TECHNOLOGISCHE SOUVERÄNITÄT: VORAUSSETZUNG FÜR MEHR CYBERSICHERHEIT

Update zum Impulspapier vom Dezember 2019 | Juni 2022

Zusammenfassung

Im Dezember 2019 hat die Wissenschaftliche Arbeitsgruppe des Nationalen Cyber-Sicherheitsrats ein Positionspapier zur technologischen Souveränität und deren Bedeutung für die Cybersicherheit in Deutschland und Europa veröffentlicht[1]. Die Entwicklungen in wichtigen Schlüsseltechnologien, aber insbesondere auch die aktuelle geopolitische Lage verdeutlichen die Dringlichkeit des politischen Handelns. Das vorliegende Papier greift deshalb die wichtigsten Empfehlungen des Positionspapiers von 2019 auf und schärft sie nach, soweit dies durch die geänderte Lage geboten erscheint. Bei der Erstellung des Papiers 2019 standen Maßnahmenempfehlungen im Mittelpunkt, um insbesondere mittel- bis langfristig „vor die Lage zu kommen". Die Empfehlungen sollten Unternehmen, staatliche Institutionen sowie Betreiber kritischer Infrastrukturen darin unterstützen, sich effektiv und nachhaltig vor Cyberattacken zu schützen, die darauf abzielen, zu manipulieren oder Abläufe zu stören. Das ist die Voraussetzung, um europäische Werte wie Freiheit, Fairness und Offenheit nachhaltig zu gewährleisten.

Durch die aktuellen geopolitischen Entwicklungen und die erforderliche Reaktion auf einen Angriffskrieg, der auf europäischem Boden geführt wird, müssen nun vermehrt Risiken durch gezielte, staatlich gelenkte Cyberangriffe auf kritische Infrastrukturen und auf Unternehmen in Schlüsselbereichen, aber auch Fragen der gezielten Desinformation betrachtet werden. Die Frage der Resilienz von Unternehmen und Infrastrukturen in nationalen und europäischen Schlüsselbereichen gegen solche gezielten Cyberangriffe wird derzeit stark diskutiert. Die Empfehlungen im Positionspapier von 2019 haben diese relevanten Fragestellungen bereits deutlich und mit hoher Priorität adressiert. Die aktuellen Entwicklungen haben die Dringlichkeit des Handelns leider bestätigt. Um diese Handlungsdringlichkeit noch einmal zu unterstreichen, fassen wir nachfolgend die wichtigsten Empfehlungen und ihre Bedeutung in Bezug auf das Ziel der Erhöhung der Cyberresilienz noch einmal pointiert zusammen.

1 Empfehlungen aus dem Positionspapier von 2019

Das Positionspapier hat verdeutlicht, dass es nicht das politische Ziel sein kann, protektionistische Maßnahmen zu entwickeln. Es war und ist klar, dass Deutschland und Europa weder wirtschaftlich noch ressourcentechnisch in der Lage sind, alle Informations- und Kommunikationstechnologien (IKT) für vielfältige Anwendungsbereiche wie Smart City, Gesundheitsversorgung der Zukunft, Smarte Landwirtschaft oder Produktion der Zukunft mit eigenen Fähigkeiten und in eigenen Produktionsstätten nach den Prinzipien des Security by Design zu entwickeln. Deutschland wird deshalb auch in Zukunft auf die Nutzung und den Import von außereuropäischen IKT-Komponenten, -Produkten und -Dienstleistungen sowie auf die Zusammenarbeit mit außereuropäischen Betreibern von Infrastrukturen essenziell angewiesen sein. Die Sicherheit der eingesetzten Informations- und Kommunikationstechnik ist zugleich von einer überragenden Bedeutung für Staat, Wirtschaft und Gesellschaft, um die Risiken zu minimieren, die aus einem Ausfall IKT-basierter Prozesse oder Angriffen auf die Vertraulichkeit und Integrität informationstechnischer Systeme resultieren.

