Fraunhofer

Für eine substanzielle Stärkung der »Forschung für die zivile Sicherheit«

Positionspapier der Fraunhofer-Gesellschaft

Inhalt

Foto: iStock

Wir forschen für die Sicherheit von Mensch, Gesellschaft und Staat – für ein Leben in Freiheit. Verteidigung und Sicherheit gewinnen in Zeiten gesellschaftlicher und politischer Umbrüche immer mehr an Bedeutung. Wir entwickeln Technologien, Produkte und Dienstleistungen, um mögliche Gefahren frühzeitig zu erkennen, ihnen entgegenzutreten, Folgeschäden zu minimieren und dadurch insgesamt Risiken zu reduzieren.

Positionspapier der Fraunhofer-Gesellschaft

Zusammenfassung

Zu Beginn des neuen Jahrtausends sorgte eine Reihe von einschneidenden Terroranschlägen für die Erkenntnis, dass die zunehmende Dichte und Komplexität von Bedrohungen eine übergreifende, koordinierte und abgestimmte Vorgehensweise erfordert, um den facettenreichen Aspekten und Abhängigkeiten der involvierten Sektoren im Kontext einer resilienten Gesellschaft gerecht zu werden. Hätte man damals nicht bereits die nationale (und europäische) Sicherheitsforschung als querschnittliche Disziplin mit besonderen Rahmenbedingungen gestartet, man müsste es in Anbetracht der heutigen Situation jetzt tun. Die Natur und das Tempo der unsere Gesellschaft bedrohenden Ereignisse steigert sich nicht zuletzt im Kontext des Klimawandels und der Zeitenwende immer stärker.

Die Fraunhofer-Gesellschaft formuliert mit diesem Positionspapier den entsprechenden Bedarf einer substantiellen Stärkung der Sicherheitsforschung durch eine gezielte Erweiterung des ressortübergreifenden Zuständigkeitsbereichs, gibt weitere Impulse zur Steigerung der Operationalisierungs- und Implementierungsrate der Ergebnisse und bietet umfangreiche zukunftsrelevante Themenvorschläge zur Umsetzung der **»Forschung für die zivile Sicherheit«** der Bundesregierung im kommenden Programm 2024+.

Das Konzept der Resilienz als zentrales Element der kommenden »Zukunftsstrategie Forschung und Innovation«

»Wir müssen unsere Widerstandsfähigkeit gegen ein breites Krisenspektrum stärken; Resilienz gegenüber Katastrophen stärkt dabei auch unsere Resilienz gegenüber militärischen und hybriden Bedrohungen.«

Nancy Faeser,
Bundesministerin des Innern und für Heimat
Vorwort »Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen«

Die Sicherheit von Gesellschaften, Menschen, Institutionen, Gütern und Infrastrukturen ist eine Kernaufgabe demokratisch verfasster Institutionen. In Konsequenz der Terroranschläge in New York 2001, Madrid 2004 und London 2005 erkannte man die Notwendigkeit, dass die traditionell sektorspezifische Behandlung des Themas Sicherheit nicht mehr ausreichen würde, um das gesamte Spektrum der Herausforderungen zu bewältigen. Daher war ein koordinierter und ganzheitlicher Ansatz zur Entwicklung von Sicherheitsfähigkeiten notwendig – die Schaffung der neuen Querschnittsdisziplin der zivilen Sicherheitsforschung.

Nicht zuletzt seit dem operativen Start der Sicherheitsforschung in Deutschland und Europa im Jahr 2007 ist es breiter Konsens, dass es unmöglich ist, unsere Bevölkerung oder die kritischen Knotenpunkte unserer Infrastrukturen vollständig und zu jeder Zeit vor der Vielzahl der Bedrohungen zu schützen, mit denen wir konfrontiert sind. Daher hat sich im Bereich der Sicherheitsforschung seit Anbeginn das Konzept der Resilienz als vernünftiger und realistischer Ansatz und somit als Leitprinzip etabliert. Statt des (hoffnungslosen) Versuchs des umfänglichen Verhinderns etwa eines Terroranschlages oder eines Extremwetterereignisses zielt dieses Konzept darauf ab, dass unsere Gesellschaften und Infrastrukturen in der Lage sind, flexibel zu reagieren, Störungen zu absorbieren, sich von ihnen zu erholen und nach einem schockierenden Ereignis im Wesentlichen dieselbe Funktion, Struktur und Identität beizubehalten und weitere Kettenreaktionen zu vermeiden. Als essentielle Eigenschaft gilt hier auch darüber hinaus die Fähigkeit, aus solchen Ereignissen zu lernen und sich anzupassen.

Die zuletzt veröffentlichte »Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen« – kurz »Resilienzstrategie« – der Bundesregierung zur Umsetzung des »Sendai-Rahmenwerks für Katastrophenvorsorge«[1] belegt eindrucksvoll, dass ein ganzheitlicher Ansatz beim Thema Resilienz und dessen Bedeutung als essentielles Element für die erfolgreiche Weiterentwicklung von Gesellschaft, Staat und Wirtschaft und damit für die Sicherheit in Deutschland im Angesicht von Katastrophen anerkannt und verstanden sowie entsprechend ressortübergreifend in einer nationalen Strategie verankert wird. Angelehnt an das Sendai-Rahmenwerk formuliert die Resilienzstrategie zur Erreichung der angestrebten strategischen Ziele »Integration«, »Kooperation« und »Koordination« fünf Handlungsfelder:

1. Das Katastrophenrisiko verstehen
2. Die Institutionen stärken, um das Katastrophenrisiko zu steuern
3. In die Katastrophenvorsorge investieren, um die Resilienz zu stärken
4. Die Vorbereitung auf den Katastrophenfall verbessern und einen besseren Wiederaufbau ermöglichen
5. Internationale Zusammenarbeit.

Die Fraunhofer-Gesellschaft begrüßt und unterstützt die dort formulierten Ziele und Aufgaben im vollen Umfang. Diese unterstreichen insbesondere die zunehmende Bedeutung des Aspektes der zivilen Sicherheit in sektorübergreifenden Fragestellungen im Kontext einer resilienten Gesellschaft.

Die Fraunhofer-Gesellschaft zählt zu den global führenden und hervorragend vernetzten Institutionen für Lösungen der angewandten Forschung und Entwicklung im Bereich technischer, soziotechnischer sowie zunehmend auch sozioökonomischer Systeme in den jeweiligen Sektoren wie z. B. Gesundheit, Energie, Mobilität oder auch Weltraum. In dieser Rolle sieht sich Fraunhofer somit in den entsprechenden sektorübergreifenden Fragestellungen der Resilienzstrategie in der idealen Position, um in allen fünf Handlungsfeldern fundamentale Beiträge zu leisten. Insbesondere auch die Kenntnisse und Vernetzungen im Bereich der (nationalen) Verteidigung können dabei eingebracht werden und bedeutend zu einer zur Stärkung der Resilienz notwendigen Verbesserung der Kooperation und Abstimmung der jeweiligen Ressorts beitragen.

Mit anhaltender Konsequenz warnen Akteure im Bereich der zivilen Sicherheit seit Jahren vor einer zunehmenden Komplexität der Gefahren- und Bedrohungslage vor dem Hintergrund gesellschaftlicher, technologischer, geopolitischer und nicht zuletzt klimarelevanter Entwicklungen und deren steigender Auswirkungen auf die zivile Sicherheit (Pandemie, Extremwetterereignisse, Migration, Terror, Aufrechterhaltung KRITIS, Freiwilligeneinbindung/-verfügbarkeit, Zivilschutz usw.). Die letzten Jahre haben mehr als deutlich gemacht, dass diese Aussagen keineswegs übertrieben waren oder sind, aber erst die Auswirkungen der kürzlichen und aktuell anhaltenden Krisen haben die erhöhten Verwundbarkeiten durch parallele Ereignisse und die komplizierten Wechselwirkungen und Abhängigkeiten technischer, soziotechnischer und sozioökonomischer Systeme auch in der Breite der Bevölkerung schmerzhaft bewusst werden lassen.

Vergleicht man die bereits erfolgte wichtige und richtige Erhöhung des Haushaltes der nationalen Verteidigung im Kontext der Krisen der letzten Zeit, so muss eine der Resilienzstrategie entsprechende Erhöhung des Etats der zivilen Sicherheit inklusive des nationalen Sicherheitsforschungsprogramms die logische Folge sein. Nur so können die gesetzten Ziele entlang der fünf Handlungsfelder der Resilienzstrategie mit neuen zivilen Lösungen und Initiativen unterstützt und die zivile Führungsrolle im Inland in ressortübergreifenden Fragen des Bevölkerungs- und Zivilschutzes erfüllt werden. Die zuletzt angekündigten Kürzungen des Haushalts des Bundesministeriums des Inneren in Milliardenhöhe lässt zumindest grundsätzlich für den Bereich der zivilen Sicherheit Gegenteiliges befürchten. Im Herbst erscheint die für die Forschungs- und Entwicklungsbereiche aller Sektoren entscheidende »Zukunftsstrategie Forschung und Innovation[2]« der Bundesregierung, die die Innovationskraft Deutschlands und die technologische Souveränität Europas sichern soll. Die bisher dort aus dem Koalitionsvertrag übertragenen Zukunftsfelder für Forschung und Innovation ließen oberflächlich zunächst auf eine eher untergeordnete Rolle des Aspekts der Sicherheit unter dem Punkt »Gesellschaftliche Resilienz, Diversität und Zusammenhalt stärken« schließen. In der nun veröffentlichten Resilienzstrategie der Bundesregierung hingegen ist die Anpassung und Vorbereitung auf zukünftige Katastrophen das zentrale Element.

Die in der Resilienzstrategie implizit formulierte zunehmende Bedeutung des Aspekts der Sicherheit im Kontext einer gesamtstaatlichen Resilienz lässt eine Führungsrolle der zivilen Sicherheit auch bei Teilfragen aus anderen Sektoren ableiten. So etwa bei der Untersuchung der Änderung der Interdependenzen im Zusammenhang mit der angestrebten Energiewende, die zunächst zur Reduktion bestehender, aber zeitgleich zur Schaffung neuer Verwundbarkeiten und Abhängigkeiten führt – von Aspekten hinsichtlich Wandlern für erneuerbare Energien und Verfügbarkeit von entsprechenden Materialien

1 »Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen«

2 »Zukunftsstrategie Forschung und Innovation« der Bundesregierung

bis zu den offensichtlichen Faktoren der stärkeren Vernetzung einer erhöhten Anzahl dezentraler Energielieferanten und weiterer Energiesystembeteiligter. Auch zu gesellschaftlichen Aspekten lassen sich sicherheitsrelevante Fragestellungen identifizieren, wie beispielsweise, ob man die zu erwartenden klimawandelbedingten Migrationswellen neben der Abfederung des gesamtgesellschaftlichen demografischen Wandels nicht auch zur Mitigation der mangelnden Verfügbarkeit von Freiwilligen im Katastrophenschutz nutzen kann. Vergleichbar lassen sich weitere ressortübergreifende Forschungsfragen vor dem Hintergrund einer ganzheitlichen / systemischen Resilienz der Führungsrolle der zivilen Sicherheit unterordnen, wie z. B. aus dem Bereich der Cyber- und IT-Sicherheit, oder wie zuletzt durch die Pandemie und Extremwetterereignisse belegt, in Fragen des Gesundheitssektors oder der ländlichen bzw. urbanen Entwicklung.

Zudem ist nicht zuletzt aufgrund der hohen Belastung auch aus haushälterischer Sicht eine Doppelung von Forschungsaktivitäten der unterschiedlichen weiteren Ressorts und Institutionen zur Beantwortung der kommenden »Zukunftsstrategie für Forschung und Innovation« auf Bundesebene zu vermeiden.

So bleibt zu hoffen, dass sich das Konzept der Resilienz, den Krisen der letzten Jahre folgend, gebührend umfangreich in der »Zukunftsstrategie« wiederfinden wird und somit der nationalen Sicherheitsforschung im ressortweiten Beitrag zu deren Umsetzung eine prioritäre Rolle zuteilwird. Denn weiterhin ist ein koordinierter und ganzheitlicher Ansatz zur Verbesserung und Entwicklung von Sicherheitsfähigkeiten die beste Option zur nachhaltigen Stärkung der Resilienz von Gesellschaft und Staat und somit auch zum Schutz der Bürgerinnen und Bürger.

Foto: iStock

Klimawandel, Zeitenwende, Energiewende – um nur einige große Faktoren der Zeit zu nennen. Hieraus ergeben sich zahlreiche Herausforderungen, die es zum Schutz der Bürgerinnen und Bürger und zur Förderung einer resilienten Gesellschaft zu beantworten gilt.

Positionspapier der Fraunhofer-Gesellschaft

Bisherige Erkenntnisse aus 15 Jahren **»Forschung für die zivile Sicherheit«**

Die bisher bereits erfolgten Umsetzungen des nationalen Sicherheitsforschungsprogramms seit 2007 haben umfangreiche Ergebnisse, aber auch zahlreiche »lessons learned« produziert. Im letzten Programm der »Forschung für die zivile Sicherheit 2018 - 2023« haben sich die daraus resultierenden Optimierungsansätze als zielführende Weiterentwicklung des immer noch vergleichsweise jungen Forschungsfelds der zivilen Sicherheit erwiesen. Die Identifikation der richtigen Stellgrößen in diesem interdisziplinären und von einer Vielzahl von Interessenträgern geprägten Forschungsfeld vor dem Hintergrund einer sich verändernden und immer komplexeren Gefahrenlage stellte und stellt alle Beteiligten jedoch weiterhin vor große Herausforderungen. So bildet etwa die »Natur« der unmittelbaren Nutzer-, Käufer- oder auch Anwendungsseite der Lösungen aus diesem Bereich – primär öffentliche Behörden und Organisationen mit Sicherheitsaufgaben (BOS) – einen Markt, sofern man ihn so nennen kann, der nicht den üblichen Gesetzen eines freien Markts folgt und somit schwierig zu »lesen« ist. Die »Abnehmerseite« dieses »Markts« ist eine sehr heterogene Gruppe (z. B. operativ, strategisch, taktisch), die vielen verschiedenen Disziplinen angehört (z. B. Katastrophenschutz, polizeiliche Gefahrenabwehr oder Cyber), auf unterschiedlichen Ebenen (Bund, Länder, Landkreise, Kommunen) und in verschiedene Phasen des Resilienzzyklus von Krisen- und Sicherheitsereignissen (Vorbereiten, Vorbeugen, Schützen, Reagieren, Regenerieren) eingebunden ist. Das Resultat ist ein extrem zerklüfteter, kleinteiliger und unübersichtlicher Markt im interdisziplinären Feld der zivilen Sicherheit und daraus resultierend eine mangelnde Übersicht darüber, was bereits aktuell an Lösungen verfügbar ist. Mangelnder Innovationsdruck in der öffentlichen Hand und daraus folgend eine Budgetierung, die eher an Beschaffung als an der Planung und Entwicklung von Innovationen orientiert ist, führen zusätzlich dazu, dass sich die strategische, gemeinsame und fähigkeitsgetriebene Entwicklung von später erfolgreich etablierten innovativen Lösungen als sehr vielschichtig und schwierig erweist. Letztendlich führt dies bisher häufig noch zu einer schwerpunktmäßig anbieter- und technologiegetriebenen Umsetzung von Forschung und Entwicklung, obwohl genügend Raum zur Bedarfsformulierung und Priorisierung geschaffen wird, sobald verschiedene Konsultationen mit einer Vielzahl von Interessengruppen stattfinden. Dennoch basiert die Auswahl der identifizierten Fragestellungen für die Ausschreibung weiterer Forschungsprojekte oft nicht auf unabhängig analysierten operativen Bedürfnissen. Eine langfristig angelegte, auf existierenden und antizipierten Bedarfen aufsetzende Gestaltung des Forschungs- und Realisierungsportfolios, idealerweise über Behördengrenzen hinweg, wird daher zunehmend wichtiger, auch um mit vorhandenen Budgets effizient arbeiten zu können.

