TECHNOLOGISCHE SOUVERÄNITÄT: VORAUSSETZUNG FÜR DIE CYBERSICHERHEIT

Impulspapier | Dezember 2019

Zusammenfassung

Die fortschreitende Digitalisierung aller Lebensbereiche erhöht das Risiko einer wachsenden technologischen Abhängigkeit. Die technologische Souveränität, also die Fähigkeit, selbstbestimmt und unabhängig agieren zu können, ist dadurch massiv gefährdet. Jedoch ist es ökonomisch nicht leistbar, alle erforderlichen Informations- und Kommunikationstechnologien (IKT) in Deutschland oder in der EU selber zu entwickeln. Deutschland wird weiterhin auf nicht-europäische IKT-Produkte und -Dienstleistungen angewiesen bleiben. Das Ziel muss es deshalb sein, durch ein abgestimmtes Maßnahmenbündel, das zentrale Technologiefelder abdeckt, die **technologische Souveränität zu erhöhen** und damit auch ein **hohes Maß an Cybersicherheit** zu erreichen. Erforderlich sind folgende Maßnahmen:

- Ein gezielter **Kompetenzausbau in Schlüsselbereichen**, um mögliche Risiken beurteilen zu können, die durch Abhängigkeiten entstehen (in Bezug auf Hersteller, Herkunftsland, Einsatz, Wechselwirkungen).
- Für kritische Bereiche müssen **alternative Schlüsseltechnologien entwickelt** bzw. **existierende Technologien erweitert** werden, um Abhängigkeiten zu reduzieren und den Einsatz existierender Technologien beherrschbar zu gestalten.
- Über **Regulierungen** müssen Vorgaben für den Einsatz von Technologien mit hohem Risikopotenzial für sicherheitskritische Bereiche gemacht und es müssen **Prüfverfahren und -techniken für eine kontinuierliche Zertifizierung** geschaffen werden, um einen beherrschbaren Einsatz sicherheitskritischer Technologien zu ermöglichen.
- Zukunftstechnologien müssen **frühzeitig gestaltet** werden, um Erfahrungen in internationale Standards einfließen zu lassen und die neuen Technologien von Anfang an zu beherrschen.

Das Papier identifiziert Schlüsseltechnologien, die für die Cybersicherheit essenziell sind, und leitet Handlungsempfehlungen für die Politik ab. Um die Cybersicherheit substanziell zu stärken und die technologische Souveränität nachhaltig zu verbessern und damit mittel- und insbesondere langfristig „vor die Lage zu kommen“, empfiehlt der Beirat mit hoher Priorität folgende fünf Themenfelder zu adressieren.

1. **Elektronische Hardware entwickeln:** Vertrauenswürdige Hardwarekomponenten werden für alle sicherheitsrelevanten Anwendungen benötigt. Unbekannte Funktionen, wie Hintertüren, müssen weitestmöglich ausgeschlossen werden können. Der Markt wird jedoch von nicht-europäischen Herstellern dominiert. Alternativen, die aus vertrauenswürdiger Quelle stammen und nachvollziehbare, überprüfbare Sicherheitseigenschaften aufweisen, fehlen. Solche Alternativen können mit ökonomisch vertretbarem Aufwand als Open-Source-Hardware basierend auf RISC-V entwickelt werden. Zusammen mit Technologien zur Absicherung von Entwicklungs-, Liefer- und Fertigungsketten kann eine nachhaltige Verbesserung der Cybersicherheit erreicht werden.
2. **Daten sicher bereitstellen:** Die Gefährdung der Verfügbarkeit der Daten in fremdkontrollierten Cloud-Infrastrukturen, und der damit einhergehende Kontrollverlust, stellt eine massive Bedrohung der Cybersicherheit dar. Deutschland kann keine komplett neue, eigene Infrastruktur schaffen, sondern sollte Technologien zur Ergänzung existierender Infrastrukturen entwickeln, damit ein offenes und vertrauenswürdiges Ökosystem zum sicheren Datenaustausch entsteht, basierend auf zertifizierten Komponenten.
3. **Netzkomponenten beherrschbar einsetzen:** Der Markt für 5G-Netzkomponenten wird von nicht-europäischen Anbietern dominiert. 5G-Komponenten dringen tief in Infrastrukturen von Organisationen vor. Daher sind diese Infrastrukturen in hohem Maß von der Verfügbarkeit und Vertrauenswürdigkeit der genutzten Technologie abhängig. Um den Technikeinsatz in sicherheitskritischen Bereichen beherrschbar zu machen, ist deren Einsatz zu regulieren, z. B. ist durch Zertifizierungen und High-Tech-Prüf- und -Evaluierungsmethoden die Einhaltung von Sicherheitsvorgaben kontinuierlich, auch während der Technologienutzung, zu überprüfen.
4. **Systeme der Künstlichen Intelligenz (KI) vertrauenswürdig gestalten:** Unternehmerische Entscheidungen basieren zunehmend auf Ergebnissen von KI-Systemen. Die Abhängigkeit von der Korrektheit und Vertrauenswürdigkeit dieser Systeme wächst rasant. Mit Zertifizierungen unterschiedlicher KI-Kritikalitätsstufen, KI-Prüfmethoden und technischen Richtlinien kann ein hoher Sicherheitsstandard für vertrauenswürdige KI geschaffen werden.
5. **Zukunftstechnologien gestalten:** Jetzt muss in Forschung und Entwicklung für Technologien wie 6G und Quantencomputing investiert werden, um eigene deutsche bzw. europäische Technologien am Markt zu platzieren und Standards von Beginn an mitzubestimmen.

