Fraunhofer

FORTFÜHRUNG DER ZIVILEN SICHERHEITSFORSCHUNG

POSITIONSPAPIER DER FRAUNHOFER-GESELLSCHAFT

INHALT

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

Prof. Dr.-Ing. Jürgen Beyerer
Vorsitzender Fraunhofer-Verbund
Verteidigungs- und Sicherheitsforschung VVS

Prof. Dr. Peter Martini
Stellvertretender Vorsitzender Fraunhofer-Verbund
Verteidigungs- und Sicherheitsforschung VVS

Autoren
Daniel Hiller
Fraunhofer-Institut für Kurzzeitdynamik,
Ernst-Mach-Institut, EMI

Dr. Tobias Leismann
Fraunhofer-Institut für Kurzzeitdynamik,
Ernst-Mach-Institut, EMI

Redaktion
Caroline Schweitzer
Geschäftsführung Fraunhofer-Verbund
Verteidigungs- und Sicherheitsforschung VVS

Mit Beiträgen der Fraunhofer-Institute
– für Angewandte Festkörperphysik IAF
– für Hochfrequenzphysik und Radartechnik FHR
– für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
– für Kurzzeitdynamik, Ernst-Mach-Institut, EMI
– für Naturwissenschaftlich-Technische Trendanalysen INT
– für Optronik, Systemtechnik und Bildauswertung IOSB
– für Integrierte Schaltungen IIS
– für System- und Innovationsforschung ISI

Titelbild © iStock

© Fraunhofer-Gesellschaft e.V., München 2016

EXECUTIVE SUMMARY

© iStock

Sicherheit ist und bleibt eines der wichtigsten Bedürfnisse unserer Gesellschaft. Aufgrund veränderlicher Bedrohungen ist dieses Thema nach wie vor hochaktuell. Die zivile Sicherheitsforschung ist in Deutschland als querschnittliche Forschungsdisziplin erfolgreich etabliert. Von Beginn an eingebettet in die Hightech-Strategie der Bundesregierung, tragen viele Akteure aus Wissenschaft, Forschung, Wirtschaft, Behörden und Sicherheitsorganisationen in Verbundprojekten zur Erarbeitung konkreter Lösungen zur Bewältigung komplexer Herausforderungen bei. Letztere haben sich gerade in jüngster Vergangenheit aufgrund sicherheitspolitischer, gesellschaftlicher und technologischer Veränderungen stark erweitert. Das neue Forschungsprogramm der Bundesregierung ab 2017 muss diesen Veränderungen strukturell und inhaltlich zusätzlich Rechnung tragen.

Die aus Sicht der Fraunhofer-Gesellschaft dafür notwendigen Leitlinien sind:

Sicherheit – Resilienz – Nachhaltigkeit

Durch das Konzept der Resilienz wird im Sinne einer konsequenten Weiterentwicklung der Sicherheitsforschung die Verknüpfung zwischen Sicherheit und Nachhaltigkeit geschaffen. Das bedeutet für die Zukunft: Alle gesellschaftlich relevanten Systeme als Ganzes werden resilient, also widerstandsfähig, robust, lern- und anpassungsfähig sein müssen.

Starke Forschungsstandorte strukturell fördern

Mittlerweile haben sich in Deutschland exzellente Forschungsstandorte und -organisationsformen mit ausgeprägten Profilen und interdisziplinären Arbeitsgruppen etabliert. Im Sinne einer Exzellenzförderung gilt es, etablierte und neue Standorte durch spezielle Formate auch strukturell zu unterstützen, um Spitzenforschung auszubauen und dauerhaft zu sichern.

An internationale Flaggschiff-Initiativen anknüpfen

Parallel zu nationalen Anstrengungen wurden in Europa und weltweit wegweisende Initiativen, Projekte und Netzwerke etabliert. Um die Stärke des Forschungs- und Innovationsstandorts Deutschlands zu erhalten und auszubauen, müssen der Anschluss an diese Entwicklungen und internationale Vernetzungsaktivitäten noch stärker unterstützt werden.

Technologische Durchbrüche ermöglichen

Die Optimierung und Weiterentwicklung von Technologien und Konzepten für unterschiedliche Endnutzer sind wichtig und richtig. Dennoch braucht es daneben auch Förderformate, die bahnbrechende Technologieentwicklungen ermöglichen.

Stärkung der gesamten Hightech-Strategie durch Sicherheitsforschung

Wichtige Schnittstellen zwischen anderen Themenfeldern und dem Thema Sicherheit, wie Energiewende und Sicherheit, Mobilität und Sicherheit, digitale Wirtschaft und Sicherheit, bedürfen spezieller Förderung, um die Souveränität in Schlüsseltechnologiebereichen zu halten und auszubauen.

Fähigkeiten gezielt entwickeln

Sicherheitsforschung muss am operationellen Bedarf orientiert sein, um Innovationen hervorbringen zu können. Dies kann nur gewährleistet werden, wenn die Bedarfe der unterschiedlichen Nutzer in standardisierter Weise analysiert und Lösungen in engster Abstimmung mit dem Endnutzer entwickelt und getestet werden. Hier muss eine stärkere Integration von operationellem Bereich und analytischer Forschungsplanung durch entsprechende Kooperationsmodelle gefördert werden.

ZEHN JAHRE SICHERHEITSFORSCHUNG IN DEUTSCHLAND – EINE ERFOLGSGESCHICHTE

Als Reaktion auf eine bis dato in Dimension und Auswirkung völlig neue Bedrohungslage nach den Anschlägen von New York (2001), Madrid (2004) und London (2005) wurde parallel zum ersten europäischen Sicherheitsforschungsprogramm im Jahr 2007 das erste zivile Sicherheitsforschungsprogramm in Deutschland ins Leben gerufen. Zunächst noch geprägt vom klassischen Sicherheitsparadigma der Gefahrenabwehr und des Schutzes von Bürgern, Infrastrukturen und der Wirtschaft vor Bedrohung durch Terrorismus und organisierter Kriminalität, erfuhr das neue Programm von 2012 bis 2017 bereits eine deutliche Erweiterung. Das bezog sich sowohl auf das Verständnis von Sicherheit in ihren verschiedenen Dimensionen, als auch auf die in den Forschungsvorhaben zu adressierenden Herausforderungen. Die wichtigsten Eckpunkte dieser Weiterentwicklung lassen sich aus Sicht der Fraunhofer-Gesellschaft wie folgt zusammenzufassen:

Sicherheit der digitalen Evolution. Mit den Möglichkeiten, die die digitale Vernetzung von Privatpersonen, Unternehmen, Infrastrukturbetreibern und Sicherheitsbehörden bietet, steigen auch die damit verbundenen Risiken durch Missbrauch und Manipulation.

