Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)080

Ausschuss Digitale Agenda
z.Hd. Frau Cornelia Schultz
Sekretariat PA 23

Deutscher Bundestag
Platz der Republik 1
11011 Berlin

Isabel Skierka
Digital Society Institute

ESMT Berlin
Schloßplatz 1
10178 Berlin

E-Mail: isabel.skierka@esmt.org

Per Email an: ada@bundestag.de

Berlin, den 10.12.2019

Betr.: Fragenkatalog Anhörung des Ausschusses Digitale Agenda zum Thema „IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität“ am 11. Dezember 2019

Frage 1: Digitale Souveränität ist eine Grundvoraussetzung für die staatliche Souveränität Deutschlands. Wie sehen Sie Deutschland und Europa - hinsichtlich der Bürger, der Unternehmen, der Verwaltung - diesbezüglich aufgestellt und wo sehen Sie welchen regulativen Handlungsbedarf mit Blick auf die verschiedenen Akteure?

„Digitale Souveränität“ ist ein rhetorisch oft genutzter, aber selten klar definierter Begriff. Im Kontext dieser Stellungnahme werde ich den Begriff folgendermaßen verwenden: Digitale Souveränität bedeutet die Fähigkeit zum selbstbestimmten Handeln und Entscheiden im digitalen Raum.[1] Grundlage ist die Beherrschung von Schlüsselkompetenzen und -technologien sowie die Fähigkeit, selbstbestimmt zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner zu entscheiden und diese gegebenenfalls weiterzuentwickeln.[2] Souveränität bedeutet nicht, ausschließlich auf eigene Ressourcen zurückzugreifen. Vielmehr besteht sie gerade darin, gegebenenfalls nötige Abhängigkeiten einzugehen und durch ausreichende Beurteilungs- und Handlungsfähigkeit beherrschen zu können. Gesellschaften, Organisationen und Staaten sind digital souverän, wenn sie über die Fähigkeit verfügen, die wesentlichen Funktionskriterien der von ihnen genutzten Informationstechnik kontrollieren zu können.[3] Zugang zu vertrauenswürdigen und sicheren IT-Systemen (im Sinne von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität) ist dafür eine notwendige Voraussetzung. Die Gewährleistung von IT-Sicherheit wiederum erfordert technische,

[1] Bundesministerium für Wirtschaft und Energie (2015). „Leitplanken Digitaler Souveränität“. Nationaler IT-Gipfel 2015.
[2] Bitkom. (2015). „Digitale Souveränität, Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa“; Forschungszentrum Informatik, Accenture, Bitkom Research. (2015). „Kompetenzen für eine Digitale Souveränität“.
[3] Weber et al. (2018). “Sovereignty in Information Technology. Security, Safety and Fair Market Access by Openness and Control of the Supply Chain”. http://www.QuattroS-Initiative.org/

organisatorische und regulatorische Maßnahmen, aber auch die Förderung von Innovationen von Technologien und Verfahren in Europa.

Am Digital Society Institute der ESMT Berlin arbeiten wir im angewandten Bereich unserer Forschung vorwiegend mit mittelständischen und größeren Industrieunternehmen in Deutschland zusammen, die kommerziell verfügbare IT anwenden oder auf ihre Sicherheit prüfen. Aus dieser wirtschaftlichen Anwenderperspektive heraus ergibt sich hinsichtlich der Frage, wie Deutschland und Europa bezüglich digitaler Souveränität aufgestellt sind, folgendes Bild.

Erstens steigt derzeit Deutschlands und Europas Abhängigkeit von ausländischen Technologieanbietern, wobei die Beherrschbarkeit von Schlüsselkompetenzen und -Technologien eher sinkt. In einigen Industrien ist Europa noch führend, zum Beispiel bei Enterprise Software[4], industrieller Robotik[5], Herstellern von Mobilfunktechnik[6] und bei intelligenten Sprachverarbeitungssystemen[7]. Doch in anderen wesentlichen Technologiebereichen sind europäische IT-Anwender zunehmend abhängig von ausländischen Anbietern, insbesondere in den Bereichen Cloud- und Dateninfrastruktur und Software bzw. bei mobilen oder Desktop-Betriebssystemen. Im Bereich der Produktion von Halbleitern und Mikroprozessoren ist der globale Marktanteil europäischer Produzenten ebenfalls seit einigen Jahren kontinuierlich gesunken, während die Produktionskapazitäten in Asien (vor allem in Südkorea, Taiwan und Japan) stark gestiegen sind.[8] Im Bereich der IT-Sicherheitstechnologien entwickeln Wissenschaftler und Unternehmen in Deutschland konkurrenzfähige IT-Sicherheitslösungen. Auf dem internationalen Markt haben diese sich jedoch noch nicht erfolgreich durchsetzen können.[9]

In der Forschung und der Ausbildung von Experten ist Europa eine der führenden Regionen weltweit, kämpft aber damit, die Talente zu behalten. Die professionellen Angebote im Privatsektor ausländischer Firmen und teilweise auch in ausländischen Hochschulsystemen sind für viele Hochschulabsolventen attraktiver als jene von europäischen Firmen und Hochschulen. Dies zeigt sich insbesondere im Bereich der Künstlichen Intelligenz (KI).[10] Die meisten Regierungen in Europa haben dieses Problem erkannt (s. deutsche und französische KI-Strategien). Ob die geplanten Maßnahmen erfolgreich sein werden, wird sich innerhalb der nächsten Jahre zeigen.