1 Ausgangslage

Aufgrund der zunehmenden Durchdringung und Vernetzung sämtlicher Lebensbereiche durch die Digitalisierung erhöht sich das Risiko wachsender technologischer Abhängigkeit. Geräte im Internet of Things (IoT), Netzwerkkomponenten, (Edge-)Cloud-Infrastrukturen oder aber auch KI-Systeme werden zentrale Bestandteile von IT-Infrastrukturen in allen Bereichen, insbesondere auch in kritischen Infrastrukturen sein. Damit einhergehend wird die technologische Abhängigkeit von den entsprechenden Technologieanbietern und -betreibern weiter rasant steigen. Gleichzeitig ist klar, dass Deutschland und Europa weder wirtschaftlich noch ressourcentechnisch in der Lage sind, alle IT-Technologien, die für die vielfältigen Anwendungsbereiche notwendig sind, wie für IoT, Smart Home, Smart City, Gesundheitsversorgung der Zukunft, smarte Landwirtschaft oder auch Produktion der Zukunft, neu zu entwickeln. Deutschland ist deshalb auf die Nutzung und den Import von nicht-europäischen IT-Komponenten, -Produkten und -Dienstleistungen, sowie auf die Zusammenarbeit mit ausländischen Infrastrukturbetreibern essenziell angewiesen. Die Sicherheit der eingesetzten Informationstechnik ist zugleich von einer überragenden Bedeutung für Staat, Wirtschaft und Gesellschaft, um die Risiken zu minimieren, die aus einem Ausfall IT-basierter Prozesse oder Angriffen auf die Vertraulichkeit und Integrität informationstechnischer Systeme resultieren.

Um bei dieser Ausgangssituation die **technologische Souveränität** zu verbessern und die Cybersicherheit nachhaltig zu erhöhen, ist ein abgestimmtes Bündel an Maßnahmen erforderlich. Die technologische Souveränität eines Staates wird hier als seine Selbstbestimmtheit und Unabhängigkeit von einer Einflussnahme durch Dritte verstanden. Technologische Souveränität erfordert die Fähigkeit, zu beurteilen, ob spezifische Technologien die Souveränität substanziell beeinträchtigen könnten und welche Alternativen nutzbar sind. Sie erfordert Kompetenzen, um verfügbare Technologien zu beherrschen, diese so einzusetzen bzw. ggf. so zu erweitern, dass Abhängigkeiten und Verwundbarkeiten kontrollierbar werden. Souveränität erfordert aber auch die Bereitstellung von Alternativen. In Schlüsselbereichen müssen deshalb gezielt Technologiealternativen entwickelt und verfügbar gemacht werden. Zukunftstechnologien müssen frühzeitig aufgegriffen und proaktiv gestaltet werden. Souveränität erfordert aber auch Regulierungen, um Rahmenbedingungen für den Einsatz und die Nutzung von Technologien in sensitiven, sicherheitskritischen Bereichen zu definieren.

Das Papier identifiziert fünf technologische Schlüsselbereiche, die für die Cybersicherheit essenziell sind, und leitet im abschließenden Abschnitt Handlungsempfehlungen für die Politik ab.

2 Souveränität bei kritischen Hardwarekomponenten

Alle informationsverarbeitenden Systeme, die in den verschiedensten Anwendungsbereichen zum Einsatz kommen, wie Industrie 4.0, IoT, Smart Health oder Smart Home, bestehen aus elektronischen Hardwarekomponenten und Software. Schwachstellen in der Hardware können jegliche Software-Sicherheitsmaßnahmen außer Kraft setzen. In Geräte eingebettete, leistungsstarke Prozessoren führen kritische Berechnungen, Sicherheitsfunktionen und Steuerungsaufgaben lokal durch und treffen autonom Entscheidungen. Sowohl zur Erfüllung der Safety-Anforderungen als auch zur Erzielung ausreichender Informationssicherheit ist es notwendig, unbekannte Funktionen, wie Hintertüren, Trojaner oder sonstiges undokumentiertes Verhalten im System weitestmöglich auszuschließen. Es wird nie vollständig ausgeschlossen werden können, dass neue Phänomene, wie in den letzten Jahren die Instabilität von DRAM-Speichern (z. B. Rowhammer) oder Cache-Seitenkanäle (z. B. Meltdown und Spectre) für Angriffe ausgenutzt werden. Ein den Sicherheitsanforderungen besser angepasster Systementwurf, der nicht gezwungen ist, Standardkomponenten einzusetzen, würde solche Angriffe aber deutlich unwahrscheinlicher machen. So sind beispielsweise Systeme mit separierten Speichern und CPUs nicht anfällig für diese Angriffe.

Vertrauen und Integrität kann nur erreicht werden, wenn alle Teile dieser Systeme – insbesondere die Hardwarekomponenten (CPUs, Systems-on-Chips (SoCs), Sensoren, Speicher) als Basis aller darauf aufbauenden Softwarekomponenten – vertrauenswürdig sind. Durch die Marktdominanz nichteuropäischer Hersteller fehlen heute jedoch Alternativen, die aus vertrauenswürdiger Quelle stammen und nachvollziehbare, überprüfbare Sicherheitseigenschaften aufweisen. So entwickeln neben Google (Titan) auch Amazon (Nitro) und Microsoft (Cerberus) eigene Chips als Cloud-Sicherheitsanker. Sichere Hardware zusammen mit Technologien zur Absicherung von Entwicklungs-, Liefer- und Fertigungsketten gehören somit zu den Schlüsseltechnologien, die für die technologische Souveränität und die Cybersicherheit in Deutschland essenziell sind. Erforderlich sind zudem Fähigkeiten, um den Funktionsumfang der Hardware vorab festzulegen, die Umsetzung in Hardwarebestandteile zu steuern und in den fertigen Produkten nachprüfen zu können.