Resilienz als umfassender Ansatz für nachhaltige Sicherheit. Entgegen idealistischen Vorstellungen einer umfassend sicheren Welt findet zunehmend das Konzept der resilienten Gesellschaft Eingang in Forschungsprogramme weltweit. Die Implementierung von Resilienz ist ein Ansatz zur vorausschauenden, nachhaltigen Gewährleistung und stetigen Verbesserung der Sicherheit. Definiert wird Resilienz als die Fähigkeit bzw. Eigenschaft technischer und soziotechnischer Systeme, sich auf widrige Ereignisse vorzubereiten, sie einzukalkulieren, sie – wenn möglich – abzuwehren, sie zu verkraften, sich davon zu erholen und sich ihnen immer schneller anzupassen.

Einführung des All-Gefahren-Ansatzes. Neben dem Fokus der Terrorismusabwehr und der Kriminalitätsbekämpfung wird auch die Bewältigung von Großschadenslagen durch Naturkatastrophen und Großunfälle umfassend adressiert. Mithin betrachtet das Konzept der Resilienz gleichermaßen die Sicherheitsaspekte Security und Safety.

Forschung auf Augenhöhe. Zu Beginn wurden die nicht technischen Wissenschaftsdisziplinen in der sogenannten »Begleitforschung« zusammengefasst. In der zweiten Programmphase gelang eine vollwertige Integration aller beteiligten Wissenschaftsdisziplinen bei der Erarbeitung von Lösungen.

Einbindung von Endanwendern. Während der zweiten Phase des Sicherheitsforschungsprogramms ist es zunehmend gelungen, Akteure aus Sicherheits- und Katastrophenschutzbehörden aktiv in die Forschung miteinzubeziehen und deren konkrete technische und konzeptionelle Bedarfe zu adressieren.

Internationale Vernetzung. Der effiziente Einsatz öffentlicher Mittel im Bereich Sicherheitsforschung kann in einem Europa der offenen Grenzen nur durch eine enge Abstimmung nationaler Anstrengungen mit europäischen Programmen sowie durch eine erfolgreiche Beteiligung nationaler Akteure an eben diesen Programmen gelingen. Die Fraunhofer-Gesellschaft erfüllt mit ihrem anwendungsorientierten Forschungsansatz seit Beginn der Sicherheitsforschung in Deutschland eine Schlüsselfunktion als Bindeglied zwischen Wissenschaft, Wirtschaft und Behörden und trägt wesentlich zu Erfolgen deutscher Akteure im europäischen Sicherheitsforschungsprogramm bei.


© Shutterstock

EMPFEHLUNGEN FÜR DAS NEUE ZIVILE SICHERHEITSFORSCHUNGS-PROGRAMM 2017+

© indigo/Fraunhofer IOSB

»Darüber hinaus müssen wir die gesamtstaatliche und gesamtgesellschaftliche Resilienz in Deutschland und innerhalb der Europäischen Union stärken. Nur so bewahren wir unsere offene Gesellschaft und schützen unsere freiheitliche Art zu leben.« (Bundeskanzlerin Angela Merkel, Weißbuch 2016 der Bundesregierung zur Sicherheitspolitik und Zukunft der Bundeswehr)

Gerade die Ereignisse der jüngeren Vergangenheit in Deutschland und Europa, wie zunehmende Cyberangriffe, terroristische Anschläge mit hohen Opferzahlen oder auch Extremwetterereignisse, verdeutlichen die Fragilität und Verwundbarkeit unserer freien, demokratischen und offenen Gesellschaften. Krisenherde an verschiedenen Rändern Europas und deren Folgeschäden stellen uns zunehmend vor massive Herausforderungen. Auch die volkswirtschaftliche Dimension dieser Entwicklungen ist nicht zu vernachlässigen: Als Exportnation ist Deutschland eng in internationale Handels-, Finanz- und Investitionsströme eingebunden und daher auf gesicherte Transportwege sowie verlässliche Informations- und Kommunikationssysteme angewiesen.

Ferner stellen auch technologische Entwicklungen und gesellschaftliche Trends komplexe Aufgaben an die Sicherheitsforschung: Aus Themen wie Energiewende, Digitalisierung der Wirtschaft, Autonomes Fahren und Smart Technologies für Privathaushalte leiten sich viele Forschungsfragen ab, die direkt mit Aspekten der Sicherheit und Widerstandsfähigkeit verknüpft sind.

Aus Sicht der Fraunhofer-Gesellschaft als einem der größten Player im Bereich der Zivilen Sicherheitsforschung sollte das neue Forschungsprogramm folgende **Themenschwerpunkte** enthalten:

Sicherheit und Resilienz kritischer Infrastruktursysteme

- Verwundbarkeit und Vernetzung von Versorgungsinfrastrukturen verstehen, modellieren und potenziell widrige Ereignisse simulieren, um Risiken besser zu verstehen und auf dieser Grundlage die Sicherheit und die Resilienz ausbauen zu können.
- Anpassungs- und Lernfähigkeit sowie Schutz technischer und organisatorischer Systeme durch neue ingenieurtechnische sowie organisatorische Lösungen sicherstellen.