Zweitens ist für Innovationen in Europa weniger Kapital verfügbar als in den USA oder China. Im Jahr 2016 beliefen sich die Risikokapitalinvestitionen in der EU auf rund 6,5 Mrd. EUR, während der vergleichbare US-Wert 39,4 Mrd. EUR betrug.[11] Öffentliche Investitionen in Forschung und Entwicklung

[4] Mit Weltmarktführern wie SAP oder Amadeus

[5] 8 von 20 Weltmarktführern haben ihr Headquarter in Europa, davon die Hälfte in Deutschland. TechNavio Blog. (2019). „Top 21 Industrial Robotics Companies in the World 2019". 05.02.2019, https://blog.technavio.com/blog/top-21-companies-in-the-industrial-robotics-market

[6] Zwei der drei Weltmarktführer (Ericsson und Nokia) haben ihre Headquarters in Europa

[7] Fast die Hälfte der 12 führenden Firmen sind europäisch. Quelle: GS Research Unit. (2016). "Profiles in Innovation: Artificial Intelligence: AI, Machine Learning and Data Fuels the Future of Productivity" zit. in: Ulrike Franke. (2019). "Harnessing artificial intelligence". European Council on Foreign Relations.

[8] European Political Strategy Centre of the European Commission. (2019). "Rethinking Strategic Autonomy in the Digital Age". EPSC Strategic Notes, Issue 30.

[9] Forschungszentrum Informatik, Accenture, Bitkom Research. (2015). „Kompetenzen für eine Digitale Souveränität"

[10] Vgl. Ulrike Franke. (2019). "Harnessing artificial intelligence". European Council on Foreign Relations. https://www.ecfr.eu/publications/summary/harnessing_artificial_intelligence#_ftn21

[11] Europäische Kommission. "VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups", https://ec.europa.eu/commission/presscorner/detail/en/IP_18_2763 zitiert in: Charlotte Stix.

sind in Europa auch oft niedriger als in den USA oder China. Diese Investitionen müssen in Europa daher sehr gezielt eingesetzt werden, um erfolgreich Innovationen zu fördern (s. Antwort auf Frage 21).

Drittens werden Technologien zunehmend komplexer und mit Hinblick auf IT-Sicherheit weniger beherrschbar. Die Lieferketten der meisten Technologien sind global, die in den meisten IT-Systemen verbauten Komponenten intransparent für Anwender. Dieses Problem steht aktuell im Zentrum der Debatte um den Einsatz chinesischer Netzwerktechnologien in zukünftigen 5G-Netzwerken. Die schwindende Beurteilungsfähigkeit und Beherrschbarkeit von IT-Sicherheit ist jedoch nicht nur in Deutschland und Europa, sondern weltweit ein Problem.

Viertens verfügt die EU mit dem zweitgrößten Wirtschaftsraum der Welt und der Hoheit über darin geltenden Standards über eine große regulatorische Macht. Mit der EU Datenschutzgrundverordnung und einigen Regulierungen im Bereich der IT-Sicherheit (die EU NIS-Richtlinie (deren Umsetzung in Deutschland das IT-Sicherheitsgesetz ist) sowie die eIDAS-Verordnung und der EU Cybersecurity Act) bilden ein robustes Regelwerk, das zunehmend international Gültigkeit entfaltet. Diese tragen klar zu einem höheren Datenschutz- und IT-Sicherheitsniveau für IT-Anwender in Europa bei. Hinzu kommen zahlreiche fachspezifische gesetzliche Regelungen im Bereich IT-Sicherheit und Datenschutz, welche jedoch noch zu fragmentiert sind. Regulativer Handlungsbedarf besteht hier bei der Weiterentwicklung des Datenschutz- und IT-Sicherheitsrechts sowie bei der Vereinheitlichung von IT-sicherheitsrechtlichen Regeln auf EU-Ebene.

Bezüglich der Förderung digitaler Souveränität und der Stärkung der europäischen Technologiebranche werden sich regulatorische Fragen auch im wettbewerbsrechtlichen und industriepolitischen Bereich ergeben, welche hauptsächlich auf EU-Ebene anzugehen sind.