Maßnahmen zur Erhöhung der technologischen Souveränität

Nationale Sicherheitscontroller, die aufsetzend auf existierender Hardware in auditierten Entwicklungsumgebungen vertrauenswürdig entwickelt und mit etablierten Verfahren zertifiziert werden können, stellen bereits heute eine Alternative für spezifische Anwendungsbereiche mit hohen Si-

cherheitsanforderungen dar. In vielen Anwendungen ist es jedoch aus wirtschaftlichen, oder produktbedingten Gründen nicht möglich, dedizierte Sicherheitscontroller einzusetzen, zum Beispiel wenn kein Platz für einen zusätzlichen Chip vorgesehen ist. Außerdem wird üblicherweise die Funktionalität der Hardwarekomponente nicht in den Sicherheitscontroller integriert, sodass weitere Komponenten wie Prozessoren notwendig sind, um wichtige Systemfunktionen zu erfüllen.

Es sind neue Ansätze erforderlich, um mit vertrauenswürdiger Hardware ressourcenschwache Sensoren und Edge-Devices so abzusichern, dass eine sichere, lokale Datenvorverarbeitung „at the edge" erfolgen kann. Die Hardwarekomponenten müssen nachweislich hohe Anforderungen an Datensicherheit und Privatheit erfüllen und mit ökonomisch vertretbarem Aufwand auch in kleiner Stückzahl, zugeschnitten auf spezifische Nutzeranforderungen, gefertigt werden können. Um zu solchen technologischen Alternativen zu kommen, werden neue integrierte Entwicklungsinfrastrukturen benötigt, damit ein Ökosystem mit zertifizierten, vertrauenswürdigen Hardwareblöcken und -chips entstehen kann.

Um die Forderung nach Offenheit, Transparenz und Nachvollziehbarkeit der Entwicklung zu erfüllen, sollten – analog zu Open-Source-Software-Lösungen wie Linux – Hardwarekomponenten als Open Source auf Basis von RISC-V, entwickelt werden. Das Interesse und die Entwicklungsressourcen um die Prozessorarchitektur RISC-V nehmen weltweit aktuell in hohem Maße zu. Schon mittelfristig kann man davon ausgehen, dass für Mikrocontroller reife offene Hardwaredesigns vorliegen werden. Ziel sollte es sein, Entwicklungs-und Testwerkzeuge bereitzustellen, um damit in der Lage zu sein, die Entstehung des Gesamtprodukts über alle seine Entwicklungs- und Produktionsschritte hinweg zu kontrollieren und schlussendlich das Gesamtprodukt als vertrauenswürdig zu zertifizieren. Google hat im November 2019 bereits eine eigene OpenTitan-Entwicklung auf Basis von RISC-V angekündigt[1]. Es muss deshalb mit hohem Nachdruck an Alternativen geforscht und entwickelt werden. Die Offenheit der entsprechenden Designs ermöglicht eine weltweit verteilte Entwicklung und Weiterentwicklung sowie die Prüfung durch eine Vielzahl von Akteuren, um Schwachstellen frühzeitig aufzudecken und die Cybersicherheit zu erhöhen. Cybersichere Systeme könnten so in Zukunft auf Open-Source-Kryptografie-Bibliotheken, -Betriebssystemen und auch -Hardware aufsetzen.

3 Souveränität über Dateninfrastrukturen

Im Bereich der Cloud-Plattformen wird der Markt von nicht-europäischen Akteuren dominiert, den sogenannten Hyperscalern. Zunehmend werden auch sicherheitskritische Abläufe und die dafür erforderlichen Daten in solche Cloud-Plattformen ausgelagert (z. B. Microsoft Office 365). Dies betrifft hoheitliche Prozesse, wie z. B. Polizeidaten, ebenso wie unternehmenskritische Daten und Prozesse, z. B. aus Logistik, Entwicklung und Produktion. Die Verfügbarkeit der Daten in fremdkontrollierten Cloud-Infrastrukturen, der Verlust der Kontrolle über eine mögliche Weitergabe der Daten, u. a. an staatliche Institutionen (z. B. im Zuge des US-amerikanischen Cloud Act und des US Patriot Act), stellt eine massive Bedrohung der Cybersicherheit dar. Es entstehen hohe Abhängigkeiten, da eine Datenmigration auf andere Infrastrukturen schwierig bis unmöglich ist (Lock-in-Effekt), was die Handlungsfreiheit substanziell einschränkt. Hier entstehen somit absehbar für die deutsche Industrie Abhängigkeiten mit dem Risiko, dass durch eine mangelnde Datensouveränität, also der fehlenden Fähigkeit natürlicher und juristischer Personen zur Selbstbestimmung über ihre Daten, die Innovations- und Wettbewerbsfähigkeit der deutschen Wirtschaft massiv beeinträchtigt ist. Deutschland und Europa kann diesen bereits etablierten Hyperscalern aber keine von Grund auf neue, eigene Infrastruktur entgegenstellen.

Maßnahmen zur Erhöhung der technologischen Souveränität

Mit der im Oktober 2019 offiziell gestarteten, industriegetriebenen Initiative GAIA-X sollen Technologien entwickelt werden, um virtuelle Hyperscaler als Alternative zu den physischen Hyperscalern zu schaffen. Virtuelle Hyperscaler sind Netzwerke aus verschiedenen Clouds. Über die zu entwickelnde GAIA-X-Technologie sollen am Markt befindliche und auch neue Cloud-Anbieter in das Netzwerk sicher und zertifiziert eingebunden werden können. Es soll ein offenes und vertrauenswürdiges Ökosystem zum einfachen und sicheren Datenaustausch entstehen, mit Möglichkeiten, auch Applikationen und Funktionen von Drittanbietern zu nutzen. Es soll auf die internationale Standardisierung Einfluss genommen werden, um eine leichte Datenmigration zu ermöglichen und dem Lock-in-Effekt entgegenzuwirken. Mit diesem Ansatz werden bestehende Technologien kontrolliert nutzbar gemacht, indem über Zertifizierung die Einhaltung von Qualitätsvorgaben nachgewiesen werden muss. Die sichere Datenbereitstellung ist z. B. unabdingbar für den erfolgreichen Einsatz von KI in der Fläche.

1 Vgl. https://www.heise.de/newsticker/meldung/OpenTitan-Googles-legt-Sicherheitschip-mit-RISC-V-Technik-offen-4573734.html

4 Souveränität bei sicherheitskritischen Netzkomponenten

Wie bereits einleitend gesagt, werden Deutschland und Europa es mit eigener Kraft nicht schaffen, in allen Schlüsseltechnologien, eigene Technologiealternativen zu entwickeln und wirtschaftlich erfolgreich am Markt gegen die internationalen Wettbewerber zu positionieren. Ein prägnantes Beispiel sind die Netzkomponenten, die insbesondere für den 5G-Ausbau maßgeblich von nicht-europäischen Anbietern wie Huawei und Cisco bereitgestellt werden. Mit Nokia und Ericsson stehen europäische Alternativen zur Verfügung, die aber nur ein vergleichsweise kleines Marktsegment abdecken. Sicherheitskritische Netzkomponenten werden zukünftig auch sehr tief in bestehende Infrastrukturen in Unternehmen integriert werden. Dies ist die Folge des so genannten Edge-Computings in 5G, bei dem die Datenverarbeitung in räumlicher Nähe („at the edge") der Datenquellen erfolgt, zum Beispiel in Unternehmen. Insbesondere durch die Möglichkeit, 5G-Campusnetze zu errichten, zum Beispiel auf einem Fabrikgelände oder in einem Stadtgebiet, entstehen private, abgeschottete 5G-Netze, die auf Netzkomponenten basieren, über die sehr viel unternehmenskritisches Datenvolumen verarbeitet werden wird. Daraus ergibt sich eine sehr hohe Abhängigkeit von den jeweiligen Technologieanbietern, da der zuverlässige und sichere Betrieb der unternehmerischen und staatlichen Infrastrukturen unmittelbar von der Verfügbarkeit und Vertrauenswürdigkeit[2] der genutzten Technologie abhängt. Ende-zu-Ende-Verschlüsselung ist hilfreich, um manche der möglicherweise versteckt implantierten Hintertüren (Backdoors) wirkungslos zu machen, aber reicht als Maßnahme nicht aus.

Maßnahmen zur Erhöhung der technologischen Souveränität

Zur Verbesserung der technologischen Souveränität sind regulatorische Vorgaben und Zertifizierungen für sicherheitskritische Bereiche erforderlich. Um den Einsatz kritischer Netzkomponenten beherrschbar zu gestalten, muss die Kritikalität von Komponenten bewertet werden. Hierfür sind technische Prüf-, Evaluierungs- und Zertifizierungslabore aus- und aufzubauen.

Die deutsche Forschungslandschaft verfügt über wissenschaftlich hervorragende Standorte wie Bochum, Darmstadt, Karlsruhe, Saarbrücken und München, an denen bereits seit Jahren Analysetechniken und Prüfmethoden für die Sicherheit von Komponenten entwickelt werden, insbesondere auch von Hardwarekomponenten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet seit langem eng mit den jeweiligen Gruppen zusammen. Der erreichte Stand reicht jedoch nicht aus, um die oben skizzierten Herausforderungen zu meistern. Als Ergänzung der Forschungslabore müssen unabhängige Prüf- und Evaluierungslabore für sicherheitskritische Technologien etabliert und mit Technologien ausgestattet werden, die dem neuesten Stand von Wissenschaft und Technik entsprechen – so wie sie in den Forschungslaboren erprobt werden. Die neuen Labore müssen wirtschaftlich unabhängig agieren können, um unabhängig von Industrieinteressen und möglicher Einflussnahme tiefgehende Sicherheitsevaluationen nach dem neuesten Stand der Wissenschaft und Technik durchzuführen.

Eine statische Evaluation, wie sie heute üblich ist, wird den Herausforderungen zukünftiger Technologiegenerationen nicht länger gerecht. Es sind neue, kontinuierliche Prüfverfahren zu erforschen und zu erproben, um im Sinne von „Predictive Security" Abweichungen vom erwarteten Komponentenverhalten im operativen Betrieb frühzeitig zu erkennen. Derartige Verfahren sind dringend erforderlich, um die zurzeit etablierte technische Evaluation von Komponenten mittel- bis langfristig zu ergänzen. Auf die neuen Herausforderungen für die Cybersicherheit, die sich aus der hohen Dynamik der Systeme ergeben, sind weder Unternehmen noch die öffentliche Hand ausreichend vorbereitet. Neben der erforderlichen Technologie, die noch weiter erforscht und erprobt werden muss, fehlen auch fachkundige Mitarbeiter. Deshalb muss sowohl in die Aus- und Weiterbildung investiert werden als auch in die Entwicklung von nicht umgehbaren, kontinuierlichen Test- und Evaluierungsverfahren. Deutschland muss sich hierzu aktiv in die Zertifizierung einbringen und Zertifizierungsstandards aktiv mitgestalten.

