Hochschule Bremen
City University of Applied Sciences

Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)116

11.01.2023

Hochschule Bremen · Flughafenallee 10 · D-28199 Bremen

Betr.: Schriftliche Stellungnahme „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Bremen, 10.01.2023

Prof. Dr. jur. Dennis-Kenji Kipker
Professor für IT-Sicherheitsrecht

Flughafenallee 10
28199 Bremen
T +49 421 5905 5465
dennis-kenji.kipker@hs-bremen.de

Sehr geehrte Damen und Herren,

anliegend übersende ich Ihnen meine schriftliche Stellungnahme zu Ihrem Fragenkatalog für die öffentliche Anhörung „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“ des Ausschusses für Digitales im Deutschen Bundestag am Mittwoch, den 25. Januar 2023, 14:00-16:00 Uhr.

Mit freundlichen Grüßen

Prof. Dr. Dennis-Kenji Kipker

Hochschule Bremen
City University of Applied Sciences

Prof. Dr. jur. Dennis-Kenji Kipker

Schriftliche Stellungnahme

„Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Deutscher Bundestag, Ausschuss für Digitales

Öffentliche Anhörung am 25. Januar 2023

Frage 1:

„Im Koalitionsvertrag haben die Regierungsparteien vereinbart, dass sie „einen strukturellen Umbau der IT-Sicherheitsarchitektur“ einleiten und das „Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger“ aufbauen und es als „zentrale Stelle im Bereich IT-Sicherheit“ ausbauen wollen. Wie sollte die Cybersicherheitsarchitektur auf nationaler und europäischer Ebene ausgestaltet werden, um effektiver, wirksamer und widerspruchsfreier aufgestellt zu sein und wo bedarf es einer Neuordnung oder auch Bündelung der Kompetenzen zwischen Bund, Ländern und der Europäischen Union und bedarf es auch angesichts der aktuellen Herausforderungen einer Diskussion über innere und äußere Sicherheit und der diesbezüglichen Kompetenzen und Grenzen? Welche anderen Akteure neben dem BSI (also etwa Cyber-Abwehrzentrum, Nationaler Cyber-Sicherheitsrat, ZITiS), die in Deutschland für Cybersicherheit zuständig sind, sollten reformiert werden und wie?“

Das von den Regierungsparteien im Koalitionsvertrag vereinbarte Ziel, einen strukturellen Umbau der nationalen IT-Sicherheitsarchitektur einzuleiten, wozu insbesondere auch eine unabhängigere Rolle der Gestaltung des BSI gehört, ist grundsätzlich zu begrüßen. Bereits in der aktuellen nationalen „Cybersicherheitsstrategie für Deutschland 2021“ (CSS 2021)[1] des

[1] Bundesministerium des Innern und für Heimat, Cybersicherheitsstrategie für Deutschland, 8. September 2021, abrufbar unter: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html.

Bundesministeriums des Innern, für Bau und Heimat (BMI) tritt der Widerstreit zwischen allgemeinen öffentlichen Sicherheitsinteressen und Cybersicherheit an verschiedenen Stellen deutlich zutage und legt damit zugleich Zielkonflikte offen. Bei einer entsprechenden rechtlichen Würdigung der gegenläufigen Interessen darf ebenso nicht ausgeklammert werden, dass auch die Herstellung und Gewährleistung effektiver Cybersicherheit ein immer schwerwiegenderes öffentliches Interesse darstellt, was sich verstärkt in der erhöhten Cyber-Bedrohungslage seit der Corona-Pandemie und mit dem Beginn des Russland-Ukraine-Krieges beispielsweise für den Sektor der versorgungsrelevanten Kritischen Infrastrukturen (KRITIS), aber auch für kommunale Einrichtungen und kleine sowie mittelständische Unternehmen (KMU) widerspiegelt. Gegenwärtige Interessenkonflikte in der nationalen Cybersicherheitsstrategie betreffen u.a. die Frage der Gefahrenabwehr bei Cyberangriffen, die damit verbundene Abgrenzung der verfassungsrechtlich definierten Zuständigkeiten im Bund-Länder-Kompetenzgefüge und die begriffliche Reichweite der Gefahrenabwehr (Abgrenzung zur „aktiven Cyberabwehr“ und zum „Hackback“, dazu noch im Folgenden), den Umgang mit Verschlüsselungstechnologie, um gleichsam auch Strafverfolgungs- und Sicherheitsbehörden den Zugang zu geschützter Kommunikation zu eröffnen („Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“), den staatlichen Umgang mit Zero-Day-Schwachstellen und Exploits (dazu ebenfalls noch im Folgenden) und damit verbunden auch den Handlungsrahmen der im Geschäftsbereich des BMI liegenden Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), sowie schlussendlich Fragen der Cyberverteidigung und damit verbunden ein Tätigwerden der Bundeswehr im Cyber- und Informationsraum (CIR) – insbesondere auch in Abgrenzung zur aktiven Cyberabwehr und zum Hackback, die an jeweils unterschiedliche rechtliche Voraussetzungen geknüpft sind. Die sich in der CSS 2021 abzeichnenden Interessenkonflikte werden teils durch die 2022 ebenfalls durch das BMI vorgestellte „Cybersicherheitsagenda: Ziele und Maßnahmen für die 20. Legislaturperiode“[2] perpetuiert. So

[2] Bundesministerium des Innern und für Heimat, Cybersicherheitsagenda: Ziele und Maßnahmen für die 20. Legislaturperiode, 12. Juli 2022, abrufbar unter:

heißt es hier z.B., dass die Cyberfähigkeiten des Bundesamtes für Verfassungsschutz (BfV) und deren Nutzbarmachung im Verfassungsschutzverbund fortzuentwickeln sind, ein konsequenter Ausbau von ZITiS erfolgen soll, um digitale Ermittlungswerkzeuge für die Sicherheitsbehörden zur Stärkung der Auswerte- und Analysefähigkeiten im Kampf gegen Cybercrime wie beispielsweise Online-Hasskriminalität zu entwickeln, ein EU-weiter und nationaler Rechtsrahmen zur Bekämpfung sexualisierter Gewalt gegen Kinder (im Netz) gefördert und entwickelt wird, die Prüfmöglichkeiten für „kritische Komponenten“ erweitert werden und die digitale Souveränität verbessert werden soll.

Augenfällig ist bei einer systematischen Untersuchung des *status quo* der nationalen deutschen Cybersicherheitsarchitektur einerseits, dass zahllose und höchst unterschiedliche Zuständigkeits- und Themenbereiche unter dem generellen Dach der „Cybersecurity“ miteinander vermengt sind, die im Ergebnis zwangsläufig zu Widersprüchen in der Umsetzung führen müssen. Zweifellos wird sich andererseits bei der thematischen Vielfalt eine vollständige Widerspruchsfreiheit nicht herstellen lassen, da die die Cybersicherheit in ihrem Schutzbereich betreffenden informationellen Grundrechte[3] mit den ebenfalls verfassungsrechtlich geschützten, widerstreitenden Interessen unter Wahrung des rechtsstaatlichen Verhältnismäßigkeitsgrundsatzes in einen angemessenen Ausgleich zu bringen sind, so zum Beispiel im Hinblick auf die Interessen der öffentlichen Sicherheit und der Strafverfolgung. Speziell für die Cybersecurity bedeutet dies jedenfalls im Ergebnis, dass für eine Reform der nationalen Cybersicherheitsarchitektur zuvorderst ein klares ontologisches Verständnis über den Begriff der

https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html.

[3] So i.e.L. das Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (GVIiS) sowie das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Im weiteren Sinne betroffen sein können ja nach staatlicher Eingriffsmaßnahme auch die Berufsausübungsfreiheit gem. Art. 12 Abs. 1 S. 2 GG, das Grundrecht auf Unverletzlichkeit der Wohnung gem. Art. 13 Abs. 1 GG und unter Umständen auch die Eigentumsfreiheit gem. Art. 14 Abs. 1 GG.

„Cybersicherheit“ gewonnen werden sollte, das in Deutschland zurzeit nicht vorhanden ist und deshalb in der Umsetzung von Maßnahmen Konflikte und Wertungswidersprüche zur Folge hat. Sowohl die CSS 2021 und insbesondere die nationale Cybersicherheitsagenda belegen eine deutliche Überdehnung in der begrifflichen Auslegung der Cybersicherheit, indem beispielsweise die Bekämpfung von Online-Hasskriminalität, digitaler Kinderpornografie und die digitale Souveränität als Bestandteil der nationalen Cybersicherheit geführt werden. Dies sind zwar zweifellos auch hochrangige und berechtigte staatliche Digitalisierungsinteressen mit daran anknüpfenden gewichtigen grundrechtlichen Schutzgütern, die jedoch anderen Regulierungsfeldern unterfallen und deshalb strategisch nicht mit der Cybersicherheit gleichgesetzt werden sollten.