Frage 2: Wo besteht gesetzgeberischer Handlungsbedarf, um die digitale Souveränität auf nationaler und auf EU-Ebene langfristig zu sichern? Welche Spielräume hat der nationale Gesetzgeber und welche Vorgaben sollten zwingend auf EU-Ebene getroffen werden? Welche Aspekte, Technologien und Standards unterstützen am meisten die digitale Souveränität der Bürgerinnen und Bürger – und wie kann der Staat diese am besten fördern?

Die Stärkung digitaler Souveränität ist eine strategische Aufgabe, die sowohl sicherheits- als auch wirtschafts- und industriepolitische Dimensionen hat. Weder in Deutschland noch auf EU-Ebene existieren ein Überblick über notwendige Kompetenzen und Technologien, geschweige denn eine ganzheitliche Strategie für digitale Souveränität. Bevor Staaten auf nationaler oder EU-Ebene gesetzgeberisch tätig werden, sollten sie zunächst strategische Ziele und Maßnahmen für die Stärkung digitaler Souveränität definieren.

In einem ersten Schritt sollten Entscheidungsträger in Deutschland und Europa daher bestimmen, über welche Schlüsseltechnologien und –Kompetenzen sie selbst verfügen sollten und in welchen Bereichen sie Abhängigkeiten eingehen können. Damit einhergehen muss die Beantwortung der Frage nach dem Umgang mit Abhängigkeiten von ausländischen Technologieanbietern, welche sich zwangsläufig in der globalen Wertschöpfungskette ergeben. Mit welchen Partnern kann und soll Europa in welchem Rahmen langfristig in diesem Rahmen kooperieren? Die Vertrauenswürdigkeit des politischen und

(2019). “A survey of the European Union’s Artificial Intelligence ecosystem”, Centre for the Future of Intelligence.

rechtlichen Systems sowie bisherige Erfahrungen innerhalb eines Bündnisses mit Partnern sollten eine wichtige Rolle bei dieser Abwägung spielen.

Darauf aufbauend sollte der Staat Innovationen gezielt fördern. Dazu kann er Gelder in Forschung und Entwicklung sowie angewandte innovative Projekte investieren (auch in Kooperation mit dem Privatsektor), seine Rolle als Anwender zur Beschaffung ausgewählter Technologien einsetzen und Rechtssicherheit für den Einsatz neuer Technologien schaffen. Innovationspolitik kann Deutschland sowohl auf nationaler als auch auf EU-Ebene betreiben. Um Transparenz und Kontrollmöglichkeiten von IT, aber auch Innovationsmöglichkeiten, zu stärken, sollte der Gesetzgeber (möglichst auf EU-Ebene) Hersteller und Anbieter zur Öffnung von Technologien und größerer Interoperabilität verpflichten. EU-Mitgliedstaaten sollten außerdem wettbewerbsrechtliche und andere Instrumente prüfen und stärken, die ein „Level Playing Field" auf dem europäischen Markt ebnen.

Frage 3: IT-Angriffe und -Kriminalität, auch Tätigkeiten ausländischer Nachrichtendienste, sind eine große Herausforderung mit Blick auf IT-Sicherheit und Souveränität. Wo sehen Sie hier den dringendsten Handlungsbedarf? Wie kann eine digitale Souveränität erreicht werden, die nicht allein auf Abschottung setzt und sich sinnvoll mit einer offenen und freien Netzarchitektur verbindet?

Ein wesentliches strukturelles Problem in der IT-Sicherheit ist die Qualität und Sicherheit von IT-Produkten und -Diensten. Hier besteht im Kontext digitaler Souveränität dringender Handlungsbedarf. Die steigende Komplexität von IT-Systemen macht diese immer weniger beherrschbar und erschwert eine Beurteilung ihrer Sicherheit. Viele Geräte, die im „Internet der Dinge" vernetzt sind, erfüllen oft nicht einmal grundlegende Sicherheitsanforderungen. Auch Komponenten, die in kritischen Einsatzumgebungen eingesetzt werden (Medizingeräte, Roboter, Produktionsanlagen u.a.) sind in vielen Fällen nicht ausreichend abgesichert. Hinzu kommt die Gefahr, dass Hersteller und Lieferanten auf Anweisung von Sicherheitsbehörden Hintertüren in Soft- und Hardware einbauen, die dann von Nachrichtendiensten oder Kriminellen genutzt werden können.

Die Risiken der mangelnden Sicherheit von Komponenten und Systemen in Design, Entwicklung und Betrieb lassen sich durch technische, organisatorische und regulatorische Maßnahmen reduzieren. Mit Hinblick auf dieses Problem haben EU-Mitgliedstaaten den EU Cybersecurity Act geschaffen, welcher Zertifizierungsschemata für die IT-Sicherheit von IT-Produkten, -Diensten und -Prozessen auf EU-Ebene schafft. Diese werden zunächst jedoch nur freiwillig für Hersteller und Anbieter anwendbar sein.