5 Souveränität bei kritischen KI-Systemen

Maschinelle Lernverfahren und Systeme der Künstlichen Intelligenz (KI) werden bereits heute in zahlreichen IT-Infrastrukturen als zentraler Baustein zur Analyse, Prognose und Steuerung eingesetzt. Autonomes Fahren, Gesundheitsversorgung, Energieversorgung oder auch Produktion der Zukunft sind ohne KI nicht mehr denkbar bzw. nicht mehr zukunftsfähig. Die Vertrauenswürdigkeit derartiger Systeme ist für Unternehmen aller Branchen, aber auch für staatliche Institutionen von höchster Wichtigkeit. Unternehmerische Entscheidungen werden zunehmend auf Ergebnissen von KI-Systemen basieren; es entsteht eine gefährliche Abhängigkeit, da die Ergebnisse von maschinellen Lernverfahren meist nicht nachvollziehbar sind und auch die Qualität der Daten, die zum Anlernen genutzt werden, für die Nutzenden

2 Hier ist z. B. an den sogenannten „Kill Switch" zu denken: d.h. der Hersteller hat eine Maßnahme integriert, um sozusagen auf Knopfdruck die Funktionalität, wie Netzwerkkommunikation für den Kunden, abzuschalten.

nicht prüfbar ist. Diese Wissenslücke zusammen mit der zunehmenden Abhängigkeit stellt unabhängiges unternehmerisches oder staatliches Handeln und Entscheidungsfreiheit in Frage. Dies gefährdet massiv die technologische Souveränität deutscher Unternehmen und staatlicher Organe.

Aufgrund ihres Einsatzes in einer Vielzahl sicherheitskritischer Bereiche werden verlässliche, zertifizierte KI-Systeme benötigt. Derzeit gibt es jedoch noch keine Zertifizierungsmethoden und Prüfverfahren für komplexe KI-Verfahren und -Systeme. Diejenigen, die hierfür die Standards entwickeln, können Einfluss darauf nehmen, welche Produkte sich am Markt mittel- bis langfristig durchsetzen werden. Es ist eine Chance für den Qualitätsstandort Deutschland, in dieser Frage eine Vorreiterrolle einzunehmen und zeitnah die erforderlichen Standards mit zu erarbeiten.

Maßnahmen zur Erhöhung der technologischen Souveränität

Die Umsetzung einer KI-Zertifizierung ist äußerst anspruchsvoll und zeitlich herausfordernd. Dies ist sowohl in der Breite der Thematik als auch in der Geschwindigkeit der technologischen Entwicklungen begründet. Deshalb sind Einzelmaßnahmen zum Aufbau einer KI-Zertifizierung nicht zielführend: Es bedarf eines koordinierten Ansatzes für die Entwicklung einer KI-Zertifizierung. Grundlage für eine Zertifizierung ist die Übersetzung der Empfehlungen von Expertenkommissionen in konkrete Anforderungen, die von einer technischen Prüforganisation überprüfbar sind. Für KI-Systeme fehlt bereits das Sicherheitsfundament, nämlich allgemein anerkannte Sicherheitsziele – sowohl hinsichtlich Betriebs- als auch Angriffssicherheit). Diese Ziele gilt es zu entwickeln. Festzulegen sind unterschiedliche Kritikalitäts- und Zertifizierungsstufen für KI-Algorithmen sowie Prüfkataloge und -verfahren, wie auch technische Richtlinien für die Entwicklung resilienter KI-Produkte. Um branchenspezifischen, regulatorischen Anforderungen Rechnung zu tragen, sind zudem branchenspezifische Kataloge und technische Prüfverfahren erforderlich.

6 Souveränität bei Zukunftstechnologien

Technologische Souveränität eines Staates zeigt sich auch darin, frühzeitig die Chancen und Gefährdungspotenziale zukünftiger Technologien zu erkennen und rechtzeitig Maßnahmen zur Vorsorge und zum Minimieren möglicher Risiken, insbesondere Cybersicherheitsrisiken, in die Wege zu leiten. Die nächste Generation des Mobilfunks, 6G, und auch das Quantencomputing (QC) sowie die auf Prinzipien der Quantenphysik basierende, sichere Kommunikation (Quantum Key Distribution, QKD) sind Beispiele für solche Zukunftstechnologien.

Durch den rasanten Fortschritt in der Entwicklung von Quantenprozessoren rücken die Anwendungen von Quantenalgorithmen in Sichtweite von wirtschaftlicher Relevanz. QC bietet neue Möglichkeiten für Problemstellungen, die mit heutigen Hochleistungsrechnern bisher als unlösbar gelten. Bereits heute ermöglichen Firmen wie IBM und Google einen cloudbasierten Zugang zu den neuesten Quantencomputern, sodass deren Nutzung bereits mit überschaubarem Ressourcenaufwand möglich ist. Für die Cybersicherheit werden die neuen Berechnungsparadigmen dramatische Konsequenzen haben, da durch hinreichend große Quantencomputer nahezu alle der heute eingesetzten Public-Key-Verschlüsselungsverfahren (Signatur-, Schlüsselaustausch- und asymmetrische Verschlüsselungsverfahren) unsicher werden. Dies betrifft unter anderem auch die meisten aktuell verwendeten kryptografisch abgesicherten Internetverbindungen (z. B. über HTTPS oder Virtual Private Network (VPN)). Die NSA warnte bereits 2015 vor den Auswirkungen von Quantencomputern und hat eine Migration hin zu quantencomputerresistenten Verfahren eingeleitet; das US-amerikanische National Institute of Standards (NIST) hat im Jahr 2017 einen Standardisierungsprozess für quantencomputerresistente Verfahren gestartet. Das BMBF hat frühzeitig reagiert und eine Forschungsagenda zur Entwicklung von Post-Quanten-Kryptografie gestartet. Es werden u. a. quantencomputerresistente Signaturverfahren erforscht, die für einen sicheren Update-Prozess und für den Aufbau einer sicheren Kommunikation zwischen unbekannten Partnern, wie sie bei IoT-Verbindungen üblich ist, benötigt werden.

Maßnahmen zur Erhöhung der technologischen Souveränität

Es ist unabdingbar, dass in Deutschland Fähigkeiten zur Evaluation und Analyse von Post-Quanten-Kryptoverfahren weiter ausgebaut werden. Es handelt sich dabei um Verfahren, die quantencomputer-resistent sind und langzeitsicher auf heutigen Architekturen eingesetzt werden können. Ebenso ist der Kompetenz- und Technologieausbau bei Quantenkryptoverfahren zu forcieren, also bei Verfahren, die auf Effekten der Quantenphysik basieren und einen hochsicheren Austausch von kryptografischen Schlüsseln ermöglichen. Dies ist eine zentrale Voraussetzung für hochsichere Systeme. Bereits jetzt müssen Migrationsstrategien für einen einfachen Übergang auf Post-Quanten-Kryptoverfahren entwickelt und erprobt werden. Quantencomputer ermöglichen Berechnungen, die mit klassischen Computern nicht umsetzbar sind. Aktuelle Forschungsarbeiten deuten zudem auch darauf hin, dass Quantencomputer bestimmte Teilprobleme im Umfeld des maschinellen Lernens effizienter lösen könnten als klassische Rechner. Noch weitestgehend unerforscht sind die möglichen Risiken, die sich aus der Nutzung des Quantencomputers für Maschinelle Lernverfahren (ML)

ergeben, um damit gänzlich neue Klassen von Attacken auf die Cybersicherheit zu ermöglichen. Neueste Forschungsergebnisse verdeutlichen, dass auch hier ein hoher Forschungsbedarf besteht. Deutschland muss hier Kompetenzen zur Analyse von ML auf Quantencomputern aufbauen, um frühzeitig Anforderungen an die Entwicklung QC-resilienter ML abzuleiten und derartige Verfahren zu entwickeln und zu erproben.

Derzeit konzentriert sich die Forschung im Bereich der Software für QC weitestgehend auf die Entwicklung von Quantenalgorithmen, die das Potenzial von Quantencomputern nutzt. Absehbar werden jedoch große Organisationen, insbesondere auch aus dem Umfeld kritischer Infrastrukturen, wie die Energieversorger oder Banken, vor der Frage stehen, wie die Möglichkeiten des QC mit klassischen Cloud-Infrastrukturen sicher gekoppelt werden können, sodass sowohl die Datensouveränität bei der Nutzung der QC-Technologien erhalten, als auch wertvolles Wissen (IP), das in den QC-Algorithmen steckt, geschützt bleibt. Deutschland könnte sich hier einen Vorsprung erarbeiten, wenn gezielt in die Forschung und Entwicklung von sicherer QC-ready-Betriebssoftware investiert würde, sodass eine sichere Einbindung von Quantencomputern in hybride Betriebsmodelle, u. a. bei Cloud-Anbindungen, ermöglicht wird.

Handlungsempfehlungen für die Politik

Die nachfolgenden Handlungsempfehlungen zielen darauf ab, sowohl kurz- als auch mittel- und langfristig die technologische Souveränität in Deutschland und damit nachhaltig die Lage der Cybersicherheit zu verbessern. Die Handlungsempfehlungen sind deshalb als direkt anzugehende Maßnahmenempfehlungen zu verstehen, deren Wirkungen sich aber unterschiedlich schnell einstellen werden. Bereits kurz- bis mittelfristige Wirkungen wird man durch die Bereitstellung sicherer Dateninfrastrukturen und die Zertifizierung kritischer Netzkomponenten erzielen können. Ebenfalls kurz- bis mittelfristig wirksame Effekte sind zu erwarten durch erste Schritte bei der KI-Zertifizierung und bei der Entwicklung sicherer Hardwarealternativen basierend auf Open-Source-Hardware. Auch wenn Zukunftstechnologien einen langfristigen Wirkungshorizont haben, sind kurz- bis mittelfristige Wirkungen bei entsprechendem politischem Handeln zu erzielen. Zu nennen ist hier beispielsweise die frühzeitige Erarbeitung von Migrationspfaden, um Anwendungen, deren Daten über 30, 50 oder 100 Jahre aufbewahrt werden müssen, bereits heute QC-resilient abzusichern. Die Politik muss mit einer gezielten Industriepolitik nationale Forschungs- und Entwicklungsanstrengungen transferorientiert fördern und nationale Cybersicherheitstechnologien unterstützen. Dafür sind ggf. vorhandene Rahmenbedingungen anzupassen, damit nationale Interessen gewahrt bleiben.

Souveränität bei vertrauenswürdiger Hardware

Mit der Forschungsfabrik Mikroelektronik wird eine innovative Chipfertigung am Standort Deutschland bereits ermöglicht. Die Politik sollte konsequenterweise die nächsten Schritte gehen und neben der Chipfertigung auch die erforderlichen Maßnahmen in die Wege leiten, so dass technisches Know-how und technische Umgebungen aufgebaut werden, damit vertrauenswürdige Chips am Standort Deutschland individualisiert und auch in geringen Stückzahlen mit ökonomisch vertretbarem Aufwand gefertigt werden können. Hierzu könnten beispielsweise Shared-Reticle-Programme etabliert werden, wie sie aus dem universitären Umfeld mit Europractice bekannt sind. Mit einem solchen Ansatz können die in der Herstellung sehr teuren Masken, die für die Fertigung anwendungsspezifischer integrierter Chips (ASICs) benötigt werden, gleichzeitig für Designs von unterschiedlichen Unternehmen verwendet werden, so dass die Maskenproduktion auch für kleine Stückzahlen rentabel ist. Das Projekt Europractice hat gezeigt, dass eine Kostenreduktion auf 5 bis 10 Prozent möglich ist. Beispiele für solche Chips können sichere Mikrocontroller sein oder auch ASICs mit dediziertem integriertem Vertrauensanker (Secure Element) auf Basis von Open-Source-Hardware. Um vertrauenswürdige Hardwarekomponenten für die verschiedensten sicherheitskritischen Anwendungsbereiche einfach nutzbar zu machen, muss zudem in die Entwicklung von vertrauenswürdigen, auf Open Source basierten Betriebssystemen für IoT-Systeme investiert werden.

Open-Source-Hardware wie RISC-V befindet sich noch in einer Frühphase der Entwicklung. Sie ist aber ein zentrales Instrument, nicht nur um technologische Alternativen zu entwickeln, sondern auch um mögliche Backdoors oder Schwachstellen, wie sie mit Spectre und Meltdown bekannt geworden sind, im Rahmen von Evaluationen des Chipdesigns zu erkennen. Die Politik sollte deshalb massiv in die Entwicklung von RISC-V investieren. In niederen Leistungsklassen können solche offenen Designs schon mittelfristig für Unternehmen nützlich sein, um vertrauenswürdige Schaltkreise für IoT-Geräte, Medizingeräte etc. zu fertigen. Die Entwicklung wird in diesem Bereich über die Jahre weiter fortschreiten und es ist davon auszugehen, dass auch leistungsfähigere Prozessoren auf Basis offener Designs möglich sein werden. Es sollte zudem die Entwicklung technischer Methoden gefördert werden, die dazu dienen, elektronische Komponenten automatisiert zu prüfen. Die Förderung eines Ökosystems rund um die Open-Source-Hardware-Architektur RISC-V mit zertifizierten vertrauenswürdigen Hardwarekomponenten könnte eine erfolgreiche Initiative für vertrauenswürdige Hardware darstellen.

Die Politik sollte zudem regulatorische Vorgaben für den Einsatz zertifizierter, vertrauenswürdiger Hardware und eingebetteter Systemkomponenten in sicherheitskritischen Infrastrukturen machen.

Souveränität bei Dateninfrastrukturen
Die Politik sollte den Aufbau von virtuellen Hyperscalern mit GAIA-X-Technologien substantiell und nachhaltig unterstützen. Ggf. ist es auch sinnvoll, die Phase zwischen Inbetriebnahme und Profitabilität durch staatliche Maßnahmen zu unterstützen, um das sogenannte „Tal des Todes" zu überwinden, und auf die Entwicklung und Einhaltung von Standards und Zertifizierungen einzuwirken. Die so entstehenden vertrauenswürdigen Hyperscaler sollten von der öffentlichen Hand auch selber genutzt werden, u. a. zum Betrieb öffentlicher Dienstleistungen in einer Cloud-Umgebung unter Berücksichtigung der Anforderungen an Sicherheit, Verfügbarkeit und Datensouveränität.

Zur Umsetzung der Ziele von GAIA-X sollen so weit wie möglich vorhandene oder in Entwicklung befindliche Technologien einbezogen werden. Dazu gehören die Referenzimplementierungen, die bereits in dem Vorhaben IDS (International Data Space) der Fraunhofer-Gesellschaft, unterstützt von Industriepartnern aus dem Industrieverein IDSA, umgesetzt wurden. Die Arbeiten zum IDS wurden durch das BMBF und das BMWi bereits substanziell unterstützt, sodass es sinnvoll ist, die hier bereits getätigten Investitionen zu sichern und durch gezielte Erweiterungen in GAIA-X-Lösungen zu überführen. Mit GAIA-X könnte eine vertrauenswürdige, sichere Dateninfrastruktur etabliert werden, die Abhängigkeiten reduziert. Daten, als Grundlage aller Cybersicherheitsaktivitäten, können damit kontrolliert, sicher und vertrauenswürdig dezentral verwaltet sowie nachvollziehbar und datenschutzkonform gemeinsam genutzt werden. Eine solche sichere Datenbereitstellung ist essentielle Voraussetzung für eine flächendeckende Nutzung sicherer KI-Verfahren in allen Branchen.

Souveränität bei sicherheitskritischen Netzkomponenten
Der Aufbau und Betrieb von wirtschaftlich unabhängigen Prüf- und Evaluierungslaboren für sicherheitskritische Technologien (5G, IoT, maschinelles Lernen (s.o.), QC (s.u.)) sollte substanziell unterstützt werden. Es sollten regulatorische Vorgaben erarbeitet werden, die das Zertifizieren kritischer Technologiekomponenten für deren Nutzung in kritischen Infrastrukturen verpflichtend vorschreiben. Mit einer abgestimmten europäischen Industriepolitik könnten technologische Alternativen im europäischen Binnenmarkt etabliert werden.

Souveränität bei KI-Systemen
Der Aufbau einer KI-Zertifizierungsinfrastruktur mit Methoden, Werkzeugen und Prüfverfahren zur Zertifizierung von KI-Systemen sollte substanziell unterstützt werden. Regulatorische Vorgaben für den Einsatz zertifizierter KI-Systeme in sicherheitskritischen Infrastrukturen sollten entwickelt werden.

Souveränität bei Zukunftstechnologien
Die Politik sollte gezielt in den Aufbau von Strukturen investieren, um frühzeitig und umfassend die Chancen und Risiken des QC zu erforschen und technologische Alternativen zu erproben.