Systemtheorie für die Sicherheit

- Entwicklung einer mathematisch formulierten, disziplinübergreifenden Querschnittstheorie der Sicherheit mithilfe der Zusammenführung von Ansätzen aus verschiedenen Domänen wie der Informatik, System- und Spieltheorie u. v. m., um technologie- und disziplinübergreifend Sicherheitssysteme analysieren, entwickeln und optimieren zu können.
- Mithilfe neuer theoretischer Ansätze die Quantifizierung von Risiko, Verwundbarkeit, Robustheit, Zuverlässigkeit und Resilienz verbessern.
- Grundlagen sicherer IT-Systeme: Programmierkonzepte für hochsichere IT-Systeme in besonderen Anwendungsumgebungen (kritische Infrastrukturen) sowie Erforschung menschlicher Faktoren bei der Gestaltung sicherer IT-Systeme zur Identifikation und Vermeidung von Fehlerquellen.

Cybersicherheit und Cyberresilienz

- Risiken hoch vernetzter, automatisierter Systeme (Industrie 4.0, Mobilität, Energieversorgung etc.) verstehen und quantifizieren.
- Schutzmaßnahmen entwickeln, die unabhängig von konkreten Angriffsszenarien wirksam sind.

Kriminalitätsbekämpfung und Terrorismusabwehr

- Bedrohungsszenarien analysieren und modellieren, um daraus effektive Methoden und Technologien zur Früherkennung, zum Schutz und zur Abwehr ableiten und entwickeln zu können.
- Verfahren zur Unterstützung des (nationalen und EU-weiten) Informationsaustauschs zwischen Sicherheitsbehörden weiterentwickeln.

Resilience Engineering als Perspektiverweiterung der Ingenieurwissenschaften

- Entwicklung neuer Methoden und Ansätze, um ein resilientes Systemdesign sicherzustellen.
- Entwicklung neuer akademischer Ausbildungsprogramme für zukünftige Ingenieure, die wissenschaftliche Grundlagen ebenso betrachten wie Themen der Vorausschau und Forschungsplanung.

Integrierte sozioökonomische und soziotechnologische Forschung

- Empirische Forschung zum Thema Wahrnehmungsverschiebung von allgemeinen sozialen Ängsten auf Sicherheitsthemen; gefühltes subjektives Risiko vs. objektivwissenschaftlich vorliegendes Risiko; German Angst.
- Gesellschaftliche Auswirkungen zunehmender informationstechnischer Überwachung – Risiken und Gefahren für demokratische Systeme.
- Rechtliche und regulatorische Aspekte: Analyse des bestehenden regulatorischen Rahmens mit dem Ziel, rechtliche Hemmnisse bezüglich der Umsetzung systemischer und resilienzsteigernder Lösungen zu identifizieren und Ansatzpunkte für die Weiterentwicklung der Regulation abzuleiten (Regulation for Resilience).

© iStock

Neben diesen inhaltlichen Schwerpunkten erachtet die Fraunhofer-Gesellschaft folgende **übergreifende Initiativen** als erforderlich:

Resilienz als vorausschauender und nachhaltiger Ansatz zur Stärkung der Sicherheit in umsetzbare Lösungen überführen. Mithilfe welcher Methoden, Entwicklungsprozesse und Ausbildungsinhalten Technologie, Organisationen, Wirtschaft und Gesellschaft resilient werden, muss noch erforscht werden.

Ziel: Erarbeitung von Grundlagen zur Entwicklung und Kommunikation von Methoden, Technologien und Konzepten zur Erhöhung der Resilienz. Förderung der Etablierung von Resilience Engineering als eigenständige Disziplin im Rahmen von Ingenieur-, Wirtschafts- und Gesellschaftswissenschaften.

Starke Forschungsstandorte strukturell fördern. In Deutschland haben sich verschiedene Standorte und Forschungsorganisationsformen herauskristallisiert, an denen Forschung, Wissenschaft und Wirtschaft besonders erfolgreich zusammenarbeiten. Begünstigt wurde diese Entwicklung nicht zuletzt auch durch universitäre Spitzenförderung wie die Exzellenzinitiative oder den »Spitzencluster-Wettbewerb« des BMBF. Mit sogenannten Leistungszentren hat die Fraunhofer-Gesellschaft zudem ein Instrument entwickelt, um Standorte mit hoher Präsenz von Fraunhofer, starker Wirtschaft und etabliertem Forschungsprofil gemeinsam mit einer lokalen Universität strukturell zu fördern. Die Fraunhofer-Gesellschaft begrüßt ausdrücklich den Ansatz des BMBF, mit den in 2016 erfolgten Bekanntmachungen zur Schaffung von Kompetenzzentren und den Nachwuchsforschergruppen diesen Weg fortzusetzen.

Ziel: Innerhalb der zivilen Sicherheitsforschung sollte verstärkt auf die Förderung bestehender und, wo thematisch geboten, die Bildung weiterer Spitzenstandorte mit ausgewiesenem Forschungsprofil gesetzt werden.

Übergeordnetes Ziel sollte sein, auch internationale Strahlkraft für deutsche Innovationen im Bereich Zivile Sicherheit zu erzeugen und attraktiver Wissenschafts- und Forschungsstandort zu bleiben.

An internationale Flaggschiff-Initiativen anknüpfen. Lokale und regionale Krisen wirken sich in einer globalisierten Welt rasch auf andere Regionen und Räume aus. Große internationale Organisationen (IO), Nichtregierungsorganisationen (NGO) sowie Wirtschaftsverbände und Allianzen haben bereits eine Vielzahl an Forschungsprogrammen und Initiativen lanciert, die weite Bereiche der zivilen Sicherheitsforschung adressieren und starken Anwendungsbezug aufweisen. Zu nennen sind zum Beispiel das Programm »Sendai Framework for Disaster Risk Reduction« der Vereinten Nationen, das »100 Resilient Cities«-Programm der Rockefeller Foundation in den USA oder die von der Weltbank betriebene »Global Facility for Disaster Reduction and Recovery – GFDRR«.

Ziel: Die Unterstützung deutscher Akteure, um an diesen Flaggschiff-Initiativen prominent teilzunehmen.