Unter diesem Gesichtspunkt sollte für eine Reform der nationalen Cybersicherheitsarchitektur basierend auf einem engen, vorwiegend operationellen und technisch-organisatorischen Verständnis der Cybersicherheit als Voraussetzung einer fehlerfreien Funktionsweise von IT-Systemen angedacht werden, gesetzliche Vorgaben und damit behördliche Zuständigkeiten klarer als bislang aufzutrennen, um ein höheres Maß an Transparenz, Nachvollziehbarkeit und damit Vertrauenswürdigkeit in der Zusammenarbeit von Behörden, Bürgern und Unternehmen zu erzielen. Dazu gehört ebenso, dass rechtlich und behördenorganisatorisch sehr deutlich zwischen operativer Cybersicherheit als Bestandteil der tagtäglichen Aufgaben von Staat und Wirtschaft und der Reaktion auf außergewöhnliche Erfordernisse und Vorkommnisse im Cyberraum unterschieden wird. Ein solches enges begriffliches Verständnis der Cybersicherheit als vornehmlich präventive, technisch-organisatorische Maßnahme schließt auch aus, dass offensive Cyberoperationen, Hackbacks oder die aktive Cyberabwehr Gegenstand einer „Cybersicherheitsagenda“ sein können.

Überdies hat sich die Cybersicherheit in den vergangenen Jahren mehr und mehr zu einer ressortübergreifenden Aufgabe entwickelt, die eine umfassende Kooperation von Staat, Wirtschaft und Gesellschaft erfordert. Dies bedeutet im Ergebnis auch, dass eine

historisch gewachsene Verortung des BSI im Geschäftsbereich des BMI immer weniger sinnhaft erscheint, da das BSI schon seit Langem nicht mehr im Wesentlichen nur Aufgaben zum digitalen Schutz der Bundesverwaltung wahrnimmt und sowohl das IT-SiG 1.0 (2015), als auch die EU NIS-Richtlinien 1 (2016) und 2 (2022) und das IT-SiG 2.0 (2021) dazu beigetragen haben, dass das BSI eine horizontale und bereichs- sowie regulierungsebenenübergreifende Zuständigkeit in der Cybersicherheit besitzt. Dies wird durch die jüngsten rechtpolitischen Entwicklungen zum EU Cyber Resilience Act (CRA)[4] als Mittel einer strategischen europäischen Überformung nationalen Rechts weiter deutlich verstärkt. Unabhängig von der politischen Diskussion eines BSI als selbstständige oberste Bundesbehörde oder anderer institutioneller Vorschläge (siehe dazu nachfolgend Frage 2) sollten daher jedenfalls Maßnahmen erwogen werden, das BSI aus der alleinigen Zuständigkeit des BMI herauszulösen. Eine solche Maßnahme dürfte sich auch als vertrauensbildend zur Förderung von essenziellen Public Private Partnerships (PPP) in Sachen Cybersicherheit zwischen Staat und Wirtschaft auswirken.

Bei der rechtspolitischen Diskussion um einen „strukturellen Umbau der IT-Sicherheitsarchitektur“ in Deutschland geht es folglich in einem ersten Schritt nicht darum, nur die Rolle des BSI, von weiteren einzelnen Gremien und Fachbehörden bzw. sonstigen Einrichtungen zu bewerten, sondern ausgehend von einer neuen und vereinheitlichen Definition der Cybersicherheit systematisch und umfassend zu untersuchen, welches staatliche Handeln tatsächlich Interessen der Cybersicherheit im engeren Sinne bedient oder aber ressortmäßig anders zu verortenden Interessen und Zielen zu dienen bestimmt ist. Auch im Hinblick auf die Rechtsetzung auf europäischer Ebene stellen sich mittlerweile vergleichbare Probleme, die zwangsläufig mit einer zunehmend schnell wachsenden Digitalregulierung einhergehen, die in der Praxis bislang nur wenig Gelegenheit zur Erprobung hatte. Nur auf diese Weise lässt sich auch der sog. „Verantwortungsdiffusion“, von der mittlerweile in Cybersecurity-Expertenkreisen zunehmend die

[4] European Commission, Cyber Resilience Act, 15. September 2022, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

Rede ist, entgegenwirken, indem fortwährend neue Gremien und übergreifende Zuständigkeiten zur nationalen Cybersicherheit begründet werden.

Frage 2:

„Wie kann das Ziel, das BSI unabhängiger aufstellen zu wollen, konkret erreicht werden und wo bedarf es neben der Rechtsaufsicht seitens des BMI auch einer Fachaufsicht – oder anders herum gefragt: wo sind die bestehenden Abhängigkeiten das größte Hemmnis mit Blick auf die Akzeptanz und das Vertrauen in das BSI und welche Möglichkeiten sehen Sie, diese abzubauen?“

Gem. § 1 BSIG ist das BSI eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch. Diese vorgenannte gesetzliche Beschreibung des BSI legt nahe, dass es sich um eine Behörde handelt, die als in Deutschland zentral für die Informationssicherheit zuständiges Organ ihre Entscheidungen tatsachenbasiert-nachprüfbar und damit wissenschaftlich-fundiert trifft. Dies deckt sich mit dem allgemeinen Verständnis der Informationssicherheit als technisch-informatischer Disziplin. Wie bereits im Rahmen der Beantwortung von Frage 1 dargelegt wurde, ist das BSI zwar historisch aus der Zentralstelle für das Chiffrierwesen als einem Arbeitsbereich des BND hervorgegangen und hatte ursprünglich einen sehr eingeschränkten Aufgabenbereich des Schutzes u.a. auch vornehmlich der Bundes-IT, der jedoch im Rahmen zahlreicher Gesetzesnovellen laufend erweitert wurde, sodass kaum noch eine direkte Vergleichbarkeit des „ursprünglichen“ BSI zur aktuellen Behörde, deren Aufgabenbereichen und Struktur sowie Vernetzung im nationalen und europäischen Gefüge der Informationssicherheit gegeben ist. Insbesondere durch das IT-SiG 1.0 (2015) und das IT-SiG 2.0 (2021) sowie durch die europarechtlichen Überformungen hat die Behörde einen deutlichen Kompetenzaufwuchs erfahren,

mit dem enorme zusätzliche Planstellen einhergehen. Hinzu kommt, dass die deutsche Behörden- und Gremienstruktur zur Informationssicherheit nicht mehr mit dem Stand verglichen werden kann, der bei Gründung des BSI zum 01.01.1991 vorherrschte. Gleichwohl finden sich auch in der aktuellen Fassung des BSIG nach wie vor Passagen, die aus jenem mittlerweile mehr als 30 Jahren alten Errichtungsgesetz stammen und nicht diese erhebliche rechtliche, personelle, technische und organisatorische Weiterentwicklung insbesondere der letzten Jahre und damit auch die deutlich geänderte Rolle und öffentliche Wahrnehmung der Behörde berücksichtigen, indem beispielsweise in § 3 Nr. 13 BSIG weiterhin eine wesentliche Aufgabe des Bundesamtes darin liegt, Nachrichtendienst-, Sicherheits- und Strafverfolgungsbehörden bei der Erfüllung ihrer Aufgaben zu unterstützen. Gesetzliche Anforderungen und praktische Realität fallen damit auseinander.

Folglich ist es auch für die Verbesserung der Unabhängigkeit des BSI zunächst notwendig, seinen Aufgabenrahmen neu und stärker im Hinblick auf ein engeres Verständnis der Cybersicherheit als bislang zu definieren (siehe dazu schon die Beantwortung von Frage 1 mit Blick auf den gesamtstaatlichen Horizont der Cybersicherheit). Hierzu gehört auch, dass das BSI als wissenschaftlich-technische Fachbehörde kein Organ zum Treffen oder Transportieren rein sicherheitspolitischer Entscheidungen ist, wie es jedoch in der Vergangenheit mehr und mehr gesetzgeberisch gesehen und in Teilen auch in der Praxis durchgeführt wurde, so beispielsweise mit der Einführung des seinerzeit im Gesetzgebungsverfahren bereits hoch umstrittenen § 9b BSIG („Untersagung des Einsatzes kritischer Komponenten“, der eine vornehmlich politische Prüfbefugnis des BMI enthält, die deshalb eine im BSIG systemwidrige Regelung darstellt). Mit der Neuordnung des Aufgabenrahmens des BSI sind sodann ebenfalls strukturelle Änderungen innerhalb der Behörde durchzuführen. Dazu gehört, dass Abteilungen bzw. Referate, die nicht dem engen Verständnis der Cybersicherheit entsprechen, aus dem BSI auszugliedern und in andere, thematisch näherliegende Fachbehörden zu überführen sind. Erst in einem darauffolgenden Schritt ist über die Frage der weiteren Verortung und Unabhängigkeit des BSI nachzudenken. Die ausführliche Diskussion

darum ist jedoch nicht neu und es werden bereits seit geraumer Zeit verschiedene Modelle vertreten, die allesamt Vor- und Nachteile aufweisen.[5] Ohne diese Debatte verkürzen zu wollen, ist im Ergebnis jedoch festzustellen, dass Cybersicherheit zuvorderst das Vertrauen aller daran beteiligten Akteure erfordert – und dies sind mittlerweile nicht nur und schon lange nicht mehr ausschließlich staatliche Einrichtungen, sondern vornehmlich KMU, Industrieunternehmen, Kommunen sowie Verbraucher:innen, zumal das BSI auf den effektiven Informationsaustausch mit diesen Akteuren angewiesen ist. Ein solches Vertrauen lässt sich nur durch Transparenz und Nachvollziehbarkeit von Entscheidungswegen und -inhalten feststellen. Daher bieten Modelle wie eine ausschließliche Rechtsaufsicht durch das BMI oder ein Ressortwechsel beispielsweise in das Bundesministerium für Digitales und Verkehr (BMDV) nur begrenzte Vorteile im Hinblick auf diese Transparenz und das damit herzustellende Vertrauen. Auch aufgrund der ressortübergreifenden Aufgaben des BSI und der mittlerweile nahezu alle Lebens- und Arbeitsbereiche betreffenden Relevanz der Cybersicherheit erscheint es deshalb sachgerechter, nach vorangehend geschildertem Befugniszuschnitt den Weg einer selbstständigen obersten Bundesbehörde zu gehen und cybersecurity-irrelevante Befugnisse an andere Ressorts auszulagern. Ob dabei das BSI im begrifflichen Sinne „das BSI“ bleibt, ist eine andere Frage, so könnten durchaus auch cybersicherheitsbezogene Themen aus anderen Behörden und Ministerien in eine solche neue „Behörde für digitale Resilienz“ ausgelagert werden, die auf diese Weise auch besser einer beabsichtigten Zentralstellenfunktion gerecht werden kann. Jedenfalls nicht (mehr) ausreichend sind bloße politische Beteuerungen einer irgendwie gearteten und fachlich nicht näher

