Deutscher Bundestag **Drucksache 19/30736**

19. Wahlperiode 03.06.2021

Unterrichtung

durch die Bundesregierung

Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit Digital. Sicher. Souverän.

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 2. Juni 2021.

Strategische Ziele
Daten und Know-how: geschützt und genutzt
Digitaler Wandel: sicher und nachhaltig
Demokratie und Gesellschaft: stabil und digital
Privatheit und Datenschutz: selbstbestimmt und innovativ
Innovation und Transfer: weltspitze und zukunftssicher
Führende Köpfe: qualifizieren und gewinnen
Deutschland und Europa: technologisch souverän
Herausforderungen
Sicherheit und Vertrauen
Digitale Infrastrukturen sichern
IT-Sicherheit benutzbar gestalten
Vertrauen in IKT durch IT-Sicherheit stärken
Demokratie
Grundrechte schützen
Desinformation bekämpfen
Technik nach demokratischen Werten souverän gestalten
Technologische Souveränität
Nachhaltigkeit und Zukunftssicherung
IT-Sicherheit in Anwendungsfeldern stärken
IT-Sicherheit in der Quanteninformationsverarbeitung
Zukün..ige Technologien der IT-Sicherheit beherrschen
Partnerschaft und Exzellenz
Technologische Souveränität ausbauen
Deutschlands in der Wissenschaftslandschaft positionieren
Kooperation und Transfer weiter verbessern
Umsetzung
Wissenschaftliche Kompetenzen fördern
Innovationsökosystem und Transfer ausbauen
Akteure vernetzen
In den gesellschaftlichen Dialog treten
Europäisch und international forschen

1 Digital. Sicher. Souverän.

Menschlicher Fortschritt ist eng mit technologischen Entwicklungen verbunden. Die Digitalisierung verwandelt unsere Welt so schnell, dass wir kaum mehr hinterherkommen. In vielerlei Hinsicht verändert sich unser Leben durch Smartphones, Internet und Computer zum Guten: Das Wissen der Welt ist nur einen Klick entfernt, digitale Innovationen erleichtern uns den Alltag und die Wissenschaft leistet dank des digitalen Fortschritts jeden Tag aufs Neue Großartiges. Doch Teil der Wahrheit ist auch, dass wir zunehmend abhängig und herausgefordert werden: von Geräten, die unsicher sind; von Technik, die wir nicht verstehen; von Unternehmen, deren Geschäftsmodell darin besteht, unsere Daten zu Geld zu machen; von Informationen, deren Echtheit und Wahrheitsgehalt fragwürdig ist.

Wir müssen jetzt handeln: Wir Menschen in Deutschland und Europa leben in einer durch und durch technologisierten und datafizierten Welt, die wir sicher gestalten müssen. Denn Sicherheit und Privatheit bleiben heute vielfach auf der Strecke. Ob Cyberangriffe auf staatliche Institutionen, Hochschulen und Unternehmen, Desinformationen in sozialen Netzwerken, die Menschen manipulieren und verunsichern, oder Quantencomputer, die mit ihrer enormen Rechenleistung künftig heute gängige Verschlüsselungsverfahren überwinden können: Die Herausforderungen sind komplex und werden mit der Datenexplosion sowie dem Voranschreiten von Technologien wie Künstlicher Intelligenz (KI) und Quantencomputing weiter zunehmen. Wir müssen jetzt vorsorgen, um auch in der Zukunft ein digitalisiertes Leben auf Basis von Vertrauen und Sicherheit zu ermöglichen. Forschung für IT-Sicherheit und Privatheit in der digitalen Welt ist hierfür der Schlüssel. Denn eigenes Wissen und eigene Fähigkeiten sind für unsere Souveränität unverzichtbar. Forschung und deren wirkungsvoller Transfer in die Praxis bauen die Kompetenzen auf, die in einer digitalen Welt geprägt von globalisierten Wertschöpfungsketten, Plattformökonomie und Netzwerkeffekten dringend notwendig sind.

Die Voraussetzungen sind gut: Schon heute verfügen wir in Deutschland und Europa über eine exzellente wissenschaftliche Basis. Mit dem Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015-2020“ hat die Bundesregierung frühzeitig die Weichen gestellt. Doch der technologische Wandel schreitet weiter voran, und die Forschung muss den Anspruch haben, diesem Wandel immer mindestens einen Schritt voraus zu sein. Dabei sind Herausforderungen in Zeiten der Digitalisierung stets nicht nur, aber eben auch, technischer Natur. Deshalb kommt es darauf an, in der technologischen Forschung in der Weltspitze zu sein – ebenso wie darin, über Disziplinen und Ländergrenzen hinweg Allianzen zu schmieden und zu kooperieren. Nur so können Deutschland und Europa in Zukunft technologisch souverän sein. Das Forschungsrahmenprogramm ist eng verknüpft mit der BMBF-Digitalstrategie, der Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels und der Hightech-Strategie 2025 der Bundesregierung.

Spitzenforschung: Deutschland und Europa stärken, die Welt gestalten

Anspruch unserer Forschungs- und Innovationspolitik ist es, die weltweit besten und zukunftssicheren Lösungen in Deutschland und Europa zu entwickeln. Dies sind demokratische, am Menschen orientierte, nachhaltige Lösungen auf höchstem technischen Niveau. Wir brauchen Innovationen, die unsere Werte tragen und müssen diese zum Standard machen – und damit zur Grundlage für unseren künftigen wirtschaftlichen Erfolg und gesellschaftliche Stabilität. Deutschland ist Innovationsland – und soll dies auch in der Zukunft sein, denn Ideen und Innovationen sind hierzulande unsere wichtigsten Rohstoffe.

Dieses Forschungsrahmenprogramm gründet fest auf europäischen Normen und Werten wie Freiheit, Demokratie, Rechtsstaatlichkeit und informationeller Selbstbestimmung. Die Bundesregierung versteht diese Werte als Innovationstreiber für eine menschengerechte Digitalisierung.

Mit dem vorliegenden Forschungsrahmenprogramm bereiten wir für die kommenden Jahre den Weg für eine exzellente Forschung für IT-Sicherheit und Privatheit, für wirtschaftliche Prosperität und technologische Souveränität in Deutschland und in Europa. Wir tun dies in der Absicht, ein besseres digitales Leben möglich zu machen – damit wir alle in Zukunft digital, sicher und souverän leben können.

2 Strategische Ziele der IT-Sicherheitsforschung[1]

Das Forschungsrahmenprogramm leistet einen wichtigen Beitrag zur Umsetzung der Hightech-Strategie 2025[2] der Bundesregierung. Übergeordnetes Ziel ist es, die großen gesellschaftlichen Herausforderungen anzugehen und die Forschungs- und Innovationsförderung auf aktuelle und zukünftige Bedarfe auszurichten. Es geht dabei um technologische und nicht-technologische einschließlich sozialer Innovationen, bei denen der Nutzen für den Menschen im Mittelpunkt steht. Im Themenfeld „Sicherheit: Für eine offene und freie Gesellschaft" der Hightech-Strategie 2025 hat die Bundesregierung beschlossen, die IT-Sicherheitsforschung in Deutschland erheblich zu stärken. Das vorliegende Programm orientiert sich an dieser Zielsetzung der Bundesregierung und ist daher ein Programm für IT-Sicherheitsforschung und nicht für Informationssicherheit. Konkret orientiert sich das Programm an folgenden strategischen Zielen.

2.1 Digitaler Wandel: sicher und nachhaltig

Die Digitalisierung prägt gesellschaftliche Entwicklungen und ist ein wesentlicher Treiber von Innovation. Neue Technologien eröffnen neue Interaktionsformen, neue Gestaltungsräume gesellschaftlichen Zusammenlebens und neue Geschäftsfelder. So haben beispielsweise Text- und Sprachnachrichtendienste das Kommunikationsverhalten radikal verändert, soziale Netzwerke kanalisieren gesellschaftliche Strömungen und eine steigende Anzahl von Start-ups entwickelt neue digitale Dienstleistungen. Gemeinsam ist all diesen Entwicklungen, dass große Mengen von Daten verarbeitet und gespeichert werden. Aufgrund der Durchdringungstiefe und des genutzten Datenumfangs müssen diese Dienste, Datenbanken und Datenräume nachhaltig sicher gestaltet werden. Ziel des vorliegenden Programms ist es daher, wesentlich zur Entwicklung sicherer Grundlagen für IT-Systeme beizutragen, um mögliche Schadensfälle effizient handhaben zu können und existierende Systeme abzusichern, bevor Schadensfälle eintreten.

2.2 Daten und Know-how: geschützt und nutzbar

Die zunehmende Digitalisierung in allen Lebensbereichen führt zu einer Datenexplosion, der Umfang der nutzbaren Daten nimmt stetig zu. Diese Daten bilden die Grundlage für zahlreiche Anwendungen zum Beispiel im Kontext von Maschinellem Lernen, das konstant an Bedeutung gewinnt. Die Bundesregierung hat sich im Rahmen der Datenstrategie dazu entschlossen, Chancen durch das Zugänglichmachen, Nutzen und Teilen von Daten noch stärker zu ergreifen. Die Trainingsdaten wie auch die erlernten Modelle stellen einen enormen Wert dar und müssen sicher nutzbar gemacht werden. Sicherheit bezieht sich hier auf Fragen der Datenqualität, der Datenauthentizität, des Datenschutzes und des geistigen Eigentums. Große Meilensteine dabei sind die Errichtung von Industrial und International Data Spaces für die Digitalisierung der deutschen Industrie sowie von GAIA-X als europäische Kooperation. Für die Umsetzung digitaler Liefer- und Produktionsketten in Europa werden offene Wertschöpfungsstrukturen auf Basis sicherer Systeme in einem sicheren Rechtsrahmen benötigt. Die föderierte, dezentrale Infrastruktur GAIA-X leistet einen wertvollen Beitrag dazu. Maximale Sicherheit sowie Schutz der Daten in diesen Datenräumen, welche sich aus Cloud- und Edge-Infrastrukturen sowie zugehörigen Diensten zusammensetzen, sind ein Grundpfeiler technologischer Souveränität. Ziel des Programms ist es daher, die Absicherung aller Datenräume von Grund auf, insbesondere auch im Hinblick auf Integrität und Datenschutzkonformität, zu etablieren und so dazu beizutragen, dass Daten sicher genutzt werden können.

2.3 Demokratie und Gesellschaft: stabil und digital

Das Internet hat die Welt näher zusammengebracht. Soziale Medien verbinden Menschen allerorts, Benachteiligte in vielen Ländern und marginalisierte Gruppen haben durch digitale Kommunikationskanäle eine Stimme erhalten und das Wissen der Welt ist häufig nur eine Suchanfrage entfernt. Doch es gibt auch Entwicklungen, die demokratische Systeme herausfordern: So hat sich zum Beispiel bei den sozialen Medien eine Datenökonomie herausgebildet, in der wenige Unternehmen den Markt beherrschen und weitreichenden Einfluss ausüben. Sie erreichen mit ihren Plattformen und anderen Angeboten Milliarden von Menschen und binden diese etwa durch sogenannte Lock-in-Effekte an sich. In den digitalen Geschäftsmodellen spiegeln sich zudem jeweils spezifische Wertvorstellungen, die globale Wirkung entfalten. Die große Reichweite der Plattformen wird auch zur gezielten Verbreitung von Informationen genutzt. Problematisch ist dies beispielsweise, wenn durch die gesammelten Daten der Plattformen gezielt Desinformationen verbreitet werden, insbesondere, wenn dadurch demokratische Prozesse manipuliert werden sollen. Ziel des vorliegenden Programms ist es daher, Forschung anzustoßen, die bei den

[1] Indikatoren zur Erfolgskontrolle sind im Abschnitt 5.3 aufgeführt

[2] https://www.hightech-strategie.de/de/hightech-strategie-2025-1726.html

Menschen das Bewusstsein für alle Belange von IT-Sicherheit und Datenschutz stärkt und so Selbstbestimmung sowie sichere digitale Partizipation ermöglicht. Ebenso zielt das Programm darauf ab, zur Erkennung und Bekämpfung von Desinformationskampagnen beizutragen.

2.4 Privatheit und Datenschutz: selbstbestimmt und innovativ

Transparenz und informationelle Selbstbestimmung sind entscheidende Faktoren für das Vertrauen von Nutzenden zu Unternehmen ebenso wie zu staatlichen Institutionen. Dieses Vertrauen ist die Grundvoraussetzung für eine schnelle und effiziente Digitalisierung. Nur wenn Menschen digitalen Systemen vertrauen können, akzeptieren sie diese breitflächig in ihrem Leben. Eine konsequente informationelle Selbstbestimmung dient also sowohl dem Schutz von Grundrechten als auch langfristig als Wettbewerbsvorteil. Ziel des vorliegenden Programms ist es, auch in Zeiten umfassender Digitalisierung durch Forschung eine nachhaltige Basis für einen umfassenden Schutz der Privatsphäre von Bürgerinnen und Bürgern sicherzustellen. Dazu wird die Erforschung technischer und nicht-technischer Aspekte unterstützt. Den Schutz dieser Rechte versteht die Bundesregierung nicht als Bremse für Wachstum und Beschneiden des Innovationspotenzials, sondern als Katalysator für Innovation. Unter dem Eindruck immer neuer Nutzungsmöglichkeiten von Daten sollen mithilfe der Forschungsförderung Lösungen entstehen, die „Privacy by Design“, Benutzbarkeit und Transparenz europäischer Prägung zum weltweiten Erfolgsmodell machen.

2.5 Innovation und Transfer: weltspitze und zukunftssicher

Deutschland ist Innovationsland und eine der führenden Industrienationen der Welt. Unter dem Stichwort Industrie 4.0 ist die Digitalisierung und Vernetzung der Industrie weit fortgeschritten. Durch Entwicklungen wie beispielsweise 5G steigen die Anforderungen an maßgeschneiderte IT-Sicherheitskonzepte ständig. Auch die Digitalisierung des Gesundheitswesens schreitet massiv voran. Ebenso wird der Verkehr immer digitaler: Assistiertes und autonomes Fahren auf Straßen und auf der Schiene sowie gänzlich neue Mobilitätsangebote sind auf dem Vormarsch. Für Deutschlands wirtschaftliche Prosperität und technologische Souveränität ist es wichtig, Zukunftstechnologien in all diesen Anwendungsfeldern maßgeblich mitzugestalten. Da die modernen digitalen Produkte und Dienste vielfach in sensiblen Bereichen zum Einsatz kommen, ist ihre Sicherheit von entscheidender Bedeutung. Spitzenleistungen in der IT-Sicherheitsforschung müssen deshalb schnell und konsequent in innovative High-End-Produkte umgesetzt werden. Die im internationalen Vergleich bereits sehr gut aufgestellte Forschungslandschaft muss hierfür noch zielgerichteter mit der Industrie verknüpft werden. Ziel dieses Programmes ist es daher, Deutschlands Position unter den innovativsten Standorten für die Entwicklung von IT-Sicherheitstechnologien weiter zu stärken. Hierfür muss unter anderem der Pfad von der Forschung bis zum Produkt, zum Beispiel auch durch Ausgründung, weiter gestärkt werden.

2.6 Führende Köpfe: qualifizieren und gewinnen

Hervorragende operative IT-Sicherheit, eine exzellente Forschungslandschaft sowie eine innovative IT-Sicherheitsbranche benötigen herausragende Fachkräfte. Diese müssen sowohl ausgebildet als auch gewonnen und langfristig am Innovationsstandort Deutschland gehalten werden. Hierzu müssen wir attraktive Rahmenbedingungen schaffen. Diese umfassen neben genereller Lebensqualität und finanziellen Aspekten auch herausfordernde berufliche Aufgaben, insbesondere auch bei staatlichen Einrichtungen, sowie Exzellenz und internationale Sichtbarkeit der Forschungsstandorte. Ziel des vorliegenden Programms ist es daher, Einrichtungen mit internationalem Renommee, wie die bestehenden nationalen Forschungszentren für IT-Sicherheit und anwendungsbezogene Forschungseinrichtungen, die IT-Sicherheit industrienah bearbeiten, weiterzuentwickeln und andere aufschließen zu lassen. Weiterhin soll das Programm exzellenten Forschenden ermöglichen, den europäischen Weg in der Digitalisierung maßgeblich mitzugestalten. Insgesamt zielt das Programm darauf ab, die Qualifikation im Bereich IT-Sicherheit durch Aus- und Weiterbildung weiter zu verbessern und so mehr exzellente Köpfe hervorzubringen. Diese Kombination aus starker Forschung, hoher Lebensqualität und hervorragendem Personal wird dazu beitragen, Deutschland zu einem der attraktivsten Standorte für die Entwicklung von IT-Sicherheitskomponenten weltweit zu machen.

2.7 Deutschland und Europa: technologisch souverän

Deutschland und Europa müssen in der Lage sein, Schlüsseltechnologien zu verstehen, zu entwickeln und wieder zu produzieren. Dies hat etwa die intensiv geführte Debatte um die Netzwerktechnik für die Mobilfunkgeneration 5G gezeigt. Die Wertschöpfungsketten der Informations- und Kommunikationstechnik (IKT) sind globalisiert und für Anwendende wenig transparent. Fragen der IT-Sicherheit werden oft nicht hinlänglich berücksichtigt. Als moderne Industrie- und Technologienation ist Deutschland jedoch auf diese IKT-Infrastrukturen angewiesen, wodurch das Risiko steigt, in Zukunft nicht selbstbestimmt und unabhängig agieren zu können. Ziel des vorliegenden Programms ist es daher, diese Abhängigkeiten zu reduzieren und europäische Alternativen zu entwickeln. Wir müssen Fähigkeiten schaffen beziehungsweise ausbauen, um zentrale sicherheitskritische Komponenten selbst zu entwerfen und zu produzieren. Ebenso benötigen wir das Know-how, um weniger sicherheitskritische Teile effizient zu prüfen, zu bewerten und zu integrieren. Offene Standards und Normen haben hierfür eine besondere Bedeutung, weil sie künftig eine sichere Basis für Systeme bilden können. Sowohl beim Aufbau notwendiger technischer Fähigkeiten als auch beim Setzen von Standards wird Deutschland im starken Verbund mit seinen europäischen Partnern handeln. Ziel ist es, eine strategische europäische Gesamtperspektive zu entwickeln, die auf die Errichtung eines europäischen Ökosystems entlang der Wertschöpfungskette ausgerichtet ist, die vorhandenen Stärken der etablierten Hersteller integriert sowie die Innovationspotenziale ausschöpft.

3 Herausforderungen für die IT-Sicherheit

Das vorliegende Rahmenprogramm thematisiert die aktuellen und zukünftigen Herausforderungen der IT-Sicherheitsforschung und differenziert dabei vier Handlungsfelder. Das Programm spiegelt die Digitalisierung in ihrer Gesamtheit und ihrer Auswirkung auf den gesellschaftlichen Wandel. Die damit einhergehende Durchdringung aller gesellschaftlichen Bereiche bedeutet, dass sowohl technologische als auch gesellschaftliche Themen in der IT-Sicherheitsforschung berücksichtigt werden müssen. So stehen neben technologiebasierten Innovationen auch Fragen zu Privatheit, Datenschutz und Selbstbestimmung im Fokus der Forschungsförderung. Ziel ist es, mit einer an diesem Anspruch orientierten Forschung europäischer Prägung Innovationen anzustoßen und dadurch die technologische Souveränität Deutschlands und Europas in Zukunft zu wahren und in wichtigen Schlüsselbereichen auszubauen.

3.1 IT-Sicherheit bietet Schutz und schafft Vertrauen

Digitale Systeme sind heute allgegenwärtig: Mobiltelefone, Smart Homes, Industrie 4.0, moderne Medizin, Autos, Züge und andere Kritische Infrastrukturen (KRITIS) sind ohne Vernetzungstechnologien, KI oder Mikroelektronik nicht mehr denkbar − und IT-Sicherheit ist unverzichtbar für das Vertrauen in sie. Die Gefahren, die von Angriffsvektoren wie beispielsweise Sicherheitslücken in Hard- oder Software ausgehen, sind bereits heute groß. Sie wachsen aufgrund der Allgegenwärtigkeit und Durchdringungstiefe digitaler Systeme drastisch weiter. Die IT-Sicherheitsforschung muss daher sowohl Lösungen für dringende Probleme von heute, als auch Lösungen für die Herausforderungen von morgen bereitstellen. Sie ist eine auf Dauer angelegte Aufgabe. In einem iterativen Prozess sind Risiken und Sicherheitsanforderungen immer wieder neu zu bewerten und entsprechende Lösungen regelmäßig anzupassen. Nur so kann aktuellen Gefahren und Herausforderungen von morgen gleichermaßen wirksam begegnet werden. Dabei besteht ein großes Ungleichgewicht, da IT-Sicherheit stets das komplette Gefahrenspektrum in angemessener Tiefe abdecken muss, während es für erfolgreiche Angriffe ausreicht, gezielt einzelne Angriffsvektoren auszunutzen. Berichte über Hackerangriffe, Schadprogramme, Datenmissbrauch und Identitätsdiebstahl − häufig sogar eigene Erfahrungen damit − verringern das Vertrauen in moderne digitale Systeme. Der Erfolg digitaler Technologien hängt jedoch maßgeblich davon ab, dass Menschen und Organisationen den eingesetzten Lösungen vertrauen können, sie breitflächig einsetzen und so die Chancen der Digitalisierung für Innovation, Wohlstand und gesellschaftliche Entwicklung nutzen können. Nur mit Nutzungsfreundlichkeit und einem risikoadäquaten Maß an IT-Sicherheit kann eine erfolgreiche und nachhaltige Digitalisierung gelingen. Für eine sichere digitale Zukunft brauchen wir deshalb Forschung, die nachweisbar sichere, dauerhaft über den Lebenszyklus verlässliche und nutzungsfreundliche IKT-Produkte und -Dienstleistungen entwickelt. Deutschland und Europa haben aktuell einen besonderen Vertrauensvorschuss im Hinblick auf Datensicherheit – diesen gilt es, durch gezielte Forschung zu nutzen, weiter auszubauen und in marktfähige Lösungen für Bürgerinnen und Bürger, für Unternehmen und für öffentliche Einrichtungen umzusetzen.

3.1.1 Digitale Infrastrukturen sicher entwickeln und einsetzen

Es ist wichtig, alle digitalen Systeme von Grund auf sicher zu gestalten und Sicherheit als zentrales Designprinzip zu verankern (Security by Design und Security by Default). Sicherheit muss hierfür mit komplexen Systemen und kurzen Entwicklungszeiträumen in Einklang gebracht werden. Dabei darf Sicherheit nicht mit dem Abschluss der Entwicklung enden, sondern muss im vollständigen Lebenszyklus von IKT-Systemen fest verankert sein. Da es für Anwendende, von Bürgerinnen und Bürgern über KMU bis hin zur Großindustrie, nahezu unmöglich ist, die Sicherheit jeder Komponente selbst zu prüfen und über einen möglichen Einsatz zu entscheiden, sind verlässliche Hilfen wie Zertifizierungen ebenso wie innovative Werkzeuge zur Prüfung und Messung der Sicherheit notwendig. In die Entwicklung solcher Hilfen muss die jeweilige Zielgruppe unmittelbar einbezogen werden, um eine spätere Nutzung sicherzustellen. Forschung kann auf all diesen Feldern große Fortschritte möglich machen.

Beispiele für künftige Handlungsfelder sind:

- **Sicherheit auf allen Systemschichten gewährleisten:**

Moderne IKT-Systeme sind aus vielen Einzelkomponenten zusammengesetzt. Es müssen sichere Komponenten (Software und Hardware) für alle Systemschichten und für die Komposition von sicheren Gesamtsystemen aus diesen Komponenten erforscht werden. Forschungsfragen sind unter anderem die Vergleichbarkeit und Transparenz der Sicherheitseigenschaften, die Abstimmung und Passfähigkeit von Soft- und Hardwarekomponenten (Hardware-Software-Co-Design), formale und statistische Sicherheitsnachweise, Ausschluss oder Mitigation von

Seitenkanälen sowie der Umgang mit unsicheren Komponenten. Hier bestehen besonders enge Anknüpfungspunkte zum Rahmenprogram der Bundesregierung für Forschung und Innovation 2021 – 2024 „Mikroelektronik. Vertrauenswürdig und nachhaltig. Für Deutschland und Europa“[3].

- **Edge- und Cloud-Computing-Infrastrukturen sowie Hyperscaler sicher gestalten:**

Es entstehen umfangreiche Datenräume in unterschiedlichsten Größen. Die mit GAIA-X avisierte verteilte europäische Dateninfrastruktur schafft auf Basis einer Architektur von Standards Interoperabilität. Perspektivisch wird ein Zugang zu passgenauen Lösungen ermöglicht, zum Beispiel für die Datenspeicherung (Clouds) und lokale Berechnungen (Edges). Solche Datenräume müssen sicher gestaltet und die Um- und Durchsetzung von Richtlinien für Datensouveränität sichergestellt werden.

- **Vertrauenswürdige Systeme zur sicheren Verarbeitung und Nutzung von Daten weiterentwickeln:**

Durch die immer umfangreichere Datafizierung ergeben sich große Herausforderungen für den vertrauenswürdigen Umgang mit Daten, insbesondere auch bei der immer breiteren Nutzung von KI. Wesentliche Forschungszweige behandeln hier die Methoden der vertraulichen und zweckgebundenen Verarbeitung und Bereitstellung von Daten. Diese Methoden können hardwarebasiert (zum Beispiel Confidential Computing, Trusted) aber auch softwarebasiert (zum Beispiel Secure Multiparty Computation, Private Information Retrieval, Differential Privacy) sein.

- **Sichere digitale Identitäten schaffen:**

Grundlage für sichere Kommunikation sowie deren praktische Umsetzung sind eindeutige Identitäten von Menschen oder Objekten. Dies gilt nicht nur für die individuelle Kommunikation, sondern insbesondere im Kontext sehr großer Systeme und von Systemen mit sehr vielen leistungsschwachen Komponenten wie im industriellen Internet der Dinge (Industrial Internet of Things − IIoT). Dazu zählt eine Verknüpfung mit dem digitalen Zwilling, mit der Verwaltungsschale und mit sicherheitskritischen Komponenten, in Hard- und in Software.

Cloud und Edge Security

Cloud-/Edge-Systeme bestehen aus zahlreichen Systemkomponenten, diese müssen perfekt aufeinander abgestimmt sein, um ein hohes Niveau an IT-Sicherheit zu gewährleisten. Dies beginnt bei den eigentlichen Geräten sowie den Netzwerken. Hier sind klassische Fragen wie Zugriffschutz zu adressieren. Insbesondere müssen auch die verschiedenen Datenströme sicher voneinander getrennt, geschützt und authentisiert werden. Im Rahmen des Zugriffs auf Daten sind insbesondere Identitäts- und Zugriffsverwaltung von großer Bedeutung. Neben der Sicherheit der Cloud/Edge Infrastruktur muss auch die Sicherheit der entstehenden Plattformen und Cloud-Anwendungen sichergestellt werden.

Ausgewählte Aspekte von Cloud Security:

- die physische Sicherheit der Rechenzentren,
- die Sicherheit der Server,
- die Sicherheit der Netzwerkstrukturen und Datenflüsse,
- die Sicherheit der Daten,
- das sichere Management Identitäten und Rechten,
- die Sicherheit der Plattform und der Anwendungen.

3.1.2 IT-Sicherheit verständlich und benutzbar entwickeln

Aktuelle IKT-Systeme sind hochgradig komplex und somit oft schwer zu verstehen und zu beherrschen. Die zugrundeliegenden systemischen Zusammenhänge sind für Nutzende in der Regel verborgen. In der Folge haben Menschen unvollständige oder falsche Vorstellungen von der Funktionsweise digitaler Technologien. Dies kann dazu führen, dass falsche Entscheidungen getroffen werden können und dadurch Sicherheitsprobleme auftreten. Hinweise wie „Das Dokument enthält potenziell gefährliche Inhalte. Wollen Sie fortfahren?“ stellen die Nutzenden vor gleich mehrere mentale Herausforderungen und einen Zielkonflikt. „Ist der Inhalt tatsächlich gefährlich?

[3] www.elektronikforschung.de/rahmenprogramm

Was heißt gefährlich? Habe ich Alternativen?“ versus „Ich möchte das Dokument lesen, aber keinen Schaden anrichten.“ Derartige Probleme betreffen nicht nur das Privatleben, sondern reichen auch in den Arbeitskontext hinein. Sie müssen insbesondere in sicherheitskritischen Bereichen vermieden werden, da sie die Nutzenden überfordern. Damit steigt das Risiko von Fehlentscheidungen, die Sicherheitsprobleme nach sich ziehen können. Die Ursache des Problems ist jedoch nicht bei den Menschen zu suchen, sondern in den mangelhaft gestalteten Systemen. Nicht alle Entscheidungen können automatisch getroffen werden; individuelle Entscheidungen werden auch in Zukunft notwendig sein und maßgeblich Einfluss auf Daten- und Systemsicherheit haben. Eine wesentliche Herausforderung ist es daher, zukünftige IKT-Systeme und insbesondere sicherheitskritische Entscheidungen klar, nachvollziehbar und insbesondere zielgruppengerecht zu gestalten.

Usable Security und Privacy

Neue Technologien halten ständig Einzug in unseren Alltag. Dabei werden bisher die Auswirkungen von Designentscheidungen auf die Sicherheit und den Datenschutz nicht mitgedacht. Zum Beispiel können neue Technologien sensible Daten generieren oder den Zugang zu sensiblen Daten ermöglichen. Daraus ergibt sich die Notwendigkeit, die Art und Weise, wie neue Technologien entwickeln werden grundlegend zu überdenken. Usable security und privacy zielt darauf ab, den Faktor Mensch zu berücksichtigen, um sowohl bestehende Sicherheitsmechanismen zu verbessern als auch neue Sicherheitsmechanismen zu entwerfen.

Einige aktuelle Themen im Bereich Usable security und privacy sind:

- Benutzer Authentifizierung,
- Biometrische Sicherheitsverfahren,
- Sicherheit bei Augmented Reality,
- Sichere Interaktion mit Smart Home Technologien,
- Ethische, psychologische und soziologische Aspekte von Sicherheit.

Beispiele für künftige Handlungsfelder sind:

- **Sicherheitskritische Schnittstellen nutzungsfreundlich und verständlich gestalten:**

Interaktionsschnittstellen für sensible Dienste wie Online-Banking, E-Mobility-Abrechnung oder digitale Verwaltungsdienstleistungen müssen nutzungsfreundlich und verständlich gestaltet werden können, um Fehlbedienungen möglichst auszuschließen.

- **Faktor Mensch besser verstehen:**

Um Schnittstellen für Nutzende sicher bedienbar zu machen, muss erforscht werden, welche mentalen Modelle bei unterschiedlichen Nutzungstypen vorliegen, unter anderem um bessere Hilfestellungen zur sicheren Bedienung geben zu können und vorauszusehen, wie welche Gruppen von Menschen Entscheidungen treffen, um darauf aufbauend passende Strategien für den Schutz der Nutzenden zu entwickeln.

- **Interfaces der Zukunft sicher designen:**

Neuartige Geräte verfügen häufig nicht über klassische Interaktionsmöglichkeiten wie Tastaturen oder Bildschirme. Für diese Geräte müssen sichere Interaktionsschnittstellen erforscht und entwickelt werden.

- **Werkzeuge zur Entwicklung von Programmen nutzungsfreundlicher machen:**

Auch Softwareentwicklerinnen und -entwickler müssen im Zusammenhang mit IT-Sicherheit unterstützt werden. Dazu zählt beispielsweise die Weiterentwicklung von Entwicklungsumgebungen und Werkzeugen, die es den Programmierteams erleichtern, auch ohne komplexes IT-Sicherheitswissen sichere Software schnell zu schreiben.

- **Digitale Souveränität durch Bildung stärken:**

Es bedarf Forschung zum optimalen und zielgruppengerechten Einsatz von modernen und innovativen Lehr- und Lernmethoden zur Vermittlung von Digitalkompetenz, insbesondere zur sicheren Nutzung von Geräten und Diensten.

3.1.3 Vertrauen in IKT durch IT-Sicherheit stärken

Angesichts von kriminellen Angriffen, Identitätsdiebstählen, Erpressungstrojanern und digitaler Wirtschaftsspionage bestehen häufig Bedenken hinsichtlich des Einsatzes von IKT-Systemen. Wirksame Maßnahmen gegen Cyberkriminalität, Sabotage und Spionage unterstützen das Vertrauen in digitale Systeme ebenso wie ein transparenter und sicherer Umgang mit Daten. Die zentrale Herausforderung ist es, Sicherheitseigenschaften wie die Stärke der eingesetzten Verschlüsselung, die organisatorische Sicherheit oder den Verfügbarkeitszeitraum von Updates transparent für die Nutzenden zu kommunizieren, damit diese so zu einem echten Entscheidungskriterium werden. IT-Sicherheit muss selbstverständlich werden. Es müssen wirksame Methoden geschaffen werden, um auch nicht selbst entwickelte IKT-Systeme und deren Komponenten auf Sicherheitseigenschaften zu testen. Zudem müssen Bürgerinnen und Bürger, öffentliche Einrichtungen sowie die Wirtschaft darauf vertrauen können, dass Vorfälle aufgeklärt werden. Hierzu müssen die Behörden, insbesondere die Strafverfolgungsbehörden, unter anderem mit entsprechenden IT-Werkzeugen in die Lage versetzt werden, digitale Spuren zu finden und beweissicher zu nutzen. Ebenso sind neue Ermittlungsverfahren und -taktiken notwendig, die nicht die Sicherheit aller verringern, mit den Grundrechten im Einklang stehen und mit der schnellen Entwicklung im Bereich IKT mithalten können. Neben den hier im Vordergrund stehenden technischen Fragen und Aspekten der IT-Sicherheit gibt es umfangreiche weitere Fragestellungen im Bereich Abwehr, Bekämpfung und Aufklärung von Cyberkriminalität. Diese werden im Rahmenprogramm der Bundesregierung „Forschung für die zivile Sicherheit 2018–2023“ zugehörige Fragestellungen adressiert.[4]

Künstliche Intelligenz und IT-Sicherheit

Künstliche Intelligenz (KI) und Lernende Systeme können das Leben vieler Menschen verbessern, wenn sie richtig eingesetzt werden. Damit das gelingt, müssen Politik, Wirtschaft, Wissenschaft und Gesellschaft gemeinsam offene Fragen diskutieren sowie Chancen und Risiken des technologischen Fortschritts ergründen. Auch der Bereich der IT-Sicherheit ist stark von den Entwicklungen im Bereich der Künstlichen Intelligenz betroffen. Erstens sind IT-Sicherheitsaspekte von KI-Systemen ein wichtiges und forderndes Forschungsfeld, zweitens können KI basierte Systeme dazu beitragen die IT-Sicherheit zu erhöhen und drittens können KI-Systeme auch eingesetzt werden um Angriffe auf andere IT-Systeme durchzuführen.

- IT-Sicherheit für Künstliche Intelligenz

  KI-Systeme inklusive ihrer Trainingsdaten müssen vor Angriffen und Manipulationen geschützt werden. Beispiele für Angriffe die adressiert werden müssen sind: Adversarial Attacks, Generative Adversarial Networks, Data Poisoning und Model Extraction.
- IT-Sicherheit durch Künstlicher Intelligenz
- KI kann digitale Systeme sicherer machen. Durch KI-Verfahren und Maschinelles Lernen (ML) können Schwachstellen oder Angriffsmuster automatisiert und selbstlernend erkannt bzw. abgewehrt werden. Beispiele für KI basierte Sicherheitsverfahren sind: Anomalieerkennung, Codeanalyse, Thread Identification, Neural Fuzzing, Malware Detection und Spam Detection.
- IT-Sicherheit gegen Künstliche Intelligenz

  Angreifende können Anwendungen der KI nutzen, um in IT-Systeme einzudringen. Entsprechend gilt es auch hier, bestehende Ansätze und Verfahren zur Abwehr stetig weiter zu entwickeln. Beispiele sind: Malware Mutation, Neural Fuzzing und Password Guessing.

Beispiele für künftige Handlungsfelder sind:

- **Sicherheit durch KI schaffen:**

Die Nutzung von Daten als Grundlage für Verfahren der KI gewinnt in vielen Anwendungen, Komponenten und Branchen immer mehr an Bedeutung. Doch Datengrundlagen können manipuliert werden, was Fehlentscheidungen provoziert. Dies ist insbesondere von Bedeutung, wenn Trainingsdaten aus einem geteilten Datenraum genutzt werden. Es werden Methoden und Verfahren benötigt, die Qualität und Herkunft von Daten zu verifizieren, insbesondere, wenn diese anonymisiert sind. In diesem Kontext ist die Frage der Grenzen der vollständigen Überprüfbarkeit und Nachvollziehbarkeit eines informationstechnischen Systems relevant. Die von der Datenethikkommission benannten fünf Kritikalitätsstufen für algorithmische Systeme können als grobe Orientierung zur

[4] https://www.sifo.de/de/sicherheitsforschung-forschung-fuer-die-zivile-sicherheit-1693.html

Beurteilung der Gefährlichkeit der Technikfolgen von KI-Systemen genutzt werden. Eine wichtige Frage für die Forschung ist, wie herkömmliche Zertifizierungs- und Auditierungsmechanismen der IT-Sicherheit dynamisiert werden können, um mit der rasanten Anpassungsgeschwindigkeit von Software Schritt zu halten.

- **Sicherheit für KI-Systeme und Anwendungen:**

KI-Anwendungen bieten eine breite Palette neuer Anwendungen. Für deren größtmöglichen Nutzen müssen diese Anwendungen sicher gestaltet sein und die KI muss über alle Ebenen ihres Einsatzes kontrollierbar sein. Nur so ist es möglich, KI-Anwendungen zu schaffen, die vertrauenswürdig sind und die bei großen Teilen der Gesellschaft auf Akzeptanz treffen. Damit diese Sicherheit und Vertrauenswürdigkeit allgemein und über einzelne Anwendungen hinweg sichergestellt werden kann, braucht es Konzepte und Lösungen für eine umfassende Zertifizierung von KI-Anwendungen, die nationalen und internationalen Maßstäben gerecht werden.

- **Sicherheitsvorfälle aufklären:**

Bei Sicherheitsvorfällen müssen die Eindringungswege und die Verbreitung in einem IT-System sehr genau und schnell bestimmt werden. Der angerichtete Schaden kann so nachvollzogen und im Sinne einer schnellen und passgenauen Antwort auf IT-Sicherheitsvorfälle eingedämmt und behoben werden (Incident Response). Von besonderer Bedeutung in diesem Zusammenhang ist auch die Weiterentwicklung von Verfahren zur gerichtsfesten Beweissicherung, der sogenannten IT-Forensik. Dies ist eine besondere Herausforderung, da Spuren in digitalen Systemen zumeist leicht veränderbar sind. Es besteht kontinuierlicher Forschungsbedarf, da die Forensik mit jeder neuen Innovation Schritt halten muss. Zur IT-Forensik gehört neben der Untersuchung „post mortem“ und der Online-Forensik auch die strategische und technische Vorbereitung von Systemen und Prozessen, um Forensik zu ermöglichen.