Technologische Durchbrüche ermöglichen. Bisher ist zivile Sicherheitsforschung stark ausgerichtet auf die konkreten technischen und konzeptionellen Bedarfe der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sowie auf die Belange des Katastrophenschutzes. Auch in Zukunft muss Forschung dazu beitragen, dass diese Akteure praktische Werkzeuge und Anwendungen erhalten, um Krisensituationen zu bewältigen, Menschen und Infrastrukturen vor Gefahren zu schützen und Folgeschäden zu bewältigen. Doch neue Technologien und Methoden aus ganz anderen Anwendungsbereichen führen auch zu überraschend neuen Lösungsansätzen, z. B. die Nutzbarmachung der Digitalisierung für eine Sicherheit 4.0.

Daher muss innerhalb eines Programms auch Raum sein für Forschung, die noch nicht einen unmittelbaren Bedarf adressiert, sondern weiter in die Zukunft blickt und zu Technologiedurchbrüchen und wirtschaftlichem Erfolg führen kann.

Ziel: Pro Jahr sollte mindestens eine themenoffene Bekanntmachung die Förderung explorativer Forschungsprojekte mit höherem Risikofaktor unter klaren Rahmenbedingungen ermöglichen.

Stärkung der gesamten Hightech-Strategie durch stärkere Sicherheitsforschung. Als Querschnittsdisziplin leistet die Zivile Sicherheitsforschung bereits einen wichtigen Beitrag zur Integration relevanter Forschungsbereiche. Gerade Zukunftsthemen wie Industrie 4.0, Autonomie in der Mobilität oder die Energiewende mit ihrem hohen Anspruch an länderübergreifende Vernetzung müssen von Anfang an Erkenntnisse der Sicherheitsforschung einbeziehen.

Ziel: Um die Erkenntnisse der Sicherheitsforschung zielgerichtet in alle relevanten Bereiche zu integrieren, müssen konkrete Projektförderungen zum Thema Sicherheit in den Bereichen Energie, Mobilität, Produktion, Telekommunikation und Nachhaltige Urbanität erfolgen. Dabei sollten neben entwickler- und anbieterseitigen Aspekten auch nutzer- und anwenderseitige Fragestellungen berücksichtigt werden.

SCHWERPUNKTTHEMEN FÜR DAS NEUE SICHERHEITSFORSCHUNGSPROGRAMM AUS SICHT DER FRAUNHOFER-GESELLSCHAFT

In Anlehnung an die Empfehlungen des Wissenschaftlichen Programmausschusses Sicherheitsforschung empfiehlt die Fraunhofer-Gesellschaft die folgenden Forschungsthemen für das neue Sicherheitsforschungsprogramm. Dabei liegt jedem Themenkomplex in seiner Gliederung das Konzept der Resilienz zugrunde:

Sicherheit und Resilienz kritischer Infrastruktursysteme

Risiken und Verwundbarkeiten kennen (Preparedness)
Erforschung neuer Simulationswerkzeuge zur Visualisierung hochkomplexer Schadensszenarien, d. h. Abbildung systemischer Abhängigkeiten und Verwundbarkeiten, z. B. in den Bereichen intermodale Verkehrsnetze, transnationale Energienetze oder komplexe IT-Systeme.

Simulative Voruntersuchungen zu geeigneten Sensortechniken und -hierarchien sowie zu robusten Fusionsalgorithmen und entsprechenden statistischen Sensormodellen zur Detektion/Abwehr terroristischer Bedrohungen. Insbesondere Zusammenführen von Methoden zur Terrorabwehr mittels Technologie für die Gefahrenstoffdetektion sowie für die Erkennung und Verfolgung von Drohnen (UAS).

Entwicklung von resilienten Systemen zur Früherkennung und Abwehr von Gefahren konventioneller wie auch nicht konventioneller Art.

Verstehen und Bewerten von Sicherheitsbedarf und Investitionsbereitschaft bei Kunden aus der Wirtschaft. Analyse und Weiterentwicklung der Geschäftsmodelle von Dienstleistungsanbietern im Sicherheitsbereich.

Vorsorge treffen (Prevention)
Erforschung ingenieurtechnischer Methoden für ein resilientes Design von technischen und soziotechnischen Systemen und deren Komponenten, d. h. z. B. Entwicklung von Indikatoren und Metriken zur Quantifizierung von Resilienz oder die Entwicklung von Designprozessen für Stadtplaner und Architekten zur frühzeitigen Umsetzung resilienter Designs (z. B. dezentrale vs. zentrale Systemarchitekturen in unterschiedlichen Infrastrukturbereichen, wie beispielsweise Wasser, Energie, etc.).

Experimente zur Detektionsrate und Falschalarmwahrscheinlichkeit in unterschiedlichen Szenarien terroristischer Bedrohungen in Absprache mit Betreibern kritischer Infrastrukturen sowie polizeilichen Behörden und entsprechender Begleitforschung.

Entwicklung leistungsfähiger Überwachungssensorik (ortsfest, mobil und drohnengestützt) zur frühzeitigen Erkennung von drohenden Gefahrenlagen, denen nicht allein durch robustes Design begegnet werden kann.

Aufbau, Bewertung und Schutz verfügbarer sowie zukünftiger optischer bzw. optronischer Warnsysteme sowie Kompensation atmosphärischer Störungen zur Optimierung der Leistungsfähigkeit der dabei eingesetzten Sensorik.

Optimierung der Lage der Stützpunkte, der Techniken, der Verfahrensabläufe für die Notversorgung der Bevölkerung bei einem länger andauernden Ausfall kritischer Infrastrukturen und zu deren Wiederaufbau.

Schützen (Protection)
Wirkungsminderung von Extremwetterereignissen oder terroristischen Anschlägen durch Erforschung ansprechender, schützender und zugleich nachhaltiger (d. h. energieeffizient, ressourcenschonend) baulicher Systemlösungen für Gebäude, Brücken, Tunnel, Straßen, etc.

Schutz vor Gefahrstoffen, wie z. B. schmutzigen Bomben, und anderen terroristischen Gefahren anhand eines Schalenmodells zu unterschiedlichen Stufen der Detektionsrate zur Erkennung z. B. von Gefahrstoffen und Waffen zusammen mit anonymisiertem und robustem Personentracking. Fusion von Messinformationen eines verteilten Sensornetzes und Kontextinfos als Entscheidungshilfe für weitere präventive Maßnahmen.

