20. Wahlperiode

Deutscher Bundestag
Ausschuss für Digitales

Wortprotokoll
der 27. Sitzung

Ausschuss für Digitales
Berlin, den 25. Januar 2023, 14:00 Uhr
10117 Berlin, Adele-Schreiber-Krieger-Str. 1
Sitzungssaal: MELH 3.101

Vorsitz: Tabea Rößner, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 03**

Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland

Liste der Sachverständigen
Ausschussdrucksache SB20(23)13 NEU

Fragenkatalog

Ausschussdrucksache SB20(23)14

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
SPD	Becker, Dr. Holger	Bartz, Alexander
	Kassautzki, Anna	Diedenhofen, Martin
	Klüssendorf, Tim	Esken, Saskia
	Marvi, Parsa	Hakverdi, Metin
	Mesarosch, Robin	Kaiser, Elisabeth
	Mieves, Matthias David	Leiser, Kevin
	Schätzl, Johannes	Müller (Chemnitz), Detlef
	Wagner, Dr. Carolin	Papendieck, Mathias
	Zimmermann, Dr. Jens	Peick, Jens
	Zorn, Armand	Schneider, Daniel
CDU/CSU	Biadacz, Marc	Bär, Dorothee
	Brandl, Dr. Reinhard	Hahn, Florian
	Durz, Hansjörg	Hauer, Matthias
	Hoppermann, Franziska	Heilmann, Thomas
	Jarzombek, Thomas	Henrichmann, Marc
	Kemmer, Ronja	Metzler, Jan
	Reichel, Dr. Markus	Müller, Florian
	Santos-Wintz, Catarina dos	Schön, Nadine
	Zippelius, Nicolas	Steiniger, Johannes
BÜNDNIS 90/DIE GRÜNEN	Außendorf, Maik	Bär, Karl
	Bacherle, Tobias B.	Christmann, Dr. Anna
	Gelbhaar, Stefan	Grützmacher, Sabine
	Khan, Misbah	Klein-Schmeink, Maria
	Rößner, Tabea	Notz, Dr. Konstantin von
FDP	Funke-Kaiser, Maximilian	Föst, Daniel
	Mordhorst, Maximilian	Höferlin, Manuel
	Redder, Dr. Volker	Konrad, Carina
	Schäffler, Frank	Kruse, Michael
AfD	Lenk, Barbara	Höchst, Nicole
	Schmidt, Eugen	König, Jörn
	Storch, Beatrix von	Naujok, Edgar
		Wiehle, Wolfgang
DIE LINKE.	Domscheit-Berg, Anke	Pau, Petra
	Sitte, Dr. Petra	Reichinnek, Heidi
fraktionslos	Cotar, Joana	

Tagesordnungspunkt 1

Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland

Die Vorsitzende **Tabea Rößner**: Ich möchte die öffentliche Anhörung zum Thema "Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland" eröffnen. Als erstes begrüße ich die Ausschussmitglieder ganz herzlich. Auch die Vertreterinnen und Vertreter der Bundesregierung und der Bundesländer, die an der Sitzung teilnehmen, heiße ich herzlich willkommen. Das Bundesministerium des Innern und für Heimat wird durch den Parlamentarischen Staatssekretär Johann Saathoff und Herrn Abteilungsleiter Andreas Könen vertreten, herzlich willkommen.

Diese Sitzung ist öffentlich und wird live im Parlamentsfernsehen und im Internet übertragen. Ich begrüße daher alle Zuschauerinnen und Zuschauer, die uns hier im Saal auf der Tribüne und virtuell zuschauen. Ich freue mich, dass unsere Arbeit auf so großes Interesse stößt. Ich begrüße ebenfalls die geladenen Sachverständigen hier im Saal:

- Ammar Alkassar,
  ehemaliger Bevollmächtigter für Innovation und Strategie und CIO des Saarlandes

- Manuel Atug,
  Gründer und Sprecher AG KRITIS

- Dr. Annegret Bendiek,
  Lehrstuhlvertretung an der Universität Osnabrück "Europäische Studien",
  Stellvertretende Forschungsgruppenleiterin EU/Europa, SWP Projektleitung "European Repository on Cyber Incidents"

- Dr. Stefanie Frey,
  Geschäftsführerin Deutor Cyber Security Solutions GmbH

- Dr. Sven Herpig,
  Leiter für Internationale Cybersicherheitspolitik, Stiftung Neue Verantwortung e. V.

- Prof. Dr. Dennis-Kenji Kipker,
  Professor für IT-Sicherheitsrecht, Hochschule Bremen, Fakultät für Elektrotechnik und Informatik

- Prof. Dr. Martina Angela Sasse,
  Professorin und Lehrstuhlleitung Menschzentrierte IT Sicherheit, Ruhr-Universität Bochum, Fakultät Informatik

- Julia Schuetze,
  Projektleiterin Internationale Cybersicherheitspolitik,
  Stiftung Neue Verantwortung e.V.

- Prof. Ulrich Kelber,
  Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)

- Dr. Gerhard Schabhüser,
  Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Zum Ablauf der Sitzung: Die Sachverständigen sind gebeten, zu Beginn ein fünfminütiges Eingangsstatement abzugeben. Dann erhält jede Fraktion ein Zeitfenster von fünf Minuten für Fragen und Antworten. Die Sachverständigen antworten unmittelbar innerhalb dieser fünf Minuten. Sie brauchen nicht darauf zu warten, dass ich Ihnen das Wort erteile.

Die Reihenfolge in der Fragerunde ergibt sich aus der Stärke der Fraktionen. Bei jeder weiteren Fragerunde lege ich als Vorsitzende die Reihenfolge entsprechend den Vorgaben unserer Geschäftsordnung fest. Die Redezeit pro Runde wird bei Bedarf verkürzt, da im direkten Anschluss noch die reguläre Sitzung unseres Ausschusses folgt und wir daher zeitlich limitiert sind.

Es gibt einen gemeinsamen Fragenkatalog, den die Fraktionen erstellt haben. Dieser wurde als Ausschuss-Drucksache mit der Nummer SB20(23)14 verteilt und veröffentlicht. Alle abgegebenen schriftlichen Stellungnahmen der Sachverständigen wurden auf der Internetseite des Ausschusses veröffentlicht. Es wird ein Wortprotokoll über die Sitzung angefertigt und die Anhörung wird auf Kanal 3 live im Parlamentsfernsehen gestreamt und ist

anschließend über die Online-Mediathek des Bundestages abrufbar.

Die Besucherinnen und Besucher auf der Tribüne im Saal möchte ich darauf hinweisen, dass – auch wenn diese Sitzung öffentlich ist – das Anfertigen von Bild- und Tonaufnahmen während der Sitzung nicht zulässig ist. Entsprechende Geräte sind daher abzuschalten. Zuwiderhandlungen können nach dem Hausrecht des Deutschen Bundestages nicht nur zu einem dauerhaften Ausschluss von den Sitzungen dieses Ausschusses sowie des ganzen Hauses führen, sondern auch strafrechtliche Konsequenzen nach sich ziehen.

Einige Hinweise zum technischen Verfahren. Die Bitte an die Sachverständigen, die sich virtuell beteiligen: Achten Sie bitte darauf, dass Sie nach den Redebeiträgen auch das Mikrofon wieder ausschalten. Sollten Sie technische Probleme haben oder etwas anmerken wollen, so nutzen Sie gerne die Chat-Funktion. Die im Saal Anwesenden bitte ich, das Saalmikrofon zu nutzen und dieses ebenfalls nach den Redebeiträgen auszuschalten sowie die Mikrofone aller Ihrer mitgebrachten Geräte auszuschalten.

Das Thema der heutigen Sachverständigenanhörung ist „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“. Die Cyberkriminalität hat in den vergangenen Jahren stark zugenommen. Das Bundesamt für Sicherheit in der Informationstechnik legt jährlich einen Bericht zur Lage der IT-Sicherheit in Deutschland vor und gibt einen Überblick über die Bedrohungen im Cyber-Raum. Für das Jahr 2022 wird im Bericht auch die IT-Sicherheitslage im Kontext des russischen Angriffskrieges auf die Ukraine bewertet. Ransomware-Angriffe stellten demnach eine der Hauptherausforderungen und Hauptbedrohungen für Staat, Wirtschaft und Gesellschaft dar. Insgesamt hat sich im Berichtszeitraum die bereits zuvor schon angespannte Lage noch weiter zugespitzt.

Staaten, Behörden, Wirtschaftsunternehmen und Privatpersonen können Opfer von Cyberkriminalität werden. Die Angriffe in den vergangenen Monaten haben uns vor Augen geführt, wie verletzlich unsere Gesellschaft ist. Cyberangriffe gegen Deutschland werden mit dem Ziel durchgeführt, die kritischen Infrastrukturen gezielt anzugreifen, um die Versorgung der Gesellschaft mit Energie, Telekommunikation, Gesundheitsversorgung, Verkehr oder Finanzen lahm zu legen.

Der durch Cyberangriffe verursachte Schaden ist groß. Neben den wirtschaftlichen Folgen können Cyberangriffe unsere demokratischen Grundlagen beeinträchtigen und schwächen. Desinformations- und Fehlinformationskampagnen in den sozialen Medien haben deutlich zugenommen. Sie sollen die Menschen verunsichern und greifen in den freien Meinungsbildungsprozess ein.

Informations- und Cybersicherheit – genauso wie Prävention – sind die zentralen Voraussetzungen für unsere Demokratie und für die digitale Transformation unserer Gesellschaft. Für uns stellt sich die Frage, wie eine moderne Cybersicherheitsarchitektur denn aussehen muss – und zwar auf allen Ebenen, vor allem auf nationaler und europäischer Ebene –, um für Cybersicherheit zu sorgen. Welche Instrumente gibt es bereits? Welche müssen noch weiterentwickelt werden und welche Aspekte gilt es zu beachten?

Um diese Fragen zu beantworten, holt der Ausschuss für Digitales mit dieser öffentlichen Anhörung externen Sachverstand ein. Wir beleuchten die Zuständigkeiten und Instrumente in der Bundesrepublik zum Thema Cybersicherheit und welchen Handlungsbedarf es für uns als Gesetzgeber gibt. Ich freue mich auf Ihre Beiträge. Wir starten mit den fünfminütigen Eingangsstatements und zuerst darf ich Herrn Atug das Wort geben.

SV **Manuel Atug:** Die AG KRITIS, um eine Zuordnung zu haben, ist ein unabhängiger, ehrenamtlicher Zusammenschluss von Expertinnen und Experten, die sich täglich mit kritischen Infrastrukturen beschäftigen – durch Planung, Bau, Betrieb, Prüfung, Beratung, etc. von den jeweiligen IT-Systemen und Anlagen. Wir haben uns intensiv über viele Jahre mit Cybersicherheits- und physischen Sicherheitsfragestellungen befasst. Die Arbeitsgruppe selbst ist vollständig unabhängig von Staat oder Wirtschaft und vertritt keine Interessen von Unternehmen oder Wirtschaftsverbänden.

Unser Ziel ist einzig und allein, die Versorgungssicherheit der Bevölkerung zu erhöhen. Dazu gehört eben auch die Cybersicherheit in Deutschland, um die es wieder einmal geht. Schauen wir dort genauer hinein. Bitte anschnallen, der Weg wird holprig und erfordert in weiten Strecken eine disruptive Erneuerung.

Wir reden von dem Deutschland, das in der Bildungspolitik als Industrienation Fabrikarbeiter:innen ausbildet, statt Medienkompetenz, IT-Knowhow, IT Security-Kenntnisse, Programmierung, Algorithmen und Datenstrukturen auszubilden, um die Informationsgesellschaft in digitaler Souveränität auszubilden und digital kompetent in Forschung, Wirtschaft, Staat und Politik zu entlassen. Das ist ein Defizit, was wir haben. Wir können so viel koordinieren, machen, steuern und wünschen – das Knowhow muss einfach vorhanden sein. Aber stattdessen muss die Sicherheitsforscher:innen-Community in Deutschland oft genug mit Entscheider:innen auf dem digitalen Kompetenzniveau eines Faxgeräts diskutieren, warum gewisse Vorgehensweisen und offensive Wunschträume schlicht Gegenteiliges erzeugen und weder digital nachhaltig sind, noch den Menschenschutz in den Vordergrund stellen. Technologieschulden für kommende Generationen sind daher vorprogrammiert. Mit denen leben wir gerade – bei den Ransomware-Angriffen zum Beispiel – und wir als AG KRITIS sind dauernd damit beschäftigt, Brandherde zu löschen, während großflächig von diesen Entscheider:innen und weiteren staatlichen Akteuren neue Feuer durch offensive Wunschträume gesetzt werden.

Generell gilt dabei: Durch Glitzer und Hype wie KI und Blockchain gibt es nur Schaufenster und Leuchttürme für die Selbstprofilierung, aber keine konkreten Sicherheitsmaßnahmen, zum Beispiel bei KRITIS-Betreibern:innen oder eben in der Cybersicherheit in Deutschland generell. Zu viele Akteure und zu viele ineffektive Gesetze machen die Cybersecurity komplex. Komplexität ist der Feind von Sicherheit. Evaluierung der Gesetze: oftmals Fehlanzeige. Überwachungsgesamtrechnungen, wie im Koalitionsvertrag verankert: nicht in Sicht.

Echte Cybersecurity durch Etablieren von Knowhow und eine gute Digitalisierung durch Security by Design oder Privacy by Design als wissenschaftlich evaluierte Design-Prinzipien, die funktionieren: Auch Fehlanzeige, wenn es nicht wirklich sein muss. Denn bei der Software von Airbags beispielsweise funktioniert das sehr zuverlässig, da die Hersteller sonst haften und das wirklich teuer würde. Mit Rechtsdurchsetzung würde also vieles gehen, wenn der Staat das nur wollen würde und könnte. Von den 300.000 Polizist:innen in Deutschland beispielsweise kann jede:r uns ein Knöllchen ausstellen, aber nur ein minimaler Bruchteil ist in der Lage, eine Strafanzeige für Onlinevorfälle entgegenzunehmen und das bei einem demokratischen Rechtsstaat mit Verfassung und Grundgesetz. Irgendwie fühlt sich das nicht so richtig nach „Cyber“ und nach „Sicherheit“ an.

Wir müssten dringend die Cybersicherheitsarchitektur in Deutschland entschlacken. Nicht nur von den vielen Akteuren, die wir im Wimmelbild der Verantwortungsdiffusion haben. Alle wollen mitspielen, niemand ist verantwortlich, wenn etwas passiert – so geht es irgendwie auch nicht. In Deutschland sind alle und jeder Opfer von Tätern und krassen Angreifern und hinter jedem desolat betriebenen System standen fiese, krasse Angreifer. Aber keiner fragt sich, ob die Systeme nicht doch eher grob fahrlässig betrieben werden, wenn archäologisch wertvolle Fernwartungen im Betriebssystem oder Netzwerkkomponenten mit uralten Schwachstellen betrieben, aber keine Patches installiert werden und Hersteller diese aufgrund des Alters nicht mehr anbieten oder sogar als Hersteller gar nicht mehr existieren.

Wir stellen fest: Es fehlt eine defensive Cybersicherheitsstrategie in Deutschland – für ganz Deutschland. Die Cybersicherheitsstrategie für Deutschland 2021 ist weder für ganz Deutschland gültig, noch ist es eine Strategie. Diese Struktur der Verantwortungsdiffusion bringt uns schlicht nicht zum Ziel. Wir bräuchten also zum Beispiel eine Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom Bundesministerium des Innern und für Heimat (BMI), um besagte offensive Interessen, die gegensätzlich sind, aufzudröseln, offen gehaltene Sicherheitslücken zu beheben und Möglichkeiten

des Hackbacks zu unterbinden, weil wir damit tatsächlich Cybersicherheit in Deutschland gestalten könnten.