- **Muster bei Cyberkriminalität erkennen:**

Ebenso wie bei Einbruchsbanden sind bei Cyberkriminellen immer wiederkehrende Muster zu erkennen, wie sie bei Eindringversuchen vorgehen. Es muss erforscht werden, welche Muster es gibt und wie diese frühzeitig erkannt werden können, um ehestmöglich Warnungen und Handlungsempfehlungen zu veröffentlichen. Wichtig ist in diesem Zusammenhang auch eine Kooperation zum Austausch der Erkenntnisse. Hierfür bedarf es eines Baukastens zur Analyse und europäischer Standards zum Austausch von Informationen.

3.2 IT-Sicherheit braucht Nachhaltigkeit und ist Zukunftssicherung

IT-Sicherheit ist grundlegende Voraussetzung für den Einsatz digitaler Systeme und muss daher nachhaltig angelegt sein. Nachhaltigkeit bedeutet in Bezug auf IT-Sicherheit insbesondere, langfristig zu planen und zukunftsorientiert zu denken. Sie bedeutet zudem, IT-Sicherheit als dem Menschen dienlich zu verstehen. IT-Systeme sind stets Teil des sozialen Gefüges und sind somit soziotechnische Systeme. Aktuelle Systeme müssen abgesichert werden, doch auch die Technologien von morgen müssen in der Forschung und Entwicklung schon jetzt sicher gestaltet werden. Exzellentes Know-how aus der IT-Sicherheitsforschung muss deshalb im Sinne des Ansatzes „Security by Design“ immer von Anfang an in die Systementwicklung einfließen. Das heißt aus Nachhaltigkeitssicht auch, dass möglichst sämtliche Gruppen späterer Nutzender sowie unfreiwillig durch die Systeme Betroffene auch in den frühen Entwurfsphasen auf mindestens drei Ebenen mitbedacht werden: 1. Ein sicheres IT-System ist so gestaltet, dass spätere Nutzende es effektiv, effizient und zufriedenstellend bedienen können (Gebrauchstauglichkeit); 2. Ein sicheres IT-System ist insoweit fehlersicher, dass menschliche Eingabe- oder Bedienungsfehler unmöglich sind oder abgefangen werden; 3. Ein sicheres IT-System benachteiligt Menschen nicht aufgrund ihrer spezifischen Merkmale.

Eingesetzte Systeme müssen konsequent gewartet, aktualisiert und gegebenenfalls nachgerüstet oder gekapselt werden – insbesondere auch durch den schnellen Transfer aktuellster wissenschaftlicher Erkenntnisse. Neue Systeme müssen so entwickelt werden, dass sie langfristig aktualisiert werden können. Neben Sicherheitsaspekten trägt eine langfristige Nutzung auch zur Nachhaltigkeit bei. Nur so kann Deutschland auch zukünftig im internationalen Wettbewerb bestehen. Diese Herausforderung besteht für alle Anwendungsfelder und ist insbesondere für den deutschen Mittelstand entscheidend für künftigen Erfolg. Industrie 4.0 wird in nahezu allen Betrieben Einzug halten, 5G und perspektivisch 6G werden in allen Lebensbereichen relevant und müssen sicher gestaltet werden. Dabei kommt offenen Standards wie Open RAN eine zentrale Rolle zu, um die Sicherheit und digitale Souveränität Deutschlands und Europas zu gewährleisten. Die Herausforderung ist es, die sich beschleunigende

Digitalisierung und Vernetzung für Unternehmen und die Gesellschaft sicher zu gestalten. Voraussetzung hierfür ist eine IT-Sicherheitsforschung auf internationalem Spitzenniveau.

Open RAN

In Abgrenzung zu einem traditionellen Mobilfunknetz verfolgt Open RAN verstärkt die Trennung von Hardware und Software und zeichnet sich durch offene und überprüfbare Schnittstellen der Netzkomponenten aus. Mit Open RAN sollen geschlossene Mobilfunksysteme geöffnet werden (von vertikalen Marktstrukturen zu horizontal interoperablen Lösungen). Um dies zu ermöglichen, müssen Hersteller ihre Produkte durch die Verwendung offener, standardisierter Schnittstellen für Software von Drittanbietern öffnen. Offene und überprüfbare Schnittstellen tragen dazu bei, die Detektion und Mitigation von Spionage und Sabotage in 5G-Netzen zu ermöglichen. Darüber hinaus erhalten Netzbetreiber die Möglichkeit, die Netze mit Kombinationen verschiedener Lieferanten aufzubauen, was auch zu einem stärkeren Wettbewerb und besseren Angeboten für die Netzbetreiber führt. Mit der wachsenden Bedeutung von Software in der Netzsteuerung kann Open RAN für den Netzausbau Vorteile bieten. So können die Netze schneller mit neuen Technologien aktualisiert werden bzw. Sicherheitsprobleme schnell behoben werden.

3.2.1 IT-Sicherheit in Anwendungsfeldern stärken

Kein Unternehmen kann heute ohne eine funktionierende IKT-Infrastruktur bestehen. Bereits kleinste Geschäfte verfügen zumindest über ein digitales Kassensystem und zumeist auch über ein Zahlungsterminal. Der deutsche Mittelstand und internationale Konzerne sind ohne IKT-Systeme nicht denkbar und nicht wettbewerbsfähig. Videokonferenzen, vernetzte Produktion, Losgröße eins, Logistik-on-Demand oder prädiktive Instandhaltung sind nur einige der aktuellen Themen, die eine massive Digitalisierung voraussetzen und damit gleichzeitig die Relevanz der IT-Sicherheit weiter erhöhen. IT-Sicherheit ist für Unternehmen einerseits ein Kostenfaktor und muss sich daher anderen Kostenfaktoren in einem Wettbewerb stellen. Andererseits wertet die Eigenschaft IT-Sicherheit aber auch Produkte und Dienstleistungen auf und stellt einen Mehrwert dar. Zentrale Herausforderung für die Forschung zur IT-Sicherheit im gewerblichen Umfeld sind daher ökonomische Fragestellungen. Es müssen sichere digitale Ökosysteme mit sicheren Produkten und Anwendungen entlang der jeweiligen Wertschöpfungskette entwickelt werden. Eine wichtige Herausforderung in diesem Zusammenhang ist die Gestaltung der Kooperation von Unternehmen bei offenen Architekturen, Spezifikationen und Software für sichere Systeme. Diese bilden die Basis für eine sichere und souveräne Gestaltung und Nutzung von IKT-Systemen sowie der in ihnen verarbeiteten Daten und umgesetzten Prozesse.

Auch Kritische Infrastrukturen (KRITIS) sind digitalisiert und somit in ihrer Funktion von der IT-Sicherheit abhängig. Sie stehen unter besonderem Schutz. Die aktuellen gesellschaftlichen Aufgaben wie Energie- und Mobilitätswende oder eine nachhaltige und umfassende Gesundheitsversorgung wirken als Treiber für einen schnellen Um- und Ausbau großer Teile der KRITIS und deren weitere Digitalisierung. Im Zusammenhang mit KRITIS geht es neben wirtschaftlichen Fragestellungen auch um solche der Daseinsvorsorge. Aufgrund der daraus resultierenden notwendigen Zuverlässigkeit der Systeme stellen sich hier Anforderungen über das normale Maß hinaus. Zentrale Herausforderung ist es, gemeinsam mit den KRITIS-Betreibern und -Zulieferern Methoden und

Werkzeuge für eine zuverlässige digitale Absicherung der lebenswichtigen IT-Systeme zu entwickeln, sodass systemrelevante Versorgungsleistungen jederzeit garantiert werden können.

Netzwerksicherheit

Durch den allgegenwärtigen Einsatz von vernetzten IKT-Systemen in allen Bereichen ist Netzwerksicherheit ein besonders relevantes Thema der IT-Sicherheit. Die Schutzmaßnahmen und Technologien sind dabei genauso vielfältig wie die zu schützenden Systeme. Daher sind z.B. auch der Schutz von Cloud-Infrastrukturen und IoT-Systemen Teil der Netzwerksicherheit. Es gibt jedoch auch Maßnahmen und Technologien, welche weniger vom zu schützenden System abhängen. Einige dieser Technologien sind die folgenden:

- Software defined Security

Von Software defined Security spricht man, wenn Sicherheitsfunktionen von der Hardware abstrahiert werden, auf der sie laufen, und zu virtuellen Netzwerkfunktionen werden. Diese Virtualisierung ermöglicht zusätzliche Funktionen wie die Segmentierung und neue Sicherheitsebenen. Gerade in schnell wachsenden, volatilen Netzen wie sie im Bereich IoT und IIoT anzutreffen sind ist die Kombination von Software defined Security und Software defined Security ein relevanter Ansatz.

- Maschinenlesbare Bedrohungsinformationen

Kollaborative IT-Sicherheit ist gerade im Bereich von KMU von großer Bedeutung, da diesen die Ressourcen fehlen, um umfangreiche Informationen über aktuelle Bedrohungslagen selbst zu sammeln. Eine wichtige Technologie in diesem Zusammenhang sind maschinenlesbare Bedrohungsinformationen, welche zentral zusammengestellt und dann vielen Nutzenden zur Verfügung gestellt werden. Diese können dann Ihre Sicherheitsentscheidungen wie z.B. Firewall Regeln oder Intrusion Detection Systeme entsprechen automatisch anpassen.

- Cyber thread Intelligence und kooperative Cybersicherheit

Um eine effektive und schnelle Cyber-Verteidigung aufzubauen, benötigen Organisationen tiefe Einblicke in die Cyber-Bedrohungslandschaft, insbesondere aktuelle Bedrohungen und Fähigkeiten von zu erwartenden Angreifern. Entsprechende Systeme sammeln unterschiedliche Daten, analysieren sie und ermitteln so digitale Risiken. Diese Informationen dienen als Ausgangspunkt für zeitnahe, teils auch automatische, Sicherheitsmaßnahmen. Gerade im Bereich KMU, welche keine eigene Cyber Thread Intelligence betreiben können, kann durch Kooperation eine starke Verbesserung der Sicherheit erreicht werden.

Besonders relevante Anwendungsfelder sind:

- **IT-Sicherheit für Industrie 4.0**

Während digitale Endgeräte und Softwarelösungen ständig überarbeitet und angepasst werden und entsprechend einen relativ kurzen Lebenszyklus haben, sind Lebenszyklen bei Produktionsanlagen und IT-Systemen in der Produktion sehr lang. Daher bedarf es Konzepte und Lösungen für eine nachhaltige IT-Sicherheit über den gesamten Lebenszyklus der industriellen Maschinen und Anlagen hinweg, unter Berücksichtigung der industriellen Spezifika. Unter anderem sind Ansätze zu entwickeln, wie IT-Sicherheitslösungen im Nachhinein in Bestandssysteme integriert werden und wie Sicherheitsupdates ohne Beeinträchtigung von Betriebssicherheit durchgeführt werden können. Um die Lösungen vergleichbar und übertragbar zu gestalten, sind zusätzlich Konzepte zur Sicherheitszertifizierung nötig. Für die digitale Vernetzung der Produktion werden die einzelnen beteiligten Komponenten inklusive aller Eigenschaften sowie die Kommunikationsschnittstelle sogenannter digitaler Zwillinge gespiegelt und über eine sogenannte Verwaltungsschale gesteuert. Hierbei muss die Kommunikationsschnittstelle, aber auch der Zugriff auf die Verwaltungsschale selbst, sicher gestaltet sein. Im Rahmen der Industrie 4.0 wird nicht nur die sogenannte Operational Technology der Produktion untereinander vernetzt. Zunehmend findet auch eine Vernetzung mit den sonstigen IKT-Systemen im Unternehmen statt. Hieraus ergeben sich neue Herausforderungen an die Sicherheit, wozu es spezifischer Sicherheitslösungen bedarf.

- **IT-Sicherheit für Medizin, Gesundheit und Pflege**

Die Digitalisierung schreitet auch in der Medizin weiter voran und betrifft dort alle Bereiche von der allgemeinmedizinischen Praxis über das Labor bis hin zu den Menschen in Behandlung. Entsprechend sind auch für alle digitalen Anwendungen in diesen verschiedenen Bereichen nutzungsfreundliche, wirtschaftliche und zukunftsfähige Sicherheitslösungen und -konzepte notwendig, die die Sicherheit auf allen Ebenen gewährleisten. Beispiele sind die Vernetzung der Medizintechnik in Laboren und Krankenhäusern, die Integration von mobilen Geräten in klinische IT-Umgebungen (zum Beispiel Tablets für die digitale Patientenakte), digitale Anwendungen in der medizinischen Betreuung im Wohn- und Pflegebereich (etwa Medikationsapps), Telemedizin beispielsweise in der hausärztlichen Betreuung, Health-Wearables (zum Beispiel Fitnessarmbänder) sowie Apps und Chatbots zur Unterstützung der medizinischen Diagnosestellung. Da medizinische Daten, insbesondere auch in klinischer Forschung, besonders sensibel sind und zunehmend in das Visier von Cyberkriminellen rücken, müssen zudem übergeordnet neue Anwendungen und Konzepte entwickelt werden, die eine sichere Speicherung und nachvollziehbare Nutzung aller körperlichen Fitness- und medizinischen Daten zulassen. Gleichwohl sind Haftungsfragen zu klären, für den Fall, dass medizinische Daten gehackt werden. IT-Sicherheitssysteme sind nicht unfehlbar und Fehler haben weitreichende juristische und finanzielle Konsequenzen, besonders in Bereichen mit sehr sensiblen Daten. Insbesondere die schleichenden Übergänge zwischen dem medizinischen Kernbereich mit Vorsorge, Diagnose und Behandlung sowie den angrenzenden Anwendungsfeldern sind von Interesse, da die Zulassungsverfahren von Medizinprodukten nicht greifen. Aber auch die sichere Nutzbarhaltung und Modernisierung von bestehenden technischen Bestands- und Altsystemen muss Gegenstand weiterer Anstrengungen sein. IT-Sicherheit ist auch gefährdet, wenn medizinisches Personal unzulänglich im Umgang mit digitalen Systemen geschult ist und die notwendige Sensibilisierung für IT-Sicherheit nicht ausreichend erfolgt.

- **IT-Sicherheit in sensiblen Infrastrukturen**

Immer mehr Alltagsgeräte, vom Kühlschrank über das Babyphone bis hin zur Kaffeemaschine, verfügen über digitale Schnittstellen, sind über das Internet miteinander vernetzt und bilden so das Internet der Dinge (Internet of Things − IoT). Da viele dieser Geräte beispielweise als Smart-Home-Anwendungen äußerst private Daten sammeln oder gegebenenfalls auch direkten digitalen Zugriff auf unsere Kinder zulassen sowie neue Formen digitaler (häuslicher) Gewalt insbesondere gegen Frauen mit sich bringen können (beispielsweise heimliche Stalking-Apps auf dem Smartphone der Ex-Partnerin, heimliche Raumüberwachung durch Privatpersonen, Upskirting), sind sie besonders sensibel und müssen mit flexiblen und innovativen Lösungen im Sinne des Privatheitsschutzes sicher gestaltet werden. Eine weitere sensible Infrastruktur sind Rechenzentren, insbesondere auch Hochleistungsrechenzentren, da hier die Daten einer Vielzahl an Anwendungen zusammenlaufen und Angriffe entsprechend große Auswirkungen haben können. Besonders wichtig ist es daher, auch hier Ansätze und Lösungen weiterzuentwickeln, die der Relevanz und Exposition dieser Anlagen gerecht werden.

- **IT-Sicherheit in Kritischen Infrastrukturen**

KRITIS wie zum Beispiel das Schienennetz, bei der Strom- oder der Wasserversorgung, in Krankenhäusern aber auch im Finanzsektor sind systemrelevant für unser gesellschaftliches Leben und bedürfen daher eines besonderen Schutzniveaus, insbesondere da Angriffe auf KRITIS auch hierzulande in den letzten Jahren stattgefunden haben. Da die Angreifenden immer neue Techniken und Ressourcen einsetzen, müssen Angriffspotenziale und mögliche Gegenmaßnahmen bei KRITIS stetig anhand neuer Lösungen und Konzepte bewertet und analysiert werden. Angesichts der sich fortlaufend ändernden Bedrohungslage gilt es, immer wieder neue, umfassende digitale Schutzkonzepte für die IT-Infrastrukturen der KRITIS zu entwickeln. Hierzu beitragen können auch Lösungen zum Erkennen von Störungen und Anomalien, die auf KI basieren und die gegebenenfalls auch automatisiert Abwehrmaßnahmen einleiten. Damit dies möglich wird, sind Konzepte notwendig, die übergeordnet sicherheitsrelevante Ereignisse in Echtzeit erfassen und bewerten. So können Echtzeitlagebilder entstehen, aus denen entsprechende Maßnahmen zum Schutz der IT-Infrastrukturen ableitbar sind. Zudem gilt es, wie in der Industrie 4.0, Lösungen dafür zu entwickeln, wie auch in KRITIS bereits vorhandene IT-Infrastrukturen an die sich ändernden Sicherheitsrahmenbedingungen angepasst werden können. Neben diesen Maßnahmen ist das Problembewusstsein für IT-Sicherheit bei KRITIS-Betreibern durch öffentlichkeitswirksame Maßnahmen und gezielte Ansprache zu schärfen. Einige KRITIS-Bereiche können nur EU-weit geschützt werden, wie der Finanzdienstleistungs- und der schienengebundene Transportsektor, andere können auch im deutschen Wirtschaftsraum geschützt werden, wie das digitale Gesundheitssystem.

IoT-Sicherheit

IoT-Geräte kommen meist in großer Anzahl und in den unterschiedlichsten Größen, Bauformen und Leistungsklasse vor. Daher sind klassische Sicherheitsmechanismen wie Endpoint-Security schwierig umzusetzen. Auswahl wichtige Maßnahmen der IoT-Sicherheit im Überblick:

- Systementwicklung

IoT-Sicherheit erfordert einen holistischen Ansatz. Sicherheit muss über den gesamten Produktlebenszyklus zentral Berücksichtigt. Es ist entscheidend, Sicherheit bereits in der Designphase von Hardware und Software zu berücksichtigen.

- Netzwerksicherheit

IoT-Netzwerke sind zunehmend drahtlos. Dies erhöht die Komplexität der Herausforderung IoT-Netzwerke sicher zu betrieben, da es eine Vielzahl von neuen HF- und drahtlosen Kommunikationsprotokollen und -standards gibt.

- Authentifizierung

IoT-Geräte müssen von allen legitimen Benutzern authentifiziert werden. Die Methoden für eine solche Authentifizierung reichen von statischen Passwörtern bis hin zu Zwei-Faktor-Authentifizierung, Biometrie und digitalen Zertifikaten.

- Verschlüsselung

Verschlüsselung ist notwendig, um unbefugten Zugriff auf Daten und Geräte zu verhindern und die Authentizität von Daten sicherzustellen. Dies ist aufgrund der Vielfalt der IoT-Geräte und Hardware-Profile eine besondere Herausforderung.

- Seitenkanalanalyse

Selbst bei ausreichender Verschlüsselung und Authentifizierung ist eine weitere Bedrohung möglich, nämlich Seitenkanalangriffe. Seitenkanalangriffe sammeln Betriebscharakteristika wie zum Beispiel Ausführungszeit, Stromverbraucher und elektromagnetische Abstrahlung um kryptographische Schlüsseln auszulesen. Solche Seitenkanäle müssen erkannt und abgesichert werden.

- **Autonomes und vernetztes Fahren**

Ein Beispiel für besondere Sensibilität ist der Bereich des autonomen und vernetzten Fahrens. Diese Art der Fahrzeugführung wird dadurch möglich, dass eine Vielzahl an Daten durch das Fahrzeug und die Infrastruktur erfasst und ausgewertet werden. Eine Manipulation der Daten kann im schlimmsten Fall zu Unfällen, mindestens aber zu großflächigen Störungen der Verkehrssysteme führen. Entsprechend relevant ist es, Lösungen, Konzepte und Prüfverfahren zu entwickeln, die im Kontext des autonomen und vernetzten Fahrens sichere Gesamtinfrastrukturen ermöglichen. Dies reicht von einzelnen Komponenten und Fahrzeugen über Datenschnittstellen bis zur sicheren Einbindung der Leit- und Sicherungssysteme für Straße und Schiene mittels IoT-basierter Kommunikationswege.