[5] So beispielsweise *Herpig*, Die „Unabhängigkeit“ des Bundesamtes für Sicherheit in der Informationstechnik, Stiftung Neue Verantwortung, September 2020, abrufbar unter: https://www.stiftung-nv.de/sites/default/files/snv-unabhaengigkeit_des_bsi_final.pdf oder auch Gesellschaft für Informatik, Stellungnahme des Fachbereichs Sicherheit – Schutz und Zuverlässigkeit – zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0), 9. Dezember 2020, abrufbar unter: https://gi.de/fileadmin/GI/Allgemein/PDF/2020-12-09_Stellungnahme_FB_SICHERHEIT.pdf.

umrissenen „Unabhängigkeit“.[6] Zur genauen Fundierung dieses vorgeschlagenen Ansatzes bedarf es jedoch weitergehender fachlicher Prüfung.

Frage 3:

„Könnten Sie bitte den Begriff der aktiven Cyberabwehr und die unterschiedlichen Stufen und Möglichkeiten der aktiven Cyberabwehr (auch vor dem Hintergrund einer allein defensiv ausgerichteten bzw. einer offensiv ausgerichteten Cyberabwehr) definieren und wo sehen Sie konkrete Defizite im geltenden Recht und in den geltenden Kompetenzen, die einer wirksamen Cyberabwehr entgegenstehen?“

Ein im Jahr 2019 durch den Bayerischen Rundfunk in Teilen öffentlich wiedergegebenes Konzeptpapier der Bundesregierung[7] beschreibt den Vorschlag für ein dezidiertes Vorgehen und ein vierstufiges Durchführungsraster gegen erhebliche Cyber-Angriffe aus dem Ausland. Das Durchführungsraster beschreibt Maßnahmen von unterschiedlicher technischer Intensität: Innerhalb der ersten beiden Stufen soll schadhafter Datenverkehr lediglich blockiert oder umgeleitet werden. Damit verbunden ist somit noch kein digitaler Gegenschlag im Sinne eines „Hackback“. Die dritte Stufe hingegen soll Sicherheitsbehörden dazu ermächtigen, fremde Netze aktiv zu infiltrieren mit dem Ziel, Daten zu verändern oder zu löschen. In der vierten Stufe sollen technische Eingriffsmittel ermöglicht werden, die über den Umgang mit Daten oder Software hinausgehen und auch Hardware betreffen können. In dem Konzeptpapier werden in diesem Zusammenhang Maßnahmen wie das „Eindringen in Systeme“ und das „Herunterfahren“ genannt – diese Gegenmaßnahmen sind jedoch nicht abschließend und können in ihrer Intensität und in ihrem Umfang durchaus darüber

[6] So noch 2017 im Sinne einer „Chinesischen Mauer“ zu ZITiS: *Welchering/Kloiber*, IT-Sicherheitskongress: Experten fordern Meldepflicht für Sicherheitslücken, 20. Mai 2017, abrufbar unter: https://www.deutschlandfunk.de/it-sicherheitskongress-experten-fordern-meldepflicht-fuer-100.html.
[7] *Kipker*, Hackback in Deutschland: Wer, was, wie und warum?, Verfassungsblog, 3. Juni 2019, abrufbar unter: https://verfassungsblog.de/hackback-in-deutschland-wer-was-wie-und-warum/.

hinausgehen. Das Konzeptpapier sieht sodann einen vordefinierten Zuständigkeitsrahmen für die Entscheidungsbefugnis über Maßnahmen der aktiven Cyberabwehr vor. Im Nationalen Cyber-Abwehrzentrum (NCAZ) soll zunächst fachlich beurteilt werden, ob die Voraussetzungen eines „erheblichen Cyber-Angriffs aus dem Ausland“ erfüllt sind, die eine aktive Cyberabwehr zu evozieren geeignet sind. Falls dies bejaht wird, gibt (nach damaligem Stand der Ressortzuordnungen) in einem nächsten Schritt ein Gremium bestehend aus Vertretern des Kanzleramts, des AA, des BMJV, des BMVg und des BMI die politische Bestätigung zur Durchführung der Cyberabwehrmaßnahme. Als Akteure zur Durchführung der Maßnahme werden in dem Konzeptpapier der BND und „Polizeibehörden“ genannt.

Zur politischen, technischen und rechtswissenschaftlichen Debatte um die aktive Cyberabwehr/Hackbacks/digitale Gegenschläge ist zunächst festzustellen, dass es auch hier wie bereits für die Cybersicherheit in der Beantwortung der Fragestellungen 1 und 2 an einem einheitlichen Begriffsverständnis und einer inhaltlichen Vorstellung der Maßnahmen fehlt – und dies muss hier ebenso zwangsläufig zu Problemen in der politischen Einordnung führen. So muss in der Debatte um die Cyberabwehr deutlich zwischen technisch-organisatorischen Maßnahmen unterschieden werden, die zum Alltagsgeschäft eines jedes operativen ISMS gehören und solchen, die inhaltlich (deutlich) darüber hinausgehen und deshalb Ausnahmefälle darstellen. Technische und organisatorische Maßnahmen wie die Blockade oder Umleitung von Datenverkehr stellen keine aktive Cyberabwehr nach dem Verständnis der aktuell geführten rechtspolitischen Debatte dar und sind deshalb befugnisrechtlich unproblematisch. Alle Maßnahmen, die darüber hinausgehen, sind juristisch jedoch anders zu würdigen. Die in dem zuvor vorgestellten Konzeptpapier der Bundesregierung dargestellten Ansätze sind dabei allesamt nicht ausreichend bzw. lassen zentrale Fragen der nationalen Befugnisordnung und damit verbundener gesetzlicher Legitimierung außer Betracht und würden zu einem teils rechtswidrigen Cyber-Einsatz führen. So ist der BND als Auslandsnachrichtendienst für die aktive Cyberabwehr *per se* nicht zuständig, da seine Aufgabe in der

Informationssammlung und Gewinnung von Erkenntnissen liegt, die von außen- und sicherheitspolitischer Bedeutung für Deutschland sind. Auch andere, in diesem Zusammenhang teils für zuständig gehaltene Behörden verfügen im nationalen Rechtsgefüge nicht über die Ermächtigung, IT-Systeme im Ausland aktiv und physisch zu kompromittieren. National allein zuständig für die Durchführung aktiver Cyberabwehr im hier verstandenen Sinne ist die Bundeswehr, die zu diesem Zweck ein eigenes „Kommando Cyber- und Informationsraum“ (KdoCIR) in Dienst gestellt hat und über ein „Zentrum Cyberoperationen“ (ZCO) verfügt. Die Bundeswehr kann verfassungsrechtlich außer zur Verteidigung jedoch nur unter höchst eingeschränkten Voraussetzungen tätig werden. Art. 87a GG bestimmt dazu, dass die Streitkräfte außer zur Verteidigung nur dann eingesetzt werden dürfen, soweit es das Grundgesetz ausdrücklich zulässt. Dieser Ausnahmevorbehalt ist eng auszulegen und betrifft vornehmlich Situationen des inneren Notstands oder überregionale Unglücksfälle. Der Einsatz der Bundeswehr zur aktiven Cyberabwehr setzt folglich einen Verteidigungsfall voraus, und das bedeutet die Reaktion auf eine militärische Gewaltanwendung, die von außen kommt. Offensivmaßnahmen der Bundeswehr im CIR, die nicht unter dieses Selbstverteidigungsrecht fallen, sind völkerrechtswidrig, da sie das Gewaltverbot missachten. Nicht umsonst gehen auch die Überlegungen fehl, allgemein einen NATO-Bündnisfall generell für Cyberattacken anzunehmen, da diese vielfach nicht die Schwelle zu einem bewaffneten Angriff überschreiten. Deutlich geworden ist dies bislang auch während des Russland-Ukraine-Kriegs, der im Wesentlichen nicht als „Cyberwar“ geführt wurde, auch wenn es im Allgemeinen vermehrt zu Bedrohungen für die IT-Sicherheit gekommen ist.

Unabhängig von dieser juristischen Frage stellen sich in technischer Hinsicht evidente Fragen nach der Möglichkeit und Sinnhaftigkeit effektiver Cyberabwehr, so beispielsweise im Hinblick auf die Zurückhaltung von Schwachstellen, Gegenreaktionen („Vergeltungsschlägen“) und der Attibuierbarkeit von Cyberangriffen im digitalen Raum. Insoweit wird auf die entsprechende technische Diskussion verwiesen.