Die Empfehlungen des Positionspapiers von 2019 zur Stärkung der technologischen Souveränität haben nach wie vor Bestand. Sie wurden in dem Papier bereits mit unterschiedlichen Zeithorizonten dargestellt, so dass auch deren Wirkung sich unterschiedlich schnell einstellen wird. Die derzeitigen (April 2022) vielfach im öffentlichen Raum artikulierten Forderungen nach stärkerer Entkopplung von dominierenden außereuropäischen Herstellern wurde in den Empfehlungen von 2019 ebenso schon adressiert, wie die Problematik der Erhöhung der Resilienz. Nachfolgend werden die wesentlichen Empfehlungen des Positionspapiers noch einmal knapp zusammengefasst und im Licht der Entwicklungen des Jahres 2022 überprüft.

1) **Schlüsseltechnologien entwickeln:** Empfohlen wurde, den Aufbau von Fähigkeiten in Form von technologischen Kompetenzen, Produktions- und Fertigungsfähigkeiten sowie das Setzen eines regulatorischen Rahmens in Deutschland, aber auch europaweit mit hoher Priorität voranzutreiben. Das Ziel muss es sein, für (sicherheits)kritische Bereiche **alternative Schlüsseltechnologien** zu entwickeln, diese in Europa zu produzieren beziehungsweise bei Bedarf existierende Technologien modifizieren oder auch erweitern zu können. Das Ziel ist zudem, Abhängigkeiten zu reduzieren und den Einsatz existierender Technologien beherrschbar zu gestalten.
   Kurz- bis mittelfristigen Wirkungen erzielen: Es wurden folgende vier Maßnahmen dringend empfohlen: die **Bereitstellung sicherer Dateninfrastrukturen** und -Plattformen, die **Zertifizierung kritischer Netzkomponenten**, erste Schritte in Richtung einer **Zertifizierung von Künstlicher Intelligenz (KI)** und Maßnahmen zur Entwicklung **sicherer Hardware-Alternativen**, unter anderem basierend auf Open-Source-Hardware.
2) **Beurteilungsfähigkeit stärken:** Das Papier empfahl Maßnahmen zur Stärkung der Beurteilungsfähigkeit, die für den souveränen Umgang mit Technologie erforderlich sind. Empfohlen wurde ein gezielter Kompetenzausbau in Schlüsselbereichen, um mögliche Risiken, die durch Abhängigkeiten entstehen (Hersteller, Herkunftsland, Einsatz, Wechselwirkungen), systematisch beurteilen zu können. Eine zentrale Maßnahme, die mit hoher Dringlichkeit angeraten wurde, ist die Entwicklung von (standardisierten) **Prüfverfahren und -Laboren** für eine kontinuierliche **Zertifizierung** von kritischen Hard- und Softwarekomponenten, um einen beherrschbaren Einsatz sicherheitskritischer Technologien zu ermöglichen.
3) **Regulierung für den Einsatz von Technologie** in sicherheitskritischen Bereichen verstärken: Es wurde zudem empfohlen, Regulierungsanstrengungen voranzutreiben, um Vorgaben für den Einsatz von Technologien mit hohem Risikopotenzial für sicherheitskritische Bereiche zu machen.
4) **Zukunftstechnologien gestalten:** Es wurde zudem empfohlen, für Zukunftstechnologien, die eine große Bedeutung für die Cybersicherheit und technologische Souveränität haben, wie 6G und Quantencomputing frühzeitig die erforderlichen, politischen Weichenstellungen voranzutreiben, auch wenn diese erst einen langfristigen Wirkungshorizont haben werden. Dazu gehört auch, massiv in Forschung und Entwicklung für Technologien wie **6G und Quantencomputing** zu investieren, um eigene deutsche und europäische Technologien am Markt zu platzieren und Standards von Beginn an mitzubestimmen.

2 Umsetzungsstand

Einige wichtige Schritte und Maßnahmen in den Themenbereichen **Schlüsseltechnologien entwickeln** und **Zukunftstechnologien gestalten**, die in den Empfehlungen angeregt wurden, wurden bereits angestoßen. Zu nennen sind nationale und europäische Initiativen im Bereich des Aufbaus **vertrauenswürdiger Hardware**. Dazu gehören die Leitinitiative „Vertrauenswürdige Elektronik“ des Bundesministeriums für Bildung und Forschung (BMBF), der EU Chip Act und auch der Aufbau der Forschungsfabrik Mikroelektronik der Fraunhofer-Gesellschaft. Zur Bereitstellung sicherer Dateninfrastrukturen fördern das BMBF und das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) Maßnahmen zum Aufbau der **GAIA-X-Multicloud-Infrastruktur** und zum Aufbau von souveränen Datenräumen, wie dem **Mobility Data Space**. Über die Data Space-Initiativen der EU und mit dem Europäischen Data Act sind auch wichtige Initiativen auf der **europäischen Ebene** auf den Weg gebracht worden.