Das Risiko des gezielten Einbaus von Hintertüren durch Nachrichtendienste oder andere Angreifer aber lässt sich in einer global verteilten Wertschöpfungskette schwer bis gar nicht kontrollieren.[12] Viele Details der Komponenten und von deren Implementierungen innerhalb eines IT-Systems sind für Kunden und Anwender intransparent. Selbst wenn ein System auf seine IT-Sicherheit getestet und zertifiziert ist, besteht immer ein Restrisiko, dass ein böswilliger Akteur wie ein ausländischer Nachrichtendienst, eine nur ihm bekannte Schwachstellen im System ausnutzt. Mit IT-Sicherheitsmechanismen lässt sich also nur begrenzt die Vertrauenswürdigkeit von Technologien gewährleisten.

Eine Abschottung der Lieferkette zum Schutz vor potentiellen Hintertüren in Komponenten ausländischer Hersteller, etwa durch eine rein europäische Produktion von Hard- und Software, ist technisch und wirtschaftlich nur für eine kleine Zahl von Produkten (wie Kryptogeräte,

[12] Weber et al. (2018). "Sovereignty in Information Technology. Security, Safety and Fair Market Access by Openness and Control of the Supply Chain". http://www.QuattroS-Initiative.org/

Sicherheitschips) machbar. Eine Abschottung der physischen Internetinfrastruktur ist praktisch nicht mit der Wahrung eines offenen demokratischen Internets vereinbar.

Wie in der Antwort auf Frage 1 erläutert bedeutet digitale Souveränität auch, nötige Abhängigkeiten einzugehen und durch ausreichende Beurteilungs- und Handlungsfähigkeit zu beherrschen. Hinsichtlich entsprechender Instrumente verweise ich auf meine Antwort auf Frage 8.

Frage 8: Trotz aller Sicherheitsvorkehrungen kann es eine absolute Sicherheit bezüglich eingesetzter Hard- und Software nicht geben. Daher stellt sich, unabhängig von einzelnen Unternehmen, die grundsätzliche Frage des Vertrauens in die Integrität der Hersteller und dem Rechtssystem im Herstellerland. Welche Möglichkeiten sehen Sie, um Risiken bestmöglich zu streuen, einseitige Abhängigkeiten zu vermeiden und die Frage der Vertrauenswürdigkeit – nicht im Sinne von Abschottung – als formalisiertes Merkmal von IT-Sicherheitskonzepten zu etablieren? Welche Bedeutung kommt Haftungsregimen zu? Wie wichtig sind verpflichtende Mindeststandards und Zertifizierungsverfahren? Welche Rolle sollten (unabhängige) Aufsichtsstrukturen spielen? Sind Vereinbarungen hierzu auch auf internationaler Ebene notwendig und realistisch – und wenn ja welche?

Einige für die Beantwortung dieser Frage relevanten Punkte finden sich in der Antwort auf Frage 3.

Sicherheitsevaluationen, Code-Inspektionen und andere Maßnahmen können nur bis zu einem gewissen Maß Sicherheitsrisiken von Technologien reduzieren. Vertrauen in Technologie lässt sich daher auch nur begrenzt durch technische Maßnahmen abbilden. Technologien sind immer in einen politischen Kontext eingebettet. Die Bewertung der Vertrauenswürdigkeit von Schlüsseltechnologien und Technologien, die *safety*-kritische Funktionen erfüllen, muss daher technische und nicht-technische Risiken (z.B. das Rechtssystem im Herstellerland oder Governance-Struktur des Herstellers) umfassen.

Folgende Instrumente könnten die Beherrschbarkeit und Beurteilungsfähigkeit von IT-Sicherheit zusätzlich stärken:

- Regulatorische Anforderungen an die IT-Sicherheit von Hard- und Software, deren Einhaltung Hersteller und Anbieter nachweisen müssen. Dazu gehört auch die Einrichtung standardisierte Prozesse zur Offenlegung und zum Management von Schwachstellen (s. ISO/IEC 29147) und gegebenenfalls Bug Bounty Programme als Anreiz zur Weitergabe von Informationen über Schwachstellen und deren Behebung betreiben. Für Komponenten, die in kritischen Umgebungen eingesetzt werden sollen, sollten entsprechend höhere Anforderungen und eine Pflicht zur Prüfung und Bewertung durch eine unabhängige dritte Stelle gelten. In bestimmten Fällen sollte auch eine Inspektion des Codes auf Schwachstellen und Fehlfunktionen vorgenommen werden.
- Prüfung der Vertrauenswürdigkeit von Herstellern auf Grundlage technischer sowie nicht-technischer (politisches und rechtliches Umfeld des Betreibers) Risikofaktoren (s. EU-weites „Risk Assessment“ der Cybersicherheit von 5G Netzwerken).
- Verpflichtung zur Einrichtung effektiver Risikomanagement-Prozesse bei Betreibern von kritischen Systemen, welche Prinzipien wie Redundanz, Verlässlichkeit (reliability) und Resilienz priorisiert. Fallen Teile eines Systems aus, muss es trotzdem funktionsfähig bleiben.