Das führt zu folgender Erkenntnis: Losgelöst von der technischen Diskussion um die Durchführbarkeit und Sinnhaftigkeit von Maßnahmen aktiver Cyberabwehr besteht aktuell kein gesetzgeberischer Handlungsbedarf zu dem Thema, da der Einsatz bloßer passiver technischer Mittel bereits begrifflich keine Cyberabwehr im hier verstandenen offensiven Sinne darstellt und bereits durch geltende Ermächtigungsgrundlagen von Fachbehörden gedeckt wird. Für tatsächliche „Hackback"-Szenarien hingegen wäre die Bundeswehr zuständig, für die der geltende verfassungs- und wehrrechtliche Rahmen einschlägig ist, der ein Tätigwerden im CIR nur in absoluten Ausnahmefällen rechtskonform gestattet.

Frage 4:

„Weitere Instrumente, die der Koalitionsvertrag adressiert, sind etwa auch

- **das Recht auf Verschlüsselung,**
- **ein Schwachstellenmanagement und die Pflicht, Sicherheitslücken zu melden,**
- **die Stärkung der digitalen Souveränität und die Beachtung der Vertrauenswürdigkeit von Unternehmen,**
- **die Vorgaben „security-by-design/default" als Standard,**
- **Stärkung der Produkthaftung und der IT-Sicherheitsforschung,**
- **das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI.**

Welche dieser Maßnahmen sollten mit welcher Priorität ungesetzt werden, wo besteht aus Ihrer Sicht darüber hinausgehender Handlungsbedarf und wo bestehen insbesondere Defizite?"

Eine pauschale Priorisierung der vorgenannten Maßnahmen lässt sich nicht ohne Weiteres vorschlagen, da die unterschiedlichen Instrumente eine jeweils unterschiedliche Relevanz für verschiedene technische, rechtliche und wirtschaftliche Bereiche besitzen. Alle betreffen jedoch die Cybersicherheit in abgestufter

Granularität. Letztlich sollte es (rechts)politisch darum gehen, Deutschland noch weiter als bislang zu einem leistungsfähigen und technologiesouveränen Standort in der Europäischen Union auszubauen. Das bedeutet, dass ein verfassungsrechtlich sowohl in der EU als auch in Deutschland bereits anerkanntes Recht auf Verschlüsselung/verschlüsselte digitale Kommunikation nur in absoluten Ausnahmefällen derogiert werden darf.[8] Überdies darf bei einer nationalen Betrachtung der Cybersicherheit nicht die zunehmende europarechtliche Überformung unberücksichtigt bleiben. Durch den bereits erwähnten europäischen Vorstoß zu einem „Cyber Resilience Act" (CRA) wird Cybersicherheit erstmals als einheitlicher horizontaler Regelungsstandard definiert. Die Überarbeitung der EU-Produkthaftungsrichtlinie aus dem Jahr 1985 bezieht u.a. neue Technologien wie KI und die Verantwortlichkeit für Fehler bei Software-Updates ein. Dieser Ansatz ist folgerichtig, denn nur durch ein größtmögliches Maß an Rechtssicherheit, Transparenz und Nachvollziehbarkeit in der Cybersicherheit kann ein angemessener Innovationsrahmen auch in Deutschland geschaffen werden. Die Anforderungen zu „Security by Design" und „Security by Default" werden somit aktuell bereits auf den Weg gebracht und hierzu gehört denknotwendigerweise auch ein funktionierendes Schwachstellenmanagement und der vertrauensvolle, effektive und effiziente Umgang mit Sicherheitslücken.

Die IT-Sicherheitsforschung sowie die Förderung von offenen Standards können jeweils eine Möglichkeit darstellen, um dringend benötigte nationale und europäische Technologiesouveränität zu fördern. Anzumerken ist jedoch, dass gesetzgeberische Maßnahmen und Forschungsförderung stets nur einen Teilaspekt

[8] Auch ein „Recht auf Verschlüsselung" gilt infolge widerstreitender verfassungsrechtlicher Positionen nicht schrankenlos, ein grundsätzlich legitimierbarer Eingriff ist jedoch äußerst strengen Voraussetzungen unterworfen, die eine anlasslose Massenüberwachung verschlüsselter Kommunikation sowohl auf europäischer wie auch auf nationaler Ebene jedenfalls unzulässig machen. Hierzu im Detail: *Kipker*, Das „digitale Briefgeheimnis": Existiert ein „Recht auf Verschlüsselung" und falls ja, welchen juristischen Rahmenbedingungen unterliegt es? (Arbeitstitel), Rechtsgutachten im Auftrag der Friedrich-Naumann-Stiftung für die Freiheit, im Erscheinen (2023).

darstellen können, um eine nachhaltige und am Markt orientierte Innovation zu schaffen.[9]

Wie bereits bei der Beantwortung dieser Frage zuvor angemerkt wurde, bedingen Innovation und Rechtssicherheit einander. Soweit deshalb in der Frage die „Vertrauenswürdigkeit von Unternehmen" aufgeworfen wird, ist Folgendes festzustellen: Cybersicherheit ist wie der Begriff der „Sicherheitslücke" vornehmlich ein technisch-organisatorisches Thema.[10] Gegenteiligen Auffassungen kann insoweit nicht gefolgt werden, als sie bei Annahme einer legitimierten beliebigen politischen Überformbarkeit cybersicherheitsrelevanter Entscheidungen jegliche Rechtssicherheit und Nachvollziehbarkeit staatlichen Handelns zerstören würden und damit der Cybersicherheit und der Vertrauenswürdigkeit von entsprechenden nationalen Akteuren dauerhaft und nachhaltig Schaden zufügen.[11] Cybersicherheit ist nicht politischer Aktionismus – dies gilt nicht nur für Themen wie die sog. EU „Chatkontrolle", sondern ebenso für die Beurteilung der Vertrauenswürdigkeit von Unternehmen. Soweit derartige Beurteilungen nicht auf fundierten und öffentlich nachweisbaren fachlich-technischen Sachkenntnissen basieren, unterfallen sie nicht der Zuständigkeit des BSI, sondern sind als rein politische Feststellungen der ministeriellen Ägide der Bundesregierung zuzuordnen. Im Rahmen einer Neustrukturierung der nationalen Cybersicherheitsarchitektur sollte dies im Besonderen berücksichtigt werden.

[9] Im Detail dazu *Kipker*, Innovationsgesetzgebung – bessere Digitalisierung durch mehr Regulierung?!, Tagesspiegel Background Cybersecurity, 16. Juni 2022, abrufbar unter: https://background.tagesspiegel.de/cybersecurity/innovationsgesetzgebung-bessere-digitalisierung-durch-mehr-regulierung.

[10] *Kipker*, Alles eine Frage der Perspektive?, Tagesspiegel Background Cybersecurity, 27. Oktober 2022, abrufbar unter: https://background.tagesspiegel.de/cybersecurity/alles-eine-frage-der-perspektive sowie *Kipker*, Der Rechtstaat wird herausgefordert: Die BSI-Warnung vor Kaspersky, MMR 2022, 1031, abrufbar unter: https://rsw.beck.de/cms/?toc=mmr.30&docid=454363.

[11] So aber wohl *Shulman/Waidner*, Wie Deutschland mit nicht vertrauenswürdiger IT besser umgehen kann, F.A.Z., 24. Oktober 2022.

Frage 5:

„Vor dem Hintergrund des hybriden Angriffskrieges Russlands gegen die Ukraine sind erneut Forderungen nach Instrumenten der sogenannten offensiven Cyberabwehr laut geworden. Wie beurteilen Sie diese Forderungen und die Argumentation, offensive Instrumente vermeintlich unterhalb der Schwelle von Hackbacks einzusetzen, im Hinblick auf ihre Recht- und Zweckmäßigkeit?“

Zur Beantwortung dieser Frage wird inhaltlich im Wesentlichen auf die Beantwortung der Frage 3 verwiesen. Zusätzlich ist anzumerken, dass auch der Russland-Ukraine-Krieg nichts an den generell schon vorher bestehenden Bedenken an Maßnahmen des Hackbacks geändert hat – dies sowohl in technischer wie aber insbesondere auch in rechtlicher Hinsicht. Außerdem ist unklar, welches „offensive Instrumente“ sein sollen, die „unterhalb der Schwelle des Hackbacks“ liegen. In der Beantwortung von Frage 3 wurde die mögliche Abstufung und entsprechende rechtliche Würdigung im Detail wiedergegeben. Insoweit dürfte schon fraglich sein, ob technische Instrumente, die unterhalb der Schwelle des Hackbacks angesiedelt sind, überhaupt nach den rechtlichen Maßstäben des Hackbacks zu beurteilen wären oder nicht vielmehr nur den anerkannten operativen Maßnahmen zur Cybersicherheit unterfallen, für die bereits die allgemeinen rechtlichen Grundsätze greifen.

Frage 6:

„Was kann die Bundesrepublik Deutschland in ihrer nationalen und internationalen Cybersicherheitspolitik von anderen Ländern und internationalen best practices konkret lernen, insbesondere im Hinblick auf staatliche Stellen, Governance, verfügbare Instrumente, Fokus und Kapazitäten?“

Von einer Beantwortung dieser Frage wird abgesehen.

Frage 7:

„Welche politischen und rechtlichen Herausforderungen stellen sich bei der Schaffung eines Regelwerks für eine Meldepflicht für Sicherheitslücken (zero days) und einen gesetzlich strukturierten Umgang mit Schwachstellen („wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen“)?“

Ebenso wie die Fragen der Unabhängigkeit des BSI sowie zur rechtlichen Ausgestaltung von aktiver Cyberabwehr wird der gesetzlich strukturierte Umgang mit Schwachstellen bereits seit mehreren Jahren diskutiert. Einen Überblick über den politischen und rechtlichen Stand der Diskussion im europäischen Vergleich gibt der entsprechende Bericht der „European Union Agency for Cybersecurity“ (ENISA) vom 13.04.2022, auf den an dieser Stelle daher verwiesen wird.[12] Mit Blick auf die nationale Situation in Deutschland sei zuvorderst festgestellt, dass der Umgang mit Schwachstellen technisch und rechtlich eng mit den Zielen verknüpft ist, die der Staat nachfolgend im weiteren Umgang mit ermittelten Schwachstellen zu verfolgen gedenkt. Dementsprechend ist ein „wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen“ für die Realisierung effektiver Cybersicherheit wichtig. Zwar hat die technisch-organisatorische Absicherung von IT-Systemen und damit die Cybersicherheit Verfassungsrang, indem sie aus verschiedenen Grundrechten wie z.B. dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität von informationstechnischen Systemen (IT-Grundrecht bzw. Computer-Grundrecht, siehe dazu bereits oben Fn. 3) ableitbar ist. Wie schon für ein Recht auf Verschlüsselung und auf verschlüsselte Kommunikation gilt dieser Schutz aber nicht absolut und ist in einen verfassungsgerechten Ausgleich zu anderen, eventuell entgegenstehenden grundrechtlichen Positionen zu bringen. Überdies gilt eine Besonderheit: Cybersicherheit ist regelmäßig kein abstraktes Schutzziel, sondern verfolgt durch die Aufrechterhaltung der

[12] ENISA, Coordinated Vulnerability Disclosure Policies in the EU, 13. April 2022, abrufbar unter: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.

Funktionsfähigkeit von IT-Systemen und entsprechenden Netzwerken weitere Interessen, die persönlicher oder betriebswirtschaftlicher Art sein können, letztlich aber bis zur Funktionsfähigkeit Kritischer Infrastrukturen reichen können. Daher lässt sich unter Umständen im Rahmen eines Schwachstellenmanagements nicht immer konkret auf Anhieb absehen, welchen Schaden eine eventuell zurückgehaltene Sicherheitslücke tatsächlich anzurichten vermag.

Das Bundesverfassungsgericht hat diese komplexe faktische und damit auch juristische Interessenlage in einem Beschluss aus dem Jahr 2021 zum staatlichen Umgang mit Sicherheitslücken zum Ausdruck gebracht:[13] So bestehe zwar einerseits durchaus eine staatliche Schutzpflicht zur Cybersicherheit, die aber denknotwendigerweise einer weiten Einschätzungsprärogative unterliegen muss. In diesem Sinne verstanden kann es somit als Staat auch verfassungsrechtlich zulässig sein, bislang unbekannte IT-Sicherheitslücken auszunutzen, um z.B. eine Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durchzuführen und somit ein IT-System zu kompromittieren. Hierzu bedürfe es laut des Gerichts aber einer Regelung, die die im Einzelfall widerstreitenden Interessen angemessen in Ausgleich bringt. Das bedeutet, dass die zuständige Behörde für den Fall des Bekanntwerdens einer Zero-Day-Schwachstelle eine Abwägung der konkreten gegenläufigen Belange durchführen muss. Diese Abwägung muss sowohl in qualitativer Hinsicht wie auch in quantitativer Hinsicht erfolgen. Je nachdem, worin diese Einzelfallabwägung resultiert, ist zu entscheiden, ob die Schwachstelle dem Hersteller zu melden oder weiterhin zu Zwecken ihrer Ausnutzung offenzuhalten ist. Diese rechtlichen Erkenntnisse des BVerfG aber sind keineswegs neu oder überraschend, sondern werden in verschiedenen Staaten weltweit in ähnlicher Form

[13] BVerfG, Beschluss des Ersten Senats vom 8. Juni 2021 - 1 BvR 2771/18 -, Rn. 1-74, abrufbar unter: http://www.bverfg.de/e/rs20210608_1bvr277118.html. **In diese Entscheidung des BVerfG ebenfalls einbezogen wird eine juristische Würdigung des Begriffs der „Sicherheitslücke“ nach § 2 Abs. 6 BSIG. Das BVerfG differenziert dabei zwischen N-Day- und Zero-Day-Sicherheitslücken – beiden gemein ist jedoch, dass sie technischer Natur und damit grds. patchbar sind.**

bereits zur Anwendung gebracht, so beispielsweise in den USA.[14] Gleichgültig, wie detailliert, transparent und nachvollziehbar ein solches Verfahren jedoch ausgestaltet ist, wird es in der Praxis letztlich immer mit rechtlichen Unsicherheiten und auch mit entsprechender Kritik an eventuell nicht nachvollziehbaren Entscheidungen verbunden sein – trotz seiner verfassungsrechtlich grundsätzlich bestehenden Legitimationsmöglichkeit, da auch die IT-Sicherheit als Grundrecht nicht schrankenlos gilt.

Im Hinblick auf das IT-SiG 2.0 hat der gesetzlich angeordnete Umgang mit entdeckten Schwachstellen in der Vergangenheit jedoch Verbesserungen erfahren. So schreibt § 7b Abs. 3 BSIG mittlerweile vor, dass wenn durch aktive Detektionsmaßnahmen des BSI Sicherheitslücken oder Sicherheitsrisiken erkannt werden, die Verantwortlichen des betroffenen IT-Systems hierüber unverzüglich zu informieren sind. Aus Sicht der Cybersicherheit wünschenswert wäre zusätzlich eine gesetzlich entsprechende Regelung, die sich ausdrücklich nicht nur auf das Verfahren nach § 7b Abs. 1 BSIG (Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit) bezieht. Ob dies in der Praxis widerstreitender verfassungsrechtlicher Güter – und somit jenseits alleiniger Cybersicherheitsbetrachtungen – möglich und angebracht ist, bedarf näherer Untersuchung und fachlicher Abstimmung.

Jedenfalls steht fest, dass eine stärker als bisher anzustrebende weitergehende institutionelle Unabhängigkeit des BSI sicherlich dazu beitragen dürfte, die Vertrauenswürdigkeit in staatliche CVD-Prozesse signifikant und für die Öffentlichkeit nachvollziehbar kommunizierbar zu verbessern. Bereits jetzt weist die Behörde in ihrer CVD-Richtlinie auf die Vertraulichkeit „innerhalb des gesetzlichen Rahmens“ hin.[15] Wenn wie bereits in der Beantwortung von Frage 1 dargelegt der Begriff „staatlicher

[14] Siehe zur konkreten Ausgestaltung eines staatlichen Schwachstellenmanagements zunächst unabhängig von der rechtlichen Frage *Schulze*, Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie 2019/S 10, 8. Mai 2019, abrufbar unter: https://www.swp-berlin.org/en/publication/governance-von-0-day-schwachstellen#hd-d38399e3160.

[15] Bundesamt für Sicherheit in der Informationstechnik, CVD-Richtlinie, abrufbar unter: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html.

Cybersicherheit“ eine eng gefasste Neudefinition erführe, könnten mit der Cybersicherheit konfligierende Interessen hiervon besser getrennt werden. Der staatliche Umgang mit Schwachstellen wird sich auch in Zukunft praktisch nicht vermeiden lassen, jedoch sollten der Cybersicherheit entgegenstehende Interessen nicht als eine Maßnahme der Cybersicherheit dargestellt werden, wie dies gegenwärtig noch der Fall ist und insbesondere durch die neue Cybersicherheitsagenda perpetuiert wird.

Frage 8:

„Die Bundesregierung hat Eckpunkte eines KRITIS-Dachgesetzes verabschiedet und will dabei insbesondere eine bessere Verschränkung des Schutzes digitaler und physischer Infrastruktur erreichen: Welche organisatorischen und rechtsdogmatischen Ansatzpunkte sind denkbar, um physische und digitale Komponenten kritischer Infrastruktur gemeinsam und kohärent zu regulieren und inwiefern kann der Gesetzgeber hier insbesondere auf geltendem Recht und Regulierungsvorschlägen aus der Vergangenheit (etwa rund um das IT-Sicherheitsgesetz 2.0) aufsetzen?“

Zu dieser Fragestellung ist vorab anzumerken: Der Schutz von Kritischen Infrastrukturen auch in physischer Hinsicht ist nicht erst seit den Ereignissen des Jahres 2022 und dem Beginn des Russland-Ukraine-Kriegs relevant. Das Bundesministerium des Innern (BMI) legte beispielsweise schon am 17. Juni 2009 die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) vor.[16] In diesem Dokument wird bereits auf eine hybride Bedrohungslage abgestellt, die schon seit den Terroranschlägen vom 11. September 2001 in den USA bestand und auch den Sabotageschutz von KRITIS und deren physische Kompromittierung durch terroristische Anschläge betrifft. Diese schon seit Jahren vorhandene Erkenntnis

[16] Bundesministerium des Innern, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 17. Juni 2009, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf.

wird in der aktuellen politischen und medialen Debatte um ein neues KRITIS-Dachgesetz nur unzureichend wiedergegeben.

Darüber hinaus sind weder das BSIG noch das IT-SiG 2.0 als übergreifendes Artikelgesetz KRITIS-spezifische Fachgesetze mit einem Schwerpunkt ausschließlich auf Cybersecurity, sondern regulieren darüber hinaus viele weitere Bereiche der digitalen Souveränität bis hin zum B2C-Segment, wo Cybersicherheit ebenfalls eine Rolle spielt, jedoch grds. ohne jegliche KRITIS-Relevanz ist. Die Annahme zu tätigen, ein KRITIS-Dachgesetz würde nun „spiegelbildlich“ ein für lange Zeit übersehenes und fehlendes „Puzzlestück“ im nationalen KRITIS-Schutz darstellen, geht deshalb inhaltlich fehl.

Selbst die kürzlich vorgestellten „Eckpunkte für das KRITIS-Dachgesetz“ legen nahe, dass bereits zahlreiche fachgesetzliche Regelungen für den nationalen KRITIS-Schutz vorhanden sind. Dies ist auch einleuchtend, denn Kritische Infrastrukturen werden in Deutschland bereits seit Jahrzehnten betrieben und von den bislang zuständigen Fachbehörden betreut und überwacht.

Rechtsdogmatisch haben die IT-Sicherheitsregulierung von Kritischen Infrastrukturen und die Sicherstellung ihres physischen Schutzes vor „analogen“ Bedrohungen deshalb erst einmal nur wenig gemeinsam, da die Regelungen nicht nur unterschiedliche Bedrohungslagen adressieren, sondern auch verschiedener Präventiv- und Abwehrmaßnahmen bedürfen, aufgefächerte behördliche Zuständigkeiten vorhanden sind und die Vorgaben deshalb in unterschiedlichen fachgesetzlichen Vorschriften geregelt sind. Deshalb kann ein KRITIS-Dachgesetz nur ein weiteres Omnibus- bzw. Artikel-Gesetz sein, das die Bestandgesetze zum physischen KRITIS-Schutz bei festgestellten Defiziten und Schwachstellen ergänzt, nicht aber komplett neue und weitere Verantwortlichkeiten schafft, die bestenfalls noch zusätzlich unter die „Cybersicherheit im weitesten Sinne“ gefasst werden. Eine solche begriffliche Überdehnung wäre fatal, da sie zwangsläufig eine nahezu vollständige Konturlosigkeit der nationalen Cybersicherheitsarchitektur zur Folge hätte. Das KRITIS-Dachgesetz soll und darf somit nicht pauschal auf dem IT-SiG 2.0 aufsetzen,

sondern sich ausschließlich an den inhaltlichen Regelungslücken bestehender Fachgesetze orientieren. Auf diese Weise kann es regulatorisch nicht nur möglichst schlank gehalten und gesetzgeberisch (auch infolge der aktuellen Bedarfslage) möglichst schnell umgesetzt werden, sondern auch die Betreiber können die Umsetzung in ihre gewohnten und etablierten Strukturen und Prozesse einbringen. In jedem Falle zu vermeiden ist eine zunehmend ausufernde Überbürokratisierung angedockt an die Cybersicherheit, wie sie durch die Eckpunkte für das KRITIS-Dachgesetz nach gegenwärtigem Stand offensichtlich verfolgt wird. Es erschließt sich in diesem Zusammenhang auch keineswegs, weshalb das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu einer „übergreifenden" Behörde ausgebaut werden soll und bisher zuständige Aufsichtsbehörden nur „gegebenenfalls" hinzuzuziehen sind. Falls ein solcher Bedarf dennoch bestehen sollte, ist zuvorderst qualifiziert nachzuweisen, inwieweit sich die aktuelle Bedrohungslage beispielsweise von den in der Vergangenheit bereits vorhandenen Bedrohungen für KRITIS signifikant unterscheidet und wie eine neue Dachbehörde ein effektives und effizientes Instrument sein kann, um dieser neuen Bedrohungslage Herr zu werden.

Frage 9:

„Mit Blick auf Redundanzen in der Kommunikationsinfrastruktur der Deutschen Bahn könnte das Netzwerkprotokoll TCP/IP als Rückfallebene bei etwaigen Sabotageakten verwendet werden. TCP/IP müsste dabei aber nicht über Mobilnetze, sondern kabelgebunden verwendet werden. Dafür müsste die DB-Netze ein kleines Matrix-Netz an den Knoten aufbauen, das bspw. mit der Kabelinfrastruktur einzelner Netzbetreiber verbunden ist. Dann läuft das System weiter, auch wenn die Infrastruktur punktuell beschädigt, oder zerstört würde. Was könnten Gründe dafür sein, dass ein solches Matrix-Netz nicht bereits existiert?"

Von einer Beantwortung dieser Frage wird abgesehen.

Frage 10:

„Wenn in Deutschland entscheidende Bestandteile für kritische Infrastrukturen (KRITIS) beschafft werden – etwa für Telekommunikationsnetzwerke –, dann können Produzenten unter bestimmten Bedingungen davon ausgeschlossen werden. Die Hürden hierfür sind jedoch hoch. So kann dies erst nach wiederholten Verstößen gegen die Vertrauenswürdigkeit geschehen (bspw. wenn ein Hersteller falsche Angaben gemacht hat, Sicherheitsüberprüfungen nicht unterstützt oder IT-Schwachstellen nicht unverzüglich meldet und beseitigt). Sehen Sie in Anbetracht der sog. „Zeitenwende" Anlässe den geltenden Rechtsrahmen zu verschärfen (etwa in einem IT-Sicherheitsgesetz 3.0) und, falls ja, wie?"

Die Fragestellung nimmt Bezug auf die Untersagungsbefugnis für den Einsatz kritischer Komponenten gem. § 9b BSIG, im Gesetzgebungsverfahren zum IT-SiG 2.0 stand hier noch der Schutz sog. „KRITIS-Kernkomponenten" im Mittelpunkt. Ob es sich – wie in der Frage dargestellt – um eine „Zeitenwende" handelt oder ob es vielmehr um eine Entwicklung geht, die sich bereits seit mehreren Jahren deutlich abzeichnet, sei dahingestellt. Fraglich jedenfalls ist, ob eine vornehmlich politische Regelung wie § 9b BSIG nachhaltig in der Lage ist, für ein höheres Niveau der Cybersicherheit in Deutschland prominent Sorge zu tragen. Bereits im gesetzgeberischen Prozess zum IT-SiG 2.0[17] war die Vorschrift hoch umstritten, da durch sie die konfliktgeladene politische Debatte um die vielzitierte „digitale Souveränität" ohne Weiteres in eine gesetzliche Vorschrift übertragen wird, ohne an den tatsächlichen technischen Verhältnissen und Möglichkeiten nachhaltig etwas zu verändern[18]. Überdies ermöglicht die Vorschrift des § 9b BSIG den Ausschluss von Herstellern bzw. Produzenten kritischer

[17] *Kipker*, Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0), 2. Dezember 2020, abrufbar unter: https://intrapol.org/wp-content/uploads/2020/12/Dennis-Kenji-Kipker-Universitaet-Bremen-Stellungnahme-IT-SiG-2.0.pdf.
[18] So jüngst noch DER SPIEGEL, Abhängigkeit von China: Deutschland setzt bei 5G verstärkt auf Huawei-Technik, 17. Dezember 2022, abrufbar unter: https://www.spiegel.de/wirtschaft/5g-deutschland-setzt-verstaerkt-auf-huawei-technik-a-9e272b10-fa73-4c0b-855f-20fc1224e789.

Komponenten nur als *ultima ratio* – vorrangig steht die Untersagungsbefugnis des BMI für den Einsatz der kritischen Komponente selbst, soweit eine Vorabprüfung Sicherheitsbedenken für die öffentlichen Interessen der Bundesrepublik Deutschland ergibt. Dabei zu berücksichtigen sind bereits und vorrangig herstellerrelevante Fragestellungen wie beispielsweise die unmittelbare oder mittelbare Kontrolle durch eine Regierung oder durch die Streitkräfte eines Drittstaates sowie eine potenzielle Beteiligung des Herstellers an Aktivitäten, die den sicherheitspolitischen Zielen Deutschlands entgegenstehen. Die Vertrauenswürdigkeit des Herstellers kann gesetzlich überdies dann beeinträchtigt sein, wenn er bestimmte Transparenz- und Mitwirkungspflichten nicht erfüllt, seine Produkte schadhafte technische Eigenschaften aufweisen oder ihm Böswilligkeit in seinem Handeln unterstellt werden kann. In diesem Rahmen kann das BMI letztlich nicht nur den weiteren Einsatz aller kritischen Komponenten desselben Herstellers untersagen, sondern in schwerwiegenden Fällen einer nicht (mehr) gegebenen Vertrauenswürdigkeit den Einsatz aller kritischen Komponenten des Herstellers untersagen. Dies kommt im Ergebnis einem faktischen Verbot des Herstellers im KRITIS-Umfeld gleich.