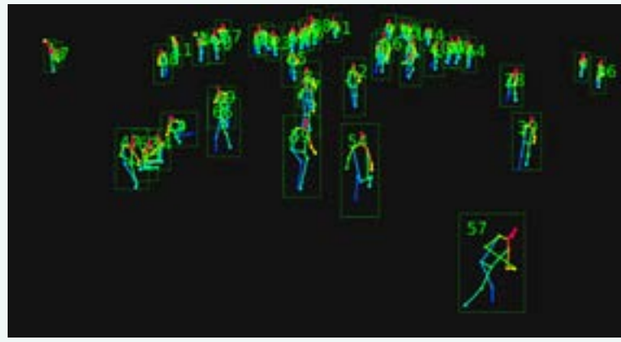
Nichtsdestotrotz sind die Effekte der bisher erfolgten Schritte zur Anpassung und Optimierung im Rahmenprogram »Forschung für die zivile Sicherheit 2018 - 2023« beträchtlich gewesen. Die Fraunhofer-Gesellschaft hat sich in der Umsetzung dieses Programms als starker Partner für innovative Ansätze und Lösungen entlang des gesamten Anwendungsfelds und Ausschreibungsspektrums der zivilen Sicherheitsforschung erwiesen.

Aktuell lassen die umfassende Ausrichtung und Implementierung des ganzheitlichen Konzepts der Resilienz gegenüber Katastrophen als erstrebenswerte Eigenschaft von Staat, Gesellschaft und gesellschaftlichen Funktionen und die damit einhergehende fortgeführte Ersetzung des eher statischen und nicht zu erreichenden Zustands der Sicherheit auf eine grundlegende und wertvolle Fortführung der Optimierung der Umsetzung einer zivilen Sicherheitsforschung schließen. Viele Elemente und Instrumente des noch aktuellen Programms haben sich bereits als hilfreiche und nützliche Werkzeuge erfolgreicher Forschungs- und Entwicklungsaktivitäten erwiesen, wie etwa »Anwender innovativ«[3], die dem fähigkeitsgetriebenen Ansatz folgend die späteren Nutzer der Lösungen ins Zentrum stellt.

3 »Anwender innovativ« im Rahmenprogram »Forschung für die zivile Sicherheit 2018–2023«.

Es ist zudem notwendig, gewisse Kernelemente beizubehalten, nicht zuletzt, um ihnen Zeit zu geben, sich in diesem Multi-Stakeholder-Kontext in der Breite zu etablieren und zu optimieren, anstatt frühzeitig Ansätze neu zu erfinden. Dabei spielt insbesondere das komplementäre Zusammenspiel der Instrumente aus nationalen und staatenübergreifenden Initiativen, primär im Rahmen der europäischen Sicherheitsforschung, eine große Rolle. Aber auch parallele (nicht-anwendungsgetriebene) themenoffene Ausschreibungen sollten weiterhin Raum finden, um innovative Durchbrüche zu ermöglichen. Neben der fortgeführten Verbesserung der Anbindung der nationalen Aktivitäten an die Initiativen der europäische Sicherheitsforschung gilt es nun, das Potential zukünftiger Ergebnisse zur Stärkung der Resilienz im Kontext von Katastrophen (natürlich, absichtlich oder unabsichtlich menschen-/ technologieverursacht) zu steigern, den fähigkeits- bzw. anwendungsorientierten Ansatz der Forschungs- und Entwicklungsaktivitäten weiter auszubauen und weitere Stellschrauben zur Erhöhung der späteren Operationalisierungs- und Implementierungsrate zu identifizieren.

Die Fraunhofer-Gesellschaft formuliert dazu Empfehlungen für den Ausbau bzw. die Implementierung der folgenden Ansätze:



o., M., u.:
Die Ahr zwischen Altenahr und Rech nach dem Hochwasser, das große Teile der Versorgungsinfrastruktur zerstörte und die Kommunikation lahmlegte.
Foto: Fraunhofer FKIE

Die erhöhte Waldbrandgefahr in Mitteleuropa erfordert eine verbesserte, ressortübergreifende Abstimmung, Kooperation und Ausbildung auf europäischer und nationaler Ebene. Foto: iStock

Beispielergebnis eines Verfahrens zur Schätzung menschlicher Posen (bspw. Agression, Sturz oder regungsloses Liegen). Quelle: Fraunhofer IOSB

Stärkung bisheriger Ansätze zur Optimierung des Transfers in die Gesellschaft und zur Erhöhung des Potentials neuer Lösungen zur Steigerung der Resilienz – **Empfehlungen für 2024+**

Zusätzliche Förderung der Optimierung der ressort- und sektorübergreifenden Kooperation

Ein umfassendes Risikomanagement in Zusammenhang mit Katastrophen umfasst auch die Befassung mit Zukunftsszenarien, die sich aus den aktuell bekannten und antizipierbaren Gefährdungen ergeben.[4] Worst-Case-Szenarien, etwa die theoretische Annahme der Nicht-Erreichung des 2°C-Ziels und deren kaskadierende Folgen, müssen dabei ebenso betrachtet werden wie Szenarien mit weniger drastischen Auswirkungen, um ein umfassendes Bild zu erlangen.[5] Selbst wenn man wie aktuell Konsens »lediglich« von einer stetigen Verschlimmerung bzw. weiteren Häufung beispielsweise von Extremwetter ereignissen ausgeht, so zeichnet sich vor dem Hintergrund der aktuellen Kapazitäten und Strukturen ab, dass die zivilen Sicherheitselemente kurz- bis mittelfristig nicht alleine ausreichend sein werden, um deren Auswirkungen abzufedern. Die möglichen Kombinationen aus Lagen oder hybride Bedrohungen und deren zeitliche Häufung werden unsere größtenteils auf freiwilligen – und damit in weiteren Berufen beschäftigten – Kräften beruhenden Strukturen ohne Frage vor noch größere Herausforderung stellen als bisher. Zudem sind die Gefahren (Energieversorgung, Bürgerunruhen, Cyberangriffe, etc.) für die Sicherheit in Deutschland, die sich etwa durch den Angriffskrieg Russlands auf die Ukraine und dessen potentiell langfristige Folgen ergeben, nicht nur militärischer Natur (siehe etwa Gasmangellage oder weitere Lieferketten), genau wie die Gefahren, die durch den Klimawandel auf uns zukommen, nicht rein ziviler Natur sind (Flüchtlingswellen, Konfliktpotential bei der Erschließung wertvoller Rohstoffe etwa in der Arktis oder bei Wasser etc.).

Für ein funktionierendes, möglichst reibungsloses und flexibles Krisenmanagement zur Beantwortung einer Katastrophe ist also die Kooperation und Vernetzung mit anderen Ressorts, insbesondere dem der nationalen militärischen Verteidigung dringend erforderlich. Hierbei gilt es, entsprechend der jeweiligen Mandate die ineinandergreifenden Prozesse, Abläufe, Strukturen und technologischen und nicht-technologischen Schnittstellen des jeweiligen Ressorts im Falle von Katastrophen und/oder des Zivilschutzes maximal zu optimieren und zu standardisieren, wie etwa mit dem ab Oktober 2022 operativen »Territorialen Führungskommando der Bundeswehr (TerrFüKdoBw)«, einer neuen Struktur zur operativen Führung der im Heimat- und Katastrophenschutz sowie allgemein im Inneren eingesetzten Bundeswehrkräfte.

Aber auch im Zusammenhang mit zivilen Kräften des europäischen und internationalen Auslands sind verbesserte Abläufe und Strukturen, etwa zur Entsendung von Einsatzkräften wie im Rahmen des Union Civil Protection Mechanism, oder der verbesserte Austausch von Wissen wie, z. B. durch Trainings lokaler Feuerwehreinheiten durch Einsatzkräfte des Mittelmehrraums oder durch die Förderung des Austauschs von Best Practices, von entscheidender Bedeutung und sollten zusätzlich gezielt gefördert werden.

4 z. B. The Intergovernmental Panel on Climate Change oder der Global Risk Report des World Economic Forums.
5 z. B. Kemp, L. et al, Climate Endgame: Exploring catastrophic climate change scenarios, https://doi.org/10.1073/pnas.2108146118.

Zur grundsätzlichen Förderung der ressortübergreifenden Kooperation sowie zur Vermeidung von Doppelungen der Forschungsagenden zur Umsetzung der »Zukunftsstrategie« sollte mithilfe von Dialogformaten eine Abstimmung bzw. ein Austausch zu Forschungsthemen stattfinden. Dies betrifft insbesondere den Austausch und die mandatsgerechte Abstimmung der BOS mit den Sektoren Verteidigung und Weltraum, um mögliche Synergien aus Sicht der zivilen Sicherheit mit zu generieren und zu gestalten (Themen z. B. sichere Kommunikation, Lagedarstellung, Command & Control, Digitale Zwillinge, Cyber, Logistik…) sowie in den Instrumenten und Ergebnissen der nationalen Sicherheitsforschung anschlussfähig an mögliche kommende Initiativen auf europäischer Ebene zu bleiben.[6]

Folglich sollte zum einen die (nationale wie internationale) sektor- und ressortübergreifende Optimierung und Standardisierung von Prozessen und Abläufen in der Kooperation (inklusive den Prozessen der Forschung) und/oder Entsendung, sowie der Entwicklung von technischen Standards, des Austauschs und des gegenseitigen Lernens und Trainierens als Element der nationalen Sicherheitsforschung implementiert werden. Dieses erweiterte Element unter dem Mandat der nationalen Sicherheitsforschung muss entsprechend im Etat des kommenden Programms zusätzlich berücksichtigt werden. Das erwähnte Mittel der Entwicklung von nationalen Standards sollte dabei strategisch mit Blick auf die Beteiligung an europäischen Standardisierungsprozessen und auf die Stärkung der Wettbewerbsfähigkeit der nationalen Sicherheitsindustrie im europäischen und internationalen Umfeld vorangetrieben werden.

Viele dieser Aspekte werden u. a. auch in der Nachlese des Forschungsgipfels 2022 im Papier »Innovationspolitik nach der Zeitenwende – Leitlinien für eine Zukunftsstrategie« oder auch im »Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie« unterstützt.

Anwendungsgetriebene Forschung auf der Basis verbesserter strategischer Planung

Wie nicht zuletzt aus dem Handlungsfeld 1 »Katastrophenrisiken verstehen« der Resilienzstrategie deutlich wird, ist die Notwendigkeit einer abgestimmten und auf einer Kombination aus sicherheitsspezifischer Zukunfts- und Erfahrungsanalyse mit paralleler Beobachtung der Verwertbarkeit von technologischen Trends beruhenden strategischen Planung bereits in weiten Feldern erkannt.

Aus Sicht der nationalen Sicherheitsforschung oder grundsätzlich vom Standpunkt der Forschung und Entwicklung ist die Ausrichtung auf relevante zukünftige Szenarien essentiell, um den aus diesen Szenarien entstehenden Bedarf zeitgerecht mit geeigneten Lösungen decken zu können, da deren Entwicklung Zeit benötigt. Lösungen, die jetzt in aktuellen Forschungs- und Entwicklungsprojekten angestrebt werden, können für gewöhnlich erst in fünf bis zehn Jahren einen marktreifen Zustand vorweisen, sofern es nicht um die individuelle Anpassung bereits vorhandener Lösungen geht.

Für die Umsetzung einer strategischen Planung mangelt es dabei nicht an Input für eine sicherheitsspezifische Zukunftsanalyse und entsprechende Grundlage zur Identifikation zukünftiger Bedarfe, beginnend bei globalen Analysen, wie beispielsweise dem Global Risk Report des World Economic Forums[7], über nationale Aktivitäten, wie den aktuellen Foresight-Prozess VORAUS:schau![8] des BMBF, über die Themensetzung der LÜKEX-Übungen[9] des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, ebenfalls ressortübergreifend z. B. im Referat für Zukunftsanalyse des Planungsamts der Bundeswehr RefZukA, bis hin zu konkreten Szenarien aus nationalen Foresight-Aktivitäten oder Planspielen im institutionellen Bereich[10]. Gleiches gilt für den Aspekt der parallelen Vorausschau und Bewertung technologischer und gesellschaftlicher Entwicklungen. Unsere Beobachtung ist jedoch zum einen, dass es hier an der Systematisierung derartiger Aktivitäten mangelt (auch hier wieder Ein- und Anbindung in und an den europäischen Kontext), und zum anderen, dass sich aus den Ergebnissen derartiger Aktivitäten keine ressortübergreifende Verantwortlichkeit ableitet, die in konkrete Handlungsaufträge (Analyse zukünftiger Fähigkeitsanforderungen, Bedarfsermittlung, Bedarfsdeckung) und resultierende, abgestimmte Gesamt- und Teilstrategien einer strategischen Fähigkeitsplanung mündet. Die Situation zur Optimierung der strategischen Planung ist daher nicht von einem Mangel an relevanten Erkenntnissen, sondern von einem Operationalisierungsdefizit geprägt.