Eine wichtige Voraussetzung dafür ist, dass Komponenten unterschiedlicher Hersteller genutzt werden (multi sourcing Strategie).

- Einrichtung von effektiven Plattformen und Maßnahmen zum Informationsaustausch über Risiken, Evaluationen, Best Practices u.a. zwischen Herstellern, Anbietern und Anwendern.
- Förderung von Offenheit und Diversität von Technologien durch Anreize, gegebenenfalls vertragliche Vergabe- / Beschaffungsvorschriften und Regulierung.
- Förderung deutscher und europäischer Technologieanbieter durch Beschaffungspolitik, öffentliche Förderprogramme für Forschung und Entwicklung und für angewandte Projekte, Schaffung vorteilhafter Rahmenbedingungen u.a.

Frage 9: Wie bewerten Sie die Wirksamkeit vertraglicher Vereinbarungen, wie z.B. NoSpy-Abkommen, sei es auf zwischenstaatlicher Ebene oder im Rahmen privatrechtlicher Verträge? Halten Sie Konformitätsprüfungen in Bezug auf Vertrauenswürdigkeit und Hardware/Software Integrität für wirksam durchführbar oder wäre eine „Abschottung" und Ausschluss von Komponenten-Anbietern wirksamer?

Die Wirksamkeit vertraglicher NoSpy-Abkommen und Vertrauenswürdigkeitserklärungen halte ich mit Hinblick auf die tatsächliche Gewährleistung von IT-Sicherheit für eher gering. Verletzungen des Abkommens müssten nachweisbar und mit entsprechenden Sanktionierungsmechanismen durchsetzbar sein. Im Kontext der globalen Lieferkette ist dies schwer umsetzbar.

Die Konformitätsprüfung ist ein Instrument, mit dem die Umsetzung bestimmter Anforderungen nachgewiesen werden kann. Im Bereich der IT-Sicherheit erfolgen solche Prüfungen durch Evaluierung und Testing eines Systems. Die Intensität der Prüfung kann je nach Anforderungen angepasst werden und auch Code-Reviews oder Penetrationstests umfassen. Doch technische Maßnahmen sind zur Stärkung von Vertrauen nur bis zu einem bestimmten Maß wirksam. Einen Ausschluss von Komponenten-Anbietern allein aufgrund des Herstellerlandes halte ich nicht für wirksam. Entscheidungen über den Einsatz von Technologien müssen auf einer Risikobewertung basieren. (Für weiteres, siehe Antwort auf Frage 8 für weitere Informationen.)

Frage 11: Welchen Beitrag können dynamisch angepasste Minimalstandards und Zertifizierungen, offene Standards, Interoperabilität, Open Source, Open Hardware usw. zu mehr IT-Sicherheit leisten?

Minimalstandards und Zertifizierungen für IT-Sicherheit können die Sicherheit von IT-Systemen in der Breite erheblich verbessern und sollten daher unbedingt vom Gesetzgeber eingesetzt und weiterentwickelt werden. Insbesondere für das sogenannte „Consumer Internet of Things" kann so ein grundlegendes Niveau von Sicherheit gewährleistet werden, welches systemische Risiken wie Botnetz-basierten Distributed Denial of Service-Angriffen u.a. reduzieren kann. Dabei ist zu beachten, dass die jeweiligen Prüf- und Zertifizierungsverfahren skalierbar, effizient (sowohl zeitlich als auch monetär) und dynamisch (s. häufige Änderungen von Software, beispielsweise durch Updates) sein müssen. Zudem sollten sie auf einheitlichen internationalen Standards basieren und keine Parallelstandards schaffen. Der EU Cybersecurity Act schafft einen Rahmen für die Erarbeitung von Zertifizierungsschemata. Die Zertifizierung wird jedoch zunächst freiwillig sein. Die Gesetzgebung sollte weiterentwickelt werden, sodass Minimalstandards verpflichtend gelten.

Interoperabilität und die Implementierung offener Standards können ebenfalls einen großen Beitrag zu IT-Sicherheit leisten. Sie sollten wo möglich Teil von verpflichtenden Mindeststandards und Zertifizierungen sein. „Open source“ Hard- und Software ist zwar nicht per se fehlerfrei (s. *Heartbleed*-Bug), ermöglicht aber unabhängige Inspektionen, Prüfungen und Anpassungen. Ihr Beitrag geht über IT-Sicherheit hinaus, da interoperable Soft- und Hardware und offene Standards die Anpassung und Weiterentwicklung von Technologien und damit Innovation ermöglichen. Aus diesen Weiterentwicklungen können neue Anwendungen und Diversität von Angeboten entstehen, welche wiederum einen wichtigen Beitrag zu digitaler Souveränität von IT-Anwendern leisten.

Eine Herausforderung für die Zukunft und Feld für Innovation wird die Entwicklung von automatisierten/intelligenten Verfahren zur Inspektion und Verifizierung von IT-Sicherheit komplexer Systeme sein.

Frage 13: Welche Rolle spielen Sicherheitslücken und der Handel mit ihnen für die IT-Sicherheit? Halten Sie eine Meldepflicht staatlicher Stellen für Sicherheitslücken für ratsam?

Schwachstellen in Hard- und Software sind Grundlage für IT-Angriffe. Die Nutzung unbekannter Schwachstellen (Zero-Days) durch staatliche Sicherheitsbehörden (oder jeden anderen Akteur) birgt hohe Risiken für das IT-Ökosystem und die Gesellschaft insgesamt.

Deutschland könnte einen an den "Vulnerabilities Equities Process" (VEP) aus den USA angelehnten Prozess einsetzen.[13] Die Bewertung sollte demnach die Kritikalität einer Schwachstelle für einzelne Benutzer und die systemische Sicherheit der IT gegen den Wert dieser Schwachstelle zur Aufklärung von Verbrechen oder der nationalen Sicherheit abwägen. Nach dem Vorbeugeprinzip sollten Schwachstellen, die bei Ausnutzung durch kriminelle Akteure schwerwiegende Auswirkungen auf Leib und Leben, die Umwelt oder die Wirtschaft haben würden, immer dem Hersteller der Technologie mitgeteilt werden. Ein VEP-ähnlicher Prozess sollte auf einer klaren Rechtsgrundlage basieren und richterlicher Aufsicht unterliegen. Während die IT-Branche, Vertreter der Justiz und der Zivilgesellschaft nicht an einzelnen Entscheidungsprozessen teilnehmen werden können, sollte die Regierung einen regelmäßigen Dialog über den Umgang mit Schwachstellen mit ihnen einleiten und Informationen teilen. Darüber hinaus sollte die IT-Branche selbst ihren eigenen Umgang mit Schwachstellen in ihren Produkten transparent dokumentieren und die Anwender bei deren Behebung unterstützen.

Frage 16: Was muss aus Ihrer Sicht zwingend Eingang in die Reform des IT-Sicherheitsgesetzes finden?

Ein reformiertes IT-Sicherheitsgesetzt sollte enthalten:

- Eine Erweiterung der vom IT-Sicherheitsgesetz betroffenen Branchen über kritische Infrastrukturen hinaus auf Unternehmen, deren Funktionsfähigkeit eine hohe Bedeutung für die Gesellschaft haben.
- Das geplante IT-Sicherheitskennzeichen und Mindeststandards für Hersteller von IT-Produkten und Diensten. Dieses muss jedoch klar mit Kennzeichen und Standards auf europäischer Ebene in Einklang sein.

[13] Martin Schallbruch und Isabel Skierka. (2018). „Cybersecurity in Germany”. Springer Briefs in Cybersecurity. Springer: London

- Eine Pflicht zur Prüfung und Zertifizierung von KRITIS-Kernkomponenten, welche ebenfalls mit europäischen Standards abgestimmt sein müssen.

Frage 18: Das Gefüge der europäischen, nationalen und länderbezogenen IT-Sicherheitsarchitektur ist mit dutzenden Behörden mit unterschiedlichen Rechtsgrundlagen und Befugnissen sehr komplex. Wie sollte dieses Gefüge in Zukunft aufgestellt werden? Welche Verbesserung auf Bundesebene bei Strukturen und Prozessen für Programm-, Projekt- und Architekturmanagement schlagen sie vor?

Aufgrund der stetigen Weiterentwicklung von Technologien und IT-Sicherheitsbedrohungen ist die Organisation einer effektiven IT-Sicherheitsarchitektur eine ständige Herausforderung. Die regelmäßige Evaluation bestehender Strukturen und Institutionen anhand messbarer Kriterien und entsprechende Anpassungen sollten fester Bestandteil der IT-Sicherheitspolitik in Deutschland und Europa sein. Die IT-Sicherheitsarchitektur in Deutschland leidet unter ihrer Komplexität, Zuständigkeitskonflikten und institutionellen Parallelstrukturen. Im Folgenden einige Vorschläge für eine bessere Koordination:[14]

Allgemein – Konsolidierung von Strukturen und Zuständigkeiten; Stärkung von vertrauensvoller Kooperation: Eine Umorganisation der IT-Sicherheitsarchitektur hin zu kohärenteren und konsolidierten Strukturen für die Zusammenarbeit von Bund, Ländern, Wirtschaft und internationalen Partnern ist dringend nötig. Die begrenzten Ressourcen, insbesondere Fachkräfte[15] im IT-Sicherheitsbereich, müssen so effizient wie möglich genutzt und geteilt werden. Die IT-Sicherheitsarchitektur und im weiteren Sinne die Umsetzung der Cybersicherheitsstrategien sollten regelmäßig evaluiert werden und die Ergebnisse öffentlich zugänglich sein. Der Schwerpunkt bei der Aufstellung der IT-Sicherheitsarchitektur sollte auf der Stärkung von Kooperation, Verantwortungsverteilung und Vertrauen anstatt auf einen immer weiteren Ausbau der Befugnisse staatlicher Stellen für die IT-Sicherheit liegen, welche der Entwurf des IT-Sicherheitsgesetzes 2.0 für das BSI anzustreben scheint. Selbst das BSI mit seinen Fachbereichen und hohem Expertiseniveau kann die Gewährleistung von IT-Sicherheit nur als Teil einer Kooperationsstruktur und nicht allein mit anderen Sicherheitsbehörden übernehmen.

Neuorganisation des Cyber-Abwehrzentrums (Cyber-AZ): Auf Bundesebene besteht keine klare Verantwortlichkeit für die Cyberabwehr. Die Effektivität des bestehenden Cyber-AZ ist begrenzt; die anlassbezogene Zusammenarbeit Vertreter unterschiedlicher Behörden in ihren jeweiligen Kompetenzbereichen wird dem Anspruch einer Behörden-übergreifenden Koordination von Cyberabwehr-Maßnahmen und -Strategien nicht gerecht. Die seit langem geplante Umorganisation des Cyber-AZ in ein „Cyber-AZ Plus“ (s. Koalitionsvertrag) sollte daher so schnell wie möglich erfolgen. Ein Cyber-AZ Plus sollte in seiner Ausstattung und Kompetenzen gestärkt werden. Die enge Verbindung mit dem BSI sollte aufgrund der vorhandenen Expertise und Fachbereiche im Bundesamt bestehen bleiben. Ein Cyber-AZ Plus muss sowohl die für Cybersicherheit zuständigen Stellen in den Ländern einbinden sowie die privaten Betreiber kritischer Infrastrukturen und Unternehmen, die wichtige gesamtgesellschaftliche Aufgaben erfüllen. Ein kontinuierlicher und koordinierter Informationsaustausch zwischen Bund, Ländern und Wirtschaft sollte hier höchste Priorität haben.

Rein defensive Ausrichtung des BSI im zivilen Bereich der Cybersicherheit: Das BSI sollte von Aktivitäten im Bereich der aktiven Cyberabwehr ausgeschlossen sein. Auch wenn es grundsätzlich über die

[14] Die folgenden Empfehlungen basieren auf: Martin Schallbruch und Isabel Skierka. (2018). „Cybersecurity in Germany”. Springer Briefs in Cybersecurity. Springer: London. S. 31 ff.
[15] Julia Schuetze. (2018). „Warum dem Staat IT-Sicherheitsexpert:innen fehlen“. Stiftung Neue Verantwortung.

notwendigen Fähigkeiten verfügt, entsprechen aktive Operationen nicht dem Charakter des präventiven Sicherheitsauftrags der Behörde.

Verbesserung der Zusammenarbeit zwischen zuständigen Stellen auf Bundes- und Länderebene: Da die innere Sicherheit in erster Linie Sache der Länder (Polizeien und Nachrichtendienste) ist, sind diese oft für IT-Sicherheitsvorfälle zuständig. Die Schaffung von Cyber-Verteidigungsbehörden in den Bundesländern ist aufgrund der Internationalität der Cyber-Verteidigung, ihrer Nähe zur militärischen Verteidigung und der Kosten für die Entwicklung personeller und technischer Ressourcen unmöglich. Da die Länder dennoch für die Polizei und den Nachrichtendienst zuständig sind, muss eine zentrale Einrichtung jedes Bundeslandes eng mit dem Cyber-AZ Plus des Bundes, idealerweise eine Zentraleinheit der Landespolizei, verbunden sein. Auch die direkte Verbindung zum BSI kann so und mit dem vorgesehenen (teilweise bereits erfolgten) Einsatz von BSI-Verbindungsbeamten auf Landesebene gestärkt werden. Diese Schritte können dem Aufbau von Parallelstrukturen auf Länderebene (siehe Landesamt für Sicherheit in der Informationstechnik) entgegenwirken.

