen müssen Behörden sowie Unternehmen frühzeitig reagieren, um handlungsfähig zu bleiben.

Problemstellung:

- Die Versorgungssicherheit von kritischen FMCG-Gütern mit hohem Umschlag muss auch in Krisenzeiten sichergestellt werden
- Behörden und Unternehmen müssen in Krisenzeiten handlungsfähig bleiben, um Probleme schnell aufzudecken sowie effizient darauf zu reagieren, um resilient zu bleiben
- Kritische Risikofaktoren und vulnerable Knoten in der Versorgungskette werden oft nicht identifiziert oder sind den Unternehmen nicht bewusst. Das frühzeitige Erkennen möglicher Störungen in der (trans-) nationalen Versorgung ist aufgrund der Lieferkettenvernetzung und deren Abhängigkeiten höchst komplex
- Das Monitoring der Versorgungslage von kritischen Warengruppen ist oftmals nur rudimentär in Unternehmen vorhanden, wodurch sich anbahnende Engpässe lange unentdeckt bleiben. Es kommt zu Out-of-Stock-Situationen
- Aufgrund der Mangelsituation können irrationales Handeln und Panik in der Bevölkerung entstehen. In Unternehmen erhöht sich die Gefahr eines Bullwhip-Effekts, welcher ein schwieriges Wiedereinpendeln zur Folge hat (z.B. überbeanspruchte Lager- und Maschinenkapazitäten, Verteilungsprobleme durch Mangelsituationen, etc.).

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Schaffung von Transparenz im österreichischen Handel für kritische FMCG-Güter
- Früheres Aufdecken von Störungen durch kontinuierliches Monitoring der Versorgungsnetzwerke
- Identifizierung von kritischen Warenströmen und vulnerablen Knoten sowie Analyse von Risikopotenzialen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.3 Wissenschaftliche Analyse einer breiten Teststellung von E-Fahrzeugen im praxisnahen Polizeieinsatz

Kontakt: Bundesministerium für Inneres

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

Die österreichische Polizei als Einzelorganisation verfügt gegenwärtig über die größte Fahrzeugflotte in Österreich. Ihre staatlichen Aufgaben erfordern eine absolut zuverlässige Mobilitätslösung, da die Sicherheit Österreichs wesentlich von einer jederzeitigen Mobilität abhängt. Die Anforderungen an Fahrzeuge einer Blaulichtorganisation sind allerdings sehr spezifisch, etwa hinsichtlich Fahrzeug- und Antriebsart, Motorleistung, Zusatzverbraucher, Laderaumgröße und Belastung, und insbesondere im Vorhinein nicht planbar. Den derzeit dominierenden konventionellen Benzin- und Dieselmotoren haften aber entscheidende Nachteile bei den Schadstoffemissionen an, was den momentan angepeilten Paris-Klima-Zielen von 2015 und Bestrebungen zur Emissionsreduktion und Energieeffizienz Österreichs und Europas zuwiderläuft.

Das Bundesministerium für Inneres (BMI) verfolgt die Ausarbeitung eines umfassenden E-Mobilitätskonzepts, das von Forschungsaktivitäten begleitet wird. So wird im Zuge der KIRAS-Studie „Die ELEktromOBilität im REAlen PraxiseiNsatz bei der Polizei (Delorean) eine praxisnahe Teststellung von mindestens 20 Fahrzeugen im Blaulicht- und Zivilbereich an unterschiedlichen Dienststellen vorbereitet werden, um diese Fahrzeuge später unter realen polizeilichen Praxisbedingungen einzusetzen zu können. Erst dadurch ist eine Verifikation der Herstellerangaben durch ein bewusstes Aussetzen der Fahrzeuge an tatsächliche Praxisbedingungen und Grenzbereiche möglich. Nur eine fundierte begleitende wissenschaftliche Analyse kann sicherstellen, dass auftretende Problemfelder rasch identifiziert werden und man ihnen effektiv begegnen kann. Damit wird ein unmittelbares und reales Bild der Elektromobilität im Polizeibereich generiert, um diesen disruptiven Technologiesprung einer alternativen Antriebsform bei gleichzeitiger Sicherstellung einer ständigen Mobilität für die Polizei aktiv zu gestalten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie adressieren die Fahrzeuge die definierten Anforderungen einer Polizeiorganisation hinsichtlich Ausstattung, Einsatzzweck, Ladegutsicherung, Batterie, Leistungsparameter, polizeiliche Mehrverbraucher, Gesamt-Energieverbrauch?
- Wie gehen die ausgewählten Dienststellen und Standorte konkret mit den Fahrzeugen um und welche standortspezifischen Erkenntnisse können daraus gezogen werden?
- Wie muss die Infrastruktur technisch, praktisch und verwendungsspezifisch beschaffen sein, um Polizeifahrzeuge optimal in ihrem Mobilitätsbedarf zu bedienen?
- Welche praxisrelevanten Anwendungsprobleme können identifiziert werden und welche Begegnungsstrategien sind effektiv?
- Welche internen und externen Praxisanforderungen und -abläufe im Betrieb und technischen, strukturellen und ablauforganisatorische Grenzbereiche müssen hinreichend evaluiert werden?
- Welche Bedrohungen, Risiken, Ansatzpunkte für etwaige Manipulationsansätze sind gegeben und können durch welche Resilienzstärkende Maßnahmen – insbesondere bei Blackoutszenarien – adressiert werden?

Die begleitenden KIRAS-Forschungsaktivitäten zum umfassenden E-Mobilitätskonzept des BMI sind so konzipiert, dass die entsprechenden Ergebnisse jeweils im nächsten Umsetzungsschritt beziehungsweise in einem aufbauenden Projektvorhaben genutzt und verwertet werden können.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.4 Sicherstellung der Kommunikation in krisenhaften Situationen

Kontakt: Bundesministerium für Inneres

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

Das Wesen der kritischen Kommunikationsinfrastruktur liegt, wie der in der Bezeichnung bereits enthaltene Verweis auf die Kritikalität, in der Verlässlichkeit und Verfügbarkeit auch in vom Normalzustand abweichenden Situationen.

Technologische Entwicklungen im Bereich der Providerlandschaft, die den Ausbau der Infrastrukturen zu immer leistungsfähigeren asynchronen Datennetzwerken anstreben, bergen auch das Risiko, dass Ausfälle dieser Strukturen mittlerweile auch die Kommunikationsdienste betreffen.

Dies führt letztlich dazu, dass die Kommunikationsverbindungen, die für die Koordination, Lagebeurteilung und Maßnahmensetzung erforderlich sind, ebenfalls nicht zur Verfügung stehen.

Wesentliche Ansprechpunkte, wie die Notrufentgegennahmestellen (PSAP – Public Service Answering Point) sind aufgrund ihrer Bedeutung redundant und resilient aufgebaut. Letztlich bestimmt aber die öffentliche Infrastruktur (Festnetz- und Mobiltelefoniesysteme) maßgeblich die Erreichbarkeit dieser Dienste.

Die aktuelle geopolitische Situation bedeutet für das BMI, insbesondere auch abseits der Normalsituation erreichbar und handlungsfähig zu bleiben und Vorsorgekonzepte dieser Entwicklung entgegenzustellen. Dies heißt nicht, sich dem technologischen Fortschritt zu verweigern, sondern vielmehr vorhandene Infrastrukturen im gesamtstaatlichen Interesse auch krisenfit zu gestalten. Neben den resilienten Infrastrukturen ist dazu auch die Sicherstellung einer ausreichenden Kompetenz im staatlichen Bereich notwendig. Vertraglich erbrachte Leistungen stehen in einer krisenhaften Situation, aus dem vis major Grundsatz, sehr rasch nicht mehr zur Verfügung.

Daher bedeutet eine ausreichende Eigenkompetenz und der Betrieb einer möglichst autarken Infrastruktur eine jedenfalls mit den Interessen und Aufgaben des BMI konformgehende Strategie, der auch besonderes Augenmerk zukommen muss.

Hierzu ist es notwendig, ein wissenschaftlich fundiertes Vorgehensmodell zur Identifikation und Bewertung von Handlungspotenzialen aber auch Risiken und Erfolgskriterien unter den speziellen, über den allgemeinen Standards liegenden Anforderungen und Rahmenbedingungen eines Sicherheitsresorts (wie beispielsweise Hochverfügbarkeit, Sicherheit, Redundanz, etc.) zu entwickeln. Die Praxistauglichkeit soll anhand eines Beispiels gezeigt werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erarbeitung eines krisentauglichen technischen Maßnahmensets zur Sicherstellung resilienter Kommunikationsverbindungen, die auch die speziellen Bedürfnisse der Behörden und Organisationen mit Sicherheitsaufgaben implizieren
- Neben der Erhebung und Bewertung der technischen Maßnahmensetzung, ist im Rahmen des Forschungsprojekts auch eine Bewertung über die zur Krisenbewältigung sicherzustellende Kompetenz eine Forschungsfrage
- Es handelt sich dabei um durchwegs um technisch komplexe Systeme, die sich in einer ganzheitlichen Zusammenhaltung befinden und die sich durch Wechselwirkungen untereinander und zu ihrer Umwelt (Geschäftsprozesse) befinden. Ihre Vielschichtigkeit und ihrer Tendenz zur Verwehrung gegen einfache Maßnahmen, erfordern Analysen bis in die einzelnen Objekte, deren technisches und prozessuales Verständnis und letztlich die Risikobewertung und die Erarbeitung eines Risikomanagementplanes.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.5 Entwicklung eines Verfahrens und eines IT-gestützten Demonstrators zur Beobachtung und Analyse von Rücküberweisungen in relevante Herkunftsländer von irregulärer Migration

Kontakt: Bundesministerium für Inneres

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

Ein zentrales Moment für irreguläre Migration ist auch die Vorstellung, Europa zu erreichen, um Einkommen zu generieren – sei es aus Arbeitsleistung oder Sozialleistungen –, um Rücküberweisungen (engl. Remittances) an Verwandte im Herkunftsland zu tätigen. Rücküberweisungen werden in den Herkunftsländern als Beweis für wirtschaftlichen Erfolg wahrgenommen und haben dadurch eine positive Rückwirkung auf die Migrationsbereitschaft der im Herkunftsland verbliebenen Bevölkerung. Die Summen der Rücküberweisungen übersteigen häufig die Summen der Entwicklungszusammenarbeit (EZA) und sind oftmals für Herkunftsländer von großer wirtschaftlicher Bedeutung. Aus Sicht von EU-Staaten wie Österreich, die Zielland von irregulärer Migration sind, erscheint dabei insbesondere problematisch, dass die transferierten Mittel zu einem gewissen Teil auch von irregulären Immigranten stammen, welche diese Mittel teilweise auch aus illegaler Arbeit oder Sozialleistungen generieren und damit einen Pullfaktor für weitere illegale Migration auslösen.

Daher ist die Entwicklung eines Verfahrens und eines IT gestützten Analyseinstruments zur Beobachtung und Analyse zur Beobachtung und Analyse von Rücküberweisungen aus Österreich in relevante Herkunftsländer illegaler Migration von Interesse.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation der relevanten Drittstaaten bzw. Herkunftsstaaten illegaler Migration, in die Rücküberweisungen aus Österreich in signifikantem Ausmaß erfolgen, Analyse der Nationalität der Überweisenden und des Anteils der Überweisungen aus illegaler Arbeit bzw. aus Sozialleistungen
- Analyse der Informationen über die Empfänger wie z.B. Privatpersonen versus Unternehmen, Schlepper sowie der für die Rücküberweisung genutzten Kanäle
- Entwicklung einer Methodik zur Erhebung des Anteils der Rücküberweisungen aus illegalen Quellen oder Tätigkeiten bzw. aus Sozialleistungen (deren Zweck in der Sicherung des Lebensunterhalts im Gastland besteht)
- Aufbau eines Demonstrators zur Analyse der Rücküberweisungen unter Berücksichtigung datenschutzrechtlicher und anderer legaler Anforderungen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.6 Erkennungsdienstliche Behandlung

Kontakt: Bundesministerium für Inneres

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

Eine erkennungsdienstliche Behandlung wird üblicherweise von der Polizei in den einzelnen Polizeidienststellen durchgeführt. Es handelt sich hierbei um eine umfangreiche Aufnahme der Identität einer Person, inklusive Dokumente, DNA-Proben, biometrischer Gesichtsbilddaufnahmen aus verschiedenen Winkeln, Ganzkörperaufnahmen und Bildaufnahmen besondere Merkmale (Narben, Tattoos). Jedes einzelne Datum besteht aus einer Aneinanderreihung von komplexen, zeitlich langwierigen Aufgaben, die der Beamte durchführen muss. Jede Polizeidienststelle muss mit dementsprechenden Kameras ausgerüstet sein, welche derzeit hochauflösende und damit auch kostenintensive Digitalkameras sind, welcher zusätzlich auch bei der Einbindung in die Erfassungsworkflowsoftware durch notwendige, aber technisch laufend wechselnde SDK (Software Development Kit) Verbindungen Probleme bereiten. Üblicherweise werden die Eingaben auf einem Stand-PC getätigt. Die Ausstattung der vielen Polizeidienststellen mit dementsprechenden Kameras, die Instandhaltung und Beschaffung die Installation und Anpassungen der zugehörigen Software, etwa bei nicht mehr vorhandenen Kameramodellen sind kostenintensiv und implizieren einen höheren Wartungsaufwand. Das Projekt soll Technologien aufzeigen die zukünftig am Smartphone wie sie in der österreichischen Polizei in einem sicheren Netzwerk bereits verwendet werden. Dies soll nicht nur zur Zeit- und Kostenersparnis, sondern vor allem auch automatisierte Qualitätssicherung und Qualitätsprüfung vor allem der Gesichtsbilder, welche nachfolgend für Gesichtsfeldererkennungssysteme zum Vergleich herangezogen werden, während des Aufnahmeprozesses ermöglichen.

Es wäre wünschenswert die Prozesse möglichst mobil und effizient, auch möglichst mittels intelligenter Unterstützung am Smartphone der Polizei durchzuführen. Die österreichische Polizei ist bereits durchgängig mit Smartphones ausgerüstet über welche auch dienstliche Datenbankabfragen über ein sicheres Netzwerk durchgeführt werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Implementierungsmöglichkeiten intelligenter Aufnahmesysteme am Smartphone
- Automatisierte maßstabgetreue Aufnahmetechnologien für besondere Merkmale
- Möglichst gute Erkennung und automatisierte Aufnahme von Profilbildern mit automatisierter Qualitätsprüfung
- Prototypische Entwicklung eines Tools zur Bewertung von ICAO konformen Gesichtsbilddaufnahmen insbesondere bei Halbprofilgesichtsbildern
- Einfachstes Userinterface mit kontextbezogener Benutzerführung
- Schnelle Übergabe und Übertragungsmechanismen von diversen Aufgaben zwischen Smartphone und Stand-PC
- Mögliche Onlineanbindung in die polizeilichen erkennungsdienstlichen Workflowsysteme.

Ein dementsprechendes kooperatives F&E Projekt soll die Ergebnisse des KIRAS-Projekts Biometrie Capture Tool für die Polizei im mobilen Einsatz (Projektkurztitel: BioCapture) berücksichtigen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.7 Mobile digitale Aufnahmetechnologie für Schuhspurenerfassung

Kontakt: Bundesministerium für Inneres

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

An Tatorten sind als wichtige Beweismittel oftmals auch vorhandene Schuhspurenabdrücke zu erfassen, welche nachfolgend unter Anwendung von Mustererkennungssoftware auch gegen andere bereits erfasste Schuhspuren anderer Tatort verglichen werden müssen, um hier mögliche Tatortzusammenhänge erkennen zu können. Die derzeitigen Aufnahmetechnologien hängen einerseits von der Art der vorhandenen Schuhspur ab (Eindruck, Abdruck, bereits sichtbar oder noch latent) und andererseits von der vorhandenen Technik und Erfahrung von Tatortexperten zur bildmäßigen Erfassung solcher Spuren, um sie nachher auch in Suchsystemen oder Einzelvergleichsuntersuchungen auf Übereinstimmung vergleichen zu können.

Alle Aufnahmetechnologien erfordern umfassende Sachkenntnis und Erfahrung und bei der Bilderfassung mit Kameras auch spezifische Kenntnisse im Umgang mit hochwertigen Fotokameras, um ausreichende Datenqualität zu erlangen.

Es wäre wünschenswert hier unter Verfolgung des angesprochenen Lösungsansatzes wie er schon für die Bilderfassung von Dokumenten oder besonderen Kennzeichen beschrieben ist, auch für derartige Tatortfotografie von Schuhabdruckspuren oder vielleicht weiterführend später auch für andere Formspuren wie etwa Werkzeugspuren udgl. weiter zu verfolgen und Bildaufnahmen in qualitativ geeigneter Weise durch Mobiltelefone welche als Polizeiwerkzeug für klassische Datenerfassungen und Datenbankabgleiche in Österreich bereits genutzt werden, auch für die Aufnahme solcher Tatortspuren nutzen zu können. Die Prozesse sollten möglichst mobil und effizient und auch möglichst mittels intelligenter Unterstützung am Smartphone von Polizeibeamten, welchen keine hochspezifische Tatortausbildung und Sonderausrüstung zur Verfügung steht, durchgeführt werden können. Damit könnten solche oft wichtigen Tatortspuren für weitere Spurenableiche auch bei niederschwelliger Kriminalität sachgerecht gesichert und als Beweismittel genutzt werden. Die österreichische Polizei ist bereits durchgängig mit Smartphones ausgerüstet über welche auch dienstliche Datenbankabfragen über ein sicheres Netzwerk durchgeführt werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Möglichst gute Erkennung und automatisierte Aufnahme von Schuhabdruckspuren mit automatisierter Qualitätsprüfung
- Prototypische Entwicklung eines Tools zur Bewertung von ausreichender Bildqualität bei der Aufnahme
- Automatisierte maßstabgetreue Aufnahmetechnologien für derartige Schuhspuren
- Einfachstes Userinterface mit kontextbezogener Benutzerführung
- Implementierungsmöglichkeiten intelligenter Aufnahmesysteme am Smartphone
- Schnelle Übergabe und Übertragungsmechanismen von diversen Aufgaben zwischen Smartphone und Stand-PC
- Mögliche Datenübernahmeschnittstellen in Polizeiliche Spurendatenbanken bzw. Mustererkennungssysteme für Schuhspurensysteme.

Ein dementsprechendes kooperatives F&E Projekt soll die Ergebnisse des KIRAS-Projekts „IT unterstützte Suche und Vergleich von Schuhspuren in einer Tatspurendatenbank und einem Schuhkatalog – impress (Projektkurztitel: Impression Evidence and Shoe Model Search – impress) berücksichtigen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.8 UAV-UGV-Teaming zur kooperativen Raumüberwachung von sicherheitsrelevanten Gebieten

Kontakt: Bundesministerium für Inneres

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

Grenzsicherung, Grenzüberwachung und der Kampf gegen Schlepperei haben sich in den letzten Jahren als zentrale Aufgabenstellungen definiert. Wie auch in anderen Bereichen, ist es insbesondere bei der Bewältigung dieser Aufgaben von wesentlicher Bedeutung, dass - in sinnvoller Ergänzung zum Einsatz wichtiger technischer Hilfsmittel - eine Auseinandersetzung mit möglichen innovativen technologischen Lösungen vorausschauend und damit frühzeitig erfolgt.

Um eine Raumüberwachung von sicherheitsrelevanten Gebieten sowohl verfassungskonform und unter Beachtung des Datenschutzes, als auch mit verhältnismäßigen Einsatzressourcen und reduziertem Einsatzrisiko, wahrnehmen zu können, bedarf es einer aufgabenorientierten und skalierbaren Systemautonomie, die durch ein optimiertes Zusammenspiel heterogener boden- und luftgestützter Systeme auf Basis von „Machine Learning“, Methoden der Künstlichen Intelligenz (Soft-KI) und der Selbstorganisation (Schwarmintelligenz) erreicht werden kann.

So könnten kooperative Lösungsansätze unter Einbindung von heterogenen (teil-)autonomen UAV (Unmanned Aerial Vehicle) und UGV (Unmanned Ground Vehicle) Systemen ermöglichen auf Basis unterschiedlicher, sich ergänzender

Systemeigenschaften eine zielgerichtete Unterstützungsleistung der Einsatzkräfte bei Wahrnehmung ihrer Aufgabenstellungen ermöglichen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- KI-gestützter, ortsveränderbarer multisensoraler (optisch, thermal, Radar) Kommunikationsknoten als zentrales Modul für die kooperativen und kollaborativen Managementansätze („Teaming“ von heterogenen Schwärmen)
- Entwicklung von robusten Kommunikationslösungen, insbesondere auf Basis von 5G-Technologien, für innovative Kooperationsansätze zwischen den einzelnen Modulen und einer Einsatzzentrale
- Generierung eines Moduls zur simulationsunterstützten Vor-Ort-Systeminstallation und -kalibrierung
- Entwicklung von semantischen echtzeitfähigen Algorithmen und Methoden für die Detektion sowie automatisierte, KI-basierte Datenanalyse
- Zusammenführung der zeit- und geo-orientierten Informationen der einzelnen Module und Managementlösung mit dezentralem Datenzugriff
- Möglichkeiten zur Einbindung von und in andere Systeme mit ähnlichem Aufgabengebiet via 5G (beispielsweise ortsfeste oder mobile Sensoren, Drohnenabwehrsysteme oder Ähnliches)
- Sozialwissenschaftliche Analyse zur Akzeptanz (teil-)autonomer technologischer Lösungen seitens der Einsatzkräfte und der Bevölkerung.