Härtung essenzieller elektronischer Systeme, auch gegenüber neuartigen Angriffsszenarien mit Hochleistungsmikrowellen.

Auf Krisen- und Katastrophenereignisse reagieren (Response)
Entwicklung von bildgebenden Visualisierungssystemen, basierend auf multipler Sensorik für kritische Infrastrukturen, sowie Entwicklung von Verfahren zur inhaltlichen Fusionierung der so gewonnenen Daten, um im Sinne einer echtzeitfähigen Lagebewertung Rettungs- und Sicherungsmaßnahmen schneller, sicherer und effizienter durchführen zu können.

Neuartige, zerstörungsfreie Wirkmittel gegen elektronische Komponenten angreifender Systeme (Fahrzeuge, Drohnen, Fernsteuerungen).

Umfassende Lagebewertung durch Fusion von heterogenen Informationen (soft, z. B. Kontextinformation, textuelle Berichte, und hard, z. B. Chemo- oder Radioaktivsensorik).

Förderung zu Untersuchungen des Blue Force Trackings und der automatisierten Bildauswertung.

Weitere Erforschung der Technologien zur Drohnenabwehr, da sich bisher bekannte Maßnahmen noch als technologisch schwierig gestalten.

Aus Krisen lernen und sich anpassen (Recovery)
Entwicklung akademischer Aus- und Weiterbildungsprogramme im Bereich Resilience Engineering.

Systemtheorie für die Sicherheit

Sicherheit komplexer soziotechnischer Systeme involviert viele unterschiedliche Disziplinen: Ingenieurwissenschaften, Informatik, Rechts-, Geistes- und Sozialwissenschaften. Für die Planung, den Entwurf und den Betrieb von Systemen, die hierfür Sicherheit erhöhen und gewährleisten sollen, gibt es bis heute keine grundlegende Querschnittswissenschaft, die alle oben genannten Disziplinen übergreift und eine technologie- und anwendungsdomänenübergreifende Methodik zur Verfügung stellt, mit der eine umfassende formale Problembeschreibung gelingt und komplexe Sicherheitssysteme im soziotechnischen Kontext analysiert, entworfen und optimiert werden können. Außerdem werden die Sicherheitsaspekte Safety, Security und Zuverlässigkeit in der Regel unnötigerweise getrennt betrachtet und behandelt.

Hierzu bedarf es einer mathematischen Systemtheorie für die Sicherheit, die von den Spezialitäten der Disziplinen und Technologien abstrahiert, gleichzeitig aber ausdrucksmächtig genug ist, um die Erfordernisse der Disziplinen ausreichend abzudecken. Eine solche Theorie kann sich aus verschiedenen etablierten mathematischen Apparaten gleichsam wie aus einem Baukasten bedienen: z. B. aus der Informatik, der Systemtheorie, der Spieltheorie, der statistischen Entscheidungstheorie, dem Systems Engineering und der Kybernetik. Auf der Basis einer solchen mathematisch formulierten Theorie kann auch die quantitative Ausprägung des Resilienzkonzepts vorangetrieben werden.

Die Förderung der Sicherheitsforschung sowohl in Deutschland als auch durch die EU hat viele sehr gute Ergebnisse hervorgebracht, war aber sehr stark szenario- und anwendungsgetrieben, setzte also gewissermaßen überwiegend auf eine Bottom-up-Herangehensweise.

Die Zeit ist nun reif, auch eine Top-down-Förderung zu initiieren, die vereinheitlichende Theorien und Methoden für die Sicherheit soziotechnischer Systeme zu erforschen und zu entwickeln erlaubt.

Risiken und Verwundbarkeiten kennen (Preparedness)
Entwicklung einer mathematisch formulierten Theorie mithilfe der Zusammenführung von Ansätzen aus verschiedenen Domänen wie der Informatik, System- und Spieltheorie u. v. m., um technologie- und disziplinübergreifend Sicherheitssysteme analysieren, entwickeln und optimieren zu können.

Erforschung menschlicher Faktoren bei der Gestaltung sicherer IT-Systeme zur Identifikation und Vermeidung von Fehlerquellen.

Entwicklung von Modellierungsmethoden und dynamischen Modellen zur Beschreibung und Analyse systemischer Risiken unter Berücksichtigung der dynamischen Wechselwirkung technischer wie auch nicht technischer Teilsysteme.

Vorsorge treffen (Prevention)
Modellgestützte Analysen großer, soziotechnischer Systeme zur Ableitung von Strategien zu deren Umgestaltung im Sinne der Erhöhung der Resilienz (Transitionsstrategien).

Mithilfe neuer theoretischer Ansätze die Quantifizierung von Risiko, Verwundbarkeit, Robustheit, Zuverlässigkeit und Resilienz verbessern.

Schützen (Protection)
Programmierkonzepte für hochsichere IT-Systeme in besonderen Anwendungsumgebungen (kritische Infrastrukturen).

Cybersicherheit und Cyberresilienz

Risiken und Verwundbarkeiten kennen (Preparedness)
Entwicklung von Methoden und Verfahren zur systematischen Beurteilung/Messung des IT-Sicherheitsbewusstseins von IT-Nutzern, dessen Abwesenheit Risiko und Verwundbarkeit darstellt.

Entwicklung effektiver und effizienter Methoden zum kooperativen Austausch von Bedrohungsinformation (z. B. beobachtete Angriffstechniken) unter Berücksichtigung bestehender Vertraulichkeitsanforderungen, z. B. mittels maßgeschneiderter Pseudonyme.

Erforschung neuer Verfahren zur Darstellung hochkomplexer IT-Landschaften, d. h. Abbildung systemischer Abhängigkeiten und Verwundbarkeiten in Cyberumgebungen und kritischen Infrastrukturen; insbesondere unter Einbeziehung des Faktors Mensch.

Erforschen und besseres Verstehen von menschlichen Einflussfaktoren bei der Konzeption und Gestaltung von IT-Systemen, um Fehlerquellen zu finden und zu vermeiden.

Erforschung von technischen Schwachstellen, dabei Hauptaugenmerk auf der Betrachtung der gesamten Systemlandschaft und nicht nur einzelner Komponenten.

Erforschung geeigneter Test- und Zertifizierungsmechanismen für die Vermeidung von infrastrukturübergreifenden Angriffen auf Cyber-/IT-Infrastrukturen.

Vorsorge treffen (Prevention)
Identifikation und Untersuchung von infrastrukturübergreifenden Verwundbarkeiten und Resilienzen im Kontext der fortschreitenden Digitalisierung und Vernetzung, sowohl im Kontext von Cyberbedrohungen als auch im Kontext von physikalischer/technischer Resilienz der Netzwerkinfrastrukturen und ihrer Betreibermodelle.

Entwicklung von Verfahren und Analysemethoden zur Bewertung und Erfassung von durch Datenverlust/-diebstahl/-veränderung induzierten, potenziellen Schadensszenarien. Bewerten des Impacts dieser Schadensszenarien in verschiedenen Dimensionen: direkte Sicherheit (Zugang, Geheimhaltung etc.), wirtschaftliche Sicherheit (Geschäftsgeheimnisse, Insiderwissen, Forschungsergebnisse etc.), gesellschaftliche Prozesse (Desinformation, Leaking etc.).

Entwicklung von neuen Programmierkonzepten für den Bau von hochsicheren IT-Systemen für spezifische Anwendungsumgebungen (da Cybersysteme für kritische Infrastrukturen auf denselben IT-Technologien wie Consumer-IT aufbauen).

Erforschung des Faktors Mensch als Einflussgröße, um bisher unbeachtete systemische Schwachstellen zu identifizieren und zu beseitigen.

Entwicklung von (korruptions-/betrugs-)sicheren und resilienten Transaktionssystemen.

Schützen (Protection)
Kontrolle durch Überwachung der IT-Nutzung unter Berücksichtigung von Vertraulichkeits- und Datenschutzanforderungen, z. B. mittels maßgeschneiderter Pseudonyme.

Entwicklung von nutzergerechten Werkzeugen, die eine Anwendung einfacher und effektiver Schutzmechanismen zur Absicherung von Cyberumgebungen und kritischen Infrastrukturen ermöglichen.

Entwicklung von Schutzmaßnahmen, die unabhängig von konkreten Angriffen wirksam werden.

Auf disruptive Ereignisse reagieren (Response)
Der Faktor Mensch spielt beim Incident Response eine sehr große Rolle: Erforschung der Reaktion der Menschen auf disruptive Ereignisse, Bereitstellung von Mitteln, mit denen sie schnell ein Lagebild auswerten und Gegenmaßnahmen einleiten können.

Erarbeitung von technischen Verfahren, die auch während eines Angriffs verlässlich einen sinnvollen Minimalbetrieb gewährleisten können.

Systematische Betrachtung von Maßnahmen zur Reaktion auf Vorfälle. Insbesondere effektive opferbezogene Reaktionen, z. B. bei Diebstahl von Online-Identitäten (z. B. E-Mail-Adresse und Passwort) – kaum untersucht, aber dringend erforderlich. Wer informiert Opfer bei festgestelltem Diebstahl, so dass vom Opfer geeignet reagiert werden kann?

Entwicklung von sicheren und resilienten Anwendungen von Cyberwährungen/virtuellen Währungen, Blockchains etc.

Entwicklung einer systematischen Methode zur Ermittlung effektiver Response-Maßnahmen.

Testmethodik für Response-Maßnahmen.

Methoden und Verfahren zur Ermittlung und Umsetzung erforderlicher Notlaufeigenschaften.

Aus Krisen lernen und sich anpassen (Recovery)
Erarbeitung von Verfahren zur Gewährleistung des Neustarts aus unbekanntem Systemzustand in ein integres laufendes Gesamtsystem.

Kriminalitätsbekämpfung und Terrorismusabwehr

Risiken und Verwundbarkeiten kennen (Preparedness)
Modellierung von Bedrohungsszenarien in enger Zusammenarbeit mit BOS.

Analyse von Angriffs- und Schmuggelszenarien, abhängig vom Transportmittel (Lkw, Bahn, Seefrachtcontainer, Luftfracht, Paketsendungen etc.).

Sicherheitswirtschaft: Privatisierung von Sicherheitsleistungen: gewünschte und ungewünschte Effekte und Folgen.

Technologien zu Predictive Policing, Predictive Analytics, Kriminalitätsprävention.

Technologien zum Screening sozialer Netzwerke auf verdächtige Kommunikation.

Multisensorielle Echtzeitauswertung von Einzelbildern und Videobildfolgen zur Situationserkennung, Objektdetektion, -erkennung und -verfolgung, einschließlich der Mensch-System-Integration.

Vorsorge treffen (Prevention)
Bildverbesserungsverfahren (Rauschen, Bewegungsunschärfen) und Verfahren zur nachträglichen Steigerung der Auflösung (Super Resolution).

Fusion von Bildern multisensoriellen Ursprungs für geschichtete Gesamtsichten und eine verbesserte automatisierte Analyse. Unterstützungsmöglichkeiten durch technische Systeme, basierend auf neuesten Forschungsergebnissen, modellieren und entwickeln.

Sensorik zur frühzeitigen Gefahrenerkennung (chemisch, biologisch, radiologisch, nuklear, explosiv).

Erkennung und Abwehr neuer Gefahrensituationen, z. B. durch Drohnen, in urbanem Umfeld.

Verbesserung von Bild-, Video- und Dokumentenanalyse, letztere auch in entsprechenden Sprachen, sowie Weiterentwicklung von Verfahren zur Verknüpfung gewonnener Informationen auf der inhaltlichen (semantischen) Ebene zur Unterstützung des Informationsaustauschs zwischen Sicherheitsbehörden, national und im Rahmen der EU.

Entwicklung von nicht invasiven Inspektionstechnologien und -verfahren, wie beispielsweise Röntgentechniken, Radar, Terahertz, Ultraschall, Thermografie oder chemische Spurenanalyse zur effektiven Detektion von illegalen und gefährlichen Gütern mit minimaler Beeinträchtigung des Warenflusses.

Testumgebungen zur Verifikation von Forschungsergebnissen und Untersuchung organisatorischer Abläufe (Beispiel: Einsatz der Bundeswehr im Inneren) entwickeln und betreiben.

Entwicklung von (korruptions-/betrugs-)sicheren und resilienten Transaktionssystemen.

Entwicklung von sicheren und resilienten Anwendungen von Cyberwährungen/virtuellen Währungen, Blockchains etc.

Schützen (Protection)
Sicherheit und Resilienz in der drahtlosen Kommunikation (z. B. Mobiltelefonie, IP-Kommunikation etc.).

Systemintegration sowie Mensch-Computer-Integration für Monitoring-, Schutz- und Überwachungsaufgaben.

Anwendungsprototypen im Zusammenspiel zwischen Anwendern, Forschungsinstituten und Industrie entwickeln und in Anwendungsszenarien evaluieren.

Der Liegenschaftsschutz von morgen wird bei der Bekämpfung organisierter Kriminalität eine wesentliche Rolle spielen: verstärkte Betrachtung von multisensoriellen Ansätzen zur Überwachung mittels heterogener, verteilter Sensorik. Entwicklung unbemannter/autonomer Fahrzeuge für den polizeilichen Einsatz.

Hochleistungsmikrowellensysteme zur zerstörungsfreien Einwirkung auf elektronische Systeme, z. B. zur Verhinderung von Löschaktionen auf PCs, Unterbindung von Fernsteuerungen oder dem gewaltlosen Stoppen flüchtender/angreifender Fahrzeuge.

Technologien zur Abwehr von Drohnen (Flugsicherheit; Schutz der Privatsphäre).

Auf disruptive Ereignisse reagieren (Response)
Entwicklung von Systemen zur echtzeitfähigen Lagebewertung und Intervention.

Technologien zur Tatortanalyse (z. B. 3-D-Tatort-Scanning, modellgestützte Tatortanalyse).

Gerichtfeste Sicherung von Beweismitteln für eine wirksame Strafverfolgung, auch als soziokulturellen Beitrag zur Erhöhung der Resilienz.

Innovative Verfahren zur automatisierten, gerichtsfesten Sicherung von Beweismitten bzw. zur forensischen Analyse.

Katastrophenmanagement im Sinne von Disaster Resilience

Vorsorge treffen (Prevention)
Entwicklung und »offizielle« Ausbreitung einer App, über die Zivilpersonen Katastrophen melden können, wobei diese App zur Vermeidung von Informationsbrüchen interoperabel zu dem Informationsaustauschstandard der Einsatzkräfte sein sollte.

Entwicklung von Sensorkonzepten zur weiträumigen Überwachung von Orten/Einrichtungen/Gebieten, die gemäß Preparedness als risikohaft und verwundbar erkannt wurden, um
- frühzeitig Daten über eine sich anbahnende kritische Situation zu erhalten (Aufweichen von Dämmen, steigende Pegel, etc.).
- im Katastrophenfall ausreichende Daten und Informationen für die Bereitstellung eines umfassenden Lagebildes zu erhalten.

Erforschung von neuartigen Fusionsalgorithmen zur Berechnung von kritischen Situationen und aktuellen, verlässlichen Lagebildern.

Systemarchitekturen für die vernetzte Simulation sowie die Generierung von Gelände-, Gebäude- und Infrastrukturmodellen für Einsatz- und Planungssimulationen.

Schützen (Protection)
Verbesserung der Sensorik zur frühzeitigen Erkennung von Gefahrenlagen: Ein Ziel der Sicherheitsforschung ist die Entwicklung geeigneter Systeme zum Schutz von Infrastruktur und Personen in besonderen Situationen. Durch den Einsatz optischer, akustischer oder elektromagnetischer Sensoren und deren Kombination können Gefahrenlagen frühzeitig erkannt und gegebenenfalls notwendige Schutz- oder Rettungsmaßnahmen eingeleitet werden. Die Verbesserung der Sensorik im Hinblick auf Empfindlichkeit, Präzision und Effizienz sowie die Entwicklung besonderer Verfahren und Prozesse für konkrete Anwendungen ist eine wesentliche Aufgabe der Forschungsinstitute.

Entwicklung eines Warnsystems für Rettungskräfte: Rettungskräfte müssen bei ihren Einsätzen besonders geschützt werden, da jedes Katastrophenszenario auch immer eine Gefahr für die Retter selbst darstellt. Besonders in unübersichtlichen, sich zeitlich fortwährend ändernden Lagen kann modernste Sensorik die Einsatzstelle überwachen und so die Einsatzkräfte durch ein Warnsystem schützen. Neben einer bildhaften Überwachung muss ein entsprechendes Sensorsystem auch kleinste Veränderungen detektieren können, aber auch den Geschwindigkeitsvektor verschiedener bewegter Objekte. Eine geeignete Sensorik muss auch kleinste Trümmerbewegungen in einem komplexen Szenario erkennen und zeitlich verfolgt können, um die Einsatzkräfte rechtzeitig vor umstürzenden Trümmern zu warnen.

Auch muss eine Sensorik unter widrigen Umgebungs- oder Witterungsbedingungen funktionieren, z. B. durch dichten Rauch hindurchschauen können, so dass die Rettungskräfte sowohl Brandherde erkennen können als auch potenziell durch den Brand geschädigte Gebäudestrukturen. So können sich Feuerwehrleute bei der Rettung eingeschlossener Personen durch entsprechende Sensorik vor den Gefahren bei Bränden schützen.

Schutz von Großveranstaltungen und besonders gefährdeten Bereichen: Großveranstaltungen und besonders gefährdete Bereiche (z. B. Flughäfen) müssen vor ungewollten Abstürzen oder absichtlich herbeigeführten Angriffen durch Drohnen geschützt werden. Ein Sensorsystem muss hierbei in allen drei Raumdimensionen (Azimut, Elevation, Entfernung) die Position in der Zeit detektieren und somit die Flugtrajektorie in Echtzeit aufzeichnen. Darüber hinaus muss ein Sensorsystem in der Lage sein, eine Drohne in großer Entfernung zu analysieren und zu klassifizieren, um wesentliche Parameter über die Art der Drohne (Quadcopter, Octocopter, Flugzeug) und deren Nutzlast (Kamera, Sprengvorrichtung, etc.) zu erhalten.