Mit dem BMBF-geförderten Aufbau von **KI-Kompetenzzentren** in Deutschland und ersten Ansätzen zur Zertifizierung von KI-Systemen wurden wichtige Schritte zur Erhöhung der technologischen Souveränität getan.

Im Bereich **Quantencomputing** wurde 2021 ein großes BMBF-Forschungsprogramm zum Aufbau von Demonstrations-Quantencomputern in Deutschland gestartet, mit dem Ziel, innerhalb von fünf Jahren einen wettbewerbsfähigen deutschen Quantencomputer mit mindestens 100 individuell ansteuerbaren Qubits zu schaffen – skalierbar auf mindestens 500 Qubits. Es werden bundesweit mehrere Zentren gefördert, die unterschiedliche Hardwareplattformen entwickeln, um Fähigkeiten zur Entwicklung von Quantenrechnern in der Breite und Tiefe voranzutreiben.

Für das zentrale Zukunftsfeld der **6G-Kommunikation** wurden ebenfalls im Jahr 2021 erhebliche BMBF-Mittel für die Förderung von Forschungsarbeiten zur Entwicklung von 6G-Technologie bereitgestellt.

Diese angestoßenen Maßnahmen sind äußerst begrüßenswert und zielen genau in die richtige Richtung.

3 Aktuelle politische Lage und Auswirkungen

Die Durchdringung und Vernetzung sämtlicher Lebensbereiche durch die Digitalisierung hat durch die **Covid-19-Pandemie** rasant an Geschwindigkeit zugenommen. IoT-Geräte, Netzwerkkomponenten, (Edge-)Cloud-Infrastrukturen oder auch KI-Systeme werden in deutlich schnellerem Tempo als noch vor wenigen Jahren prognostiziert zu zentralen Bestandteilen von IKT-Infrastrukturen in allen Bereichen, ins-

besondere auch in kritischen Infrastrukturbereichen. Damit ist wie prognostiziert, die **technologische Abhängigkeit** von den entsprechenden Technologieanbietern und -betreibern rasant weiter angestiegen. So konstatiert eine Erhebung des Bundesverbands der Deutschen Industrie[2] aus dem Jahr 2020 eine massive Abhängigkeit von China beim Import digitaler Technologien. Auch das aktuelle Gutachten der Expertenkommission Forschung und Innovation[3] von 2022 weist auf diese hohe Abhängigkeit hin und zeigt unter anderem auf, dass chinesische Hersteller bei 9 von 13 identifizierten Schlüsseltechnologiefeldern zu den Hauptlieferanten gehören. Diese zunehmende Abhängigkeit wurde durch die **Engpässe in den Lieferketten**, die in den letzten Jahren gravierende Ausmaße angenommen haben, dramatisch bestätigt. Zu nennen sind hier unter anderem die Engpässe bei der Verfügbarkeit wichtiger Rohstoffe, aber auch die **Engpässe bei der Bereitstellung von Chips und Halbleitern**. Die Folge der Abhängigkeit ist in allen Bereichen der verarbeitenden Industrie zu spüren und hatte erhebliche wirtschaftliche Konsequenzen. Beispielsweise kam es zu Produktionsverzögerungen bis hin zu Produktionsstopps, unter anderem im Maschinenbau oder der Automobilindustrie. Aber auch die anhaltende Diskussion um den Einsatz von Produkten chinesischer Unternehmen, die derzeit für den schnellen Ausbau von 5G-Netzen erforderlich sind, verdeutlichen die **große Dringlichkeit, bei nationalen und europäischen Herstellern die Fähigkeiten zur Entwicklung von Schlüsseltechnologien und bei Zulieferern, Integratoren und Betreibern zur Beurteilung der Sicherheit von Software- und Hardware-Komponenten mit höchster Priorität voranzutreiben.** Nur so wird es möglich sein, die erforderlichen nationalen und europäischen Fähigkeiten zu erlangen beziehungsweise zu stärken, um souverän, also selbstbestimmt und unabhängig zu agieren.

Weiterhin hat die Analyse der **Cyberangriffe**, die gegen ukrainische Infrastrukturen gestartet wurden, gezeigt, dass diese Angriffe lange vorbereitet waren. Dies umfasst Angriffe, um Schadcode auf Systemen zu platzieren und sich bei Bedarf Zugang auf Systeme von Betreibern von (kritischen) Infrastrukturen wie Banken, Telekommunikationsunternehmen, oder auch Energieversorgern zu verschaffen. Die Ukraine war gut aufgestellt, um solche Angriffe frühzeitig zu erkennen und abzuwehren. Diese Entwicklung lehrt, dass eine hohe **Resilienz gegen Cyberangriffe**, die sich gegen **systemrelevante** Infrastrukturen (nicht nur kritische Infrastrukturen) richten, essenziell ist. Entsprechende Maßnahmen müssen eine sehr hohe Priorität erhalten, damit auch Deutschland in Zukunft gegen staatlich initiierte Cyberattacken besser gewappnet ist. Unternehmen und Behörden müssen darin unterstützt werden, ihre Infrastrukturen **ganzheitlich und kontinuierlich** zu schützen. Dazu muss der Auf- und Ausbau von **Prüflaboren** zur kontinuierlichen Überprüfung und **Zertifizierung** von kritischen Hard- und Softwarekomponenten mit Nachdruck vorangetrieben werden. Auch die **Regulierung** und die Entwicklung von **Verfahren** zur Überprüfung des Umsetzungstandes der Vorgaben zur Erhöhung der Resilienz von Unternehmens- und behördlichen Infrastrukturen muss mit Nachdruck vorangetrieben werden.

Die aktuellen geopolitischen Entwicklungen haben zudem einmal mehr verdeutlicht, dass bei den Initiativen zu Datenräumen, wie GAIA-X und Catena-X, die **Cybersicherheit und die Resilienz der Plattformen gegen Cyberangriffe** ganz erheblich verstärkt werden müssen. Dazu wird dringend empfohlen, die Zertifizierung der eingesetzten Soft- und Hardware und die Etablierung vertrauenswürdiger Ausführungsumgebungen auf Cloudplattformen im Sinne des Confidential Computings, aber auch die konsequente Umsetzung des Zero-Trust-Prinzips mit hohem politischen Druck voranzutreiben.

Die Lehren aus der 5G-Entwicklung haben gezeigt, dass es unabdingbar ist, bereits jetzt **Sicherheitskonzepte für 6G-Komponenten** und -Szenarien zu erforschen und zu erproben. 6G wird eine zentrale Rolle für die Cybersicherheit spielen, da die 6G-Technologie noch tiefer in alle Lebens-, Produktions- und Arbeitsbereiche hineingreifen wird als die 5G-Technologie, die neben der Kommunikation über öffentliche Netze vordringlich im industriellen Bereich oder Smart City Szenarien zum Einsatz kommt.

Die aktuelle politische Lage hat aber auch einen **neuen Aspekt** in den Vordergrund gerückt, der in den Empfehlungen von 2019 noch nicht explizit adressiert wurde. Durch die massenhafte Verbreitung von gefälschten digitalen Medieninhalten wurde die zunehmende Bedeutung der politisch gesteuerten **Desinformation** für das politisch souveräne Handeln verdeutlicht. Unter Nutzung maschineller Lernverfahren können gefälschte Medieninhalte, wie insbesondere Sprachnachrichten und Videos, als sogenannte **Deepfakes** einfach mit kostenloser Software erstellt werden. Dies eröffnet eine neue Möglichkeit der politischen Meinungsbeeinflussung, sodass die **souveräne Entscheidungsfindung massiv gefährdet** wird. Gefälschte Medieninhalte, die zum Beispiel Sprache, Gestik und Mimik einer Person täuschend echt imitieren, erhöhen wesentlich die Gefahr, dass den Inhalten vertraut wird. Politisches Handeln ist deshalb dringend erforderlich.

Empfohlen wird, folgende sich ergänzende Maßnahmen voranzutreiben:

- Förderung der Forschung zur automatisierten, KI-basierten Deepfake-Erkennung, um eine Detektion unter Realbedingungen zu ermöglichen.
- Aufbau von vertrauenswürdigen, frei nutzbaren Validierungsdiensten zur Überprüfung zweifelhafter Videos, Audios und Bilder.
- Förderung des Aufbaus von Infrastrukturen zur automatisierten Markierung von Medieninhalten mit Ursprungsnachweisen und deren einfacher Validierung.
- Entwicklung normativer Vorgaben für Betreiber von Social-Media-Plattformen, um die Verbreitung von Desinformation mittels Deepfakes zu unterbinden und erkannte Deepfakes von den Plattformen zu löschen.

4 Handlungsempfehlungen angesichts der aktuellen politischen Lage

Die technologischen und politischen Entwicklungen der vergangenen drei Jahre haben die **hohe und wachsende Abhängigkeit** von Drittanbietern aus außereuropäischen Ländern dramatisch verdeutlicht. Es wird deshalb **mit Nachdruck** empfohlen, die nachfolgenden fünf Punkte mit **höchster Priorität** voranzubringen.

Die politischen Entwicklungen haben die immense **Wichtigkeit der Resilienz** kritischer Systeme und Infrastrukturen insbesondere auch gegen politisch motivierte Cyberattacken verdeutlicht, um die Souveränität des unternehmerischen und politischen Handelns nachhaltig zu gewährleisten. Wir empfehlen deshalb,

1) die **Beurteilungsfähigkeit weiter** zu steigern und **zusätzlich** die **Erhöhung der Resilienz** voranzutreiben. Zentrale Maßnahmen für beide Fähigkeiten – Beurteilung und Angriffsresilienz – sind der Auf- und Ausbau von **Prüflaboren** zur kontinuierlichen Sicherheitsüberprüfung und die **konsequente Zertifizierung** von kritischen Hard- und Softwarekomponenten. Wir empfehlen zudem, die Umsetzung des **Zero-Trust**-Prinzips bei Sicherheitsarchitekturen zu fordern und zu fördern. Die USA verfolgen diesen Ansatz bereits und können Orientierung bieten.

Zur Stärkung der Angriffsresilienz wird weiterhin empfohlen,

2) Anstrengungen zur **Regulierung** des Einsatzes von Technologie in sicherheitskritischen Bereichen mit dem **Fokus auf Resilienz und Kontrollierbarkeit** zu verstärken und automatisierte Verfahren zur skalierenden Überprüfung des Umsetzungstandes zum Einsatz zu bringen. In diesem Zusammenhang wird auch empfohlen, das **Beschaffungswesen** den Erforderlichkeiten anzupassen und nationale Interessen stärker zu berücksichtigen.

Die Stärkung der Resilienz und Erhöhung der technologischen Souveränität erfordert weitere Anstrengungen, vertrauenswürdige Alternativen bei Schlüsseltechnologien bereitzustellen. Es wird deshalb empfohlen,

3) **Schlüsseltechnologien** insbesondere im Bereich sicherer Dateninfrastrukturen, zertifizierter KI und sicherer Hardware-Plattformen weiter voranzutreiben und bei den Dateninfrastrukturen wie **GAIA-X** und den **Datenräumen das Thema Cybersicherheit zu verstärken**.

Aufgrund der massiven Bedeutung der IT-Sicherheit des zukünftigen 6G-Standards, der tief in alle Lebens-, Produktions- und Arbeitsbereiche eingreifen wird, wird empfohlen,

4) für die **Zukunftstechnologie 6G** neue **Sicherheitskonzepte, -protokolle und -dienste** frühzeitig zu erforschen, in Reallaboren zu erproben und in die internationale Standardisierung einzubringen.

Um der zunehmenden Bedrohung des souveränen Handelns durch politisch gesteuerte **Desinformationskampagnen mittels Deepfakes** entgegenzutreten, wird empfohlen,

5) Maßnahmen zu fördern, die einerseits der **Erkennung von Deepfake-Desinformationen** und andererseits der **automatisierten Markierung** von Medieninhalten mit Ursprungsnachweisen dienen. Auf der rechtlichen Seite gilt es, **normative Vorgaben für Betreiber** von Social-Media-Plattformen voranzubringen, um die Verbreitung von Desinformation mittels Deepfakes zu unterbinden.

1 www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2022-06-impulspapier-technologische-souveraenitaet-update.pdf
2 bdi.eu/publikation/news/europas-digitale-souveraenitaet-nachhaltig-staerken
3 www.e-fi.de/publikationen/gutachten

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: Thomas Caspers, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert (Hauptautorin dieses Impulspapiers), Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner