Bundesministerium
für Bildung
und Forschung

Agenda Cybersicherheitsforschung

Maßnahmen im Zuge der Zeitenwende

Inhaltsverzeichnis

Einleitung

Die von Bundeskanzler Olaf Scholz Ende Februar 2022 festgestellte Zeitenwende beschreibt mit einem Wort eine Zäsur in der politischen Agenda. Die veränderten weltpolitischen Rahmenbedingungen betreffen auch die künftige Cybersicherheit und damit die Forschung zur IT-Sicherheit in Deutschland und Europa.

Der Krieg in der Ukraine führt uns vor Augen, wie politische und militärische Spannungen heute vermehrt auch im digitalen Raum ausgetragen werden. Und er verdeutlicht, wie essenziell eine hohe Cybersicherheit für moderne Gesellschaften geworden ist: Cyberangriffe auf kritische Infrastruktur sowie die Netze von Unternehmen und Behörden werden zunehmend Bestandteil von staatlichen Auseinandersetzungen und hybrider Kriegsführung. Desinformationskampagnen mittels Fake News, Verschwörungstheorien und Propaganda werden gezielt eingesetzt, um Ängste und Unsicherheiten zu schüren, Meinungen zu manipulieren und den gesellschaftlichen Zusammenhalt zu schwächen. Kommunikationsinfrastrukturen werden attackiert, um Lieferketten, Verkehrsströme oder die Energieversorgung zu stören.

Diesen Entwicklungen und damit einhergehenden Herausforderungen muss auf allen Ebenen begegnet werden. Durch eine gut aufgestellte und zielgerichtete Forschungsförderung geht das Bundesministerium für Bildung und Forschung (BMBF) diese Herausforderungen an und legt damit das Fundament für die zukünftige Cybersicherheit in Deutschland. Im aktuellen Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Digital. Sicher. Souverän.“[1] bestimmen die technologische Souveränität Deutschlands sowie der Schutz demokratischer Werte bereits die forschungspolitische Agenda. Die grundsätzliche Ausrichtung des Programms und dessen Schwerpunkte in der Forschungsförderung sind vor dem Hintergrund der Zeitenwende aktueller denn je.

Die vorliegende Agenda Cybersicherheitsforschung fasst in Ergänzung Maßnahmen des BMBF zusammen, um den durch die Zeitenwende ausgelösten Herausforderungen noch zielgenauer zu begegnen. Die wesentlichen Leitgedanken der Agenda bilden drei übergreifende förderpolitische Ziele:

1. Die technologische Souveränität Deutschlands und Europas muss weiter gestärkt und kritische Abhängigkeiten in der Cybersicherheit müssen reduziert werden.

2. Cybersicherheit, Privatheit und Nachhaltigkeit müssen als zentrale Grundprinzipien in Forschung, Entwicklung und Innovation verankert werden.

3. Fördermaßnahmen müssen noch stärker auf allen Ebenen der Gesellschaft vernetzt und so der Transfer von der Forschung in Wirtschaft und Gesellschaft intensiviert werden.

Diese Ziele stehen im Einklang mit dem Koalitionsvertrag 2021–2025, in dem vereinbart wurde, digitale Bürgerrechte und IT-Sicherheit zu stärken. Der Koalitionsvertrag zielt auf einen starken Technologiestandort Deutschland, der auf europäischen Werten basiert, Talente anzieht sowie Zukunftsfähigkeit und Wohlstand sichert. Um all dies zu gewährleisten, ist eine am Menschen orientierte, breit aufgestellte und innovative Cybersicherheitsforschung Grundvoraussetzung.

Die vorliegende Agenda Cybersicherheitsforschung leistet einen wichtigen Beitrag zur Zukunftsstrategie Forschung und Innovation[2], zur Digitalstrategie[3] und zur Weiterentwicklung der Cybersicherheitsstrategie für Deutschland.

1 Online verfügbar unter: https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/5/31672_Digital_Sicher_Souveraen.pdf
2 vgl. https://www.bmbf.de/bmbf/de/forschung/zukunftsstrategie/zukunftsstrategie_node.html
3 vgl. https://digitalstrategie-deutschland.de

1. Sichere, widerstandsfähige digitale Systeme schaffen

Die umfassende Digitalisierung hat enorme positive Effekte auf Wohlstand und Fortschritt weltweit. Allerdings geht sie auch mit Risiken einher, die durch die veränderte weltpolitische Lage noch deutlicher als bisher zu Tage treten. Die Angriffsflächen für Cyberattacken auf kritische und staatliche Infrastruktur, Lieferketten und Produktion nehmen mit der fortschreitenden Digitalisierung und Vernetzung weiter zu. Um diesen Herausforderungen mittel- und langfristig zu begegnen, müssen wir unsere digitalen Informations- und Kommunikationsinfrastrukturen in Deutschland und Europa möglichst resilient und krisensicher aufstellen. Hierfür müssen wir unsere Innovationsökosysteme ausbauen, das heißt die Forschung zu wichtigen Basistechnologien weiter stärken, aber auch den Transfer von der Forschung in die Wirtschaft intensivieren. Im Speziellen müssen wir:

Maßnahmen im Zuge der Zeitenwende

- kritische Netzinfrastrukturen zukünftig noch besser absichern und möglichst resiliente Informations- und Kommunikationssysteme erforschen und entwickeln;
- die Kommunikationssysteme der nächsten Generation von Anfang an sicher gestalten (Security by Design), unter anderem mit der Verankerung von Cybersicherheit als elementarem Baustein in der Forschung und Entwicklung des zukünftigen Mobilfunkstandards 6G;
- Post-Quanten-Kryptografie erforschen und in die breite Anwendung bringen, um für das künftige Zeitalter der Quantencomputer gerüstet zu sein;
- durch die zügige Entwicklung und Integration von Quantenkommunikation unsere IT-Sicherheitsökosysteme zukunftssicher aufstellen;
- mit erweiterter Gründungsförderung (wie der Initiative „StartUpSecure“) Technologien und Innovationen der IT-Sicherheit schneller in die Anwendung in Wirtschaft und Gesellschaft bringen.

2. Komplexe Herausforderungen interdisziplinär angehen

Es lassen sich immer aufwändigere und komplexere Cyberangriffe beobachten, die verschiedene Angriffsvektoren kombinieren und teils von langer Hand geplant werden. Wir erleben, dass Cyberbedrohungen durch potente, staatlich gelenkte Akteure zunehmend Realität werden. Zusätzliche Komplexität entsteht durch die steigende digitale Vernetzung unterschiedlichster Gesellschaftsbereiche mit Entwicklungen wie dem Internet der Dinge. Dies erfordert eine ganzheitliche Betrachtung und Herangehensweise, die verschiedene Forschungsgebiete, wie IT-Sicherheit und Kommunikationssysteme, Rechts- und Sozialwissenschaft, miteinander verbindet. Die interdisziplinäre Zusammenarbeit über die jeweiligen Grenzen einzelner Forschungsgebiete hinaus wird vermehrt notwendig, um der Komplexität der digitalen Vernetzung und damit einhergehender neuartiger Cybergefahren gerecht zu werden. Deshalb wollen wir:

Maßnahmen im Zuge der Zeitenwende

- die Sicherheit, Resilienz und Vertrauenswürdigkeit unserer hochvernetzten Informations- und Kommunikationsinfrastruktur durch eine neue Leitinitiative „Hyperkonnektivität“ in den Fokus nehmen und ganzheitlich realisieren;
- die Entwicklung von Konzepten und Technologien für ein sichereres Internet der Dinge fördern und als Basis für vertrauenswürdige Produkte und Infrastrukturen etablieren;
- die Forschung für benutzbare IT-Sicherheit weiter ausbauen, um die Akzeptanz von und das Vertrauen in Sicherheitslösungen zu stärken;
- die Kooperation der Forschung zu Quantenkommunikation und 6G intensivieren;
- mit dem Ausbau der interdisziplinären „Plattform Privatheit“ die gesellschaftlichen Herausforderungen des digitalen Lebens analysieren, diskutieren und Alternativen aufzeigen.

3. Cybersicherheit in der Forschungslandschaft stärken

Deutschland besetzt auf vielen Forschungsgebieten internationale Spitzenpositionen, so auch in der IT-Sicherheit. BMBF-geförderte Einrichtungen wie das CISPA Helmholtz-Zentrum für Informationssicherheit und das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE forschen auf höchstem Niveau. Gleichzeitig sieht sich auch die Forschung zunehmenden Cyberangriffen ausgesetzt; eine Entwicklung, die durch die Zeitenwende nochmals verstärkt wird. Wir müssen unsere Forschungs-IT daher besser absichern und die hierfür notwendigen Strukturen schaffen. Deshalb wollen wir:

Maßnahmen im Zuge der Zeitenwende

- speziell auf die Forschungslandschaft ausgerichtete Cybersicherheitsarchitekturen entwickeln und erproben lassen, die zu einer Stärkung der digitalen Forschungsinfrastrukturen beitragen;
- mit dem Ausbau der Forschung zur Cybersicherheit in der institutionellen Förderung wichtige Impulse und methodische Grundlagen für innovative IT-Sicherheitslösungen bereitstellen;
- mit der Etablierung eines eigenen Arbeitskreises im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) den Informationsaustausch zu Cybervorfällen und Schutzmaßnahmen zwischen Forschungseinrichtungen verbessern.

4. Zusammenarbeit mit Wertepartnern ausbauen

Die neue weltpolitische Lage stellt unsere Wertegemeinschaft auf eine Probe. Es zeigt sich, dass wir gemeinsam stark sind und erfolgreich für unsere Werte eintreten können. Wir müssen diese Stärke weiter ausbauen, um auch kommenden Herausforderungen erfolgreich begegnen zu können. Dafür müssen wir in der Forschung die Zusammenarbeit mit europäischen und internationalen Wertepartnern intensivieren. Unsere Bindungen stärken wir durch gezielte bilaterale und multilaterale Kooperationen, wie beispielsweise:

Maßnahmen im Zuge der Zeitenwende

- in der Zusammenarbeit mit dem Europäischen Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung (ECCC) und dem zugehörigen Netzwerk Nationaler Koordinierungszentren (NCC), die die Förderung von Forschung und Entwicklung zur Cybersicherheit auf europäischer Ebene vernetzen, koordinieren und bündeln;
- durch EU-weite Initiativen wie EuroQCI zum Aufbau einer sicheren europäischen Infrastruktur für Quantenkommunikation, die die Ziele von mehr Cybersicherheit und technologischer Souveränität in Europa befördern;
- durch ausgewählte Forschungskooperationen mit internationalen Wertepartnern zu globalen Technologien und Standards im Bereich Cybersicherheit.

5. Cyberresilienz und -kompetenz der Gesellschaft steigern

Die Stabilität unserer demokratischen Gesellschaft wird auf vielfältige Weise angegriffen. Dies geschieht akut im Kontext des Ukrainekrieges, etwa durch Cyberattacken und Desinformationskampagnen, aber auch langfristig durch eine andauernde Cyberbedrohungslage, die geeignet ist, das Vertrauen in digitale Infrastrukturen und staatliche Institutionen nachhaltig zu schädigen. Daher müssen wir uns vor Cybergefahren jeglicher Art schützen sowie die Cyberresilienz und -kompetenz in der gesamten Gesellschaft ausbauen. Dies kann nur gelingen, indem wir in der Gesellschaft das Bewusstsein für Cyberbedrohungen stärken sowie technisch innovative Lösungen entwickeln, die ein Höchstmaß an IT-Sicherheit, Benutzbarkeit und Datenschutz auch für die Zukunft sicherstellen. Im Speziellen müssen wir:

Maßnahmen im Zuge der Zeitenwende

- die Forschung zum Erkennen, Verstehen und Bekämpfen von Desinformationskampagnen intensivieren, um das Vertrauen in die Berichterstattung der seriösen Medien zu erhalten;
- mit dem Forschungsnetzwerk Anonymisierung eine sichere und die Privatsphäre schonende Datennutzung fördern;
- Datenschutz als Innovationstreiber verstehen und dies unter anderem über Start-ups befördern;
- mit Kommunikationsinitiativen und Informationsangeboten das Bewusstsein für Cyberbedrohungen stärken, insbesondere auch in der jungen Bevölkerung (wie mit der aktuellen Initiative „Sichere die digitale Zukunft!“);
- Daten-, Digital- und Medienkompetenz entlang der gesamten Bildungsbiografie stärken.

Impressum

Herausgeber
Bundesministerium
für Bildung und Forschung (BMBF)
Referat Vernetzung und Sicherheit digitaler Systeme
53170 Bonn

Stand
Dezember 2022

Text
BMBF, VDI/VDE Innovation + Technik GmbH

Gestaltung
VDI/VDE Innovation + Technik GmbH

Bildnachweis
Titel: Adobestock/Gorodenkoff

@BMBF_Bund
@bmbf.de
@bmbf.bund

bmbf.de