Förderung der Kooperation von Forschungsinstituten und Behörden anhand von abgestimmten Szenarien bei Demonstrationen zur Erprobung von innovativen Technologien.

Auf disruptive Ereignisse reagieren (Response)
Entwicklung mobiler Führungssysteme (etwa auf gehärteten Tabletts) und eines Kommunikationsstandards zum schnellen Informationsaustausch zwischen den unterschiedlichen Einsatzkräften, um im Sinne einer echtzeitfähigen Lagebewertung Rettungs- und Sicherungsmaßnahmen schneller, sicherer und effizienter durchführen zu können. Position und Zustand der Rettungskräfte sowie die Katastrophenlage müssen in ein gemeinsames Lagebild einfließen, um einen effizienten und optimalen Einsatz zu gewährleisten. Hierfür müssen auch Sensorinformation zu beispielsweise Position, Einsatzziel und physiologischer Parameter fusioniert und ergonomisch dargestellt werden.

Aufbau von drahtloser Ad-hoc-Kommunikationsinfrastruktur. Mobile Energieversorgungssystem zur Überbrückung.

Echtzeitlagebeurteilung durch mobile bzw. drohnengestützte Sensorik.

Management von Epidemien/Pandemien – Entwicklung von Technologien zur raschen bzw. Echtzeitdiagnose bestimmter Infektionskrankheiten.

Aus Krisen lernen und sich anpassen (Recovery)
Förderung der Zusammenarbeit von Forschung und Endnutzern im Bereich der Fähigkeitsentwicklung bzw. Forschungsplanung mit dem Ziel, bedarfsgerechtere Forschung betreiben zu können. Wichtig ist hier vor allem die Verbesserung von Methoden zur Bedarfsanalyse sowie zur Auswahl und Weiterentwicklung von geeigneten technischen oder konzeptionellen Lösungen in verschiedenen technologischen Reifegraden bis hin zur Operationalisierung.

Kognitiven Eigenschaften von künftigen Sensorsystemen: Zukünftige Sensorsysteme stimmen ihre Funktionalität individuell auf die jeweilige Situation ab und orientieren sich an den aktuellen Anforderungen und Bedürfnissen. Sie müssen kognitive Eigenschaften haben, damit sie im Laufe der Zeit ihre Aufgaben – durch einen »Erkenntnisgewinn« – immer besser durchführen können. Als wissensbasierte Systeme agieren sie auf verschiedenen Ebenen der Wahrnehmung und setzen dabei maschinelles Lernen durch Verfahren, wie z. B. Deep Learning, ein. Daten und Erkenntnisse aus Krisen werden deshalb als Input zukünftiger Sensorik dienen, so dass diese bei anschließenden Krisen deutlich wirkungsvoller eingesetzt werden können.

Anpassen von Simulationsszenarien sowie Verbesserung der Fusionsalgorithmen.

Integrierte sozioökonomische und soziotechnologische Forschung

Risiken und Verwundbarkeiten kennen (Preparedness)
Empirische Forschung zum Thema Wahrnehmungsverschiebung von allgemeinen Ängsten auf Sicherheitsthemen: Wesentlicher Ansatzpunkt für derartige Forschungen ist die Unterscheidung von gefühltem subjektivem Risiko und objektiv-wissenschaftlich vorliegendem, statistisch abgesichertem Risiko. Zwischen beiden können erhebliche Differenzen bestehen, indem etwa die Wahrscheinlichkeit von Großschadensereignissen subjektiv überschätzt wird und selbst eingegangene, schleichende Risiken (wie etwa Rauchen) systematisch unterschätzt werden. Unter dem Schlagwort »German Angst« hat die kollektive Neigung zu diffuser Furcht bereits Eingang in den täglichen Sprachgebrauch gefunden.

Umfassende Untersuchung der gesellschaftlichen Auswirkungen zunehmender informationstechnischer Überwachung.

Untersuchung der Risiken und Gefahren der Verbreitung allgegenwärtiger Überwachungs- und Sicherheitssysteme für demokratische Systeme.

Vorsorge treffen (Prevention)
Frühe Einbindung von Bürgerinnen und Bürgern in FuE; Erprobung neuer Partizipationsformen, um die Akzeptanz technischer Lösungen sicherzustellen (Participatory Design).

Erarbeitung datensparsamer IuK-Systeme: IuK-Systeme sind vom Systemdesign so auszulegen, dass ein Dual-Use der Nutzungsdaten vermieden werden kann (Privacy by Design).

Untersuchung der rechtlichen und regulatorischen Aspekte von Resilienz: Analyse des bestehenden regulatorischen Rahmens mit dem Ziel, rechtliche Hemmnisse bezüglich der Umsetzung systemischer und resilienzsteigernder Lösungen zu identifizieren und Ansatzpunkte für die Weiterentwicklung der Regulation abzuleiten (Regulation for Resilience).

Schützen (Protection)
Hebung lokalen Expertenwissens durch Citizen-Science-Ansätze: Betroffene/Laien sind hinsichtlich potenzieller Schutzziele und Verfahrensweisen zu befragen, um umfassende technologische Lösungen hervorzubringen.

Entwurf dezentraler, resilienter soziotechnischer Systeme: Entwurf und Umbau zentraler Infrastruktursysteme (wie Wasser, Strom, Kommunikation) die ein Funktionieren auch im Großschadensfall ermöglichen.

Auf disruptive Ereignisse reagieren (Response)
Mensch-Maschine-Interaktion und angemessenes Nutzer-Involvement: Mensch-Maschine-Schnittstelle ist so zu gestalten, dass komplexe technische Systeme beherrscht werden können und angemessene Reaktionsweisen des Nutzers erlauben.

Aus Krisen lernen und sich anpassen (Recovery)
Inter- und transdisziplinäre Ex-post-Analyse der Angemessenheit technischer Systemdesigns: Systemlösungen sind kontinuierlich hinsichtlich ihrer Angemessenheit, der empirischen Akzeptanz und der normativ-ethischen Akzeptabilität zu untersuchen und anzupassen.