Wenn die Fragestellung nun darauf verweist, dass die „Hürden“ hierfür „hoch“ sind, so muss dies relativiert werden, denn die gesetzlichen Regelungen lassen dem BMI als ausführender Behörde durchaus weitgehende Auslegungs- und Interpretationsspielräume, um zu einem Herstellerverbot für kritische Komponenten zu gelangen. Da hiermit gleichzeitig auch ein erheblicher Einschnitt in die ggf. grundrechtlich geschützten Interessen auch des Herstellers verbunden ist, wäre eine weitere Absenkung der gesetzlichen Schwellen und damit eine pauschale Erweiterung des behördlichen Handlungsrahmens unverhältnismäßig. Berücksichtigt werden muss außerdem, dass sich sowohl die rechtspolitische Debatte um den § 9b BSIG wie auch um das Verbot bzw. die Limitierung des Einsatzes ausländischer Hersteller bislang auf wenige und ausgewählte Unternehmen bezogen hat, die in die öffentliche Wahrnehmung in Deutschland bereits flächendeckend Eingang gefunden haben.

Nicht zuletzt handelt es sich bei der Vorschrift nach § 9b BSIG vorwiegend um eine politische Prüfbefugnis. Wie bereits an anderer Stelle in dieser Stellungnahme im Rahmen der Beantwortung von Frage 2 angemerkt wurde, ist die Vorschrift im BSIG systemfremd, weil sie allerhöchstens mittelbar Fragen der Cybersicherheit, und vorrangig politische Fragen (unzureichender) digitaler Souveränität in Deutschland adressiert, die sich technisch und faktisch nur schwer überprüfen lassen. Außerdem wird das BMI und nicht das BSI als handelnder Akteur in den Mittelpunkt gestellt. Empfohlen wird deshalb – beispielsweise im Rahmen eines IT-SiG 3.0 – die Schwellen für das Verbot eines Einsatzes kritischer Komponenten nicht pauschal abzusenken, sondern stärker als bislang im Gesetzestext ausgeführt zwischen rein sicherheitspolitischen Erwägungen (dann BMI) und technischen Prüfungen und Anforderungen (dann BSI) zu diversifizieren, um zu nachvollziehbareren, transparenteren und öffentlich besser kommunizierbaren Entscheidungsergebnissen zu gelangen.

Im Jahr 2022 hat sich bereits die Verwendung von § 7 BSIG („Warnungen“) aus vornehmlich politischen Erwägungen heraus als rechtlich im Mindesten äußerst fragwürdig erwiesen.[19] Mit der seinerzeit durch das BSI vorgelegten inhaltlichen Begründung wäre eigentlich § 9b BSIG anstelle von § 7 BSIG der juristisch korrekte Handlungsrahmen gewesen. Indem jedoch eine rechtlich unzulässige Vermengung von technischer und geopolitisch-strategischer Argumentation durch das BSI stattgefunden hat, wurde der nachweislich technische Begriff der „Sicherheitslücke“[20] rechtsfehlerhaft perpetuiert überdehnt, womit – falls keine Korrektur stattfindet – der Rechtsunsicherheit Tür und Tor geöffnet

[19] Tagesschau, Schwierige Warnung vor Kaspersky, 5. August 2022, abrufbar unter: https://www.tagesschau.de/investigativ/br-recherche/software-kaspersky-sicherheit-warnungen-101.html.

[20] *Kipker*, Alles eine Frage der Perspektive?, Tagesspiegel Background Cybersecurity, 27. Oktober 2022, abrufbar unter: https://background.tagesspiegel.de/cybersecurity/alles-eine-frage-der-perspektive. Dazu im Detail in Kürze auch *ders.*, MMR Ausgabe 2/2023, im Erscheinen. Zur Auslegung von § 7 BSIG siehe auch *Kipker/Reusch/Ritter*, Recht der Informationssicherheit, § 7 BSIG. In diesem Sinne auch BVerfG, Beschluss des Ersten Senats vom 8. Juni 2021 - 1 BvR 2771/18 -, Rn. 7, abrufbar unter: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html.

wäre und die technisch durchaus sinnvolle Vorschrift des § 7 BSIG in der Anwendungspraxis entwertet wird, indem staatlichen Einrichtungen wie dem BSI jederzeit der Vorwurf gemacht werden könnte, aus diesem oder jenem politischen Motiv heraus nicht rechtzeitig vor ausländischen Produkten und Diensten gewarnt zu haben, wie es eigentlich eine Maßnahme staatlicher Schutzpflicht zur IT-Sicherheit gewesen wäre. So wäre es nach derzeitigem Auslegungsstand des § 7 BSIG durchaus konsequent, sowohl vor chinesischen, russischen, US-amerikanischen, israelischen und im Zweifelsfall auch indischen Digitalprodukten und Diensten im Generellen und nicht nur herstellerbezogen zu warnen – allein schon deshalb, weil diese Staaten umfassende Geheimdienstaktivitäten verfolgen, vielfach keine flankierenden und ausreichenden rechtlichen Schutzmechanismen besitzen, eine staatliche oder gar militärische Kontrolle von dort angesiedelten Unternehmen nicht zweifelsfrei ausgeschlossen werden kann und die Staaten teilweise schon nachweislich in Aktivitäten zur Kompromittierung von IT-Systemen auch in Deutschland beteiligt gewesen sind bzw. über entsprechende flächendeckende globale Überwachungsprogramme verfügen. Eine solche „Generalwarnung“ hat bislang aber nicht stattgefunden und belegt damit deutlich das juristische Defizit und das Transparenzdefizit, das mit operativen politischen Cybersicherheitsbefugnissen verbunden ist und die im Ergebnis deshalb nicht zu einer nachhaltigen Förderung der nationalen Cybersicherheit beitragen können.

Frage 11:

„Wie bewerten Sie die Lage von IT-Fachkräften – insbesondere für Cybersicherheit – auf dem Arbeitsmarkt und was müssten staatliche (Sicherheits)-Behörden verbessern, um noch mehr kompetente IT-Fachkräfte zu gewinnen?“

Von einer Beantwortung dieser Frage wird abgesehen.

Frage 12:

„Wie könnte die Ausbildung von IT-Cyberfachkräften sowohl in quantitativer als auch in qualitativer Hinsicht in Deutschland weiter verbessert werden?“

Aus juristischer Warte soll an der Stelle dieser Frage ein zusätzlicher und zentraler Aspekt angesprochen werden, der in der bisherigen akademischen und ausbildungsbezogenen Debatte um Cybersicherheit weitestgehend vernachlässigt wurde: Cybersicherheit ist gerade in der unternehmerischen Praxis eine erhebliche Compliance-Frage, die aufgrund von vertraglichen Beziehungen und Haftungsansprüchen einerseits Außenwirkung entfalten kann, andererseits aber auch unternehmensintern von zentraler Bedeutung ist, um betriebliche und personelle Schädigungen zu vermeiden. Daher sind regelmäßig auch Jurist:innen mit der rechtlichen Bewertung cybersicherheitsrelevanter Fragestellungen befasst. Für diese rechtliche Bewertung ist jedoch auch entsprechendes technisches Know-how vonnöten, das vielfach nicht vorhanden ist und nach wie vor auch nicht Gegenstand der klassischen juristischen Ausbildung ist. Daher sollte bei einer Betrachtung der Ausbildungslage von „IT-Cyberfachkräften“ nicht nur das Augenmerk auf die technisch-informatischen Ausbildungsgänge, sondern ebenso verstärkt auf juristische Berufsfelder gelegt werden. Denkbar ist beispielsweise, angehenden Jurist:innen nach Abschluss ihres LL.B. oder des Ersten Juristischen Staatsexamens die Möglichkeit zu eröffnen, technisch-informatische Studiengänge nach Ablegung eines Vorkurses oder mit speziell auf sie zugeschnittenem Curriculum im Sinne eines technischen Aufbaustudienganges zu Cybersicherheit speziell für juristische Berufsfelder zu studieren.[21] Derzeitige Studiengänge sind in der gegenwärtigen juristischen Ausbildungslandschaft in Deutschland jedoch trotz ihres Bedarfes noch nicht vorhanden und es wäre daher wünschens- und unterstützenswert, die Einrichtung derartiger interdisziplinärer Ausbildungsangebote deutlich stärker

[21] *Eren/Kipker*, Konzept für einen berufsbegleitenden Studiengang M.Sc. in Cybersecurity Management for Lawyers, 2022 (hochschulinternes Konzeptpapier).

als bislang zu fördern und in den akademischen Alltag zu integrieren.

Frage 13:

„Wie bewerten Sie die vorhandenen technischen Fähigkeiten in Deutschland für eine wirksame Cyberabwehr – auch mit aktiven Cyberabwehr-Instrumenten?“

Von einer technischen Beantwortung dieser Frage wird abgesehen. Im Übrigen wird für die rechtlichen und institutionellen Aspekte der Fragestellung auf die Ausführungen zur Beantwortung der Frage 3 verwiesen.

Frage 14:

„Welche Rolle spielen private Cybersicherheits-Unternehmen für eine effektive staatliche Cyberabwehr im internationalen Vergleich?“

Von einer Beantwortung dieser Frage wird abgesehen.