Wir sollten also beispielsweise diese Strukturen so aufbauen, dass in den Zuständigkeiten gewünschtes Schwachstellenmanagement nicht wegoptimiert wird. Stattdessen sollten Schwachstellen nicht gemanagt, sondern behoben werden, damit alle in der Verantwortung sind, diese zu melden und zu beheben. Das schließt die öffentliche Verwaltung ein, die Sicherheitsbehörden, die Nachrichtendienste und alle anderen staatlichen Akteure. Das wäre ein Wunsch, den wir hätten. Auch aktive Cyberabwehr sollte koordiniert und nur defensiv und nicht offensiv vorgenommen werden. Ob sie aktiv oder passiv heißt, ist völlig belanglos, es muss defensive Cyberabwehr sein, die wir brauchen, und dafür brauchen wir entsprechende Strukturen, die das anbieten.

SV **Ammar Alkassar**: Die Cybersicherheit und deren Architektur werden immer wichtiger. Nicht nur für den staatlichen Schutz, sondern für alle gesellschaftlichen Belange.

Ich würde in Anbetracht der Kürze der Zeit aus der schriftlichen Stellungnahme nur einige Aspekte herausgreifen, die ich für besonders wichtig erachte. Zunächst einmal muss man festhalten, dass die Aufstellung der deutschen Cybersicherheitsarchitektur in den vergangenen 25 Jahren ein Erfolgsmodell war. Wenn man das mit vielen anderen Ländern vergleicht, die sich heute immer noch schwer tun – insbesondere in der Abgrenzung zwischen zivilen Aufgaben der Cybersicherheit und nachrichtendienstlichen Aufgaben – merkt man, dass wir hier einen Weg gegangen sind, der tatsächlich vorbildhaft ist und dazu beigetragen hat, dass wir eine Behörde haben, die ein weitestgehend großes Vertrauen genießt bei den entsprechenden Stakeholdern.

Vertrauen ist in dem Zusammenhang der Cybersicherheit die wesentliche Grundlage. Jede Cybersicherheitsarchitektur, die weiterentwickelt wird, muss als wesentliche Grundlage auch weiterhin haben, dass die Integrität dieser Behörde zweifelsfrei erhalten bleibt. Wenn man jetzt die Frage, die aufgegriffen worden ist, thematisieren möchte, was das heißt, ob wir eine größere Unabhängigkeit des BSI brauchen: Ich glaube, der entscheidende Punkt ist weniger – was oft diskutiert worden ist – in welchem Ressort beispielsweise das BSI aufgehängt werden kann, sondern viel stärker, inwieweit tatsächlich die Aufgaben des BSI so erfüllt werden können, dass die gesellschaftlichen Erwartungen erfüllt sind.

Man muss auch festhalten, dass Cybersicherheit keine rein technische Frage mehr ist, sondern natürlich in einem politischen Umfeld steht und auch immer wichtiger wird. Das heißt, sie wird auch in Zukunft Teil des Regierungshandelns sein und damit natürlich auch einer Steuerung durch die Bundesregierung unterliegen. Inwieweit das einen Nachteil in bestimmten Bereichen umfasst, ist etwas, das man diskutieren kann. In der öffentlichen Diskussion wird zum Beispiel oftmals ein Punkt verkannt: Dass es richtig ist, dass das BMI auch die Fachaufsicht über Behörden hat, die ein Stück weit Sicherheit in einem anderen Kontext sehen, vor allem im Zusammenhang mit der Strafverfolgung, und dafür möglicherweise an einer anderen Stelle Instrumente einsetzt, die die Cybersicherheit aushebeln. Aber trotz dieser Doppelfunktion des BMI hat sich das BSI in den letzten 30 Jahren positiv entwickelt und das BMI konnte – zumindest meiner Einschätzung nach – das BSI vor einer Vereinnahmung durch die Sicherheitsbehörden bewahren. Es ist also eine theoretische Diskussion.

Wenn man sich aber die praktische Erfahrung der letzten 30 Jahre anschaut, dann sieht man, dass wir dies tatsächlich nicht als Grundproblem haben. Es bleibt die Frage, ob wir bestimmte Bereiche haben, die tatsächlich komplett unabhängig sein müssten. Das könnte man auch außerhalb des BSI machen. Als Beispiel: Man könnte eine Art Stiftung für Cybersicherheit gründen – so ähnlich wie die Stiftung Wissenschaft und Politik, die im Geschäftsbereich des Bundeskanzleramtes liegt, oder wie das Bundesinstitut für Risikobewertung, die komplett unabhängig sind, da sie am Ende des Tages keine exekutive Gewalt ausführen, sondern einen Beratungsauftrag schaffen.

Vielleicht ein paar Punkte, die man auch herausgreifen kann: Wir haben beispielsweise die Schaffung eines Chief Information Security Officers (CISO) für den Bund in der Diskussion. Das ist ein wesentlicher Punkt, der sehr hilfreich

wäre, aber auch nur dann, wenn er in Personalunion mit dem BSI-Präsidenten geschaffen wird. Es würde keinen Sinn machen, die CISO-Organisation – das ist das BSI – vollkommen losgelöst zu halten von der Einrichtung einer solchen Stelle. Vielleicht auch ein Punkt zu der Frage Schwachstellen und Schwachstellenmanagement: Das sehe ich sehr ähnlich wie Manuel Atug. Es muss jedem klar sein, dass jede einzelne Schwachstelle, die offen bleibt, ein Risiko für die Cybersicherheit ist und das Managen von Schwachstellen eigentlich nur mit großen Bauchschmerzen in der Form passieren darf, dass diese Schwachstellen offen gehalten werden. Am Ende des Tages kann das nur funktionieren, indem man einen sehr restriktiven Zeitraum am besten gesetzlich definiert, der dafür Sorge trägt, dass jede Schwachstelle – auch wenn sie von staatlichen Behörden verwendet und genutzt wird – geschlossen wird. Das ist ein ganz entscheidender Punkt.

Noch ein letztes Wort zur aktiven Cyberabwehr: Auch da teile ich die Sichtweise – am Ende des Tages ist es ein unglücklicher Begriff, genauso wie Hackback und die anderen Begriffe, die in der öffentlichen Diskussion verwendet werden. Fast jede Cyberabwehr ist aktiv oder hat aktive Komponenten. Die Frage ist: Wo kommen diese Komponenten und die Maßnahmen zum Einsatz und ist dies durch die bisherigen rechtlichen Rahmenbedingungen gedeckt?

SVe **Dr. Annegret Bendiek**: Aufgrund meiner fachlichen Expertise decke ich im Prinzip mit meiner Stellungnahme nur die Fragen 1 bis 6 ab. Ich möchte mich darauf beschränken. Cyberangriffe sind nicht nur ein bundesdeutsches, sondern eben auch ein gesamteuropäisches Problem. Diesen Aspekt möchte ich insbesondere auch vor dem Hintergrund unseres großen europäischen Konsortiums für den Aufbau eines europäischen Repositoriums über Cybervorfälle, die für cyber-, außen- und sicherheitspolitische Fragen von Relevanz sind, noch einmal betonen.

Grundsätzlich ist davon auszugehen, dass die Umsetzung, die von Bundeskanzler Olaf Scholz angemahnte neue strategische Kultur in der Cybersicherheit, nur dann gelingen kann, wenn a) nationale Cybersicherheit einer europäischen beziehungsweise transatlantischen Bündnisfähigkeit unterliegt, b) dem Vorrang der Diplomatie in einer kooperativen Sicherheit, insbesondere nach dem 24. Februar 2022, verpflichtet ist und c) auf inklusive, transparente und privat-öffentliche Partnerschaften und parlamentarisch kontrollierte Verfahren setzt. Das heißt, die deutsche Cybersicherheit ist ein Kernbereich der künftigen umfassenden nationalen Sicherheitsstrategie Deutschlands. Diese Bemühungen sind in die EU-, G7- und EU-NATO-Zusammenarbeit eingebunden. Das heißt, ein wichtiger Referenzpunkt für unsere deutsche Sicherheitspolitik ist und bleibt die EU-Strategie von 2020.

Die Bundesregierung, die Mitgliedstaaten der EU und die Union folgen prinzipiell der Idee von Due Diligence bei der Umsetzung ihrer Cybersicherheitsstrategien. Diese Sorgfaltsverantwortung unterliegt einem gesamtgesellschaftlichen Sicherheitsverständnis und verpflichtet Staaten, aber auch nichtstaatliche Akteure, in Friedenszeiten dafür zu sorgen, dass von ihrem Territorium keine Handlungen ausgehen, welche die Rechte anderer Staaten verletzen.

Ich glaube, dass der Hinweis auf diese Sorgfaltsverantwortung absolut wichtig ist, da sie in den letzten zwei, drei Jahren in Vergessenheit geraten ist. Die vertrauens- und sicherheitsbildenden Maßnahmen im Rahmen von regionalen, aber auch internationalen Organisationen, die die Bundesregierung insbesondere durch das Auswärtige Amt anstrengt, sind durch die mangelnde Ergebnisorientierung aufgrund der schwierigen internationalen Lage etwas in Vergessenheit geraten.

Die Cybersicherheitsstrategie 2021 und die Cybersicherheitsagenda des BMI vom Juli 2022 folgen grundsätzlich dieser Idee. Sie weisen aber auch richtigerweise darauf hin, dass Cybersicherheit für einen modernen, hoch technologisierten und digitalisierten Industriestaat wie Deutschland essenziell ist. Infrastrukturresilienz, die Abwehr und Aufklärung von auch staatlich gelenkten Cyberangriffen sowie die Sensibilisierung für Desinformationskampagnen wären demzufolge zu stärken. Das Problem ist, dass wir hier ein strategisches Vakuum zwischen der

Cyberdiplomatie der vertrauens- und sicherheitsbildenden Maßnahmen, wozu auch restriktive Maßnahmen, also Cybersanktionen der Europäischen Union gehören, auf der einen Seite und der Cyberverteidigung auf der anderen Seite haben, wo wir im Prinzip schon oberhalb der Schwelle eines bewaffneten Konflikts liegen und damit auch im humanitären Völkerrecht. Mit dem strategischen Kompass und der EU Cyber Posture, die fälschlicherweise in den deutschen Übersetzungen als aktive Verteidigung übersetzt wurde, aber eigentlich aktive Cyberabwehr meint, haben sich die EU-Mitgliedstaaten und damit auch eigentlich die Regierung der Bundesrepublik Deutschland bereits im vergangenen Jahr darauf verständigt, diese Lücke zu verkleinern, indem ihre aktive Cyberabwehr zum Zwecke der Strafverfolgung verbessert werden soll, so heißt es auf europäischer Ebene. Das ist aber ein rechtlich nicht bindendes Instrument. Aber wir haben uns der politischen Kohärenz mit den EU-Staaten auf der EU-Ebene verpflichtet. Der rechtliche Rahmen der Cybersicherheit wird in Europa durch – wie wir alle wissen – den Binnenmarkt, aber auch durch die Soft Law Gesetze- oder Nichtgesetzgebung geregelt.

Wir sind der Meinung, dass diese strategische Lücke zwischen der Cyberdiplomatie auf der einen und der Cyberverteidigung auf der anderen Seite nur geschlossen werden kann, indem die Strafverfolgung insgesamt verbessert wird, nicht nur auf nationaler, sondern auch auf europäischer Ebene. Das erfordert unseres Ermessens nach im Prinzip eine Stärkung von Bundeskompetenzen im Bereich der aktiven Cyberabwehr bei einer Gefahrenlage. Vergleichbar zur Terrorismusbekämpfung im Gemeinsamen Terrorismusabwehrzentrum (GTAZ) wäre es sinnvoll, die Befugnisse für das Bundeskriminalamt im Nationalen Cyberabwehrzentrum zu stärken und gleichzeitig die stärkere Unabhängigkeit des BSI im Sinne eines Bundesamts für Statistik oder vergleichbar – wie die Stiftung Wissenschaft und Politik auch – wirklich unabhängig von den Ministeriumsvorgaben zu machen und ihnen damit eine Eigenständigkeit in der Cyberresilienz zu gewähren.

SVe **Dr. Stefanie Frey**: Für uns als Cyberkrisenmanager bei Deutor ist es ein extrem wichtiges Anliegen, die Systeme heute zu beleuchten.

Deutor ist lateinisch und steht für "Jemandem übel mitspielen" – und das ist genau, was die Cyberkriminellen mit ihren Taten tagtäglich tun. Was wir jeden Tag erleben dürfen und müssen, sind enorme finanzielle Schäden, die Zerstörung von Infrastrukturen bis hin zu verbrannter Erde, verzweifelte Manager und auch ratlose IT-Verantwortliche. Das darf und kann nicht sein und für uns ist es ein Anliegen, dass wir auch die Strafverfolgung stärken. Die Täter sind hoch motiviert, sehr professionell und haben große Ziele. Diese wollen sie um jeden Preis erreichen. Wir haben aktuelle Fälle, wo Morddrohungen bei Nichtzahlung der Erpressungssummen ausgesprochen werden, Fotos von Kindern und Familien im Netz sind – und es kommt keine Hilfe. Das ist eine unzumutbare Situation, die trotz unserer Bemühungen mit der Cybersicherheitsarchitektur, mit unseren ganzen Akteuren, nicht funktioniert.

Wir haben ein neunundneunzigprozentiges Dunkelfeld, wo von den bekannten Fällen nur 30 Prozent ermittelt werden. Das heißt, wir haben 0,3 Prozent Aufklärung der Cyberfälle. Das ist eine unzumutbare, untragbare Situation. Unsere Kunden würden zu 100 Prozent eigentlich nicht zur Polizei gehen – wir raten an, zu gehen, damit die Prozesse sauber sind. Von den 100 Prozent unserer Kunden sind 100 Prozent ungeklärte Fälle. Die Täter müssen wir nicht einmal identifizieren, sie identifizieren sich selber in den Schreiben. Wir wissen, mit wem wir es zu tun haben, können es aber nicht aufklären. Was die Täter können, können wir auch. Die große Frage, die ich in den Raum stellen möchte: Warum wird es trotz dieser Bemühungen nicht besser? Was in der Realität dort unten passiert, korrespondiert nicht mit unseren Bemühungen auf nationaler und internationaler Ebene.

Wir regen an, dass mehr investiert wird in die Repression. Die Täter dürfen sich nicht in einem straffreien Raum bewegen. Sie müssen sich vorstellen, wie dreist es ist, wenn sich Täter identifizieren, denn sie wissen, dass nichts passiert. Das ist schon eine Situation, in der wir uns alle fragen müssen, ob wir auf dem richtigen Weg sind. Wir fordern mehr Investition in Repression.

Die Strafverfolgungsbehörden müssen so ausgestattet sein, dass sie auch ermitteln können und dürfen. Sie müssen befugt sein und sie müssen auch die technischen Fähigkeiten dazu bekommen. Wir sehen, dass viele Menschen von der Polizei in die Privatwirtschaft gehen, da es keine Anreize gibt, für die Strafverfolgung zu arbeiten. Wenn Sie das mit Amerika vergleichen: Dort gibt es die Anreize. Die Gehälter müssen höher sein. Ich weiß nicht, wer von Ihnen zuletzt im Landeskriminalamt bei der Cyber Crime Unit war. Das sind keine Bedingungen, mit denen man derzeit viele Leute aus der Uni anziehen kann. Das ist nicht attraktiv. Also auch hier Anreize schaffen, die Mittel geben, damit die Strafverfolgung das tun kann, wofür sie eigentlich da ist: Täter ermitteln. Ohne Strafaktionen werden wir dieses Problem trotz NIS-Richtlinie, trotz allem, was wir da oben tun, nicht in den Griff bekommen.

Auch müssen wir uns darüber ganz klar werden, dass die ganzen Präventionsmaßnahmen sehr gut und sehr hilfreich sind, aber am Ende des Tages, wie wir jetzt sehen, on the ground nicht funktionieren. Also auch hier: Wir müssen krisenresilient werden, krisenfester werden. Wir können die Vorfälle nicht vermeiden, aber wir können die Krisen vermeiden.

Dahin müssen wir kommen: Anreize für Unternehmen schaffen, mit gutem Gewissen – und nicht nur, weil sie bestraft werden von oben – ihre Prävention und ihre IT-Sicherheit zu stärken und die Polizei befähigen sowie die ganze Cybersicherheitsarchitektur, die wir in der Bundesrepublik Deutschland haben, bündeln mit Leistungsbeschreibungen. Die Tapete der Stiftung Neue Verantwortung – ich nenne das eine Tapete – hat viel zu viele Akteure, die gar nicht im Bereich Cyber tätig sind. Zu den Strukturen von Cybercrime: Von 134 Mitarbeitern im Landeskriminalamt sind zehn für schwere Cyberfälle zuständig. Alle anderen sind in anderen Gebieten des Onlinebetruges tätig, und das ist keine tragbare Situation.

Wir regen an, die Strafverfolgung mit allen Mitteln für die Repression zu stärken.

SV **Dr. Sven Herpig**: Wir haben es gehört: Nach Berichten und Lagebildern des Bundesamts für Sicherheit in der Informationstechnik, des Bundeskriminalamts und des Bundesamts für Verfassungsschutz ist die Bedrohungslage im und aus dem Cyberraum nach wie vor auf einem sehr hohen Niveau. Was gilt es also zu tun? Ich möchte hier vier der Empfehlungen aus meiner schriftlichen Stellungnahme hervorheben.

Erstens: Laut Koalitionsvertrag hat sich die Bundesregierung vorgenommen, einen strukturellen Umbau der IT-Sicherheitsarchitektur einzuleiten. Das ist ein begrüßenswerter Schritt. Möglicherweise haben einige von Ihnen unsere Visualisierung – auch Wimmelbild oder Tapete genannt – vor Augen. Man macht es sich aber vielleicht zu einfach, wenn man allein auf Basis dieser Visualisierung die deutsche Cybersicherheitsarchitektur als Zuständigkeitschaos bezeichnen würde. Es ist eine dezentrale Struktur mit verbindenden zentralen Akteuren wie dem Nationalen Cybersicherheitsrat, dem Nationalen Cyberabwehrzentrum und nicht zuletzt dem BSI.

Ein Teil der Wahrheit ist jedoch auch, dass es seit 2011 keine strukturelle Konsolidierung der Architektur gegeben hat. Es wurden lediglich neue Akteure geschaffen und den bereits bestehenden weitere Ressourcen und Befugnisse zugeteilt. Selbst von Anfang an zum Scheitern verurteilte Initiativen wie der Nationale Pakt Cybersicherheit werden künstlich am Leben gehalten, da sich niemand traut, auch einmal etwas abzuschaffen. Um die Effektivität und Effizienz der deutschen Cybersicherheitsarchitektur aber abschließend beurteilen zu können, fehlt es uns an öffentlich verfügbaren Informationen.

Ich rege daher an, dass die Bundesregierung eine mit unabhängigen Expert:innen und Praktiker:innen besetzte Kommission zur Evaluierung der deutschen Cybersicherheitsarchitektur und zur Erarbeitung des entsprechenden Reformbedarfs einsetzt. Der dort identifizierte Reformbedarf sollte zwingend während dieser Legislaturperiode umgesetzt werden.

Zweitens: Wir sollten die Unabhängigkeit des BSI vom BMI nicht als Selbstzweck diskutieren, sondern im Rahmen seiner Funktion als Vertrauensanker.

Das hat auch SPD-Obmann Dr. Jens Zimmermann

in seinem Tagesspiegel-Background-Cybersecurity-Beitrag vom Montag noch einmal deutlich gemacht. Vertrauensanker – wofür eigentlich? Vertrauensanker vor allem für Wirtschaft, Wissenschaft, Zivilgesellschaft, sodass Unternehmen beim Melden von IT-Sicherheitsvorfällen darauf vertrauen können, dass sie vom BSI fachliche Unterstützung bekommen und IT-Sicherheitsforschende darauf vertrauen können, dass ihre gefundenen Schwachstellen einem Coordinated Vulnerability Disclosure-Verfahren zugeführt werden.

Politik, Wirtschaft und Gesellschaft müssen darauf vertrauen können, dass das BSI seine Entscheidungen auf fachlicher Grundlage trifft – und es da, wo das nicht der Fall ist, als politische Entscheidung des Ressorts gekennzeichnet wird und für eine Überprüfung Dritter nachvollziehbar ist. Letzteres kann im Rahmen einer Aufsicht außerhalb des Ressorts – zum Beispiel durch zuständige Bundestagsausschüsse – erfolgen.

Drittens: Wir diskutieren seit über sechs Jahren das Thema aktive Cyberabwehr. Wir diskutieren es in einem luftleeren Raum, da das BMI sich bisher weigert, ein konkretes Konzept öffentlich zur Debatte zu stellen. Lediglich ein sehr einfach gehaltenes Vier-Stufen-Modell, das vermutlich mittlerweile veraltet ist, wurde in der Öffentlichkeit angesprochen und trotzdem unter Verschluss gehalten. Auf dieser Basis eine Grundgesetzänderung einzufordern, halte ich für höchst problematisch. Ich bin mittlerweile versucht zu sagen, dass das Innenressort – außer ein paar Randfällen und hochgradig konstruierten Beispielen – überhaupt keine empirische Grundlage hat, die belegt, dass die geforderte Grundgesetzänderung zu mehr IT-Sicherheit führt. Das ist vielleicht etwas überzogen, aber ich würde mich gerne eines anderen belehren lassen. Wenn es tatsächlich so ein Konzept geben sollte, muss es dem öffentlichen Diskurs zur Verfügung gestellt werden, bevor wir das Grundgesetz anfassen.

Viertens und letztens: Die Bundesregierung tut sehr gut daran, das Recht auf Verschlüsselung ausnahmslos umzusetzen und rechtlich zu verankern. Hierbei muss es sich um die sichere Implementierung starker Verschlüsselung handeln, die weder durch Hintertüren, Vordertüren, Lawful Access-Schnittstellen oder andere technische Maßnahmen unterminiert wird. Hierzu zählt auch das im Rahmen der Chatkontrolle diskutierte Client Side Scanning. Hierfür muss sich die Bundesregierung nicht nur national, sondern vor allem europäisch einsetzen und ihre in der letzten Legislaturperiode vertretene Position in Brüssel geraderücken. Für jedwede Erweiterung von Befugnissen der Sicherheitsbehörden sollte die im Koalitionsvertrag genannte Überwachungsgesamtrechnung als Grundlage dienen.

Professor Peter Zweier bezeichnete die heutige Zeit einmal als das „Goldene Zeitalter der Überwachung“. Niemals zuvor hatten Sicherheitsbehörden Zugriff auf eine solche Masse von Daten. Einen Sicherheitsanker unserer modernen Kommunikationsinfrastruktur – die Verschlüsselung – auszuhebeln, um Sicherheitsbehörden Zugriff auf noch mehr Daten zu ermöglichen, erscheint töricht.

Schließlich bleibt über alle genannten Bereiche festzuhalten, dass es den bisherigen Bundesregierungen bei der deutschen Cybersicherheitspolitik massiv an a) Transparenz und proaktiver Kommunikation, b) konstruktiver Einbeziehung von Wirtschaft, Wissenschaft und Zivilgesellschaft sowie c) Evaluations- und Reformwillen mangelte. Die teils antagonistische Beziehung zwischen der Exekutive auf der einen Seite und Vertreter:innen von Wirtschaft und Wissenschaft, aber vor allem Zivilgesellschaft auf der anderen Seite, ist zum Großteil auf diese Mängel zurückzuführen. Diese Beziehung sollte dringend verbessert werden, um die deutsche Cybersicherheitspolitik gemeinsam bestmöglich aufzustellen und Deutschland im Cyberraum zu mehr Resilienz zu verhelfen.

SV **Prof. Dr. Dennis-Kenji Kipker**: In dieser kurzen Zusammenfassung meiner ausführlichen schriftlichen Stellungnahme möchte ich vor allem die nachfolgenden Schwerpunkte in den besonderen Fokus einer rechtspolitischen Betrachtung rücken.

Erstens: Den Begriff der Cybersicherheit. Die derzeit in Deutschland kritisierte Verantwortungsdiffusion ist die Folge einer unzureichenden Definition und Eingrenzung des Begriffs der Cybersicherheit. Deutlich wird das

vor allem an der im letzten Jahr durch das BMI vorgelegten sogenannten Cybersicherheitsagenda. Wir brauchen ein ganz klares, ontologisches Verständnis der Cybersicherheit als technische und organisatorische Reaktion auf die gegenwärtigen Herausforderungen im digitalen Raum. Fragen wie zum Beispiel die Regulierung von Online-Hass, Kriminalität, Plattformregulierung, Chatkontrolle oder generell der schillernde Begriff der digitalen Souveränität haben damit zunächst relativ wenig zu tun. Es geht bei der Cybersicherheit primär um die Aufrechterhaltung der Funktionsfähigkeit der vernetzten IT-Systeme, und daran sollten sich legislative und exekutive Maßnahmen künftig stärker orientieren, um keine systemimmanenten Widersprüche zu generieren. Operative Cybersicherheit in Deutschland ist primär eine technische und keine politische Aufgabe.

Zweitens: Digitaler Gegenschlag beziehungsweise aktive Cyberabwehr. Sämtliche im Konzeptpapier der Bundesregierung aus 2019 angegebene Strukturen und behördliche Akteure sind weder geeignet noch verfassungsrechtlich legitimiert, einen digitalen Gegenschlag durchzuführen, beziehungsweise darüber zu entscheiden. National allein zuständig ist für diesen Fall die Bundeswehr mit dem Kommando Cyber- und Informationsraum. Das setzt national verfassungsrechtlich einen Verteidigungsfall und international völkerrechtlich das Bestehen eines Selbstverteidigungsrechtes voraus. Hier fehlt es bislang an einem klaren begrifflichen Verständnis. Aktive Cyberabwehr betrifft nämlich nicht die bloße Blockade und Umleitung schadhafter Datenverkehre, die bereits vom gegenwärtig bestehenden gesetzlichen Rahmen gedeckt sind. Daraus folgt, dass es aufgrund der verfassungsrechtlich eindeutigen Bestimmtheit der Zuständigkeit der Bundeswehr zurzeit keiner Gesetzesänderung beziehungsweise Neuschaffung von Gesetzen in diesem Bereich bedarf.

Drittens: Umgang mit Zero Days. Die Cybersicherheit und mit ihr verbundene öffentliche- und Individualinteressen haben grundsätzlich Verfassungsrang, der aber nicht absolut gilt. Das bedeutet, dass der verhältnismäßige Ausgleich zu anderen ebenfalls verfassungsrechtlich geschützten Interessen herzustellen ist. Das Bundesverfassungsgericht hat im Jahr 2021 klar entschieden, dass es deshalb als staatliche Maßnahme grundsätzlich verfassungsrechtlich zulässig sein kann, IT-Sicherheitslücken zum Beispiel zur Durchführung von Quellen-Telekommunikationsüberwachung einzusetzen. Derlei Maßnahmen müssen jedoch ausgehend von der bundesverfassungsgerichtlichen Rechtsprechung auf Einzelfälle limitiert und auf das absolut notwendige Maß beschränkt sein.

Umso wichtiger sind an dieser Stelle klare funktionale Trennungen in der nationalstaatlichen Cybersicherheitsarchitektur, in der die cyberkompromittierenden Maßnahmen nicht Bestandteil einer nationalen Cybersicherheitsagenda sind.

Viertens: KRITIS-Dachgesetz. Insbesondere unter dem Eindruck des verheerenden Russland-Ukraine-Krieges wurde die Vulnerabilität der nationalen kritischen Infrastruktur nochmals besonders deutlich. Das Problem ist aber keineswegs neu, sondern besteht mittlerweile schon seit Jahrzehnten. So stellt zum Beispiel das Innenministerium in der nationalen KRITIS-Strategie aus dem Jahr 2009 bereits auf die hybride Bedrohungslage infolge terroristischer Anschläge seit dem 11. September 2001 in den USA ab. Dieser Fakt wird in der aktuellen politischen und medialen Debatte leider unzureichend wiedergegeben.

Die Annahme, dass es sich bei dem KRITIS-Dachgesetz um eine spiegelbildliche Regelung zur KRITIS-Cybersicherheit im Analogen handelt, geht deshalb fehl, denn auch das IT-Sicherheitsgesetz 2.0 regelt weitaus mehr als nur kritische Cybersicherheit, und wir verfügen auch bereits seit Jahren über unzählige bereichsspezifische Fachgesetze für den nationalen KRITIS-Schutz. Deshalb kann ein KRITIS-Dachgesetz nur ein weiteres Artikelgesetz sein, das die Bestandsgesetze zum physischen KRITIS-Schutz bei nachgewiesenermaßen 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.

Fünftens: Ausbildung von Cyberfachkräften in Deutschland. Wenn wir im Unternehmerischen von Cyber Security Compliance sprechen, dann geht es mittlerweile vor allem auch um rechtliche Fragestellungen. Wie bereits angesprochen, haben wir in Deutschland und in der EU eine Vielzahl von Fachgesetzen, die juristische Anforderungen für die Cybersicherheit festschreiben. Hier ist es dringend erforderlich, die juristische Ausbildung zu reformieren und weitaus interdisziplinärer als bislang zu gestalten. Wir brauchen in Deutschland unbedingt mehr IT-Juristen, die sowohl die rechtlichen Fragestellungen beherrschen als auch das zur Anwendung notwendige technische Knowhow besitzen. Gerichtet an die Hochschulen möchte ich deshalb das Ausbildungsmodell eines technischen Cyber Security Masters nach Abschluss des juristischen Studiums vorschlagen.

SVe **Prof. Dr. Martina Angela Sasse**:
Cybersicherheit ist kein rein technisches Problem. Digitale Produkte und Dienste werden von Menschen genutzt. Dieser Aspekt wird von bisherigen Ansätzen oft vernachlässigt oder – noch schlimmer – falsch verstanden oder falsch dargestellt. Das Stichwort hier ist die Schwachstelle Mensch. Der Kollege Atug hat das Wimmelbild der Verantwortung, das zurzeit besteht, sehr schön dargestellt und die daraus resultierende Verantwortungsdiffusion. Das macht es für Nicht-Experten sehr schwierig herauszufinden, wo sie kompetente Informationen und Hilfe bekommen können. Wenn sich zum Beispiel Bürgerinnen und Bürger an die Polizei wenden, da sie vermuten oder befürchten, angegriffen zu werden, kann ihnen dort durch SMS-Phishing oder Phishing von E-Mails nicht geholfen werden. Die Polizei kann nicht helfen, wenn keine Straftat oder kein Verdacht auf eine Straftat vorliegt. Selbst die Polizei weiß nicht, dass man dies als Bürgerin und Bürger bei der Bundesnetzagentur melden sollte, als eine der vielen Akteur:innen in diesem sehr fragmentierten Raum.

Die Menschen fühlen sich dann eben einfach allein gelassen, und das untergräbt letztendlich das Vertrauen in den Staat.

Zusätzlich zum Problem der Verantwortungsdiffusion kommt auch noch dieses Verantwortungsabladen, was zurzeit Hersteller, Sicherheitsexperten und auch viele staatliche Stellen betreiben – unter dem Stichwort Schwachstelle Mensch. Statt Produkte und Dienste bestmöglich zu sichern, werden umständliche Maßnahmen erst eingeführt, wenn vorher bekannte Schwachstellen im großen Stil ausgenutzt werden. Diese Maßnahmen erfordern von den IT-Nutzer:innen sehr viel Aufwand. Es kann aber nicht sein, dass wir alle Mini-me-Sicherheitsexperten werden, um uns im digitalen Raum sicher bewegen zu können. Deshalb sind IT Security by Design und Produkthaftung notwendig.

Natürlich brauchen Menschen auch ein gewisses Grundwissen in Bezug auf IT, digitale Sicherheit und digitale Souveränität. Dafür sollte ein qualifizierter Kanon für die Ausbildung in verschiedenen Schulen, Universitäten und so weiter entwickelt werden. Am besten in Kooperation mit Wissenschaftlern, die auf der Höhe der Zeit sind. Im Moment gibt es sehr viele kostenlose Ratschläge zur digitalen Sicherheit, aber auch hier präsentiert sich ein Wimmelbild von Kampagnen und Webseiten von verschiedenen Akteuren. Entwickelt, in Auftrag gegeben und oft von gut bezahlten Werbeagenturen sehr attraktiv gestaltet, aber ohne Qualitätskontrolle, was den Inhalt angeht. Viele Ratschläge sind veraltet, nicht sicher und oft viel zu aufwendig, sodass sie von den meisten Menschen einfach ignoriert werden. Eine Qualitätskontrolle, eine Evaluation, das Lernen, was für welche Gruppe funktioniert und was nicht, findet dagegen nicht statt. Darin wird quasi gar nichts investiert.

Auch im kommerziellen Bereich gibt es sehr viele Security Awareness-Produkte, für die jedes Jahr Milliarden ausgegeben werden, die wieder zusätzlich Zeit der Mitarbeitenden beanspruchen, aber die Risikowahrnehmung und die Sicherheitskompetenz nicht verbessern. Zusätzlich dazu ist der weit verbreitete Einsatz von simulierten Phishing-Kampagnen, bei denen Mitarbeitende von ihrem eigenen Unternehmen oder im Auftrag ihres eigenen Unternehmens angegriffen werden zu angeblichen Schulungszwecken, auch wieder ein Zeichen für die falsch verstandene Art und Weise, wie man Kompetenz bei Menschen steigern kann. Dies

führt zu Angst und Passivität, aber nicht zur Verbesserung der Sicherheitskompetenz. Der oft vermeldete Abklang der Klickraten ist immer nur von kurzer Dauer.

Die Zusammenfassung: Wir müssen weg von der Idee, dass der Mensch eine Schwachstelle ist. Cybersicherheit erfordert Vertrauen und Kooperation zwischen den Akteuren, und das setzt erst einmal Respekt voraus. Menschen im digitalen Zeitalter haben wenig Zeit und Aufmerksamkeit. Das müssen wir respektieren. Wenn wir alle Mini-me-Sicherheitsexperten sein müssen, um im digitalen Raum sicher unterwegs zu sein, bedroht das letztendlich die Produktivität des Wirtschaftsstandorts Deutschland. IT-Sicherheitshersteller, -dienstleister und -experten müssen die Hauptarbeit machen und nicht die Verantwortung in Bausch und Bogen auf die Menschen abschieben.

SVe **Julia Schuetze**: Ich fokussiere mich vor allem auf ausgewählte Reform- und Optimierungsmaßnahmen, die das Zusammenspiel von Bundesländern und kommunaler Ebene verbessern sollen. Vor allem auch im Hinblick auf die NIS-2-Umsetzung sehe ich es als Chance, diese föderale Zusammenarbeit in Deutschland zu optimieren.

Für mich sind drei Aspekte besonders wichtig. Erstens: Den Beitrag der Länder zu definieren. Zweitens: Den Informationsaustausch zur Resilienzförderung zu optimieren. Drittens: Die Kommunalverwaltung in die NIS-2-Umsetzung einzubeziehen.

Deutschlands staatliche Cybersicherheitsarchitektur ist in den vergangenen Jahren zu einem hochkomplexen Gebilde herangewachsen, und darin sind staatliche Akteure auf Bundes-, Landes- und kommunaler Ebene involviert. Ansprechstellen und zuständige Behörden auf Landesebene werden immer wichtiger. Sie sind zum Beispiel bei der Beratung zu Resilienzmaßnahmen näher an der Zielgruppe, etwa die Kommunalverwaltungen an kleinen und mittelständischen Unternehmen.

Jedoch ist der Beitrag der Länder beim Thema Cybersicherheit und Resilienz sehr unterschiedlich und überschneidet sich in Teilen. Deswegen sollte die nächste deutsche Cybersicherheitsstrategie keine alleinige des Bundes sein, sondern gemeinsam mit den Ländern entwickelt werden. Dort sollten auch die Beiträge der Länder gegenüber dem Bund – zum Beispiel im Informationsaustausch und gegenüber bestimmten Zielgruppen, wie zum Beispiel Kommunalverwaltungen – festgelegt werden.

Ich denke, es ist vor allem ein politischer Auftrag, koordiniert vorzugehen, weil wahrscheinlich einige der Aufgaben und Zuständigkeiten auch in Landesgesetze umgesetzt werden müssten. So könnten auch Doppelungen vermieden und Leistungen so viel wie möglich entweder nachnutzbar gemacht oder untereinander aufgeteilt werden. Wer zum Beispiel Sensibilisierungsmaterialien von Grund auf neu entwickelt, die es womöglich anderswo bereits in guter Qualität gibt, fällt für die Beratung zur Umsetzung von IT-Sicherheitsmaßnahmen aus – eine unnötige Ressourcenverschwendung. Oder wenn man sich nicht koordiniert, um Frau Sasses Punkt aufzugreifen, ist die Qualität vielleicht einfach nicht sonderlich gut.

Zum Thema Optimierung des Informationsaustausches: Für den Resilienzaufbau bei Einrichtungen, zum Beispiel auch KRITIS, ist es wichtig, geeignete Instrumente für den Austausch von Cybersicherheitsinformationen zu implementieren. Und zwar nicht irgendwie, sondern in einem Format, das dabei hilft, Bedrohungsinformationen und -analysen, Warnungen zu Cyberaktivitäten und Reaktionsmaßnahmen so schnell und automatisch wie möglich auszutauschen und zu verstehen. Dass wir von dieser Art des Informationsaustausches noch entfernt sind, zeigt sich beispielhaft an dem fehlenden bundesweiten Lagebild, aber auch an der schieren Anzahl nichtstandardisierter Formate von Informationsdiensten. Es ist außerdem nicht empfehlenswert, sich Policies und Prozesse, die auf einen besseren Informationsaustausch abzielen oder effektivere Meldewege entwickeln sollen, nur in der Theorie auszudenken.

Deswegen ist die Empfehlung, wie auch in anderen Staaten Cybersicherheitsübungen zu nutzen und verschiedene Optionen zu testen, diese mit Praktiker:innen auszuprobieren und dann die am besten Funktionierenden zu nutzen. Man könnte hier zum Beispiel auch die geplante

LÜKEX (Länder- und Ressortübergreifende Krisenmanagementübung) nutzen. In den Kommunalverwaltungen kommt es vermehrt zu IT-Sicherheitsvorfällen, bei denen tage- und wochen-, teilweise monatelang Bürgerservices ausfallen. Sie sind demnach nicht resilient.

Die NIS-2 macht klar, dass die Mitgliedstaaten bei der Definition von Einrichtungen öffentlicher Verwaltung auf regionaler Ebene Spielraum haben. Außerdem können Mitgliedstaaten über die Anwendung von NIS-2 auf der sogenannten lokalen Ebene eigenständig entscheiden. Es empfiehlt sich, die öffentliche Verwaltung auf lokaler Ebene in die Umsetzung der NIS-2 einzubeziehen. Sie enthält verschiedene Vorgaben, die ganz oder teilweise zum Beispiel über ein Stufenmodell für lokale öffentliche Verwaltung verpflichtend sein können, zum Beispiel Berichtspflichten, aber auch der Zugang zu Computer Security Incident Response Team (CSIRT)-Leistungen. Das Risiko, dass die Länder die Kommunen bei der Umsetzung von NIS-2 ganz unterschiedlich einbinden und unterschiedliche Anforderungen stellen, sollte dabei minimiert werden.

Deswegen sollte der Beitrag des Bundes, der Länder und der Kommunen in gemeinsamen Eckpunkten oder in der Strategie festgelegt werden. Zum Beispiel ist das Ziel, Resilienz von Kommunalverwaltungen zu erhöhen. Dabei sollte jede Kommunalverwaltung auf CSIRT-Leistungen zugreifen, aber auch in den Informationsaustausch und in die Meldewege eingebunden werden.

Die **Vorsitzende**: Herzlichen Dank. Wir kommen jetzt in die Frage- und Antwortrunde, und als erstes hat von der SPD-Fraktion Dr. Jens Zimmermann das Wort.

Abg. **Dr. Jens Zimmermann** (SPD): Ich würde meine erste Frage gerne an Sven Herpig richten. Ein Teil des Wimmelbildes ist natürlich auch, dass wir in einem föderalen Staat leben. Das heißt, wir haben viele Dinge immer 16- oder 17-mal. Das macht das Bild immer schon relativ voll. Die Frage ist: Wie können wir dieses Bild aufräumen? Meine Frage in Ihre Richtung: Beim Thema Grundgesetzänderung, das die Bundesinnenministerin ins Spiel gebracht hat, geht es vor allem darum, zu sagen: Wir wollen auf Bundesebene mehr Zuständigkeiten zentralisieren. Denn es ist natürlich total cool, wenn hier im Bundestag über die Landeskriminalämter gerantet wird. Da würde ich sagen: Absender unbekannt verzogen.

Deswegen jetzt die Frage: Wenn es keine Grundgesetzänderung gibt – wie kann das Wimmelbild aufgeräumt werden? Wenn es eine Grundgesetzänderung gibt – in welche Richtung sollte es aus Ihrer Sicht gehen?

SV **Dr. Sven Herpig**: Wie die Sachverständige Schuetze gerade sehr gut ausgeführt hat, ist es an den Ländern, wirklich on the ground die Arbeit im Bereich der Cyber- und IT-Sicherheit zu leisten, da sie dort näher an den Vorfällen sind. Wir müssen uns im Endeffekt angucken, was wir eigentlich brauchen. Was brauchen wir für Dienstleistungen? Was brauchen wir für Unterstützungsleistungen und wer kann sie erbringen? Manchmal müssen wir sie doppelt und dreifach bauen, weil wir sie doppelt und dreifach brauchen – manchmal auch nicht. Dann macht es natürlich Sinn, auf der Bundesebene eine koordinierende Funktion zu haben.

Ob nun das BSI diese koordinierende Rolle einnimmt oder ob wir das Nationale Cyberabwehrzentrum (Cyber-AZ) in einer Art und Weise reformieren, dass diese Institution die Rolle einnehmen kann, darüber kann man sicherlich diskutieren. Sollten wir das beim Cyber-AZ verorten, dann müssen wir natürlich zuerst mehr Länder dort einbeziehen und zum anderen die Rechtsgrundlage für das Cyber-AZ vernünftig aufstellen. Das funktioniert in dem Rahmen, wie es gerade läuft, ganz solide. Der Informationsaustausch ist da, Kooperation ist da, vielleicht braucht man dafür auch nicht mehr als irgendwelche Kooperationsabkommen unter den Behörden. Aber wenn wir sagen, es soll mehr Befugnisse bekommen, es soll die zentrale Drehscheibe zwischen Bund und Ländern werden, dann müssen wir es auch rechtlich auf vernünftige Füße stellen. Kurz gesagt: Form follows function. Wir sollten uns anschauen, was gebraucht wird. Wer kann es leisten? Wer soll es leisten? Wir sollten es so effizient wie möglich machen und dann schauen, ob wir dafür eine Grundgesetzänderung benötigen oder nicht. Aber auch hier möchte ich gerne erst das Konzept sehen und öffentlich diskutieren, damit wir wissen, ob wir das Grundgesetz überhaupt

anfassen müssen. Vielleicht müssen wir es, vielleicht müssen wir es auch nicht. Ich glaube, das Ganze kann im Rahmen dieses Gremiums entstehen. Ich habe vorhin eine Kommission vorgeschlagen, die sich das wirklich in Ruhe anschaut, mit unterschiedlicher Expertise besetzt ist und dann analysieren kann: Wo wollen wir weiter hin und wer kann es machen?

Abg. **Dr. Jens Zimmermann** (SPD): Ich würde Frau Bendiek gerne noch fragen. Sie haben in Ihren Ausführungen gesagt, es brauche mehr Bundeskompetenz und Unabhängigkeit. Vielleicht können Sie ausführen, warum Sie diesen Zweiklang als so wichtig erachten.

SVe **Dr. Annegret Bendiek**: Der Zweiklang ist für mich wichtig, denn – wie man in der Literatur auch sehr schön lesen kann – wir haben sehr viele Resilienzmaßnahmen in die Wege geleitet in den letzten Jahren, aber das hat nicht unbedingt dazu geführt, dass unsere Strukturen sicherer geworden sind und die Anzahl von Cyberangriffen und ihre Effektivität wirklich abgenommen haben. Insofern gibt es einen Bedarf – auch im Rahmen einer europäischen Handlungsfähigkeit –, dass diese Art von Strafverfolgung verbessert wird.

Deshalb sehe ich die Notwendigkeit, dem Bundeskriminalamt, vergleichbar – wie ich eingangs gesagt habe – wie im gemeinsamen Terrorabwehrzentrum quasi die Federführung zu geben, die Moderation und die Einladung durchzuführen, um damit im Prinzip die Gefahrenlage im Vorfeld besser sondieren und einen vertraulichen und inklusiven Informationsaustausch mit allen Ländern zusammen gewährleisten zu können, der zum Ziel hat, diese Strafverfolgung zu effektivieren.

Das ist der eine Standpunkt und der zweite ist das BSI. Wie wir gesehen haben, ist Cybersicherheit mittlerweile so breit gefächert, dass es eine gesamtgesellschaftliche Aufgabe ist. Es braucht auch Vertraulichkeit. Insofern glaube ich auch, dass es für eine europäische Koordinierung unabdingbar ist, dass das BSI diese Eigenständigkeit hat, um die Vertrauenswürdigkeit nicht nur nach innen, sondern auch nach außen gewährleisten zu können. Deshalb haben wir eine gute Balance, wo wir einerseits restriktiver werden und auf der anderen Seite aber auch der gesellschaftlichen Resilienz besser gerecht werden können.

Abg. **Nadine Schön** (CDU/CSU): Ich würde gern das Thema aufgreifen, über das eigentlich alle gesprochen haben: Wie können wir Strukturen und Kompetenzen neu ordnen und die Ressourcen sinnvoller einsetzen? Frau Schuetze hat dazu vorgeschlagen, die Cybersicherheitsstrategie nicht nur auf Bundesebene zu erstellen, sondern auch mit Ländern und Kommunen. Das erscheint mir sehr sinnvoll.

Ich würde gerne Ammar Alkassar befragen, was er von diesem Vorschlag hält. Wir haben natürlich nicht ewig Zeit, zu diskutieren, sondern müssen sehr schnell zu Lösungen kommen. Und die konkrete Frage wäre: Wie tariert man Ressourcen und Kompetenzen bestmöglich aus, um eine möglichst effiziente Aufstellung zu haben? Gerade, da wir sehen, dass sich die Situation im letzten Jahr noch deutlich zugespitzt hat.

SV **Ammar Alkassar**: Es ist ein grundsätzliches Thema, dass wir nicht viel Zeit haben. Das Thema Cybersicherheit in seiner Viralität und Entwicklung erfordert von allen Beteiligten schnelle Maßnahmen. Ich fand es schade, dass beispielsweise die Cybersicherheitsstrategie im vergangenen Jahr nicht noch einmal fortgeschrieben und upgedatet worden ist. Ich glaube schon, dass dies in immer kürzeren Zeiträumen aufgegriffen werden muss. Die Idee, eine Cybersicherheitsstrategie nicht nur des Bundes zu machen, sondern eine für Deutschland, an der die Länder maßgeblich mitwirken, aber auch mit Verantwortung übernehmen, das ist der entscheidende Punkt. Das halte ich tatsächlich für sehr wichtig.

Wichtig ist in dem Zusammenhang auch, wirklich dafür Sorge zu tragen, dass wir wenige Dopplungen haben. Es gibt – da hatte ich selber Verantwortung in einem Bundesland übernommen – die Entwicklung dahin, Landesämter für die Sicherheit der Informationstechnik zu schaffen. Flächendeckend halte ich das für eine falsche Entwicklung. Ich glaube, dass dort viel stärker abgegrenzt werden muss, welche Dinge tatsächlich vor Ort und welche zentral gemacht werden müssen. Dazu gehört es sicherlich auch, die Rechtsgrundlagen für das BSI zu stärken. Die Diskussion darüber in

Sachsen-Anhalt, dort helfen zu können oder nicht, ist ausgiebig geführt worden. Das BSI muss tatsächlich weiter gestärkt werden, damit es diese Aufgabe auch leisten kann.

Abg. **Nadine Schön** (CDU/CSU): Vielleicht kann ich da gleich anknüpfen. Wir waren mit dem Digitalausschuss in Estland und Finnland und haben gespürt, wie international anerkannt das BSI ist, das haben uns wirklich alle immer wieder bestätigt. Deshalb ist es bei allen Reformbemühungen wirklich wichtig, das BSI tatsächlich zu stärken. Daher die Anschlussfrage: Was wären die wichtigsten Punkte, die zur Stärkung des BSI führen? Und was sollte man besser nicht machen?

SV **Ammar Alkassar**: Was man nicht machen sollte, habe ich eingangs gesagt, und das haben die meisten Kollegen auch geteilt: Man sollte Strafverfolgung, technische Strafverfolgung und Cybersicherheit strikt trennen. Das ist im Grundsatz in den vergangen Jahren mit der Aufstellung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) genau gemacht worden. Die Einrichtungen müssen weiter ausgebaut werden, aber ich glaube, die strikte Trennung ist dort sehr wichtig.

In den vergangen Jahren hat sich positiv entwickelt, dass das BSI auch in der öffentlichen Wahrnehmung mit einer eigenen Stimme – auch weit über seine Verwaltungsaufgaben hinaus – wahrgenommen wird, was natürlich auch mit einer starken Stellung des BSI-Präsidenten zusammenhängt. Diese ist nicht negativ, sondern positiv, weil sie das Vertrauen der Zivilgesellschaft und der Wirtschaft in eine Verwaltungsbehörde trägt. Das ist ein ganz wichtiger Aspekt. Ein Aspekt, den dieses Haus maßgeblich mitsteuert, ist, dass es sehr gut war in den vergangen Jahren, das BSI mit einer umfassenden Erhöhung von Haushaltsmitteln und Planstellen auszustatten. Das wird aber weitergehen. Es ist nicht so, dass man sagen kann: Jetzt haben wir genug gemacht und das ist jetzt zu Ende – sondern es ist anzunehmen, dass das in den nächsten Jahren weitergehen wird. Das sind die wesentlichsten Aspekte.

Vielleicht noch ein Punkt, der in dieser Diskussion, auch in den Fragen, immer wieder durchschimmerte: Wie stark am Ende des Tages bestimmte Durchgriffsrechte des zuständigen Ressorts sind. Auch in der Zukunft, egal wie man es regelt, ob man es unabhängiger oder weniger unabhängig macht: Am Ende wird es immer auch in einer gewissen Öffentlichkeit stehen. Die Dinge, die das BMI für sich auch aus politischen Gründen für wichtig erachtet und möglicherweise auch „par ordre du mufti“ beim BSI durchsetzt, werden bei einer politischen öffentlichen Rechtfertigung immer im Raum stehen, und ich glaube, das gehört zum politischen Tagesgeschäft dazu.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Meine erste Frage geht an Frau Schuetze. Sie haben in Ihren Stellungnahmen – mündlich und schriftlich – schon auf die besonderen Herausforderungen im föderalen Staat verwiesen. In zentralisierten Staaten brauchen sie aber auch einen effektiven Informationsaustausch über die verschiedenen Ebenen. Von daher die Frage: Inwieweit sind die Herausforderungen dort anders? Und da es auch zum Föderalismus passt: Sie haben eine Art Eva-Prinzip empfohlen für Prävention und auch für Detektionswerkzeuge. Wer sollte Ihrer Meinung nach die Standards setzen?

SVe **Julia Schuetze**: Zentral organisierte politische Systeme haben es zum Beispiel einfacher, zu sagen: Wir wollen die Verwaltung schützen – unsere Verwaltung. So hat man eine Ebene, und die Angriffserkennungssysteme zum Beispiel und die Technologie, die dafür genutzt wird, werden dann einfach bei allen ausgerollt. Das können wir hier nicht machen. Das müssten die Länder übernehmen, auch die Kommunalverwaltungen. Und davon haben wir Tausende. Das ist eine Herausforderung bei uns, die einzigartig ist. Ich hatte gleichzeitig aber auch gesagt, dass es große Chancen gibt, regionale Strukturen aufzugreifen und diese zu nutzen.

Ähnlich sieht es bei einem Meldeverfahren aus. Das ist zentral, wenn es um die KRITIS-Betreiber geht, aber freiwillige Meldungen – wie auch schon angesprochen –,kommen vielleicht bei der Polizei an, manchmal meldet man vielleicht trotzdem ans BSI. Es gibt aber natürlich auch Landesbehörden, die Meldungen annehmen – und so hat man keinen zentral organisierten Informationsaustausch. Wir müssen Wege finden, wie wir uns einigen, wer welche Informationen

aufnimmt und wie diese geteilt werden – und da kommt zum Beispiel auch diese Zentralstellenfunktion ins Spiel. Sagen wir, wir wollen permanent automatisch sowie strukturiert Informationen austauschen und wir brauchen dafür auch gemeinsam eine Technologie, die wir nutzen? Die wird dann vielleicht vom BSI bereitgestellt oder die Informationen laufen beim BSI so zusammen, dass es ein Informationsknotenpunkt wird und Datenbanken entstehen.

Wenn es eine Grundgesetzänderung braucht, dann genau für diese Policy-Option. Dann kann man das gut diskutieren, da es eine Funktion hat. Wir müssen einfach mit dem föderalen System arbeiten. Bei dem zweiten Punkt: Das Eva-Prinzip ist ein Beispiel für Leistungen wie zum Beispiel Sensibilisierungsmaßnahmen nach einer bestimmten Qualität, die dann auch bundesweit geteilt werden können. Ich sehe da ganz klar, dass das BSI diese Standards setzen sollte. Das BSI hat die Expertise, und man kann zusammenarbeiten, um zum Beispiel in einem Stufensystem zu sagen: Für kleine Kommunalverwaltungen ist es innerhalb von einem Jahr nicht möglich, diesen BSI-Grundschutz sofort umzusetzen, aber vielleicht können wir das in einem Schrittverfahren. Es gibt auch schon Bewegungen, die in diese Richtung gehen. Von daher sollten die Standards bei Leistungen, die nachnutzbar sind, geteilt und vom BSI gesetzt werden.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Sie sprechen in Ihrem Gutachten von einer IT-Sicherheits-Fachkräfteinitiative. Auf dem globalen Markt haben IT-Fachkräfte nach Deutschland relativ privilegierten Zugang. Ich wüsste gerne von Ihnen: Inwieweit unterscheidet sich Ihre IT-Sicherheits-Fachkräfteinitiative von Konzepten, die es schon gibt? Welche speziellen Bedarfe sehen Sie? Gibt es konkrete Good Practices, die Sie hervorheben wollen?

SVe **Julia Schuetze**: Wir versuchen, momentan folgendermaßen Fachkräfte auszubilden: Wir haben einen Standard, den zum Beispiel IT-Sicherheitsbeauftragte kennen sollten. Das macht auf jeden Fall in Teilen Sinn. Aber wenn wir über Krisenmanagement nachdenken oder Notfallbearbeitung im Business Continuity Management-Standard, sehe ich eigentlich das Potenzial, dass wir schon Krisenstäbe in Deutschland haben.

Wir haben Kommunikationsmanager:innen, die schon sehr gut ausgebildet sind und die vielleicht Teile von dem BCM-Standard kennen sollten – im Falle von einem Cybervorfall in ihrer Organisation oder in Kommunalverwaltungen. Dort sehe ich Potenzial für Zielgruppen, diesen Standard, das Wissen und die Weiterbildung zu organisieren. Ich sehe noch keine koordinierte Initiative deutschlandweit, bei der man sagt: Okay, Krisenstäbe müssen das können und so können sie das lernen.

Abg. **Maximilian Funke-Kaiser** (FDP): Es wurde schon mehrfach ausgeführt, dass wir keine Zeit mehr haben. Das ist klar. Wir leben in einer angespannten geopolitischen Lage. Gerade heute haben prorussische Hacker der Gruppe Killnet die Drohung ausgegeben – aufgrund der Entscheidung, die richtigerweise jetzt von der Bundesregierung getroffen wurde, Leopard-Panzer zu schicken – mit Cyberattacken auf deutsche Firmen und Behörden zu antworten. Was klar ist: Wir müssen uns dagegen verteidigen. Wir brauchen allerdings keine offensive Cyberstrategie, sondern eine defensive Cybersicherheitsstrategie. In Ihrer Stellungnahme, Herr Atug, haben Sie darauf hingewiesen, dass man nicht zwischen aktiver und defensiver Cyberabwehr unterscheiden sollte, sondern zwischen offensiver und defensiver Cyberabwehr. Könnten Sie zu Beginn erst einmal Bezug darauf nehmen, wo hier die Grenze verläuft?

SV **Manuel Atug**: Ich weiß nicht, was unter aktiver Cyberabwehr zu verstehen ist. Aber „defensiv – offensiv“ ist das, was man im Cyberraum kennt. Man kann defensiv oder offensiv agieren. Die Grenze zwischen offensiver und defensiver Cyberabwehr ist im Wesentlichen die Erhaltung der Integrität und Vertraulichkeit der entfernten, angegriffenen Systeme, die in der Regel selber Opfer eines Angriffs waren und jetzt als Angriffssystem missbraucht werden. Wenn ich ein Angreifer wäre, würde ich nicht von meinem System aus Deutschland oder kritische Infrastruktur in Deutschland angreifen, sondern erst einmal etliche verschiedene Systeme kompromittieren und von denen aus angreifen. Im Idealfall – wenn man mich wirklich wegcybern möchte, mit irgendwelchen Hackbacks oder anderen offensiven Maßnahmen – nehme ich ein

Krankenhaus, also kritische Infrastruktur in Deutschland und kompromittiere dort ein System. Diese sind meist recht desolat aufgestellt. Ich nehme vielleicht ein kommunales oder ein Landessystem, die meistens auch sehr archäologisch wertvoll betrieben werden. Dort kann ich also schnell etwas übernehmen. Wenn man tatsächlich meint, einen Gegenangriff starten zu wollen – aktiver Sorte –, um mich auszuschalten und ich immer noch ein ausreichendes Dutzend anderer Systeme habe, nehme ich eine Cloud-Infrastruktur. Dann werden noch mehr Leute zurückgesammelt. Abgesehen davon: Wenn von einem System eine Infrastruktur angegriffen wird und man einen Gegenangriff startet, dann nennt man das im Völkerrecht – soweit ich das richtig verstanden habe – einen Vergeltungsschlag. Das ist normalerweise nicht so ganz legitim. Wir sollten darüber also gar nicht reden, weil wir immer noch verfassungsrechtlich korrekt agieren wollen.

Aber wenn ich als Angreifer, als Akteur mehrere Hundert oder sogar Zehntausende Systeme für Distributed Denial of Service (DDoS)-Angriffe übernehmen, steuern und aktiv betreiben kann, ist es vermessen, zu behaupten, ich könnte mit aktiven, also offensiven Maßnahmen etwas lahmlegen. Das ist ein Wunschtraum, aber in der Realität hilft einfach nur, in der Defensive die Systeme stabil zu betreiben, durch strukturiertes Sicherheitsmanagement, durch prozessorale Vorgehensweisen, die wirklich gelebt werden.

So wie ich es im Eingangsstatement gesagt habe: Ein Airbag zündet genau dann, wenn er soll – nicht einmal zu viel, nicht einmal zu wenig. Darin steckt Firmware, die programmiert worden ist mit Produkthaftung, mit Verantwortung und mit sicherer Umsetzung. Ransomware-Tätergruppierungen haben anfangs desolate, schrottige Müllsoftware produziert. Die Polizeibehörden haben entsprechende Schlüssel, damit sie sofort zurückgenerieren können, weil sie schlechte Verschlüsselung, schlechte Programmierung gemacht haben. Heutzutage ist Ransomware mit die am besten programmierte Software der Welt, weil sie einfach sicher programmiert wird. Es wird sicher entwickelt, es wird minimal entwickelt, es gibt eine starke Verschlüsselung, es gibt eine ordentliche Implementierung der Verschlüsselung. Die haben daraus gelernt, weil sie einfach jedes Jahr hunderte Millionen Dollar im Jahr an Umsatz machen. Der ist meist steuerfrei und dann auch gleich dem Gewinn. Das ist eine sehr hohe intrinsische Motivation. Aber es liegt nur an der Motivation. Man kann das defensiv lösen.

Abg. **Maximilian Funke-Kaiser** (FDP): Sie haben gerade ausgeführt, dass Schwachstellen im Grunde auch sehr gerne genutzt werden. Für wie wichtig erachten Sie den Passus im Koalitionsvertrag, ein wirksames Schwachstellenmanagement einzuführen? Und wie sollte das Ihrer Ansicht nach umgesetzt werden?

SV **Manuel Atug**: Auf gar keinen Fall – Schwachstellen werden behoben und nicht gemanagt. Das ist völliger Humbug. Jede Schwachstelle, die wir offen halten, halten wir offen für den Staat, für die Wirtschaft, für die Forschung und Wissenschaft und für die Zivilbevölkerung – und ganz nebenbei auch für kritische Infrastrukturen. Jede Schwachstelle, die nicht behoben wird, bedroht Menschenleben in Deutschland, in Europa und weltweit. Wir können nicht ausklammern, dass andere Systeme davon mitbetroffen werden, die uns persönlich auch belangen. Als Zivilgesellschaft und als Bürger dieser Nation würde ich gern sagen: Ich möchte keine Schwachstellen gemanagt bekommen. Ich möchte sie behoben bekommen.

Abg. **Steffen Janich** (AfD): Meine ersten Fragen gehen ebenfalls an Herrn Manuel Atug. In Ihrem Gutachten auf Seite 21 warnen Sie vor IT-Schnittstellen für Sicherheitsbehörden, die bereits seit den 1990er Jahren ebenso wie normale Softwareschwachstellen von Unbefugten ausgenutzt werden. Sind Ihnen in dieser Richtung Studien, Gutachten oder Berichte bekannt, die die unbefugte Nutzung speziell von IT-Schnittstellen für Sicherheitsbehörden einmal umfassend dokumentieren?