- **Vertrauenswürdige und sichere Lieferketten**

Lieferketten müssen umfassend abgesichert werden, beispielsweise durch die Schaffung von sicheren digitalen Schnittstellen und Standards zwischen den einzelnen Produktionsbeteiligten entlang der kompletten Wertschöpfungskette. Ebenso sind technische Sicherungen wie beispielsweise Physically Unclonable Functions, Reproducible Builds und Distributed Ledger sowie grundlegend neue Testverfahren erforderlich. Durch die Digitalisierung sind Produktionsprozesse ebenso wie Dienstleistungen auch über Unternehmensgrenzen hinweg sehr stark miteinander vernetzt. Dadurch können Sicherheitsprobleme an einer Stelle der Produktion schnell zu Schwierigkeiten an einer anderen Stelle im Prozess führen und sich von einem Unternehmen auf das andere übertragen. Im Zuge der Datafizierung können auch Datenflüsse als Teil der Lieferkette gesehen werden und müssen ebenso authentisiert und gesichert werden.

- **Querschnittsbereiche, die branchenübergreifend Mehrwerte schaffen**
    - Um IT-Systeme sicher zu gestalten, sind von Unternehmen, aber auch von Privatnutzenden Investitionen notwendig. Deren finanzieller Nutzen wird, wenn überhaupt, erst im Nachhinein − nach einem

erfolgreichen oder abgewehrten Angriff − deutlich, weshalb nach wie vor nicht ausreichend in IT-Sicherheit investiert wird. Hierzu sind detaillierte und maßgeschneiderte Analysemethoden und Werkzeuge notwendig, die insbesondere KMU in den Blick nehmen, um mögliche Schäden durch Cyberangriffe zu quantifizieren und die Vorsorge ökonomisch planen zu können.

- Um eigene Ressourcen zu schonen, lagern Unternehmen insbesondere bei der Datenverarbeitung und -speicherung zunehmend interne Prozesse auf digitale Infrastrukturen Dritter aus, zum Beispiel per Cloud-Computing. Hierbei ergeben sich zahlreiche Sicherheitsrisiken, welche adressiert werden müssen. Es bedarf weitgehend automatisierter Kontroll- und Überwachungsmechanismen für die Einhaltung von Sicherheitsstandards, die von der Kundschaft selbst oder von Dritten genutzt werden können, unabhängig von Standort und Rechtsrahmen des Unternehmens, das den jeweiligen Service anbietet (zum Beispiel kontinuierliches Audit).

3.2.2 IT-Sicherheit in der Quanteninformationsverarbeitung frühzeitig entwickeln

Wie bei den heutigen informationsverarbeitenden Systemen spielt die IT-Sicherheit auch in der Verarbeitung und Nutzung von Quanteninformationen eine wichtige Rolle. Vernetzte Quantencomputer oder Quantensensoren können ebenso Ziel von Angriffen werden wie gewöhnliche Computer und Informationssysteme. Damit Quantentechnologien zukünftig in Industrie und Gesellschaft ihr volles Potenzial entfalten können, müssen ganzheitlich sichere Architekturen für die Quanteninformationsverarbeitung geschaffen werden. Die Nutzung quantenmechanischer Verschränkung über ganze Netzwerkstrukturen wird es ermöglichen, weitere innovative Sicherheitskonzepte zu realisieren.

Eine Schlüsseltechnologie für Abhörsicherheit ist zudem die Quantenkommunikation. Sie ermöglicht es, durch die Nutzung grundlegender physikalischer Effekte die Vertraulichkeit von sensiblen Informationen zu wahren − und leistet damit einen wichtigen Beitrag für Deutschlands technologische Souveränität. Die Quantenkommunikation bietet dabei nicht nur neue Sicherheitsmechanismen für die heute gängige Informationsverarbeitung, sondern auch für die Quanteninformationsverarbeitung.

Die Forschung zur Quantenkommunikation beschäftigt sich bislang hauptsächlich mit der abhörsicheren Übertragung von Schlüsseln. Bei der Verteilung von Schlüsseln bestehen andere, zum Teil geringere Anforderungen an die Übertragungsqualität als bei der Vernetzung von Quantencomputern. Auf dem Weg zu einer zukünftigen Version des heutigen Internets, das Quantenkommunikation umfasst, stellt die Entwicklung leistungsfähiger Komponenten zum Prozessieren und Speichern von Quanteninformationen und zur Verarbeitung quantenoptischer Signale eine große Herausforderung dar. Weitere Herausforderungen bestehen bei der Erforschung und Entwicklung geeigneter Quantennetzwerkstrukturen und deren Implementierung in Verbindung mit bestehenden klassischen Infrastrukturen. Das bereits vorhandene Know-how aus Deutschlands hervorragend aufgestellter Grundlagenforschung muss dafür auf Umsetzungspartner transferiert werden, die es in die Anwendung bringen. Neben den Aspekten der IT-Sicherheit, die in diesem Programm adressiert werden, werden die technologischen Grundlagen zukünftiger quanteninformationsverarbeitender Systeme im aktuellen Rahmenprogramm der Bundesregierung „Quantentechnologien – von den Grundlagen zum Markt“[5] sowie dem kommenden Forschungsprogramm Quantensysteme adressiert[6].

Quantenkommunikation

Die Quantenkommunikation ist eine Schlüsseltechnologie für abhörsichere Vernetzung auf Basis grundlegender physikalischer Effekte. Sie bietet auch zukünftig Abhörsicherheit vor dem Hintergrund, dass leistungsfähige Quantencomputer schon bald viele kryptografische Verfahren entschlüsseln könnten, die heute z. B. beim Online-Banking oder beim Abrufen von E-Mails verwendet werden. Die weltweite Forschung befindet sich derzeit im Wettbewerb um die ersten anwendungstauglichen Quantenkommunikationssysteme. Dabei gilt es die aktuell sehr vielfältigen technologischen Ansätze zu erproben, zu kombinieren und in bereits existierende Kommunikations- und IT-Infrastrukturen einzubetten. Diese Schritte sowie die Entwicklung von geeigneten Quantennetzwerkstrukturen und skalierbaren Quantenkommunikationskomponenten stellen derzeit große Herausforderungen dar, die zur Entwicklung zukünftiger praxistauglicher Quantennetzwerke überwunden werden müssen.

---

5 https://www.quantentechnologien.de/qt-in-deutschland/programm.html

6 https://www.quantentechnologien.de/ (in Vorbereitung)

Beispiele für künftige Handlungsfelder sind:

- **Sichere und effiziente Quantennetzwerke:**

Theoretische und experimentelle Grundlagen zur Architektur sicherer und effizienter Quantennetzwerke müssen weiterentwickelt und deren Einbindung in klassische Netzwerke weiter untersucht werden – beispielsweise in den Bereichen quantenlogische Signalverarbeitung, Fehlerkorrekturmechanismen, Netzwerkprotokolle und weitere innovative Konzepte der Kodierung von Quanteninformation zur Verbesserung des Leistungsvermögens derzeit bestehender Systeme.

- **Quantenmechanisch basierte Sicherheitskonzepte:**

Die Leistungsfähigkeit und Robustheit von Quantenkommunikationskomponenten sowie für andere quantenmechanisch basierte Sicherheitskonzepte müssen verbessert und ihre Sicherheitseigenschaften detailliert erforscht werden.

- **Verbesserung von sicheren Quantenkommunikationssystemen:**

Es bedarf der Entwicklung hybrider Quantenkommunikationssysteme auf Basis faseroptischer Kommunikation und Freiraumkommunikation unter Verwendung verschiedener Arten von Quantenspeichern.

- **Sichere Quanteninformationsverarbeitungssysteme:**

Mögliche Angriffsstrategien auf Systeme zur Quanteninformationsverarbeitung müssen analysiert und wirksame Gegenmaßnahmen zur Verbesserung der IT-Sicherheit entwickelt werden.

3.2.3 Zukünftige Technologien der IT-Sicherheit beherrschen

Ein schnell voranschreitendes Forschungsgebiet sind neue Rechner- und Chiparchitekturen, wie Quantencomputing und andere, die dem „Beyond-von-Neumann"-Trend folgen. Diese sind für Spezialanwendungen häufig deutlich leistungsfähiger. Basierend auf den Erkenntnissen über Schwächen bisheriger Architekturen, wie der am weitesten verbreiteten Von-Neumann-Architektur, muss Sicherheit von Anfang an mitgedacht werden. Herausforderungen dabei sind sowohl die grundlegende Erforschung von Angriffsmöglichkeiten auf solche Architekturen als auch die Entwicklung von leistungsfähigen Sicherheitskonzepten, um solche Angriffe abzuwehren. Mit der, nach Einschätzung von Expertinnen und Experten wahrscheinlichen, Verfügbarkeit von fehlertoleranten und leistungsfähigen Quantencomputern werden die meisten asymmetrischen kryptografischen Verfahren, die heute relevant sind, keine ausreichende Sicherheit mehr gewährleisten können. Die verwendeten Schlüssel können von Quantencomputern ermittelt werden, damit ist die Verschlüsselung gebrochen. Dieser Herausforderung muss mit weiterer Forschung an Post-Quanten-Kryptografie und Kryptoagilität begegnet werden.

Neben Bedrohungen durch gänzlich neue Architekturen und Konzepte muss insbesondere der Bereich KI fokussiert werden. In wenigen Jahren wird eine immense Zahl von digitalen Systemen KI-Komponenten enthalten. Daher wird die Sicherheit von KI sämtliche digitalen Systeme maßgeblich beeinflussen. Die Forschung und Entwicklung zur Absicherung dieser Systeme muss wesentlich schneller erfolgen als bei bisherigen neuen Technologien.

Beispiele für künftige Handlungsfelder sind:

- **Sichere Verschlüsselungsverfahren für die Zukunft:**

Die klassische Public-Key-Kryptografie muss mit Blick auf die Bedrohung durch Quantencomputer durch alternative Verfahren der Post-Quanten-Kryptografie ersetzt oder ergänzt werden. Entsprechend muss erforscht werden, wie Komponenten, die klassische Public-Key-Kryptografie verwenden, in das Zeitalter der Post-Quanten-Kryptografie überführt werden können, beziehungsweise wie diese klassische Kryptografie mit Verfahren der Post-Quanten-Kryptografie und Quantenkryptografie kombiniert werden kann.

- **Sicherheit von neuen Rechner- und Chiparchitekturen:**

Verschiedene Forschungsgebiete beschäftigen sich mit der Erhöhung der Rechenleistung und sind disruptive Konzepte des „Beyond-von-Neumann"-Trends. Beispiele sind „Rechnen-im-Speicher", „neuromorphe Chips", „künstliche Synapsen" und „Analogrechner". Auch bei diesen Neuentwicklungen gilt es, das Konzept der

Security by Design von Grund auf mitzudenken und umzusetzen. Im Bereich von neuromorphen Chips sowie anderen neuen Chiparchitekturen müssen insbesondere auch Sicherheitsrisiken von Anfang an mit untersucht werden. Diese ergeben sich aus der Vernetzung vieler solcher Chips, unter anderem für Zugriffskontrollen, Fernwartung, Betriebssicherheit, Überwachung, Wartung o der Fehlerkorrekturverfahren.

- **Sicherheit zukünftiger Quantencomputer:**

Als gänzlich neue Umgebung der digitalen IKT bietet der Bereich Quantencomputing die Möglichkeit, die Sicherheit der Anwendungen im Sinne des Ansatzes der Security by Design von vorneherein mitzudenken und Lösungen und Konzepte für die Zukunft zu entwickeln, damit diese bei der Entwicklung anwendungsreifer Systeme zur Verfügung stehen.

3.3 IT-Sicherheit schützt Privatheit und stützt Demokratie

Um die Privatheit jedes einzelnen Menschen ebenso wie unsere demokratische Gesellschaft als Ganzes zu stärken, brauchen wir Forschung und Innovation in der IT-Sicherheit. Denn digitale Technologien bieten viele Möglichkeiten der Kontrolle und Überwachung – und sind damit potenziell eine Bedrohung für die informationelle Selbstbestimmung von Menschen. IT-Sicherheitstechnologien können durch Ansätze wie Privacy by Design und Security by Design sowie Privacy by Default und Security by Default Menschen Kontrolle, Selbstbestimmung und Souveränität über ihre Daten ermöglichen − auch in einer vollvernetzten Welt.

Die bekannten Schutzziele der Informationssicherheit, zu der die IT-Sicherheit gehört, sind Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und deren Gewährleistung (siehe IT-Grundschutz-Kompendium des BSI). Das bedeutet, dass IT-Sicherheit den Datenschutz in einer besonderen Weise stützt.

Informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind in Deutschland zentrale Grundrechte, die durch Datenschutz realisiert werden. Diese Grundrechte sind aus dem allgemeinen Persönlichkeitsrecht (Artikel 2 Absatz 1 und Artikel 1 Absatz 1 des Grundgesetzes) abgeleitet. In Verbindung mit dem Diskriminierungsschutz durch Artikel3 Absatz 2 und 3 des Grundgesetzes bedeutet dies zudem, dass Menschen durch automatisierte Datenverwendung auch nicht aufgrund rassistischer Zuschreibungen, ihres Geschlechts, ihrer Religion oder Weltanschauung, ihrer Behinderungen oder ihrer Herkunft benachteiligt werden dürfen und die Gleichberechtigung von Männern und Frauen gefördert werden muss. Auch die EU sichert in ihrer Grundrechtecharta mit den Artikeln 7 und 8 Schutz vor Überwachung und unbefugtem Datenzugriff und den Artikeln 20, 21 und 23 Diskriminierungsschutz zu. Die DSGVO ist hier eines der wichtigsten EU-weiten Regelwerke. Datenschutz ist jedoch durch neue digitale Technologien und höhere Komplexitäten laufend herausgefordert. Denn inzwischen gehört es zu vielen Geschäftsmodellen, umfangreiche Daten, insbesondere über Personen, zu erfassen und zu nutzen. Häufig geht es dabei um sensible Informationen wie Gesundheitsdaten, Kommunikationsinhalte oder das individuelle Surf- und Kaufverhalten. Durch die allgegenwärtige Vernetzung sammeln neben smarten Fernsehern und digitalen Assistenten inzwischen auch Lichtsysteme, Staubsauger, Kühlschränke und Fahrzeuge Informationen über ihr Umfeld. Und dies sind nur Beispiele: Denn in Zukunft wird das Internet der Dinge, befördert von neuen Vernetzungstechnologien wie 5G und 6G, enorm anwachsen und allgegenwärtig sein, Daten sammeln und so auch Aufschluss über Nutzungsverhalten geben.

Online-Plattformen bringen sehr viele Nutzende zusammen. Begünstigt durch Netzwerkeffekte entsteht eine Plattformökonomie mit großen Marktanteilen einzelner Unternehmen. Während soziale Medien und Messengerdienste Menschen ermöglichen, sich spielend leicht miteinander zu verbinden, werden dort auch in großem Umfang Desinformationen verbreitet. Die Herausforderung für die Forschung ist es, Lösungen zu entwickeln und anzubieten, die in Daten- und Plattformökonomien eine Balance zwischen persönlichem Nutzen, wirtschaftlicher Verwertung, Demokratie und Datenschutz ermöglichen. Der Schutz von Daten ist hier keineswegs ein Hemmnis für Innovation, sondern durch neue Anforderungen und Ziele ein wichtiger treibender Faktor. Es gilt zu zeigen, dass privatsphäreschonende Geschäftsmodelle und die Vermeidung der Diskriminierung von Nutzenden (beispielsweise durch Gender Targeting bei Stellenanzeigen, diskriminierende Auftragsvergabe auf Plattformen), insbesondere durch den Einsatz innovativer technischer Lösungen, ökonomisch tragfähig sein und dass digitale Möglichkeiten Demokratien stärken können. Im Zuge der Übernahme von Regelungen der DSGVO werden auch international Technologien benötigt, die die Privatsphäre schonen und verbessern. Deutschland hat hier aufgrund der starken Datenschutzgesetzgebung einen Vorsprung in Wissen und Technik. Dieser Vorsprung muss konsequent ausgebaut und langfristig als Standortvorteil etabliert werden. Hierzu gehört auch, Erfahrungen mit Problemen durch

Datenschutz konsequent zu adressieren, diese als wichtige Impulse für Innovation zu nutzen und Alternativen zu entwickeln, welche datenschutzfreundlich und nutzbar sind.

3.3.1 Grundrechte und informationelle Selbstbestimmung schützen

Sichere IKT-Systeme und Verschlüsselung sind wichtige Grundlagentechnologien, die Nutzende in die Lage versetzen, ihr Recht auf digitale Selbstbestimmung wahrzunehmen und selbst zu entscheiden, welche Daten über sie erhoben und wie diese Daten genutzt werden dürfen. Über die eigentlichen Inhalte hinaus sind sogenannte Metadaten von immer größerem Interesse. Diese können auch Rückschlüsse auf personenbezogene Daten wie Alter oder Geschlecht ermöglichen, selbst wenn diese nicht explizit erhoben werden. Auch hier leisten Technologien aus der IT-Sicherheit wie zum Beispiel die der Anonymisierung einen wichtigen Beitrag zur Selbstbestimmung von Bürgerinnen und Bürgern. Eine der Herausforderungen ist es, Technologien von Grund auf so zu gestalten, dass sie die Grundrechte der Bürgerinnen und Bürger nicht aushöhlen, sondern sie in der Wahrung ihrer Rechte und der Kontrolle über ihre Daten unterstützen. Hierzu bedarf es neben technischer, verständlicher Schutzlösungen auch eines Diskurses, welche Art der Datennutzung erwünscht ist und wie eine zeitgemäße Interpretation der Grundrechte aussieht. Hierbei muss insbesondere die europäische Dimension berücksichtigt werden.

Beispiele für künftige Handlungsfelder sind:

- **Bürgerinnen und Bürger bei der Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung unterstützen:**

Es muss untersucht werden, wie der Schutz der Grundrechte bei allen technischen Entwicklungen berücksichtigt werden kann (Privacy by Design und Privacy by Default sowie Security by Design und Security by Default).

- **Datenschutz technisch umsetzen:**

Es bedarf Konzepte und benutzbarer Werkzeuge zur Durchsetzung der Zweck- und Kontextbindung personenbeziehbarer Daten, technisch wie rechtlich. Zudem sollen auch die Rahmenbedingungen zur kollektiven Wahrnehmung von Betroffenenrechten, zum Beispiel in Form von Datentreuhändern, untersucht und gegebenenfalls entsprechende Konzepte für die Umsetzung entwickelt werden.

- **Privatsphäreschonende Technologien (Privacy Enhancing Technologies, PETs) und Geschäftsmodelle entwickeln:**

Zur Etablierung von Datenschutz als Innovationstreiber müssen tragfähige und die Privatsphäre schonende Geschäftsmodelle entwickelt und erprobt werden. Weiterhin bedarf es auch PETs, um die sichere digitale Teilhabe zu stärken. Dies umfasst unter anderem Depersonalisierung und Anonymisierung von Daten ebenso wie weitere Verfahren, die eine sichere, mehrwertige Verarbeitung von Daten ermöglichen. Dazu gehört beispielsweise Private Information Retrieval (PIR) und Secure Multiparty Computation (SMPC).

- **Zukunftstechnologien privatsphäreschonend gestalten:**

Von besonderer Bedeutung ist es, KI-, IoT- und Cloud-Systeme privatsphäreschonend zu gestalten (Privacy Preserving Computing) und Konzepte für effiziente und privatheitsfreundliche Werbung zu entwickeln. Besonderes Augenmerk ist auf Systeme in besonders sensiblen Bereichen wie etwa der Personalauswahl zu richten.

- **Einbeziehung von Technik- und Datenschutzfolgenabschätzungen:**

Neben technischen Konzepten sind umfassende Datenschutzfolgenabschätzungen im Sinne der DSGVO – auch im Hinblick auf mögliche Diskriminierungen – ein wichtiges Instrument, um den Grundrechtsschutz beim Einsatz digitaler Technologien zu gewährleisten. Daneben helfen Technikfolgenabschätzungen, die Gefahr unerwünschter Auswirkungen von IT-Systemen bereits frühzeitig zu erkennen. Um diese Verfahren von Anfang an in der Systementwicklung mitzudenken, müssen diese fest in die technische Entwicklungsperspektive integriert werden.

- **Risikoabschätzungen vornehmen:**

In die Forschung zu IT-Sicherheit müssen Rechts-, Sozial- und Ethikwissenschaftlerinnen und -wissenschaftler eingebunden werden, um Technologien dahingehend zu bewerten, inwiefern sie die Privatsphäre gefährden oder Menschen diskriminieren.

Privacy Enhancing Technologies (PETs)

Technologien zum Schutz der Privatsphäre sind Technologien, die grundlegende Datenschutzprinzipien verkörpern, indem sie die Erhebung personenbeziehbarer Daten minimieren oder die Nutzung dieser Daten bei gleichzeitigem Schutz der Privatheit ermöglichen. Die dabei bearbeiteten Fragen und Problemstellungen sind auf allen Ebenen von IKT-Systemen und Infrastrukturen angesiedelt und die genutzten Technologien entsprechend vielfältig.

Ein Ausschnitt der Technologien sind die folgenden:

- Privacy Preserving Data Mining,
- Secure Multiparty Computation,
- Zero-knowledge proofs,
- Homomorphic encryption,
- Anonymous credentials,
- Privacy-Preserving Routing Protocols.

3.3.2 Desinformation bekämpfen

Digitale Desinformationskampagnen stellen demokratische Systeme vor große Herausforderungen. Die Verbreitung von schwer als solche zu erkennenden Falschinformationen schwächt die faktenbasierte Berichterstattung und erschwert es politischen Akteuren, Behörden, Medien und Bürgerinnen und Bürgern, sich ein verlässliches Bild zu machen. Über Chatgruppen, soziale Netzwerke, Videoplattformen und Blogs werden Falschinformationen und Verschwörungserzählungen verbreitet. Dabei tritt die tatsächliche Information und ihr Wahrheitsgehalt in den Hintergrund. Es geht in vielen Fällen nur darum, Emotionen auszunutzen und letztlich Unsicherheit zu erzeugen. Durch die einfachen Weiterleitungsmöglichkeiten erreichen emotionalisierende Behauptungen schnell zehntausende Menschen und mehr. Die Eindämmung erweist sich als schwierig, insbesondere, weil die Geschwindigkeit der Verbreitung die Kapazitäten zur Gegenwehr übersteigt. Darüber hinaus werden die Initiierenden von Desinformationen immer professioneller, da KI-basierte Werkzeuge für die Manipulation von Bild- und Videoinhalten niederschwellig zugänglich geworden sind. Zudem ist es wichtig, freie Diskussionsräume für die politische Willensbildung einer kritischen und mündigen Gesellschaft zu stärken. Die Herausforderung in diesem Bereich ist zweigeteilt: Zum einen ist ein gesellschaftlicher Diskurs notwendig, nach welchen Grundregeln Debatten geführt und wie Informationen verbreitet und rezipiert werden sollen. Zum anderen können technische Lösungen dabei unterstützen, in der Vielzahl von täglichen Informationen Quellen zu überprüfen und Fälschungen zu erkennen. Bei der Entwicklung derartiger Technologien müssen die gesellschaftlichen Rahmenbedingungen also von Anfang an Berücksichtigung finden, um ethischen, rechtlichen und sozialen Implikationen Rechnung zu tragen. Die Bekämpfung von Desinformationen ist eine komplexe Aufgabe, die sowohl technische als auch starke Aspekte des Zivilschutzes aufweist. Parallel zu diesem Programm, in dem technische Fragen der IT-Sicherheit im Vordergrund stehen, adressiert auch das Rahmenprogramm der Bundesregierung „Forschung für die zivile Sicherheit 2018–2023“ die Bedeutung des Themas für Gesellschaft und Demokratie[7].

Beispiele für künftige Handlungsfelder sind:

- **Wirksame Gegenmaßnahmen entwickeln:**

Charakteristika von Desinformationen und ihre Wirkungen auf Gesellschaft und Individuum sowie technische und rechtliche Gegenmaßnahmen müssen erforscht werden, um eine wirksame Bekämpfung von Desinformationen zu bewirken, ohne dabei die Meinungsfreiheit und legitime demokratische Auseinandersetzung zu beeinträchtigen.

- **Gefälschte Inhalte erkennen und bekämpfen:**

Digitale Medien ermöglichen sehr niederschwellig täuschend echte Fälschungen. Daher sind technische Werkzeuge zum Erkennen von gefälschten Informationen wie Deepfakes und Manipulationen durch Malicious Social Bots erforderlich.

---

[7] https://www.sifo.de/de/sicherheitsforschung-forschung-fuer-die-zivile-sicherheit-1693.html

- **Vertrauenswürdige Quellennachweise schaffen:**

Anstatt Desinformationen zu erkennen und zu verhindern, können auch valide Informationen als solche gekennzeichnet werden. Hierfür müssen sichere und benutzbare Werkzeuge sowohl für Inhaltsschaffende als auch -nutzende entwickelt werden.

- **Alternative Geschäftsmodelle für Onlineplattformen entwickeln:**

Durch Werbung monetarisierte Aufmerksamkeit führt dazu, dass besonders pointierte Meldungen attraktiv sind. Dies bereitet den Nährboden für Desinformation. Ein möglicher Ausweg sind Geschäftsmodelle, die nicht darauf basieren, möglichst viel Aufmerksamkeit zu erzeugen.

- **Soziale Medien in den Blick nehmen:**

Einerseits bieten soziale Medien Raum für vielfältige Meinungen und ermöglichen jeder und jedem eine individuelle Entfaltung und Selbstdarstellung. Forschung zeigt jedoch, dass gerade hier „Filterblasen" der Desinformation entstehen oder Jugendliche geschlechterstereotypen Körpernormen folgen und diese bewerben. Ein gravierendes Problem ist zudem Hassrede. Darüber hinaus müssen unter anderem Empfehlungsalgorithmen genauer untersucht werden – beispielsweise mit Blick darauf, inwieweit es möglich ist, mittels eines algorithmengesteuerten Detektors oder hybrider Verfahren (Interactive Machine Learning) Hassrede zu löschen, ohne die Meinungsfreiheit einzuschränken (Overblocking).

3.3.3 Technik nach demokratischen Werten souverän gestalten

Soziale Medien, vom sozialen Netzwerk über Messenger bis zum Wiki, sind zentraler Bestandteil im Leben nahezu aller online aktiven Menschen geworden. Große Teile sozialer Interaktion finden online statt. Analoge Gruppen von beruflichen Teams über den Sportverein bis zur Familie haben fast immer auch ein digitales Gegenstück. Durch die Corona-Krise hat sich der Trend verstärkt und gemeinsame Kneipenaufenthalte, Filmabende oder Konzert- und Theaterbesuche können auch digital in sozialen Medien stattfinden. Dabei haben die technischen Rahmenbedingungen der Plattformen einen stark strukturierenden Charakter. Handlungsweisen werden durch Regeln ermöglicht oder verhindert. Diese erweiterte Realität entwickelt sich rasant und fördert sozio-technologische Innovationen. Sie stellt jedoch auch etablierte Kulturtechniken vor große Herausforderungen. Aufgrund des schnellen Wandels in der digitalen Kommunikation – gestern Facebook, heute TikTok, morgen eine ganz andere Anwendung – zersplittert das gemeinsame Verständnis von Kommunikation und Diskurs zusehends. Doch die Gesellschaft braucht eine einheitliche Sprache und ein gemeinsames Verständnis von Diskurs: eine Netzkultur. Der Umgang mit Daten und persönlichen Informationen in öffentlichen oder halböffentlichen Räumen wird eine zunehmende Herausforderung: Das Internet vergisst nicht. Technologien der IT-Sicherheit wie Verschlüsselung, Anonymisierung, aber auch Kenntnisse aus der sicheren Gestaltung von Benutzungsinteraktion werden umso bedeutsamer. Sie müssen weiter erforscht und transferiert werden, um Technologien für Bürgerinnen und Bürger souverän nutzbar zu machen.

Beispiele für künftige Handlungsfelder sind:

- **Standards, Normen und Kennzeichnungen weiterentwickeln:**

Deutschland ist bekannt für ein hohes Datenschutzniveau. Die gemeinsame europäische Datenschutzgrundverordnung (DSGVO) bildet erst den Ausgangspunkt für die europäische und internationale Anhebung des Datenschutzstandards. Um Handlungssicherheit für Unternehmen zu erreichen und die Reibungsverluste zu vermeiden, ist die Weiterentwicklung von Standards, Normen und Kennzeichnungen bedeutend.

- **Werte in die Technikentwicklung einfließen lassen (Values by Design):**

Kommunikationsinfrastrukturen und digitale Plattformen sollten so ausgestaltet werden, dass demokratische Werte wie Meinungs- und Pressefreiheit sowie Diskriminierungsschutz optimal berücksichtigt werden. IT-Sicherheit bildet eine verlässliche und vertrauenswürdige Basis im digitalen Raum, ein Fundament, auf dem gesellschaftliche Wertvorstellungen bei der Technikgestaltung verankert werden können.

- **Individuellen Umgang mit Daten besser verstehen:**

Es gilt interdisziplinär zu untersuchen, welche Auswirkungen der mit dem digitalen Wandel einhergehende Wertewandel hat, insbesondere in Bezug auf die damit zusammenhängenden sozialen Praktiken und Kulturtechniken wie den Umgang mit privaten und persönlichen Daten. Es kommt darauf an, digitale Räume mit einem Augenmerk auf Datenschutz bewusst zu gestalten und Techniken der IT-Sicherheit zentral zu nutzen.

3.4 IT-Sicherheit benötigt Partnerschaft und Exzellenz

Europa ist bei IKT-Systemen von vielen außereuropäischen Akteuren abhängig, da die Mehrheit der größten Unternehmen im Ausland sitzt. Deutschland muss gemeinsam mit seinen europäischen Partnern eigene technologische Kompetenzen in der IT-Sicherheit ausbauen und in der Lage sein, alle eingesetzten Systeme zu kontrollieren: von Server und Netzwerk über Laptop und Smartphone bis zu IoT und Sensoren. Dies ist unerlässlich, um mehr technologische Souveränität zu erreichen und so Sicherheit und Versorgung der Bevölkerung sicherzustellen. Gleichzeitig kann IT-Sicherheit in einer globalisierten, grenzüberschreitend vernetzten Welt nicht einzelstaatlich gedacht werden. Eine Abschottung ist schlicht nicht mehr möglich.

Deutschland muss daher internationales Recht und prüfbare internationale Standards aktiv mitgestalten, um IT-Sicherheit und Privatheit in einer digitalen Welt zu stärken. Damit dies gelingt, braucht es hervorragende wissenschaftliche Erkenntnisse aus unterschiedlichen Disziplinen wie Informatik, Elektrotechnik, Physik, Rechts-, Gesellschafts- und Sozialwissenschaften. Durch Bündelung dieser und weiterer Disziplinen verfügt Deutschland bereits über exzellente Forschung und Entwicklung im Bereich IT-Sicherheit und ist im Schutz von Privatheit weltweit führend.

Wir müssen auch weiterhin klare Schwerpunkte setzen und ein attraktives Umfeld für Innovationen in der IT-Sicherheit schaffen. Nur so kann es gelingen, international führende Köpfe der Wissenschaft in Deutschland zu halten, den benötigten Nachwuchs für die Themen zu begeistern und ausreichend Fachkräfte exzellent auszubilden. Deutschland ist in der Forschung Weltspitze, jedoch kann die IT-Sicherheitsindustrie den Bedarf, insbesondere im starken deutschen Mittelstand, kaum befriedigen. Auch auf den zügigen Technologietransfer aus der Forschung in die Wirtschaft kommt es an: Viele Ideen bleiben noch immer ungenutzt oder werden von Dritten aufgegriffen. Deutschland und Europa müssen daher ihre IT-Sicherheitsbranche konsequent weiter ausbauen. Dazu gehört insbesondere auch eine noch umfassendere Innovations- und Wagniskultur, die es ermöglicht, Spitzenforschung sehr schnell an den Markt zu bringen. Gerade innovative Start-ups können einen wichtigen Beitrag zum Ausbau einer dynamischen, innovativen und prosperierenden europäischen IT-Sicherheitsindustrie leisten. Die Partnerschaft zwischen Forschenden und Anwendenden − von der Privatperson über das KMU bis zum Großkonzern − ist entscheidend, um existierende Lösungen in die Praxis zu überführen. Dabei ist vernetztes Denken und Handeln über Disziplingrenzen und Prozessketten hinweg von zentraler Bedeutung. Daher müssen neben technischen auch gesellschaftliche, rechtliche und wirtschaftliche Fragestellungen von Anfang an mitberücksichtigt werden.

3.4.1 Technologische Souveränität mit IT-Sicherheit ausbauen

Abhängig von Dritten zu sein, ist insbesondere im Bereich IT-Sicherheit problematisch, da Sicherheit für alle IKT-Systeme von zentraler Bedeutung ist. Unsichere Systeme können manipuliert, Produktionsanlagen außer Kraft gesetzt oder Betriebsgeheimnisse abgezogen werden. Deutschland und Europa müssen in der Lage sein, IKT-Systeme sicher zu betreiben und selbst zu kontrollieren – dies ist eine Grundvoraussetzung für technologische Souveränität. Akteure in Deutschland und Europa müssen dafür die Vertrauenswürdigkeit von IKT-Systemen und deren Komponenten aus allen Weltregionen aufgrund eigenen Wissens und eigener Fertigkeiten beurteilen können. Darüber hinaus muss untersucht werden, welche IKT-Systeme von so zentraler Bedeutung für die öffentliche Sicherheit und Ordnung sind, dass sie idealerweise in Deutschland oder in Zusammenarbeit mit europäischen Partnern selbst entwickelt und gefertigt werden sollten. Dabei ist davon auszugehen, dass einzelne Komponenten von so zentraler Bedeutung sind, dass ihre Entwicklung und Herstellung nicht einmal wirtschaftlich sein muss.

Ein weiterer wesentlicher Schritt in Richtung technologischer Souveränität ist es, sichere Normen und Standards sowie quelloffene Software kooperativ zu entwickeln. Viele IT-Produkte unterschiedlicher Anbieter setzen für bestimmte Module und Schichten bereits die gleiche offene Basis ein. Eine Kooperation bei der Entwicklung und Absicherung gemeinsamer IT-Komponenten nutzt deshalb allen Beteiligten. Zusätzlich zu diesen offenen IT-

Komponenten gilt es für die Forschung, Prozesse zu entwerfen, die die Sicherheitseigenschaften von Gesamtsystemen effizient messen, prüfen oder sogar garantieren.

Letztlich sollen alle Aktivitäten im Rahmen dieses Programms und darüber hinaus technologische Souveränität fördern. Daher sind alle Handlungsfelder (Kapitel 3.1 bis 3.4) auch als Handlungsfelder mit dem Ziel des Ausbaus technologischer Souveränität zu sehen.

Bei den besonderen Schwerpunkten der IT-Sicherheitsforschung für technologische Souveränität orientiert sich dieses Programm an den folgend zusammengefassten Empfehlungen der Wissenschaftlichen Arbeitsgruppe des Nationalen Cyber-Sicherheitsrats:

- **Souveränität bei vertrauenswürdiger Hardware**

Open-Source-Hardware befindet sich noch in einer Frühphase der Entwicklung. Sie kann aber ein Instrument sein, um mögliche Backdoors oder Schwachstellen im Rahmen von Evaluationen des Chipdesigns zu erkennen. In niederen Leistungsklassen können solche offenen Designs schon mittelfristig für Unternehmen nützlich sein, um vertrauenswürdige Schaltkreise etwa für IoT- oder Medizingeräte zu fertigen. Für leistungsfähigere Prozessoren muss schon heute die Basis mit offenen Designs gelegt werden. Zudem sollen technische Methoden entwickelt werden, die dazu dienen, elektronische Komponenten automatisiert zu prüfen. Insbesondere das bereits etablierte und weiterwachsende Ökosystem rund um RISC-V mit perspektivisch zertifizierten, vertrauenswürdigen Hardwarekomponenten ist eine vielversprechende Initiative. Neben diesem Programm, in welchem ausschließlich Fragen der IT-Sicherheit berücksichtigt werden, fördert die Bundesregierung Forschung zu vertrauenswürdiger Elektronik im Rahmenprogram der Bundesregierung für Forschung und Innovation 2021–2024 „Mikroelektronik. Vertrauenswürdig und nachhaltig. Für Deutschland und Europa“[8].

- **Souveränität bei Dateninfrastrukturen**

Es bedarf Forschung, um mit GAIA-X vertrauenswürdige, sichere Dateninfrastrukturen zu etablieren und so Abhängigkeiten von einzelnen Anbietern zu reduzieren. Daten, als Grundlage aller Cybersicherheitsaktivitäten, können damit kontrolliert, sicher und vertrauenswürdig dezentral verwaltet sowie nachvollziehbar und datenschutzkonform gemeinsam genutzt werden.

- **Souveränität bei sicherheitskritischen Netzkomponenten**

Der Aufbau und Betrieb von wirtschaftlich unabhängigen Prüf- und Evaluierungslaboren für sicherheitskritische Technologien (5G, IoT, Maschinelles Lernen, Quantenkommunikation) soll unterstützt werden.

- **Souveränität bei KI-Systemen**

Der Aufbau einer KI-Zertifizierungsinfrastruktur mit Methoden, Werkzeugen und Prüfverfahren zur Zertifizierung von KI-Systemen und genutzten Trainingsdaten soll substanziell unterstützt werden. Regulatorische Vorgaben für den Einsatz zertifizierter KI-Systeme in sicherheitskritischen Infrastrukturen sollen entwickelt werden. Dies gilt auch für die Qualität der Trainingsdaten.

- **Souveränität bei Zukunftstechnologien**

Im Sinne von Security by Design ist es wichtig, die Technologieentwicklung eng mit der IT-Sicherheitsforschung zu verzahnen. Beispielsweise wird bereits jetzt die Mobilfunktechnologie 6G hierzulande vorentwickelt. Sicherheitsaspekte müssen von Anfang an berücksichtigt werden.

Mobilfunksysteme der 6. Generation (6G)

Deutschland ziel darauf ab, die Mobilfunksysteme der kommenden 6. Generation (6G) maßgeblich mitzugestalten, frühzeitig technologische Grundlagen zu entwickeln und somit das Fundament dafür zu legen, bei dieser Schlüsseltechnologie mit innovativen und international wettbewerbsfähigen Produkten wichtiger Akteur am globalen Markt zu werden. Ein wichtiger Aspekt bei der Erforschung der Grundlagen von 6G soll dabei

[8] www.elektronikforschung.de/rahmenprogramm

darauf liegen, dass die Sicherheit ein integraler Bestandteil wird und dass das Gesamtsystem eine hohe Resilienz aufweist. Ergänzend werden durch die Förderung die Kompetenzen aufgebaut, um die zukünftigen 6G-Netze souverän und sicher betreiben zu können.

3.4.2 Deutschland in der Wissenschaftslandschaft positionieren

In einer globalisierten Welt, in der durch die Digitalisierung alles mit allem vernetzt ist, ist der Einfluss einzelner nationaler Regularien oder technologischer Entwicklungen begrenzt. Damit Deutschland die weitere Digitalisierung im Sinne seiner Werte und Prinzipien regulatorisch und technologisch mitgestalten kann, braucht es starke Partner. Mit dem vorliegenden Forschungsrahmenprogramm soll die Kooperation im Europäischen Forschungsraum in den Bereichen IT-Sicherheit und Datenschutz weiter gestärkt werden. Innovationen sollten die europäischen Wertvorstellungen und Ansprüche widerspiegeln, aber gleichzeitig global anschlussfähig bleiben. Die Herausforderung liegt darin, sich international eindeutig zu positionieren, eigene Ziele und Wertvorstellungen durchzusetzen und dabei das Ziel einer technologischen Souveränität Europas weiter voranzutreiben. Bei diesem Prozess müssen die Offenheit und Interoperabilität der eigenen Systeme und Entwicklungen nach allen Seiten hin gewahrt bleiben, um keine Inseln zu schaffen. Dabei gilt es, deutsche und europäische Stärken weiter auszubauen, zum Beispiel auf dem Gebiet des Datenschutzes, der Quantenkommunikation oder der sicheren Industrie 4.0. Zudem kommt es darauf an, die eigene Technologiepalette so weit zu ergänzen und zu diversifizieren, dass bisherige Abhängigkeiten von externen Anbietern weiter reduziert werden und die einzelnen Forschungsergebnisse gleichzeitig eine noch größere internationale Durchschlagskraft entwickeln können.

Beispiele für künftige Handlungsfelder sind:

- **Internationale Standards erarbeiten:**

Für einen besseren internationalen Transfer von Forschungsergebnissen bedarf es einheitlicher und offener Standards, insbesondere im Sicherheitskontext. Diese müssen erweitert und an neue Rahmenbedingungen angepasst werden.

- **Stärken nutzen, Doppelungen vermeiden:**

Um noch besser auf das Ziel einer europäischen digitalen Souveränität abzielen zu können, müssen die nationalen Forschungsstärken von Deutschland in der IT-Sicherheit noch besser in Zusammenarbeit mit den europäischen Partnern abgestimmt und identifiziert werden, um unnötige Doppelungen auf zu kleinem nationalen Raum zu vermeiden.

- **International kompatibel bleiben:**

Beim Fokus auf die eigene Souveränität gilt es, den Blick und die Anschlussfähigkeit über den europäischen Tellerrand hinaus nicht zu verlieren. Im Sinne einer globalen Interoperabilität und Interdependenz muss eine weltweite Integrationsfähigkeit der Entwicklungen sichergestellt sein, wozu es umfassender Konzepte bedarf.

3.4.3 Kooperation und Transfer weiter verbessern

Wirtschaftliche, wissenschaftliche und gesellschaftliche Strukturen sind in Deutschland ausgesprochen divers. Diese vielfältige und offene Struktur ist eine große Stärke, führt jedoch im Hinblick auf IT-Sicherheit zu verschiedenen Herausforderungen. Ebenso unterschiedlich wie die Anwenderinnen und Anwender sind der Aufbau, die Art, der Zweck und die Nutzung von IKT-Systemen: von Kioskkasse, Smartphone, Auto oder Heizung über Arztpraxis und Großlager bis hin zu Verkehrslenkung und Stahlwerken. Daher sind auch Sicherheitslösungen bisher nur schwer übertragbar und Skaleneffekte können nicht greifen. Der grundsätzliche Aufbau von IKT-Systemen gleicht sich jedoch zunehmend an. So sind Smartphones und Tablets beispielsweise auch als Kassensystem im Einsatz und die zunehmende Nutzung von Cloud- und Edge-Infrastrukturen führt weg von individuellen Serverlösungen. So werden Kooperationen im Bereich IT-Sicherheit möglich. Zu untersuchen und zu erproben, wie diese konkret und effizient gestaltet werden können, ist eine wichtige Herausforderung der kommenden Jahre. Dies bezieht sich sowohl auf Unternehmen als auch auf Bürgerinnen und Bürger. Letztere sind noch vulnerabler als Unternehmen, da ihnen noch weniger Ressourcen für ihren Schutz zur Verfügung stehen. Zudem gilt es, die Fortentwicklung der IT-Sicherheit an der Schnittstelle Wirtschaft, Wissenschaft und Gesellschaft generell weiter auszubauen. Die etablierte, stark ausdifferenzierte und vielfältige Wissenschaftslandschaft auf dem Gebiet der IT-

Sicherheit ist auch im internationalen Vergleich exzellent. Jedoch bestehen sowohl zwischen den einzelnen Disziplinen als auch an der Schnittstelle zur Wirtschaft noch Reibungsverluste.

Beispiele für künftige Handlungsfelder sind:

- **Vielversprechende Forschung effizienter in die Praxis transferieren:**

Es werden Transferkonzepte benötigt, um exzellente deutsche (IT-Security made in Germany) und europäische Forschungsergebnisse der IT-Sicherheit schnell zu deutschen und europäischen Produkten zu entwickeln. Solche Produkte werden international wahrgenommen werden und De-Facto-Standards im Bereich Sicherheit setzen.

- **Plattformen für Kooperation in der IT-Sicherheit ausbauen:**

Um Skaleneffekte im Bereich IT-Sicherheit nutzen und sie so effizienter gestalten zu können, braucht es Zusammenarbeit über Unternehmensgrenzen hinweg. Es müssen unter anderem Konzepte zur Kooperation entwickelt und erprobt werden.

- **Erhöhen des allgemeinen Wissenstands:**

Es braucht passgenaue Wissensvermittlungsformate, die sowohl den Umgang mit IT-Sicherheit im Alltag vermitteln als auch sehr spezifisch auf den jeweiligen beruflichen Kontext ausgerichtet werden können. Bildung zur IT-Sicherheit ist relevant in allen Lebensbereichen: im Privaten ebenso wie im Beruf und hier insbesondere für entscheidungsbefugte Personen. Ein grundlegendes Verständnis der Potenziale und Herausforderungen ist die Basis für einen souveränen Umgang mit Informations- und Kommunikationstechnologien.

- **Unterschiede zu IT-Sicherheit in anderen Wirtschaftsräumen verstehen:**

Da einige deutsche Unternehmen weltweit Produkte, Systeme und Dienste vertreiben, sind Regulierungen, Zulassungsauflagen und technische Standards in anderen wichtigen Wirtschaftsräumen von hohem wirtschaftlichen, aber auch wissenschaftlichen Interesse. Dazu zählt das China Cybersecurity Law mit der OSCCA-Zertifizierung und den TC-260-Standards, letztmalig im Januar 2020 geändert, das IoT Security Law in den USA mit den NIST-Standards, veröffentlicht im Dezember 2020, aber auch GOST in Russland und SCOSTA in Indien. Insbesondere bei neuen Algorithmen, wie bei der Post-Quanten-Kryptografie, werden divergierende Entwicklungen in den genannten Wirtschaftsräumen erwartet. Das hätte unmittelbar Auswirkungen, zum Beispiel auf den Maschinen- und Automobilbau in Deutschland. Um die zukünftigen Exporte zu sichern beziehungsweise auszubauen, ist hier eine wissenschaftliche Beobachtung und ein wirtschaftlicher Austausch über Firmengrenzen hinweg angezeigt.

4 Umsetzung

Ein Forschungsprogramm muss adaptiv sein, um den rasanten technischen Entwicklungen immer wieder aufs Neue Rechnung zu tragen. Es gilt, mit Forschung dem gesellschaftlichen Wandel und der temporeichen und innovationsgetriebenen Digitalisierung zu begegnen. In dieser Dynamik verändern sich sehr schnell die Bedarfe und Ansprüche an Technik. Diese gilt es, im Schulterblick mit dem Umfeld zu erkennen und mit Forschung und Fördermaßnahmen passgenau zu adressieren. Das vorliegende Programm zur IT-Sicherheitsforschung ist deshalb als lernendes Programm ausgelegt. Dazu gehört ein kontinuierlicher Dialog mit allen zentralen Zielgruppen − von Forschungscommunities über Akteurinnen und Akteure aus Wirtschaft und Politik bis hin zu Bürgerinnen und Bürgern, den späteren Nutzerinnen und Nutzern der digitalen Technologien. Durch einen immerwährenden Austausch wird Wissenstransfer gestärkt und Partizipation unterstützt. So können kontinuierlich und bedarfsgerecht Fokusthemen ebenso wie Förderinstrumente angepasst werden. Die zuvor beleuchteten technologischen und gesellschaftlichen Herausforderungen (siehe Kapitel 3) geht das Programm mit bewährten und innovativen Werkzeugen an.

4.1 Wissenschaftliche Kompetenzen und Exzellenz fördern

Eine innovative IT-Sicherheitsforschung bietet die Chance, nicht nur Cyberbedrohungen abzuwehren, sondern auch Deutschland zu einem führenden Anbieter für IT-Sicherheitstechnologie zu machen und die technologische Souveränität zu stärken. Im Rahmen der Forschungsförderung werden vielfältige Fördermodule und -instrumente eingesetzt, um an allen Stellen Spitzenforschung zu fördern und zu ermöglichen. Neben der Förderung von Forschung an Hochschulen und Universitäten, institutionellen Forschungseinrichtungen und in der Wirtschaft ist ein gut qualifizierter wissenschaftlicher Nachwuchs Voraussetzung dafür, Forschungskompetenz, Innovationsfähigkeit und die akademische Ausbildung in Deutschland nachhaltig zu sichern.

4.1.1 Horizontale und aufbauende Förderprojekte

In horizontalen Förderprojekten werden die Kompetenzen aus Universitäten, Hochschulen und außeruniversitären Forschungseinrichtungen sowie Praxiswissen aus Unternehmen in der übergreifenden Verbundforschung gebündelt. Gefördert werden themengerechte Projektverbünde unter wissenschaftlicher Führung mit dem Ziel, die Basis für eine umfassende IT-Sicherheit zu schaffen. Der starke Grundlagencharakter und die integrative Zusammenarbeit fördert die Vernetzung und den Know-how-Transfer zwischen Wissenschaft, Wirtschaft und Praxis von Beginn an und verschafft allen Akteuren einen wertvollen Wissensvorsprung. Zusätzlich zu wissenschaftlich geführten Forschungskonsortien setzen maßgeschneiderte Instrumente und Initiativen übergreifende Impulse in der deutschen Forschungslandschaft der IT-Sicherheit.

IT-Sicherheit muss Angriffe von morgen bereits heute antizipieren. Nur durch einen sehr frühen Einstieg kann die Forschung zur IT-Sicherheit mit der technischen Entwicklung in anderen Disziplinen Schritt halten. Daher sind in der IT-Sicherheitsforschung innovative Verbundvorhaben im Frühstadium wichtige Wegbereiter. Dazu gehören auch Vorhaben ohne konkreten Praxisbezug wie zukunftsweisende „Moonshot-Projekte“ oder Forschungsideen, die auf antizipierten technischen Entwicklungen beruhen.

4.1.2 Institutionelle Förderung

Deutschland verfügt mit der Fraunhofer-Gesellschaft, der Helmholtz-Gemeinschaft, der Max-Planck-Gesellschaft und der Leibniz-Gemeinschaft über leistungsstarke Wissenschaftsorganisationen, die ein zentraler Pfeiler der IT-Sicherheitsforschung sind. Hierfür wurden durch die konsequente Förderung und Verstetigung von drei nationalen Forschungszentren für IT-Sicherheitsforschung des Bundes entscheidende Weichen gestellt: Mit dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE in Darmstadt, dem Helmholtz-Zentrum für Informationssicherheit CISPA in Saarbrücken und dem Kompetenzzentrum für Angewandte Sicherheitstechnologie KASTEL am Karlsruher Institut für Technologie (KIT) sind herausragende Leuchttürme der IT-Sicherheitsforschung mit internationaler Strahlkraft entstanden. Ihre Weiterentwicklung und Vernetzung im nationalen und internationalen Kontext bleibt ein wichtiges Ziel der Ausgestaltung der IT-Sicherheitsforschung in Deutschland.

Komplettiert wird die Landschaft der IT-Sicherheitsforschung in Deutschland durch zahlreiche Institute, die direkt oder im Rahmen von interdisziplinären Forschungsprojekten zur IT-Sicherheitsforschung beitragen. Dies sind unter anderem das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC, das Fraunhofer-Institut für Sichere Informationstechnologie SIT, das Max-Planck-Institut für Sicherheit und Privatsphäre, die DLR-Institute für KI-Sicherheit, Quantentechnologien sowie Kommunikation und Navigation, das Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF, das Fraunhofer Heinrich-Hertz-Institut HHI, das Max-

Planck-Institut für die Physik des Lichts MPL, das Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden, das Max-Planck-Institut für Quantenoptik, das Fraunhofer-Institut für System- und Innovationsforschung ISI, das Fraunhofer-Institut für offene Kommunikationssysteme FOKUS, das Fraunhofer-Institut für Experimentelles Software Engineering IESE, das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB, die Fraunhofer-Einrichtung für Mikrosysteme und Festkörper-Technologien EMFT, das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, das Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM, das Fraunhofer-Institut für Produktionstechnologie IPT, das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS, das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE sowie weitere bedeutende Forschungsinstitutionen. Dazu gehören etwa die Hochschulen und die Ressortforschung wie die des BSI oder der Hochschule der Bundeswehr.

4.1.3 Nachwuchs für IT-Sicherheit

Die zukünftige Wettbewerbsfähigkeit Deutschlands hängt von kreativen und exzellent ausgebildeten Fachkräften ab. Dies gilt insbesondere für den Bereich der IT-Sicherheit, die eine notwendige Grundlage für die technologische Souveränität in der digitalen Zukunft darstellt. Es gilt, die Elite von morgen bereits heute zu fördern. Deshalb wird der akademische Nachwuchs mit weitreichenden Fördermaßnahmen unterstützt. Eine gute MINT-Bildung entlang der Bildungskette ist dafür ein ebenso entscheidender Beitrag. Entsprechende Schwerpunkte setzt auch der MINT-Aktionsplan des BMBF[9].

Wissenschaftlicher Nachwuchs

Die Talente und Potenziale des wissenschaftlichen Nachwuchses können von Beginn an durch exzellentes Mentoring weiterentwickelt werden. Alle institutionell geförderten Einrichtungen wie die nationalen Forschungszentren bieten attraktive Nachwuchsprogramme an. Dazu gehören vernetzende Graduiertenschulen und -netzwerke und Angebote wie beispielsweise die International Federation for Information Processing Summer School. Sichtbarkeit und Anerkennung in der akademischen Welt macht Deutschland zum Anziehungspunkt für die besten Köpfe. Hier leistet das Programm mit seinem ganzheitlichen Ansatz einen wesentlichen Beitrag, Deutschland zu einem interessanten IT-Sicherheitsstandort zu machen.

Grand Challenge der Quantenkommunikation

Die Grand Challenge der Quantenkommunikation ist ein Innovationswettbewerb für junge Nachwuchsforschungsgruppen. Thema des Wettbewerbs sind Quanten-Token, die zur künftigen sicheren Authentifizierung von Systembenutzerinnen und -benutzern – auch von leistungsfähigen Quantencomputern – dienen sollen. Technologische Schlüsselfaktoren für Quanten-Token, wie beispielsweise Kohärenzzeiten von Quantenspeichern, sollen im Rahmen des Forschungswettbewerbs verbessert werden. Ein starker Fokus liegt dabei auf der Weiterentwicklung von quantenspeicherbasierten Ansätzen, da diese einen wichtigen Forschungsschwerpunkt sowohl für die Quantenkommunikation als auch für andere Bereiche der Quantentechnologien bilden.

Schülerinnen und Schüler, Auszubildende und Studierende

Um das hohe Innovationsniveau aufrechtzuerhalten und das notwendige Wachstum der IT-Sicherheitsbranche zu unterstützen, brauchen wir eine kontinuierlich steigende Zahl an gut ausgebildeten Nachwuchskräften. Mit dem dualen Bildungssystem ist Deutschland im internationalen Vergleich hervorragend aufgestellt. Die Stärken der beiden Zweige praktischer und akademischer Bildung müssen auch im Bereich IT-Sicherheit gestärkt und genutzt werden. Um mögliche Nachwuchskräfte früh zu begeistern, schaffen wir durch zielgruppengerechte, kreative Angebote wie Wettbewerbe vielfältige Möglichkeiten, Fähigkeiten über den Unterricht, die Ausbildung oder das Studium hinaus zu vertiefen und Erfahrungen zu sammeln. Ein im Bereich der IT-Sicherheit besonders attraktives Format sind dabei Hackathons. Ein besonderes Anliegen dabei ist es, Mädchen und junge Frauen für die vielfältigen Fragen der IT-Sicherheit, die weit über Hacken hinausgehen, zu begeistern, und sie zu ermutigen, in diesem Feld tätig zu werden.

[9] https://www.bmbf.de/de/mint-aktionsplan-10115.html

4.2 Innovationsökosystem und Transfer ausbauen

4.2.1 Pilotinitiativen

IT-Sicherheit ist als zentrales Querschnittsthema digitaler Systeme ein wichtiger Aspekt staatlicher Daseinsvorsorge und technologischer Souveränität. Neben Risiken hemmen oft hohe Barrieren den Markteintritt – gerade auch von neuen Schlüsseltechnologien. Im Rahmen von Pilotinitiativen werden deshalb breit aufgestellte Verbünde aus Wissenschaft und Wirtschaft gefördert, um weiter souverän bei zentralen technologischen Entwicklungen an der internationalen Spitze zu stehen. Dazu gehört die vom BMBF 2019 ins Leben gerufene Initiative QuNET. Die Forschenden entwickeln dort die technologischen Grundlagen für eine quantengesicherte Pilotstrecke zwischen Bundeseinrichtungen mit dem Ziel, gemeinsam mit Partnern aus der Wirtschaft, die Voraussetzungen für eine spätere deutsche und europäische Quantenkommunikationsinfrastruktur zu schaffen.

BMBF-Initiative QuNET

Das Vorhaben „QuNET-alpha – Demonstrationsexperiment zur Kommunikation unter Einsatz von Quantentechnologien“ stellt einen wichtigen Meilenstein bei der Umsetzung der Quantenkommunikation in alltagstaugliche Systeme dar. Ergebnisse aus der Grundlagenforschung werden im Projekt zu praxistauglichen Lösungen weiterentwickelt und in der Anwendung erprobt. In einer quantengesicherten Videokonferenz zwischen zwei Bundeseinrichtungen werden die Projektergebnisse auf Basis verschiedener Quantentechnologien demonstriert. Dabei sollen zur Übertragung der Quantenzustände sowohl Glasfasern als auch freistrahlbasierte Kommunikationskanäle eingesetzt werden. Durch letztere können künftig weite Strecken teilweise per Satellit überbrückt werden, um ein europaweiten Quantennetzwerk zu schaffen. Die Quantenverschlüsselung wird im Projekt zusätzlich mit modernsten Verschlüsselungsverfahren kombiniert werden, deren Algorithmen auch resistent gegen Angriffe von Quantencomputern sind. Damit wird die praktische Sicherheit unter realen Bedingungen optimiert. Die Projektergebnisse schaffen, basierend auf Deutschlands starker Grundlagenforschung zu Quantentechnologien, die Voraussetzung für eine deutsche und europäische Quantenkommunikationsinfrastruktur.

4.2.2 Vertikale Förderprojekte

Der gesellschaftliche und wirtschaftliche Einfluss von Forschungs- und Entwicklungsprojekten zur IT-Sicherheit ist dann besonders groß und nachhaltig, wenn die Projektverbünde die komplette oder einen Großteil der Wertschöpfungs- beziehungsweise der Verwertungskette der Entwicklung abbilden. Entsprechende Strategien und Ansätze können so bereits während des Projektverlaufs mitgedacht werden und müssen nicht erst ad hoc nach Projektende aufwendig entwickelt werden. Ein Beispiel für eine solche erfolgreiche vertikale Fördermaßnahme ist das Nationale Referenzprojekt zur Sicherheit in Industrie 4.0 IUNO. Im Rahmen vertikaler, industriegeführter Verbundprojekte wird die themenspezifische Kompetenz von relevanten Stakeholdern mit Forschungseinrichtungen zusammengebracht, um Problemstellungen mit Praxisbezug entlang der Wertschöpfungskette zu erforschen. So werden zielgerichtet Innovationen zur Lösung von aktuellen Herausforderungen auf dem Gebiet der IT-Sicherheit entwickelt. Das BMBF wird begleitend Förderinitiativen an den Start bringen, die Forschung entlang der Wertschöpfungskette adressieren.

4.2.3 Förderung von kleinen und mittleren Unternehmen sowie Start-ups

Neben Forschung in der Wissenschaft und in Großunternehmen sind KMU sowie Start-ups wichtige Treiber von Innovationen und Hort neuer Ideen. Häufig stehen sie vor der Herausforderung, nicht über ausreichend Ressourcen und Netzwerke zur Umsetzung und Verbreitung ihrer Entwicklungsvorhaben zu verfügen. Im Rahmen des vorliegenden Programms werden spezifische Fördermaßnahmen für KMU und Start-ups weiterentwickelt und im Austausch mit der Community neue Formate gestaltet. Besonders wichtig sind dabei Vernetzungsformate, um den Transfer zwischen Start-ups untereinander sowie zu potenziellen Kunden und Investoren zu stärken und zu beschleunigen. Das Ziel ist es, innovative Produkte junger Unternehmen schneller am Markt zu platzieren.

StartUpSecure

Forschungsteams an deutschen Hochschulen oder in der Industrie sind mit ihren Ideen und unkonventionellen Ansätzen häufig Vorreiter neuer Entwicklungen. Um gute Ideen im Bereich der IT-Sicherheit schneller in die Anwendung zu bringen, bietet das BMBF seit 2018 die Initiative StartUpSecure. Darin werden Unternehmensgründungen in der IT-Sicherheit in zwei Phasen gefördert: In der ersten Phase erarbeiten die Forschungsteams Strategien, wie die Idee technisch umgesetzt werden kann. Mit der Gründung des Unternehmens startet die zweite Phase, während der das BMBF die Teams bei einem erfolgreichen Unternehmensstart unterstützt. Für die Begleitung der jungen Gründungen wurden an den Nationalen Forschungszentren für IT-Sicherheit ATHENE (Darmstadt), CISPA (Saarbrücken), KASTEL (Karlsruhe) sowie an der Ruhr-Universität Bochum Gründungsinkubatoren eingerichtet.

KMU-innovativ

KMU-innovativ (KMUi) ist dafür konzipiert, speziell KMU effektiv in Innovationsprozessen zu unterstützen. Mithilfe der Förderung zu Informations- und Kommunikationstechnologien sollen sich KMU im Markt für IKT etablieren und wettbewerbsfähiger werden. Die Förderung ist offen für die gesamte Themenbreite des Programms zu IT-Sicherheit und Datenschutz.

4.2.4 Sprunginnovationen ermöglichen

Mit der Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) und der Agentur für Sprunginnovationen (SPRIN-D) hat die Bundesregierung zwei Einrichtungen geschaffen, um hochinnovative Risikoprojekte zu fördern. Die Cyberagentur identifiziert Innovationen auf dem Gebiet der Cybersicherheit und vergibt konkrete Aufträge für die Entwicklung innovativer Lösungen. Mit dem Fokus auf die äußere und innere Sicherheit ergänzt die Cyberagentur die anderen Initiativen der Bundesregierung. SPRIN-D sucht nach Antworten auf die sozialen, ökologischen und ökonomischen Herausforderungen unserer Zeit. Ziel ist es, von Deutschland aus neue Sprunginnovationen zu entwickeln, also Produkte, Dienstleistungen und Systeme, die unser Leben spürbar und nachhaltig verbessern. SPRIN-D und Cyberagentur sollen sichere Räume schaffen, in denen Anwendende Risiken eingehen und radikal anders denken können.

4.3 Akteure vernetzen

IT-Sicherheit ist ein Querschnittsthema, das alle gesellschaftlichen, wirtschaftlichen und wissenschaftlichen Akteure und Schichten betrifft. Weitere wichtige Querschnittsthemen sind durch die Datafizierung aller Lebens- und Wirtschaftsbereiche die Themen Datenschutz und Privatheit. Vor diesem Hintergrund zielt das vorliegende Programm darauf ab, alle Akteurinnen und Akteure zu vernetzen. Dies betrifft sowohl die horizontale Vernetzung im Rahmen interdisziplinärer Forschung als auch die vertikale Vernetzung von Wissenschaft, Wirtschaft und Endanwendenden. Die notwendige Kooperation geht dabei über einzelne Förderprojekte und Maßnahmen hinaus. Das Programm wird daher existierende Kooperationsformate, wie das Forum Privatheit, ausbauen und neue Formate schaffen.

4.3.1 Interdisziplinäre Forschungsnetzwerke

Um die gesellschaftlichen Dimensionen von Datenschutz und Informationssicherheit zu erforschen und passende Lösungsansätze zu entwickeln, ist es essenziell, interdisziplinäre Perspektiven auf die Problembereiche einzubeziehen und diese synergetisch zu nutzen.

Plattform Privatheit

Die Plattform Privatheit bildet das Fundament für die umfassende, interdisziplinäre Analyse aktueller Fragestellungen zu Datenschutz und Privatheit sowie für die Entwicklung zielgenauer Lösungen. Auf der Plattform gründen verschiedene thematische Säulen. Das bisherige, sehr erfolgreiche, Forum Privatheit bildet die erste Säule, und bündelt sozialwissenschaftliche, psychologische, juristische und ethische Expertisen. Es werden gesellschaftlich relevante und aktuelle Fragestellungen zum Schutz der Privatheit aus verschiedenen wissenschaftlichen Perspektiven analysiert und Vorschläge für ganzheitliche Lösungsansätze erarbeitet. Bei Bedarf wird das BMBF sukzessive weitere thematische Säulen aufbauen.

Forschungsnetzwerk Depersonalisierung und Anonymisierung

Mit dem Forschungsnetzwerk Depersonalisierung werden künftig Fragen der Anonymisierung und des technischen Datenschutzes gebündelt. Der Kern des Netzwerks besteht aus Living Labs zu unterschiedlichen Anwendungsdomänen, in denen die Anwendung von Depersonalisierung und Anonymisierung am praktischen Beispiel untersucht wird. Die Living Labs werden dabei an GAIA-X als gemeinsamer Datenraum angebunden. Im Sinne einer Diversifizierung und Nutzung des vollen Innovationspotenzials werden die zentralen Living Labs durch eine Maßnahme zur Förderung ergänzender Projekte flankiert.

4.3.2 Innovationsnetzwerke

Innovationsnetzwerke fördern die Innovationskultur und steigern die Ideenvielfalt. Sie machen es möglich, unterschiedliche Sichtweisen in die Forschung und Entwicklung einzubeziehen und Ergebnisse schneller in die Praxis zu bringen.

Forschungshub Quantenkommunikation

Mit der Einrichtung eines Innovationshubs für Quantenkommunikation wird die in Deutschland bestehende Lücke zwischen der sehr guten Forschungsleistung und der industriellen Entwicklung von Komponenten, Systemen und Lösungen für die Quantenkommunikation geschlossen. Ziel ist es, ein Ökosystem von Herstellern und Anbietern von Quantenkommunikationslösungen in Deutschland zu schaffen. Zentral ist hierfür ein gezielter Know-how-Transfer aus den Forschungslaboren in die deutsche Wirtschaft durch das Zusammenspiel von industriell geführten Pilotprojekten und Testlaboren für KMU sowie einem Schirm-Projekt zur Koordination der Aktivitäten. Weitere Forschungs- und Entwicklungsvorhaben komplettieren das Förderportfolio. Dabei sollen auch Synergien mit der geplanten Plattform 6G genutzt werden.

Regionale Innovationscluster

Innovationscluster sind regionale Zusammenschlüsse von Forschungseinrichtungen, Unternehmen und weiteren Multiplikatoren mit dem Ziel, die Innovationsdynamik nachhaltig zu verbessern. Durch die räumliche Nähe ist ein besserer Austausch zwischen den Clusterbeteiligten möglich. Im Bereich der IT-Sicherheit gibt es bereits verschiedene Cluster, die regional vorhandene Forschungs- und Entwicklungsressourcen bündeln und als Innovationstreiber sowie als Transferschnittstellen von der Universität bis zur Industrie wirken. Neben den bereits bestehenden Innovationsclustern und Clusterinitiativen, wie der themenoffenen Zukunftsclusterinitiative (Clusters4Future), sollen zukünftig weitere regionale Cluster zur IT-Sicherheit aufgebaut werden. Im Rahmen des Programms wird der Austausch mit den verschiedenen Netzwerken und Plattformen weiter ausgebaut, um einerseits mögliche Forschungs- und Entwicklungsbedarfe frühzeitig zu erkennen und zu unterstützen und andererseits mögliche Verbünde zur Umsetzung dieser Bedarfe besser zusammenführen zu können.

Forschungs-Hubs 6G

Im Rahmen der Umsetzung des Konjunkturpaketes „Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken“ der Bundesregierung erfolgt die Förderung der 6G-Forschungs-Hubs. Die 6G-Forschungs-Hubs bauen auf wissenschaftliche Exzellenz: Aus der Zusammenarbeit herausragender Forschungsinstitute und Hochschulen sollen Innovationen für die Kommunikationstechnologien der Zukunft entstehen. Dabei soll das Thema IT-Sicherheit von Anfang an mitgedacht werden. Begleitet werden die Hubs durch die Plattform 6G zur Bündelung der Aktivitäten und durch industriegeführte Verbundprojekte der 6G-Initiative. Durch eine enge Anbindung an europäische Förderprogramme kann Deutschland den internationalen 6G-Standard gerade auch in der Sicherheit und im Datenschutz maßgeblich mitgestalten und frühzeitig sichere technologische Grundlagen entwickeln. Damit wird das Fundament dafür gelegt, bei dieser Schlüsseltechnologie mit innovativen und international wettbewerbsfähigen Produkten wichtiger Akteur am globalen Markt zu werden.

4.3.3 Strategische Netzwerke

Strategische Netzwerke sind ein wichtiges Instrument, um relevante Akteure zusammenzubringen und für eine nachhaltige Stärkung der gesamten Forschungslandschaft zu sorgen.

Nationaler Cybersicherheitsrat

Der 2011 eingerichtete Nationale Cyber-Sicherheitsrat (Cyber-SR) gestaltet unter dem Vorsitz des Beauftragten der Bundesregierung für Informationstechnik (BfIT), die Zusammenarbeit im Bereich Cybersicherheit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft. Seit Oktober 2018 unterstützt die ständige Wissenschaftliche Arbeitsgruppe – unter geteilter Leitung des Bundesministeriums des Innern, für Bau und Heimat (BMI) sowie des BMBF − den Cyber-SR. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Allianz für Cybersicherheit

Die Allianz für Cybersicherheit des BSI verbindet als größte nationale Vernetzungsinitiative zur IT-Sicherheit in Deutschland eine Vielzahl von Unternehmen und Institutionen sowie andere Verbünde und Verbände. Sie verfolgt das Ziel, Informationen, Wissen und Erfahrung zwischen den Mitgliedern auszutauschen und so den Ausbau von Sicherheitskompetenzen zu fördern. Insbesondere Fragestellungen hinsichtlich der Forschungs- und Entwicklungsbedarfe spielen dabei eine besondere Rolle.

Wissenschaftliche Akademien

Wissenschaftliche Akademien als Plattformen und Zusammenschlüsse exzellenter Forschender fungieren auch als Politikberatung zu aktuellen technischen und wissenschaftlichen Herausforderungen. Zudem haben sie wissenschaftliche Themen und Entwicklungen im Blick, die zukünftig maßgebliche gesellschaftliche Auswirkungen haben werden, wozu auch der Bereich IT-Sicherheit zählt. Die Deutsche Akademie der Technikwissenschaften (acatech) fokussiert vor allem technische Themen und Zukunftsfragen im Technologiebereich, unter anderen zum Dachthema „Sicherheit in der digital vernetzten Welt“. Die Nationale Akademie der Wissenschaften Leopoldina als übergeordnete nationale Akademie beschäftigt sich ebenfalls mit Aspekten der Digitalisierung und Privatheit, die auch Relevanz für die IT-Sicherheitsforschung haben.

4.4 In den gesellschaftlichen Dialog treten

Technische Innovationen können nur im Alltag ankommen, wenn künftige Nutzende sie akzeptieren, ihre Vorteile erkennen und ihnen vertrauen. Wissenschaftliche Praxis muss daher eng im Dialog mit der Gesellschaft erfolgen.

4.4.1 Bürgerinnen und Bürger in der Forschung

Nur durch die Teilhabe aller wichtigen Akteure an Forschung und die Berücksichtigung spezifischer Bedarfe und Ansprüche an Technik und Fortschritt ist sichergestellt, dass sie zum Nutzen aller praktikabel umgesetzt wird. In der Förderung von IT-Sicherheitsforschung werden deshalb partizipative Entwicklungsansätze sowie interaktive Dialogformate und zielgruppenspezifische Maßnahmen der Wissenschaftskommunikation umgesetzt.

Touchpoints für Gründungsberatung

Bei der BMBF-Gründungsförderung nehmen Plattformen zur Vernetzung und Dialogformate eine besondere Rolle ein. An den nationalen Forschungszentren zur IT-Sicherheit ATHENE in Darmstadt, CISPA in Saarbrücken und KASTEL in Karlsruhe sowie an der Ruhr-Universität Bochum organisieren die dort angesiedelten Beratungszentren für Forschungsteams regelmäßig Gründungsstammtische, diverse Informationsveranstaltungen und Workshops – zum Beispiel unter dem Titel Hub Nights.

Dialog für Cybersicherheit

Mit Dialogformaten nimmt das BSI neue Impulse und Ideen aus allen gesellschaftlichen Gruppen auf und erkennt dabei frühzeitig ihre spezifischen Bedarfe. Die Formate bieten den Teilnehmenden eine Plattform, um ihre Themen und Vorstellungen zur Cybersicherheit zu diskutieren. Gleichzeitig erhalten die Beteiligten wertvolles Feedback zu eigenen Lösungen und können ihre Entscheidungen und Handlungen transparent präsentieren.

4.4.2 Kommunikationskampagne für Sichtbarkeit und Sensibilisierung

Lösungen der IT-Sicherheit für Anwendungen der Zukunft werden in Deutschland durch eine international renommierte Forschungscommunity entwickelt und in die Gesellschaft transferiert. Die Bürgerinnen und Bürger haben hiervon vielerorts jedoch keine Kenntnis. Das BMBF startet daher zur Begleitung des neuen Forschungsprogramms eine nationale Kampagne zur Erhöhung der Sichtbarkeit und des Verständnisses der IT-Sicherheitsforschung in der Öffentlichkeit. IT-Sicherheitsforschung soll mit dem Leitgedanken „Forschung ist der Schlüssel für eine sichere digitale Zukunft“ als grundlegender Problemlöser für eine erfolgreiche digitale Zukunft positioniert werden. Im Mittelpunkt der integrierten Kampagne stehen spielerische Elemente in alltagsnahen Szenarien, um die Wissenschaft im Umfeld der komplexen IT-Sicherheitsforschung erlebbar und erfahrbar zu machen. Eine Informationstour an Schulen und kulturellen Einrichtungen wie „Mitmach-Museen“ runden die Kampagne ab.

4.5 Europäisch und international forschen

Forschung und Innovation in Deutschland stehen im Kontext internationaler Entwicklungen und Bestrebungen zur Lösung der Herausforderungen der Digitalisierung. Um die eigene Rolle am globalen Markt, die Wettbewerbsfähigkeit und Souveränität Deutschlands und Europas zu stärken, bringt sich Deutschland in bilaterale und multilaterale Maßnahmen sowie Initiativen, insbesondere der EU, ein.

4.5.1 Bilaterale Kooperation

Bilaterale Forschungsmaßnahmen und -initiativen wie „2+2“-Förderprojekte im Bereich IT-Sicherheit mit Ländern Europas und weltweit, wie die erfolgreichen Formate Deutschland-Frankreich, Deutschland-Israel und Deutschland-Japan, werden im Rahmen des Programms ausgebaut, neue Formate und Kooperationsmaßnahmen werden angestrebt.

Deutsch-französische Kooperationen

Das BMBF und das französische Forschungsministerium (MESRI) haben sich auf dem sechsten Forum zur deutsch-französischen Zusammenarbeit geeinigt, eine starke deutsch-französische Forschungsachse zur Cybersicherheit zu entwickeln. Diese Vereinbarung wird unter anderem durch die Richtlinie zur Förderung von deutsch-französischen Verbundprojekten zur Cybersicherheit umgesetzt. Ziel dieser Förderung ist es, hochinnovative Lösungen zur Wahrung der Privatsphäre zu entwickeln. Dabei sollen durch die Verbundprojekte die deutsch-französische Zusammenarbeit gestärkt und die sich aus der Kooperation ergebenden Synergien genutzt werden, um weitreichende Fortschritte in der Cybersicherheit zu erzielen.

Das CISPA und das INRIA/Loria in Nancy werden gemeinsam die Cybersicherheitsforschung und entsprechende Transfer- und Innovationsaktivitäten zwischen Frankreich und Deutschland stärken. In dem French-German-Center for Cybersecurity sind die Kräfte der größten und renommiertesten Forschungszentren für Cybersicherheit in Europa gebündelt. Das Zentrum wird bilaterale deutsch-französische Forschungsgruppen aufbauen. Neben der länderübergreifenden inhaltlichen Zusammenarbeit ist die Nachwuchsförderung ein Kernelement. Junge Forschende erhalten die Möglichkeit, durch individuelles Mentoring früh in ihrer akademischen Karriere eigenständig Forschungsinteressen voranzutreiben.

Deutsch-israelische Kooperation

Das BMBF und die National Technological Innovation Authority of the State of Israel (NATI) − vertreten durch das Israel-Europe R&I Directorate (ISERD) − fördern im Rahmen der bilateralen Fördermaßnahme Maßnahme in den Forschungsbereichen „Zivile Sicherheit“ und „IT-Sicherheit“ die Kooperation zwischen deutschen und israelischen Unternehmen, Forschungspartnern und Anwendern der Wirtschaft. Gefördert werden bilaterale Projekte, die innovative Lösungen für die Verbesserung des Schutzes der Bevölkerung und Wirtschaft entwickeln, unter anderem gegen Bedrohungen durch Terrorismus, Cyberangriffe, organisierte Kriminalität, Naturkatastrophen und technisches Versagen.

Deutsch-japanische Kooperation

Deutschland und Japan haben vereinbart, einen engen wissenschaftlichen Austausch zu pflegen und gemeinsame Forschungsarbeiten zum autonomen Fahren durchzuführen, einschließlich für die hierfür nötige IT-Sicherheit.

4.5.2 Multilaterale Vernetzung

Gemeinsam mit internationalen Partnern können Synergien bei der Entwicklung von weitreichenden sowie belastbaren Lösungen genutzt und gemeinsam neue internationale Standards gesetzt werden. Deutsche Akteure werden eine führende Rolle bei der europäischen IT-Sicherheitsforschung einnehmen, indem sie ihre Kompetenzen, insbesondere in Vorhaben unter dem europäischen Rahmenprogramm für Forschung und Innovation „Horizon Europe 2021-2027“, einbringen und sich an weiteren multilateralen Maßnahmen beteiligen.