6 Siehe u. a. »Action Plan on Synergies between civil, defence and space industries«, Europäische Kommission, Feb 2021.
7 Global Risk Report 2022.
8 VORAUS:schau!
9 Länder- und ressortübergreifende Krisenmanagementübung (EXercise) LÜKEX des BBK..
10 z. B. Pandemische Influenza in Deutschland 2020 – Szenarien und Handlungsoptionen, Fraunhofer INT 2013.

Die nationale wie die europäische Sicherheitsforschung strebt seit einiger Zeit richtigerweise einen fähigkeitsgetriebenen Ansatz in der Forschung an und konzentriert sich konsequenterweise auf formulierte Bedarfslücken der Anwendungsseite, wie etwa auf europäischer Ebene auf die Fähigkeitslücken des International Forum to Advance First Responder Innovation IFAFRI[11]. Dieser Fokus auf Fähigkeiten ergibt sich alleine aus der unüberschaubaren Menge an möglichen Bedrohungslagen, potenziert durch das Thema der hybriden Bedrohungen und die logische Erkenntnis, dass man sich nicht auf jede Lage einzeln vorbereiten kann. Hingegen bleiben die im Wandel der Zeit notwendigen Fähigkeiten entlang des Resilienzzykluses (Vorbereiten – Vorbeugen – Schützen – Bewältigen – Wiederherstellen) zur grundsätzlichen Beantwortung von Lagen deutlich besser adressierbar, um diese zukunftsfähig und resilient auf- bzw. auszubauen.

In der einfachen Abfrage entsprechender Bedarfe der Anwendungsseite hinsichtlich der notwendigen Verbesserung von Fähigkeiten beschreiben diese aber in der Regel mehr oder weniger zufällig aktuell in Einsatz und Übung identifizierte Lücken. So werden häufig in der Nachlese der Krise erkannte Lücken adressiert bzw. dienen diese regelmäßig in Forschung- und Entwicklungsprojekten als Sicherheitsszenarien, um die Notwendigkeit des geplanten Vorhabens zu unterstreichen. In der Folge laufen die Ergebnisse zum Zeitpunkt der Fertigstellung der Entwicklungsprozesse – also bei Markteinführung und nicht am Ende des jeweiligen Projekts – häufig zeitlich und in der spezifischen Anpassung dem Bedarf hinterher. Für eine erfolgreich(er)e und bedarfsorientiert(er)e Operationalisierung späterer Ergebnisse aus Forschungs- und Entwicklungsaktivitäten ist es daher unumgänglich, die Anwendungsseite zu befähigen, sich strategisch, frühzeitig und zukunftsgerichtet an entsprechenden Prozessen zu beteiligen und diese mitzugestalten. Dafür braucht es zunächst das grundsätzliche Verständnis über die Zeithorizonte von Forschungs- und Entwicklungsprozessen und über die daraus resultierende Notwendigkeit einer vorausschauenden Planung. Wie sehen meine Aufgaben unter relevanten Zukunftsszenarien aus? Bin ich dafür bereits aufgestellt bzw. wo gibt es Bedarfe zu decken? Welche technologischen Neuerungen sind in Zukunft zu erwarten und haben diese eine Relevanz für die Umsetzung meiner Aufgaben? Wie kann ich deren Entwicklung mitgestalten, um dann später an meine Umgebung angepasste Lösungen beschaffen zu können?

Wie zuvor erwähnt, sind die Ansprechpartner zur Steuerung der entsprechenden Prozesse und zur gemeinsamen Beantwortung dieser Fragen in den verschiedenen Ressorts und relevanten Institutionen auf nationaler und europäischer Ebene bereits zu großen Teilen vorhanden. Das nationale Sicherheitsforschungsprogramm muss daher in Richtung einer klaren Weiterentwicklung von Strukturierung, Priorisierung und Konkretisierung der relevanten Aktivitäten in Deutschland gehen und basierend auf einer regelmäßigen Analyse zukünftiger Bedrohungen und der gemeinsamen Ermittlung der daraus erwachsenden Forschungs- und vor allem zivilen Fähigkeitsbedarfe weiterentwickelt werden. Der Weg muss also weg von zufälliger Identifikation aktueller Fähigkeitslücken in Einsatz oder Übung und hin zur gezielten Identifizierung zukünftiger Bedarfe unter Einbeziehung der vielfältigen Stakeholder führen. Nur so kann eine lösungsoffene (also neben dem Bereich des technologischen Equipments auch aus den Bereichen der Organisationsstruktur, der involvierten Personen und beteiligten Prozesse) Entwicklung von wirklich innovativen Lösungen zur Deckung der Fähigkeitslücke erreicht werden.

Die derzeitig identifizierten aktuellen Fähigkeitslücken sind eine Aufgabe der erweiterten Instrumente der Beschaffung und können nicht zeitnah durch Forschung und Entwicklung adressiert werden. Die gute Nachricht ist, dass es für nahezu alle aktuell identifizierten Bedarfe bereits Lösungen auf dem nationalen und europäischen Markt – und damit den entsprechenden Regularien insbesondere des Datenschutzes und der Ethik folgend – gibt. Durch eine verbesserte Anbindung und Verknüpfung mit Strukturen und Elementen der erweiterten Beschaffung wie Formaten des »pre-commercial procurement« auch auf Seiten der Europäischen Union[12] oder dem Kompetenzzentrum innovative Beschaffung (KOINNO)[13] können diese am Bedarf optimiert geschlossen werden – wenn auch nicht ideal und von Beginn (niedriges TRL) an für den Bedarf entwickelt. Aber insbesondere vor dem Hintergrund des extrem zerklüfteten Marktes ergeben sich hier national wie europäisch immense Potentiale für eine Beantwortung aktueller Bedarfe und damit für eine Stärkung der Resilienz gegenüber Katastrophen, bis man auch im Bereich der Forschung und Entwicklung ganzheitlich »vor die Lage kommt«.

11 IFAFRI Capability Gaps.
12 Überblick der Förderinstrumente der Europäischen Sicherheitsforschung, NKS Sicherheitsforschung.
13 Kompetenzzentrum innovative Beschaffung (KOINNO).

Positionspapier der Fraunhofer-Gesellschaft

Resilience by Design – das »richtige System« statt das »System richtig« entwickeln

Das Potential zukünftiger Lösungen zur Stärkung einer resilienten Gesellschaft lässt sich durch die Maximierung der Anpassung an die spätere operative Umgebung steigern. Je besser eine Lösung in das existierende Umfeld eingebettet werden kann, umso besser kann sie ihrer eigentlichen Funktion »nachkommen«. Dem zu Beginn der Sicherheitsforschung geprägten Begriff »Security by Design« folgte in Anerkennung der besonderen Werte und Schutzrechte auf europäischer Ebene der Begriff »Privacy by Design«. Zur tiefen Verankerung des Konzepts der Resilienz wird es Zeit zur Prägung des Begriffes »Resilience by Design«.

Die simple Entwicklung einer einzelnen Lösung/Technologie ist fast nie die vollständige Antwort auf einen Bedarf. In der Regel müssen Rahmenbedingungen und umgebende Prozesse usw. geändert und/oder reflektiert werden, um eine neue Lösung erfolgreich zu operationalisieren. Ergebnisse von Test- und Demonstrationsaktivitäten in Rahmen von Forschungs- und Entwicklungsaktivitäten zeigen bei mangelhafter Umsetzung sehr häufig statt einer Validierung der Funktionalität der angestrebten Lösung die fehlende Berücksichtigung des operativen Umfelds. So sind die zur Testung einbestellten Anwender häufig gar nicht ad hoc in der Lage, die neuen Lösungen zu testen, da die dafür notwendigen Abläufe oder Personalstrukturen nicht abbildbar sind. Folglich werden bereits in der Entwicklungsphase die richtigen Akteure mit entsprechendem (breitem) Verständnis und Weitblick in Bezug auf die spätere Operationalisierung der Lösung in ihrem jeweiligen Kontext des Resilienzzykluses (Vorbereiten – Vorbeugen – Schützen – Bewältigen – Wiederherstellen) benötigt. Dies umfasst auch die Aspekte der späteren Beschaffung und gilt gleichbedeutend sowohl für Lösungsanbieter als auch Anwender (Einsatzkräfte während Piloten und Demos reichen nicht aus – operative, taktische, strategische Ebene) und politische Entscheider. Eine iterative Evaluierung (bedarfs-/fähigkeitsorientierte Verifizierung und Validierung) muss von Beginn des Projektes/der Lösungsentwicklung an mit einer systemischen Perspektive implementiert werden, die die Gesamtauswirkungen der Lösung in ihrem operativen Umfeld berücksichtigt – neben der reinen Funktionalität auch an Schnittstellen zu anderen Lösungen reicht dies von der Benutzerakzeptanz und Benutzerfreundlichkeit bis hin zu ethischen/rechtlichen/gesellschaftlichen/politischen/organisatorischen/prozeduralen/ökonomischen Aspekten im Umfeld der Operationalisierung. Diesen gängigen Aspekten einer systemischen Perspektive ist vor dem Hintergrund der gesamtgesellschaftlichen Resilienz der Faktor der Nachhaltigkeit hinzuzufügen. Auch die im Rahmen der Funktion mögliche Flexibilität und An- bzw. Lernfähigkeit der Lösung sind von entscheidender Bedeutung für ein frühzeitig implementiertes Resilienzkonzept.

Neben diesen Aspekten des operativen Umfelds angestrebter Innovationen sind auch die Wechselwirkungen mit der direkten und indirekten Umgebung des weiteren Einsatzgebiets von entscheidender Bedeutung für die »Resilienzkraft« einer neuen Lösung. In unserer zunehmend komplexen, vernetzten Welt sind zur Abschätzung dieser Interdependenzen umfangreiche Simulationssysteme in Verifizierungs- und Validierungsprozessen notwendig. Das von Bund und dem Land Berlin geförderte und kürzliche gestartete Fraunhofer-Zentrum für die Sicherheit Sozio-Technischer Systeme SIRIOS setzt genau diese Aspekte um und bietet sich in Kombination mit der Gesamtheit der in der Fraunhofer-Gesellschaft verfügbaren Lösungskompetenzen als idealer Entwicklungspartner für entsprechend systemisch durchgeführte FuE-Aktivitäten an.

Gesamtgesellschaftliche Resilienz – methodisch gestützte aktive Einbindung aller beteiligten Akteure

Die zivile Sicherheit und die angestrebte Stärkung der Resilienz gegenüber Katastrophen ist ein hochgradig von Interdisziplinarität und einer fast unüberschaubaren Vielfalt und Vielzahl von Akteuren geprägtes Feld. Naturgemäß verstehen Menschen mit unterschiedlichen Hintergründen (disziplinär, geschlechtlich, kulturell, ökonomisch etc.) Begrifflichkeiten oder eigentlich gemeinsam formulierte Ziele sehr unterschiedlich, wie etwa die Vorstellung des »Zeithorizonts zur Lösung eines Problems« bei einer Einsatzkraft im Vergleich zu einem Forschenden oder auch die Deutung der Begriffe »Krise« oder »Risiko«. Insbesondere die Relevanz und die Verknüpfungen von soziotechnischen Systemen mit der angestrebten verbesserten Einbindung der Bevölkerung (Citizen Science) führen beispielsweise zu

14 Basierend u. a. auf Hartung, S.; Wihofszky, P.; Wright, M. T. (2020). Partizipative Forschung. Wiesbaden: Springer Fachmedien Wiesbaden.

einer notwendigen engen Zusammenarbeit der sprachlich sehr unterschiedlichen Sozial- und Ingenieurswissenschaften, der Industrie, der politischen Entscheidungsträger sowie der Einsatzkräfte und der Bevölkerung.

Um in einem solchen Multi-Stakeholder-Kontext einen koordinierten Beteiligungsprozess zu ermöglichen, empfiehlt es sich, auf Ansätze aus der partizipativen Forschung zurückzugreifen. Das Ziel derartiger Ansätze ist es, alle Perspektiven der unterschiedlichen Gruppen zur Wissensgenerierung zusammenzuführen, u. a. um die von Maßnahmen oder Entscheidungen Betroffenen möglichst früh einzubeziehen, nicht in der Beschlussfindung zu übergehen und um ein gemeinsames Verständnis zu schaffen. Durch den Einbezug vieler Akteure können neue Ideen und Lösungen sichtbar werden oder entstehen.[14] Ein solcher Prozess der gemeinsamen Entscheidungsfindung/ Produktentwicklung erfolgt »ko-kreativ«.

Die Weiterentwicklung der zivilen Sicherheit ist geradezu ein Musterbeispiel für einen solchen Multi-Stakeholder-Kontext. Zur Umsetzung und Optimierung ganzheitlicher, inklusiver und ko-kreativer Innovationsprozesse in diesem Umfeld ist folglich eine entsprechend methodische Unterstützung des Dialogs empfehlenswert, was nicht zuletzt den umfassenden Austausch auf Augenhöhe von Anwendern (Bedarfsträgern) und einschlägigen Fachexperten (Bedarfsdeckern) und der Bevölkerung fördert. Dieser verbesserte Dialog führt mittelfristig zu einer vermehrten und notwendigen Offenheit sowohl der Anwendungsseite als auch der Bevölkerung gegenüber innovativen Lösungen, zur Erkenntnis des Mehrwerts einer aktiven Beteiligung an Forschungs- und Entwicklungsprozessen, zum erhöhten Vertrauen in die öffentlichen Apparate des Bevölkerungsschutzes und damit in die Regierung sowie langfristig in der Folge zu einer Verschiebung der Budgetierung in Richtung von Forschung und Entwicklung bei Behörden und Organisationen mit Sicherheitsaufgaben.

Alle genannten Aspekte würden damit auch einen erheblichen Beitrag zu der angestrebten Verbesserung einer abgestimmten sowie anwendungsgetriebenen, strategischen Planung leisten.