SV **Manuel Atug**: Es gibt ein sehr bekanntes Beispiel, wie Sicherheitsbehörden und Nachrichtendienste das haushoch vergeigt haben. In den USA haben Geheimdienste Schwachstellen zu Hauf und auch Sicherheitslücken strukturiert gesammelt und gegen Freunde oder eben auch Nicht-Freunde verwendet. Da ist unter anderem EternalBlue verschwunden. Was mindestens fünf

Jahre von den Geheimdiensten in den USA bekannt war, ist eine wesentliche Schwachstellenkonstellation in Microsoft Windows-Serversystemen gewesen. Das wurde abgegriffen, von anderen Akteuren in WannaCry und NotPetya implementiert und anschließend auf die Welt losgelassen. Was Nachrichtendienste da herausgefunden und zurückgehalten haben, hat mehrere 100 Millionen Schäden bei großen Konzernen und Milliardenschäden insgesamt auf der ganzen Welt produziert. Alle zucken die Achseln, selbst die Wirtschaft hat darauf nicht angemessen reagiert. Aber diplomatisch war das schon relativ uncool, was man da fabriziert hat.

Ansonsten gibt es auch Lawful Interception-Schnittstellen, wie für Staatstrojaner, die auch Schwachstellen missbrauchen und solche Schnittstellen besitzen müssen. Das ist natürlich auch eine Schwierigkeit, da wir die nicht davor schützen können, dass insoweit Kriminelle agieren. Der Chaos Computer Club hat gezeigt, wie so eine Implementierung aussehen kann, wenn man ein solches System missbraucht und verwendet, um Vollzugriff auf die kompromittierten Systeme zu erhalten. Ansonsten gibt es noch die sogenannte Paragraph 9-Schnittstelle der DE-Mail. Das war ein Insidergag über Jahre. Zur DE-Mail hieß es: Das ist starke Verschlüsselung, Ende-zu-Ende, alles sicher, jeder bekommt ein sicheres Postfach. Leider ist es Ende-zu-Ende-zu-Ende gewesen. Denn dazwischen schaut man ganz kurz in Antivirus und Spam und die Nachrichtendienste gucken dann auch nochmal in den Inhalt – das ist insofern auch ein Missbrauch, und dieser Missbrauch findet durch staatliche Akteure statt.

Weltweit ist eine Büchse der Pandora geöffnet worden, die im Cyberraum ganz massiv skaliert. Es ist nicht so, dass eine Schwachstelle *ein* Türschloss ist, das ich aufbreche und dann in *ein* Haus eindringe, sondern ich öffne einfach weltweit jedes baugleiche Türschloss. Die Kriminellen werden nicht einfach sagen: Der Kelch geht an mir vorbei, die paar 100 Millionen hole ich nicht ab. Nachrichtendienste greifen sich natürlich gegenseitig genau diese Schwachstelle ab. Wir haben auch bei Uniper, bei Cisco und bei allen möglichen anderen Herstellern gesehen, dass solche Lücken implementiert wurden. Und dann wurde gesagt: Oh, Entschuldigung, das haben wir gar nicht so gemeint. Immer erst dann, wenn eine solche Hintertür für Nachrichtendienste publik und von Kriminellen missbraucht wurde, wurde so eine Schwachstelle geschlossen. Das sind ein paar Beispiele und Auszüge.

Abg. **Steffen Janich** (AfD): Auf Seite 22 Ihrer Stellungnahme schildern Sie als grundrechtsschonende Strafermittlung die richterliche Beschlagnahme von Computern und deren forensische Untersuchung. Die Ermittlungsbehörden sind jedoch auch auf die Auswertung laufender Kommunikation von Verdächtigen angewiesen – so wie früher die richterliche Öffnung von Briefpost erfolgte. Welche technischen Maßnahmen sehen Sie dafür als grundrechtsschonend und geeignet an?

SV **Manuel Atug**: Technisch genau gar keine. Die Maßnahmen sind nicht grundrechtsschonend. Sie brauchen eine vernünftige Ausbildung von Mitarbeiter:innen, die kompetentes Niveau haben, und auch gutes Arbeitsmaterial. Die Polizeibehörden arbeiten teilweise mit Vorkriegsmodellen auf Menü-Interface-Art. Ich hab mir das angeguckt und gesagt: So musst du das eintippen? Dann verstehe ich, dass du keinen Bock mehr darauf hast. Da wird man ja wahnsinnig schon beim Versuch, das Ganze einzutragen. Abgesehen davon, dass die teilweise noch nicht einmal genau wissen, was eine Online-Strafanzeige gegen Rechtsradikale mit Hakenkreuzen oder gegen Leute ist, die Frauen Direct Messages schicken: "Ich werde dich vergewaltigen, hier ist deine private Adresse". Die sind ja noch nicht einmal in der Lage, das aufzunehmen. Was soll man denn da noch technisch kompromittieren und die Unsicherheit für alle Systeme integrieren? Es ist immer noch so, dass Ermittlungsbehörden mit ordentlicher Arbeit wirklich hocheffektiv sind und auf „Cyber-Irgendwas-Protokollen-Logdaten“ in den seltensten Fällen irgendwelche Terroristen erwischen. Wir haben ganz andere Probleme. Das sollten wir nicht auf technische Art lösen. Wir brauchen kompetente Ermittlungsbehörden, die kompetent arbeiten und nicht mit irgendeiner technischen Lösung vermeintliche Allheilmittel für soziale Probleme mit sich bringen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Meine Fragen richten sich zunächst an Frau Professor

Sasse. Es gibt – das haben wir schon in den Eingangsstatements gehört – diverse verschiedene und parallele Informationsangebote, vor allem auch online. Können Sie uns erläutern, wie man – anstatt immer mehr parallele Angebote zum gleichen Thema zu schaffen – die Wirkung auf eine andere Art und Weise erreichen kann, zielgruppenspezifiziert et cetera? Das würde mich interessieren.

SVe **Prof. Dr. Martina Angela Sasse**: Tatsächlich wäre zielgruppenspezifische Aufbereitung gut und dann auch auf die Kanäle und Medien zu gehen, wo diese Zielgruppen unterwegs sind – denen sie vertrauen, wo sie zum Beispiel eine Ansprechgruppe haben. Wenn man über spezifische Bedrohungen und Betrugsmaschen aufklärt, die in Online Gaming-Foren gängig sind, dann wäre es am besten, darüber auf diesen Plattformen selbst und in den Foren, wo Gamer sich treffen und Informationen austauschen, zu sprechen und wie sie sich dagegen schützen können. Das wird immer noch nicht genug genutzt. Das Gleiche gilt für die sozialen Medien, wo viele junge Leute unterwegs sind.

Das wären auch die richtigen Medien, um die Bedrohungen und Gefahren, die für sie relevant sind, zu besprechen. Denn erst einmal hat dies den Vorteil, dass man diese Zielgruppen dort erreicht. Das Zweite ist, dass dadurch diese Bedrohung in den Diskurs dieser Gruppen kommt. Das heißt, es ist wichtig, dass sie untereinander – also Teenager mit anderen Teenagern – über diese Bedrohung und über die Schutzmaßnahmen sprechen. Dinge von oben, von einer offiziellen Behörde oder von irgendwelchen angeblichen Autoritätsfiguren, kommen nicht besonders gut an.

Ich denke, das ist noch nicht verstanden worden, und das ist wichtig. Wenn wir in unseren Untersuchungen fragen „Wo holen Sie sich Informationen über Bedrohungen und wie Sie sich davor schützen können?“, dann sind top immer die populären Medien oder Freunde und Familie. Wie gut die Ratschläge und Anweisungen sind, die da verbreitet werden, ist sehr gemischt. Wir sollten trotzdem diese Kanäle nutzen, aber dafür sorgen, dass die richtigen Informationen zur Verfügung stehen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich höre heraus: Der durchschnittliche 16-Jährige sucht nicht auf der Plattform des BSI. Ich würde bei dem groben Thema bleiben. Sie haben in Ihrer Stellungnahme auch Begriffe wie Usable Security und Human Centred Security erwähnt. Können Sie uns aufklären, was sich dahinter verbirgt und warum das wichtig ist?

SVe **Prof. Dr. Martina Angela Sasse**: Was sich dahinter verbirgt ist, dass wir die Technik so gestalten müssen, dass sie nach bestem Wissen und dem jetzigen Wissensstand sicher sein muss und die Sicherheit einfach zu nutzen ist. Im Moment wird das oft nicht gemacht und stattdessen wird massiv auf sogenannte Security Awareness und Trainingsmaßnahmen gesetzt, die aber erst einmal in der Qualität oft nicht gut sind und zweitens auch kein sicheres Verhalten ausbilden und unterstützen.

Es müsste umgekehrt werden: Wir sollten mehr darin investieren, die Sicherheit so gut wie möglich entweder automatisch zu machen oder so einfach wie möglich benutzbar zu machen. Und wir sollten nicht mehr so lange über Kommunikation reden.

Das andere ist, dass Kompetenzen trainiert werden müssen. Das sehe ich gerade auch in Schulen oder auch da, wo Fachkräfte geschult werden, zum Beispiel IT-Sicherheitsentwickler, die oft letztendlich die Schwachstellen in den Code einbauen. Man sollte nicht immer nur mit geschriebenem Material werben, sondern die Umsetzung des richtigen Programmierens üben. Die Kompetenz muss etabliert werden. Da sind wir im Moment sehr schwach. Es geht alles nur über Text und Anweisungen, und das bringt nichts.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Können Sie am Beispiel Passwörter das Thema noch einmal erläutern? Bekannt ist ja – wir kennen das auch hier im Bundestag: Alle sechs Monate muss man sich ein neues Passwort nach bestimmten Kriterien ausdenken. Ist das ein guter Tipp?

SVe **Prof. Dr. Martina Angela Sasse**: Nein, es ist wissenschaftlich nachgewiesen, dass ständiges Passwörterverändern zu schwächeren Passwörtern führt, was inzwischen auch das BSI offiziell in Kampagnen als Sicherheitsirrtum bezeichnet. Es wird immer über Komplexität geredet und es werden Beispiele gegeben, die die Leute völlig

verschrecken. Keiner redet über Multi-Faktor-Authentifizierung, Passwortmanager und einfache Methoden, die wirklich die Passwörter sicherer machen würden.

Die **Vorsitzende**: Als Ausschussvorsitzende möchte ich Professor Kipker gerne zur Sicherheitsarchitektur befragen. Das Wimmelbild ist beschrieben worden. Die Verantwortungsdiffusion ist mehrmals genannt worden. Sie schreiben auch selber in Ihrer Stellungnahme von Zielkonflikten. Wie würden Sie die institutionellen Zuständigkeiten neu verteilen und welche Akteure und Institutionen sollten aus Ihrer Sicht tendenziell gestärkt, welche vielleicht auch vernachlässigt werden? Welche Rolle sollte das BSI spielen? Wie kann die Zusammenarbeit insgesamt verbessert werden? Sie sprechen von einer möglichen essenziellen Public Private Partnership-Zusammenarbeit. Wie könnte so eine Zusammenarbeit aussehen? Wenn man diese ganzen Veränderungen voranbringt, welche Priorität würden Sie setzen?

SV **Prof. Dr. Dennis-Kenji Kipker**: Die Rolle des BSI ist schon mehrfach bei den anderen Anhörungen zur Sprache gekommen. In erster Linie geht es darum, erst einmal zu ermitteln, was überhaupt die Aufgabe des BSI ist und vorgelagert, was überhaupt Cybersicherheit ist. Das habe ich auch zur Geltung gebracht. Wir haben in den letzten Jahren die Tendenz gehabt – und deswegen sprechen wir mittlerweile auch von diesem Wimmelbild der Verantwortungsdiffusion –, dass wir eben in den Bereich Cybersicherheit oder IT-Sicherheit, wie man den Begriff auch definieren mag, immer mehr Akteure einbezogen haben.

Wenn man das Ganze von einer juristischen Warte aus anschaut, dann ist es so: Cybersicherheit ist grundrechtlich, verfassungsrechtlich verbürgt, einerseits im Rahmen des Computergrundrechts, aber andererseits ist es natürlich auch so, dass Cybersicherheit mittelbar andere grundrechtlich geschützte Interessen schützen kann. Also beispielsweise auch Leib, Leben und körperliche Unversehrtheit. Das hat Manuel Atug in seiner Stellungnahme dargestellt. Dort muss man ganz deutlich abschichten. Es wird auf jeden Fall so sein: Selbst wenn man eine neue nationale Cybersicherheitsarchitektur aufstellen sollte, wird diese nie zu hundert Prozent frei von Konflikten und Interessenkonflikten sein, weil wir letzten Endes immer in einem Austausch der Grundrechte leben.

Was die Rolle des BSI und auch die Rolle der Cybersicherheitsarchitektur angeht, ist mein Vorschlag, zuerst zu überlegen: Was ist Cybersicherheit? Fallen beispielsweise Maßnahmen wie hoch umstrittene digitale Gegenschläge in den Bereich der Cybersicherheit im operativen Sinne hinein? So verstehe ich Cybersicherheit in erster Linie. Ich glaube, es ist auch relativ deutlich geworden, dass Cybersicherheit operative, technische und organisatorische Maßnahmen zum Schutz von Behörden, Unternehmen und Bürgern sind. Alles, was darüber hinausgeht, also insbesondere im Hinblick auf dieses Thema digitale Gegenschläge, hat meiner Meinung nach erst einmal relativ wenig damit zu tun. Unabhängig natürlich von der völkerrechtlichen, verfassungsrechtlichen Dimension und der natürlich technisch äußerst zweifelhaften Dimension.

Was die Rolle des BSI angeht, wurde insbesondere seit dem letzten Jahr sehr viel über die Unabhängigkeit oder die – wie auch immer geartete – fehlende Unabhängigkeit des BSI gesprochen. Natürlich ist es so: Wir haben ein BSI, das unter der Ägide des BMI arbeitet. Das bringt natürlich Interessens- und Zielkonflikte mit sich. Eine Ressortverschiebung – das hatte ich auch in meiner Stellungnahme dargelegt – würde meiner Meinung nach relativ wenig bringen, weil dann andere Interessens- und Zielkonflikte bestehen. Das heißt, wir müssen wirklich darüber nachdenken, wie man das BSI stärken kann. Wir reden hier auch über den Ausbau der Zentralstellenfunktion des BSI. Wir reden über eine Grundgesetzänderung, die aber auch dann in einem nachgelagerten Schritt nur Sinn macht, wenn man sich überhaupt bewusst ist, was eine solche Grundgesetzänderung letzten Endes bezwecken soll. Dann kann man auch darüber reden, das BSI in einer anderen Rolle zu sehen. Die unterschiedlichsten Ansätze werden schon seit Jahren diskutiert. Das ist nicht neu.

Die Stiftung Neue Verantwortung ein Papier dazu verfasst und auch verschiedene andere Organisationen, wie man so etwas organisatorisch umsetzen und aufhängen könnte. Aber ich glaube, das ist etwas – wie Sven Herpig auch schon gesagt

hat – was nähere fachliche Betrachtung benötigt, wie man diesen Interessenausgleich herstellen kann. Eine bloße Ressortverschiebung bringt meiner Meinung nach relativ wenig. Wir müssen definitiv über eine größere, institutionelle Unabhängigkeit der Behörde nachdenken und überlegen, ob Bereiche aus der Behörde, die nicht originär Cybersicherheit im operativ-technisch-organisatorischen Sinne abdecken, gegebenenfalls auch anderen Ressorts zugeschoben werden können. Was die Verbesserung der Zusammenarbeit angeht, das war der zweite Teil der Frage: Wir haben bereits – insbesondere im Bereich KRITIS-Schutz – umfassende Public Private Partnership umgesetzt und implementiert. Meiner Meinung nach in den letzten Jahren auch recht erfolgreich und wir haben beispielsweise das BSI für Bürger – was auch grundsätzlich eine sehr lobenswerte Initiative ist – unabhängig von der Frage, wer tatsächlich auf die Seite des BSI schaut. Aber es ist so, dass gerade der Mittelstand, die KMU, die immer wieder erfolgreich angegriffen werden, nicht immer diese ganzen Cyberbedrohungen, Abwehrmaßnahmen und Zuständigkeiten kennen. Dort besteht meiner Meinung nach noch erheblicher Verbesserungsbedarf. Insoweit stellt sich für mich die Frage, ob an dieser Stelle wirklich eine Zentralstellenfunktion des BSI etwas nutzen kann. Wir in Bremen arbeiten zurzeit an einer neuen Cybersicherheitsstrategie, und da geht es gerade darum, digitalen Bürgerschutz vor Ort zu stärken, weil Cybersicherheit auch eine Frage von Vertrauen ist. Wen kennt man und wen spricht man im Zweifelsfall von behördlicher Seite auch auf Cybervorfälle an?