Frage 15:

„Inwieweit sind aus technischer Sicht sog. Software-Schwachstellen (nicht gemeint sind spezifische IT-Schnittstellen für Sicherheitsbehörden, wie sie z. B. derzeit im Rahmen des 3GPP-Gremiums für den künftigen 6G-Mobilfunkstandard unter Beteiligung von ZITiS und Cyberagentur entwickelt werden) erforderlich, um Sicherheitsbehörden Zugriff auf Kommunikationsendgeräte im Rahmen von Strafermittlungen zu verschaffen oder gibt es mittlerweile hinreichend wirksame Technologien, wie z. B. kryptographische Verfahren, die weniger Kollateralschäden aufweisen und inwieweit ist diese Schwachstellen-Diskussion auf mittlere Sicht hinfällig, wenn wir an Entwicklungen wie Quantenkommunikation denken?“

Von einer Beantwortung dieser Frage wird abgesehen.

Frage 16:

„Wie sollte ein Schwachstellen-Management technisch, personell und organisatorisch aufgesetzt werden, sind dafür z. B. Risiko Management-Standards als ein Vorbild denkbar und welche Ziele kann sich ein Schwachstellen-Management setzen, angesichts von über 20.000 Software-Schwachstellen, wie sie zuletzt der BSI-Lagebericht festgestellt hat und inwieweit ist für die Konzeptionierung und Implementierung eines solchen Schwachstellen-Managements tatsächlich ein unabhängiges BSI zwingend erforderlich?“

Im Hinblick auf die Unabhängigkeit des BSI und den Anforderungen an ein Schwachstellen-Management unter rechtlichen Gesichtspunkten wird zur Beantwortung dieser Frage auf die Fragestellungen 1, 2 und 7 verwiesen.

Frage 17:

„Anhand welcher Maßnahmen und/oder Methoden kann das Sicherheitsverständnis und -verhalten von IT-Nutzer*innen effektiv in den Mittelpunkt gerückt, eine höhere IT-Sicherheitskultur aufgebaut und das individuelle Vertrauen in die digitale Umgebung gestärkt werden?“

Alljährlich veröffentlicht das Hasso-Plattner-Institut (HPI) aus Potsdam eine Auflistung der beliebtesten Passwörter des jeweiligen Jahres in Deutschland.[22] Alle Jahre wieder tritt dabei deutlich zutage, dass eine erhebliche Zahl an Bürger:innen auf leicht zu erratende Standardpasswörter setzt, um ihre (personenbezogenen) Daten zu schützen. Überdies belegt der nach wie vor stattfindende erhebliche Zuwachs an erfolgreichen Ransomware- und Phishing-Vorfällen, dass vielen Anwender:innen bereits grundlegende Kenntnisse in der Cybersicherheit fehlen. Soweit daher die Cybersicherheit in Deutschland flächendeckend für die IT-

[22] Für das Jahr 2022: HPI, Die beliebtesten deutschen Passwörter 2022, 19. Dezember 2022, abrufbar unter: https://hpi.de/pressemitteilungen/2022/die-beliebtesten-deutschen-passwoerter-2022.html.

Nutzer:innen sowohl im privaten wie im beruflichen sowie im wirtschaftlichen und behördlichen Kontext verbessert werden soll, müssen Kenntnisse über die Standardmaßnahmen der Cybersicherheit effektiver als bislang vermittelt werden und auch in der Breite der Bevölkerung angelangen. Initiativen wie „Deutschland sicher im Netz“ (DsiN) und das „BSI für Bürger“ stellen in diesem Sinne sicherlich sinnvolle Maßnahmen dar, können aber nicht ausreichend sein. Im Hinblick auf die föderale Architektur der Cybersicherheit als Aufgabe der Gefahrenabwehr sind vor allem auch die einzelnen Länder (teils deutlich) stärker als bisher gefordert, nicht nur zum Schutz der eigenen Verwaltung und von großen Wirtschaftsbetrieben tätig zu werden, sondern Aufklärungsmaßnahmen zur Cybersicherheit auf transparente, verständliche und realistisch umsetzbare Weise an die allgemeine Bevölkerung vor Ort zu vermitteln. Diese Anforderung sollte daher in die jeweiligen Landes-Cybersicherheitsstrategien explizit aufgenommen werden, soweit bislang noch nicht geschehen.[23] Für Bürger:innen muss auch in den jeweiligen Ländern eine zentrale Anlaufstelle in Sachen Cybersecurity vorgehalten werden, die einerseits proaktiv informiert, andererseits in Notfällen als direkter Ansprechpartner zur Verfügung steht und an die richtigen Institutionen und Akteure vor Ort verweist, was das notwendige Maß an Vertrauen in eine solche Einrichtung als Maßnahme des „digitalen Bürgerschutzes“ voraussetzt. Zur Vermeidung von und zur Vorbereitung auf Cybervorfälle gehören überdies regelmäßige Informationsangebote in Betrieben und Behörden, um ein dringend benötigtes einheitliches Grundniveau an Cybersicherheit herzustellen.

Anforderungen wie „Security by Design“ und „Security by Default“, die gegenwärtig außerhalb des vertraglichen Rahmens breitenwirksam durch den grds. begrüßenswerten europäischen Entwurf für einen „Cyber Resilience Act“ (CRA)[24] adressiert werden,

[23] So auch beschrieben in der „Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien“ der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz.

[24] Zum EU-Kommissionsentwurf für einen CRA im Detail *Kipker*, Resilienz für alle(s)?! – Der Entwurf des neuen Cyber-Reslience-Act (CRA) der EU-Kommission liefert einen Rundumschlag in Sachen „Cybersecurity by Design“, <kes> Zeitschrift für Informations-

können ebenso dazu beitragen, die allgemeine Cybersicherheit von Anwender:innen zu unterstützen, indem sie leicht umsetzbare und vorkonfigurierte IT-Lösungen zur Verfügung stellen und die Update-Prozesse von OS und Software stärker als bislang automatisieren.

Frage 18:

„Wer bzw. was muss alles in den Blick genommen werden, wenn wir über Zuständigkeiten und Instrumente zur Verbesserung der IT-Sicherheit nachdenken, wo liegen die jeweiligen Defizite sowie Verbesserungsmöglichkeiten und wie bewerten Sie die Effektivität aktueller Informations- und (Weiter-)Bildungsmaßnahmen?“

Zur Teilfrage der Effektivität von bisherigen Informations- und Weiterbildungsmaßnahmen in der Cybersicherheit wird auf die ausführliche Beantwortung von Frage 17 verwiesen.

Abschließend sei zur Beantwortung der Frage 18 darauf hingewiesen, dass sich sowohl die nationale wie auch die europäische Digitalregulierung in den letzten Jahren potenziert haben. Dies ist einerseits den bahnbrechenden Entwicklungen digitaler Vernetzung und damit einhergehenden neuen Geschäftsmodellen und technischen Möglichkeiten geschuldet, andererseits auch auf das damit einhergehende Entstehen neuer und immer zahlreicher werdender Angriffsvektoren zurückzuführen. Wo Regulierung als „Leitplanke“ für die Cybersicherheit grds. sinnvoll ist, muss im Hinblick auf die strategische Ausrichtung der nationalen und europäischen Cybersicherheitsarchitektur auch beachtet werden, dass Cybersicherheit im unternehmerischen wie im behördlichen Kontext nur eine – wenn auch vergleichsweise wichtige – Teilaufgabe des täglichen Pflichtenkatalogs darstellt.[25] Daher bedarf es wie bereits an verschiedenen Stellen innerhalb dieser

Sicherheit, Ausgabe Nr. 5/2022, 6. Siehe zur Darstellung des CRA aktuell außerdem *Chiara*, The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements, International Cybersecurity Law Review 3, 255-272 (2022).

[25] Siehe dazu auch *Von dem Bussche*, in: Kipker (Hrsg.), Rechtshandbuch Cybersecurity, S. 115 ff.

schriftlichen Stellungnahme festgestellt wurde einerseits klarer Regelungsziele und entsprechender Maßnahmen zur möglichst flächendeckenden Verbesserung der Cybersicherheit im eng verstandenen Sinne, andererseits jedoch müssen durch den Gesetzgeber auch Regulierungsgrenzen gezogen und anerkannt werden, denn sowohl Cybersicherheit, als auch digitale Resilienz und digitale Souveränität lassen sich nicht in unlimitiertem Maßstab durch Gesetze und Behördenhandeln herstellen. Sowohl die aktuelle nationale Cybersicherheitsstrategie wie auch die durch das BMI im Jahr 2022 vorgelegte nationale Cybersicherheitsagenda werden diesen Anforderungen bei Weitem nicht durchgängig gerecht, indem sie zunehmend die Vollregulierung des digitalen Raums bei nur beschränkter tatsächlicher Durchsetzungsmöglichkeit erstreben. Auch zeigen sich im europäischen und nationalen Rahmenwerk zur Digitalregulierung immer mehr Wertungswidersprüche und teils auch behördliche Doppelzuständigkeiten, denen in vorgelagerten gesetzgeberischen Prozessen nicht immer ausreichend Beachtung geschenkt wurde. Deshalb sollte sich eine weitergehende und zukunftsgerechte Cybersecurity-Regulierung stets vor Augen führen, ob eine bestimmte, vorgeschlagene Maßnahme auch in ihrer praktischen Anwendung tatsächlich zu einer signifikanten Verbesserung des *status quo* beitragen kann oder lediglich politische Zuständigkeiten neu definiert, erweitert oder verschiebt.