Eine Berücksichtigung und Verwertung von Teil-/Ergebnissen aus laufenden wie abgeschlossenen Forschungsaktivitäten ist für ein Projektvorhaben, das zum gegenständlichen Ausschreibungsschwerpunkt eingereicht werden soll, besonders wichtig. Von besonderer Relevanz sind dabei die kooperativen KIRAS F&E-Projekte UASwarm und KI-Secure, WatchDog, NRT-COP, SCALA, SILBOS und AMBOS. Darüber hinaus sind relevante F&E-Projekte aus dem Verteidigungsforschungsprogramm FORTE zu berücksichtigen.

Ebenso sollen bereits in der Projektkonzeption deutliche Synergieeffekte durch Kooperation mit jenem Projektvorhaben, das zum Ausschreibungsschwerpunkt „Nutzung von Drohenschwärmen zum Schutz kritischer Infrastruktur – Drohnenabwehr“ eingereicht wird, vorgesehen werden.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.9 Erhöhung der Sicherheit und Effizienz im Strafvollzug durch digitalisierte und automatisierte Prozesse

Kontakt: Bundesministerium für Justiz

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

Obwohl die Bediensteten im österreichischen Strafvollzug auf eine breite Unterstützung durch IT-Systeme zurückgreifen können, sind speziell im Bereich der Gewährleistung von Sicherheit und Ordnung meist noch analoge Prozesse vorherrschend. Während der Großteil der Informationen zu den Insassen bereits digitalisiert in der IVV (integrierten Vollzugsverwaltung) verfügbar ist, wird den umfangreichen Dokumentationspflichten meist durch handschriftliche Eintragungen in Listen und Büchern oder elektronisch in der Form von Excel-Listen entsprochen. Diese Daten erlauben durch entsprechende Analyse einerseits Einblicke um punktuell Maßnahmen zur Erhöhung der Sicherheit (wo und wann gibt es vermehrt Sicherheitsvorfälle? welche Hafträume werden eventuell seltener kontrolliert? ...) zu setzen. Andererseits können sie, sofern sie in Echtzeit vorliegen, den Mitarbeiter:innen ein immer aktuelles Lagebild vermitteln, und speziell im Fall von Krisen und Notfällen auch entsprechend bei deren Bewältigung unterstützen (automatisierte Aufnahme der Daten in ein Einsatztagebuch, Dashboards, Aufenthaltslisten, ...).

Ohne aufwändiger strukturierter Nachdigitalisierung verschließen sich diese wertvollen Informationen derzeit allerdings einer weiteren Verarbeitung zum Beispiel in Form einer Steuerung über KPIs (Key Performance Indicators) oder einer Analyse durch KI-Technologien. Hauptgründe für diese Situation sind einerseits sicher die noch mangelnde Digitalisierung dieses Bereichs in Hinblick auf mögliche Automatisierung durch künstliche Intelligenz und elektronische Prozesssteuerungen, andererseits aber sicher auch, dass sich die klassische Bedienung von stationären EDV-Geräten nur schwer in den Arbeitsalltag eines Justizwachebeamten:innen im Umgang mit Insassen einfügen lässt. Durch die Unterstützung des KIRAS-Programms zur Sicherheitsforschung wurden im Zuge eines F&E Dienstleistungsprojektes Prozesse erhoben, welche Vollzugsworkflows besonders von einer solchen Digitalisierung profitieren könnten, und welche Technologien dafür in Frage kommen würden. Dabei wurden einige interessante neue Fragestellungen, besonders zu Themen wie Robustheit, Sicherheit, Technologieakzeptanz und Unterstützung durch künstliche Intelligenz aufgeworfen. Diese sollen nun im Zuge eines kooperativen Projektes entsprechend weiterführend behandelt und durch die Durchführung von mehreren Proof-of-Concepts im Feld erforscht werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Analyse, welche der aktuell manuell aufgezeichneten Informationen richtig ausgewertet zukünftig einen Beitrag zur Erhöhung der Sicherheit liefern können. Gibt es Informationen die in diesem Kontext interessant wären und derzeit nicht erfasst werden? Welche Aufzeichnungen müssen im Falle einer Krise oder eines Notfalls in Echtzeit vorliegen?
- Forschung im Bereich Machine Learning um herauszufinden wie diese speziellen Daten und Informationen in Relation gesetzt werden müssen um neue Erkenntnisse zu gewinnen
- Forschung im Bereich der Mensch-Maschinen-Kommunikation wie die umfangreichen Dokumentationspflichten im Bereich der Sicherheit in einer Justizanstalt digitalisiert und möglichst natürlich, nebenläufig, sowie sicher und robust in den Arbeitsalltag von Justizwachebeamten:innen eingebettet werden können

- Erforschung und Bewertung der Möglichkeiten, um Bedienstete und Insass:innen im Zuge digitaler Prozesse sicher und verlässlich im Alltag zu authentifizieren und Identitätsdiebstahl entgegenzuwirken
- Forschung wie Routinetätigkeiten und -kontrollen aber auch die Unterstützung besonderer Events (wie bspw. Alarm- oder Krisenfälle) bestmöglich auch durch künstliche Intelligenz digital unterstützt oder im besten Fall sogar komplett automatisiert ablaufen können
- Forschung inwieweit ein digitales Expert:innensystem in der Praxis einen entsprechenden Mehrwert bieten könnte? Kann den Vollzugswachebeamt:innen ein digitaler Assistent zur Verfügung gestellt werden, welcher aus aktuell vorliegenden Daten gespeist Handlungsempfehlungen gibt, welche sowohl in Alarm- und Krisensituationen, als auch bei Routinetätigkeiten wertvolle Entscheidungshilfen bietet und von den Anwender:innen akzeptiert wird?
- Forschung und Analyse, inwieweit die Möglichkeit zur Echtzeit-Datenkommunikation auch Auswirkung auf die Steuerung von Abläufen und Prozessen (z.B. Zuweisung von Aufgaben, Taskboards, AdHoc-Live-Videokonferenzen mehrerer im Einsatz befindlicher Justizwachebeamt:innen mit den koordinierenden Stellen)
- Umfangreiche Betrachtung der ethischen und rechtlichen Herausforderung bei der KI-unterstützten Digitalisierung von Prozessen im Strafvollzug
- Forschung und Analyse der Zusammenhänge und Besonderheiten von Datenerhebung durch Digitalisierung und Technologieakzeptanz bei der Anwendung von Technologien im Strafvollzug.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.10 Kombination einer Notstromversorgung basierend auf erneuerbarer Energieerzeugung und innovativen Speichersystemen mit Energiegemeinschaften

Kontakt: Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

E-Mail: Georg Beretits; Georg.Beretits@bmk.gv.at

Kontakt: Österreichische Koordinationsstelle für Energiegemeinschaften im Klima- und Energiefonds

E-Mail: koordinationsstelle@energiegemeinschaften.gv.at

Speziell Städte und Gemeinden sind bei Stromausfällen gefordert, eine auf Gebäude beschränkte Notstromversorgung für Einsatzkräfte und für Erstanlaufstellen für die Bevölkerung vorzusehen. Dafür werden bislang überwiegend Diesellaggregate eingesetzt. Es gibt aber auch klimafreundliche, innovative Lösungen, die von fossilen Treib- und Brennstoffen unabhängig sind und mit erneuerbaren Technologien betrieben werden. Der Aufbau einer derartigen Notstromversorgung sollte vorrangig in Kombination mit der Gründung bzw. mit dem Betrieb einer Energiegemeinschaft

erfolgen. Innerhalb der Energiegemeinschaft wird auch der Überschussstrom verteilt, solange das Stromnetz verfügbar und kein Krisenfall eingetreten ist.

In Krisenzeiten kann der Notstrom für die Versorgung gemeinsamer Infrastruktur, für die wichtigsten Strombedürfnisse u.a. für Einsatzkräfte in Krisensituationen verwendet werden. Der Betrieb einer Notstromversorgung, basierend auf erneuerbarer Energieerzeugung mit innovativen Speichersystemen, macht Teilnehmende einer Energiegemeinschaft resilienter.

Außerhalb von Krisenzeiten wird der erzeugte Strom in der Energiegemeinschaft genutzt und ebenso der Speicher, der so einzusetzen ist, dass er der Gemeinschaft einen Mehrwert bringt ohne jedoch die notwendige Krisenvorsorge zu gefährden. **Essentiell ist dabei ein Speichermanagement, das den Anforderungen im Normal- wie auch Notfallbetrieb gerecht wird.**

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erarbeitung von Lösungen für ein entsprechendes Speichermanagementsystem in Energiegemeinschaften
- Analyse, inwieweit die Gründung bzw. der Betrieb einer Energiegemeinschaft auch Anreize bieten kann, dies mit einer Notstromversorgung auf Basis erneuerbarer Energieträger für die Gemeinschaft zu verbinden.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.11 Krisenbevorratung von Lebensmitteln und landwirtschaftlichen Produktionsmitteln

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft

E-Mail: elmar.ritzinger@bml.gv.at

Ein nachhaltiges Lebensmittelsystem muss eine ausreichende und vielfältige Versorgung der Menschen mit sicheren, gesunden, nahrhaften, nachhaltig erzeugten und erschwinglichen Lebensmitteln zu jeder Zeit gewährleisten, nicht zuletzt in Krisenzeiten. Die die Lebensmittelversorgungskette in der EU und in Österreich hat sich in der COVID-19-Krise als widerstandsfähig erwiesen. Dank Produzentinnen und Produzenten der Landwirtschaft, Fischerei, Aquakultur und anderen Akteurinnen und Akteuren der Lebensmittelversorgungskette waren während der gesamten Krise Lebensmittel beinahe ohne Einschränkungen verfügbar. Es konnten aber doch einige Probleme, die das normale Funktionieren der Lebensmittelversorgungskette beeinträchtigten und eine Bedrohung für die Ernährungssicherheit hätten darstellen können festgestellt werden. Die Folgen des Angriffskriegs Russlands auf die Ukraine haben die Fragilität weltweiter Lieferketten, die Vernetzung verschiedener Systeme und Just-in-time-Lösungen weiterhin offenbart.

Einige Staaten sowohl in der EU wie auch andere Staaten halten öffentliche Vorräte an bestimmten Lebens- (oder Futter-)mitteln oder haben Systeme, mit denen die Bevorratung von Lebensmitteln zum Schutz vor plötzlichen starken Versorgungsschwankungen sichergestellt werden soll. Bekannt sind hier u.a. Beispiele aus Deutschland, der Schweiz oder den USA.

Einige Staaten halten keine strategischen Nahrungsmittelreserven als solche vor, sondern konzentrieren sich auf andere Instrumente, wie die Lenkung der Nahrungsmittelverteilung oder rechtliche Grundlagen für die Beschlagnahme von Produkten bei Herstellern und Lieferanten im Notfall (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Contingency plan for ensuring food supply and food security in times of crisis, Brussels, 12.11.202, European Commission).

Einer Umfrage von April 2021 zufolge gehen 68 % der Bevölkerung in Österreich von einer Aufrechterhaltung einer staatlichen Basisversorgung über 4 Wochen aus (Ausserladscheider, V. und Partheymüller, J. Austrian Corona Panel Project, [Krisenvorsorge: Die österreichische Bevölkerung setzt auf den Staat, weniger auf Eigenvorsorge, Wien 2021](#)).

Österreich kann sich mit dem Großteil der allgemein als Grundnahrungsmittel verstandenen Lebensmittel grundsätzlich gut selbst versorgen (hohe Selbstversorgungsgrade bei Getreide, Fleisch, Milch usw.). Eine mögliche Umlenkung der nicht direkt für die Ernährung verwendeten pflanzlichen Rohstoffe stellt einen zusätzlichen Puffer dar.

Durch die Einbindung in den Binnenmarkt ergibt sich für Mitgliedstaaten der EU eine zusätzliche Absicherung der Versorgung bei regionalen/einzelstaatlichen Ausfällen oder Mangellagen. Voraussetzung dafür sind ein funktionierender Binnenmarkt, Transportmöglichkeiten, offenen Grenzen und internationaler Handel.

Die allfällige Notwendigkeit der öffentlichen Vorratshaltung von Lebensmitteln und Hilfsstoffen ist im Lichte verschiedener Krisenszenarien unterschiedlich zu betrachten. So sind einmalige Ernteaufschläge oder Verluste von Ernten hinsichtlich der notwendigen Vorräte anders zu betrachten als plötzlich eintretende Versorgungsstörungen mit in der Folge längerfristigen Ausfällen.

Aufgrund der Szenarien sind auch zu lagernde Produkte, angestrebter zeitlicher Versorgungshorizont, Resilienz der jeweiligen Lieferketten und Sourcing-Strategien sowie daraus folgend zu bevorratende Mengen unterschiedlich zu bewerten.

Überlegungen zur allfälligen Anlegung von Krisenreserven müssen auch den Verarbeitungsgrad und eine allfällige szenarienbedingte Versorgungsstruktur für die Bevölkerung beinhalten.

Der An- und Verkauf zur Marktbeeinflussung oder sonstiger Steuerung von Agrarmärkten ist Gegenstand der Gemeinsamen Agrarpolitik der EU und daher NICHT Untersuchungsgegenstand.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Ermittlung eines Kataloges von gegebenenfalls einer Bevorratung zu unterziehenden Produkten (kritische Güter) zur Grundversorgung der Bevölkerung und von versorgungsrelevanten Unternehmen (landwirtschaftliche Betriebe, ggfs. auch Verarbeitungsunternehmen) im Bereich der Lebensmittelversorgung. Dabei sind Substitutionsmöglichkeiten und spezielle gesundheitliche/medizinische und ernährungsbezogene Erfordernisse bestimmter Bevölkerungsgruppen einzubeziehen
- Berücksichtigung verschiedener Krisenszenarien (z.B. mit/ohne Stromversorgung, Treibstoffversorgung, Kühlmöglichkeit, best case vs. worst case), jahreszeitliche Aspekte und Zeithorizonte. Entsprechend Definition des zeitlichen Ziellevels je Szenario und Produkten (Service Level)
- Skizzierung der Lieferketten pro Produkt(gruppe) unter Berücksichtigung einer erweiterten Farm-to-Fork-Betrachtung: Herkunftsregionen, Risikobetrachtung in den Dimensionen Länder, Umweltfaktoren, Ausfallsicherheit, Sourcingstrategien einschließlich Substitutionsmöglichkeiten, Energieprofile über die Lieferkette
- Aufzeigen und Bewertung möglicher Geschäftsmodelle für die Lagerhaltung nach den Kriterien: Dringlichkeit, Lagerfähigkeit, Haltbarkeit, Risiko, Kosten und Verwaltungsaufwand, rechtlicher Rahmen, Vergaberecht, Vertragsdauer, Haftung
- Organisatorische Vorkehrungen für die Lagerhaltung (Verwaltung, Umschlag, Schnittstellen der vor- und nachgelagerten Logistik, Zutrittsregelung, ...)
- Ansätze für die Verortung von Lagern auch in Hinblick auf die rasche Verteilung an die Bevölkerung
- Abschätzung des Verwaltungsaufwandes und der budgetären Auswirkungen für die identifizierten Geschäftsmodelle
- Bereits erstellte Studien, Vorarbeiten und Erfahrungen aus dem In- und Ausland (u.a. zu Bezugsberechtigungen und Geschäftsmodellen) sind zu berücksichtigen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.12 Erhebung und Berechnung von geologischen sowie geographischen Daten mittels der Kombination von Feldmethoden und der Geoanalyse von Satellitenbildern

Kontakt: Bundesministerium für Landesverteidigung

E-Mail: sicherheitsforschung@bmlv.gv.at

Die Geländebeurteilung ist zentraler Bestandteil des Führungsprozesses auf militärischen und zivilen Entscheidungsebenen. Um eine rasche Verfügbarkeit von präzisen Geländedaten sicherzustellen, fungiert u.a. das Militärische Geowesen als integraler Bereitsteller von Geodaten und Expertise im geowissenschaftlichen Bereich. Erhöhte einsatzspezifische Anforderungen an eine "klassische

Geländeanalyse“ durch komplexe Szenarien oder sich rasch verändernde Umweltbedingungen (z.B. durch den Klimawandel) bedeuten daher eine Notwendigkeit für ständige Weiterentwicklung der Methoden u.a. im Militärischen Geowesen.

Bisher wurden Geländeanalysen überwiegend auf der Basis von Geländehöhenmodellen und, soweit vorhanden, geologischer und bodenkundlicher Daten berechnet, obwohl viele andere Geländefaktoren ebenfalls wesentlich sind. Problematisch ist in diesem Zusammenhang vor allem die Verfügbarkeit von digitalen aber auch analogen Geodaten. Während im Inland auf Dienste wie die Geologische Bundesanstalt oder die Zentralanstalt für Meteorologie und Geodynamik zurückgegriffen werden kann, ist die Datenlage im Einsatzgebiet außerhalb Österreichs unbefriedigend.

Um bestehende Dienstleistungen und Produkte u.a. des Militärischen Geowesens im Sinne der Bedarfsträgerorientierung zu verbessern, müssen neue Methoden der Geodatenbeschaffung und -analyse entwickelt, sowie bestehende Methoden optimiert werden.

Hier bieten sich vor allem geowissenschaftliche Feldmethoden an, mit denen die Daten für ein besseres Verständnis der Geländeeigenschaften eines Einsatzraumes erhoben werden können. Besonders die Ableitung von Geodaten aus multispektralen Satellitenbildern bietet enormes Potential für einsatzspezifische Geoanalysen ohne Personaleinsatz vor Ort.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können geomorphologische Strukturen (als wichtiger Faktor nach Höhenmodell, Geologie und Bodenkunde) insbesondere in der Fernerkundung erhoben werden und welche Methoden eignen sich am besten für eine zeitnahe, akkurate und bedarfsträgerorientierte Analyse und Darstellung der Daten?
- Welche Bedeutung (taktisch, operativ, strategisch) haben in Geländeanalysen berechnete und dargestellte Strukturen?
- Welcher Zusammenhang besteht zwischen physischen und humangeographischen Geofaktoren?

Wichtig ist hierbei, bestehende Ergebnisse auslaufender oder bereits abgeschlossener KIRAS- Projekte zu berücksichtigen und vorhandene Synergien und Ergebnisse zu nutzen. Eine Zusammenarbeit mit den österreichischen Geodiensten (GBA, ZAMG, Landesgeologie usw.) ist für den Projekterfolg notwendig.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.13 Kontaminationsmonitor - Feststellung von Kontaminationsrückständen mit optischen Detektionsmethoden

Kontakt: Bundesministerium für Landesverteidigung

E-Mail: sicherheitsforschung@bmlv.gv.at

Nach einer Freisetzung von ABC-Gefahrstoffen ist davon auszugehen, dass Personen und Ausrüstung potentiell kontaminiert sind und dementsprechend dekontaminiert werden müssen.

Besonders bei Zivilpersonen, die überraschend und unvorbereitet betroffen sind, wird eine schnelle Feststellung benötigt. Bei Massenanlassfällen könnte mit einer solchen Detektionsmethode die Triage, wer Dekontamination benötigt und wer nicht, maßgeblich unterstützt werden. Damit würde die meistens limitierten Dekontaminationskapazitäten entlastet und zielgerichtete Hilfe erfolgen. Gleichzeitig würde ein solches Verfahren ermöglichen, die Effektivität der Dekontamination nachweisen zu können.

Bei Ausrüstungsgegenständen ist die Feststellung von Oberflächenkontamination sinnvoll, um diese im positiven Fall (nicht kontaminiert) direkt wieder zum Einsatz bringen zu können oder nur die betroffenen Stellen dekontaminieren zu müssen.

Im radiologischen Bereich kann man Personen bzw. Gegenstände mit entsprechenden Geräten „freimessen“ und dann können diese ohne Dekontamination passieren bzw. wiederverwendet werden.

Im biologischen/chemischen Bereich könnte so ein „freimessen“ über optische Methoden und Algorithmus-unterstützte Auswertung im multispektralen Bereich erfolgen. Bei Tatorten beispielsweise werden verschiedene Lichtwellenlängen und verschiedene additive Substanzen benutzt, um optisch Spuren wie Blut, Fingerabdrücke, Schmauch, Körperflüssigkeiten oder Treibstoff zu detektieren.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Können biologische und/oder chemische Gefahrstoffe optisch/spektral detektiert werden?
- Sind diese Methoden empfindlich genug, um eine Oberfläche als nicht kontaminiert einzustufen und wie kann die Empfindlichkeit der Methoden gesteigert werden?
- Können diese Methoden unter Einsatzbedingungen bei Personen angewendet werden (in Echtzeit, hochmobil, hautverträglich, unter Reduktion/Ausschluss störender Effekte wie Streulicht etc.)?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.14 Assistenzsystem zur Einsatzführung im urbanen Umfeld

Kontakt: Bundesministerium für Landesverteidigung

E-Mail: sicherheitsforschung@bmlv.gv.at

Urbane Umgebungen sind verstärkt Austragungsorte von Terroranschlägen, Konflikten mit rivalisierenden Bevölkerungsgruppen und/oder irregulären Kräften bis hin zu militärischen Auseinandersetzungen. Sogenannte "komplexe Ereignisse" hervorgerufen durch hybrid agierende Gegner, welche von der Chaos-Phase in einen Zustand zunächst nicht erkennbarer Zusammenhänge führen, erfordern ein gutes Lagebild. Unmittelbar bereitstehende technische Assistenzsysteme basierend auf Drohnen (UAV) und Bodenrobotern (UGV) sind insbesondere als hybride Schwärme zur Aufklärung auf allen Ebenen und zur Informationsgewinnung in unübersichtlichem urbanem Terrain von unschätzbarem Wert; sie ermöglichen den Aufbau eines kontinuierlich aktualisierten und umfassenden 3D-Lagebildes in der taktischen Leitzentrale der Einsatzorganisation(en). Andererseits können diese Assistenzsysteme die Einsatzkräfte vor Ort zeitnah mit sicherheitsrelevanten Informationen (Betroffeneninformation, Täterinformationen, sonstige nicht wahrnehmbaren Gefahrenpotentiale wie Gasalarne etc.) versorgen und Entscheidungen auf Einsatzebene erleichtern. Ein solches Assistenzsystem muss teilautonom und einsatzorganisationsübergreifend operieren können. D.h., die Systemkomponenten (UAVs, UGVs) müssen Tasks zwar autonom ausführen können, die Entscheidungen, welche Tasks ausgeführt werden, sind aber Aufgabe eines Managementsystems, in welchem der Mensch als Entscheider eingebunden ist (Human-in-the-loop). Dabei werden die Einsatzkräfte mit entsprechender technischer Ausrüstung (Sensorknoten, Funktechnologie, Smart Appliances) selbst integraler Bestandteil des Systems, sei es als Systemanwender und Informationsverwerter/Entscheider oder auch als Sensor (z.B. Belastungszustandsinformationen) und Transmitter-Knoten zum Transport von Informationen in alle Richtungen. Besondere Herausforderungen liegen zudem in der erschwerten Navigation, da in „confined urban spaces“ oft kein GNSS-Signal vorhanden ist, aber auch mit massiven Störungen der drahtlosen Kommunikation zu rechnen ist. Das Ensemble aus heterogenen Sensoren (UAV, UGV, Mensch) mit unterschiedlichen Möglichkeiten und Fähigkeiten erfordert im Rahmen eines innovativen Managementsystems unter Verwendung von Methoden aus KI, Selbstorganisation und Schwarmintelligenz neue Methoden der zentralen sowie dezentralen Koordination.

Daraus ergeben sich konkret folgende Forschungsthemen und -fragen:

- Flexible, resiliente und robuste Kommunikationsarchitekturen, welche es erlauben, Daten (auch breitbandig) von vorne nach hinten und von hinten nach vorne (Einsatzteams Leitzentrale) zu kommunizieren
- Die Kommunikationsarchitekturen werden bereits neue Ansätze im Rahmen der Definition von kommenden Standards (6G) berücksichtigen. Darunter sind u.a. neue flexible Architekturen basierend auf innovativen Kombinationen von Funktechnologien (5G, LTE; LoRa, UWB, BTLE, WiFi, etc.) auf unterschiedlichen mobilen Trägerplattformen zu sehen, die M2M Kommunikation und automatisiertes Ein- und Ausbuchen in Netze

- ermöglichen. Dynamisches Relaying, bei welchem UAVs und UGVs beste Positionen für die Informationsweiterleitung autonom suchen und Dynamic Network Adaptation und Open Device Management
- Verschlüsselungs- und Verschleierungs-Technologien (z.B. durch Informationsüberflutung oder multi-channel routing) für die Drahtloskommunikation
 - Kleine UAV-Plattformen, welche einerseits durch enge Bereiche mit Verbrauch (z.B. untertage) fliegen können, andererseits auch Payload-Sensorik und Hardware für die Verschwarmung tragen können
 - Optisch, thermal und LiDAR multi-sensor Systeme, um das gesamte TripleS abdecken zu können
 - KI-basierte echtzeitfähige Fusion, Auswertung und Informationsgewinnung aus den Daten des Schwarms zur Situationsdarstellung
 - Neuartige Koordinationsverfahren basierend auf einer Mischung von verteilten Ansätzen (AI, Schwarmintelligenz) als auch zentralistischen Methoden (Missionsdefinition)
 - Kooperatives Aufgabenmanagement zur Herstellung einer Gesamtkoordination der unterschiedlichen Sensoren anhand ihrer Fähigkeiten und zum Management der Taskautonomie.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.15 Alternative Technologien zur Detektion, Klassifizierung und Identifikation von Micro- und Mini-Drohnen

Kontakt: Bundesministerium für Landesverteidigung

E-Mail: sicherheitsforschung@bmlv.gv.at

Die rasante Entwicklung unbemannter Luftfahrtsysteme als potenzielles Angriffsmittel stellt eine asymmetrische Bedrohungslage dar. Das Bedrohungsbild reicht von kurz- und mittelfristigen terroristischen Bedrohungen durch Einzelakteure mit terroristischen Drohnen oder Drohnenschwärmen im ruralen und urbanen Raum bis hin zu längerfristigen systemischen terroristischen Bedrohungen und massiven Angriffen auf die kritische Infrastruktur und Souveränität Österreichs. Die fortschreitenden Entwicklungen im Bereich der Drohnensysteme (z.B. Schwarmtechnologie, Robustheit, autonomer Betrieb, Größe etc.) erfordern eine ständige Anpassung bzw. Neuentwicklung geeigneter Sensorik.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung alternativer Technologien zur Erfassung von Micro- und Mini-Drohnen - zusätzlich zu Radar, Elektrooptik, Infrarot und Akustik
- Erforschung von Grundlagen für bzw. Entwicklung von weiterer Sensorik zur Detektion, Klassifizierung und Identifizierung von Micro- und Mini-Drohnen
- Klassifizierungs- und Identifizierungsmethoden zur sicheren Klassifizierung und Identifikation von Micro- und Mini-Drohnen.

Hierbei sind relevante (Teil-)Ergebnisse aus laufenden und abgeschlossenen Forschungsaktivitäten v. a. in KIRAS zu berücksichtigen und zu verwerten. Projektziel ist die Funktionsdemonstration.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.16 Mobilitätsdaten als Instrument des Krisen- und Pandemiemanagements

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VII/A/12 – Krisenstab Gesundheitswesen

E-Mail: Krisenstab-Gesundheitswesen@gesundheitsministerium.gv.at

Im Zuge der COVID-19 Pandemiebekämpfung wurden zahlreiche nicht-pharmazeutische Interventionen gesetzt. Diese umfassen auch Maßnahmen, die das Bewegungs- und Kontaktverhalten der Bevölkerung und damit das Infektionsgeschehen beeinflussen. Dabei spielt nicht nur die Umsetzung, sondern auch deren Ankündigung selbst eine Rolle (Signalwirkung). Es besteht ein großes Erklärungspotential für das Infektionsgeschehen in maßnahmenunabhängigen Faktoren (insb. Saisonalität/Wetter und Ferienzeit) hinsichtlich ihrer Wirkung über verändertes Mobilitätsverhalten und Kontaktgeschehen (inkl. Verschiebung von indoor zu outdoor).

Die sporadische Auswertung von Mobilitätsdaten hat gezeigt, dass in den bisherigen Pandemie Jahren Maßnahmen und andere Einflussfaktoren zu unterschiedlichen Zeitpunkten in unterschiedlichem Maß mit einem veränderten Mobilitätsverhalten der Zielgruppen einhergingen. Diese Auswertungen erfolgten jedoch ad-hoc und auf hoher Aggregationsstufe, sodass die Auswirkungen einzelner Maßnahmen bzw. Maßnahmenpakete sowie einzelner maßnahmenunabhängiger Faktoren nicht ausreichend voneinander unterscheidbar sind. Ebenfalls besteht ein Bedarf nach Auswertungen auf sub-nationaler Ebene unter anderem hinsichtlich bezirksinternem und -übergreifendem Reise- und Kontaktverhalten, was ebenfalls einer diesbezüglichen Maßnahmenevaluierung, insbesondere im ländlichen Raum, entgegensteht.

Hier bedarf es einer noch tiefergehenden Analyse von intendierten (z.B. reduzierte Kontakte, vermehrtes Testen) und nicht-intendierten Kausalitätsketten zwischen Maßnahmen und der epidemiologischen Entwicklung bzw. des Fallgeschehens.

Mobilitätsdaten bergen folglich, insbesondere in Verbindung mit epidemiologischen und anderen Gesundheitsdaten ein hohes Potenzial zur Ermittlung der Kausalitäten während einer Pandemie. Sie können aber auch zur Früherkennung und Steuerung in Pandemien, sowie weiterer Krisen im Gesundheitssektor, beitragen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Evaluierung des Potentials von Mobilitätsdaten für die epidemiologische Forschung unter Berücksichtigung des Datenschutzes (inkl. internationale Vergleiche)
- Möglichkeiten zur (regelmäßigen) Verfügbarkeit, Nutzbarmachung und Auswertung von Mobilitätsdaten im Rahmen des Epidemie- und Pandemiemanagements
- Darstellung von Kausalitätsketten (Einfluss und Wirkung spezifischer Maßnahmen auf die epidemiologische Entwicklung bzw. das Infektionsgeschehen)
- Validierung von Mobilitätsdaten als Prädiktoren epidemiologischer Risiken und Entwicklungen sowie Absteckung von Limitationen bzw. Interpretationsbedarf
- Retrospektive Analyse/Evaluierung einzelner lokal (z.B. Reisebeschränkungen nach dem Hochinzidenzerlass), national und grenzüberschreitend gesetzter Maßnahmen sowie exogener Faktoren (Saisonalität) hinsichtlich Mobilität und Infektionsgeschehen mittels Nutzung von Mobilitätsdaten als Erkenntnisgewinn für das Krisenmanagement zukünftiger gesundheitlicher Krisen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.17 Abwassermonitoring als Instrument der Krisenprävention, sowie des Krisen- und Pandemiemanagements

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VII/A/11 - Übertragbare Erkrankungen, Krisenmanagement, Seuchenbekämpfung

E-Mail: IXA7@gesundheitsministerium.gv.at

Das Abwassermonitoring als Surveillance System stellt ein effektives Instrument zur Unterstützung des öffentlichen Gesundheitsmanagements dar. Im Zuge der SARS-CoV-2 Pandemie gewann die abwasserbasierte Epidemiologie zunehmend an Bedeutung und spielt eine immer größere Rolle im Pandemiemanagement. Aufbauend auf einer EU-Empfehlung hat das BMSGPK im Sommer 2021 eine Nationale Referenzzentrale (NRZ) zur Überwachung von SARS-CoV-2 im Abwasser ausgeschrieben und im Jänner 2022 die NRZ und das Nationale SARS-CoV-2 Abwassermonitoringprogramm etabliert.

Mit dem SARS-CoV-2 Abwassermonitoringprogramm wurden wichtige Rahmenbedingungen geschaffen, so dass die Weiterentwicklung des Systems auch hinsichtlich künftiger Herausforderungen im Themenbereich Wasser und Gesundheit nur folgerichtig ist. Im Zusammenhang mit mehreren übertragbaren Krankheiten (Polio, Affenpocken) ist es sinnvoll, das Potenzial des Abwassermonitorings und die Möglichkeiten der abwasserbasierten Epidemiologie als Informationssystem über die Präsenz von Krankheitserregern zu nutzen und auf neu auftretende oder auch

bekannte Infektionskrankheiten auszuweiten. Die bevorstehende Überarbeitung der kommunalen Abwasserrichtlinie (91/271/EWG), zu der die Europäische Kommission im Herbst 2022 einen Entwurf vorlegen will, wird abwasserbasierte Epidemiologie zur Überwachung unterschiedlicher pathogener Erreger auf den Weg bringen.

Abwasserbasierte Epidemiologie ist ein breit einsetzbares Surveillance Instrument im öffentlichen Gesundheitsmanagement. Sie erlaubt unabhängig von Individualdiagnostik eine zeitnahe Überwachung von bekannten aber auch neuen Pathogenen und ermöglicht somit, Ausbrüche frühzeitig zu erkennen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation potentieller Zielpathogene
- Aufbau nationaler Expertise – gebündelte Fachkompetenz in der Etablierung von Arbeitsabläufen und Prozessen für den Nachweis von pathogenen Erregern im Abwasser (generelles Abwasser-Surveillance-System)
- Evaluierung der Tauglichkeit etablierter Analysenverfahren und -abläufe für den Nachweis relevanter Zielpathogene im Abwasser
- Adaptierung des bundesweiten SARS-CoV-2-Abwassermonitorings zur Früherkennung von gesundheitlichen Risiken hinsichtlich einer möglichen Infektion mit anderen pathogenen Krankheitserregern (Methodik und Analytik)
- Entwicklung eines Evaluierungsansatzes für die Interpretation quantitativer Abwasserergebnisse vor dem Hintergrund verschiedener Erregervarianten
- Entwicklung von Konzepten für die Umsetzung von Abwassermonitoringprogrammen in Kombination mit/Ergänzung zu bestehenden Sentinelsystemen inklusive gemeinsamer Datenplattformen
- Vernetzung des Abwassermonitorings mit bestehenden Sentinelsystemen
- Konzeptstudien für die Analyse der Effektivität des Abwassermonitorings zur Überwachung des Infektionsgeschehens ausgewählter übertragbarer Krankheiten.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.18 Schutz kritischer Infrastruktur im Bereich AMR und Sicherstellung einer antimikrobiellen Therapie

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VII/A/9 - Öffentliche Gesundheit, Antibiotikaresistenz (AMR), Krankenhaushygiene, Gesundheitssystem- assoziierte Infektionen (HAI)

E-Mail: reinild.strauss@gesundheitsministerium.gv.at

Antimikrobielle Resistenz (AMR) bedroht Gesundheit und Lebensqualität weltweit. Die Europäische Behörde für die Krisenvorsorge und -reaktion bei gesundheitlichen Notlagen der Kommission (HERA) zählt AMR zu den drei größten Gesundheitsbedrohungen, die koordinierte Maßnahmen auf EU-Ebene im

Zusammenhang mit medizinischen Gegenmaßnahmen erfordern. Der HERA-Vorstand hat eine Liste veröffentlicht, die drei Kategorien lebensbedrohlicher oder anderweitig ernsthaft bedrohlicher Gesundheitsgefahren enthält, die sich auf die Mitgliedstaaten ausbreiten können: 1) Krankheitserreger mit hohem Pandemiepotenzial, 2) chemische, biologische, radiologische und nukleare Bedrohungen und 3) Bedrohungen aufgrund antimikrobieller Resistenzen (Liste der drei größten Gesundheitsbedrohungen (europa.eu)).

Durch Resistenzbildung können Infektionskrankheiten, die bisher gut durch antimikrobielle Mittel therapiert werden konnten, immer häufiger fatal enden. AMR und multiresistente Erreger führen zu erhöhter Morbidität und Mortalität, verlängerten Krankenhausaufenthalten und erhöhten Therapiekosten. Besonders immungeschwächte Personen in Alten-/Pflegeheimen, Neonatologien und Intensivstationen sind gefährdet. Durch vermehrte Personenmobilität (Globalisierung, Migration, Flucht) wird die Problematik verstärkt und resistente Keime nach Österreich gebracht. AMR stellt nicht nur ein Problem für einzelne Patient:innen dar, sondern durch Übertragungspotential und erhöhte Kosten/Personalressourcen auch für die öffentliche Gesundheit.

Um Infektionen durch Bakterien, Viren, Pilzen und Parasiten weiterhin effektiv in Österreich, auch in Zukunft, behandeln zu können, benötigt es aktive Forschung, Entwicklung und Innovation. Hiermit soll eine kritische antimikrobielle Therapie für alle Patient:innen, die diese benötigen, gesichert und der Schutz kritischer Infrastruktur im Bereich AMR, speziell die medizinische Versorgung und der Zugang zu wirksamen Medikamenten und Therapieoptionen geschützt werden.

Die Entwicklung neuer antibakterieller Behandlungen ist weltweit unzureichend, um der wachsenden Bedrohung durch AMR zu begegnen, so der jährliche Pipeline-Bericht der Weltgesundheitsorganisation. Der Bericht für das Jahr 2021 beschreibt die klinische und präklinische Pipeline von Antibiotika als stagnierend und weit davon entfernt, den globalen Bedarf zu decken. Seit 2017 wurden nur 12 Antibiotika zugelassen, von denen 10 zu bestehenden Klassen mit etablierten Mechanismen der antimikrobiellen Resistenz (AMR) gehören (WHO: 2021 Antibacterial agents in clinical and preclinical development: an overview and analysis).

Ziel ist es, alternative und/oder neue Behandlungsmethoden für (bereits) resistente Erreger voranzutreiben. Weiters soll der bisher wenig beachtete Bereich der antimikrobiellen Resistenz in Viren, Pilzen und Parasiten beleuchtet werden und der Einfluss von Antiseptika (u.a. Desinfektionsmittel) auf AMR erforscht werden.

In diesem Zusammenhang besteht folgender Forschungsbedarf:

- Erforschung neuer antimikrobieller Mittel und Alternativen zu Antiinfektiva-Therapie
- Antimikrobielle Resistenz in Viren, Pilzen und Parasiten sowie Einfluss Antiseptika auf AMR.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.19 Surveillance und Gewährleistung von Trinkwasser-Sicherheit und Wasser-Qualität

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)

E-Mail: alois.leidwein@ages.at

Kontakt: BMSGPK, III/B/13 - Lebensmittelsicherheit und Verbraucherinnen- und Verbraucherschutz: Kontrolle, Hygiene und Qualität

E-Mail: chistina.lippitsch@gesundheitsministerium.gv.at

Wasser begleitet den Menschen tagtäglich. Als wichtigstes Lebensmittel füllt es die Wasservorräte im Körper und versorgt ihn mit Mineralstoffen wie Magnesium, Calcium oder Natrium. Als Nutzwasser wird es im Haushalt oder am Arbeitsplatz verwendet, und an heißen Sommertagen dient es Mensch und Tier als Abkühlung. In Österreich kann Trinkwasser jederzeit in bester Qualität aus den Wasserleitungen entnommen werden, und auch Badegewässer weisen durchwegs höchste Qualität auf. Diese elementare Ressource gilt es umfassend zu schützen.

Der durch den Klimawandel bedingte globale Temperaturanstieg führt auch zur Erhöhung der Wassertemperaturen von Oberflächengewässern, was ein übermäßiges Wachstum von Mikroorganismen verursachen kann. Von speziellem Interesse werden die Cyanobakterien erachtet, die landläufig auch als Blaualgen bekannt sind. Eine Massentwicklung dieser Mikroorganismen (oftmals als CHAB (cyanobacterial harmful algal bloom) abgekürzt) kann die Wasserqualität beeinträchtigen und die Nutzbarkeit des betreffenden Gewässers stark einschränken. Einige Cyanobakterien-Spezies werden mit der Produktion von Toxinen assoziiert, die für Mensch und Tier gesundheitsgefährdend sind. Die Symptome, die von diesen sogenannten Cyanotoxinen ausgelöst werden, sind vielfältig und reichen üblicherweise von Hautreaktionen, Entzündungen bis hin zu Magen- und Darminfektionen. Bei Tieren, speziell bei Hunden, kommt es jedoch auch gelegentlich zu Lähmungserscheinungen oder sogar zum Tod.

Eine weitere potenzielle Auswirkung des Klimawandels auf den Landschaftswasserhaushalt wurde kürzlich erst beschrieben. Durch den tendenziell sinkenden Grundwasserstand drückt das Grundwasser anders als bisher an vielen Stellen nicht mehr nach oben und speist Oberflächengewässer wie Bäche und Flüsse (exfiltriert), sondern das Wasser der Fließgewässer versickert mehr in den Untergrund (infiltriert). Als Folge dieser Druckumkehr können mit den Oberflächengewässern auch Schadstoffe ins Grundwasser eindringen, das die wichtigste Trinkwasserquelle in Österreich darstellt.

Um Wasser als qualitativ einwandfreie Ressource zu schützen, sollen in den Bereichen (Erholungs-/Nutz-) Gewässer und Trinkwasser folgende Forschungsschwerpunkte gesetzt werden:

- Sicherheit bei anhaltenden Effekten des Klimawandels z.B. bei Einbezug von Gefahren in Nutz- und Badegewässern durch Anstieg von Cyano-Bakterien etc.

- Nationale Beobachtung von neuen, klimatisch hervorgerufenen Gefahren für Trinkwasser sowie z.B. Microcystine in Wassertieren, die auch als Lebensmittel genutzt werden
- Sicherheit und Einbezug von Wasser-Qualitäts- und Prüfdaten in digitale Systeme z.B. zur Steigerung eines stabilen Austausches zwischen Wasser-Versorgern und Analyse-Organen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.20 Neue Gefahren für die Gesundheit in Österreich durch klimawandelbedingte, neu oder wieder auftretende Infektionskrankheiten und allergieauslösende Neobiota (Vektorübertragene Infektionskrankheiten,...)

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VII/A/11 - Übertragbare Erkrankungen, Krisenmanagement, Seuchenbekämpfung

E-Mail: IXA7@gesundheitsministerium.gv.at

Kontakt: Agentur für Gesundheit und Ernährungssicherheit (AGES)

E-Mail: alois.leidwein@ages.at

Bezugnehmend auf z.B. Auftreten, Management und Systemeffekte neuer sowie wieder-auftretender vektorübertragener Krankheiten (endemisch/pandemisch) muss eine solide Datenlage für Österreich erstellt werden, um frühzeitig auf Risiken und Bedrohungsszenarien für die Gesundheit und damit die Gesundheitsversorgung zu reagieren. Daher ergeben sich u.a. folgende Forschungs-Schwerpunkte:

- Analyse, Überwachung und Management neu auftretender Gesundheitsrisiken durch invasive sowie bestehende Vektoren in Hinblick auf die Übertragung von Infektionskrankheiten (z.B. Insekten)
- Monitoring von Vektoren und Reservoirtieren (z.B. Nagetiere, Vögel) und Zusammenführung von Informationsquellen und ggf vorhandenen Datenbanken
- Weiterer Schwerpunkt ist die Entwicklung von Validierungs- und Qualitätssicherungswerkzeugen zur Erhebung diesbezüglicher Gesundheitsrisiken und zum nationalen sowie internationalen/grenzüberschreitenden Austausch von diesbezüglichen Daten, Informationen und Lösungsansätzen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.21 Resiliente Dateninfrastrukturen für Gesundheitskrisen

Kontakt: Gesundheit Österreich GmbH (GÖG)

E-Mail: claudia.habl@goeg.at, CC: alexander.degelegger-marquez@goeg.at

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VI/B/7 – Gesundheitsinformationsmanagement und Gesundheitsinformatik

E-Mail: Robert.Scharinger@gesundheitsministerium.gv.at

Gesundheitskrisen stellen eine große Herausforderung für die Gesundheitsversorgung, aber auch für die Steuerung von Gesundheitssystemen dar. So sind je nach Bedrohungslage bestimmte Datenerhebungen, -verknüpfungen und -verarbeitungen Voraussetzung für zielgerichtete Analysen, deren Ergebnisse erst die Handlungsfähigkeit der sicherheitspolitischen und Public Health-Akteure sicherstellen. Im Anlassfall müssen die richtigen Daten zur richtigen Zeit in ausreichender Qualität zur Verfügung stehen. Technischen Infrastrukturen und Prozesse müssen skalierbar sein und eine effiziente Datenverarbeitung erlauben.

Im COVID-19 Variantenmanagementplan der Bundesregierung ([BMSGKP \(Hg.\) \(2022\): COVID-19-Pandemie. Bestandsaufnahme und Handlungsrahmen. Version 2.0](#)) ist die Problematik der Fragmentierung der österreichischen Gesundheitsdatenlandschaft angesprochen. Es werden Lösungsansätze skizziert, wie etwa die Weiterentwicklung des Epidemiologischen Meldesystems. Es wird auch auf die Wichtigkeit der Nutzung der Möglichkeiten der Digitalisierung hingewiesen, etwa in Bezug auf automatisierte Schnittstellen bei der Befüllung von Public Health-Registern. Besonderes Augenmerk wird auf die Verantwortlichkeit der Bundesebene für das Krisenmanagement gelegt. In der Ausgestaltung der Governance-Strukturen für Gesundheitsdaten spielen nicht zuletzt deshalb die Bundesakteure eine zentrale Rolle.

Auf europäischer Ebene bieten die Entwicklungen rund um den Europäischen Gesundheitsdatenraum (European Health Data Space, EHDS) Möglichkeiten die Sekundärnutzung von Gesundheitsdaten für sicherheitspolitische und Public Health-Zwecke weiterzuentwickeln.

In diesem Zusammenhang ergibt sich folgender Forschungsbedarf:

- Wie kann und soll eine Dateninfrastruktur des Bundes gestaltet sein, die unter Wahrung von Datenschutz- und Datensicherheitsstandards ein effizientes und effektives Management von Gesundheitskrisen ermöglicht?
- Welche Prozesse braucht es für Datenerhebung, -auswertung und Governance (Entscheidungsfindung, Stakeholder-Einbindung, etc.)? Wie können diese so konzipiert werden, dass sie ressourcenschonend aufrechterhalten und im Anlassfall skaliert werden können?
- Wie lassen sich die durch den EHDS veränderten rechtlichen Rahmenbedingungen in Österreich nutzen, um resiliente Dateninfrastrukturen und Prozesse zur Erhebung und Auswertung krisenrelevanter Gesundheitsdaten aufzubauen?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.22 Mixed Reality Trainingsframework für das Trainieren von zivilen Expert:innen für den Einsatz bei Krisensituationen

Kontakt: Bundesministerium für europäische und internationale Angelegenheiten

E-Mail: Mag. Philipp Agathonos, philipp.agathonos@bmeia.gv.at

Zivile Fachkräfte müssen bestimmte Skills für multidimensionale, internationale Kriseneinsätze, inkl. Friedensmissionen, im Vorfeld erlernen. Derzeit fehlt hier allerdings eine überzeugende Visualisierung des späteren Einsatzortes im Training und somit die Möglichkeit, bestimmte Skills im Vorfeld überzeugend unter Stress zu trainieren.

Zu trainierende Skills reichen hier von Konfliktanalyse/interkulturelle Kompetenz/Mediation zwischen Konfliktparteien/Unterstützung bei der Umsetzung von Friedensabkommen/Wahl- und Menschenrechtsbeobachtungen hin zu strategischer Planung (Krisenmanagementpläne inklusive Evakuierung) und sogenannter Hostile Environment Awareness Trainings (HEAT) – bei welchem zivile (und militärische) Fachkräfte lernen, sich selbst im Falle einer Geiselnahme zu schützen. Für ein überzeugendes Training von Auslandseinsätzen bieten sich Virtual Reality (VR) Technologien an.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Identifikation von notwendigen Skills bei multidimensionalen, internationalen Kriseneinsätzen, inkl. Friedensmissionen. Diese beinhalten beispielsweise Mediationsskills, Verhalten in anderen Kulturen, Minenkunde, etc.
- Erarbeitung eines virtuellen Trainingsframeworks, welches geeignete Übungen für das Erlernen der notwendigen Skills bereitstellt
- Identifikation und Umsetzung von Trainingsszenarien, in denen die notwendigen Skills unter Stress eingesetzt werden sollen – z.B. Wahrnehmung von Gefahrenbereichen, richtiges Verhalten in der Kooperation mit lokalen Akteuren, an Checkpoints, bei Verletzungen von Menschenrechten, bei Evakuierung, etc.
- Möglichkeiten für die Übungsleitung, die jeweiligen Handlungen der Trainierenden zu bewerten und darauf zu reagieren – inklusive darauf basierende Änderungen im Ablauf der Simulation
- Bereitstellung einer Benutzeroberfläche für die Übungsleitung, in welcher die Übungen individuell zusammengestellt werden können bzw. der Übungsablauf gesteuert werden kann
- Erfassung von Trainingsfortschritt und Trainingswirksamkeit sowie die durchgängige Aufzeichnung von Handlungen und Ereignissen während des Trainings, um eine effiziente Nachbetrachtung zu ermöglichen bzw. aus Fehlern zu lernen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.23 Einbindung informeller Hilfsangebote in das Krisen- und Katastrophenmanagement

Kontakt: Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH

E-Mail: georg.aumayr@johanniter.at

Neben der formellen Katastrophenhilfe durch Behörden und Organisationen mit Sicherheitsaufgaben, kann bereits kurz nach dem Eintritt von Schadensereignissen eine hohe Solidarität und Hilfsbereitschaft der Bevölkerung beobachtet werden. Dies äußert sich durch die unmittelbare Unterstützung von Verwandten und Bekannten der Geschädigten, aber auch durch Initiativen von Einzelpersonen oder Unternehmen.

In solchen Fällen entsteht ein hochdynamischer und unübersichtlicher Markt, der die unterschiedlichen Bedarfe geschädigter Personen mit dem Angebot inoffizieller Helfer:innen gegenüberstellt. Das Angebot kann neben Warenspenden ebenso Dienstleistungen (z.B. einfache manuelle Tätigkeiten, Dolmetscherdienste, Einweiser- und Lotsenleistungen, etc.) beinhalten, und wird auf verschiedenen Kanälen (persönliche Netzwerke, Soziale Medien, Flugblätter etc.) kommuniziert.

Um die Effektivität und Effizienz der Katastrophenhilfe möglichst zu stärken, empfiehlt es sich die formellen Unterstützungsleistungen mit der informellen Unterstützung zu bündeln und die dafür notwendigen Aspekte in den Abläufen der Stabsarbeit zu berücksichtigen. Möglichkeiten und Lösungen hierfür sollen untersucht und entwickelt werden.

Forschungsbedarf:

- Analyse der Kommunikationsprozesse in der Einbindung ungebundener Helfer:innen und spontaner Freiwilligkeit im nationalen und internationalen Kontext
- Untersuchung der rechtlichen und ethischen Rahmenbedingungen die sich aus dem Einsatz ungebundener Helfer:innen und spontaner Freiwilliger im Krisen- und Katastrophenfall ergeben
- Untersuchung und Entwicklung von Möglichkeiten zur
- Einbindung informeller Helfer:innen in die strategische, taktische und operative Planung
- Vereinfachung der Kommunikation für die Hilfsorganisationen
- Erhöhung der Akzeptanz von Kommunikationsangeboten bei den Freiwilligen

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.24 Digitaler Kompetenzausweis

Kontakt: Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH

E-Mail: georg.aumayr@johanniter.at

In bestimmten Krisensituationen ist der Einsatz von spontanen Freiwilligen zur Bewältigung der Situation notwendig (bspw. Überflutungen, Erdbeben, Betreuung von Flüchtlingen, ...). Um diese informellen Helfer:innen bestmöglich einbeziehen zu können, müssen die professionellen Hilfsorganisationen (wie etwa die Johanniter oder das Rote Kreuz) die Personen registrieren. Wenn einige über bestimmte Spezialkenntnisse verfügen (z. B. medizinische Ausbildung, Sprachkenntnisse, handwerkliche Kenntnisse, ...), kann diese Information die Zuweisung von Ressourcen und die Wirksamkeit des Einsatzes steigern. Die Erhebung von besonderen Fähigkeiten und die Bewertung dieser Informationen ist in der Regel während eines Krisenereignisses jedoch kaum möglich. Die Erfassung und Validierung solcher Informationen vor dem Eintreten einer Krisensituation wäre eine wichtige Voraussetzung, den Einsatz von Freiwilligen auch bei spontanen Einsätzen organisationsübergreifend gezielter zu gestalten. Dafür bedarf es jedoch klarer Rahmenbedingungen über die Bestätigung von Fähigkeiten, sowie wie diese gespeichert und abgerufen werden können, um die Privatsphäre und Sicherheit dieser Informationen zu gewährleisten.

Darüber hinaus gehend ist die Nutzung von Kompetenzprofilen und -nachweisen ein wichtiger Faktor der Bindung von Ehrenamtlichen an die Organisationen. Der Nutzen eines Kompetenzprofils für ungebundene Helfer sowie für gebundene Helfer erlauben es einen Pool an Kompetenzen für Katastropheneinsätze sowie für Standardsituationen zu generieren, der regelmäßig genutzt werden kann. Im Sinne eines bidirektionalen Verständnisses können so auch Angebote von Hilfsorganisationen gezielter erstellt werden und Personen, die Hilfe anbieten wollen, ein Betätigungsfeld mit Gleichgesinnten zur Verfügung zu stellen. Bereits in Vorprojekten wie SLIC und SLIC 2 wurden für Ehrenamtliche Kompetenzprofile entwickelt. In diesem Thema sollen diese Erkenntnisse nun ausgeweitet werden und sowohl für Einsatzorganisationen als auch ungebundene Helfer und Organisationselemente entstehen, um eine Kooperation zu erleichtern, einen Ressourcen Überblick zu erstellen und eine Eingliederung der Helfer in die SKKM Prozesse zu ermöglichen.

Forschungsbedarf:

- Erhebung der organisatorischen, rechtlichen, ethischen und technischen Anforderungen
- Bedarfserhebung und Akzeptanzanalyse für strukturierende Maßnahmen bei Spontanhelfer:innen
- Entwicklung eines Konzepts für ein einfach handhabbares, sicheres Zertifizierungssystem
- Prototypische Umsetzung eines sicheren Zertifikats das ein hohes Maß an Sicherheit durch Security-by-Design aufweist
- Prototypische Umsetzung und Validierung eines ausgewählten Anwendungsfalls

- Sozio-technische Entwicklung zur Einbindung von Hilswilligen in Hilfsorganisationen als Ehrenamtliche und Nutzung der persönlichen Kompetenzen zur Stärkung der Einsatzorganisationen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.25 Entwicklung eines Wissensmanagementsystems im Österreichische Feuerwehrwesen

Kontakt: Österreichischer Bundesfeuerwehrverband – Kompetenzzentrum für wissensbasierte Gefahrenabwehr

E-Mail: gerald.czech@ooelfv.at

Wissen im Katastrophenschutz reicht von einfachen, lokalen Handlungen von Einzelpersonen bis hin zur komplexen Koordination des UN-Clustermechanismus mit vielen nationalen und internationalen Organisationen über längere Zeiträume hinweg. In Österreich sind es vor allem die Feuerwehren, die Wissen zur Gefahrenabwehr auf verschiedenste Arten zur Anwendung bringen. Dieses Wissen ist einerseits Erfahrungswissen der Feuerwehrleute und andererseits statisches (explizites) Wissen in Einsatz- und Ausbildungsunterlagen. In der jüngsten Eurobarometer-Umfrage zur Stellung von Wissenschaft und Technologie in Europa, zeigt sich, dass die Themenfelder Wissenschaft und Forschung sowie Innovation und Technologie in der Österreichischen Gesellschaft deutlich schwächer verankert sind als im Europäischen Durchschnitt. Gegenständliches Phänomen ist auch in Einsatzorganisationen erkennbar. Es zeichnet sich ein Gefälle zwischen dem Stand wissenschaftlicher Erkenntnisse und Innovationen und ihrer Berücksichtigung in der Praxis ab. Dies deutet auf ein grundlegendes Vertrauens- und Akzeptanzproblem hin, sowie auf die Notwendigkeit Strukturen und Einsatzstrategien entsprechend zu optimieren, um die Vorteile von technischen Assistenzlösungen auch nutzen zu können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Zur Verbesserung der Ist-Situation müssen technische Lösungen erreicht werden deren Verwendung nicht nur akzeptiert, sondern auch sozial-kulturell in der Einsatzbewältigung verankert sind. Dazu bedarf es als Grundlage der technischen Lösung eines fundierten sozial-kulturellen Lösungsansatzes.
- Berücksichtigung der Handhabung und Bearbeitung umfangreicher Datenmengen (“Big Data”), Datenvielfalt, Datengenerierung in hoher Geschwindigkeit, Anwendung des Data Catalog Konzeptes und der FAIR principles
- Use-Case und Szenarien basiertes Auffinden von Datenquellen
- Harmonisierung von Nutzeranforderung und Standardisierung von Szenarien
- Fokussierung auf Daten, um eine fundierte Grundlage für die weitere Anwendung wie z.B. für ein KI-basiertes Entscheidungsunterstützungssystem zu bekommen

- Relevante Metadattentypen identifizieren: Datenqualität, Inhalte (z.B. IFAFRI Gaps), Zuordnung in der Wissenspyramide, Reifegrade (TRLs), Verwendbarkeit, Sprache, Kultur, ...
- Verknüpfung eines Lessons Learned Prozesses mit Übungs- und Einsatzauswertungen
- Geographische und zeitliche Sicht auf Daten und Wissen (Berücksichtigung der föderalen und regionalen Struktur, Berücksichtigung der verschiedenen Organisationsformen im Feuerwehrwesen wie z. B. Berufsfeuerwehren, Betriebsfeuerwehren, Ehrenamt, ...)
- Spezieller Fokus auf Datensicherheit und deren Verwendung/Weiterverarbeitung (Authentifizierung, Identifizierung, Zugriffssicherheit)
- Aufzeigen von Möglichkeiten der technischen Umsetzbarkeit und Verwendbarkeit und Integration in bestehende Systeme
- Nachhaltige Konzeption der Anschluss- und Ausbaufähigkeit des Wissensmanagementsystems nach Ende des F&E-Projekts.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.26 Aufbau und Entwicklung einer innovativen Gebäudedatenbank zur Unterstützung der Analyse der physischen Verwundbarkeit von Gebäuden gegenüber Naturgefahren

Kontakt: Elementarschäden Präventionszentrum

E-Mail: h.starl@elementarschaden.at

Obwohl Naturgefahrenprozesse bereits gut dokumentiert und in den Gefahrenkarten ausgewiesen sind, erfordern Risikoanalysen für das Siedlungsgebiet Daten zu exponierten Gebäuden (u.a. Anzahl, Bauweise, Bauperiode, Stockwerke, Hauptnutzungsart, Gebäudeöffnungen, Keller). Die physische Verwundbarkeit ist von den Gebäudeeigenschaften, wie beispielsweise der Bauweise bestimmt, und international gängige Modelle zur Abschätzung der z.B. Erdbeben- oder Hochwasserrisiken erfordern sehr detaillierte lokale Gebäudedaten. So kommen die meisten Studien über Erdbebenschäden zu dem Schluss, dass die Art der vertikalen und horizontalen Tragstruktur der wichtigste Faktor ist, der die seismische Anfälligkeit von Mauerwerksbauten beeinflusst.

Jedes Gebäude in Österreich wird im Gebäude- und Wohnungsregister (AGWR) der Statistik Austria erfasst. Unter dem Begriff „AGWR II“ ist die neu gestaltete Meldeschiene „Adress-GWR-Online“ sowie das gemäß BGBl. I Nr. 125/2009 inhaltlich erweiterte Gebäude- und Wohnungsregister subsumiert. Hier werden, abgesehen von Adressdaten, wenn vorhanden ebenso Daten hinsichtlich der Struktur von Gebäuden, Wohnungen und sonstigen Nutzungseinheiten geführt. Bei dem für die Verwundbarkeit von Gebäuden interessanten Merkmal der Bauweise ergibt sich, dass speziell bei älteren Gebäuden noch keine Daten zur Bauweise im AGWR zu finden sind. Ziel ist die Erweiterung der Daten von Gebäuden (u.a. Anzahl, Bauweise,

Bauperiode, Stockwerke, Hauptnutzungsart, Gebäudeöffnungen, Keller), Vertiefung des Wissens zu regionalen Unterschieden des Gebäudebestands auf lokaler und regionaler Ebene (auf Gemeindeebene oder Zählsprengelebene).

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Methoden und Technologien zur Modularisierung von Informationen, sowie zur Integration externer und offener Informations- bzw. Wissensquellen (z.B. historische Daten)
- Flexible und zuverlässige Extraktion von Information aus strukturierten sowie unstrukturierten heterogenen Datenquellen
- Verfahren und Methoden zur Herstellung der Interoperabilität zwischen heterogenen Systemen und IT-Services
- Methoden und Technologien zur Schadensmodellierung und zum KI-gestütztem Ableiten von Schlussfolgerungen
- Entwicklung eines flexiblen und adaptiven Systems zur automatisierten Analyse und Klassifikation von unstrukturierten Daten aus unterschiedlichen Quellen unter Verwendung von Methoden der Künstlichen Intelligenz
- Verknüpfung und Visualisierung von Gebäudedaten für die Risikoanalyse verschiedener Gefahrentypen, zur Verbesserung von Datenbeständen und Vergleichbarkeit im internationalen Kontext
- KI-gestützte Verbesserung der Ereignis- und Schadensdokumentationen, zur Vertiefung des Verständnisses von Schadensmustern auf lokaler Ebene (in Verbindung mit dem KIRAS Projekt CESARE)
- Bereitstellung eines Gebäudeinventars zur Bewertung von Risiken auf Gebäude-Ebene (z.B. Entwicklung von Schadensfunktionen/Vulnerability Curves)
- Für eine ausgewählte Gefährdung (z.B. Erdbeben, Überschwemmung etc) sollen auch exemplarisch die Daten in Bezug auf eine monetäre Schadensbewertung angewendet werden und die Nutzung der Daten validiert werden.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.27 Registerdatenbasierte Netzwerkanalysen zur Identifizierung krimineller Muster und strukturellen Risikos wie Steuerhinterziehung, Schattenwirtschaft, Geldwäsche und Strohleute (PACC im BFF)

Kontakt: Predictive Analytics Competence Center (PACC) im BMF

E-Mail: Mihai Paunescu, mihai.paunescu@bmf.gv.at

Organisierte Kriminalität ist auf vielen Ebenen eine inhärente, systematische Bedrohung für den Rechtsstaat. Seit 2018 existiert in Österreich das Register der wirtschaftlichen Eigentümer (WiEReg), welches zum Zweck der Verhinderung von Geldwäscherei und Terrorismusfinanzierung geschaffen wurde. Zuvor waren umfangreiche Informationen über die wirtschaftlichen Eigentümer der Rechtsträger

mit Sitz im Inland nicht verfügbar. So können im Firmenbuch (FBU) etwa auch juristische Personen als Gesellschafter eingetragen sein, wodurch der beherrschende Eigentümer nicht direkt ersichtlich wird.

Sowohl WiEReg als auch FBU enthalten wesentliche Informationen über Strukturen von und Zusammenhänge zwischen wirtschaftlichen Akteuren in Österreich. Daneben existieren weitere öffentliche Register, wie etwa das Vereinsregister oder Bundes- und Landesregister für gemeinnützige Stiftungen und Fonds.

Diese Strukturinformationen sollen zur Verbrechens- und Betrugsbekämpfung eingesetzt werden. Der Finanzverwaltung kommt hierbei eine besondere Rolle zu, da steuerlich relevante Tatbestände, den eigentlichen strafrechtlichen Delikten oft vorausgehen oder zumindest mit ihnen einhergehen und sich ein entsprechender Anfangsverdacht daher auch aus den regulären Prüftätigkeiten der Finanzverwaltung ergeben kann. Um diese Prüftätigkeit möglichst effizient zu steuern sollen unter anderem auch Strukturinformationen aus den genannten Registerdaten genutzt werden. Methoden der Sozialen Netzwerkanalyse (SNA), der Graphentheorie, oder auch der topologischen Graphentheorie bieten Möglichkeiten diese Strukturinformation für Vorhersage- und Risikobewertungsmodelle nutzbar zu machen. Diese Modelle sollen Empfehlungen für Prüfungstätigkeiten im bestehenden Wirtschaftskreislauf liefern, aber andererseits auch präventiv zur Risikobewertung eingesetzt werden können. So existiert etwa im Rahmen der eGründung bereits ein Risikobewertungsverfahren, dass langfristig zusätzlich auch die neuen Risikoinformationen aus SNA-Ansätzen zurückgreifen können soll.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erforschung und Entwicklung von Methoden auf Basis von Social Network Analysis (SNA) bzw. Graphentheorie zur Detektion von kriminellen Akteuren und Netzwerken
- Erforschung und Entwicklung von Ansätzen zur registerübergreifenden Identifikation von Akteuren, Netzwerken und Strukturen
- SNA basierte Methoden zur Risikobewertung bei eGründungen
- SNA basierte Methoden zur Risikobewertung von Neueintragen im WiEReg.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.1.28 Drohnen in der Landwirtschaft

Kontakt: Landeskammer für Land- und Forstwirtschaft in Steiermark

E-Mail: elisabeth.reith@lk-stmk.at

Prävention und Sicherheit im Bereich der Versorgung mit landwirtschaftlichen Gütern ist ein wesentlicher Aspekt der Grundversorgung für die Bevölkerung. Landwirtschaftliche Betriebe sehen sich bei der Erzeugung ihrer Güter heute jedoch

vielfältigen Herausforderungen ausgesetzt, die in weiterer Folge zu Ernteaussfällen führen. Dabei sind unter anderen Schäden durch Hagel, Sturm und Starkniederschläge, sowie die Gefährdung von Wein, Obst und Gemüsekulturen durch bestehende und neu eingeschleppte Schadorganismen zu nennen. Darüber hinaus kommt es in Folge der Klimaerwärmung zu nachteiligen Veränderungen in der vegetativen Entwicklung (u.a. Frostschäden an Kulturpflanzen). Diese sich daraus ergebende Gefahrenlage kann durch den Einsatz stationärer Technologien (Sensorik) sowie durch unbemannte Flugobjekte (zB Drohnen und UAV's) gemildert bzw. bereits im Vorfeld abgewehrt werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Definition von Szenarien (u.a. Hagelabwehr, Identifikation und biologische Bekämpfung von Schädlingen, Reduktion der Bodenverdichtung, Reduktion der Unfallgefahr im steilen Gelände, agiles Anpassen der landwirtschaftlichen Kulturen an die lokalen Umweltbedingungen)
- Evaluierung bestehender Sensorik u. UAV-Technologie, Adaptierung und Enveiterung der bestehenden Werkzeuge abgestimmt auf den Einsatzbereich der landwirtschaftlichen Einsätze
- Erarbeiten und Durchführung innovativer Feldversuchsszenarien, dazu zählt der Einsatz stationärer und mobiler Sensoren zur Erhebung der vorherrschenden Umweltdaten
- Sowohl Umsetzung und Testung stationärer Sensorik (2.8. für das Monitoring von Schädlingsbefall) als auch UAV-Technologie im Rahmen der erarbeiteten Szenarien, sowie Erstellung und Auswertung entsprechender Datenmodelle (Big Data) inkl. deren Verifizierung physisch vor Ort
- Entwicklung von Logistik- und Betriebskonzepten für eine nachhaltige Nutzung in der Landwirtschaft
- Automatisierte drohnen-basierte Schadenserhebungsalgorithmen, Überführen der Erkenntnisse in Nutzungsszenarien für Betriebe und Behörden, Ableitung von Maßnahmen und Erkenntnissen auf lokaler, regionaler und nationaler Ebene, sowie damit verbundener Wissenstransfer
- Erforschung sämtlicher Sicherheitsaspekte im Zusammenhang mit UAV-Technologien in der Landwirtschaft unter Berücksichtigung von Dual-Use Aspekten, Datenschutz, Redundanz, Autonomie und Akzeptanz.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.2 Schutz kritischer Infrastruktur. Ausschreibungsschwerpunkte für F&E-Dienstleistungen

3.2.1 Vorurteils kriminalität in Österreich

Kontakt: Bundesministerium für Inneres

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

Vorurteilsmotivierte Straftaten oder „Hate-Crimes“ sind gerichtlich strafbare Handlungen, die aufgrund der tatsächlichen oder vermeintlichen Zugehörigkeit des Opfers oder des Tatobjekts zu einer Gruppe, die die Täter/-innen ablehnen, vorsätzlich begangen werden. Vorurteilsmotivierte Straftaten haben tendenziell stärkere Auswirkungen als andere Straftaten (Wellen der Verletzungen), die ohne Vorurteilsmotiv begangen wurden. Denn diese Straftaten treffen neben dem Opfer häufig alle Träger/-innen desselben Identitätsmerkmals und möglicherweise die gesamte Gesellschaft. Daher haben Opfer von vorurteilsmotivierten Straftaten nachweislich ein tendenziell erhöhtes Unsicherheitsgefühl und die Bereitschaft, die Taten bei der Polizei anzuzeigen, ist oft geringer als bei Delikten ohne Vorurteilsmotive.

Bezüglich der Analyse der polizeilichen Daten hinsichtlich diskriminierender Motivlagen, Evaluierung und Analyse von Daten aus relevanten nationalen und internationalen Datenquellen (Metaanalyse) und „Good Practices“ sowie der Beleuchtung des Dunkelfelds im Bereich der Hasskriminalität durch geeignete Erhebungsinstrumente besteht weiterhin Forschungsbedarf, insbesondere hinsichtlich der Bereiche (Jugend-) Prävention und des „Community Policing“ (Gemeinsam.Sicher). Betrachtet werden sollen kriminologische, soziologische und rechtliche Aspekte.

Es geht darum, handlungsrelevantes Wissen durch moderne Analysemethoden zu generieren und aufzubereiten. Ziel ist es, Spekulationen, Vermutungen und anekdotische Evidenz zu Phänomenen, hinsichtlich der Zusammenhänge, Ursachen und Ausmaße, durch wissenschaftliche Methoden gewonnenes Wissen gegenüberzustellen, damit gesicherte Aussagen getroffen werden können.

Neue Perspektiven auf bekannte Ereignisse, Themen, Phänomene und Entwicklungen zu eröffnen, Ausgeblendetes in den Vordergrund zu heben, kritisch zu analysieren (retrospektive Analyse bzw. Ist-Stand-Analyse) und schließlich innovative Lösungsansätze aufzuzeigen. Dazu gehören auch Fragestellungen zu Evaluierung, Wirkungsmessung, Kosten-Nutzen-Analyse etc.

Die Herausforderung, die Bevölkerung zum Thema „Hate Crime“ zielgerichtet und nicht nach dem Gießkannenprinzip zu erreichen, ist im Zeitalter der rasanten Digitalisierung, der Pandemiebekämpfung und der Zunahme immer vielfältiger werdender, geschützter sozialer Gruppen und persönlicher Gruppenzugehörigkeiten (Intersektionalität) gewachsen.

Gesucht wird somit nach neuen Wegen bzw. (digitalen) Instrumenten in der Präventionskommunikation, um die Bevölkerung, v.a. besonders vulnerable Gruppen möglichst wirksam, rasch und zielgerichtet (zielgruppenspezifisch oder sogar individuell personalisiert), zu informieren bzw. vor neuen/aktuellen Kriminalitätsphänomenen zu warnen. Diese sollen bestehende Instrumente der kriminalpräventiven Arbeit (Aussendungen, Infoveranstaltungen, Informationskampagnen) sinnvoll ergänzen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Kriminologisch systematische Analyse der im PAD registrierten „Hate Crime“ Tatbestände auf opfergruppenspezifische Gesetzmäßigkeiten und Besonderheiten und Ableitung maßgeschneiderter, faktenbasierter, zielgruppenorientierter Präventions- und Repressionsstrategien
- Durchführung einer repräsentativen Dunkelfeldstudie zu Hate Crime Viktimisierung in Österreich mit vertiefenden Schwerpunkten basierend auf den Ergebnissen der ersten veröffentlichten Dunkelfeldstudie
- Vergleichende Studie von „Good practices“ europäischer „Hate Crime“ Kampagnen zu Erhöhung der Sensibilität und Anzeigenbereitschaft der breiten Öffentlichkeit bzw. besonders vulnerabler Opfergruppen, von Kooperationen zwischen Strafverfolgungsbehörden und zivilgesellschaftlichen Einrichtungen sowie nationaler Datenanalysen mit besonderem Fokus auf faktenbasierte Datennutzung für polizeiliche Präventionsarbeit.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.2 Wirkungsweisen der Bewährungshilfe

Kontakt: Bundesministerium für Justiz

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

Dem Übergangsmanagement von der Haft in die Freiheit und der Nachbetreuung von Straffälligen wird große Bedeutung für die Sicherheit der Gesellschaft eingeräumt. Insbesondere die Bewährungshilfe, die in Österreich durch den Verein NEUSTART angeboten wird, ist eine höchst sicherheitsrelevante Dienstleistung, da sie Verurteilte bzw. Haftentlassene dabei unterstützt, nicht rückfällig zu werden und ihren Weg zurück in die Gesellschaft zu finden. Während die Wiederverurteilungsraten nach Bewährungshilfe bekannt sind, fehlen fundierte sozialwissenschaftliche Studien zu den Wirkungen der Bewährungshilfe auf unterschiedlichen Ebenen der Sozialintegration und deren Einfluss auf die Legalbewährung.

In einer Studie, die der heterogenen Klientel der Bewährungshilfe gerecht wird, soll erforscht werden, welche Wirkungen die Betreuung auf die Lebens-, Bildungs-, Einkommens- und Wohnsituation, den gesundheitlichen Zustand sowie auf die Entwicklung prosozialer Einstellungen und Kompetenzen ihrer Klientel hat und

welche Zusammenhänge mit einer allfälligen erneuten Straffälligkeit bestehen. Die Studie soll statistisch abgesicherte Befunde zu den zentralen Einflussfaktoren und Wirkungszusammenhängen liefern und damit den gesellschaftlichen Nutzen der Bewährungshilfe ebenso beleuchten wie Ansätze für Verbesserungen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Definition und Operationalisierung der in der Bewährungshilfe zu erreichenden Ziele und Wirkungsdimensionen, Entwicklung eines validen Messinstruments
- Befragung eines repräsentativen Samples der Klient:innen der Bewährungshilfe zu den konkreten Wirkungen der Bewährungshilfe in unterschiedlichen Bereichen, wobei auf die ausreichende Berücksichtigung relevanter Subgruppen zu achten ist
- Methodentriangulative Erhebung und Analyse der Wirkungsweisen der Bewährungshilfe sowie der zentralen Einflussfaktoren auf Legalbewährung und Sozialintegration.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.3 Fremdenrecht und Strafrecht – Schnittpunkte und wechselseitige Abhängigkeiten

Kontakt: Bundesministerium für Justiz

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

Für den Vollzug des Fremdenrechts sind Verwaltungsbehörden bzw. Verwaltungsgerichte zuständig, für die Berücksichtigung fremdenrechtlicher Aspekte im Rahmen der Strafzumessung die Gerichte. Die mitunter lange Verfahrensdauer im Bereich des Fremdenrechts kann dazu führen, dass fremdenrechtliche Entscheidungen und Reaktionen erst lange nach den strafrechtlichen Maßnahmen erfolgen und bspw. auch fremdenrechtliche Freiheitseingriffe zeitlich nach strafrechtlichen Freiheitseingriffen gesetzt werden. Umgekehrt können fremdenrechtliche Maßnahmen Strafverfahren erschweren, wenn beispielsweise wichtige Zeug:innen (etwa in Verfahren wegen Menschenhandel oder Schlepperei) infolge eines fehlenden Aufenthaltsstatus rasch abgeschoben werden und im Strafprozess nicht mehr zur Verfügung stehen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Worin liegen die Interdependenzen zwischen Straf- und Fremdenrecht?
- Wie beeinflussen strafrechtliche Entscheidungen die fremdenrechtliche Entscheidung?
- Wie beeinflussen fremdenrechtliche Aspekte strafgerichtliche Entscheidungen und allfällige strafrechtliche Reaktionen?
- Inwieweit dürfen fremdenrechtliche Gesichtspunkte bei den strafrechtlichen Reaktionen berücksichtigt werden?

- Wie kann die Kooperation zwischen Straf- und Fremdenrecht vertieft werden, um Abschiebungen direkt aus der Strafhaft durchführen zu können, ohne zusätzlich eine Schubhaft zu benötigen?
- Wie können die Interessen der Strafrechtspflege und der notwendige Vollzug fremdenrechtlicher Entscheidungen bestmöglich in Einklang gebracht werden, um beispielsweise durch die Abschiebung wichtiger Zeug:innen nicht die zentralen Beweismittel für das Strafverfahren zu verlieren?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.4 Modernes Haftmanagement durch Monitoring des sozialen Klimas in Justizanstalten

Kontakt: Bundesministerium für Justiz

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

Qualitätsmanagement im Strafvollzug beruht international zunehmend auch auf regelmäßigen Messungen des sozialen Klimas in Haftanstalten. Denn das soziale Klima in Haft und die Haftbedingungen in einer Justizanstalt sind zentrale Parameter für die Lebens- und Arbeitsbedingungen von Inhaftierten und Personal. Empirische Studien zeigen, dass ein Zusammenhang zwischen Anstaltsklima und Gewalt in Haft besteht und dass das soziale Klima in Haft nicht nur für die Qualität des Strafvollzugs, sondern auch für die Resozialisierung von wesentlicher Bedeutung ist. Die kürzlich abgeschlossene KIRAS-Studie „SiGit“ (Sicherheit hinter Gittern) zeigt zudem, dass in Österreich zwischen den Justizanstalten zum Teil sehr große Unterschiede bestehen, wie das Haftklima eingeschätzt wird: Anhaltebedingungen, Professionalität des Personals, Legitimität des Haftregimes, Respekt und Menschlichkeit im Umgang mit den Inhaftierten, Möglichkeiten für sinnvolle Beschäftigung, Anspannung und Stress oder auch Überwachung und Kontrolle werden von den Inhaftierten sehr unterschiedlich bewertet.

Während im angloamerikanischen Raum regelmäßiges, wissenschaftlich fundiertes „Klima-Monitoring“ eine bedeutende Rolle spielt, gibt es nun auch vermehrt Bemühungen, im deutschsprachigen Raum ein solches zu etablieren. In Österreich existiert mit „SiGit“ bislang nur eine erste Erhebung zum sozialen Klima in Haft aus Sicht der Inhaftierten, es gibt jedoch kein international vergleichbares und in der Praxis gut handhabbares Instrument für ein regelmäßiges Monitoring des sozialen Klimas in Haft und der Anhaltebedingungen – unter Berücksichtigung der Sichtweise der Inhaftierten und des Personals.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwicklung eines validierten Instruments zur regelmäßigen Erhebung der Wahrnehmung des Anstaltsklimas durch Inhaftierte und durch Bedienstete in Österreichs Justizanstalten auf der Basis nationaler und internationaler Vorarbeiten

- Pilotierung von Erhebungen des Anstaltsklimas in den Justizanstalten unter besonderer Berücksichtigung der Akzeptanz und Praktikabilität der Instrumente
- Entwicklung eines Auswertungsschemas für ein Pilot-Monitoring der Anstalten
- Erstellen eines Fahrplans für eine Implementierung regelmäßiger Erhebungen in den Justizanstalten auch nach Abschluss des Projekts.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.5 Zusammenhänge zwischen Partnergewalt, Geschlechterrollenbildern und psychischer Gesundheit / psychischen Erkrankungen

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VI/A/1 – Nicht übertragbare Erkrankungen, psychische Gesundheit und Altersmedizin

E-Mail: christina.dietscher@sozialministerium.at

Partnergewalt ist eine weit verbreitete Form von Gewalt und schließt physische, sexuelle und emotionale Formen von Missbrauch und Misshandlung mit ein. Aufgrund der starken Tabuisierung der Thematik sind genaue Zahlen zur Betroffenheit schwer zu erheben, es gibt aber empirische Hinweise darauf, dass die Opfer intimer Partnergewalt zu etwa 90% Frauen, zu 10% Männer sind. Jede fünfte Frau in Österreich ist ab dem Alter von 15 Jahren im Laufe ihres Lebens von häuslicher und/oder sexualisierter Gewalt betroffen ([Fundamental Rights Agency \(FRA\) \(2014\). Gewalt gegen Frauen: eine EU-weite Erhebung](#)). Es handelt sich um vergeschlechtlichte häusliche Gewaltbeziehungen. Gewalt gegen Frauen ist zwar gesetzeswidrig, in gesellschaftlichen Strukturen aber trotzdem nach wie vor verankert und dementsprechend weit verbreitet. Bestimmte maskuline Rollenbilder spielen hier eine prominente Rolle – sie implizieren einen destruktiven Umgang mit negativen Emotionen, Herausforderungen, Problemen und Konflikten – was sich u.a. in Suchtverhalten und eben in der Anwendung von Gewalt zeigen kann (Stichwort „toxische Männlichkeit“). Dies ist freilich aus einer Perspektive zu betrachten, die Gewalt als gesamtgesellschaftliches Phänomen und Problemfeld in den Blick nimmt, auf welches viele unterschiedliche Einflüsse wirken und das von unterschiedlichen sozialen, ökonomischen und kulturellen Strukturen mitgeformt wird.

Partnergewalt wirkt sich laut WHO (2012) ([World Health Organization & Pan American Health Organization. \(2012\). Understanding and addressing violence against women: intimate partner violence. World Health Organization](#)) auf vielfältige Weise kurz- und langfristig direkt und indirekt negativ auf die physische und psychische Gesundheit der Betroffenen aus. Oftmals sind die in Gesundheitseinrichtungen tätigen Berufsgruppen, die einzigen Ansprechpartner:innen für sozial isolierte Gewaltopfer. Mögliche physische Folgen sind beispielsweise Verletzungen, durch übermäßigen Stress verursachte chronische nichtübertragbare Erkrankungen, sowie in Folge sexueller Gewalt ungewollte Schwangerschaften oder Schwangerschaftsabbrüche und Infektionen mit sexuell übertragbaren Erkrankungen. Zu den möglichen psychischen Auswirkungen auf

Opfer zählen emotionaler Stress, niedriges Selbstwertgefühl, Schlafstörungen, Depressionen, Angststörungen, posttraumatische Belastungsstörungen, Essstörungen, substanzbezogene Abhängigkeiten (Alkohol, Tabak, illegale Drogen), selbstverletzendes Verhalten und Suizidgedanken. Im extremsten Fall ist die Auswirkung der Beziehungsgewalt der Tod der Opfer durch Mord (Stichwort Femizide) oder Suizid.

Wenn Kinder im Haushalt leben, kann auch von negativen Auswirkungen auf die Kinder- und Jugendgesundheit ausgegangen werden. Die WHO (2012) führt hier u.a. Angst und Depressionen an. Zudem ist das Erleben von Gewalt gegenüber der eigenen Mutter in der Kindheit ein Risikofaktor dafür, später selbst Opfer oder Ausübende:r von intimer Partnergewalt zu werden.

Die WHO (2012) führt unter anderem den Missbrauch von Alkohol- und illegalen Drogen (Thema Sucht) sowie Persönlichkeitsstörungen als Risikofaktoren für gewaltvolles Verhalten in intimen Beziehungen an. Frühere Studien haben aufgezeigt, dass bei den Tätern von Beziehungsmorden bzw. Mordversuchen häufig Suchterkrankungen (insb. Alkoholabhängigkeit) und psychische Erkrankungen (u.a. Persönlichkeitsstörungen, aber auch Depressionen, posttraumatische Belastungsstörungen, und Angststörungen) diagnostiziert oder attestiert wurden, wobei sie in der Regel vor der Tat nicht in Behandlung waren. Fragen bzgl. der Prävalenz psychischer Erkrankungen in Gewaltbeziehungen und den genauen Zusammenhängen zwischen spezifischen Krankheitsbildern und häuslicher Gewalt sind für Österreich allerdings bisher nicht hinreichend erforscht. Nachdem deutlich mehr analysierbare empirische Daten zu Täterschaft bei Männern vorliegen, wird vorgeschlagen, hier zunächst auf Männer und maskuline Rollenbilder im Zusammenhang mit spezifischen psychischen Problemlagen zu fokussieren.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Gezielte und differenzierte Erhebung von Informationen zu den Risiken von Partnergewalt in Zusammenhang mit psychischen Erkrankungen/ Störungen, Suchterkrankungen/problematischem Konsum von legalen und illegalen Substanzen (inkl. Medikamenten) und männlichen Geschlechterrollenbildern
- Basierend darauf Erarbeitung von unterschiedlichen Tätertypologien (unter Berücksichtigung von sozioökonomischen und psychosozialen Komponenten und Rahmenbedingungen) und in Verbindung dazu stehenden Rollenbildern
- Aufzeigen von Möglichkeiten der Gewaltprävention und gezielten sowie zielgruppengerechten (das heißt v.a. gender- und kultursensiblen) Interventionen mit Schwerpunkt im psychosozialen Bereich
- Ableitung von sektorenübergreifenden Policy-Empfehlungen unter Berücksichtigung von internationaler Good Practice.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.6 Psychosoziale Resilienz von Beschäftigten in kritischen Infrastrukturen

Kontakt: Gesundheit Österreich GmbH (GÖG)

E-Mail: claudia.habl@goeg.at, CC: alexander.eggerth@goeg.at

Kontakt: Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, VI/A/1 – Nicht übertragbare Erkrankungen, psychische Gesundheit und Altersmedizin

E-Mail: christina.dietscher@sozialministerium.at

Die COVID-19 Pandemie und die Maßnahmen zu ihrer Bewältigung brachten beträchtliche psychische Belastungen für die gesamte Bevölkerung mit sich, wie durch zahlreiche Studien bzw. das vom BMSGKP beauftragte „Monitoring psychische Gesundheit“ belegt wurde. Besonders betroffen waren neben jungen Menschen und Frauen auch Menschen, die bereits vorher in schwierigen Situationen waren.

Im Zuge der Pandemie wurde der zentrale Stellenwert von Gesundheits- und Sozialsystemen bzw. von „kritischen Infrastrukturen“ hinsichtlich der Gewährleistung von Versorgungssicherheit, aber auch für die Aufrechterhaltung sozialer Sicherheit und Stabilität deutlich. Als **kritische Services bzw. Infrastrukturen** werden jene Infrastrukturen definiert, deren Nichtweiterführung hohe gesellschaftliche Kosten mit sich bringt. Beispiele für kritische Services sind Blaulichtorganisationen, Lebensmittelhändler, Gesundheits- und Pflegeeinrichtungen, Apotheken, IT-Services und Energieversorger ([BMSGKP \(Hg.\) \(2022\): COVID-19-Pandemie. Bestandsaufnahme und Handlungsrahmen. Version 2.0](#)).

Mitarbeiter:innen der kritischen Infrastruktur – insbesondere des Gesundheitswesens – gehören ebenso zu besonders belasteten Bevölkerungsgruppen, was ein Risiko für ihre psychische Gesundheit darstellt. Ein hoher Anteil des Gesundheitspersonals zeigte beispielsweise Symptome von posttraumatischen Stress-Symptomen, Depression, Angst oder Schlafstörungen (Barbara, Juen (Universität Innsbruck, Österr. Rotes Kreuz); Monika, Stickler (Österr. Rotes Kreuz) ((Hg.): Empfehlungen für die psychosoziale Unterstützung des Krankenhauspersonals in COVID-19). In der kritischen Infrastruktur beschäftigte Personen sind im Rahmen der COVID-19-Pandemie vielfach gefordert gewesen, körperlich und psychisch, akut und über einen langen Zeitraum. Personen wurden an und über Belastungsgrenzen gebracht, um ein Funktionieren und Aufrechterhalten des Systems zu allen Zeiten zu gewährleisten und neben der COVID-19-relevanten Versorgung auch die Regelversorgung sicherzustellen. Psychische Belastungen von Mitarbeiter:innen der kritischen Infrastruktur und damit in Zusammenhang stehende potenzielle Ausfälle können zu einer ohnehin brisanten Planbarkeit, weniger Verlässlichkeit und größerer Unsicherheit bezüglich gesellschaftlich relevanter Versorgungsaufgaben führen.

Allerdings zeigte sich (insbesondere im Gesundheitsbereich) auch, dass viele der Belastungsfaktoren bereits vor der Pandemie spür- und messbar waren und durch die Pandemie nur noch weiter verstärkt wurden. Es sind daher sowohl Maßnahmen auf individueller Ebene als auch auf organisatorischer Ebene notwendig, um den Beschäftigten in kritischen Infrastrukturen hier entsprechende Unterstützung und

Entlastung zu bieten bzw. ihre **psychosoziale Resilienz** zu stärken (Barbara, Juen; Alexander, Kreh et. al (2021): Effekte der Covid-19 Pandemie auf das Gesundheitspersonal: organisatorische Risiko- und Schutzfaktoren. In: Trauma – Zeitschrift für Psychotraumatologie und ihre Anwendungen. 19 Jg.(2021) Heft 3).

Resilienz ist die Kraft, sich zu erholen. Es ist eine Fähigkeit, ein relativ stabiles und gesundes Maß an psychischer und körperlicher Kompetenz aufrechtzuerhalten, auch wenn man kritischen Ereignissen bzw. extremen Stressoren ausgesetzt ist (Bonanno, G. A. (2004). Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive After Extremely Aversive Events? American Psychologist, 59(1), 20–28). Resilienz ist allerdings keine rein individuelle Personeneigenschaft, sondern bestimmt sich immer aus Person- UND Umweltfaktoren (Juen, Barbara, Siller, Heidi & Nindl, Sandra (2013). Resilienz als sozialer Prozess, Gruppenpsychotherapie und Gruppendynamik 49: 238 – 251 (2013)). Insofern ist anzunehmen, dass erfolgreiche Maßnahmen zur Minderung der Belastungsfolgen und zur Steigerung der Resilienz breit (an multiplen Faktoren) ansetzen und über die individuelle Ebene (z.B. „psychologische Sprechstunde“) hinausgehen müssen. Organisationale Resilienz muss bei Rahmenbedingungen wie Ausbildung, Bezahlung, Arbeitsbedingungen und adäquater Kommunikation ansetzen.

Während die Effekte und mögliche Schutzfaktoren für das Gesundheitspersonal bereits relativ gut untersucht sind, liegen für andere Bereiche der kritischen Infrastruktur noch sehr wenig Forschungsarbeiten vor. Im Rahmen dieses Projekts soll erhoben werden, welche nationalen und internationalen Studienergebnisse und Beispiele guter Praxis es zur Resilienzförderung, Belastungsreduktion und letztendlich Attraktivierung der Jobs in der kritischen Infrastruktur zu finden und auf österreichische Verhältnisse übertragbar sind.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Eingrenzung der einzubeziehenden Berufsgruppen bzw. Bereiche der kritischen Infrastruktur (wer sind die vulnerabelsten Gruppen? Welche Art von „Bedrohung“ haben die Mitarbeiter:innen in den unterschiedlichen Bereiche der kritischen Infrastruktur?)
- Gezielte und differenzierte Erhebung von nationalen und internationalen Studien zu Belastungen in jeweiligen Berufsgruppen/Bereichen
- Differenzierte Erhebung von Studien und good practice Beispielen zu geeigneten Maßnahmen der Resilienzförderung und Belastungsreduktion
- Basierend auf den Ergebnissen Aufzeigen von Möglichkeiten zur Verbesserung der psychosozialen Resilienz der Beschäftigten in kritischen Infrastrukturen
- Ableitung von konkreten und anwendungsorientierten Umsetzungsempfehlungen für die Bereiche der kritischen Infrastruktur unter Einbeziehung der betroffenen Bereiche
- Priorisierung erster konkreter Implementierungsschritte.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.2.7 Prävention antisemitischer Gewalt im schulischen Umfeld – Antisemitismus als Herausforderung für die Schule

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung

E-Mail: moritz.wein@bmbwf.gv.at

Antisemitismus stellt eine Herausforderung für alle Ebenen der Bildungsverwaltung dar, für Lehrpersonen, für Schulleitungen, für die Entwicklung von adäquaten Lernmaterialien, für die Schulaufsicht sowie für Lehrpersonenbildungseinrichtungen in der Entwicklung von Aus- und Fortbildungsangeboten zur Prävention von Antisemitismus. Die österreichische Bundesregierung hat mit der Nationalen Strategie gegen Antisemitismus (NAS) eine gesamtstaatliche Strategie gegen Antisemitismus beschlossen, die auch den Bildungsbereich betrifft. Der Forschungsbedarf ergibt sich aus den Maßnahmen der NAS und das Forschungsprojekt soll wissenschaftsbasiert die Umsetzung der NAS unterstützen. Forschungsvorhaben im Bereich der Antisemitismus- und Rassismusforschung leisten einen wichtigen Beitrag, die Sicherheit für alle Mitglieder der Gesellschaft zu erhöhen. Antisemitismus und Rassismus schränken die Entfaltungsmöglichkeiten für Betroffene ein und stellen ein Sicherheitsrisiko für die gesamte Gesellschaft dar. Die Maßnahme 18 der NAS sieht die Nutzbarmachung von wissenschaftlichen Erkenntnisse für Schulen und Schulaufsicht vor, um mit antisemitischen Vorfällen in angemessener Weise umgehen zu können.

Der [Antisemitismusbericht](#) der Israelitischen Kultusgemeinde Wien (IKG) umfasst alle der IKG gemeldeten Vorfälle. Für 2021 wurden insgesamt 965 antisemitische Vorfälle gemeldet. Im Vergleich zum Vorjahr entspricht das einem Anstieg um 65 Prozent und somit der höchsten erfassten Anzahl antisemitischer Vorfälle seit Beginn der Dokumentation vor 20 Jahren. Die gemeldeten Vorfälle umfassen verletzendes Verhalten, Sachbeschädigungen, Bedrohungen und physische Angriffe. Eine [Studie](#) des Kompetenzzentrums für Prävention und Empowerment der Zentralwohlfahrtsstelle der Juden in Deutschland zu Antisemitismus im schulischen Kontext (2020) weist auf die konkrete Auswirkung für Betroffene hin: „Die Befragten scheinen häufig darüber nachzudenken, ob und wie sie das Risiko eines möglichen Angriffs umgehen oder minimieren und ihr Verhalten entsprechend der Situation anpassen können“. Die alltäglichen Entscheidungen und das Aufwachsen junger Erwachsener werden so durch antisemitische Erfahrungen mitgeprägt.

Eine Forschungslücke besteht derzeit in Österreich im Bereich der Betroffenenforschung. In den vergangenen Jahren haben europäische Forschungsprojekte die Perspektive von antisemitismusbetroffenen (ehemaligen) Schülerinnen und Schülern, aber auch Eltern und Lehrkräften, beforscht. Für Österreich liegen derzeit keine Studien vor, die spezifisch die Situation von Lernenden und deren Umfeld betrachten. Aufbauend auf den Ergebnissen der Betroffenenforschung soll wissenschaftlich basierte Konzepte und Maßnahmen entwickelt werden, die die Umsetzung der NAS unterstützen. Die Studie zur Perspektive von Antisemitismus Betroffenen ermöglicht es den Lehrkräften, der Schule sowie allen Akteuren der Bildungsverwaltung, adäquate Angebote für Betroffene zu schaffen und Antisemitismus präventiv entgegenzuwirken.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welche Erfahrungen machen jüdische und von Antisemitismus betroffene Schülerinnen und Schüler und ihre Familien an Schulen und in ihrem Alltag?
- Wie sicher fühlen sie sich in Bezug auf Antisemitismus und welche Situationen schildern sie?
- Wie hat das schulische Umfeld auf Antisemitismus reagiert?
- Welche Unterstützungsangebote wurden wahrgenommen?
- Welchen Bedarf erwähnen Betroffene im Umgang mit Antisemitismus im schulischen Umfeld?
- Entwicklung von Konzepten und Maßnahmen zur Intervention, Prävention und zur Beratung von Betroffenen.
- Wie können Schulen bestmöglich auf antisemitische Vorfälle reagieren, wie könnte ein Casemanagement für die Schule aussehen?
- Wie könnten Beratungsangebote konzipiert werden, damit sie den Bedürfnissen der Betroffenen Schülerinnen und Schülern bestmöglich entsprechen? (Aufbauend auf den Empfehlungen des IHRA DACH-Projektes).

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.3 Cybersicherheit. Ausschreibungsschwerpunkte für kooperative F&E-Projekte

Themenschwerpunkt „Cybersicherheit“ Kooperative F&E Projekte (Als Vorbereitung und Testlauf für ein österreichisches digitales Sicherheitsforschungsförderprogramm).

3.3.1 Erkennung von Deepfakes und medialen Manipulationen in großen Sammlungen digitaler Bild- und Videoinhalte

Kontakt: Bundesministerium für Inneres

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

Die Cyberkriminalität hat zuletzt sprunghaft zugenommen, nicht zuletzt bedingt durch die Corona-Pandemie oder den Krieg in der Ukraine. Dies kann zu einer kontinuierlichen Erosion des Vertrauens in digitale Inhalte führen. Dieser Trend wird sich weiter verschärfen, denn zwischen dem Herstellen und Verbreiten von Deepfakes und dem Erkennen und Gegensteuern herrscht, ähnlich wie auf dem Gebiet der klassischen IT-Security, ein permanenter Wettlauf, bei dem die angreifende Person oft einen kleinen Schritt voraus ist. Ein durch Desinformation mitgeprägtes Meinungsklima stellt letztendlich eine Bedrohung der Gesellschaft und der Demokratie dar.

Mit leistungsfähigen Verfahren der KI lassen sich Videos in einer Weise manipulieren, dass zumindest mit bloßem Auge nicht mehr zu erkennen ist, ob sie echt sind oder manipuliert wurden. Weiterentwicklungen in der KI-Technologie geben den Erstellern von Deepfakes neue Werkzeuge in die Hand, um immer schwerer erkennbare Fälschungen zu produzieren.

Für eine verfahrenstechnische Verwertbarkeit deren Ergebnisse ist jedoch nicht nur das Erkennen und Entdecken von Manipulationen/Deepfakes ausreichend, sondern auch deren schlüssige technische Beschreibung. Erste konkrete Projekte (z.B. FFG KIRAS defalsif-AI) demonstrieren initiale Ansätze für eine Erkennung von Deepfakes. Für eine umfassende Unterstützung von Behörden, Medienvertretern und Content Management Providern ist aber eine regelmäßige und gezielte Weiterentwicklung der eingesetzten Werkzeuge zur Erkennung von Deepfakes notwendig, um präventive und reaktive Maßnahmen ergreifen zu können.

Dies betrifft Bedrohungen für die

- Innere/Externe Sicherheit – wenn bspw. mittels gefälschter Videos Polizeigewalt unterstellt wird
- Justiz – wenn gefälschtes Bildmaterial als digitaler Beweis für beliebige Situationen genutzt wird, bspw. wenn eine verdächtige Person bei einer bekannten Veranstaltung in z.B. Bregenz gezeigt wird, während sie andernorts eine Straftat begeht
- Medienorganisationen – welche ein gesteigertes Angebot an User-Generated-Content verifizieren müssen, um ihrer wichtigen Rolle in der Demokratie gerecht zu werden
- Einzelpersonen – z.B. bei Verwendung des Gesichts einer bestimmten (unbeteiligten) Person für die Produktion eines Deepfake-Videos.

Bei der Regulierung von Deepfake-Videos sind die relevanten Grund- und Persönlichkeitsrechte zu berücksichtigen und ist insbesondere auf den besonderen Schutz der Meinungsäußerungsfreiheit und der Kunstfreiheit zu achten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erarbeitung eines Konzeptes zur laufend aktualisierten Erkennung/Detektion von Deepfakes in Bildern und Videos
- Erstellung einer Datensammlung digitaler Bild- und Videoinhalte
- Erkennung von Deepfakes und Manipulationen in Bild- und Videoinhalten
- Cross-modale Analyse unterschiedlicher Medientypen
- Kontextanalyse anhand von Open-Source-Daten
- Entwicklung eines teilautomatisierten Softwaretools – anhand des Konzeptes –, welches zudem die zukünftige, regelmäßige und gezielte Weiterentwicklung ermöglicht
- Evaluierung des Softwaretools anhand der Datensammlungen, in aktivem Austausch mit unabhängigen Faktenprüfern
- GSK- und Rechtsanalyse in Bezug auf die Regulierung von Deepfakes unter Berücksichtigung relevanter Grund- und Persönlichkeitsrechte (Schutz der Meinungsäußerungsfreiheit, Kunstfreiheit)

- Umfassende rechtliche Analyse aktueller Deepfake-Detektionstechnologie im gegebenen rechtlichen Rahmen im europäischen Kontext z.B. unter Berücksichtigung von Aspekten aus der KI, menschliche Aufsicht, Interpretierbarkeit, Untersuchung der Implikationen des Einsatzes eines Analysetools auf Grundrechtspositionen (Datenschutz, Meinungsfreiheit), Möglichkeiten der forensischen Beweissicherung vor Gericht, Sicherstellung von Opferinteressen, Einbindung der Zivilbevölkerung, rechtliche Zulässigkeit des technischen Informationsaustausches zwischen Behörden inklusive Kostenzuordnung, Verantwortlichkeitsabgrenzung und systemischen Kontrollmechanismen in der gesellschaftlichen Kommunikation
- Ausarbeitung eines Prozesses zur nationalen Umsetzung des „Aktionsplans Deepfakes“ unter enger Einbindung von Behörden, Medien und GSK-Partnern zur Schaffung eines gesamtgesellschaftlichen Zugangs.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.2 Früherkennung von Fake News und Desinformationskampagnen in sozialen Netzwerken

Kontakt: BKA

E-Mail: sipol@bka.gv.at

Kontakt: BMLV

E-Mail: sicherheitsforschung@bmlv.gv.at

Hybride Bedrohungen („Hybrid Threats“) stellen eine akute Gefahr dar und dominieren zurzeit die Sicherheitslandschaft. Desinformationskampagnen (falsche und zielgerichtete Erzeugung irreführender Information, die verbreitet wird, um politische oder wirtschaftliche Ziele zu erreichen oder einer Person, sozialen Gruppen, Organisationen oder Ländern zu schaden) offenbaren immer mehr ihre politischen, gesellschaftlichen und wirtschaftlichen Risiken. Im Rahmen von „Hybriden Bedrohungen“ haben solche Kampagnen die Erreichung einer Informationsüberlegenheit unterhalb der Schwelle eines bewaffneten Angriffes zum Ziel. Durch den Einsatz von neuen Konzepten und Technologien verändert sich auch die Dynamik bei solchen Kampagnen und erschwert somit die Früherkennung von hybriden Bedrohungen.

Hybride Bedrohungen aus dem In- und Ausland können Einfluss auf verschiedene Akteure und Domänen haben, z. B. auf politische Entscheidungsträger, Polarisierungen, geopolitischen Einfluss und der Untergrabung des Vertrauens der Öffentlichkeit in demokratische Institutionen.

Die Gesellschaft und insbesondere die Medien stehen daher vor neuen Herausforderungen. Der Hauptfokus liegt auf der Informations- und Strategie-Kommunikation, im Speziellen auf der Identifizierung von irreführenden Inhalten in Online-Medien, Erkennung von Trends und Kampagnen im Bereich der

Desinformation und der Messung der Effektivität von Gegenmaßnahmen durch Narrative. Um die Glaubwürdigkeit von Online-Medien und frei zugänglichen Informationen (OSINT) zu ermitteln, werden derzeit in der Forschung unterschiedliche Ansätze (audiovisuelle Medienforensik, Textanalyse, multi-modalen Fusion mit Hilfe von AI und Data Science

Methoden) verwendet. Eine besondere Rolle nehmen dabei Deepfakes ein - perfekt gefälschte Video, Bilder oder Audio-Inhalte in denen Personen Aussagen in den Mund gelegt werden oder in denen sie scheinbar Handlungen begehen, die in Wirklichkeit nie stattgefunden haben. Zur konkreten Bedrohung für die Innere Sicherheit können gefälschte Videos werden, die bspw. Polizeigewalt unterstellen oder vermeintlich Polizistinnen und Polizisten präsentieren, die strafbare Handlungen begehen – was zu Vertrauensverlust in Polizei und Rechtsstaat führen kann.

Durch geeignete forensische Analysen und den Einsatz von multi-modalen Anwendungen zur Kombination von Analyseergebnissen können zusätzliche Einblicke über die Authentizität von Medien gewonnen werden. Erste konkrete Projekte (z.B. FFG KIRAS defalsif-ai, RAIDAR) haben demonstriert, dass eine Erkennung von Desinformation und Hass im Netz technologisch machbar ist, jedoch kann damit nur reaktiv die Echtheit von Informationen verifiziert bzw. falsifiziert werden. Deshalb bedarf es einer flächendeckenden Analyse von Desinformationskampagnen und Trends.

Diese Auswertungen mittels AI helfen Medienorganisationen bei zeit- und ressourcenaufwändigen Prozessen zur Erkennung von Fake News. Die Ergebnisse kommen Analysten in Politik, Strafverfolgung und Nachrichtendiensten zugute, indem sie quantitative Messwerte für Desinformationstrends und erklärbare Bewertungen der Medienforensik und der Desinformationserkennung bereitstellen. Methoden zur Analyse von Hybrid Threats ermöglichen die Erkennung und quantitative Messung von Trends, die die notwendige Grundlage für die Planung und Überwachung von Gegen-Narrativen bilden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwicklung eines Frühwarnsystems zur breitflächigen Analyse von Desinformation und Trends in online Inhalten zur Früherkennung von Desinformationskampagnen
- Teilautomatisierte Unterstützung beim Aufbau von nationalen sowie Internationalen Wissensdatenbanken über aktuelle und vergangene Trends, um wiederkehrende Trends von Desinformation oder Verschwörungstheorien zu erkennen bzw. sozialwissenschaftliche Studien zu Desinformationsmustern zu ermöglichen
- Flexible und skalierbare Architekturen, die eine einfache Integration der Anwendung ermöglicht, sodass Endbenutzer:innen neue Techniken zur Erkennung von Medienmanipulation verwenden können
- Aufbau eines effektiven und koordinierten Krisenmanagementmechanismus, sowie einer Taskforce (Früherkennung von Desinformationskampagnen,

- effiziente Bekämpfung von Hass im Netz, andere digitaler Kriminalitätsformen)
- Steigerung der Zusammenarbeit bei Cybersicherheit von allen betroffenen Ressorts der Bundesregierung, Bündelung staatsanwaltlicher Ermittlungskompetenzen zur Bekämpfung digitaler Verbrechen
 - Nationale Umsetzung des European Democracy Action Plan
 - Aufbereitung medienforensischer Instrumente - über verschiedene Modalitäten hinweg - für Behörden und Medienorganisationen, sowie enge Einbindung von Medien und Providern von sozialen Netzwerken zur Schaffung eines gesamtgesellschaftlichen Zugangs unter Einbeziehung der Zivilgesellschaft (z.B. NGOs), aktiver Austausch mit Medien und unabhängigen Faktenprüfern
 - Erweiterung zur Verfügung stehender AI basierter Verfahren zur Steigerung der Nachvollziehbarkeit getroffener Entscheidungen für Nutzer:innen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.3 Resilienz von Supply Chains gegenüber Kaskadeneffekten aus dem digitalen Raum

Kontakt: Bundesministerium für Arbeit und Wirtschaft

E-Mail: michael.stern@bmaw.gv.at

Die moderne Gesellschaft ist hochgradig abhängig vom Funktionieren digitaler Services, gerade auch im Zuge der Sicherstellung der Daseinsvorsorge der Bevölkerung und Unternehmen mit kritischen Gütern und Dienstleistungen. Die erforderliche Resilienz der Lieferketten ist zwar primär Aufgabe der privaten Unternehmen als kritische Infrastrukturbetreiber, jedoch haben die Behörden vitales Interesse an einer fairen, effizienten und möglichst friktionsfreien Verteilung der dazu notwendigen Ressourcen. Im digitalen Raum (Cyber-Space) besteht ein sehr großes Potential für vernetzte Krisen, insbesondere, wenn die Informations- und Kommunikationstechnologie (IKT) Teil der Krise ist. Dazu ist es sinnvoll, die kritischen Infrastrukturbereiche mit seinen Dienstleistungen, Gütern und den Akteuren in Zusammenhang mit der Resilienz digitaler Dienste substanziell zu betrachten.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Abbildung von Supply Chains von spezifischen Komponenten und kritischen zusammengesetzten Gütern unter Berücksichtigung digitaler Einflussfaktoren
- Simulation unterschiedlicher digitaler Angriffsvektoren auf Supply Chains und deren Prozesse spezifischer Infrastrukturbereiche
- Analyse von typischen Kaskadeneffekten zu kritischen Infrastrukturen und zu versorgungsrelevanten Unternehmen als plakative Use Cases
- Validierung und Konzeption von generellen Awareness-Trainings für Schlüsselpersonal in spezifischen kritischen Infrastrukturbereichen

- Fokuserweiterung des digitalen Raums auf Cyber-Physical Systems (CPS)
- Analyse der möglichen Auswirkungen einer digitalen Krise auf die Gesellschaft.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.4 Erhöhung der Cybersicherheit für Universitäten durch proaktiven Hackerschutz im ACONet

Kontakt Bundesministerium für Bildung, Wissenschaft und Forschung

E-Mail: DI Jörg Steiner, joerg.steiner@bmbwf.gv.at

Das ACONet und die Rechenzentren der Universitäten zählen zur kritischen Infrastruktur, die immer mehr im Fokus von Cyber-Angriffen stehen. Durch proaktive Cybersicherheits- und Cyberdefence-Maßnahmen und -Analysen (wie z.B. Log-Analysen, Angriffsuntersuchung, Beobachtung auffälliger Daten-Bewegungen) sollen Angriffe verhindert bzw. schnell erkannt und abgewehrt werden. Die Ergebnisse der Forschung sollen als Grundlage für ein zentrales Security Operation Center (SOC) dienen, welches ihre Leistungen allen ACONet Teilnehmern anbieten soll. Universitäten sind aufgrund ihrer Struktur und der hohen Anzahl an Studierenden mit besonderen Herausforderungen konfrontiert, mit denen kommerzielle Anbieter nicht zu kämpfen haben. Das SOC soll auch mit der Lehre und Forschung an Universitäten zusammenarbeiten und dementsprechende Angebote und Schnittstellen entwickeln. Das SOC soll die Resilienz der kritischen Infrastruktur der Universitäten erhöhen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie kann mit künstlicher Intelligenz die Log-Analyse weiter verbessert und automatisiert werden um den Einsatz unter den speziellen Bedingungen der Universitäten effizienter zu gestalten?
- Wie kann durch den Einsatz von Open Source Software für die Abwehr und die Analyse von Cyberangriffen mehr Unabhängigkeit von Nicht-EU-Anbietern erreicht werden?
- Wie kann durch Deep Web Intelligence, also der Analyse des Umfeldes im Clearnet, Deep Web und Darknet, die Planung von Angriffen auf Universitäten erkannt und damit vermieden werden?
- Wie kann ein SOC für alle Universitäten mit einer föderalen Datenhaltung trotzdem eine datenschutzkonforme, zentrale Analyse durchführen, insbesondere durch einen Prototyp einer GAIA-X-Installation?
- Ausarbeitung eines Katalogs mit konkreten präventiven Maßnahmen für die Universitäten in Bezug auf Cybersecurity
- Erarbeitung von Empfehlungen als Grundlage für die Entwicklung von Fort- und Weiterbildungsangeboten für die verschiedenen Rollen der Security Operations und für Studierende sowie Mitarbeiterinnen und Mitarbeiter.
- Wie können die operativen Daten für Forschung und Lehre genutzt werden?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.5 Nachverfolgung von Virtual Assets im Decentralized Finance (DeFi)-Ökosystem, Blockchains von Stablecoins und anderen Cross-Chain-Modellen

Kontakt: Bundesministerium für Inneres

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

Straftäter, aber vor allem die organisierte Kriminalität, nutzen mittlerweile verstärkt die Möglichkeiten von DeFi-Ökosystemen bzw. von anderen „Chain-to-Chain“-Transaktionsmodellen (Chain-Swapping) für deren Geldwäschehandlungen. Dadurch wird es für Strafverfolgungsbehörden zunehmend erschwert, die komplexen Transaktionswege nachzuvollziehen und infolgedessen die inkriminierten Vermögenswerte sicherzustellen.

Decentralized Finance (DeFi) steht für ein neues Finanzparadigma, das darauf abzielt, die Funktionsweise etablierte Finanzdienstleistungen grundlegend zu verändern. Anstatt Finanzprodukte über zentrale Intermediäre, wie zum Beispiel Banken oder Broker, zu organisieren und zu vertreiben, bieten DeFi-Services Dienstleistungen in Form von Smart Contracts an, bei denen es sich im Wesentlichen um ausführbare Softwareprogramme handelt, die auf Distributed-Ledger-Technologien (DLT) wie Ethereum eingesetzt werden. Obwohl es sich um eine neue Entwicklung handelt, kann ein rasantes Wachstum von DeFi-Services beobachtet werden, die zum Beispiel der Verleih virtueller Vermögenswerte, der Tausch virtueller Vermögenswerte über dezentrale Kryptoasset-Exchanges (DEXs) oder die Erschaffung programmgesteuerter strukturierter Anleihen zur Realisierung von so genannten Stablecoins. Auch Wetten auf zukünftige Preisentwicklungen in Form von Derivaten wie Optionen und Futures sind bereits ermöglichen.

Die Komplexität von DeFi-Services und die fehlende Nachvollziehbarkeit von Transaktionsflüssen stellt Regulierungs- und Strafverfolgungsbehörden vor bis dato ungelöste Herausforderungen und erfordert neue forensische Lösungsansätze. Durch die immer enger werdende Verzahnung des traditionellen Finanzsystems mit Kryptoassets stellt sich außerdem zunehmend die Frage systemischer Risiken, d.h. welche Auswirkungen ein Kollaps von Stablecoins auf das traditionelle Finanz- und Wirtschaftssystem haben könnte.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Wie können illegale Zahlungsströme, die durch dezentrale Finanzprodukte über DLT-Grenzen hinweg nachvollzogen werden (Crypto Assets sowie Stablecoins)?
- Wie können forensische Analysen umfangreicher Kriminalitätsdelikte durch daten-getriebene Methoden effizienter gestaltet werden?
- Wie können effektive Massendatenverarbeitungslösungen betreffend Blockchain-Transaktionen geschaffen werden?

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.6 Testen und Validieren moderner Systeme zur Erkennung von Cyber-Angriffen

Kontakt: Bundesministerium für Inneres

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

Die Zahl als auch Raffinesse von Cyber-Angriffen nimmt seit Jahren beständig zu. Dabei reicht es für Betreiber wesentlicher Dienste und kritischer Infrastrukturen schon lange nicht mehr aus, nur präventive Maßnahmen zu ergreifen. Das Konzept der „Presumption of Compromise“ besagt, dass jede Infrastruktur erfolgreich kompromittiert werden kann oder es bereits ist. Ein Schlüsselfaktor mit dieser Entwicklung umzugehen ist damit die frühzeitige Erkennung von Angriffen und Angriffsversuchen, z.B. das initiale Ausnutzen einer Schwachstelle, das Verankern einer Schadsoftware oder die Identifikation von Command & Control Traffic, bevor größerer Schaden entsteht.

Während einzelne Unternehmen dazu bereits Lösungen im Einsatz haben, nimmt der Staat mit der Verabschiedung des NIS Gesetzes ebenfalls wichtige Aufgaben in diesem Bereich wahr. Eine Verordnung sieht dabei den Aufbau eines IoC-basierten Frühwarnsystems vor, bei dem Sensoren Netzwerkverkehr bei Organisationen abgreifen und diesen nach Spuren erfolgreicher Angriffe, sogenannte Indicators of Compromise (IoC), untersuchen.

Obwohl Konzepte für die grundlegende Architektur bereits ausgearbeitet wurden, sind viele Fragestellungen hinsichtlich der eigentlichen technischen Detektion noch offen. Beispielsweise wurde noch nicht im Detail untersucht, welche Daten welchen Mehrwert in der Erkennung liefern und mit welcher Effektivität letztendlich ein solch IoC-basiertes System arbeiten könnte. Erst wenn diese Systeme einen nachweislichen Mehrwert für alle Beteiligten bieten, vor allem Organisationen deren Netzwerkverkehr überprüft werden soll, haben diese Lösungen eine Chance, akzeptiert und eingesetzt zu werden. Insbesondere bedeutet dies den effektiven Einsatz mit zuverlässigen Erkennungsraten bei gleichzeitig geringer Anzahl an Fehlalarmen – was zum jetzigen Zeitpunkt jedoch noch schwer abzuschätzen ist.

Ein vielversprechender Ansatz, um die Effektivität solcher Lösungen auf staatlicher Ebene abzuschätzen, ist der Aufbau von Testumgebungen, um die Erkennungsraten in unterschiedlichen Szenarien, hinsichtlich unterschiedlicher Angriffstechniken, strukturiert und systematisch zu testen. Damit könnten die zu erwartende Effektivität und für den Betrieb erforderlichen Aufwände deutlich besser abgeschätzt werden. Weiters wäre selbst für einen bereits erfolgten Produktivbetrieb parallele Testumgebungen äußerst praktikabel, um einzelne IoCs vor dem breiten Ausbringen vorab zu testen und unerwartete Nebeneffekte, wie hohe Falsch-Positivraten, auszuschließen und so das Vertrauen der Stakeholder in die Fähigkeiten eines solchen Systems zu stärken.

Ein Forschungsprojekt zu diesem Thema sollte substanzielle Beiträge leisten, um Testumgebungen aufzubauen, mit denen erkenntnisbasierte Cyber-Sicherheitslösungen, besonders staatsweite IoC-basierte Frühwarnsysteme, strukturiert getestet und validiert sowie Konfigurationen optimiert werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Ausarbeitung eines anwendbaren Konzepts für die effiziente, d.h. rasche und kostengünstige, Erstellung realistischer Testumgebungen, die gängige Infrastrukturen und deren Technologien widerspiegeln
- Erstellung einer Methode zum Messen der Leistung von Sicherheitslösungen hinsichtlich der Erkennungsgenauigkeit diverser relevanter Angriffstechniken, z.B. nach MITRE ATT&CK
- Entwicklung eines Konzepts zur Validierung und Bewertung der Effektivität neuer Indicators of Compromise
- Konzipieren eines Konzepts zur operativen Anwendung der Testmethodik, vor allem hinsichtlich des Instanzierens von Testbeds, Einspielen von Schwachstellen, Durchführung von Angriffen und der Interpretation der Erkennungsergebnisse
- Implementierung eines Demonstrators für ausgewählte Szenarien als Proof-of-Concept
- Klärung rechtlicher Fragestellungen beim Betrieb IoC-basierter Früherkennungssysteme im Spannungsfeld Schutz von Betreibern wesentlicher Dienste und DSGVO.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.7 Sichere Kommunikationsinfrastruktur für GSVP Missionen

Kontakt: Bundesministerium für europäische und internationale Angelegenheiten

E-Mail: Mag. Philipp Agathonos, philipp.agathonos@bmeia.gv.at

Um sichere Kommunikationskanäle zwischen den Hauptquartieren der GSVP Missionen, dem EAD in Brüssel und den Hauptstädten der EU MS aufzubauen, bieten sich verschiedene technische Lösungen (Virtual Private Networks, Transport Layer Security, ...) an. Zentral hierfür ist es zukunftssichere kryptographische Verfahren einzusetzen, um die Kommunikation gegenüber einer großen Klasse von Angreifern schützen zu können (Sicherheit gegenüber potentiellen leistungsstarken Quantencomputern bereitstellen, Protokolle mit Vorwärtssicherheit) sowie die Authentifikation aller Kommunikationsteilnehmer. Um trotz schlechter IT-Infrastruktur diese Eigenschaften zu erreichen, ist es nötig, dass entweder die Geräte der Missionsmitglieder selbst (Laptops, Smartphones, etc.) oder (zusätzliche) dezidierte mobile Gateways (Netzwerkadapter, mobile Access Points, ...) sichere Kommunikationsnetzwerke aufbauen und bereitstellen können. Die Umsetzung muss an die technischen Gegebenheiten vor Ort der einzelnen GSVP-Missionen angepasst

werden. Zusätzlich muss die Awareness der Missionsmitglieder gegenüber dieser neuen Infrastruktur und deren Handhabung im Allgemeinen verbessert werden.

Ein weiterer Themenkomplex ist sichere Zugriffskontrolle, um selektiv Zugriff auf sensitive Daten in Information-Management-Systemen zu erlauben. Herkömmliche State-of-the-Art-Verfahren basieren auf attributbasierten Kontrollmechanismen über einen zentralen Zugriffspunkt, der einen Single-Point-of-Failure darstellt. Durch den Einsatz neuartiger kryptographischer Verfahren (insbesondere attributbasierter Verschlüsselung und ähnlicher Verfahren) kann die Zugriffskontrolle auf mathematischer Ebene ohne einen zentralen Zugriffspunkt erfolgen und damit die Sicherheit signifikant erhöht werden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Konzeption einer sicheren Kommunikationsnetzwerk-Architektur für GSVP Missionen
- Identifikation von Anknüpfungspunkten zur Integration zukunftssicherer kryptographischer Verfahren (Quanten-sicher, Vorwärtssicherheit, etc.)
- Evaluierung des Einsatzes mobiler Access Points oder Netzwerkadapter für sichere Kommunikation bei schlechter IT-Infrastruktur
- Konzeption einer dezentralen Zugriffskontrolle für Information-Management-Systeme mittels attributbasierter Verschlüsselung (o.ä.)
- Konzeption eines Trainingsprogramms zur Steigerung der Awareness gegenüber der neuen Security-Lösungen.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.3.8 Erhöhte Cybersicherheit für Österreichs Trinkwasserversorgung und Abwasserentsorgung

Kontakt: Holding Graz – Kommunale Dienstleistungen GmbH

E-Mail: Dipl.-Ing. Alexander Hintz, alexander.hintz@holding-graz.at

Kontakt: Bundesministerium für Land- und Forstwirtschaft, Regionen und Wasserwirtschaft

E-Mail: Dipl.-Ing Mario Unterwainig, MSc, MBA, mario.unterwainig@bml.gv.at

Österreich zählt zu den wasserreichsten Ländern der Welt. Nichtsdestotrotz sind die rund 5.500 Wasserversorger und über 1.900 Kläranlagenbetreiber (mehr als 50 Einwohner) mit neuen Herausforderungen konfrontiert. Neben den Auswirkungen des Klimawandels und der damit verbundenen Wasserknappheit in einzelnen Regionen, der Wasserverschmutzung und der Notwendigkeit der Erweiterung und Modernisierung der Infrastruktur aufgrund der zunehmenden Urbanisierung gilt es letztlich auch mit einer Konsequenz der zunehmenden Digitalisierung umzugehen, nämlich der Vergrößerung der Angriffsfläche für Cyberattacken. Die sichere Implementierung von neuen IKT-Landschaften unter Einhaltung von strengeren

Regulierungen (z.B. NIS-, zukünftig NIS2.0-Verordnung) sowie die Integration von bestehender mit neuer OT ohne Einbußen in der Sicherheit müssen auf dem Weg zu smarten Wasserversorgungssystemen gemeistert werden.

Diese nutzen unterschiedliche IKT-Komponenten, um beispielsweise Fernverbindung und -wartung verschiedener Systemteile sowie Optimierungs- und Automatisierungsdienste zu ermöglichen. Auch die Welt der IoT findet nach und nach Einzug in die Systemlandschaften der Wasserwirtschaft, um den Digitalisierungsprozess nach dem Stand der Technik umsetzen zu können. Die Digitalisierung schafft jedoch neben allen Vorteilen und erweiterten Möglichkeiten auch neue Schwachstellen und Angriffsflächen, wodurch die Sicherheit solcher Systeme neuen und erst in Zukunft aufkommenden Bedrohungen ausgesetzt sein wird. In den letzten zwei Jahrzehnten wurden mehr als 20 Cyberangriffe auf Wasserversorgungen gemeldet, z.B. die Serie von Cyberangriffen auf Israels Wassersystem (2020) , der Cyberangriff in Florida (2021) und der erste gemeldete Cyberangriff im Zusammenhang mit Smarter Wasserversorgung in Europa – in Norwegen (2021) . Diese Beispiele belegen, dass auch die Wasserversorgung als kritische Infrastrukturen Cyberangriffen ausgesetzt ist und funktionierende Präventionsmaßnahmen notwendig sind. Eine Früherkennung (Erkennung eines Angriffs in einem frühen Stadium) ist besonders wichtig, um Schäden für Menschen und die Umwelt zu vermeiden.

Obwohl es weltweit mehrere Studien und Projekte zu diesen Aspekten gibt, existiert derzeit kein umfassender Überblick über den aktuellen Stand der Cyber-Sicherheitsbereitschaft der Wasserversorgungs- und Abwasserentsorgungsunternehmen in Österreich mit ableitbaren Schlussfolgerungen für größere aber auch für die große Anzahl an kleineren und mittleren Betreiber von Wasserversorgungs- und Abwasserentsorgungsanlagen.

Intelligente Wasserversorgungs- und Abwasserentsorgungssysteme gehören zu den cyber-physischen Systemen, weshalb neben der Gewährleistung der physischen Sicherheit auch jener der Cybersicherheit (IT und OT) unerlässlich ist. Aufbauend auf Best Practice aus anderen OT-lastigen Sektoren wie der industriellen Fertigung soll dieses Vorhabens Technologien und Verfahren erforschen, welche zukünftig eine automatisierte 24/7-Überwachung der Wasserversorgungssysteme durch KI-gestütztes Monitoring ermöglichen, um automatisiert potenzielle Cyberangriffe auf Wasserversorgungsanlagen erkennen und davor warnen zu können. Zielrichtung dabei sollen zukünftige praktikable und umsetzbare Lösungen nicht nur für die etwa 10 größeren der NIS-Richtlinie unterliegenden österreichischen Wasserversorger, sondern auch für die überwiegende Zahl an kleinen Verbänden, Genossenschaften und kommunalen Versorgern sein. Dazu gehört auch das rechtzeitige Warnen vor potentiellen zukünftigen Fehlern in den Systemkomponenten, was auch einen Beitrag zur Ressourcenschonung und zum Umweltschutz leisten kann.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Recherche potenzieller Cyber-Bedrohungen und Entwicklung von Reaktionsverfahren mit besonderem Schwerpunkt auf Trinkwasserversorgungs- und Abwasserentsorgungsunternehmen unter

- Berücksichtigung vorhandener Studien und bereits ausgearbeiteter Umsetzungsleitfäden
- Überblick über den Digitalisierungsgrad, Schwachstellen häufig verwendeter Komponenten und Dienste sowie Sicherheitspraktiken und -verfahren in österreichischen Wasserversorgungs- und Abwasserentsorgungsunternehmen (Risiko- und Resilienzschätzung)
 - Überblick über Tools und Methoden zur Etablierung eines effektiven und pragmatischen Risikomanagements der IKT-Infrastruktur in der Wasserwirtschaft, unter Berücksichtigung der gesetzlichen Anforderungen (NISV und NISV2.0)
 - Untersuchung moderner Schnittstellen zwischen den Wasserversorgern bzw. Abwasserentsorgern und Demonstration einer Integration und Visualisierung dieser Daten in ein überregionales Lagebild inkl. Informationsaustausch zu Cyber-Bedrohungen
 - Erforschung und Entwicklung von KI-basierten Analyse- und Informationsextraktionsverfahren für multimodale Sensorsysteme zur 24/7-Überwachung von Wasserversorgungsanlagen unter besonderer Berücksichtigung von Mechanismen zur Erkennung und Lokalisierung von Cyberangriffen sowie Leckagen
 - Effiziente, die Privatsphäre wahrende und benutzerorientierte Datenverwaltung und -verarbeitung, einschließlich Edge-basierter Verarbeitung, um die Infrastrukturkosten, den Ressourcenverbrauch und die Wartungskomplexität intelligenter Wassersysteme zu minimieren
 - Ethische und datenschutzrechtliche Fragestellungen hinsichtlich KI Einsatz und Wasserverteilung
 - Vergleich von Richtlinien für ein Cyber-Sicherheitsprogramm und Aufbereitung von spezifischen Schulungsinhalten für Cyber-Awarenessstrainings in der Wasserwirtschaft.

Ausgeschriebene Instrumente:

- Kooperative Projekte (Industrielle Forschung oder Experimentelle Entwicklung)

3.4 Cybersicherheit. Ausschreibungsschwerpunkte für F&E-Dienstleistungen

Themenschwerpunkt „Cybersicherheit“ F&E-Dienstleistungen (als Vorbereitung und Testlauf für ein österreichisches digitales Sicherheitsforschungsförderprogramm).

3.4.1 Anforderungen von KMU zur Cybersicherheit

Kontakt: Bundesministerium für Inneres

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

Kleine und mittlere Unternehmen (KMU) sind ein wichtiger Bestandteil der österreichischen Wirtschaft und spielen national wie international eine wesentliche Rolle in Lieferketten. KMU haben jedoch insbesondere in Bezug auf das Thema Cybersicherheit andere Bedürfnisse als große Unternehmen und Konzerne. So haben KMU oft Schwierigkeiten, sich an neue Geschäftspraktiken in einer stärker vernetzten Welt anzupassen und sich in der digitalen Umgebung zurechtzufinden, in der Mitarbeiter im Home Office arbeiten und Prozesse zunehmend online abgewickelt werden. KMU stehen somit vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z.B. geringes Cyber-Bewusstsein, fehlende IT-Sicherheit, hohe Kosten für Cybersicherheitslösungen und ein erhöhtes Maß an Bedrohungen, wie z.B. Ransomware, für die KMU Unterstützung benötigen. Zusätzlich werden KMU zunehmend zur Zielscheibe von Cyber-Angriffen auf die Lieferkette, da sie weniger Maßnahmen zur Cybersicherheit und zum Angriffsmanagement ergreifen und über keine speziellen Sicherheitsressourcen verfügen. Solche Angriffe auf die Lieferkette wirken sich in weiterer Folge nicht nur isoliert auf KMU und ihren Betrieb aus, sondern können auch einen Kaskadeneffekt für größere Angriffe auf weitere Unternehmen wie z.B. Supply Chain Partner haben. Im Zuge der NIS2-Richtlinie der EU sind KMU unter diesem Supply Chain Aspekt in Zukunft auch verstärkt von Regulativen betroffen, die eine erhöhte Cybersicherheit in den Unternehmen fordern, was einen großen Einfluss auf die Ressourcen und Organisationstrukturen in KMU haben wird.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Erhebung der Bedürfnisse von KMU zu Cybersicherheit, Cyber-Resilienz und Cyber-Hygiene
- Erhebung der vorhandenen Fähigkeiten von KMU, branchenspezifisch
- Erhebung nationaler und internationaler Standards und Industrie-Best Practices und deren Eignung für KMU
- Erstellung einer Best Practice Guideline für KMU zu Cybersicherheit und Supply Chain Security unter Berücksichtigung der NIS2-Richtlinie
- Handlungsempfehlungen, wie aus staatlicher Sicht die KMU unterstützt werden können: einerseits bei der Cybersicherheit, andererseits auch bei den Herausforderungen in Ihren Supply Chains
- Bezug zu NIS2, Due Diligence Act, Cyber Resilience Act, etc. - Welche Anforderungen werden aktuell und zukünftig an KMU gestellt?

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.2 Digitalisierungspotential von Services in der öffentlichen Sicherheit

Kontakt: Bundesministerium für Inneres

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

Die technischen Möglichkeiten der Digitalisierung bieten für den Bereich der öffentlichen Sicherheit sowohl ungeahnte Möglichkeiten als auch ebensolche

Herausforderungen und Risiken. Angesichts der in naher bis mittlerer Zukunft steigenden Anforderungen und gleichzeitig immer weniger werdenden verfügbaren Ressourcen an Personal bzw. Experten, besteht die Notwendigkeit, Digitalisierungspotentiale und Synergien im VORHINEN zu bewerten bzw. Projekte zu deren Umsetzung zu priorisieren – auch im Sinne einer Wirkungsorientierung der dafür verwendeten Mittel.

Hierzu ist es notwendig, ein wissenschaftlich fundiertes Vorgehensmodell zur Identifikation und Bewertung von Digitalisierungspotenzialen aber auch Risiken und Erfolgskriterien unter den speziellen, über Industriestandards liegenden Anforderungen und Rahmenbedingungen eines Sicherheitsresorts (wie beispielsweise Hochverfügbarkeit, Sicherheit, Redundanz, etc.) zu entwickeln. Da es sich um durchweg komplexe Systeme handelt, erfordert das zu findende Vorgehensmodell eine hohe Expertise im Bereich der Methodik, wie auch den organisatorischen Überblick, der aus der langjährigen Kooperation gegeben ist. Die Praxistauglichkeit soll anhand eines Beispiels gezeigt werden können.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Effektive und Effiziente Verfahren zur Identifikation der wesentlichen Kernprozesse – Arbeitsflussanalysen und Erkennung von Bottlenecks
- Modellierung und Analyse der wesentlichen Akteure und Wechselwirkungen des BMI und seinen Partnern – Stakeholdermanagement
- Identifikation und Bewertung von Synergiepotentialen und Digitalisierungsmaßnahmen
- Identifikation und Bewertung von Risiken und Erfolgskriterien von Digitalisierungsmaßnahmen – Risikomanagement.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.3 Cybermobbing als Herausforderung für Pädagoginnen und Pädagogen

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung

E-Mail: barbara.huemer@bmbwf.gv.at

Es ist Ziel des österreichischen Bildungssystems, das volle Potenzial digitaler Technologien für Lernen und Lehren auszuschöpfen und digitale Fähigkeiten für alle zu entwickeln. Die Schülerinnen und Schüler sollten befähigt werden, Informationstechnologien praktisch anwenden zu können und sich kritisch mit digitalen Medien auseinanderzusetzen. Sie sollen bestmöglich auf ihren weiteren Lebensweg im digitalen Zeitalter vorbereitet werden. Doch die fortschreitende Digitalisierung birgt neue Herausforderungen für das soziale Zusammenleben, denen Pädagoginnen und Pädagogen gegenüberstehen. Zu den besonders problematischen Entwicklungen zählt die Entstehung und Zunahme von Cybermobbing, das inzwischen vielfältige Dimensionen angenommen hat.

Pädagoginnen und Pädagogen haben zum einen die Aufgabe einen geschützten Rahmen zu schaffen, in dem sich Kinder und Jugendliche entwickeln und entfalten können, und zum anderen auch die Verantwortung auf ihre eigene physische und psychische Gesundheit zu achten. Cybermobbing stellt diesbezüglich jedoch eine große Gefahr dar. Es kann sich sowohl gegen Schülerinnen und Schüler, als auch gegen Lehrerinnen und Lehrer richten, der Täter oder die Täterin ist meist anonym und das Mobbing endet nicht nach der Schule, sondern kann in digitalen Medien rund um die Uhr stattfinden. Die Auswirkungen für die Betroffenen sind massiv und können psychischen und physischen Folgen wie Schlafstörungen, Depressionen oder Angststörungen hervorrufen. Deshalb ist es zentral Pädagoginnen und Pädagogen für das Thema Cybermobbing zu sensibilisieren und sie umfangreich und bedarfsgerecht im Umgang mit Cybermobbing fortzubilden.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Welchen Bedarf an Fortbildungen sehen Pädagoginnen und Pädagogen hinsichtlich Cybermobbing? Wie entwickelt sich das Problem Cybermobbing aus der Sicht der Pädagoginnen und Pädagogen und wie akut nehmen sie es wahr?
- Wie können Pädagoginnen und Pädagogen im Rahmen von Fortbildungen bestmögliche Instrumente und Methoden im Bereich Cybermobbing vermittelt werden?
- Welche präventiven Maßnahmen werden in Bezug auf Cybermobbing in der Schule gesetzt?
- Erarbeitung von Empfehlungen als Grundlage für die Entwicklung von Fort- und Weiterbildungsangeboten von Pädagoginnen und Pädagogen.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

3.4.4 Cybersecurity-Literacy in der Wissensvermittlung der Sekundarstufe in Österreich

Kontakt: Bundesministerium für Bildung, Wissenschaft und Forschung

E-Mail: AL Mag. Eduard Staudecker, MBA, Eduard.Staudecker@bmbwf.gv.at

Die Digitalisierung ist wesentliche Voraussetzung für die Entwicklung einer modernen Gesellschaft. Zur Vorbereitung und Bewusstseinsbildung im Umgang mit digitalen Werkzeugen und zum Verhalten im digitalen Raum muss Cybersicherheit in der schulischen Bildung berücksichtigt werden, um ein resilientes Ökosystem für Cybersecurity bilden zu können. In Ergänzung des „Themenbereichs Bildung“ der Österreichische Strategie für Cybersicherheit 2021 soll eine Studie die Rahmenbedingungen für die Integration von Cybersecurity-Aspekten in den Schulunterricht strukturiert analysieren und mögliche pädagogische Ansätze zur Wissensvermittlung erarbeiten. Schwerpunkt der Ausarbeitung sollen Themenbereiche und Wissensgebiete sein, die im Besonderen für 14- bis 19-Jährige Schülerinnen und Schüler im österreichischen Bildungssystem (d.h. Berufsschulen, AHS, BMHS) anschlussfähig sind und deren Nutzungs- und Konsumverhalten in der

digitalen Welt widerspiegelt. Zudem sollen Inhalte mit Arbeitsmarktbezug, die die Beschäftigungsfähigkeit der genannten Zielgruppe erhöhen ein zentraler Aspekt der Studie sein. Lehrkräfte sollen von den pädagogischen Instrumenten, Sachanalysen und Unterrichtsmaterialien profitieren. Zielsetzung ist somit eine wissenschaftlich fundierte Aufbereitung des Themas zum Nutzen des BMBWF, um in gezielten Bereichen des Schulsystems für dieses Thema zu sensibilisieren und berufs- und arbeitsmarktbezogene Ergänzungen zu den aktuell laufenden Überlegungen zur Lehrplanentwicklung zu schaffen.

Folgender Forschungsbedarf ergibt sich in diesem Zusammenhang:

- Entwicklung eines bildungspolitischen, gesellschaftlichen und sozio-technischen Ansatzes zur Vermittlung des Themenbereichs Cybersecurity für 14- bis 19-Jährige mit besonderem Bezug zum beruflichen Kompetenzerwerb und zum Arbeitsmarkt
- Definition und wissenschaftliche Darstellung bedarfsorientierter spezifischer Cybersecurity-Themenbereiche und Wissensgebiete (mit Bezug zur Zielgruppen, dem Arbeitsmarkt und konkreten Berufen) auch im Hinblick auf Unterrichtsmaterialien und Schulbücher
- Ausarbeitung wissenschaftlicher Grundlagen möglicher Wissensvermittlungsstrategien und didaktischer Konzepte (auch über E-Learning) samt konkreten Empfehlungen für die Unterrichtsgestaltung
- Beantwortung der Frage, wie Jugendliche auf die Herausforderungen der Cybersecurity im digitalen Raum vorbereitet werden können
- Wie können bewussteinbildende Maßnahmen gestaltet werden, wie kann am Thema Haltung und Einstellung im Unterricht gearbeitet werden?
- Rückmeldungen zur Anschlussfähigkeit des Themas in bestehenden Unterrichtsfächern (z.B. digitale Grundbildung, Informatik) und Ausbildungsbereichen (z.B. HTL Informatik, digBiz HAK)
- Berücksichtigung von genderrelevante, sozioökonomische und kulturelle Bedarfe bei den Ausarbeitungen
- Schaffung eines Überblicks über die wesentlichen Akteure an der Schnittstelle Cybersecurity und Schule (mit Fokus auf die obere Sekundarstufe) in Österreich
- Erforschung der kontinuierlichen Weiterentwicklung der Begriffsdomänen Digitalisierung und Cybersicherheit.

Ausgeschriebene Instrumente:

- F&E-Dienstleistung

4 INSTRUMENTE UND ANFORDERUNGEN

4.1 Kooperatives F&E-Projekt

Beachten Sie den [Instrumentenleitfaden für Kooperative F&E Projekte \(v4.2\)](#).

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:

- 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 Subauftragnehmer des Konsortiums oder Konsortialteilnehmer.

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

Um ein ausgewogenes Kooperationsverhältnis zu gewährleisten muss:

- die Kostensumme aller F&E-Partner unter 70 % liegen
- die Kostensumme aller Wirtschaftspartner unter 70 % liegen.

Der Einbindung von Bedarfsträgern und GSK-Vertretern kommt eine besondere Rolle zu.

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

Die Ausschreibung wendet sich inhaltlich auch an Organisationen des Bundes. Mit dem Bund idente Bedarfsträger können zwar nicht als Antragsteller für Förderungen auftreten, sind jedoch ermutigt, sich im Rahmen von Konsortialbindungen an der Ausschreibung zu beteiligen. Mögliche Projektbeiträge von Bedarfsträgern in deren Funktion als Konsortialpartner können Barmittel, Personalstunden, Sachmittel, Beistellung von Infrastruktur, etc. sein.

Im Falle eines Konsortiums ist eine Einbindung und Förderung (bis maximal 10 % der im eCall angesuchten Gesamtfördersumme des Projekts) ausländischer Partner für diese Ausschreibung im Instrument Kooperatives F&E-Projekt grundsätzlich möglich.

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.

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 ein Beratungsgespräch bei einer öffentlichen Wirtschaftsförderungsagentur im Projektverlauf ein.

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 [Instrumentenleitfaden für Kooperative F&E Projekte \(v4.2\)](#).

4.2 F&E-Dienstleistung

Beachten Sie den [Leitfaden für Forschungs- und Entwicklungsdienstleistungen \(v4.3\)](#).

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 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 Ziele des Sicherheitsforschungsprogramms KIRAS weiterentwickelt und für Teilbereiche näher definiert wird.

4.2.2 Bietergemeinschaften

Das Instrument richtet sich an Partner aus den Bereichen Wirtschaft und Wissenschaft sowie an Bedarfsträger. Finanziert werden können nur Antragsteller (Konsortialführer) mit Standort in Österreich. Für ein Konsortium kann nur ein Projektpartner (Unternehmen, Forschungseinrichtung, Bedarfsträger) mit Standort in Österreich gegenüber der FFG als Einzelbieter bzw. BIEGE- Leiter auftreten.

Die Ausschreibung wendet sich inhaltlich auch an Organisationen des Bundes. Mit dem Bund idente Bedarfsträger können zwar nicht als Finanzierungsantragsteller auftreten, sind jedoch ermutigt, sich im Rahmen von Konsortialbildungen an der Ausschreibung zu beteiligen. Mögliche Projektbeiträge von Bedarfsträgern in deren Funktion als Konsortialpartner können Barmittel, Personalstunden, Sachmittel, Beistellung von Infrastruktur, etc. sein.

Im Falle eines Konsortiums ist eine Einbindung ausländischer Partner grundsätzlich möglich, allerdings dürfen diesen nicht mehr als 10 % der Finanzierung zukommen.

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.

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 Firmenbuches (Handelsregister) 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 Projekthinhalte
- **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) nach wie vor über die eCall Upload-Funktion hochgeladen werden
- Sämtliche relevante Dokumente für die Ausschreibung finden Sie auf der [Webseite der Ausschreibung](#).

Förderkonditionen, Ablauf der Einreichung und Förderkriterien sind im jeweiligen Instrumenten- bzw. Ausschreibungsleitfaden beschrieben. Die nachfolgende Übersicht zeigt für die jeweiligen Instrumente die relevanten Dokumente.

Es ist der FFG ein Anliegen, die Einreichung eines F&E-Vorhabens für alle Förderwerber:innen einfach, unkompliziert und zeitgemäß zu gestalten. Mit der Neugestaltung des elektronischen Einreichportals eCall ist nunmehr die vollständige online Einreichung Ihres Antrages im eCall System möglich. Eine einfache, einmalige und reduzierte Eingabe von Informationen wird damit erzielt. Das Anlegen des Projekts und das Einladen der Partner sowie die Eingabe der Kosten und Finanzierung im eCall bleiben wie bisher bestehen und sind davon unberührt.

Das ist neu und vereinfacht: Bis dato erfolgte die Einreichung der gesamten Projektbeschreibung mit Hilfe einer Word-Vorlage. Anstelle einer Word-Vorlage setzt sich die Projektbeschreibung nun aus den folgenden online Funktionen zusammen:

- Online-Inhaltliche Beschreibung (eCall)
- Online-Konsortium (eCall)
- Online-Arbeitsplan (eCall)
- Online-Kosten und Finanzierung (eCall)

Mit der online Eingabe können nun einzelne Kapitel von der Konsortialführung an Partner delegiert werden. Alle Partner haben in der online Eingabe Lese- und Kommentier-Rechte. Ein integriertes Kommentier- und Versionsmanagement unterstützt bei der Zusammenarbeit im Antragstellungsprozess.

Im neuen online Antrag gibt es eine Zeichenbeschränkung bei der Erstellung, sollte diese überschritten werden, ist der Abschluss des Einreichprozesses nicht garantiert.

Weitere Hinweise finden Sie im [Tutorial](#) und unter den [FAQs](#).

Als Teil des elektronischen Antrags sind die Projektbeschreibung (inhaltliches Förderungsansuchen) sowie etwaige Anhänge über die eCall Upload-Funktion anzuschließen.

Für Einreichungen im gewählten Instrument (siehe Ausschreibungsübersicht) sind die jeweils spezifischen Vorlagen zu verwenden.

Förderkonditionen, Ablauf der Einreichung und Förderkriterien sind im jeweiligen Instrumentenleitfaden beschrieben. Die nachfolgende Übersicht zeigt für die jeweiligen Instrumente die relevanten Dokumente.

Tabelle 3: Ausschreibungsdokumente

Förderungs- /Finanzierungsinstrument bzw. sonstige Information	Verfügbare Ausschreibungsdokumente
Kooperative F&E-Projekte	<ul style="list-style-type: none"> – Instrumentenleitfaden Kooperative F&E Projekte (v4.2) – Projektbeschreibung und Kosten per eCall 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	<ul style="list-style-type: none"> – Leitfaden für Forschungs- und Entwicklungsdienstleistungen (v4.3) – Projektbeschreibung und Kosten per eCall 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
Allgemeine Regelungen zu Kosten	<ul style="list-style-type: none"> – Kostenleitfaden (v2.2) (Kostenanerkennung in FFG-Projekten)

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 RECHTSGRUNDLAGEN

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

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

Informationen und Ausfüllhilfen:

- [Kostenleitfaden](#) (Version 2.2)
- [eCall Tutorial](#)

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 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 (siehe auch die [re3data Webseite](#)).

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 [hier](#).

8 ANHANG: CHECKLISTE FÜR DIE ANTRAGSEINREICHUNG

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

Tabelle 4: Formalprüfungscheckliste

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	(Angaben lt. Instrumenten-/Ausschreibungsleitfaden)	Nein	Ablehnung aus formalen Gründen