Verbesserung der Zusammenarbeit zwischen Staat und Wirtschaft bei der Cyberabwehr: Die Stärkung der Zusammenarbeit zwischen Staat und Wirtschaft ist essentiell für die gesamtgesellschaftliche IT-Sicherheit, da die meisten digitalen Infrastrukturen in privater Hand sind. Bisher erfolgt sie jedoch im Rahmen zahlreicher heterogener und sich überschneidenden Initiativen. Darunter laufen viele parallel und involvieren dieselben Akteure. Wichtig zur Konsolidierung der Kooperation zwischen Staat und Wirtschaft ist daher erstens die Einrichtung einer zentralen Plattform für Staat und Wirtschaft in Anbindung an das BSI. Branchen und Unternehmen könnten aufgefordert werden, eine gemeinsame privatwirtschaftliche Institution zu bilden, die Teil der BSI-Plattform ist. Im Oktober 2019 hat das BMI mit Unterstützung des BSI ein „Cyberbündnis“ als Teil des Nationalen Paktes für Cybersicherheit gegründet, welches jedoch noch nicht zu beurteilen ist. Zweitens sollte bei der Verbesserung staatlich-privater Kooperation der dringendste Schwerpunkt auf dem Austausch von operativen Informationen zu IT-Sicherheitsbedrohungen, Schwachstellen und Angriffsvektoren („threat intelligence“) liegen. Der Informationsaustausch zwischen Behörden und Unternehmen ist momentan inkonsistent. Staatliche Stellen wie das BSI, Polizeien und Nachrichtendienste verfügen über eine zunehmende Menge von relevanten Informationen – nicht zuletzt durch die mit dem IT-Sicherheitsgesetz eingeführten Meldepflichten und die ausgeweiteten Befugnisse von Nachrichtendiensten im digitalen Raum. Diese für Unternehmen wichtigen, oft technischen, Informationen sollten über die zentralen Plattformen besser geteilt werden. Dabei sollten hohe datenschutzrechtliche Standards eingehalten werden. Nachrichtendienstliche oder polizeiliche Informationen dürfen nur in geringem Umfang an Dritte weitergegeben werden.

Frage 21: Investieren Deutschland und Europa genug in Forschung und Entwicklung für IT-Sicherheit? Wo sehen Sie Defizite und wo dringenden Handlungsbedarf? Welche Forschungsaktivitäten im IT-Sicherheitsbereich in Deutschland werden sowohl durch EU-Mitgliedsstaaten als auch durch Nicht-EU-Staaten finanziell gefördert?

Investitionen in Forschung und Entwicklung (FuE) aus öffentlicher Hand sind unabdingbar für die Stärkung von Schlüsseltechnologien und -kompetenzen in Europa. Öffentliche Ausgaben für FuE im Technologiebereich liegen in den USA und China seit mehreren Jahren über jenen der EU-

Mitgliedstaaten.[16] Deutschland sollte als Teil einer konkreten Agenda für digitale Souveränität (s. Frage 2) gezielt in FuE im Bereich ausgewählter Schlüsseltechnologien investieren. Der Staat sollte außerdem gemeinsam mit Gesellschaft und mit der Wirtschaft gesellschaftlich bedeutsame politische Projekte („Moonshot-Projekte“) definieren, die mit (digitalen Technologien) umgesetzt werden können und müssen.[17]

Ein hervorzuhebendes Projekt im FuE Bereich für IT-Sicherheit ist das Europäische Netzwerk von Kompetenzzentren für Cybersicherheit, welches 2018 mit vier Pilotprojekten im Bereich Quantencomputern gestartet ist, an denen auch deutsche Forschungseinrichtungen teilnehmen. Die Europäische Kommission will für das Projekt zwischen 2021 und 2026 zwei Milliarden aus dem Digital Europe Fund und für den Aufbau 2,8 Milliarden aus dem Horizon 2020 Fund investieren. An einem weiteren hervorzuhebenden Projekt des EU Programms „Projekte von gemeinsamem europäischem Interesse“ (IPCEI), stellt Deutschland gemeinsam mit mit Frankreich, Italien und Großbritannien insgesamt 1,75 Mrd. EUR an Finanzmitteln für die Förderung von Innovation im Bereich der Mikroelektronik (welcher auch Halbleitertechnik umfasst) bereit. Weitere 6 Mrd. EUR wird der Privatsektor bereitstellen.

[16] European Political Strategy Centre of the European Commission. (2019). “Rethinking Strategic Autonomy in the Digital Age”. EPSC Strategic Notes, Issue 30.

[17] Dieser Vorschlag stammt aus einem Workshop, den die ESMT Berlin gemeinsam mit dem Bundesministerium für Wirtschaft und Energie und ca. 20 Vertretern aus Unternehmen, Verwaltung und Wissenschaft am 2. Juni 2017 veranstaltet hat.