Übergreifende Bedarfsermittlung sowie verbesserte Verbreitung von und Zugriff auf kommende und vorhandene Lösungen

Wie eingangs erwähnt, erschwert ein extrem kleinteiliger und zerklüfteter Markt der Anwendungsseite den schnellen Zugriff auf bereits vorhandene Lösungen des Markts oder bisheriger und aktueller Forschungsergebnisse. Es existierte bisher keine systematische Herangehensweise, die diesen notwendigen Überblick ermöglichen würde. Auch auf Seiten der Forschung und Entwicklung sprechen wir über Fähigkeitslücken, ohne zu definieren, in welchem Gesamtsystem diese Lücken eigentlich existieren. Zum besseren Verständnis dessen, was benötigt wird, lässt sich das Bild eines Schranks mit zahlreichen Schubladen bemühen, der einerseits aktuelle Lösungen und solche noch in der Entwicklung befindliche abbildet, gleichzeitig aber auch den Ort zur spezifischen Formulierung eines zukünftigen Bedarfs bietet. Alles hängt von einer gemeinsamen Kategorisierung bzw. Betitelung/ Nomenklatur der Schubladen ab. Ein solcher Schrank, mit den gesamten Fähigkeiten kategorisiert in entsprechend benannte Schubladen, würde somit gleich mehrere der vorab angesprochenen Herausforderungen unterstützend adressieren. So etwa die Harmonisierung themen- bzw. ressortübergreifender Bedarfe und somit die Förderung von Synergien in Forschungs- und Entwicklungsprozessen, beispielsweise in der parallelen Entwicklung von sicheren Kommunikationswegen sowohl in den Bereichen der polizeilichen Gefahrenabwehr als auch in der Beantwortung von Katastrophen innerhalb der zivilen Sicherheit, aber ggf. auch in Abstimmung mit den Ressorts Verteidigung und/ oder Weltraum.

Solch eine Taxonomie der Fähigkeiten wäre zudem ein Hilfsmittel zur strukturierten Darstellung und Verbreitung aktueller Forschungsergebnisse und der vorhandenen Lösungen des Markts – unabhängig von der Natur der Lösung – und könnte über eine digitale Plattform der Anwendungsseite schnellen Zugriff auf Informationen ermöglichen. Eine gemeinsame Nomenklatur hilft letztendlich auch bei der Verbesserung der Kommunikation und des gegenseitigen Verständnisses wie etwa zwischen verschiedenen Disziplinen oder Kulturen.

In Ermangelung einer ähnlich umfassenden Alternative greifen wir zur Strukturierung unserer im Anhang aufgeführten Themenvorschläge auf die kürzlich veröffentlichte Taxonomie des europäischen Sicherheitsmarkts[15] zurück. Diese soll die aktuellen technologischen Lösungen auf dem Gebiet der zivilen Sicherheit kategorisieren und hat dazu querschnittlich zu den vier Säulen der europäischen Sicherheitsforschung – Kampf gegen Kriminalität und Terror, kritische Infrastrukturen, Grenzsicherheit und katastrophenresiliente Gesellschaften[16] – und ihren jeweiligen Unterbereichen 13 sogenannte Functional Areas definiert, die einer Clusterung bestimmter Sicherheitsfähigkeiten entsprechen. Dieses Vorgehen könnte die Anbindung an die europäische Sicherheitsforschung zukünftig erleichtern, sofern diese Taxonomie wie von der Kommission angestrebt vermehrt in Forschungs- und Entwicklungsaktivitäten und deren Verbreitung Verwendung findet und sich als Kategorisierung von Lösungen aus dem europäischen Sicherheitsprogramm etabliert. Allerdings konzentriert sich diese Taxonomie auf Technologien und wird somit nicht-technologischen Lösungsansätzen zur Schließung von Fähigkeitslücken nur bedingt bis gar nicht gerecht. Dies gilt insbesondere für veränderte Prozesse/ Abläufe (z. B. Standard Operating Procedures), aber auch für Anpassungen an Personal- und Organisationsstruktur und wäre in der Nutzung einer Taxonomie zur Unterstützung einer angestrebten lösungsoffenen (ohne frühzeitige Festlegung, ob später eine nicht-technologische oder technologische Lösung den Bedarf optimal schließen kann) Ermittlung zukünftiger Bedarfe zu berücksichtigen. Auf nationaler Ebene könnte als alternative Basis für eine Struktur bzw. Kategorisierung das unter dem Mandat des neu installierten Gemeinsamen Kompetenzzentrums Bevölkerungsschutz avisierte Ressourcenregisters[17] dienen – oder umgekehrt ebenfalls auf der europäischen Taxonomie aufbauen und gemeinsam verwendet werden.

15 EU civil security taxonomy and taxonomy explorer, DG HOME 2022.
16 Auch auf europäischer Ebene wird das Thema IT-Sicherheit/Cyber von einem weiteren Ressort – hier DG CONNECT – betreut.
17 »Basierend auf den Fähigkeiten und dem Wissen aller Behörden und Organisationen werden u. a. datenbasierte Prognosen erarbeitet, gemeinsame Lagebilder erstellt oder ein umfassendes Ressourcenregister aufgebaut.«, Gemeinsames Kompetenzzentrum Bevölkerungsschutz.

Anhang

Positionspapier der Fraunhofer-Gesellschaft

Themenvorschläge der Fraunhofer-Gesellschaft zur Umsetzung im Programm der »Forschung für zivile Sicherheit« 2024+

Die Unterteilung der Themenvorschläge erfolgte wie zuvor beschrieben nach den 13 querschnittlichen »Functional Areas« der »EU civil security taxonomy«. Wenn mehrere »Functional Areas« pro Themenvorschlag benannt wurden, sind diese in Klammern hinter dem jeweiligen Titel aufgeführt. Sofern in einer Functional Area nur der Titel angegeben wurde, befindet sich die ausführlichere Beschreibung unter der fett markierten Functional Area der Aufzählung. Themenvorschläge, die eher einen methodischen oder prozeduralen/ nicht-technologischen Ansatz vermuten lassen, wurden teilweise anhand einer eher thematischen Zuordnung Functional Areas zugewiesen.

FA01 – Personal and other equipment for prevention, response and recovery

Smart Textiles zur Überwachung

Um menschliche Einsatzfähigkeiten auch an der Schnittstelle zu technischem Gerät zu erweitern, gewinnen smarte Textilien mit integrierten Zusatzfunktionen an Bedeutung.

Die Möglichkeiten der individuellen sensorischen Erfassung der Vitalfunktionen von Einsatzkräften, die Überwachung der Einsatzbefähigung, die Erfassung kritischer Zustände sowie die etwaige Zuführung von Unterstützung erweitern die Möglichkeiten eines erfolgreichen Einsatzes. Ermöglicht werden kann dies durch Integration elastischer Energiewandersysteme, die die über Textilien übertragene menschliche Bewegungskinematik elektromechanisch nutzen. Weiterhin können über eine aktorische Ansteuerung der Energiewandler die haptische Rückmeldung von Feedback- und Warnfunktionen an der Schnittstelle zu technischem Gerät und zur Umwelt erreicht und Aufmerksamkeit sowie Einsatzmöglichkeiten gesteigert werden. Zudem kann die Energiewandlung genutzt werden, um Bewegungsenergie im Sinne einer Energierückgewinnung zur energieautarken Zuspeisung von Instrumenten genutzt werden.

Positionspapier der Fraunhofer-Gesellschaft

Abwehrmöglichkeiten von zu Waffen missbrauchten autonomen UAS und Drohnenschwärmen im zivilen Raum (FA01, FA03, FA11)

Von unbemannten Flugsystemen (UAS) geht ein zunehmendes Bedrohungspotenzial aus. Diese werden zunehmend von Kriminellen und terroristischen Vereinigungen als flexible Plattformen in akuten Konflikten, zur Ausspähung von sensiblen Einrichtungen oder für den Transport von Gefahrstoffen verwendet. Dies resultiert in einem signifikanten Bedarf nach Abwehrmaßnahmen sowie im Vorlauf nach einer wirksamen, ggf. multisensoriellen Früherkennung, Klassifikation und schnellen Schadenspotenzialabschätzung als fundierte Entscheidungshilfe dazu,, wann diese zu aktivieren sind. Bislang wird vorrangig durch Hochfrequenz-Jammer eine Unterbindung der Fernsteuerung erreicht oder auch die Täuschung der Satellitennavigation durch GPS-Spoofing verursacht. Eher physisch gehen robuste Abwehrdrohnen durch direkte Kollision mit dem Ziel vor; darüber hinaus kommen auch Netzwerfer aus der Luft oder vom Boden zum Einsatz, welche nur bei schwebenden Drohnen, aber nicht bei schnelleren Fixed-Wing-Drohnen angewandt werden können. Die jüngsten Entwicklungen im Bereich der Automatikfunktionen zeigen, dass diese Abwehrsysteme zunehmend an Wirksamkeit verlieren und eines neuen flexiblen Ansatzes bedürfen.

Neutralisierung von improvisierten Sprengsätzen im zivilen Raum

IEDs (improvised explosive devices) können vor Ort durch Kampfmittelräumdienste oder aus der Entfernung mit Hilfe von Spezialrobotern begutachtet und entschärft werden. Die Entschärfungsmethoden setzen u. a. auf Ansprengen oder fernbediente Wasserschlaggewehre. Die Fähigkeitslücke besteht in besser dosierbaren Entschärfungsmethoden, die zudem aus einer sicheren Entfernung ohne potentielle Beschädigung des Entschärfungswerkzeugs und potentiell ohne drastische Beschädigung der Umgebung stattfinden kann.

Lokales initiales Krisenmanagement

In den ersten Tagen eines großflächigen Schadensereignisses ist die schnelle und zielgerichtete Koordination lokaler Kräfte – von professionellen Rettungskräften bis hin zu Spontanhelfern – entscheidend für die Rettung von Menschenleben, die Reduzierung des Schadens und die ersten Schritte in Richtung Krisenbewältigung.

Zu besonderen Herausforderungen führen der Wegfall von Kommunikationsmöglichkeiten (u. a. Mobilfunk, Internet, Telefon, BOS-Funk), abgeschnittene Zufahrts- und Fluchtwege sowie fehlende Informationen über die Schadenslage und die zur Verfügung stehenden Ressourcen. Zudem bindet eine großflächige Lage die Behörden und Kräfte eines betroffenen Lands dermaßen, dass eine flächendeckende Unterstützung nicht unmittelbar erfolgen kann – Gemeinden bleiben zunächst auf sich alleine gestellt. Die Hochwasserkatastrophe in Rheinland-Pfalz und Nordrhein-Westfalen hat hier auf schmerzhafte Weise Defizite bei dem unmittelbaren Aufbau eines Lagebilds und der Koordination von Rettungskräften und Spontanhelfern aufgezeigt.

Datenschutzkonforme, intelligente Überwachung kritischer Infrastruktur (FA01, FA02, FA03)

Überwachungsmaßnahmen auf öffentlichen Plätzen, im Bereich kritischer Infrastruktur oder auf privatem Firmengelände helfen dabei, Straftaten zu verhindern bzw. aufzuklären. Mit der Überwachung durch Kameras sind jedoch sehr hohe rechtliche Hürden und Auflagen zur Wahrung der Persönlichkeitsrechte verbunden. Während etwa die Unkenntlichmachung von Eingängen und Fenstern von Wohn- und Geschäftsgebäuden oder von Autokennzeichen ausreichend ist, ist die Verpixelung von Gesichtern o. Ä. nicht ausreichend. Zum Schutz von Einrichtungen und Veranstaltungen benötigen Betreiber und Sicherheitskräfte Informationen wie z. B. die Aktivitätserkennung von Personen, für die Kameras geeignete bzw. sogar erforderliche Sensoren sind und in absehbarer Zeit auch bleiben werden. Daher gilt es, neue Privacy-by-Design-Lösungen zu schaffen, so dass eine intelligente Videoüberwachung unter garantierter Wahrung von Datenschutz ermöglicht wird. Übertragbare Fragestellungen einer datenschutzkonformen Umsetzung ergeben sich auch bei weiteren Formen der Überwachung wie etwa im Bereich Netzwerkmonitoring und Intrusion Detection. Für die Erfassung der Informationsdaten und deren Fusion auf unterschiedlichen Ebenen ist die Entwicklung leistungsfähiger Sensorik (auch mobil bzw. als Netzwerk) und angepasster Verfahren notwendig.

Überwachung sensibler öffentlicher Bereiche mit CBRN-E-Sensoren (FA01, FA02, FA03, FA06, FA07)

Überwachungsmaßnahmen in besonderen öffentlichen Bereichen sollten Gefahrstoffsensorik (CBRN-E) einbeziehen, um so optimiert und frühzeitig die Quelle, Konzentration und Ausbreitung möglicher Gefahrstoffe zu bestimmen. Für ein Gesamtbild der Lage und den möglichen Auswirkungen etwa auf Bevölkerung, Umwelt und Strukturen oder eine Gefährderidentifizierung wäre entsprechende Datenfusion mit anderen Systemen nötig.

Erkennung von Lebenszeichen und Lokalisierung von Verschütteten (FA01, FA08)

Jedes Jahr werden Katastrophenschutzorganisationen in Deutschland und weltweit zu Einsätzen nach Gebäudeeinstürzen gerufen. Unabhängig von den Ursachen ist allen Einstürzen gemein, dass eine unbekannte Anzahl von Menschen unter den Trümmerbergen verschüttet sein kann. Je nach Gebäudestruktur besteht immer die Möglichkeit, dass die dort verschütteten Personen das Schadensereignis überlebt haben, z. B. durch entstandene Hohlräume. Auch wenn Verschüttete nicht oder nur leicht verletzt sind, kann die Situation durch Sauerstoffmangel oder durch in Bewegung geratene Trümmerstrukturen schnell lebensbedrohlich werden. Die Rettungskräfte benötigen für ihre Einsätze mobile und modulare Radargeräte mit synchronisierten Einzelsensorknoten, mit denen unterschiedliche Arten von Gelände überwacht, Verschüttete schnell geortet und deren Lebenszeichen (z. B. Atmung) erfasst werden können. Derzeit am Markt verfügbare Messsysteme gewährleisten keine zuverlässige Erfassung von Personen oder deren Vitalparametern.

Löschdrohnen zur Bekämpfung von Waldbränden (FA01, FA11)

Im Zuge des Klimawandels ist immer häufiger mit heißen Sommern und damit einhergehend auch mit Waldbränden zu rechnen. Auch in Deutschland, wie z. B. in Brandenburg, Sachsen und Sachsen-Anhalt, steigt das Risiko für Waldbrände. In mehreren Pilotprojekten wurden Drohnen bereits zum Sammeln von Informationen und speziell zur frühzeitigen Lokalisierung von Hotspots und zur Überwachung der Brandbewegung eingesetzt. Die Entwicklung von Löschdrohnen steht jedoch noch am Anfang; hier müssen noch effektive Lösungen z. B. für das Auf- und Beladen der Drohnen und die Automatisierung von Drohnenschwärmen gefunden werden. Auch der rechtlich-regulatorische Rahmen zum Einsatz von Drohnen, Trainingseinheiten für Feuerwehren und die gesellschaftliche Akzeptanz muss dabei berücksichtigt werden. Mit Hilfe von Löschdrohnen könnten in Zukunft Menschenleben gerettet werden – sowohl auf Seiten der Feuerwehr als auch in der Bevölkerung – und Schäden in Millionenhöhe verhindert werden.

Resilienz in der Energieversorgung bei fortschreitendem Klimawandel (FA01, FA04)

Die Abkehr von fossilen Energieträgern ist für das Erreichen der Klimaziele unerlässlich und führt zur Reduktion bestehender Abhängigkeiten. Zugleich besteht die Gefahr neuer Abhängigkeiten, beispielsweise für Wandler erneuerbarer Energien oder die Materialien zu deren Herstellung.

Die Versorgung mit nachhaltiger Energie ist in dezentralen Energienetzen mit einer Vielzahl zusätzlicher lokaler, verteilter Energielieferanten und weiterer Systembeteiligter verbunden. Eine stärkere Vernetzung von Anlagen und die aktive Einbindung von dezentralen Erzeugungsanlagen und steuerbaren Verbrauchern eröffnet somit einerseits mehr Angriffsflächen für gezielte oder aufgrund von zunehmenden Umweltereignissen bedingte Störungen. Andererseits können zelluläre Ansätze aber auch höhere Sicherheit bedeuten, da begrenzte Netzbereiche ohne Beeinträchtigung benachbarter Zonen gezielt aus dem Betrieb genommen werden. Es besteht folglich die Herausforderung, neue und tendenziell steigende Risiken in der Energieversorgung – bei gleichzeitig wachsender Abhängigkeit von Versorgungssicherheit – durch den Aufbau (insbes. cyber-) resilienter Versorgungsstrukturen zu reduzieren.

Einbezug von Bürgerinnen und Bürgern in Forschung rund um den Katastrophenschutz: Nutzung von Citizen Science (FA01, FA02, FA11, FA12)

Die Idee der Einbindung von Bürgerinnen und Bürgern in Forschungs- und Entwicklungsprozesse ist nicht neu und hat sich in verschiedenen Disziplinen etabliert und bewährt. Im Bereich des Katastrophenschutzes etwa zielen verschiedene Projekte auf deren aktiven Beitrag ab, beispielsweise zur Einbindung beim Sammeln von Daten zur Früherkennung von Risiken. Bislang fehlt jedoch weitestgehend eine systematische Untersuchung, wie und in welchen Phasen des Katastrophen- bzw. Resilienzmanagements von Prävention bis Regenerierung Bürgerinnen und Bürger sinnvoll und effektiv eingebunden werden können. Eine solche Vorstudie könnte einen wichtigen Beitrag für die Entwicklung neuer technischer und organisatorischer Lösungen leisten. Mögliche forschungsleitende Fragen könnten sein: Wie können Bürgerinnen und Bürger dabei helfen, ungenutzte Ressourcen zu erkennen und im Krisenfall einzusetzen? Welchen Beitrag können sie leisten, um vulnerable Personen(gruppen) vor Ort besser zu identifizieren und zu erreichen? Wie können neue Kommunikationskanäle und Interaktionsformen zwischen Wissenschaft, beteiligten Behörden und Bürgerinnen und Bürger aussehen? Welche Räume und Grenzen für Zuständigkeiten existieren? Wie kann Interesse und Motivation in der Bürgerschaft gefördert werden?

Positionspapier der Fraunhofer-Gesellschaft

Methodik zum nachhaltigen Schutz kritischer Logistiknetzwerke (FA01, FA09)

Der Schutz kritischer Infrastrukturen wird oft in Bezug auf die Ursache oder das Phänomen einer plötzlichen und umfassenden Beeinträchtigung untersucht. Forschung zur Kritikalität der transportierten Warenflüsse sowie zur Resilienz der genutzten Infrastruktur über die direkt betroffene Region hinaus hingegen ist selten.

Oft sind es kleinere Risiken (wie Unfälle), die zur Einschränkung der logistischen Infrastruktur oder Versorgungsengpässen führen, aber auch gezielte Angriffe, physisch wie im Cyberraum, spielen zunehmend eine Rolle. Ferner zeigt sich die Verwundbarkeit logistischer Infrastrukturen, wenn sie aufgrund von meteorologischen Bedingungen oder Schäden über einen längeren Zeitraum kaum nutzbar ist. Der Netzwerkcharakter der gesellschaftlich relevanten Grundversorgung, die über die logistische Infrastruktur organisiert wird, wird durch die aktuelle Forschung nicht hinreichend berücksichtigt. Es besteht folglich eine Forschungslücke. Um diese zu schließen, braucht es eine Methodik, die Infrastrukturen und die darauf fließenden Warenströme betrachtet und so bewertet, welche Elemente und Teilnetzwerke so kritisch für das logistische System sind, dass deren Schutz eine besondere Wichtigkeit erlangt.

Automatisierte Reinigung und Desinfektion (FA01, FA02)

Egal, ob in der Gesundheit, Mobilität oder Sicherheit – eine schnelle und einfache Reinigung und Desinfektion von Oberflächen und der Luft ist unverzichtbar. Dabei besteht einerseits Bedarf an nachhaltigen langzeitstabilen Oberflächen, die möglichst multifunktionell und leicht zu reinigen sind. Andererseits steigt die Nachfrage nach mobilen autarken Reinigungssystemen, die im Idealfall die Verschmutzung/ Kontamination der Oberfläche und das Material automatisch erkennen, daraus die optimale Reinigungsprozedur ableiten und dann die Reinigung automatisiert durchführen und dokumentieren. Durch integrierte elektro- oder plasmachemische Verfahren können dabei angepasste Reinigungs- und Desinfektionsmittel (ozoniertes Wasser, Hypochlorid, Wasserstoffperoxid, ..) direkt bei Bedarf dezentral hergestellt und eingesetzt werden.

FA02 – Data, information and intelligence gathering management, and exploitation

Datenschutzkonforme, intelligente Überwachung kritischer Infrastruktur (**FA01**, FA02, FA03)

Überwachung sensibler öffentlicher Bereiche mit CBRN-E-Sensoren (**FA01**, FA02, FA03, FA06, FA07)

Einbezug von Bürgerinnen und Bürgern in Forschung rund um den Katastrophenschutz: Nutzung von Citizen Science (**FA01**, FA02, FA11, FA12)

Automatisierte Reinigung und Desinfektion (**FA01**, FA02)

Zivil-militärische Zusammenarbeit (**FA02**, FA04, FA12, FA13)

Mit dem Territorialen Führungskommando der Bundeswehr (TerrFüKdoBw) wird ab Oktober 2022 in der Bundeswehr eine Struktur zur operativen Führung der im Heimat- und Katastrophenschutz sowie allgemein im Inneren eingesetzten Bundeswehrkräfte. Dem Kommando unterstehen auch die entsprechenden Landeskommandos (LKdos). Auf ziviler Seite ist der Katastrophenschutz neben dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) maßgeblich föderal organisiert. Es ist zu erforschen, wie und mit welchen technischen Hilfsmitteln die Zusammenarbeit zwischen TerrFüKdoBw und BBK auf Bundesebene sowie zwischen LKdos und bundesländerspezifischen Ämtern verbessert werden kann. Dies beinhaltet technische Einrichtungen wie etwa zur übergreifend technisch kompatiblen Lageerfassung, Lagedarstellung, Meldungserstellung, -weitergabe und zu automatisierten Meldeketten, aber auch organisatorische Aspekte wie die automatische Unterstellung bestimmter Landes-, Bezirks- und kommunaler Kräfte unter ein Kommando wie z. B. eine entsprechende Stelle im BMI, BBK oder TerrFüKdoBw bei Ausrufung bestimmter, abgestufter Gefahrenlagenstufen.

Verbesserung des Lageverständnisses auf allen Entscheidungsebenen

Kommunalverwaltungen nehmen eine entscheidende Rolle im Risiko- und Krisenmanagement ein. Die kommunalen Akteure sind im Katastrophenfall als erste vor Ort und müssen auch als erste reagieren. Als sogenannte untere Katastrophenschutzbehörden sind die Kommunen für den Schutz bei größeren Unglücksfällen oder Katastrophen verantwortlich. Jedoch ist bei größeren Lagen, die mehrere Kommunen betreffen, eine intensive Koordination mit den mittleren und oberen Katastrophenschutzbehörden (meist Regierungspräsidien und Innenministerien) notwendig. Hierzu wird eine resiliente (ggf. auch ad-hoc) Kommunikationsinfrastruktur als Basis benötigt.

Weiterhin ist es eine große Herausforderung, in komplexen Flächenlagen ein kontinuierlich aktualisiertes Lagebild sowie eine aktuelle Lagebewertung zu erhalten. Aus der permanenten Abfrage von Berichten aus allen Ebenen bildet sich nicht automatisch ein umfassendes Lagebild. Es müssen die unterschiedlichen Berichts- und Meldesysteme zusammengeführt und ausgewertet werden. Die Bündelung der verschiedenen Erkenntnisse stellt eine besondere Herausforderung dar, für die neue Verfahren benötigt werden.

Kombinierte Risiken und Kaskadeneffekte in kritischen Lieferketten verstehen und quantifizieren (FA02, FA03)

Nahrungsmittelversorgung, Automobilproduktion oder auch Energieversorgung: Der Wohlstand öffentlichen und wirtschaftlichen Lebens in Deutschland basiert auf einem mittlerweile komplexen, europäisch und international hochgradig vernetzten Netz an Versorgungssystemen und Warenketten. Wie verwundbar und sensitiv diese auf maximale Effizienz ausgesteuerten Systeme auf Störungen und Ausfälle reagieren, wurde während der Corona-Pandemie oder auch im Zuge des russischen Angriffskriegs in der Ukraine deutlich. Um die vielschichtigen Ursachen und Wirkungen solcher Ereignisse umfänglich zu erfassen, zu verstehen und daraus wirkungsvolle Sicherheits- und Resilienzmaßnahmen abzuleiten, brauchen Politik und Wirtschaft analytische Werkzeuge und Metriken; z. B. können Modelle von Lieferketten und deren Kopplung mit anderen Systemen dazu beitragen, Kaskadeneffekte besser zu verstehen und diesen entgegenzuwirken.

Metriken und Parameter für ein ganzheitliches Resilienzmanagement für Kommunen und Unternehmen (FA02, FA03)

Im Zuge der Corona-Pandemie hat das Konzept der Resilienz prominenten Einzug gehalten als notwendige Eigenschaft von Organisationen und Unternehmen, um komplexen Risiken und Gefahren proaktiv zu begegnen. Noch fehlt es aber an standardisierten und in öffentlicher Verwaltung und Wirtschaft akzeptierten Resilienzmanagement-Ansätzen, um politische Entscheidungsprozesse und wirtschaftliches Handeln entlang quantifizierbarer Resilienzmanagement-Ansätze zu orientieren. Im Sinne eines Allgefahrenansatzes müssen Risiko- und Gefahrenquellen strukturiert erfasst, Verwundbarkeiten und damit einhergehende potentielle Kaskadeneffekte verstanden und geeignete technische, organisatorische und finanzielle Maßnahmen entwickelt werden, um Verwaltungsorganisationen und Unternehmen zu befähigen, Resilienz proaktiv zu managen. Langfristig ist eine Umsetzung dieser Metriken und Parameter in eine ganzheitliche Softwarelösung für die Anwendungsseite erstrebenswert.

Prognosefähigkeit bezüglich Auswirkungen von zukünftigen Extremwetterlagen im Zuge des Klimawandels (FA02, FA03, FA07, FA08)

Die dramatischen Hochwasserereignisse im Sommer 2021 haben einen Einblick in die dramatischen Folgen des Klimawandels gegeben. Zusätzlich wurden aber auch die vorhandenen Vulnerabilitäten aufgezeigt sowie der Bedarf deutlich, zukünftig bessere Vorhersagen der Auswirkungen treffen zu können und diesen mit wirksamen Schutzmaßnahmen begegnen zu können. Um dieser Fähigkeitslücke entgegen zu wirken, bedarf es neuer Methodiken, die es ermöglichen, die klimabedingten Folgen der Extremwetterereignisse schneller und zutreffender prognostizieren zu können sowie deren Verlauf besser großräumig und überregional verfolgen zu können. Dies umfasst auch die Fähigkeit, örtlich hoch aufgelöste kritische Zustände erfassen zu können.

Risiken quantifizieren, die sich aus der Anwendung Künstlicher Intelligenz in sicherheitskritischen Technologien ergeben (FA02, FA04)

Quantitative Risikomodelle beschreiben reproduzier- und nachvollziehbar Risiken abhängig von quantifizierbaren Unsicherheiten, die sich aus Parameter-, Szenario- und Modellunsicherheiten zusammensetzen. Derzeitige sicherheitskritische Systeme, die auf Künstlicher Intelligenz (KI) basierenden Modellaussagen im Rahmen von Objekterkennung oder Zeitreihenanalysen aufbauen, weisen notwendigerweise ebenfalls

Unsicherheiten auf. Durch das Training der Algorithmen mit entsprechenden Trainingsdatensätzen entstehen Unsicherheiten, die bislang nicht verlässlich quantifiziert werden können. Hier besteht eine Fähigkeitslücke, die dazu führt, dass dasdurch die Verwendung von KI-Methoden bestehende Risiko in sicherheitskritischen Anwendungen und Systemen nicht nachvollziehbar quantitativ bewertet werden kann. Entsprechend zu entwickelnde und zu beschreibende KI-Komponenten können dann im weiteren Schritt Teil der im Aufbau befindlichen Ingenieurdisziplin zu KI werden – des KI-Engineering – und mit vertrauenswürdigen Leistungsgarantien und verlässlichen Merkmalen nach ingenieursmäßigen Vorgehensmodellen eingesetzt werden.

Explainable AI

Anwendungen aus dem Bereich der Künstlichen Intelligenz erobern immer mehr Einsatzbereiche, z. B. in der Energieversorgung oder im Katastrophenschutz. Gerade Modelle aus dem Bereich des Maschinellen Lernens, die durch den Menschen aufgrund ihrer Komplexität nicht mehr nachvollziehbar sind, besitzen oftmals eine hohe Performanz bei ausreichend guten Bedingungen und sind dadurch attraktiv für den Einsatz. Allerdings bieten sie einem Nutzer im Gegensatz zu regelbasierten Verfahren keine Möglichkeit, die Entscheidungsgrundlage für ein Ergebnis nachzuvollziehen. Methoden der Explainable AI liefern Ansätze, um punktuell das Verhalten und die Auffassung derartiger Algorithmen darzustellen. Hierdurch ergibt sich das Potenzial, mögliche Sicherheitsrisiken oder unzureichende Robustheit für außergewöhnliche Situationen zu erkennen.

Optimierter und überwachter Ressourceneinsatz beschränkter Güter im Krisenfall bzw. in der Krisenvorbereitung (FA02, FA08)

Durch die Zunahme von Krisensituationen mit globalen Auswirkungen (z. B. Umwelt: Dürren, Überschwemmungen; geopolitisch: Ukraine-Krieg; pandemisch: Corona) wird es immer wieder zu Unterbrechungen von Lieferketten und Ressourcenengpässen kommen. Hierbei wird es nötig werden, dass staatliche Organisationen die Verteilung und Überwachung von kritischen Ressourcen koordinieren. Dafür ist einerseits robuste, vertrauenswürdige Sensorik notwendig, die Ort, Zeit und Zustand von Ressourcen zuverlässig bestimmen kann. Andererseits braucht es computergestützte Optimierungsverfahren, welche eine schnelle Entscheidung zur optimalen Verteilung bzw. zum optimalen Einsatz von begrenzten Ressourcen/Gütern (z. B. Hilfsgütern, Notstromaggregaten, Personal, …) auch unter Unsicherheiten bzw. Prioritätensetzung erlauben. Aktuelle digitale Technologien, Entwicklungen im Bereich der mathematischen Optimierung sowie die Kombination mit Foresight-Methodiken lassen es zu, auch »Softwareprototypen« zu entwickeln, die später in kurzer Zeit für die jeweilige Krisensituation angepasst und zur Entscheidungsunterstützung eingesetzt werden können.

Methoden zum Schutz vor Missbrauch von KI- und autonomen Systemen (FA02, FA03, FA04)

Insbesondere im Bereich von KRITIS, aber auch in Bereichen der polizeilichen und nicht-polizeilichen Gefahrenabwehr werden die Einsatzmöglichkeiten von KI und autonomen Systemen zunehmend größer – sowohl auf Seiten der Einsatzkräfte als auf Seiten der zu schützenden Strukturen bzw. Gesellschaften. Dies schafft neue Abhängigkeiten und Verwundbarkeiten und eröffnet u. a. auch neue Angriffsflächen für eine mögliche Manipulation, woraus sich zahlreiche dringende Forschungsfragen ableiten lassen. So etwa die Frage, wie man Fahrzeuge mit autonomen Fähigkeiten (Autos, UAVs etc.) so sichert, dass sie nicht digital gekapert und für Anschläge missbraucht werden können. Auch aus dem Bereich der sozialen Medien lassen sich bisher wenig berücksichtigte, aber relevante Fragestellungen identifizieren, etwa zu sogenannten Adversarialen, also Manipulationen von Bildern und Texten, die die KI, aber nicht den Menschen zu Fehlanalysen verleiten. Die Nutzung derartiger Mittel kann weitreichende Folgen haben, etwas in der Fusion von Informationen zur Lagedarstellung oder bei der Überwindung von Filtern, die adversarial verfälschte Hass-Mails oder Aufrufe zu Gewalttaten nicht mehr erkennen.

Sichere Datenräume für KRITIS und die Gefahrenabwehr (FA02, FA12)

In Gesellschaft und Industrie ist der Bedarf an digitalen Plattformen, welche die Kontrolle und damit den strategischen Wert von Datenressourcen während des Austauschs und der Nutzung sicherstellen, seit Jahren von zunehmender Bedeutung. Durch die Vielzahl an verwendeten Standards, Qualitätsniveaus und unspezifischen rechtlichen Grundlagen sowie nicht zuletzt durch Sicherheitslücken in als vertrauenswürdig geltenden Systemen lassen sich allerdings vermehrt Vertrauensverluste gegenüber solchen Plattformen verzeichnen. Der Lösungsweg führt über die Schaffung von (dezentralen) Datenräumen nach höchsten anerkannten Sicherheits- und Vertrauensleveln. Mit Blick auf die zivile Sicherheit lässt sich in Anbetracht der Menge an sensitiven Daten, die im Bereich von KRITIS, aber auch der polizeilichen und nicht-polizeilichen Gefahrenabwehr anfallen können, ein sehr großer Bedarf feststellen, diese Daten, unter völliger Wahrung der Datensouveränität in Händen der Datenerzeuger, austauschen und nutzen zu können. Eine entsprechende Entwicklung von Konzepten und Technologien

sowie die langfristige Umsetzung und Implementierung, an die spezifischen Bedarfe sowie Nutzungs- und Rahmenbedingungen der Akteure der zivilen Sicherheit angepasst, ist erstrebenswert.

Quantencomputing für KRITIS und die Gefahrenabwehr (FA02, FA04, FA12)

Die zukünftige Entwicklung von in der Praxis einsetzbaren Quantenrechnern wird voraussichtlich die heute auch in zivilen Systemen eingesetzten IT-Sicherheitsmechanismen obsolet machen, da sie zu großen Teilen asymmetrische Kryptographie einsetzen, deren Sicherheit auf der Annahme beruht, dass bestimmte mathematische Probleme (wie das Faktorisieren großer Zahlen) nicht effizient lösbar sind – eine Annahme, von der bereits bekannt ist, dass sie bei Einsatz von Quantenrechner nicht mehr gelten wird. Gleichzeitig werden Quantenrechner wiederum neue Möglichkeiten für sichere Kommunikation (z. B. Quantentunnel) eröffnen, die wiederum auch in Gegenwart von Quantenrechnern sicher sein werden. Die Umstellung auf diese neuen Sicherheitstechnologien wird große technische Umwälzungen erfordern, die auch die kritischen Infrastrukturen betreffen wird. Daraus ergibt sich die Notwendigkeit, Ansätze für die sichere Transition der IT-Sicherheitsinfrastrukturen insbesondere beim Einsatz in kritischen Infrastrukturen zu erforschen, unter Berücksichtigung der Menge an sensitiven Daten, die im Bereich von KRITIS anfallen.

FA03 – Monitoring and surveillance of environments and activities

Datenschutzkonforme, intelligente Überwachung kritischer Infrastruktur (**FA01**, FA02, FA03)

Überwachung sensibler öffentlicher Bereiche mit CBRN-E-Sensoren (**FA01**, FA02, FA03, FA06, FA07)

Abwehrmöglichkeiten von zu Waffen missbrauchten autonomen UAS und Drohnenschwärmen im zivilen Raum (**FA01**, FA03, FA11)

Kombinierte Risiken und Kaskadeneffekte in kritischen Lieferketten verstehen und quantifizieren (**FA02**, FA03)

Metriken und Parameter für ein ganzheitliches Resilienzmanagement für Kommunen und Unternehmen (**FA02**, FA03)

Prognosefähigkeit bezüglich Auswirkungen von zukünftigen Extremwetterlagen im Zuge des Klimawandels (**FA02**, FA03, FA07, FA08)

Methoden zum Schutz vor Missbrauch von KI- und autonomen Systemen (**FA02**, FA03, FA04)

RF-Monitoring zur optimalen Nutzung des Funkspektrums

Im Zeitalter der drahtlosen Datenübertragung und der uneingeschränkten Nutzung elektronischer Medien sowie der satellitengestützten Navigation ist das hierfür genutzte elektromagnetische Spektrum (EMS) eine Schlüsselressource. Trotz bestehender Regulierungen zur Frequenznutzung und für den Immissionsschutz kommt es dabei immer wieder zu Störungen oder Einschränkungen bei der Datenübertragung. Die Gründe sind vielfältig und können neben der gezielten Störung auch von defekten Geräten, nicht den Abstrahlungsnormen entsprechenden Anlagen oder fehlerhafter Frequenznutzung ausgehen. Obwohl es hier bereits Lösungen zur Fehlersuche für konkrete Geräte oder aufwendige Frequenzanalysemethoden mit Großgerät gibt, fehlt es an kompakten, leistungsfähigen und universell einsetzbaren Methoden und Geräten zum zeitnahen lokalen Monitoring des EMS, sogenannten »RF-Scanner«. Deren Einsatzzweck ist die Detektion von Störungen und die Lokalisierung von Störquellen bzw. von problematischen Komponenten. In der Folge wird sich eine deutliche Verbesserung der lokalen EMS-Nutzung einstellen.

Schutz der Weltrauminfrastruktur

Staatliche Akteure nutzen in großem Maße weltraumgestützte Dienste zur Aufklärung, Überwachung kritischer Infrastrukturen, Kommunikation und Navigation. Häufig werden diese Dienstleistungen durch private Anbieter bereitgestellt und sind dadurch dem unmittelbaren staatlichen Zugriff entzogen. Bereits ein teilweiser Ausfall dieser Dienste könnte zu erheblichen Beeinträchtigungen der Sicherheit und des sozialen

Zusammenlebens führen. Um in Zukunft in Deutschland souverän agieren zu können, ist es von größter Bedeutung, diese kritischen Abhängigkeiten durch vorausschauendes, strategisches Handeln zu vermeiden und die Hoheit über sicherheitsrelevante Technologien zu erlangen oder zu stärken.

Mit steigender Abhängigkeit von diesen Diensten steigt auch die Bedeutung der Resilienz von Weltrauminfrastrukturen. Redundante Systemauslegung und Satellitenkonstellationen sowie robustes und zuverlässiges Systemdesign einerseits bzw. das rechtzeitige Erkennen nicht-kooperativen Verhaltens Dritter und die Härtung sämtlicher Komponenten gegen Eingriffe von außen (mittels Laser, EMP, Jamming etc.) andererseits sind von größter Wichtigkeit.

Ausfallsichere, robuste energieeffiziente Kommunikation für systemrelevante Infrastrukturdienste (FA03, FA12)

Die Vernetzung von Sensoren und Objekten im Internet der Dinge nimmt stetig zu und findet auch zunehmend Einsatz im Bereich kritischer Infrastrukturen; beispielsweise, um aus der Ferne den Überblick über den aktuellen Zustand von Assets (z. B. Transformatorstationen, Wasserstände von Flüssen) zu erhalten, um Schaltvorgänge in Steueranlagen von Energieversorgungsunternehmen auszulösen oder auch um notwendige Warenströme im Krisenfall bedarfsgerecht zu lenken.

Zunehmend hängen immer mehr kritische Infrastrukturen von dieser Vernetzung ab, die Sicherheit und Zuverlässigkeit spielt dabei eine übergeordnete Rolle. Die Anbindung der Sensoren und Objekte erfolgt dabei zunehmend durch sogenannte Low-Power-Wide-Area-Netzwerke. Aktuelle LPWAN-Technologien hängen dabei allerdings von einem funktionsfähigen Internet ab. Im Krisenfall kann mit den aktuell eingesetzten Lösungen keine Verfügbarkeit garantiert werden. Speziell bei Stromausfällen oder sonstigen, vor allem auch gezielt herbeigeführten Störungen des Internets fehlt die Möglichkeit zur autarken Überwachung und Steuerung von infrastrukturkritischen Komponenten.

Automatisierte Beobachtung und Erkennung von Fake-News, Desinformationskampagnen und Beeinflussungsversuchen über digitale Medien

Durch digitale Medien kann jeder einfach auf eine Vielzahl von Informationskanälen zugreifen, um sich zu informieren bzw. sich informiert zu fühlen und um Informationen, aber auch Meinungen und Desinformation zu verbreiten. Das Problem mit diesen scheinbar kostenlosen Angeboten ist jedoch, dass sie durch Werbeeinnahmen finanziert werden und teilweise entsprechend versucht wird, Klicks und damit Einnahmen daraus zu generieren. Längerfristige Ziele der sachlichen Berichterstattung und der Qualitätssicherung stehen dahinter zurück.

Das digitale Informationsumfeld ist zudem anfällig gegenüber Beeinflussung und kann dazu genutzt werden, gesellschaftliche Prozesse zu manipulieren. Gelangen einseitige oder falsche Informationen mit großer Verbreitung in Umlauf, kann dies wirtschaftliche Schäden anrichten, aber auch den demokratischen Rechtsstaat schwächen. Es ist daher wichtig, Entwicklungen im öffentlichen Informationsraum zu beobachten und Ereignisse zu erkennen, um daraus für das eigene Handeln zeitnah die richtigen Schlüsse zu ziehen. Hierfür werden Tools benötigt, mit denen die notwendigen Analysen wenigstens teilautomatisiert durchgeführt werden können.

Sichere Schifffahrt (**FA03**, FA04, FA07, FA08)

Der Transport von Waren per See wird für unsere Gesellschaft immer wichtiger, auch vor dem Hintergrund steigender Bezüge von Flüssiggas (LNG). Der Überwachung sowohl der Seestraßen als auch der Schiffe, und zwar insbesondere unter Wasser, kommt daher eine immer wichtigere Rolle zu. Anschläge auf ein einzelnes LNG-Terminal könnten die künftige Energieversorgung des ganzen Landes gefährden. Monitoring insbesondere mit optischen Technologien verknüpft mit KI kann Anschläge oder technische Havarien auf und in Schiffen und Häfen verhindern oder zumindest begrenzen und damit die Resilienz des Systems erhöhen.

FA04 – Security of information systems, networks and hardware

Resilienz in der Energieversorgung bei fortschreitendem Klimawandel (**FA01**, FA04)

Zivil-militärische Zusammenarbeit (**FA02**, FA04, FA12, FA13)

Sichere Schifffahrt (**FA03**, FA04, FA07, FA08)

Methoden zum Schutz vor Missbrauch von KI- und autonomen Systemen (**FA02**, FA03, FA04)

Quantencomputing für KRITIS und die Gefahrenabwehr (**FA02**, FA04, FA12)

Resilienz cyber-physikalischer Systeme

Konflikte zwischen Staaten- und Staatengruppen werden in Zukunft und vielleicht sogar bereits jetzt nicht mehr klar in eine »kalte« (politische Diskussion, Handelskonflikte, Zollabkommen etc.) und eine »heiße« (kriegerische Handlungen) Phase zu trennen sein. Bereits jetzt zeigt sich, dass teils in Vorbereitung von kriegerischen Konflikten, teils auch als probates Mittel des vorkriegerischen Konflikts Angriffe im Cyber- und Informationsraum auch auf Staatenebene oder durch diese motiviert durchgeführt werden.

Dies kann die bewusste Desinformation einer Bevölkerung zum Ziel haben – aber auch die Schwächung oder Dysfunktion der gesamten Infrastruktur eines Staats. Da Angriffe dieser Art nie zu hundert Prozent ausgeschlossen oder abgewehrt werden können, ist zu erforschen, wie cyber-physikalische Systeme so auszulegen sind, dass deren Reaktion auf Angriffe mit minimalen, lokal begrenzten oder begrenzbaren Schäden einhergeht. Kurzum: Wie kann sich die Bundesrepublik Deutschland resilient gegen Cyberangriffe im obigen Sinne aufstellen?

Frühzeitige Schwachstellenerkennung durch automatisierte Testverfahren

Zum Zweck der automatisierten Schwachstellenerkennung kommt in letzter Zeit zunehmend Fuzzing zum Einsatz. Fuzzing ist ein automatisiertes Testverfahren, welches durch mehr oder weniger zufällige Testfälle versucht, Schwachstellen aufzudecken. Zum jetzigen Zeitpunkt wird Fuzzing schon an einigen Stellen eingesetzt, jedoch ist es für einen Endanwender noch mit einem hohen Zeit- und Arbeitsaufwand verknüpft. Weiterhin stellen moderne, zustandsbehaftete Komponenten durch ihre Komplexität aktuell noch Herausforderungen für einen effektiven Einsatz von Fuzzing dar.

Durch weitere Forschung wird ermöglicht, Fuzzing als automatisiertes Testverfahren weiter zu verbreiten um damit die allgemeine Sicherheit von IT-Systemen wie kritischen Infrastrukturen zu verbessern. Die zu bewältigenden Herausforderungen bestehen dabei insbesondere darin, Methoden zur effizienten Extraktion und zum gezielten Einsatz von Zustandsmodellen, möglicherweise unter Zuhilfenahme von ML-Verfahren, zu entwickeln. Zu diesem Zweck muss u. a. auch die nichtdeterministische bzw. parallele Ausführung der zu testenden Komponenten berücksichtigt werden.

Human-in-the-Loop-basierte Intrusion Detection für Energiesysteme

Die ausschließliche Verwendung Künstlicher Intelligenz in sicherheitskritischen Anwendungen führt aufgrund der eingeschränkten Datenverfügbarkeit sowie der oftmals speziellen Daten- und Prozesscharakteristika in einigen Fällen zu suboptimalen und nicht vertrauenswürdigen Ergebnissen. Für eine bessere Integration in bestehende IT-Sicherheitsmanagementsysteme wird eine stärkere Verschneidung mit menschlichem Expertenwissen benötigt, um die KI-basierten Überwachungslösungen auf die individuellen Gegebenheiten auf Grundlage eines »Human-in-the-Loop«-Ansatzes besser anzupassen. Hierzu werden KI-basierte NIDS-Anwendungen um ein interaktives Experteninterface erweitert, welches zum einen den Informationsfluss vom KI-System zum Benutzer um Erklärbarkeits- und Unsicherheitsindikatoren erweitert und zum anderen einen Rückkanal vom Benutzer zum KI-System über einen Feedback-Mechanismus ermöglicht. Somit können auch nach Abschluss einer initialen Trainingsphase nachträgliche Anpassungen am KI-Modell durch Bewertungs- oder Annotationsmechanismen erfolgen.

Sichere Navigation ohne Navigationssatellitensysteme (FA04, FA08, FA09)

Globale Satellitennavigationssysteme (GNSS) stellen heute das weltweit wichtigste System zur Positionsbestimmung und Ortung dar. Es existiert dazu keine praktikable Alternative, welche in Bezug auf Zuverlässigkeit, Kostenaufwand oder Genauigkeit mit diesen Systemen vergleichbar ist. Aufgrund des technischen Fortschritts sind Angreifer jedoch inzwischen bereits mit geringem technischen und finanziellen Aufwand in der Lage, GNSS-Koordinaten böswillig und unentdeckt zu manipulieren und zu fälschen (engl. »Spoofing«). Entsprechendes elektronisches Equipment und Anleitungen sind offen im Internet verfügbar. Ein Angreifer kann so leicht ein Fahrzeug oder ein Schiff vom Kurs abbringen, um es zu beschädigen oder abzufangen. Satellitenkonstellationen sind zudem zunehmend der Gefahr der Zerstörung durch Weltraumschrott ausgesetzt; darüber hinaus sind viele Nationen technisch in der Lage, Satelliten im Orbit anzugreifen. Um die Auswirkungen von Navigations-Spoofing oder eines Ausfalls der GNSS zu verringern, sollten alternative, nicht von GNSS abhängige Technologien zur Positionierung erforscht und entwickelt werden.

Intelligente Unterdrückung illegaler Kommunikationsverbindungen (FA04, FA12)

Die unerlaubte Nutzung von Mobilfunkgeräten – insbesondere von Mobiltelefonen – ist ein Sicherheitsrisiko, das in vielen sicherheitsrelevanten Einrichtungen besteht, z. B. in Regierungsgebäuden, Gerichten, Justizvollzugsanstalten. Die illegale Kommunikation mittels drahtloser Sendegeräte dient dabei sowohl kriminellen Aktivitäten wie Drogenhandel oder Zeugenbeeinflussung als auch Spionagezwecken. Sicherheitskräfte fordern daher seit Langem robuste Technologien zum Blockieren und Stören illegaler elektronischer Übertragungen, die jedoch den Betrieb der regulären Systeme im Gebäude oder im Umfeld des Einsatzes nicht beeinträchtigen sollten. Künftige RF-Störungstechnologien sollen daher »intelligenter« sein als bestehende »Brute-Force«-Techniken mit hoher Sendeleistung und keine Störungen oder Dienstausfälle für Dritte verursachen. Ein weiteres Anwendungsgebiet solcher intelligenter Störtechnologien ist die Abwehr von Drohnenangriffen, bei der das Fernsteuerungssignal des Fluggeräts unterdrückt wird.

Hybride KI-basierte Intrusion-Prevention-Systeme für cyber-physische Systeme

Im Zuge der Digitalisierung von Systemen, wie z. B. Produktionssystemen oder zukünftigen Innenstadtlösungen, werden Automatisierungssysteme zunehmend sowohl untereinander als auch mit Unternehmensnetzwerken sowie dem Internet vernetzt. Diese komplexen Systemlandschaften ergeben neue Gefahren für Automatisierungssysteme hinsichtlich der IT-Sicherheit, die man sonst bereits aus dem klassischen IT-Bereich kennt. Problematisch dabei ist, dass bestehende industrielle Kommunikationsprotokolle und Automatisierungssysteme häufig ohne ausreichende Schutzmaßnahmen wie Authentifizierung, Autorisierung oder Verschlüsselung entwickelt wurden. Zudem ist die Nachrüstung bestehender Systeme aufwendig und teuer. Durch weitere Forschung können selbstlernende Sicherheitslösungen Automatisierungssysteme schützen. Das Lernen des Normalverhaltens von technischen Anlagen aus den Prozessdaten dient zur Erkennung von Anomalien. Mustererkennungsalgorithmen können Angriffsmuster in den Kommunikationsdaten erkennen. Basierend auf Fusionsmodellen, die Ergebnisse der zuvor genannten Algorithmen intelligent zusammenführen, können Handlungsempfehlungen für die Betreiber der Systeme abgeleitet und automatisierte Verteidigungsmaßnahmen eingeleitet werden.

Bewertung von Sicherheitsvorfällen für cyber-physische Systeme

Cyber-physische Systeme bestehen aus verteilten und miteinander vernetzten Teilsystemen, die weitgehend durch ebenfalls verteilte Automatisierungskomponenten wie z. B. Steuerungen, Sensoren und Aktorengesteuert und überwacht werden. Der zuverlässige Betrieb dieser Systeme hängt u. a. direkt von dem Funktionieren der Kommunikationsnetze ab. Mit Netzwerkanalysesystemen können heute die Kommunikation zwischen Komponenten überwacht und Sicherheitsvorfälle detektiert werden. Ein vom Netzwerkanalysesystem detektierter Sicherheitsvorfall wird dann durch das Servicepersonal zunächst bewertet, bevor eine Handlungsmaßnahme festgelegt wird. Dieser Vorgang dauert heute in der Regel mehrere Stunden, da das Servicepersonal zunächst zum Ort des betroffenen Systems (großflächig verteilte Systeme in Städten und ländlichen Regionen) fahren und ggf. Ersatzteile besorgen muss. Die Interpretation der Warnmeldungen und der Rückschluss auf die Ursache gerade bei Netzwerkproblemen ist zum einen allgemein sehr schwer und erfordert zum anderen ein hohes Level an IT-Expertise.

Durch weitere Forschung können selbstlernende Bewertungssysteme das Servicepersonal unterstützen, um geeignet auf Sicherheitsvorfälle zu reagieren. Das Lernen eines Ereignismodells aus Ereignisberichten und das Lernen eines Netzwerkmodells aus Netzwerkereignissen dienen als Grundlage eines Bewertungssystems. Das Bewertungssystem kann nun Korrelation bilden und Handlungsempfehlungen generieren.

Auswirkungen von elektromagnetischen Störsignalen auf Sensorik und Informationssicherheit

Elektronische Geräte sind in vielen zivilen und behördlichen Ausstattungen eingebaut, um die jeweilige Funktion zu unterstützen oder erst möglich zu machen. Der Betrieb von elektronischen Systemen, welche einen zunehmenden Grad an Automatikfunktionen aufweisen, basiert auf einem kontinuierlichen Zugriff auf Messdaten von entsprechenden Sensoren wie beispielsweise Ströme und Spannungen, aber auch Beschleunigungen, Bild- und Positionsdaten oder auch CBRN-Messdaten. Die Sensoren bilden zusammen mit den Kommunikationsschnittstellen sowie der weiteren Datenverarbeitung ein Sensorsystem. Durch eine elektromagnetische Störeinkopplung in die Sensorsysteme können hierdurch beispielsweise Unterdrückungen, aber auch signifikante Beeinflussungen der bereitgestellten Daten verursacht werden. Diese Manipulationen der Sensordaten sind vor allem im Kontext von autonomen Systemen, CBRN-Sensoren, Füllstandsensoren, optischen Sicht- und Zielführungssystemen oder auch taktisch eingesetzten, unbeaufsichtigten Bodensensoren als kritisch anzusehen.

Automatisiertes Asset- und Patchmanagement

Kritische Infrastrukturen sind aufgrund ihrer Komplexität, aber auch durch ihre Bedeutung für die nationale Sicherheit ein attraktives Ziel für Cyberangriffe. Diese nutzen dabei sowohl prozessuale als auch technische Schwächen aus, so dass die IT- und OT-Sicherheit in kritischen Infrastrukturen nicht nur unter Berücksichtigung netzwerk- und hostspezifischer Schwächen, sondern auch unter Überprüfung operativer Prozesse und Zulieferbeziehungen erfolgen muss. Es besteht daher die Notwendigkeit der Erforschung von Verfahren zur gezielten und automatisierten Identifikation von Prozessen, Systemen und weiteren Assets kritischer Infrastrukturen, um gegen deren Schwächen gezielt vorgehen zu können. Personalintensive Prozesse wie das Vulnerability-, Asset- und Patch-Management sind dann mit weniger Ressourcenverbrauch und wirtschaftlich nachhaltig durchführbar.

FA05 – Physical access control

Sichere und vertrauenswürdige Identitäten (FA05, FA06, FA07)

Sichere und vertrauenswürdige Identitäten sind eine wesentliche Voraussetzung zur Identifizierung und Authentisierung von Personen und Dingen in digitalen wie analogen Prozessen. Damit stellen sie eine wesentliche Grundlage für die Gewährleistung von Sicherheit dar, sei es bei Grenzkontrollen, für die physische Zugangskontrolle zu kritischen Infrastrukturen oder zur Absicherung der Integrität der an kritischen Prozessen beteiligten Maschinen. Dies erfordert verlässliche Technologien, welche die digitale Souveränität der deutschen und europäischen Wirtschaft sowie Gesellschaft gewährleisten.

FA06 – Identification and authentication of persons, assets and goods

Überwachung sensibler öffentlicher Bereiche mit CBRN-E-Sensoren (**FA01**, FA02, FA03, FA06, FA07)

Sichere und vertrauenswürdige Identitäten (**FA05**, FA06, FA07)

FA07 – Detection of goods, substances, assets and people and incidents

Überwachung sensibler öffentlicher Bereiche mit CBRN-E-Sensoren (**FA01**, FA02, FA03, FA06, FA07)

Prognosefähigkeit bezüglich Auswirkungen von zukünftigen Extremwetterlagen im Zuge des Klimawandels (**FA02**, FA06, FA08)

Sichere Schifffahrt (**FA03**, FA04, FA07, FA08)

Sichere und vertrauenswürdige Identitäten (**FA05**, FA06, FA07)

Automatische Detektion von verbotenen Gegenständen

Im Rahmen diverser Sicherheitsforschungsprogramme auf sowohl nationaler als auch EU-weiter Ebene wurde über den Zeitraum der letzten 10 Jahre eine robuste Sicherheitsinfrastruktur für den Einsatz in der zivilen Luftfahrt in den Bereichen Gepäckkontrolle, Personenkontrolle und Güterkontrolle hinsichtlich der Detektion von Explosivstoffen aus dem militärischen und zivilen Bereich sowie von Selbstelaboraten („home made explosives“, HME) etabliert. Die Methoden von potenziellen Attentätern und Organisationen mit terroristischem Background werden jedoch stetig weiterentwickelt. Daraus lässt sich die Notwendigkeit der frühzeitigen Identifizierung von Bestandteilen möglicher verbotener Gegenstände ableiten.

Zielsetzung ist die Entwicklung von KI-gestützten Detektionsalgorithmen, welche automatisch Schusswaffen, Granaten, Zünder, Munition usw. in allen Lagen und Zustandsformen (komplett oder zerlegt) detektieren. Die gesetzte Aufgabe ist prädestiniert für die Entwicklung einer Mustererkennung, welche mit Hilfe einer großen Anzahl an Bildern und selbstlernenden Algorithmen durch KI erreicht werden kann.

Charakterisierung von chemischen Substanzen, die toxische Gase ausbilden können

Basierend auf dem Hintergrund des vorab beschriebenen Bedarfs einer automatischen Detektion von verbotenen Gegenständen lässt sich analog ein zweites Bedrohungsszenario ableiten, für das aktuell eine Forschungslücke besteht: die Verwendung von chemischen Stoffen, welche unter Zugabe von Wasser oder Säure toxische Gase freisetzen. Es besteht ein Bedarf, umfänglich die potenziellen Gasbildner zu erfassen; dabei sollten die folgenden kritischen Parameter erforscht werden:

- Freisetzungsreaktion (Welche Edukte werden benötigt, um die toxischen Stoffe freizusetzen?)
- Gasbildungsrate (Wieviel toxisches Gas wird über einen definierten Zeitraum freigesetzt?)
- Ausbreitung auf Basis der physikalischen und chemischen Parameter (z. B. schwerer oder leichter als Luft)
- Risikoabschätzung für bestimmte Räume (z. B. Flugzeug (Passagierkabine, Frachtraum); Zugwagons, Bus, Passagierschiffe, Innenräume von Gebäuden)
- Risikoabschätzung für den Menschen (medizinische Aspekte)

Datenerfassung für integratives, echtzeitfähiges und datenschützendes Resilienzmanagement (FA07, FA08)

Organisationen und Unternehmen, aber auch Städte und Gemeinden stehen zunehmend unter dem Druck, auf sich schnell entwickelnde Lagen zielgenau und angemessen zu reagieren zu können. Dabei fehlen jedoch zumeist Kernindikatoren, anhand derer Entscheidungen getroffen werden können. Um dieses Problem zu adressieren, sind Informationen aus einer Vielzahl an heterogenen Daten abzuleiten, welche die Entscheidungen in jeder Phase des Resilienzzykluses (Vorbereiten – Vorbeugen – Schützen – Bewältigen – Wiederherstellen) optimieren können. Dies erstreckt sich von der Sichtbarkeit von Waren innerhalb einer Lieferkette bis zu sich schnell entwickelnden Krisen in Großstädten. Gleichzeitig stehen diese Konzepte in einem Spannungsfeld mit der Akzeptanz einzelner Stakeholder (z. B. Bürger in Bezug auf Datenschutz).

Unabhängige systematische Überprüfung und Evaluation von CBRNE-Detektoren und Detektionssystemen

CBRNE-Detektoren und Detektionssysteme müssen im realen Einsatz viele Kriterien erfüllen, die oftmals nicht unabhängig getestet werden. Insbesondere wäre hier auch eine stärkere Einbeziehung von Endanwendern und anderen Experten für den Einsatz wünschenswert. Dazu müssten unabhängige Testlabore aufgebaut und gefördert werden und die Entwicklung von Testkonzepten und Testvorrichtungen sowie die Anpassung von Standards (z. B. ANSI) etc. vorangetrieben werden. Das würde letztlich die Fähigkeit erhöhen, im Ernstfall Bedrohungen zu detektieren und rasch zu bewerten.

Detektion von elektromagnetischen Störangriffen

Wird über elektromagnetische Wellen zusätzliche Energie in ein elektronisches Gerät eingebracht, so ergeben sich bei Überschreiten seiner frequenzspezifischen Empfindlichkeitsschwellen Störungen der Funktion bis hin zur Beschädigung. Tatsächlich lassen sich starke zivile Hochfrequenzsendeanlagen für schädliche Fernwirkungen zweckentfremden. In der Militärforschung werden zudem dedizierte Störquellen für High Power Electromagnetics (HPEM) entwickelt. Eine solche Bedrohung kann gerade im Falle von Schlüsselsystemen in kritischen Infrastrukturen über ein ganzheitliches Schutzkonzept adressiert werden. Neben organisatorischen, baulichen und technischen Bestrebungen zur Abmilderung solcher Schadwirkungen ist auch ein geeignetes Detektionssystem, welches überhaupt erst Aufschluss über die Ursachen ansonsten unspezifischer Gerätefehlfunktionen gibt, essentiell.

Neben der technischen Entwicklung eines elektromagnetisch robusten Detektionssystem für HPEM-Angriffe sind auch weitere Überlegungen zur Einbindung eines Detektionssystems in kritische Infrastrukturen notwendig.

Oberflächenschutz

Eine Vielzahl von physikalischen, chemischen, biologischen oder elektromagnetischen Angriffen auf Geräte und Menschen erfolgt durch Einwirkung auf Oberflächen. Beispiele sind starke elektromagnetische Impulse oder Strahlung (Blackout von Geräten), Laserstrahlung hoher Intensität (Blendung von Piloten sowie von empfindlichen optischen Systemen, insbesondere in der Luft), Kontamination durch Giftstoffe etc. Moderne, innovative Schutzausrüstung von Material und dessen Oberflächen sowohl für Menschen als auch für kritische Systeme (Satelliten, Drohnen) kann die Gesundheit und Funktionalität von optischen Systemen schützen. Beispiele können Laserschutzbeschichtungen für Helmvisiere, EMV-Schutzbeschichtungen oder auch antivirale oder -mikrobielle Beschichtungen bzw. Oberflächenbehandlungen sein.

FA08 – Positioning and localisation, tracking and tracing

Erkennung von Lebenszeichen und Lokalisierung von Verschütteten (**FA01**, FA08)

Prognosefähigkeit bezüglich Auswirkungen von zukünftigen Extremwetterlagen im Zuge des Klimawandels (**FA02**, FA03, FA07, FA08)

Sichere Navigation ohne Navigationssatellitensysteme (**FA04**, FA08, FA09)

Datenerfassung für integratives, echtzeitfähiges und datenschützendes Resilienzmanagement (**FA07**, FA08)

Sichere Schifffahrt (**FA03**, FA04, FA07, FA08)

Smarte Schwingungskontrolle zur Steigerung von Präzision, Kompatibilität und Effizienz

In beweglichen, insbesondere mobilen Systemen zu Land, Luft und Wasser werden empfindliche Instrumente in deren schwingungsbehafteter Einsatzumgebung durch systemintern oder -extern generierte Störungen belastet. Plakatives Beispiel sind instrumentierte Drohnen, die mit oft empfindlichen sensorischen Instrumenten ausgerüstet werden. Dies führt meist zu negativen Effekten in der betrieblichen Nutzung wie reduzierter Präzision und Auflösung. Deren Mitigation erfordert teils aufwendige, schwere oder empfindliche, präzise abgestimmte mechanische Isolationslösungen. Dies kann am Beispiel der vorgenannten Drohne zu eingeschränkter Robustheit oder verminderten Einsatzzeiten, zu wenig effizienter Rekonfiguration der erforderlichen Instrumente oder zu reduzierter Performanz führen.

Aktive Lösungen zur smarten Schwingungsisolation erlauben eine schnelle Anpassung schwingungstechnischer Systemeigenschaften sowohl vor als auch während des Betriebs. Gleichzeitig können diese smarten Systeme für die Überwachung der technischen Systeme verwendet werden. Dies erweitert und flexibilisiert die Einsatzmöglichkeiten des Zielsystems.

GNSS-lose Navigation unbemannter Flugsysteme

Bis zur Mitte der 2030er – so der Plan der europäischen Luftfahrtbehörden – sollen sich autonome Luftfahrzeuge den Luftraum gleichwertig mit bemannten Luftfahrzeugen teilen. Damit sie selbstständig ihr Ziel finden und nicht mit anderen Flugverkehrsteilnehmern kollidieren, brauchen sie ein gutes Verständnis von ihrer eigenen Position und der der anderen. Eine Kombination aus Satellitennavigation (GNSS) und funkbasiertem Traffic Management (UTM) bietet hierfür eine skalierbare und kostengünstige Lösung. Was passiert jedoch, wenn die Funkverbindung zum Tower abbricht? GNSS und drahtlose Kommunikation sind leicht zu stören und stellen ohne Rückfallebene ein erhebliches Sicherheitsrisiko für die Luftfahrt dar. Eine autonome Luftfahrt braucht daher autarke Lösungen für die Navigation und Umfelderkennung wie z. B. optische Navigationsverfahren. Diese sollen so weiterentwickelt werden, dass sie eine jederzeit einsetzbare Alternative zur Satellitennavigation bei Tag, Nacht und schlechter Sicht darstellen. Ihr Vorteil ist, dass sie ohne weitere Infrastruktur wie z. B. Funkemitter auskommen und nur schwer zu stören sind.

FA09 – Mobility and deployability

Sichere Navigation ohne Navigationssatellitensysteme (**FA04**, FA08, FA09)

Methodik zum nachhaltigen Schutz kritischer Logistiknetzwerke (**FA01**, FA09)

Der Schutz kritischer Infrastrukturen wird oft in Bezug auf die Ursache oder das Phänomen einer plötzlichen und umfassenden Beeinträchtigung untersucht. Forschung zur Kritikalität der transportierten Warenflüsse sowie zur Resilienz der genutzten Infrastruktur über die direkt betroffene Region hinaus ist hingegen selten.

Oft sind es kleinere Risiken (wie Unfälle), die zur Einschränkung der logistischen Infrastruktur oder zu Versorgungsengpässen führen. Ferner zeigt sich die Verwundbarkeit logistischer Infrastrukturen, wenn sie aufgrund von meteorologischen Bedingungen oder Schäden über einen längeren Zeitraum kaum nutzbar sind. Der Netzwerkcharakter der gesellschaftlich relevanten Grundversorgung, die über die logistische Infrastruktur organisiert wird, wird durch die aktuelle Forschung nicht hinreichend berücksichtigt.

Es besteht folglich eine Forschungslücke. Um diese zu schließen, braucht es eine Methodik, die Infrastrukturen und die darauf fließenden Warenströme betrachtet und so bewertet, welche Elemente und Teilnetzwerke so kritisch für das logistische System sind, dass deren Schutz eine besondere Wichtigkeit erlangt.

FA010 – Investigation and forensics

Post-Blast-Spurenanalyse – Zielverbindungen militärischer, ziviler und sogenannter Homemade-Explosivstoffe

Sowohl im militärischen (z. B. bei sogenannten Friedenseinsätzen der Bundeswehr) als auch im zivilen Bereich (z. B. bei der forensischen Spurensicherung durch das BKA) besteht ein großes Interesse daran, Schadens- oder Anschlagsereignisse auf Basis der forensischen Spurenanalyse zu rekonstruieren und aufzuklären, mit der Zielsetzung, sich proaktiv auf zukünftige Szenarien vorzubereiten. Im Fokus stehen hier die Analyse von Spuren nach einer Explosion, um herauszufinden, welche Stoffe zum Einsatz gekommen sind bzw. wie der Aufbau und die Wirkweise der improvisierten Sprengvorrichtung waren.

FA011 – Decontamination and neutralisation

Abwehrmöglichkeiten von zu Waffen missbrauchten autonomen UAS und Drohnenschwärmen im zivilen Raum (**FA01**, FA03, FA11)

Löschdrohnen zur Bekämpfung von Waldbränden (**FA01**, FA11)

Einbezug von Bürgerinnen und Bürgern in Forschung rund um den Katastrophenschutz: Nutzung von Citizen Science (**FA01**, FA02, FA11, FA12)

FA012 – Secure and public communication, data and information exchange

Einbezug von Bürgerinnen und Bürgern in Forschung rund um den Katastrophenschutz: Nutzung von Citizen Science (FA01, FA02, FA11, FA12)

Zivil-militärische Zusammenarbeit (FA02, FA04, FA12, FA13)

Sichere Datenräume für KRITIS und Gefahrenabwehr (FA02, FA12)

Quantencomputing für KRITIS und die Gefahrenabwehr (FA02, FA04 FA12)

Ausfallsichere, robuste energieeffiziente Kommunikation für systemrelevante Infrastrukturdienste (FA03, FA12)

Intelligente Unterdrückung illegaler Kommunikationsverbindungen (FA04, FA12)

Fehlende oder irreführende Kenntnisse über radiologische Gefahren und Bedrohungen in der Bevölkerung

Radioaktivität und die hiermit einhergehenden Gefahren sind in weiten Kreisen der Bevölkerung mit irreführenden Vorstellungen verbunden. Das kann im CBRN-E-Ernstfall zu problematischen (Über-)Reaktionen führen und die Lage verkomplizieren. Breitangelegte Informations- und erprobte Trainingsangebote für die Bevölkerung könnten hier Abhilfe schaffen.

FA013 – Training and exercises

Zivil-militärische Zusammenarbeit (FA02, FA04, FA12, FA13)

Ungenügendes Training für First Responder in Bezug auf RN-Detektion

Einsatzkräfte vor Ort wie Feuerwehr oder Polizei sind vielfach nur ungenügend für die Detektion von radioaktiven Stoffen ausgebildet. Insbesondere ein Training mit echten Quellen für alle First Responder – nicht nur Multiplikatoren – wäre wünschenswert. Zumindest simulierte oder virtuelle Quellen könnten in solchen Trainingseinheiten genutzt werden, auch, wo möglich, mit Einbeziehung nuklearen Materials. Dazu müssten Trainingskonzepte entwickelt und entsprechende Einrichtungen ertüchtigt werden.

Impressum

Herausgeber
Prof. Dr.-Ing. Reimund Neugebauer
Präsident der Fraunhofer-Gesellschaft

Prof. Dr.-Ing. Jürgen Beyerer
Vorsitzender Fraunhofer-Leistungsbereich Verteidigung, Vorbeugung und Sicherheit VVS

Prof. Dr. Michael Lauster
Stellvertretender Vorsitzender Fraunhofer-Leistungsbereich Verteidigung, Vorbeugung und Sicherheit VVS

Prof. Dr. Peter Martini
Stellvertretender Vorsitzender Fraunhofer-Leistungsbereich Verteidigung, Vorbeugung und Sicherheit VVS

Autoren
Isabelle Linde-Frech
Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT

Dr. René Bantes
Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT

Redaktion
Caroline Schweitzer
Geschäftsführerin Fraunhofer-Leistungsbereich Verteidigung, Vorbeugung und Sicherheit VVS

Bildquellen: Cover, iStock

Layout: Silke K. Schneider

Mit Beiträgen der Fraunhofer-Institute
- für Angewandte Festkörperphysik IAF
- für Betriebsfestigkeit und Systemzuverlässigkeit LBF
- für Chemische Technologie ICT
- für Hochfrequenzphysik und Radartechnik FHR
- für Integrierte Schaltungen IIS
- für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
- für Kurzzeitdynamik, Ernst-Mach-Institut, EMI
- für Naturwissenschaftlich-Technische Trendanalysen INT
- für Optronik, Systemtechnik und Bildauswertung IOSB

Und Beiträgen der Fraunhofer-Verbünde
- Energietechnologien und Klimaschutz
- Innovationsforschung
- IUK-Technologie
- Light & Surfaces

Fraunhofer-Gesllschaft e. V.
Hanastr. 27 c
80686 München

www.fraunhofer.de