Die **Vorsitzende**: Wir kommen in die zweite Runde. Da die Zeit fortgeschritten ist, würde ich vorschlagen, wir gehen auf vier Minuten. Für die SPD hat Johannes Schätzl das Wort.

Abg. **Johannes Schätzl** (SPD): Meine Frage geht an Herrn Dr. Herpig: Auch Sie schreiben von der Notwendigkeit eines unabhängigeren BSI. Könnten Sie das aus Ihrer Sicht definieren und eventuell auch etwas zur Ausgestaltung sagen. Vielleicht auch im Hinblick auf die Frage, welche Fachabteilungen besonders weisungsfrei agieren sollten.

SV **Dr. Sven Herpig**: Grundkonsens ist, das haben wir schon mehrfach gehört, dass das BSI integer bleiben sollte. Das heißt, wir sollten das BSI auf keinen Fall aufspalten – aufgrund der internen Wertschöpfungsketten und der Prozesse, die dort vorhanden sind. Natürlich geht es hier vor allem um die fachliche Unabhängigkeit der Bereiche OC (Operative Cybersicherheit), TK (Technikkompetenzzentren) und KM (Kryptotechnik) und ähnlichen Bereichen, die fachlich unabhängig operieren sollten. Es gibt mehrere Modelle, wie wir sie in einem anderen Ressort haben könnten, wie es eine Aufsicht durch den Bundestag geben könnte, analog zum BfDI. Sollten wir uns dazu entscheiden, es innerhalb des Innenressorts zu belassen, kann die fachliche Unabhängigkeit des BSI vom BMI dadurch sichergestellt werden, dass es keine Ergebnisweisungen mehr vom BMI an das BSI geben kann, dass über breite Arbeitsprogramme gesteuert wird, dass es eine Ex post-Aufsicht der Arbeit des BSI durch das BMI gibt. Dass aber auch die politischen Entscheidungen des BMI, die fachliche Entscheidungen des BSI vielleicht übertrumpfen, in einer Registratur festgehalten werden und durch Ausschüsse wie diesen hier einsehbar sind, damit Transparenz darüber herrscht, was eine politische und was eine fachliche Entscheidung ist.

Wir sollten darüber reden, § 22 der Gemeinsamen Geschäftsordnung zu überbedenken. Warum gibt es hier eine Ausnahme? Warum muss man immer, wenn man mit dem BSI reden will als anderes Ressort, zum Innenministerium gehen und dort Bescheid sagen, beziehungsweise warum muss das BSI Bescheid sagen? Wir sollten auch darüber reden. Ich bin auch der Meinung, dass der Chief Information Security Officer des Bundes (CISO Bund) vielleicht gleichzeitig der Präsident oder die Präsidentin des BSI sein sollte. Aber dann darf diese Person nicht in einem fachlichen Weisungsverhältnis zum Innenministerium stehen, denn dort ist der Chief Information Officer (CIO) angehängt – als Staatssekretär Markus Richter. Der CISO darf laut Literatur dem CIO nicht in einem Weisungsverhältnis unterstellt sein, weil ansonsten die Cybersicherheit vernachlässigt wird. Von daher gibt es einige Ideen, wie man es umsetzen kann, sowohl im BMI-Ressort als auch außerhalb.

Abg. **Johannes Schätzl** (SPD): In Ihrer Stellungnahme setzen Sie sich auch mit aktiver

Cyberabwehr und Hackbacks auseinander. Können Sie insoweit noch einmal eine kurze Definition geben und beantworten, bis wohin aktive Cyberabwehr sinnvoll und – mit einem Fragezeichen versehen – vielleicht sogar notwendig ist, und wo hingegen rote Linien zu ziehen sind?

SV **Dr. Sven Herpig**: Ich kann meine Definition gerne nennen, aber es ist fraglich, ob die Bundesregierung diese teilt. Mich würde die Definition der Bundesregierung interessieren und welche Befugnisse darunter fallen. Aber meine oder unsere Definition, erarbeitet durch eine transatlantische Expertengruppe, ist: Aktive Cyberabwehr sind eine oder mehrere technische Maßnahmen, die von einem einzelnen Staat oder einem Kollektiv von mehreren Staaten gemeinsam durchgeführt oder von einer staatlichen Stelle angeordnet werden mit dem Ziel, die Auswirkungen einer bestimmten, laufenden, böswilligen Cyberoperation oder -kampagne zu neutralisieren und/oder abzuschwächen und/oder sie technisch zuzuordnen, also zu attribuieren.

Abg. **Johannes Schätzl** (SPD): Der zweite Teil der Frage wäre gewesen, bis wohin Sie den Einsatz von aktiver Cybersicherheit als notwendig oder sinnvoll erachten.

SV **Dr. Sven Herpig**: Auf Basis der uns zur Verfügung gestellten empirischen Grundlage durch die Sicherheitsbehörden bin ich der Meinung, dass wir aktuell gut aufgestellt sind mit den Befugnissen, die es gibt. Ich lasse mich gerne eines Besseren belehren, wenn es dafür eine empirische Grundlage gibt, die mir zur Verfügung gestellt wird.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Meine Fragen richten sich an Frau Dr. Frey. Vielen Dank für Ihren aufrüttelnden Bericht aus der Praxis und von der Basis. Es drängen sich natürlich ein paar Fragen auf. Die erste Frage ist: Warum gehen Ihre Kunden, wie Sie geschrieben haben, nicht zur Polizei?

SVe **Dr. Stefanie Frey**: Man geht eigentlich nur zur Polizei, um Hilfe zu bekommen. Wenn schon klar ist, dass die Hilfe nicht kommt, weil die Strukturen zu kompliziert sind und die Anlaufstellen nicht klar sind, besteht wenig Anreiz. Dann bleibt nur noch übrig, dass die Reputation des Unternehmens zu Schaden kommt. Es muss ein Mehrwert dadurch entstehen, zu melden. Natürlich raten wir immer dazu und es wird auch von unseren Kunden immer gemeldet. Denn das ist der Prozess, den wir fördern müssen. Wir müssen das Dunkelfeld erhellen, und das passiert nur durch Meldungen. Aber die Anreize fehlen. Die Diskussion, die wir heute Nachmittag führen, geht um Strukturen. Es geht um das BSI. Für uns ist es unwichtig, ob das BSI unabhängig oder nicht unabhängig ist. Am Ende des Tages brauche ich beim BSI jemanden, der da ist und uns helfen kann, unseren Kunden zu helfen. Das BSI muss dazu befähigt sein, uns auch aktiver in unseren Anliegen mit den Kunden zu unterstützen. Denn neunundneunzig Prozent Dunkelziffer ist ein No Go. Das geht nicht.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Sie haben gesagt, Sie identifizieren die Täter. Wie können Sie sie identifizieren und aus welchen Ländern kommen sie?

SVe **Dr. Stefanie Frey:** Das ist eine schwierige Frage. Wir sagen immer: Wenn man nicht weiß, wer es war, waren es Russland oder China. Deswegen ist auch die Hackback-Geschichte ein Problem. Wenn nicht attribuiert werden kann – gegen wen willst du hackbacken? Die Strafverfolgung muss die Täter ermitteln. Aber wie ich vorher schon erwähnt hatte: Die Täter sind schon so straffrei in ihren gemütlichen Zonen, dass sie sich selber identifizieren. Im Täterschreiben steht schon, wer es war. Wir wissen, wer es ist, aber wir können ihn nicht zur Rechenschaft ziehen. Wir können keine Strafaktionen gegen diese Täter führen, da sie sehr oft auch staatlich getrieben sind, durch organisierte Banden. Wir reden von Straftaten und organisierter Kriminalität, die auch mittelständische Unternehmen treffen. Wir wissen schon, dass diese Angriffe kommen werden. Panzerlieferungen an die Ukraine – wir wissen, dass das bei den Russen nicht gut ankommt. Der Angriff wird kommen, aber wir müssen krisenfest sein. Das sind wir nicht. Das können wir mit diesen ganzen Strukturen, die wir heute haben, absolut nicht bekämpfen.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Die Angriffe, von denen Sie reden, sind das eher Ransomware-Angriffe, wie mit der Schrotflinte, oder sind es gezielte Angriffe auf einzelne Unternehmen und wenn ja, mit welchem Fokus?

Spionage oder Erpressung?

SVe **Dr. Stefanie Frey**: Wir haben in den letzten Jahren vermehrt ganz gezielte Targeted Attacks, wo wir auch in den Adressen sehen, dass dieses Unternehmen im Ziel der Täter war. Es ist nicht mehr so ein Massenphänomen, wie wir es früher hatten, wie dieses NotPetya, sondern es ist ganz gezielt auf diese Unternehmen. Jetzt kommt das ganz Schwierige an der Geschichte: Die Täter sind meistens bis zu fünf Monaten in den Infrastrukturen der Opfer – unbemerkt. Dann kommen die Kunden und sagen: Ja, ich habe eine Firewall. Ich habe das alles. Ich habe die ganzen technischen Präventionsmaßnahmen eingeführt. Warum hat man mich angegriffen? Weil die Täter immer durchkommen. Die haben ganz klare Ziele. Also müssen wir krisenfest werden, wenn der Fall passiert.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Sie haben vorher von dem LKA gesprochen. Können Sie noch ganz kurz sagen, in welchem Land Sie mit dem LKA gesprochen haben?

SVe **Dr. Stefanie Frey**: Wir müssen immer dem LKA melden, wo der Sitz des Opfers ist. Wir haben schon ziemlich mit fast jedem LKA in der Bundesrepublik geredet.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Meine erste Frage geht an Professor Kelber. Bezogen auf Ihre Antwort auf Frage 4: In politischen Diskussionen wird der Datenschutz oftmals als Bremser oder Verhinderer dargestellt. Das ist ein Image, das den Datenschutz an der Stelle nicht loslässt. Angesichts der horrenden Schadensummen, die Bürger:innen und der Privatwirtschaft im Bereich IT-Sicherheit entstehen, ist das etwas, das nicht in ähnlicher Weise gebrandmarkt wird. Können Sie einmal die Verbindung zwischen IT-Sicherheit und Datenschutz skizzieren?

SV **Prof. Ulrich Kelber** (BfDI): In der Tat erleben wir in manchen Diskussionen in letzter Zeit, dass der IT-Sicherheit und der Cybersicherheit die gleiche Bremserfunktion oder übertriebene Anforderungen bei Lösungen zugeordnet werden. Dem Vertrauen ist auch nicht zuträglich, wenn bei solchen Lösungen diese Anforderungen, die notwendig sind, um dauerhafte Funktionsfähigkeit zu gewährleisten, entsprechend herabgesetzt werden. Aus meiner Sicht bedingen sich Datenschutz und Cybersicherheit gegenseitig, denn nur, wenn beides – der Grundrechtsschutz durch den Datenschutz und die Herstellung von Sicherheit – gewährleistet sind, erfahren die Lösungen, die Produkte, die Anwendungen auch die entsprechende Nutzbarkeit und die dauerhafte Akzeptanz. Die Datenschutzgrundverordnung sieht die Sicherheit von Verfahren vor. Wir unterhalten uns über staatliche Lösungen, aber eben auch über solche zum Beispiel in der kritischen Infrastruktur oder im täglichen Leben. Die Datenschutzgrundverordnung schreibt die Voraussetzung von Cybersicherheit vor, um überhaupt rechtskonform sein zu können. Deswegen hat dies einen hohen Stellenwert in unserer Arbeit. Auch die Zusammenarbeit mit dem BSI oder gegebenenfalls auch mit anderen Einrichtungen der Cybersicherheit macht einen Großteil unserer Arbeit aus.

Abg. **Misbah Khan** (BÜNDNIS 90/DIE GRÜNEN): Die zweite Frage habe ich an Herrn Atug. Sie sprechen in Ihrer Stellungnahme von der Notwendigkeit einer gesamtstaatlichen Sicherheitsstrategie, die zwischen den Ressorts des Bundes und der Länder abgestimmt werden soll. Können Sie ausführen, was aus Ihrer Sicht eine solche Strategie umfassen sollte?

SV **Manuel Atug**: Eine Strategie ist etwas, das man nicht in drei Monaten verwirft. Man braucht eine Vision, die man verfolgen will. Diese muss natürlich auch ganz Deutschland adressieren, wenn wir sie insoweit ausrichten wollen. Aktuell ist die Cybersicherheitsstrategie für Deutschland 2021 vom BMI entwickelt und veröffentlicht worden, zusätzlich zur Cybersicherheitsagenda des BMI selbst. An dieser Strategie war ich unter anderem beteiligt bei zwei von den vier Workshops. Ich habe dort gefragt: Das BMI ist nicht zuständig für Forschung und Wissenschaft, für die Zivilbevölkerung oder für die Länder oder die kommunalen Systeme, wie ist das denn in Einklang zu bringen? Das konnte man nicht so richtig beantworten. Es ist dann anschließend ignoriert worden. Aber eine Strategie muss ganz Deutschland umfassen und damit auch ganz Deutschland adressieren.

Sie braucht KPI (Key Performance Indicators)– Messpunkte, an denen ich adressierbar mache, worum es überhaupt geht. Die erste Version der

Strategie war ein Wunschkonzert von Befugniserweiterungen von Behörden. Anschließend kam erst die Erklärung, wofür man eigentlich was machen will. Wenn man hineinschaut, steht dort: Bildungspolitik oder Bildung in Deutschland, um die Bevölkerung mit mehr Knowhow zu versorgen. Dies wird dadurch gelöst, dass man mehr Forschungsgeld in die Bildung wirft – oder so ähnlich. So funktioniert das nicht. Strategisch muss man so agieren, dass man erstens alle abholt: Kommunen, Landkreise, Länder, Bund und anschließend Europa. Eingangs wurde schon erklärt, dass Datenpakete nicht an Länder- oder an Verantwortungsgrenzen Halt machen und sagen: Oh nein, an dieser oder an jener politischen Grenze darf ich jetzt leider nicht weitergehen. Kriminelle lachen darüber und machen sich einen Spaß daraus. Also muss ich strategisch so vorgehen, dass das Gesamtbild stimmt. Dazu müssen sich 16 Länder, der Bund und 11.500 Kommunen zusammensetzen und sagen: Wie können wir dort einheitlich agieren?

Wenn der eine Hüh und der andere Hott sagt, es einer gerne defensiv hätte und der andere offensiv, dann ist das nicht strategisch. Ich muss mich auch entscheiden, ob ich Sicherheit durch Verschlüsselung haben möchte oder Sicherheit trotz Verschlüsselung. Es geht nur das Eine oder das Andere.

Abg. **Maximilian Funke-Kaiser** (FDP): Herr Atug darf gleich weiterreden, denn ich habe eine Frage an ihn. Wir sind zu der Erkenntnis gekommen, dass Sicherheitslücken konsequent geschlossen werden müssen. Ich möchte ein ganz neues Thema aufmachen, denn gutwillige Hacker können einen wichtigen Beitrag zum Erkennen von Schwachstellen leisten. Diese begeben sich gerade aktuell selbst in Gefahr, aufgrund des § 202c Strafgesetzbuch, wo auf die §§ 202a und 202b Bezug genommen wird. Es herrscht auch immer noch eine öffentliche Debatte und eine gewisse Unsicherheit darüber, ob gutartige Vorbereitungshandlungen für die Nutzung von Software, mit denen man Daten ausspähen und abfangen kann, strafbar sind. Wir haben uns allerdings im Koalitionsvertrag darauf geeinigt, dass das, ich zitiere: "Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren legal durchführbar sein soll". Jetzt die Frage an Sie: Wie könnte so eine sinnvolle gesetzliche Regelung aussehen?

SV **Manuel Atug**: Man könnte beispielsweise der Sicherheitsforscher:innen-Community in Deutschland das Angebot machen: Es gibt eine Meldestelle in Deutschland, zum Beispiel ein unabhängiges BSI, welchem man straffrei all diese Informationen melden kann. Stand heute ist es so, dass mich im Schnitt einmal im Monat Leute ansprechen und sagen: Ich traue mich nicht, das zu melden, aber hier gibt es ein Problem in kritischer Infrastruktur oder generell bei einem großen Unternehmen. Kannst du das irgendwohin eingießen? Und dann muss ich entweder beim BSI oder CERT (Computer Emergency Response Team)-Bund anfragen oder sagen: Bestellt denen einen schönen Gruß vom Honkhasen. Die wissen schon, was sie tun müssen, weil eine Vertrauensbasis und ein Verhältnis existiert und ich das übrigens selber riskiere.

Wenn man ein unabhängiges BSI als Meldestelle für solche Schwachstellen oder für Sicherheitslücken hätte, dann könnte dieses beispielsweise anordnend diese Dinge mit den Herstellern klären. Also im Responsible Disclosure-Verfahren dem Hersteller vorab melden: Das ist das Problem, das wir festgestellt haben, bringe bitte einen Patch heraus, kümmere dich strukturiert darum. Wenn der Patch herauskommt, wird das an die Kunden ausgerollt und diese – das ist der wichtige Punkt, wenn es beispielsweise um kritische Infrastruktur geht – müssen dann auch in irgendeiner Form angeordnet diese Patches installieren, denn wir erleben teilweise auch gepatchte Systeme oder ungepatchte Systeme im Internet, die kritische Infrastruktur oder Fernwartung betreffen. Vorhin wurde die Zwei- oder Mehrfaktor-Authentisierung erwähnt und die Fernwartung, die auf archäologisch wertvollem Niveau ohne so etwas betrieben wird. Da hilft auch ein Patchen nicht.

Abg. **Maximilian Funke-Kaiser** (FDP): Eine Modifizierung des Paragrafen und eine Meldestelle beim BSI. Ich versuche, einen guten Übergang zum Thema BSI zu machen. Das möchte ich heute auch noch thematisieren. Wir haben bei den Debatten zum Thema Chatkontrolle und Recht auf Verschlüsselung gesehen, dass die Unabhängigkeit sehr wichtig ist. Sie haben in Ihrer Stellungnahme gesagt, dass Sie sich dafür einsetzen, dass die Dienstaufsicht des BSI beim

BMI verbleibt, die Fachaufsicht jedoch selbstständig nach Maßgabe wissenschaftlicher Grundlagen erfolgt. Eine grundsätzliche Frage: Was spricht denn Ihrerseits gegen eine völlige Unabhängigkeit der Behörde, wie beispielsweise des BfDI?

SV **Manuel Atug**: Genau gar nichts. Wir hätten das sehr gern, aber das bekommen wir sowieso nicht. Insofern haben wir gesagt: Dann machen wir den Abstrich und versuchen wenigstens die kleine Variante, denn die große, schon seit Jahren diskutierte kommt nicht. Ein unabhängiges BSI wäre genau das, was sich die AG KRITIS und die Zivilbevölkerung wirklich wünscht, weil sie dann sagen könnten: Hier agieren vertrauensvoll Leute miteinander auf Augenhöhe. Ulrich Kelber wird bestätigen können: Wir haben uns immer wieder gemeinsam ausgetauscht, und aufgrund der Unabhängigkeit begrüßen wir das absolut. Insofern wäre das unser ultimativer Wunsch, dass wir ein unabhängiges BSI bekommen.

Abg. **Steffen Janich** (AfD): Meine Frage geht an Herrn Kelber. Anders als die AG KRITIS mit dem hier vertretenen Sachverständigen Herrn Atug, sehen Sie durchaus einen qualitativen Unterschied zwischen Softwareschwachstellen und IT-Schnittstellen für Sicherheitsbehörden. Die Frage: Gibt es aussagekräftige empirische Befunde, dass Schnittstellen für Sicherheitsbehörden von Hackern weniger oft entdeckt und ausgenutzt werden als Softwareschwachstellen?

SV **Prof. Ulrich Kelber** (BfDI): Von einem gesetzlichen Ist-Stand aus – ohne unsere früheren kritischen Stellungnahmen zu wiederholen, aber um auf Ihre Frage einzugehen – eine natürlich durchaus kritische Sicht auf solche Schnittstellen im Allgemeinen: Es gibt natürlich im Bereich zum Beispiel der Ausleitung von Telekommunikationsverkehr auch welche, die allgemein bekannt sind. Aber in der Tat gibt es keine mir bekannten umfangreichen Studien über diesen Unterschied. Umgekehrt sind die Zeitrahmen, in denen so etwas existent ist, sehr unterschiedlich. Während, hoffentlich zumindest, die meisten Schnittstellen in einer bestimmten Zeit soweit bekannt werden, dass dann Gegenmaßnahmen getroffen werden, sind einige zu solchen Systemen auch schon mehr als ein Jahrzehnt alt.

Abg. **Steffen Janich** (AfD): Meine zweite Frage geht an Herrn Atug. Ist es absehbar, dass in Zukunft KI-Anwendungen zur autonomen Behebung von Schwachstellen eingesetzt werden können? Wäre das Ziel der Behebung sämtlicher Schwachstellen irgendwann erreichbar? Falls das mit Ja beantwortet wird: Welche Zeiträume sehen Sie insoweit?

SV **Manuel Atug**: Das beantworten wir ganz klar mit Nein. Aktuell haben wir noch nicht einmal KI, sondern eine schwache KI Machine Learning-Statistik. Selbst wenn es eine starke KI gäbe, irgendwann einmal, die wirklich intelligent wäre und eigenmächtig agieren würde, wären deren Intelligenz und Eigenmächtigkeit ungefähr auf dem Niveau der Menschen – sie agierte manchmal seltsam. Mit KI kann man vielleicht Teile automatisieren, die man auch früher in der Sicherheitsindustrie per Hand gemacht und jetzt automatisiert hat. Damit wird man weitere Automatisierungen von automatisierbaren Teilen hinbekommen, aber eine echte Behebung von allen Lücken ist schlicht unrealistisch.

Eine KI wird auch nie die Allheillösung bringen. Aktuell ist es nur Glitzer und Hype. Es wird auch die nächsten Jahre oder Jahrzehnte absehbar Glitzer und Hype bleiben und keinen Sicherheitsmehrwert bringen. Wenn es das irgendwann bringen sollte, dann werden es die rudimentären Basismaßnahmen sein. Aber dann diskutieren wir wieder auf dem Niveau, dass wir Mindestsicherheitsstandards vom BSI und solche haben, die international anerkannt sind. Sie heißen Mindestsicherheitsstandards, weil jeder nur das Mindeste an Sicherheit tut, was gezwungenermaßen reguliert gemacht wird, und alles andere tut man nicht.

Wenn man dann ein Gesetz herausbringt zum Schutz kritischer Infrastrukturen und der Schwellenwert ist, 500.000 Leute oder mehr zu versorgen und Cybersicherheit zu betreiben, legen sich bis zu 499.999 Leute in der Versorgung gemütlich zurück und sagen: Wird ja nicht gesetzlich erzwungen, dann mache ich genau Nichts. Da hilft auch keine KI.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich möchte meine verbleibende Zeit aufteilen und zunächst Frau Professor Sasse etwas fragen. Sie schreiben in Ihrer Stellungnahme, dass Hersteller,

Dienstleister und Technikanbieter oft nicht hinreichend Angriffsflächen absichern, aber trotzdem eigentlich die Hauptverantwortung dafür tragen müssten, dass Produkte sicher sind – weg von der Schwachstelle Mensch als Hauptfokus. Was müsste man als Regulierer noch machen, um zu diesem Zustand zu gelangen?

SVe **Prof. Dr. Martina Angela Sasse**: Meine Kollegen und ich hören in unserer Forschung, die wir auch mit Entwicklern, mit technischen Experten und mit Geschäftsführenden von Firmen betreiben, dieses Argument: Der Kunde will nicht für ein sicheres Produkt zahlen und deshalb machen wir das nicht. Wir könnten es, aber das wird nichts. Wenn man aber mit den Konsument:innen darüber spricht, dann sagen die: Ich kaufe ein deutsches Qualitätsprodukt, ich erwarte, dass es sicher ist. Man muss einfach den Anreiz dafür schaffen, sichere Produkte herzustellen. Wenn gesagt wird „Warum sollen wir dort investieren?“, dann macht die Konkurrenz das nicht, deren Produkte sind dann billiger und der Kunde kauft sie.

Es wäre einfacher, bestimmte Standards zu setzen, an die sich jeder halten muss. Dann kommt man auch nicht als Unternehmen oder als Entwickler in diesen Zielkonflikt zu sagen: Soll ich jetzt noch ein zusätzliches Widget oder Ähnliches machen? Oder soll ich mich um die Sicherheit kümmern? Im Moment denken sie, ihre Geschäftsführung erwarte, dass sie noch mehr Funktionalität liefern – statt der Sicherheit. Dort kann der Gesetzgeber den richtigen Standard schaffen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Kurz nachgefragt: Spielt dort auch eine IT-Produkthaftpflicht eine Rolle?

SVe **Prof. Dr. Martina Angela Sasse**: Natürlich, das ist auch ein massiver ökonomischer Anreiz, das Richtige zu tun.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich möchte in meiner verbleibende Zeit Manuel Atug aka Honkhase Fragen stellen. Wir erinnern uns alle noch ganz lebendig an Edward Snowden und daran, was er ans Tageslicht gebracht hat: Dass IT-Sicherheit durch befreundete und verfeindete Geheimdienste gefährdet wird. Was hat sich seitdem geändert? Hat sich an der Gefährdungslage irgendetwas verändert? Hat sich dort die Lage verbessert? Hat sich vor allem in der Folge die IT-Sicherheit von Unternehmen, Bevölkerung und Verwaltungen irgendwie geändert?

SV **Manuel Atug**: Die hat sich massiv geändert. Sie hat sich nämlich extrem verschlechtert. Als Edward Snowden alles öffentlich gemacht hat, hat die Zivilgesellschaft sich das angeschaut, war schockiert und hat gesagt: Wir waren ja schon teilweise paranoid, aber das, was die da treiben, geht bis zum Exzess – mit Ringtausch, alle hingen unter einer Decke. Jeder Mensch ist Freiwild. Datenschutz ist nur eine Theorie, die man durch Nachrichtendienste und Geheimdienste ad absurdum geführt hat. Wir waren alle geschockt und sagten: Okay, jetzt geht es endlich in die richtige Richtung, es wird aufgeräumt. Dann kamen alle alten weißen Männer aus der Rüstungsindustrie, von zwielichtigen Sicherheitsproduktanbietern und von Regierungen und haben gesagt: Was, das können die alles? Das wollen wir auch. Dann ist eine Phase der Beschleunigung gestartet und alle Geheim- und Nachrichtendienste haben angefangen, Sicherheitslücken zu sammeln und zu horten. Jeder muss sich irgendwie gegen alles andere verteidigen, durch offensive Maßnahmen. Dann kam Defensive Forward, Hackback und all dieses unsägliche Zeug ins Gespräch, bei dem man meint, mit offensiven Maßnahmen agieren zu können, und alles wird irgendwie besser. Ich sage noch einmal: Die Büchse der Pandora liegt bei diesen Geheim- und Nachrichtendiensten. Selbst die Kriminellen sind nicht so krass drauf, wie das, was dort teilweise getrieben wird. Die können diese Sicherheitslücken genauso wenig hundertprozentig sichern und zurückhalten. Als wäre das nicht genug, reden wir aktuell nur über Sicherheitslücken. Aber inzwischen gibt es Firmen wie NSO, die das einfach als Service permanent bereitstellen. Das heißt, man muss eigentlich auch keine Sicherheitslücken mehr kennen. Man kann von zwielichtigen Anbietern dauerhafte Services kaufen. Es ist also insgesamt gruselig geworden und wird es in Zukunft noch mehr.

Die **Vorsitzende**: Vielen Dank! Wir sind am Ende dieser öffentlichen Anhörung. Sie haben uns wertvolle Hinweise gegeben und einige Problemfelder aufgezeigt. Ganz herzlichen Dank an die Sachverständigen, die uns ihr Knowhow

zur Verfügung gestellt und uns beraten haben. Ich danke auch den Vertreter:innen der Institutionen BSI und BfDI und natürlich den Regierungsvertretern für die Teilnahme. Allen Zuhörer:innen sowohl hier im Saal als auch an den Endgeräten: Vielen Dank für das gezeigte Interesse. Nicht zuletzt möchte ich den Mitarbeiter:innen der Technik ganz herzlich danken, dass es heute so reibungslos abgelaufen ist. Ich möchte auch dem Ausschusssekretariat für die Organisation und die Unterstützung ganz herzlich danken. Wir machen gleich weiter mit der Sitzung des Ausschusses, das ist dann eine nichtöffentliche Sitzung. Deshalb müssen wir auch die Webex-Konferenz wechseln und werden eine kurze Pause machen, um den technischen Wechsel zu ermöglichen. Ich wünsche allen einen guten Tag und schließe hiermit die Sitzung. Vielen Dank.

Schluss der Sitzung: 16:00 Uhr

Tabea Rößner, MdB
Vorsitzende

Anlagenkonvolut
zum Wortprotokoll der 27. Sitzung am 25. Januar 2023

Öffentliche Anhörung „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Stellungnahmen der eingeladenen Sachverständigen:

Ammar Alkassar
Ehemaliger Bevollmächtigter für Innovation und Strategie und CIO des Saarlandes
A-Drs. 20(23)127

Manuel Atug
Gründer und Sprecher, AG KRITIS
A-Drs. 20(23)118

Dr. Annegret Bendiek
Lehrstuhlvertretung an der Universität Osnabrück "Europäische Studien",
Stellvertretende Forschungsgruppenleiterin EU/Europa,
SWP Projektleitung "European Repository on Cyber Incidents"
A-Drs. 20(23)122

Dr. Stefanie Frey
Geschäftsführerin Deutor Cyber Security Solutions GmbH
A-Drs. 20(23)120

Dr. Sven Herpig
Leiter für Internationale Cybersicherheitspolitik,
Stiftung Neue Verantwortung e. V.
A-Drs. 20(23)117

Prof. Dr. Dennis-Kenji Kipker
Professor für IT-Sicherheitsrecht, Hochschule Bremen,
Fakultät für Elektrotechnik und Informatik
A-Drs. 20(23)116

Prof. Dr. Martina Angela Sasse
Professorin und Lehrstuhlleitung Menschzentrierte IT Sicherheit, Ruhr-Universität Bochum, Fakultät Informatik
A-Drs. 20(23)121

Julia Schuetze
Projektleiterin Internationale Cybersicherheitspolitik,
Stiftung Neue Verantwortung e.V.
A-Drs. 20(23)119

Weitere Stellungnahmen:

Prof. Ulrich Kelber
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)
A-Drs. 20(23)123

Dr. Gerhard Schabhüser
Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)
A-Drs. 20(23)125