HORIZON Europe 2021 – 2027

HORIZON Europe ist eines der weltweit größten Förderprogramme für Forschung und Innovation. Das Arbeitsprogramm wird in vergleichbarer Weise zum sehr erfolgreichen Programm HORIZON 2020 entwickelt. Die Umsetzung der durch HORIZON Europe unterstützten Forschung zu IT-Sicherheit und sicherer Kommunikation wird über das neue Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit koordiniert werden. Das für die Zusammenarbeit mit dem europäischen Kompetenzzentrum einzurichtende Nationale Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (NKCS) soll hierzulande die Kompetenzen der Ressorts BMBF, Bundesministerium für Wirtschaft und Energie, Bundesministerium der Verteidigung und BMI sowie der verschiedenen nationalen Akteure bündeln und synergetisch die Arbeit des Kompetenzzentrums vorantreiben.

ERA-NET

Als Teilinitiative unter HORIZON 2020 entstanden, verfolgt ERA-NET das Ziel, durch die Zusammenarbeit von nationalen und regionalen Forschungsförderorganisationen beziehungsweise Programmagenturen die Forschungsförderung enger aufeinander abzustimmen und damit die wissenschaftliche Kompetenz Europas zu bündeln. Von gemeinsamen Aktivitäten wie Clustering, Trainingsmaßnahmen oder transnationalen Ausschreibungen konnten vor allem in Deutschland tätige KMU sowie Hochschulen oder außeruniversitäre Forschungseinrichtungen profitieren. Auch in Zukunft soll diese Unterstützung fortgeführt werden.

EUREKA

EUREKA ist eine Initiative für anwendungsnahe Forschung in Europa und bietet Industrie und Wissenschaft einen Rahmen für bi- oder multinationale Kooperationsprojekte. Die Initiative trägt dazu bei, die in Europa vorhandenen fachlichen und finanziellen Ressourcen auch in der IT-Sicherheitsforschung effektiver zu nutzen und damit die Wettbewerbsfähigkeit Europas auf dem Weltmarkt zu stärken. Dieser erfolgreiche Ansatz soll fortgeführt werden, um auch zukünftig über global wettbewerbsfähige Technologien in Europa zu verfügen. Der EUREKA-Cluster CELTIC-NEXT ist eine industriegetriebene Initiative im Bereich der Informations- und Kommunikationstechnologien mit den Themenschwerpunkten (Smarte) Vernetzungstechnologien, Datenschutz, IT-Sicherheit und Vernetzung in vertikalen Industriewertschöpfungsketten.

EuroQCI

Ziel der Initiative European Quantum Communication Infrastructure (EuroQCI), an der fast alle EU-Mitgliedstaaten beteiligt sind, ist es, die Grundlagen für eine europaumspannende Infrastruktur zur Quantenkommunikation zu entwickeln, um die europäischen Kapazitäten in den Bereichen Quantenkommunikation, Cybersicherheit und industrielle Wettbewerbsfähigkeit weiter auszubauen. Als Gründungsmitglied der Initiative wird Deutschland seine umfassende Expertise auf dem Gebiet der Quantentechnologie einbringen und so seine internationale Vorreiterrolle weiter ausbauen und festigen.

5 Rahmenbedingungen des Programms

Das vorliegende Forschungsrahmenprogramm zur IT-Sicherheit folgt auf das sehr erfolgreiche Programm „Selbstbestimmt und sicher in der digitalen Welt 2015–2020“. Im Rahmen des Vorgängerprogramms wurden vom BMBF über 350 Mio. Euro zur Verfügung gestellt. Besondere Erfolge des Vorgängerprogramms waren

- die nationalen Kompetenzzentren für IT-Sicherheit: ATHENE, CISPA, KASTEL,
- das Nationales Referenzprojekt zur IT-Sicherheit in der Industrie 4.0,
- das Forum Privatheit.

Für das vorliegende neue Programm plant alleine das BMBF, im Zeitraum von 2021–2026 über 350 Mio. Euro aus seinem Budget bereitzustellen.

5.1 Entstehung

Der digitale Wandel als grundlegende Veränderung von gesellschaftlicher, wirtschaftlicher und staatlicher Organisation ist in vollem Gang. Es ist allgemein anerkannt, dass das Gestalten einer digitalen Gesellschaft und Ökonomie eine wichtige staatliche Aufgabe ist. IT-Sicherheit ist dabei die Basis erfolgreicher Digitalisierung in allen Anwendungsfeldern und Branchen; in den Fokus rücken zunehmend auch Aspekte wie Datenschutz und Demokratie. Zur Sicherung der eigenen Handlungsfähigkeit, also der technologischen Souveränität, ist eine weitere Stärkung der IT-Sicherheitsforschung notwendig. Diese Aufwertung ist ein wesentlicher Bestandteil der nationalen Schlüsseltechnologie für Cybersicherheit. Aus dieser Notwendigkeit begründet sich ein erhebliches Bundesinteresse. Aufgrund der übergeordneten Bedeutung für den Gesamtwirtschaftsstandort Deutschland und dem damit verbundenen Bedarf an Fachkräften, ist ein länderübergreifender Rahmen für Forschungsaktivitäten notwendig. Weiterhin sind aufgrund des globalen Charakters der Digitalisierung und technologischen Entwicklung europäische und internationale Anbindungen erforderlich. Daher ist ein Forschungsrahmenprogramm auf Bundesebene zielführend. Zahlreiche Sicherheitsvorfälle auf staatlicher und wirtschaftlicher Ebene sowie bei Bürgerinnen und Bürgern zeigen, dass bisher kein ausreichendes IT-Sicherheitsniveau erreicht wurde. Ebenso bestätigte der eingesetzte wissenschaftliche Begleitkreis, dass noch umfangreicher Forschungsbedarf besteht. Die Bilanzierung des Vorgängerprogramms sowie des Programms IKT 2020 ergab, dass die größten Herausforderungen für Forschungsvorhaben fehlende Finanzierungsmöglichkeiten und wirtschaftliches Risiko sind. Aus dem erheblichen Bundesinteresse an besserer IT-Sicherheit, der Forschung als notwendige Grundlage der Verbesserung von IT-Sicherheit und der sonst nur in wesentlich geringerem Umfang stattfindenden Forschung für IT-Sicherheit leitet sich der staatliche Handlungsbedarf ab.

Das vorliegende Programm wurde mit Unterstützung von zwölf Expertinnen und Experten aus Wissenschaft, Wirtschaft und öffentlichen Einrichtungen entwickelt.

5.2 Einbindung des Programms

Das neue Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän.“ aktualisiert die Forschungsstrategie der Bundesregierung zur IT-Sicherheit zeitgemäß und knüpft unmittelbar an die Erfolge des Vorgängerprogramms an. Das vorherige Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit war das erste Programm, das die Forschungsaktivitäten des Bundes zur IT-Sicherheit bündelte. Das vorliegende Programm übernimmt diese zentrale Stellung und die bestehenden Anknüpfungen auf Landes-, Bundes- und EU-Ebene. Es steht also nicht isoliert, sondern führt die Vernetzung des Vorgängerprogramms mit zahlreichen anderen Aktivitäten der Forschungspolitik fort. Aufgrund des Charakters als Querschnittsthema der gesamten Digitalisierung sind die Verbindungen der IT-Sicherheit extrem vielfältig. Neben der übergeordneten Hightech-Strategie sind im Folgenden besonders zentrale Anknüpfungspunkte dargestellt.

Verknüpfung mit weiteren Strategien und Programmen

Das Programm trägt unter anderem zur Umsetzung der Cyber-Sicherheitsstrategie für Deutschland[10], der Datenstrategie der Bundesregierung[11], der Strategie Künstliche Intelligenz der Bundesregierung[12] und dem BMBF-

[10] https://www.bmi.bund.de/cybersicherheitsstrategie/
[11] https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632
[12] https://www.ki-strategie-deutschland.de

Aktionsplan „Natürlich. Digital. Nachhaltig.“[13] bei. Das Programm hat Berührungspunkte zu zahlreichen weiteren laufenden oder geplanten Strategien und Programmen der Bundesregierung und ihren Ressorts, insbesondere zur zivilen Sicherheit[14], zu Kommunikationstechnologien[15,] zu Industrie 4.0[16,] zur Medizintechnik[17], zum autonomen und vernetzten Fahren[18], zur Mikroelektronik[19,] zur Menschtechnik Interaktion[20], zu Quantentechnologien[21] sowie zur Zukunft der Wertschöpfung[22] da IT-Sicherheit die integraler Bestandteil von jedweder Digitalisierung ist.

Vernetzung mit weiteren Akteuren

Als Teil der Cyber-Sicherheitsstrategie für Deutschland trägt das Programm zur Verknüpfung der Aktivitäten aller staatlichen Akteure in der IT-Sicherheitsforschung bei. Dies umfasst alle Akteure auf europäischer, Bundes- und Landesebene. Durch den Austausch, das Zusammenbringen und die Bündelung der im Bund bereits vorhandenen IT-Kompetenzen soll die eigene IT-Kompetenz insgesamt ausgebaut werden. So können beispielsweise die IT-Erkenntnisse, die in den Institutionen des Bundes produziert werden, in die Entscheidungen bezüglich der weiteren Entwicklung der IKT-Strukturen des Bundes einbezogen werden.

Enge Zusammenarbeit mit dem künftigen EUCCC

Wie im Sommer 2019 von der EU mit dem Cybersecurity Act (EU) 2019/881 angekündigt, wird in 2021 eine neue EU-Agentur in Rumänien gegründet werden, mit der Bezeichnung EU Cybersecurity Competence Center (EUCCC). Damit soll ein EU-weites Netzwerk an Cybersicherheits-Laboren in den 27 Mitgliedsstaaten entstehen, das in den Bereichen „Protection“, „Detection“ und „Reaction“ neueste Erkenntnisse im Bereich IT-, IKT- und IoT-Sicherheit austauschen wird. Die intensive Zusammenarbeit mit der deutschen Forschungslandschaft soll die Sichtbarkeit im EU-Raum erhöhen und die wissenschaftlichen Kompetenzen verdeutlichen.

5.3 Erfolgskriterien, Wirtschaftlichkeit und Evaluation

5.3.1 Erfolgskriterien des Gesamtprogramms

Indikatoren für den Erfolg des Gesamtprogramms sind das IT-Sicherheitsniveau Deutschlands sowie der Beitrag der IT-Sicherheit zur technologischen Souveränität in Schlüsseltechnologien, gemessen unter anderem an der Anzahl und Schwere von IT-Sicherheitsvorfällen sowie dem Umfang des Einsatzes von IT-Sicherheitstechnologien von deutschen und europäischen Herstellern, Weitere Indikatoren sind die Anzahl von ermöglichten Forschungsvorhaben, welche sonst nicht durchgeführt worden wären, sowie erzielte Netzwerkeffekte und die Qualität der Bündelung von Kompetenzen.

5.3.2 Erfolgskriterien der strategischen Ziele

Zu den in Kapitel 2 definierten Zielen wurden zur Erfolgsmessung jeweils Indikatoren entwickelt. Diese Indikatoren stellen keine abschließende Liste der möglichen Messgrößen dar und werden gemäß der Konzeption als lernendes Programm gegebenenfalls angepasst. Grundsätzlich wird eine sachgerechte Kombination aus qualitativen und quantitativen Indikatoren angestrebt.

Digitaler Wandel: sicher und nachhaltig

Indikatoren für das Erreichen dieses Ziels sind unter anderem der Umfang, in welchem Bürgerinnen und Bürger sowie KMU Informationen über und Unterstützung bei IT-Sicherheit erhalten. Ein weiterer Indikator ist die Anzahl von IT-Sicherheits-Start-ups am Markt.

---

13 https://www.bmbf.de/de/digitalisierung-und-nachhaltigkeit-10466.html
14 https://www.sifo.de/de/sicherheitsforschung-forschung-fuer-die-zivile-sicherheit-1693.html
15 https://www.forschung-it-sicherheit-kommunikationssysteme.de/forschung/kommunikationssysteme
16 https://www.plattform-i40.de/PI40/Navigation/DE/Industrie40/Leitbild2030/leitbild-2030.html
17 http://gf-bmbf.de/
18 https://www.bmbf.de/de/automatisiertes-fahren-4158.html
19 https://www.elektronikforschung.de/rahmenprogramm
20 https://www.interaktive-technologien.de/service/publikationen/miteinander-durch-innovation
21 https://www.quantentechnologien.de/qt-in-deutschland/programm.html
22 https://www.bmbf.de/de/die-zukunft-der-wertschoepfung-in-deutschland-13891.html

Daten und Know-how: geschützt und nutzbar

Indikatoren für das Erreichen dieses Ziels sind unter anderem die Verfügbarkeit sicherer Datenräume in Deutschland und Europa, die Anzahl und Effizienz datenschutzfreundlicher KI-Lösungen sowie die Verfügbarkeit von Methoden zum Erzeugen qualitativ hochwertiger Trainingsdaten für KI. Weitere durch Forschung aber lediglich mittelbar beeinflussbare Indikatoren sind die Anzahl und Schwere der durch IT-Sicherheitsvorfälle verursachten Verletzungen geistigen Eigentums sowie Datendiebstähle.

Demokratie und Gesellschaft: stabil und digital

Indikatoren für das Erreichen dieses Ziels sind unter anderem die Beteiligung von Bürgerinnen und Bürgern zu Fragen der Verfügbarkeit von vertrauenswürdigen Nachrichten und Informationen sowie Umfang und Effizienz von Faktenchecks. Weitere Indikatoren sind die Möglichkeiten und Anwendungen von sicherer digitaler Partizipation an demokratischen Prozessen und die Verfügbarkeit freier und offener Kommunikationsstrukturen.

Privatheit und Datenschutz: selbstbestimmt und innovativ

Indikatoren für das Erreichen dieses Ziels sind unter anderem die Anzahl von Start-ups im Bereich Datenschutz und Privatheit sowie die Anzahl von Unternehmen mit privatheitsfreundlichen Geschäftsmodellen und die Zahl von Produktinnovationen. Weitere Indikatoren sind die Anzahl deutscher Vertreter in relevanten internationalen Gremien, die Breite des Dialogs sowie die Anzahl Länder weltweit mit Datenschutz europäischer Prägung.

Innovation und Transfer: weltspitze und zukunftssicher

Indikatoren für das Erreichen dieses Ziels sind im Bereich Wirtschaft die Anzahl von Produktinnovationen und Patenten, die wirtschaftliche Performance von deutschen Unternehmen in IT-Sicherheit und Datenschutz im weltweiten Vergleich sowie die Anzahl der Arbeitsplätze. Indikatoren im Bereich Wissenschaft sind unter anderem das Renommee der wissenschaftlichen Einrichtungen sowie deren Output, insbesondere auch die Zahl der Open-Access-Publikationen. Weitere Indikatoren sind die Anzahl neuer Kontakte zwischen Wissenschaft und Wirtschaft, die Anzahl neuer Kooperationen sowie die Beteiligung an internationaler Standardisierung. Im Bereich Zivilgesellschaft werden Indikatoren zu Qualität und Quantität partizipativer Entwicklungsansätze sowie interaktiver Dialogformate und zielgruppenspezifischer Maßnahmen der Wissenschaftskommunikation zugrunde gelegt.

Führende Köpfe: qualifizieren und gewinnen

Indikatoren für das Erreichen dieses Ziels sind unter anderem die Anzahl der Promotionen mit Bezug zur IT-Sicherheit sowie die Anzahl einschlägiger Publikationen junger Wissenschaftlerinnen. Weitere Indikatoren sind der Kompetenzzuwachs in Unternehmen und die Breite der technologischen Kompetenz sowie die Attraktivität des Standorts Deutschland für Forschende.

Deutschland und Europa: technologisch souverän

Indikatoren für das Erreichen dieses Ziels im Bereich der IT-Sicherheit sind unter anderem der Abdeckungsgrad von Wertschöpfungsketten beziehungsweise die Vollständigkeit des Innovationsökosystems aus der Hand deutscher und europäischer Akteure sowie Produktionsstatistiken, Exportanteile am Weltmarkt und Handelsbilanzen. Weitere Indikatoren sind die Anzahl der Patente sowie die Beteiligung an der Standardisierung.

5.3.3 Wirtschaftlichkeit der Projektförderung

Aufgrund der dynamischen Entwicklung in den Bereichen IT-Sicherheit und Datenschutz sowie zu erwartender Veränderungen der ökonomischen und technisch-wissenschaftlichen Rahmenbedingungen ist das Programm lernend angelegt. Bekannte und neue Themenfelder werden laufend beobachtet und die jeweilige Ziel-, Aufgaben- und Prioritätensetzung aktualisiert. Förderinstrumente werden entsprechend passend weiterentwickelt. Durch Technologieanalysen sowie Fachgespräche und gegebenenfalls den Begleitkreis werden im Vorfeld von Bekanntmachungen die Fördermaßnahmen dem tatsächlichen Entwicklungsstand in Wissenschaft und Wirtschaft angepasst. Den mit dem Agendaprozess intensivierten Dialog mit Wissenschaft, Wirtschaft und Zivilgesellschaft wird das BMBF zur Qualitätssicherung, Fortschreibung und Weiterentwicklung fortführen, um auf technologische, wirtschaftliche und gesellschaftliche Entwicklungen angemessen und zeitnah reagieren zu können.

Die Schwerpunktsetzung bei Verfahren und Förderkriterien erfolgt in der Regel durch die Veröffentlichung von Förderthemen in Form von Bekanntmachungen im Bundesanzeiger sowie deren Verbreitung im Internet auf den

Seiten des BMBF. Mit diesen Bekanntmachungen werden die Fördermodalitäten beziehungsweise -regularien verbindlich festgelegt. In einem zweistufigen Verfahren können zunächst Skizzen für Verbundprojekte bei dem beauftragten Projektträger eingereicht werden. Die eingereichten Projektvorschläge stehen im Wettbewerb. Das BMBF und die Projektträger behalten sich vor, sich bei der Auswahl der zu fördernden Projektvorschläge themenspezifisch durch einen unabhängigen Fachausschuss beraten zu lassen. Die der Bewertung und Auswahl zugrunde gelegten Kriterien, für beide Stufen, werden in den Bekanntmachungen der jeweiligen Fördermaßnahme veröffentlicht. In der zweiten Stufe des Auswahlverfahrens werden die Konsortien mit hinreichend hoher Priorität zur Vorlage eines förmlichen Förderantrages zu ihren Projektvorschlägen aufgefordert.

Durch die laufende Anpassung des Programms und die Qualitätssicherung für Fördermaßnahmen in Kombination mit dem wettbewerblichen Auswahlverfahren wird wissenschaftliche Exzellenz und eine große Innovationshöhe sichergestellt. Die Projektförderung im Rahmen von Förderbekanntmachungen nach diesem Prinzip folgt daher beim Mitteleinsatz grundsätzlich dem Maximalprinzip und eine Wirtschaftlichkeit ist gegeben. Förderungen außerhalb von Bekanntmachungen sind von dieser Betrachtung nicht gedeckt und benötigen gegebenenfalls eine eigenständige Wirtschaftlichkeitsprüfung.

5.3.4 Evaluation

Das Programm als solches ist lernend angelegt. Durch einen laufenden Dialog mit den Zielgruppen, das Monitoring von Förderdaten sowie die Nutzung von Informationen aus Projektberichten, inklusive der Sicherstellung der Vollzugswirtschaftlichkeit, erfolgt eine fortlaufende zeitnahe Nachjustierung des Programms. Hierzu werden insbesondere die beschriebenen Indikatoren herangezogen. So wird sowohl die forschungspolitische Wirksamkeit des Programms als auch die Maßnahmenwirtschaftlichkeit laufend geprüft und gegebenenfalls geeignet ergänzt oder angepasst. Dies erreicht eine evidenzbasierte Justierung von Inhalten und Maßnahmen und bereitet die spätere Ex-post-Evaluierung zur Zielerreichungs- und Wirkungskontrolle des Programms bereits zur Laufzeit vor.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333