Um nicht wie bei 5G den internationalen Entwicklungen hinterherzulaufen, sollte bereits jetzt massiv in die Vorentwicklung von 6G investiert werden. 6G wird voraussichtlich innerhalb der nächsten acht bis zehn Jahre auf breiter Ebene zum Einsatz kommen. Deshalb sollte diese Technologie konsequent gefördert und von Deutschland eine Vorreiterrolle eingenommen werden.

Allgemeinere politische Handlungsempfehlung
Der **Transfer von Forschungsergebnissen zur Cybersicherheit** in den Markt sollte beschleunigt werden. Förderinstrumente sollten die gesamte Kette von der Vorlaufforschung über Technologieentwicklung und den Transfer in den Markt insbesondere über Start-ups besser abbilden und gezielter unterstützen. Hersteller sicherheitskritischer Produkte sollten vor einem Aufkauf aus dem Ausland geschützt werden. Durch öffentliche Auftragsvergaben sollte ein Binnenmarkt für nationale Sicherheitsprodukte insbesondere auch für Produkte von Start-ups geschaffen werden, um deren Technologien zum Durchbruch und zur Marktakzeptanz zu verhelfen. Ausschreibungs- und Einkaufsrahmen sollten im nationalen Interesse dafür angepasst werden.

Deutschland hat mit dem **digitalen Personalausweis** erheblich in den Aufbau starker digitaler Identitäten investiert und damit eine weltweit einzigartige Technologie auf einem sehr hohen Sicherheitsniveau geschaffen. Bereits heute sind aber ausländische Marktteilnehmer wie Google und auch Apple führende Identitäts-Provider. Zu beobachten ist zudem der Trend, Smartcards auf das Smartphone zu bringen (z. B. Kreditkarten bei ApplePay). Es ist nur eine Frage der Zeit, dass auch der Personalausweis, Führerschein, die Gesundheitskarte auf mobilen Geräten gespeichert werden. D. h. hoheitliche Identitätsausweise werden auf Geräten verwaltet, die außerhalb der staatlichen Kontrolle liegen. Es muss deshalb weiter in den Ausbau der Technologien für digitale Ausweise und insbesondere in deren Nutzung investiert werden, um die staatliche Souveränität bei elektronischen Identitäten

nicht zu verlieren.

Sicherheit muss bereits bei der Entwicklung von Systemen und Anwendungen angemessen berücksichtigt werden, um sie so unempfindlich wie möglich gegen Angriffe und Störungen zu machen **(„Security by Design“)**. Ein weiteres wichtiges Element ist die herstellerseitige Auslieferung eines Produktes in einem sicheren Zustand **(„Security by Default“)**. Beides sind wesentliche Voraussetzungen für eine erfolgreiche Digitalisierung. Bewährte deutsche und europäische IT- und Sicherheitsstandards müssen in der globalisierten Welt gestärkt und erhalten werden. „Security by Design“ sowie „Security by Default“ müssen sich als Grundregeln der Informationstechnik etablieren. Hierfür sollten Anreize und eine faire Risikoverteilung für Gesellschaft, Wirtschaft und Staat geschaffen werden.

Die **Prüfung der Zuverlässigkeit, Vertrauenswürdigkeit und Korrektheit** von Softwaresystemen gewinnen als Qualitätsfaktoren unter wirtschaftlichen und gesellschaftlichen Aspekten zunehmend an Bedeutung. Das zuverlässige Funktionieren komplexer Softwaresysteme ist insbesondere für die Sicherheit von technischen Systemen von großer Relevanz. Der Erhalt und die Herstellung technologischer Souveränität in Deutschland und Europa im Bereich der Schlüsseltechnologien muss in den Fokus rücken. IT- und IT-Sicherheitsprodukte müssen kontrollierbar, transparent und nachprüfbar sein. Wir brauchen innovative und leistungsfähige Wirtschaftsunternehmen im Bereich der Informationssicherheit. Das BSI als zentrale Zertifizierungs- und Standardisierungsstelle unterstützt bei der Herstellung der erforderlichen Rahmenbedingungen. Die Vertrauenswürdigkeit von zentralen Sicherheitslösungen deutscher und europäischer Anbieter ist ein wichtiges Alleinstellungsmerkmal.

Sichere kryptografische Verfahren stellen ein unverzichtbares Element für IT-Sicherheitsmechanismen zur Wahrung von Vertraulichkeit, Integrität und Authentizität digitaler Informationen dar. Der durchgehende Einsatz sicherer Kryptografie muss in Deutschland zum Normalfall werden. Dazu gehören auch starke elektronische Identitäten. Das BSI unterstützt mit Nachdruck die Bedeutung des Erhalts der Souveränität bei elektronischen Identitäten und der Entwicklung entsprechender Schutzmaßnahmen. Die Fähigkeiten zur Evaluation und Analyse zukunftsweisender Verfahren wie Quantenkryptografie und Post-Quanten-Kryptografie müssen weiter konsequent ausgebaut werden.

Deutschland braucht mehr **Fachkräfte** auf den Gebieten der Informationstechnik und -sicherheit. Die Informations- und Cybersicherheit sind zentrale Bestandteile einer zeitgemäßen Bildungs- und Forschungspolitik. Die Themen müssen in schulischer und beruflicher Ausbildung einen angemessenen Platz bekommen. Die IT-Sicherheitsforschung muss weiter ausgebaut werden.

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Seit Oktober 2018 unterstützt die Wissenschaftliche Arbeitsgruppe den Nationalen Cyber-Sicherheitsrat. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Prof. Dr. Claudia Eckert (Hauptautorin dieses Impulspapiers), Dr. Timo Hauschild, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner