19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 48. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 8. April 2019, 14:00 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt **Seite 15**

a) Antrag der Abgeordneten Manuel Höferlin, Jimmy Schulz, Stephan Thomae, weiterer Abgeordneter und der Fraktion der FDP

Digitalisierung ernst nehmen – IT-Sicherheit stärken

BT-Drucksache 19/7698

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Jochen Haug [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

b) Antrag der Abgeordneten Anke Domscheit-Berg, Dr. Petra Sitte, Dr. Alexander S. Neu, weiterer Abgeordneter und der Fraktion, DIE LINKE.

Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors

BT-Drucksache 19/7705

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Jochen Haug [AfD]

Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

c) Antrag der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

BT-Drucksache 19/1328

Federführend:
Innenausschuss

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss für Wirtschaft und Energie
Verteidigungsausschuss
Ausschuss für Verkehr und digitale Infrastruktur
Ausschuss für Menschenrechte und humanitäre Hilfe
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Christoph Bernstiel [CDU/CSU]
Abg. Sebastian Hartmann [SPD]
Abg. Martin Hess [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

19. Wahlperiode

Deutscher Bundestag

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		CDU/CSU	
Amthor, Philipp		Berghegger Dr., André	
Bernstiel, Christoph		Frei, Thorsten	
Brand (Fulda), Michael		Gnodtke, Eckhard	
Henrichmann, Marc		Gröhler, Klaus-Dieter	
Irmer, Hans-Jürgen		Hauer, Matthias	
Kuffer, Michael		Heil, Mechthild	
Lindholz, Andrea		Heveling, Ansgar	
Middelberg Dr., Mathias		Hoffmann, Alexander	
Müller, Axel		Launert Dr., Silke	
Nicolaisen, Petra		Luczak Dr., Jan-Marco	
Oster, Josef		Pantel, Sylvia	S. Pantel
Schuster (Weil am Rhein), Armin		Schimke, Jana	
Seif, Detlef		Sensburg Dr., Patrick	
Throm, Alexander		Ullrich Dr., Volker	
Vries, Christoph de		Veith, Oswin	
Wendt, Marian		Wellenreuther, Ingo	

2. April 2019 — **Anwesenheitsliste** — Seite 1 von 5
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Castellucci Dr., Lars		Fechner Dr., Johannes	
Esken, Saskia		Gerster, Martin	
Grötsch, Uli		Högl Dr., Eva	
Hartmann, Sebastian		Juratovic, Josip	
Heinrich, Gabriela		Kolbe, Daniela	
Kaiser, Elisabeth		Lühmann, Kirsten	
Lindh, Helge		Poschmann, Sabine	
Lischka, Burkhard		Rix, Sönke	
Mittag, Susanne		Rüthrich, Susann	
Özdemir (Duisburg), Mahmut		Vöpel, Dirk	

2. April 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Seite 2 von 5

öff.

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
AfD		**AfD**	
Baumann Dr., Bernd		Elsner von Gronow, Berengar	
Curio Dr., Gottfried		Harder-Kühnel, Mariana Iris	
Haug, Jochen		Hilse, Karsten	
Herrmann, Lars		Maier, Jens	
Hess, Martin		Reusch, Roman Johannes	
Wirth Dr., Christian		Storch, Beatrix von	
FDP		**FDP**	
Höferlin, Manuel		Beeck, Jens	
Kuhle, Konstantin		Ruppert Dr., Stefan	
Schulz, Jimmy		Strack-Zimmermann Dr., Marie-Agnes	
Strasser, Benjamin		Thomae, Stephan	
Teuteberg, Linda		Toncar Dr., Florian	

2. April 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Seite 3 von 5

öff.

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
DIE LINKE.		**DIE LINKE.**	
Hahn Dr., André		Akbulut, Gökay	
Jelpke, Ulla		Dağdelen, Sevim	
Pau, Petra	Petra Pau	Movassat, Niema	
Renner, Martina		Nastic, Zaklin	
		A. Domscheit-Berg	Domscheit-Berg
BÜ90/GR		**BÜ90/GR**	
Amtsberg, Luise		Bayram, Canan	
Mihalic Dr., Irene		Brugger, Agnieszka	
Notz Dr., Konstantin von		Haßelmann, Britta	
Polat, Filiz		Lazar, Monika	

2. April 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Seite 4 von 5

19. Wahlperiode

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Beratende Mitglieder (§57 Abs. 2 GOBT) des Ausschusses	Unterschrift
Fraktionslos	
Petry Dr., Frauke	

öff.

Tagungsbüro

Deutscher Bundestag

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
AFD		
FDP		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Buczyk, Dirk	LINKE	
Wirrok, Teresa	FDP	
Pohl, Jörn	Grüne	
Spary Jeannette	SPD	
Dreyer, Markus	Grüne	
Alexander Bjick	FDP	
Jane Roth	Linke	
Quars Carlo	AFD	

Stand: 13. September 2016 / ZT4, Luisenstr. 32-34, Telefon: +49 30 227-32659
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

öff.

Tagungsbüro | **Sitzung des Ausschusses für Inneres** und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr | Seite 2

Fraktionsmitarbeiter

Name (bitte in Druckschrift)	**Fraktion**	**Unterschrift**
SCHÄFER	LINKE	
FISCHER	GRÜNE	
Gropalla	"	
SINNOKROT	SPD	
KRZEMIEN	SPD	

öff

Tagungsbüro

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Bundesrat

Land	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amtsbezeichnung**
Baden-Württemberg			
Bayern	D. Wurmdobler	Wurmdobler	MR
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern			
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz			
Saarland			
Sachsen	Kühne-Hörstel	Kühne-Hörstel	StS'in
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen			

öff.

Tagungsbüro

Sitzung des Ausschusses für Inneres und Heimat (4. Ausschuss)
Montag, 8. April 2019, 14:00 Uhr

Seite 4

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	Unterschrift	**Amtsbezeichnung**
Sekretariat	Elsner, Stephan		PD
f. Innere & Sport BTGI	Köna, Andreas		RegDir

Stand: 2. April 2019

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 8. April 2019, 14.00 bis 16.00 Uhr
„IT-Sicherheit“

Stand: 2. April 2019

Dr. Rainer Baumgart
secunet Security Networks AG, Essen

Dr. Sven Herpig
Stiftung Neue Verantwortung

Klaus Landefeld
eco – Verband der Internetwirtschaft e. V., Berlin

Frank Rieger
CCC Berlin e. V.

Präsident Arne Schönbohm
Bundesamtes für Sicherheit in der Informationstechnik, Bonn

Dr. Aleksandra Sowa
Bonn

N.N.

Sprechregister der Sachverständigen und Abgeordneten

Tagesordnungspunkt

a) Antrag der Abgeordneten Manuel Höferlin, Jimmy Schulz, Stephan Thomae, weiterer Abgeordneter und der Fraktion der FDP

Digitalisierung ernst nehmen – IT-Sicherheit stärken

BT-Drucksache 19/7698

b) Antrag der Abgeordneten Anke Domscheit-Berg, Dr. Petra Sitte, Dr. Alexander S. Neu, weiterer Abgeordneter und der Fraktion, DIE LINKE.

Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors

BT-Drucksache 19/7705

c) Antrag der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

BT-Drucksache 19/1328

Vors. **Andrea Lindholz** (CDU/CSU): Ich darf Sie ganz herzlich alle zu unserer heutigen öffentlichen Anhörung des Innenausschusses begrüßen. Ganz besonders begrüßen darf ich zunächst auch die Damen und Herren Sachverständigen. Wir bedanken uns zum einen sehr für Ihr Kommen, dass Sie den Kolleginnen und Kollegen auch für Fragen und für die Beratung zur Verfügung stehen und zum anderen auch für die bereits teilweise eingegangenen Berichte. Wir haben heute eine Anhörung zum Thema Fragen der IT-Sicherheit. Drei Anträge liegen der Anhörung heute zugrunde und wir werden das vom Ablauf her so machen, dass wir zunächst einmal Sie, liebe Damen und Herren Sachverständige bitten, ein kurzes fünfminütiges Eingangsstatement zu halten. Dann werden wir anschließend in die Fragerunde der Fraktionen eintreten. Wie viele Fragerunden wir schaffen werden, hängt ein bisschen von der zügigen Frage und Antwort ab.

Abg. **Manuel Höferlin** (FDP): Wie fragen wir denn heute, Frau Vorsitzende?

Vors. **Andrea Lindholz** (CDU/CSU): Bei den Fragen Herr Höferlin machen wir das so, wie wir das jetzt zum Schluss immer gemacht haben. In der ersten Fragerunde ist es möglich zwei Fragen an einen Sachverständigen zu stellen, eine Frage an zwei Sachverständige oder zwei unterschiedliche Fragen, davon aber jeweils nur eine an einen anderen Sachverständigen. Wenn das zügig funktioniert, kann man so auch in der zweiten Runde verfahren. Wenn nicht, dann werden wir das Verfahren für die zweite Runde ändern. Dann beginnen wir in der Reihenfolge des Alphabetes mit Herrn Dr. Baumgart.

SV **Dr. Rainer Baumgart** (secunet Security Networks AG, Essen): Vielen Dank. Meine sehr verehrten Damen und Herren. Ich versuche ein Statement etwas mehr aus der Perspektive der Wirtschaft zu geben beziehungsweise aus dem Bereich der sicherheitstechnischen nationalen Industrie. Meine sehr verehrten Damen und Herren, aus Sicht der Wirtschaft bedeutet zunehmende Digitalisierung auch zunehmender Sicherheitsbedarf. Der Bedarf an Sicherheit wächst in den letzten Jahren kontinuierlich. Darüber hinaus aber eröffnet das auch für Anbieter von Sicherheitslösungen einen Markt, eine Marktentwicklung, die hier als Wachstumsmarkt zu bezeichnen ist. Deutschland verfügt über eine leistungsfähige IT-Sicherheits- oder Cybersicherheitsindustrie, die aber vornehmlich mittelständisch beziehungsweise auch durch viele Kleinunternehmen geprägt ist. Diese Unternehmen und diese Technologien, die meistens auch in Zusammenarbeit mit behördlichen Anforderungen, mit dem BSI oder verschiedenen anderen Stellen entwickelt worden sind, genießen international eine sehr hohe Reputation. Allerdings hängt unsere digitale Souveränität zunehmend von den Fähigkeiten dieses Bereiches und der Durchsetzung der hier entwickelten Sicherheitsmechanismen und Verfahren ab und das wird zukünftig noch zunehmen. Denn Deutschland ist nahezu ein Referenzmarkt für Cybersicherheit, was insbesondere durch die Regulierung in diesem Umfeld, wie IT-Sicherheitsgesetze, BSI-Gesetz, BSI-Zertifizierungen etc. begründet ist. Allerdings, meine sehr verehrten Damen und Herren, sind nationale Anbieter nicht völlig losgelöst von den internationalen technologischen Entwicklungen. So müssen die Sicherheitsverfahren im Zusammenhang mit nicht vertrauenswürdigen Komponenten umgesetzt werden. Daher müssen zukünftig die Sicherheitsmaßnahmen unabhängig und separat und von nicht vertrauenswürdigen Plattformen ausgehend durchgesetzt werden.

Hierzu gehören unter anderem Deutschland hat keine Prozessorarchitekturen, hat keine großen im großen Stil verwendeten Betriebssysteme oder Entwicklungswerkzeuge. Ein Thema, was hier insbesondere vom BSI seit Jahren verfolgt wird, ist das Thema Separation. Das heißt also, unabhängige Implementierung von Sicherheitstechnik von diesen Systemen ausgehend. Man muss natürlich fordern, dass die Forschungsförderungen in diesem Umfeld dieser Aspekte zur Entwicklungsunterstützung zukünftig – auch im Hinblick auf Produktisierung – stärker durchsetzen und berücksichtigen und hier auch das BSI mit – wie die Industrie – stärker einbinden. Die organisatorischen Rahmenbedingungen zum sicheren Betrieb der Systeme sind natürlich ein weiterer Punkt. Hier kann man sehen, dass organisatorische Sicherheit wie Grundschutzmaßnahmen in der Vergangenheit erfolgreich waren, aber auch noch verstärkt werden können und müssen und vor allen Dingen nachprüfbar werden. Insgesamt sind ausreichende Fachkräfte der bedrohliche Flaschenhals. Meine Damen und Herren, jedoch ist das Thema IT-Sicherheit hochspannend für junge Leute. Daher müssen Aus- und Weiterbildungen in diesem Umfeld verfügbar werden und verstärkt bleiben. Insgesamt muss man sagen, der EU-Binnenmarkt hat bei der Beschaffung im öffentlichen Bereich beziehungsweise für kritische Infrastrukturen bislang keine einheitlichen Mindeststandards. Dabei gibt es zunehmend Konzentrationen in der Wirtschaft durch Übernahmen. Man muss sehen, dass auch hier europäische Staatskonzerne unserer Nachbarländer an diesen Prozessen stark beteiligt sind, die gerade in der letzten Zeit zu erheblichen Verwerfungen geführt haben. Die Exportfähigkeit unserer nationalen Sicherheitsprodukte sollte ebenfalls betrachtet und eventuell verbessert werden, denn die Wirtschaftlichkeit der nationalen Investitionen wird hier durch die Entwicklung und Forschung stärker berücksichtigt, sodass wir mehr Angebote und Wirtschaftlichkeit auch durch eine Exportverstärkung erreichen können. Die Hersteller von Sicherheitslösungen, die die Vertrauenswürdigkeit in ihrem Angebot mit auszeichnen, insbesondere indem sie diese durch Zertifizierungen nachweisen und deshalb sicherheitskritische Funktionalitäten anbieten, sind immer noch benachteiligt, weil Wirtschaft und Verwaltung gerne Funktionalität und risikobehaftete Implementierungen auch attraktiv finden. Jedoch sollten Zertifizierungen als Vertrauens- und Qualitätsnachweis zum Erfolgsfaktor und auch für den wirtschaftlichen Erfolg von Sicherheitsprodukten werden. Daher muss das BSI auch personell in die Lage versetzt werden, dass diese Zertifizierungen zügig durchgeführt werden und die Produkte zeitgerecht in den Markt kommen.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Dr. Baumgart, ich darf nur auf die Zeit hinweisen.

SV **Dr. Rainer Baumgart** (secunet Security Networks AG, Essen): Entschuldigung. Ich bin sofort fertig. Ich fasse nochmal zusammen, dass wir neben Open Source – das ist ein Thema, über das man zusätzlich hier länger sprechen könnte – Deutschland über hervorragende Sicherheitstechnologien verfügt, die auch eine Überwachung von Infrastrukturen im behördlichen Umfeld, wie im Industrieumfeld ermöglichen und Schwachstellen oder Angriffe aufdecken können. Dabei kann auch der Datenschutz gewährleistet werden. Allerdings ist diese Sicherheitstechnik nicht wie der Sicherheitsgurt im Fahrzeug vorgeschrieben und wird nicht flächendeckend eingesetzt. Man könnte mit dieser Unterstützung kritische Infrastrukturen auch im Hinblick auf Meldepflichten massiv oder die Anbieter unterstützen. Bis hierhin vielleicht. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Dr. Herpig, bitte.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Bundestagsabgeordnete. Da IT-Sicherheit als Titel dieser Ausschusssitzung eher eine Metaebene beschreibt und die Anträge ein ganzes Potpourri an IT-Sicherheitsmaßnahmen beinhalten, möchte ich nicht auf einzelne Aspekte eingehen oder dediziert zu den aktuellen Referentenentwürfen zur Harmonisierung des Verfassungsschutzgesetzes oder des IT-Sicherheitsgesetzes 2.0 Stellung nehmen, sondern versuche auch etwas auf dieser Makroebene zu antworten. Details und Verweise, weitere Analysen finden Sie in meiner schriftlichen Stellungnahme. Ich möchte auf drei Herausforderungen näher eingehen.

Erstens: Deutschland ist bei IT-Sicherheitsstrategie unfähig. Uns fehlt ein strategischer Rahmen für die Beantwortung von gegen uns gerichteten Cyberoperationen.

Der Übergang der IT-Sicherheitstrinität, Prävention, Detektion, Reaktion hinzu Repression ist unterentwickelt. Das beinhaltet sowohl ein verbindliches Attributionsverständnis, als auch eine Verknüpfung mit aktiven Cyberabwehrmaßnahmen und repressiven Maßnahmen außerhalb des digitalen Spektrums, wie z. B. Strafverfolgung, wirtschaftliche Sanktionen oder nachrichtendienstliche Operationen. Auch dort, wo wir für IT-Sicherheit dringend eine Strategie bräuchten, bei der Resilienz und hier vor allem beim Umgang mit Schwachstellen, haben wir keinen umfassenden Plan. Ein wenig Verbraucherschutz für bekannte Schwachstellen hier. Ein wenig Schwachstellenmanagement für unbekannte Schwachstellen dort. Alles gute Ansätze, ohne Frage, aber ohne eine Strategie, die sie zusammenführt, die Synergien nutzbar macht, fehlende Prozesse und Mechanismen identifiziert, ist es vermutlich weder effizient noch sonderlich effektiv. Wir bauen immer weitere Institutionen im Bereich IT-Sicherheit und öffentliche Sicherheit auf. Aktuell mit der zentralen Stelle für Informationstechnologien im Sicherheitsbereich ZITiS oder der Agentur für Innovation in der Cybersicherheit ADIC. An einer Strategie, wie wir mit dem IT-Sicherheitsfachkräftemangel in der Verwaltung umgehen sollen, ohne dass sich diese Institutionen zukünftig gegenseitig kannibalisieren, fehlt es uns aber. Auch die Blaupause für Deutschland-Cybersicherheitsarchitektur ist nicht vorhanden. Normalerweise aber eine elementare Voraussetzung für die Gründung weiterer Behörden. Die drei Institutionen, die die zentralen Elemente in unserer Cybersicherheitarchitektur darstellen, sind der nationale Cybersicherheitsrat, das Bundesamt für Sicherheit in der Informationstechnik und das nationale Cyberabwehrzentrum. Dazu habe aber ich drei Fragen. Die erste ist: Was macht eigentlich der Cybersicherheitsrat, dessen genuiner Auftrag es sein sollte, diese aufgezeigte Strategieunfähigkeit zu vermeiden. Zweitens: Warum ist das Bundesamt für Sicherheit in der Informationstechnik bis heute nicht fachlich unabhängig vom Bundesministerium des Innern, für Bau und Heimat? Und drittens: Warum schaffen wir es seit Jahren nicht, das Cyberabwehrzentrum zu reformieren? Der Reformbedarf ist vielen Beteiligten klar. Bessere Einbindung der Länder, Kommunikationspflichten der Behörden und mehr Transparenz, um nur einige der Aspekte zu nennen.

Zweitens: Das Fehlen handlungsleitender empirischer Evidenz und Teilhabe. Wir haben die Cybersicherheitsstrategien 2011 und 2016, deren Erfolg und Umsetzung wir aber nicht evaluieren. Die aktuelle Cybersicherheitsstrategie ist eine reine Wunschliste von Maßnahmen verschiedener Behörden, ohne dass ihr strategisches Verständnis oder eine Bedarfsanalyse der IT-Sicherheit in Deutschland zugrunde liegen. Es gibt auch keine Gesamtschau der Überwachungsmaßnahmen. Das heißt, die Kenntnis darüber, welche Behörden in Deutschland welche Informationen durch welche Maßnahmen erheben können und wo überhaupt noch „weiße Flecken“ bestehen. Trotzdem werden Überwachungsmaßnahmen weiter ausgebaut und nicht, wie im Koalitionsvertrag festgehalten, im gleichen Maße Schutzmechanismen und Kontrollmaßnahmen etabliert. Was wir schon seit längerem sehen, ist ein besser Haben als Brauchen der Aufgaben und Befugnissen von Sicherheitsbehörden vor allem bei Maßnahmen, die sehr invasiv in die Integrität und Vertraulichkeit informationstechnischer Systeme eingreifen. Es gibt Hausabstimmungen, Ressortabstimmungen, Verbändeanhörungen zu neuen Gesetzen, aber wo bleiben die Zivilgesellschaft und die Wissenschaft. Unsere Beteiligung hängt aktuell massiv davon ab, dass jemand Entwürfe im Internet veröffentlicht. Nimmt man dazu, dass Vertreterinnen dieser Sektoren auf Basis ihrer geringen Ressourcen mehr als nur ein paar Tage brauchen, um einen dutzenden Seiten umfassenden Gesetzestext zu analysieren und aufzubereiten, nimmt man diesen Bereichen effektiv die Möglichkeit einer Teilhabe. In diesen Organisationen sitzen Expertinnen, die zu guter Politik sehr viel beitragen und so einer geistigen Monokultur entgegenwirken können. Einige dieser Personen sitzen heute zum Glück neben mir. Diese Expertise zu ignorieren, wäre nicht nur ineffizient, sondern auch arrogant.

Drittens und letztens: Digitales Räuberschach statt Stärkung der IT-Sicherheit. Mit Begründung und zivilen Ausrichtung des Bundesamtes für Sicherheit in der Informationstechnik, der Cybersicherheitsstrategie 2011, dem IT-Sicherheitsgesetz 1.0 2015, der Verschlüsselungspolitik und vieler anderer Maßnahmen haben in Deutschland meines Erachtens einiges richtig gemacht, um die IT-Sicherheit zu stärken. Leider hat es zuletzt eine Verschiebung vom Primat des Zivilen und der IT-Sicherheit hin zur vermeintlichen Stärkung öffent-

licher Sicherheit durch Überwachung und den Einsatz von Hackingwerkzeugen sowie eine Militarisierung des Diskurses gegeben. Wie Sie in anderen Ländern, wie z. B. den Vereinigten Staaten sehen können, führt das nur dazu, dass sich die IT-Sicherheitsvorfälle häufen. Die letzte verbleibende Option ist dann oft, dem Gegenüber mehr Schaden zuzufügen als man selbst erlitten hat. Normalerweise sollte das aber die Ultima Ratio einer guten Sicherheitsstrategie sein und nicht ihr Fokus. Es ist klar, dass effektive Strategien sektor- und ressortübergreifend sein müssen. Leider wurde in den letzten Jahren viel zu oft unter dem Deckmantel der IT-Sicherheit wahlweise die Agenda der öffentlichen Sicherheit oder der militärisch-nachrichtendienstlichen Bedürfnisse vorangetrieben. Das ist nicht nur ethisch höchst problematisch, sondern vor allem kontraproduktiv für die IT-Sicherheit und damit auch die nationale Sicherheit Deutschlands. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Herr Landefeld, bitte.

SV **Klaus Landefeld** (eco – Verband der Internetwirtschaft e. V., Berlin): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren, liebe Abgeordnete. Wir sind heute bei der Anhörung IT-Sicherheit und die Beschlussanträge, die hier Grundlage sind, die beschäftigen sich alle mit dem Umgang des Staates mit vernetzten Geräten. Das ist ganz dringend und wichtig, da wir irgendwann im Laufe dieses Jahres ungefähr eine Milliarde vernetzter Geräte in Deutschland haben werden und diese Schwelle ist natürlich elementar, weil auch die Frage, was passiert damit, wenn das jetzt weitergeht, selbst wenn wir neue Gesetze haben. Was passiert mit Geräten, die jetzt schon im Markt sind. Wie gehen wir damit um? Das ist natürlich alles eine Kernfrage. Also je schneller wir da zu Lösungen kommen, umso besser ist das. Natürlich ist in der digitalisierten vernetzten Gesellschaft IT- und Cybersicherheit elementar für Zusammenleben und Ordnung im digitalen Raum. Es ist unzweifelhaft Aufgabe des Staates, die IT-Sicherheit der Bürger, Unternehmen und zuletzt natürlich auch für sich selbst zu organisieren und geeigneter Weise auszugestalten. Die Forderungen in den gegenständlichen Anträgen sind alle nachvollziehbar und greifen Defizite und Widersprüche in der bisherigen Sicherheitsstrategie des Bundes auf, die wir insbesondere in der mangelhaften Gewichtung der einzelnen Teilaspekte sehen. Der Bund hat 2011 und zuletzt 2016 die Cybersicherheitsstrategie vorgelegt, entwickelt und in 2015 haben wir ein IT-Sicherheitsgesetz bekommen, das in 2017 dann nochmal für kritische Infrastrukturen ergänzt wurde. Wir hatten erwartet, dass jetzt mit einer IT-Sicherheitsgesetz 2.0-Novelle, die irgendwo aus den NIS-Richtlinien kommt, das systematisch weitergeführt wird und nicht lauter neue Themen diskutiert werden, die bis jetzt gar nicht vorgesehen waren. Was aber komplett fehlt, ist eine Analyse darüber, wie effektiv das alles war. Wo sind eigentlich die Ergebnisse davon? Welche Teile der Sicherheitsstrategie waren sinnvoll? Welche Teile waren nicht sinnvoll? Und hat ein IT-Sicherheitsgesetz, das einige Betreiber, insbesondere alle IT- und TK-Unternehmen auch irgendwo schon betroffen hatte, hat das was gebracht? Das wissen wir bis jetzt nicht. Wir haben ein paar Statistiken gesehen, die mal vorgelegt wurden. Die waren aber neu vom ersten Jahr und natürlich ist: Eine neue Reportingpflicht macht erstmal neue Zahlen. Aber ist es schlimmer geworden? Ist es besser geworden? Hat sich irgendwas verändert? Darüber haben wir bis jetzt keinerlei Aussagen. Was wir haben, und das haben wir in den letzten zwei, drei Jahren insbesondere gesehen, sind verzerrende Presseberichte einzelner Vorfälle, deren Relevanz nicht unbedingt den Einzelfällen entsprechen. Meistens ist es der Prominenz der Opfer geschuldet, dass sie in der Presse hochstilisiert wurden - auch wenn die IT- und Systemsicherheit der eigentlichen Betreiber zu keinem Zeitpunkt gefährdet war. Naturgemäß kommt die Internetwirtschaft im Rahmen der Überlegungen dann immer wieder als Betroffene auf. Wir stellen natürlich die Infrastrukturen und Dienste bereit, die die digitale Welt ausmachen und damit die Treiber der Digitalisierung. Das ist völlig klar. Wir sind zwar auch Ausgangspunkt, können aber auch Angriffsziele und Opfer der Angriffe werden. Wir haben dabei natürlich eine Schlüsselrolle für die Gestaltung der IT-Sicherheit in Deutschland. Interessanterweise sind wir in Diskussionen über die zukünftige Umsetzung kaum einbezogen. Die meisten Gesetzesvorschläge werden von den Ministerien gemacht, ohne mit den Betreibern zu sprechen oder zumindest nicht im ausreichenden Maße zu sprechen. Jetzt gerade mit dem IT-Sicherheitsgesetz 2.0, das zumindest mal im Entwurf vorliegt, waren wir sehr überrascht, was da alles drinsteht und

man wurde dort überhaupt nicht einbezogen.

Was wir eigentlich als Kernproblem vieler Diskussionen sehen, ist die mangelnde Konsequenz hinsichtlich der Frage, ob die Sicherheit von IT-Systemen kompromisslos erhöht werden muss. Oder ob die Sicherheit der Systeme für alle zugunsten eines staatlichen Zugriffs auf IT-Systeme – was natürlich auch immer Zugriff für Dritte heißt, für andere Staaten, für Hacker, für organisierte Kriminalität und ähnliches – ob es eigentlich deswegen gefährdet werden darf. Fragen wie Hackbacks oder ähnliches, sind eigentlich rein akademisch, wenn man eine konsequente Erhöhung von IT-Sicherheit als oberstes Ziel sieht. Das ist das, was wir eigentlich bräuchten. Diese Diskussion, die spielt sich auch in der Frage über die Rolle des BSI wieder. Einen Interessenkonflikt als Hacker einerseits und das Ministerium beziehungsweise die Behörde, die mit der konsequenten Schließung von Sicherheitslücken andererseits betraut sein soll, da dachten wir schon, dass sie sich schon aufgelöst hätte, kommt jetzt aber wieder. Ist auf einmal durch die neuen Entwürfe wieder da. So ähnlich ist auch die Problematik mit der Arbeit des nationalen Cyberabwehrzentrums. Wenn man eine Koordinierungsstelle für die IT-Abwehr sein soll und gleichzeitig aber mit dem Verfassungsschutz und weiteren Geheimdiensten zusammenarbeitet, die jetzt neue Rechte bekommen sollen, selber IT-Sicherheit wieder zu gefährden, muss man sich natürlich fragen, wie arbeitet man in der Verbesserung der IT-Sicherheit und kann ein Abwehrzentrum eigentlich arbeiten, ohne wieder die Arbeit der Dienste zu gefährden oder einzuschränken. Das ist natürlich äußerst problematisch. Man muss auch sehen, dass viele dieser gefühlten von der Presse …

Vors. **Andrea Lindholz** (CDU/CSU): Ich müsste auch an die Zeit erinnern.

SV **Klaus Landefeld** (eco – Verband der Internetwirtschaft e. V., Berlin): Ich bin gleich durch. Wir beobachten große Fälle in Teilen durch das, was wir jetzt als neuen Rahmen der Datenschutzgrundverordnung letztes Jahr bekommen haben, die auch die sichere Verarbeitung von Daten schon vorsieht, gar nicht mehr vorkommen dürfte. Die meisten Pressevorfälle sind Daten, die eigentlich etwas mit Abspeicherung von Daten, mit Hacks oder Auslösen von Passwörtern oder ähnlichem aus Unternehmen zu tun hat.

Klar ist, dass wir im Moment sehr unspezifische Anforderungen an die Betreiber von Diensten und Netzen bekommen, was eigentlich staatlich ordinäre Aufgaben sind. Diese Diskussion, die, denken wir, müsste dringend geführt werden. Was ist eigentlich noch staatlich? Was müssen die Unternehmen machen? Es kann nicht alles auf die Unternehmen verlagert werden. Das ist die Tendenz, die wir momentan sehen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kämen wir zu Herrn Rieger.

SV **Frank Rieger** (CCC Berlin e. V.): Guten Tag. Vielen Dank für die Einladung. Wenn wir uns den Zustand der IT-Sicherheit momentan angucken, müssten wir eigentlich ehrlicherweise die weiße Fahne hissen. Wir müssten sagen, wir haben eine Menge an Software, die angreifbar ist, die problembehaftet ist, die schneller wächst als wir hinterher patchen können, als wir Probleme beheben können. Und darum denken wir, dass die gesetzliche Ausrichtung der IT-Sicherheit und der Aufbau der entsprechenden Systeme rein defensiv sein sollte. Wir haben momentan dieses Problem, dass wir auf der einen Seite Begehrlichkeiten der Sicherheitsbehörden und der Dienste haben, die zur Erfüllung ihrer Aufgaben gerne in IT-Systeme eindringen wollen, die aber damit den Staat in einen inneren Konflikt bringen. Wir haben den Staat mit seiner Verpflichtung zur Daseinsvorsorge, durch die er verpflichtet sein sollte, alle Hintertüren, alle IT-Sicherheitsprobleme, die ihm zur Kenntnis gelangen, schnellstmöglich zu schließen und zum Glück haben wir mit dem BSI auch eine Institution, die dafür bisher sehr gut aufgestellt ist. In dem Augenblick aber, wo wir anfangen solche Institutionen und das Vertrauen darin zu unterhöhlen, indem wir auch nur den Verdacht aufkommen lassen, dass Sicherheitslücken, die an diese Behörde gemeldet werden, am Ende bei Diensten landen, wo es dann irgendeine Abwägung gibt zwischen wie lange brauchen wir jetzt die Sicherheitslücke noch zur Erfüllung dieser Aufgabe oder wäre es besser sie zu schließen, in dem Augenblick ist das Vertrauen in solche Behörden dahin. Und das ist ein Weg, den wir nicht gehen sollten. Also wir sehen insbesondere in den USA, wo es dieses Prinzip schon sehr lange gibt, diesen sogenannten Security Vulnerability Equities Process, dass es immer schief geht. Dass sich die Geheimdienste nicht ehrlich verhalten und dass auch natürlich Sicherheitsforscher,

die über solche Probleme stolpern, keine Lust haben, in diesem Spiel mitzuspielen und diese Sicherheitslücken z. B. dann für geheimdienstliche Zwecke zu offenbaren. Das heißt, die Frage, wie man so eine Behörde aufstellt, wie eine Unabhängigkeit auch glaubwürdig gewährleistet werden kann, das ist ein zentrales Problem.

Ein zweites Problem, was wir haben, ist Bildung. Und zwar nicht unbedingt nur im Bereich von Sicherheitsexperten. Da haben wir sicherlich auch Probleme. Aber die Menge an Software, die wir in diesem Land jeden Tag produzieren, wird zum größten Teil von Menschen gemacht, die noch nie gehört haben, wie man sichere Software schreibt. Unsere zentrale Forderung an die Politik wäre dafür zu sorgen, dass niemand in diesem Land mehr programmieren lernt – egal wo, egal ob an der Schule, in der Universität, in der Fachhochschule – ohne dass er lernt, wie man sicher programmiert. Das ist nicht so schwer. Das ist kein Hexenwerk. Das ist tatsächlich nur Basiswissen. Aber zu verlangen, dass alle Ausbildungsinstitutionen sicheres Programmieren mit aufnehmen, wenn sie in irgendeiner Art und Weise programmieren lehren, ist – denke ich – der einzige Weg, wie wir langfristig dieses Problem zumindest eingrenzen können.

Ein zweiter Schritt in diese Richtung wäre zu sagen, wir müssen dafür sorgen, dass wir mehr sichere Software bekommen und dazu braucht es Förderprogramme. Die Wirtschaft selber wird es nicht hinbekommen. Und die Wirtschaft selber hat zu viele andere Prioritäten. Die wollen als Erster am Markt sein. Wir müssen da als Staat agieren. Wir brauchen Methoden, mit denen wir schnell kleine Projekte fördern können, die einzelne Softwarekomponenten sicher neu implementieren, die dann für alle zu verwenden sind.

Eine dritte Komponente dabei ist ganz sicherlich dieses Thema Zertifizierung, was heute schon häufiger kam. Wir haben das Problem, dass Zertifizierung zu statisch ist. Zertifizierung funktioniert in der IT einfach überhaupt nicht. In dem Augenblick, wo Sie ein Zertifikat haben, ist Ihr Produkt schon wieder mindestens drei Jahre alt, nach heutigem Stand der Technik, und dann können Sie es eigentlich schon wegschmeißen, weil es entweder überholt ist oder mittlerweile Sicherheitslücken darin bekannt geworden sind. Wir denken, dass der einzig sinnvolle Weg der ist, der in den bereichsspezifischen Sicherheitsanforderungen für kritische Infrastruktur angefangen wurde. Nämlich zu sagen, dass wir pro Branche eine Art Komitee, ein Gremium schaffen, was die Sicherheitsanforderungen für diese Branche dynamisch alle drei Monate erneuert. Und das in Einhalten dieser Anforderungen der einzige Weg ist, ein Zertifikat kontinuierlich zu erhalten. Weil wir haben das Problem, dass statische Zertifikate in der Vergangenheit überall versagt haben. Niemand hat es hinbekommen. Das ist einfach prinzipiell unmöglich. Das heißt, wir brauchen einen dynamischen Weg, wie wir IT-Sicherheit beurteilen und zertifizieren, was dann auch eine Grundlage dafür sein kann, um Haftungsregelungen einzuführen, um dafür zu sorgen, dass die Wirtschaft motiviert wird in die IT-Sicherheit zu investieren. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Dann Herr Schönbohm, bitte.

SV Präs **Arne Schönbohm** (BSI, Bonn): Sehr geehrte Frau Vorsitzende, meine sehr geehrten Damen und Herren. Die Anzahl und Qualität der Cyberangriffe auf staatliche und zivile Ziele nimmt eklatant zu. Auch die kritischen Infrastrukturen sind verstärkt im Fokus der Angreifer. Die hohe Dynamik bei der Weiterentwicklung von Schadprogrammen, ca. 390.000 neue Varianten pro Tag, und Angriffswegen, die steigende Betroffenheit durch ein „Smart-Everything“ sowie die zunehmende Angriffsintensität verdeutlichen die Verletzlichkeit von IT-Systemen und digitalen Infrastrukturen in einer zunehmend vernetzten Welt. Meine Vorredner haben davon teilweise schon gesprochen. In Anbetracht der erhöhten Gefährdungslage und der zunehmenden Digitalisierung von Staat, Wirtschaft und Gesellschaft ist Informations- und Cybersicherheit zur Voraussetzung für das Gelingen der Digitalisierung geworden. Wenn wir auch in Zukunft einen starken und sicheren Standort Deutschland haben wollen, müssen wir mehr in Informations- und Cybersicherheit investieren. Auch der Staat muss im Bereich Cybersicherheit verstärkt aktiv werden. Als nationale Cybersicherheitsbehörde gestaltet das BSI auf der Basis seines gesetzlichen Auftrags Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Der auch im Koalitionsvertrag von CDU/CSU und SPD festgelegte geplante Ausbau des BSI sowie die Weiterentwicklung des IT-Sicherheitsgesetzes einschließlich neuer Befugnisse

und Möglichkeiten des BSI zum Schutz der IT-Systeme des Bundes sind wichtige Schritte, die nun konsequent umgesetzt werden müssen. Das BSI ist die einzige Bundesbehörde mit klarem gesetzlichen Auftrag zur Cyberabwehr und muss angesichts der dynamischen Gefährdungslage auch in den kommenden Jahren weiterhin substantiell verstärkt werden. Die Gewährleistung von Cybersicherheit als Voraussetzung für eine gelungene Digitalisierung erfordert eine ständige Überprüfung von Prozessen, Befugnissen und Zuständigkeiten. Das BSI soll als neutrale Beratungsstelle in Fragen der IT-Sicherheit für Bund, Länder, Unternehmen und Bürgerschaft gestärkt werden. Auch eine Ausweitung der präventiven Aufsichtsbefugnisse wird angestrebt: Unternehmen und Hersteller von IT-Produkten, die wie kritische Infrastrukturen von besonderem nationalen Interesse sind, sollen hierbei stärker in die Pflicht genommen werden.

Die zunehmende Digitalisierung bietet für den Einzelnen große Chancen. Durch eine Stärkung präventiver Sicherheitsmaßnahmen sowie die geplante Einführung eines IT-Sicherheitskennzeichens, werden Anwender künftig besser geschützt und Verbrauchern mehr Orientierung geboten. Diese Aufgaben übernimmt das BSI als die zentrale Stelle für Zertifizierung und Standardisierung. Im Bereich der künstlichen Intelligenz festigt das BSI seine Rolle als Thought Leader, beispielsweise durch die Einrichtung des Kompetenzzentrums KI und bündelt darin die bereits vorhandene Expertise. Gewonnene Erkenntnisse stellt das BSI in seiner Eigenschaft als neutrales Kompetenzzentrum für die IT-Sicherheit allen Ressorts zur Verfügung. Aufgrund dieser Querschnittsfunktion ist das BSI eine Behörde von besonderer Bedeutung. Auch künftig soll das BSI zentrale Anlaufstelle für alle Fragen der IT-Sicherheit in der Digitalisierung sein. Beispiele für die Unterstützung der Ressorts sind die IT-Sicherheitsberatung aller Ressorts, die elektronische Gesundheitskarte BMG, das Smart Meter BMWi sowie das autonome Fahren für das BMVI. Durch seine integrierte Wertschöpfungskette der Cybersicherheit identifiziert das BSI unter anderem mit Hilfe der Schadsoftware-Erkennungssysteme Angriffskampagnen und Lücken in bestehenden Systemen. Die daraus abgeleiteten Warnungen adressieren Bund, Länder, Kommunen, KRITIS-Betreiber, die Wirtschaft und die Bevölkerung. Im Jahr 2018 hat das BSI über 16 Millionen Warnmails an deutsche Netzbetreiber versendet, um auf Gefahrensituationen aufmerksam zu machen. Die gewonnenen Erkenntnisse fließen in die Zertifizierung und Zulassung neuer Produkte ein. Eine sachgerechte Aufgabenerledigung und damit die Gewährleistung und Stärkung der Cybersicherheit der Bundesrepublik Deutschland kann nur im Rahmen der bestehenden Bündelung und Vernetzung von Cybersicherheitsexpertise innerhalb des BSI erfolgen.

Das BSI hat eine gesamtgesellschaftliche Verantwortung inne. Die spiegelt sich auch in den im Koalitionsvertrag neu festgelegten Aufgabenbereichen wie beispielsweise dem digitalen Verbraucherschutz, Beratung für Wirtschaft und KMUs sowie Beratungs- und Unterstützungsangebote für die Länder wider. Letzteres ist essentiell, um einer Fragmentierung, die bereits angesprochen worden ist, im Bereich Cybersicherheit entgegenzuwirken. Für die Sicherheit der Bundesrepublik Deutschland und ihrer Länder besteht die gemeinsame Verantwortung, durchgehend ein qualitativ hohes, einheitliches und angemessenes Cyber-Sicherheitsniveau sicherzustellen. Hier kommt dem BSI eine entscheidende Bedeutung zu. Alleine gegenüber den Bundesländern konnten in den vergangenen zwei Jahren neun Absichtserklärungen für eine engere Kooperation geschlossen werden. Auch in der globalen Herausforderung arbeiten wir aktiv mit. So haben wir zahlreiche Rollen und Funktionen bei der NATO oder auch bei der EU inne.

Letzten Endes sind robuste und vertrauenswürdige Netzinfrastrukturen wie 5G Grundlage der Digitalisierung in Deutschland. Gemeinsames Ziel aller beteiligten Akteure ist eine sichere Infrastruktur für den Mobilfunk der Zukunft, wobei Sicherheitseigenschaften der verschiedenen Netzbereiche herstellerneutral gestaltet und die Sicherheit des Gesamtnetzes somit unabhängig vom jeweiligen Hersteller gewährleistet werden kann.

Ich möchte mich bei Ihnen für die zahlreichen neuen Stellen bedanken und ich möchte Ihnen auch mitteilen, dass wir mit als beliebtester Arbeitgeber in diesem Bereich Ende 2018 eine Besetzungsquote von 95 Prozent erreicht haben. Ich danke Ihnen für Ihre Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Schönbohm vielen herzlichen Dank und den Schluss in der Runde macht noch Frau Dr. Sowa.

SVe **Dr. Aleksandra Sowa** (Bonn): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Bundestagsabgeordnete. Ich bedanke mich für die Einladung. Die IT-Sicherheit stärken, Freiheit erhalten, Privatsphäre stärken, effektive Maßnahmen einführen, hinreichende Ressourcen bereitstellen, Ende-zu-Ende-Verschlüsselung als Recht gewährleisten. Tolle Anträge mit guten Ideen, Lösungsansetzen und Vorschlägen, wie man IT-Sicherheit, diese „Achillesferse des Informationszeitalters“ in Deutschland und Europa stärken solle. Zuerst vielen Dank dafür. Ein Déjà-vu-Effekt setzt jedoch ein. Backdoor, Recht auf Verschlüsselung, Hackbacks und die Rolle der Bundeswehr bei all dem, Cyberabwehr und die Ausgründung oder Neugründung einer unabhängigen Behörde mit Zuständigkeit Digitales und/oder IT-Sicherheit, Überwachungssoftware und ihre Exporte, all das ist schon einmal da gewesen. Seit mehr als 20 Jahren wird debattiert, Argumente und Gegenargumente ausgetauscht, Experten angehört und Lösungen vorgeschlagen, ob im Virtuellen Ortsverein, der Möglichkeiten des Internets für die politische Arbeit erproben wollte, in der Enquete-Kommission oder zuletzt anlässlich des Widerstandes von Apple, den US-Behörden, dem FBI, Zugriff auf das iPhone des San-Bernardino-Attentäters einzuräumen. Das Ziel des Krieges sei Sieg und nicht die Fortsetzung von Kriegsoperationen, klärte Sun Tzu auf. Um es mit dem chinesischen Kriegsherrn zu halten, der Bundestag wird endlich entscheiden müssen. Denn dafür, wo Deutschland in den nächsten Jahren in dem Thema IT-Sicherheit steht, wird der Gesetzgeber verantwortlich sein.

„Anonymes Surfen, das brauche man nicht in einer Demokratie“, erklärte der Innensekretär Günter Krings der Süddeutschen Zeitung. Das Gegenteil davon ist richtig: Gerade in einem freien Land, in einer Demokratie, braucht man Anonymität im Internet, nicht weniger als im Allgemeinen. Tatsächlich können Straftaten in Computernetzen nur vermieden werden, wenn die Vertraulichkeit der Kommunikation mittels sicherer Verschlüsselung gewährleistet ist. Das wurde bereits im Jahre 1998 im Schlussbericht der Enquete-Kommission festgehalten. Während es technisch und organisatorisch relativ einfach ist, kompatible, verschlüsselte E-Mail-Kommunikation und Datentransfer in kleinen, autarken Organisationen wie einer Behörde oder Unternehmen zu implementieren, ist Etablierung und Einführung von Lösungen, die ganze Gesellschaften umfassen, weit weniger trivial. Ein Beispiel dafür ist Pretty Good Privacy von Phil Zimmermann. Damit Technologien, wie diese, zum Masseneinsatz kommen, erfordert es Unterstützung und Förderung. Ja, es wird Geld kosten. Ja, es wird Förderung bedürfen. Und ja, Politik und Staat müssen beteiligt sein.

Politik muss involviert sein, um Lösungen wie Ende-zu-Ende-Verschlüsselung zu gewährleisten, die jedermann zugänglich sind und auf die man vertrauen kann. Erstens muss die Prämisse Privacy-as-a-Right und Security-as-a-Right heißen - und nicht etwa Privacy- and Security-as-a-Service. Zweitens wird eine konsequente Positionierung hinsichtlich der Frage der Backdoors – der Hintertüren – erforderlich. IT-Sicherheit hilft zweifellos auch Kriminellen. Technologien wie Ende-zu-Ende-Verschlüsselungen oder starke Kryptografie können gewiss auch Terroristen nutzen. Aber keine IT-Sicherheit bedeutet für alle Nichtkriminellen mehr Kriminalität. Insofern gefährdet ein Staat, der vermeintliche Sicherheit vor IT-Sicherheit setzt, seine Schutzfunktion gegenüber den Bürgern.

Um des Weltfriedens willen ist es vermutlich viel wichtiger, sichere Plattformen für die Kommunikation zu haben, als dass gelegentlich ein Krimineller nicht geschnappt werden kann. Stattdessen fordert, wie im letzten Artikel von Frau Dr. Sabine Vogt, das Bundeskriminalamt wieder neue Gesetze. Tor, Darknet, eigene Strafbarkeit für Administratoren und Moderatoren der als illegal bezeichneten Plattformen usw. Wer aber die IT-Sicherheit einer vermeintlichen Sicherheit opfert, erntet nicht Sicherheit, sondern Kriminalität. Mehr Kriminalität. Es ist bedauerlich, dass diese banale Erkenntnis auch nach über 20 Jahren nach der damaligen Enquete sich noch immer nicht als Allgemeingut durchgesetzt hat. Nichts davon ist falsch. Im Gegenteil. Und aus diesem Grund ist die Herauslösung des BSI aus dem BMI vordringlich, wie es zuvor die Herauslösung des BSI aus dem BND war. Statt Strategien für Kriege der Zukunft zu entwickeln, sollten Unternehmen und Behörden ihre Systeme und Netzwerke angemessen, gemäß dem Stand der Technik, absichern, in Firewalls und Perimeter-Sicherheit und in gut ausgebildete sowie erfahrene Spezialisten investieren, damit externe Angreifer nicht mehr mit gewohnter Nonchalance in die Sys-

teme eindringen können. Und nicht auf den Hinweis der Geheimdienste warten, ob sie eventuell doch Opfer einer Cyber-Attacke geworden sind. Die Einführung genereller Meldepflichten …

Vors. **Andrea Lindholz** (CDU/CSU): Ich müsste jetzt auch an die Zeit erinnern.

SVe **Dr. Aleksandra Sowa** (Bonn): Dann komme ich schnell zum Schluss. Auch die Einführung von Meldepflichten für Sicherheitsvorfälle nach dem Vorbild der Datenschutzgrundverordnung für alle Brachen und Organisationen, unabhängig von der Größe und dem Sektor, könnte eine sinnvolle Ergänzung der detektiven IT-Sicherheit sein. Ein schlüssiges Konzept – da möchte ich auf den Vorschlag von Herrn Dr. Herpig eingehen – ein schlüssiges Konzept einer einheitlichen Strategie für mehr digitale Sicherheit wird im Antrag der Fraktion LINKE gefordert. Tatsächlich verhält es sich mit den Vorschlägen und Lösungsansätzen zur IT-Sicherheit ein wenig wie in dem Dürrenmattschen Hörspiel „Herkules und der Stall des Augias“. „Bilden wir eine Oberkommission“, ruft einer. „Beschlossen schon, wir bilden eine Oberkommission“, erwidert das Bauernparlament. Digitalministerium, ZITiS, BSI, Gründung, Neugründung, Ausgründung, Zentralisierung und Dezentralisierung. Der Bundestag wird eine grundsätzliche Entscheidung treffen müssen. Möchte man weiterhin Technologien fördern, die Überwachung, Lebens- und Arbeitskontrolle stärken oder möchte man in Technologien investieren, die neue Lebens- und Arbeitsentwürfe ermöglichen, Freiheit und Demokratie stärken und so seine Schutzfunktion gegenüber den Bürgern ausfüllen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Ich darf noch, bevor wir in die Fragerunde eintreten, zwei, drei organisatorische Sachen sagen. Die Anhörung ist anberaumt bis 16:00 Uhr. Unsere Sitzung wird im Parlamentsfernsehen übertragen und das Protokoll enthält selbstverständlich sämtliche Stellungnahmen, die eingegangen sind und wird in der Gesamtdrucksache mit übersandt. Und zu guter Letzt darf ich heute noch Herrn Könen vom BMI begrüßen. Dann kommen wir jetzt zur Fragerunde und beginnen mit Herrn Bernstiel.

Abg. **Christoph Bernstiel** (CDU/CSU): Zunächst einmal vielen Dank an alle Experten, dass Sie sich die Zeit genommen haben, heute zu diesem wichtigen Thema zu sprechen und ich freue mich auch sehr, dass eigentlich durchweg alle Experten gesagt haben, dass das Thema hohe Relevanz hat und dass auch der Staat eine wichtige Aufgabe bei dem Thema IT-Sicherheit zu erfüllen hat. Ich würde gerne eine Frage an Herrn Dr. Baumgart richten. Und zwar, wenn wir über IT-Sicherheit sprechen, dann sprechen wir nicht nur über Dinge, die der Staat tun kann, sondern vor allen Dingen auch was können die Bürger und insbesondere Sie als Vertreter der Wirtschaft, was können mittelständische Unternehmen tun. Und insbesondere würde ich Sie bitten mal darauf einzugehen, wie es denn mit dem Thema Awareness für überhaupt Cyber Security Fragen in der mittelständischen Wirtschaft aussieht, denn meines Erachtens gibt es da auch noch sehr viel Aufholbedarf. Könnten Sie schildern, was aus dieser Perspektive noch zu tun wäre. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Wir sammeln erst die Fragen, dann kann jeder von Ihnen antworten auf alle Fragen, die ihm gestellt worden sind. Dann kommen wir als nächstes zu Herrn Haug.

Abg. **Jochen Haug** (AfD): Dankeschön, Frau Vorsitzende. Ich habe zunächst eine Frage an Herrn Landefeld. Sie schreiben in Ihrer Stellungnahme, dass die Erfahrungen, die eco in Workshops mit Strafverfolgern und Ermittlungsbehörden gemacht haben zeigen, dass hier noch dringender Informations- und Nachschulungsbedarf besteht. Da würde mich interessieren, in welcher Hinsicht der genau besteht. Das heißt, einfach eine Konkretisierung, wo besteht Nachholbedarf und Schulungsbedarf? Wie sieht der aus? Und dann habe ich eine Frage an Herrn Rieger. Sie hatten gerade ein paar sehr spannende Ausführungen gemacht und zwar zu der Frage, dass man gesellschaftlich – also nicht nur in Schulen, sondern in allen Bereichen, aber auch in Schulen – nicht nur Programmieren lernen soll, sondern sicheres Programmieren lernen soll. Das hört sich auch sehr gut an. Da wäre meine Frage jetzt so laienhaft gedacht – würde ich jetzt sagen – gibt es die entsprechenden Ausbilder an den Schulen aktuell. Gibt es Personen? Und wenn ja, wie viele Personen würden Sie denn z. B. grob in Deutschland einschätzen, die Kompetenzen haben, so weit Kompetenzen haben, dass sie andere auch im sicheren Programmieren ausbilden können? Das heißt, wie würden Sie sich vorstellen, dass so ein Konzept umsetzbar wäre. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Haug, vielen Dank. Herr Hartmann.

Abg. **Sebastian Hartmann** (SPD): Frau Vorsitzende, herzlichen Dank. Ich möchte entsprechend des Protokolls unserer Anhörung eine Frage an zwei Sachverständige richten. Die Frage soll identisch sein. Und zwar möchte ich einerseits an Herrn Dr. Herpig die Frage stellen, die im Zuge der Weiterentwicklung des IT-Sicherheitsgesetzes – Sie sind jetzt auf einzelne Paragraphen nicht eingegangen, das haben Sie in Ihrer Stellungnahme auch nochmal deutlich gemacht – gibt es immer wieder den Ruf nach digitalen Gegenschlägen, sogenannten Hackbacks, die Stufe 5 auch in der BMI-Skala. Wie würden Sie, auch wenn das jetzt nicht in den Entwürfen enthalten ist, wie würden Sie die Sinnhaftigkeit beurteilen. Auch in der Frage, würden Sie eine Grenze zwischen Notwendigkeit und Verhältnismäßigkeit ziehen und wo würden Sie entsprechende rote Linien, sofern Sie das in dem IT-Sicherheitsgesetz 2.0 in dem Entwurf betrachtet haben, ziehen. Die gleiche Frage möchte ich an Herrn Schönbohm richten, der einerseits mit der entsprechenden Aufgabe betraut ist unsere Sicherheit auch sicherzustellen, den Stellenaufwuchs erfahren hat bei einer Fortentwicklung. Also wie würden Sie die Frage der Hackbacks einordnen, was unsere digitale Sicherheit angeht. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Höferlin.

Abg. **Manuel Höferlin** (FDP): Danke, Frau Vorsitzende. Vielen Dank an die Sachverständigen für die schriftlichen, aber auch vor allen Dingen für die mündlichen Darlegungen. Ich habe zwei Fragen an zwei Sachverständige. Zuerst eine Frage an Herrn Schönbohm. Sie haben auch in Ihrer schriftlichen Darlegung beschrieben, dass das BSI eine Beratungsstelle sein soll bei allen möglichen Fragen, auch für Bund, Länder, für die Bürgerschaft, die gestärkt werden soll, also eine zentrale Stelle werden soll. Das finden wir eine sehr gute Sichtweise von sich selbst, auch für das BSI, weil das können wir uns – glaube ich – alle nur wünschen. Sie haben aber dort auch und das haben Sie jetzt gerade eben in Ihrer mündlichen Darlegung auch nochmal gesagt, Sie hätten als einzige Bundesbehörde einen klaren gesetzlichen Auftrag zur Cyberabwehr. Das würde mich mal interessieren, wie Sie Cyberabwehr in diesem Zusammenhang genau definieren, weil so habe ich den gesetzlichen, den klaren gesetzlichen Auftrag noch nicht wiedergefunden. Vielleicht haben Sie auch einfach eine Stelle, wo ich nachlesen kann, wo das so klar steht. Das war mir noch nicht so ganz klar. Die zweite Frage geht dann an Herrn Landefeld. Sie haben auch in Ihrer Stellungnahme über die organisatorische Fitness von Sicherheitsbehörden gesprochen und auch über die Notwendigkeit einer unabhängigen Arbeit des BSI. Mich würde interessieren, wie denn aus Ihrer Sicht, aus Sicht der Digitalwirtschaft, denn ein BSI mit dieser Aufgabe optimal aufgestellt werden könnte. Eine große Frage ist, wie das BSI grundsätzlich angehängt oder nicht angehängt sein soll. Also ist es notwendig, dass es einem Ministerium angehängt ist oder ist es notwendig, dass es auf keinem Fall an ein Ministerium angehängt wäre oder falls man ein Ministerium dafür nehmen sollte, auch aufgrund der Beschreibung, wie vielleicht Herr Schönbohm in seiner mündlichen Stellungnahme gerade eben gesagt hat, für was für verschiedene Ministerien er zuarbeitet und für welche Gesetzesprojekte. Wo man ihm am besten anhängt ganz konkret, z. B. an ein Digitalministerium. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Frau Domscheit-Berg, bitte.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich habe zunächst eine Frage an Frau Sowa. Es wird sehr viel von der Schwachstelle Mensch gesprochen und ich möchte in diesem Zusammenhang auf das Unterthema Cybercrime, digitale Gewalt hinweisen, von der insbesondere Frauen sehr oft betroffen sind, dass sie auf ihren Geräten Spyware installiert haben und es im Moment für sie sehr wenig Möglichkeiten gibt, dafür Hilfe und Support zu bekommen. Wir haben auch das Thema, dass Doxing z. B. nicht als Cybercrime gewertet wird etc. Jetzt habe ich in dem Zusammenhang eine Frage: Wie kann man dafür sorgen, dass sich einerseits Bürgerinnen und Bürger besser schützen können vor solchen Angriffen? Und wie kann andererseits der Staat dazu beitragen, dass sie besser geschützt sind. Ich habe eine zweite Frage, die möchte ich an Herrn Dr. Herpig richten. Wie sollte eine gesetzliche Regulierung beschaffen sein, mit der man Hersteller von Hard- und Software zwingen kann für höhere Sicherheitsstandards zu sorgen. Muss man oder kann man einzelne Themenfelder dabei ausnehmen? Wäre es nicht sinnvoll, wenn man anstelle

eines fakultativen Sicherheitslabels, das im IT-Sicherheitsgesetz vorgesehen ist, verbindliche Mindestsicherheitsstandards vorschreibt. Zum Beispiel, dass bestimmte Passwörter, die unter den Top 100 der Passwörter vorkommen, einfach nicht zulässig sind. Oder dass es wie Mindesthaltbarkeitsdaten auch Mindestupdatepflichten gibt. Wäre es nicht sinnvoll, sowas verpflichtend für alle zu haben. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank und dann zum Schluss noch Herr von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Frau Vorsitzende. Vielen Dank an die Sachverständigeneinlassungen. Ich darf für meine Fraktion sagen, dass wir uns sehr freuen, dass diese Anhörung hier heute stattfindet. Unser Antrag liegt seit einem guten Jahr vor. Es gibt inzwischen von allen Oppositionsfraktionen Anträge zu dem Thema und der Kollege Bernstiel hat eben gesagt, es ist deutlich geworden bei ihnen, dass das Thema eine hohe Relevanz hat. Die Frage, die wir uns stellen ist, ob das auch für die Bundesregierung gilt. Aber ich habe auch zwei Fragen. Die erste geht an den Sachverständigen Rieger. Ich fand das ein schönes Bild mit der weißen Fahne. Wenn man die weiße Fahne jetzt nicht hissen will, was wären denn so die drei Dinge, die man jetzt unmittelbar dieses Jahr noch von der Platte kriegen muss, um sie nicht hissen zu müssen. Also sind das Haftungsfragen oder ganz konkreter Ausbau, Unabhängigstellung des BSI. Einfach so die Top 3. Und meine zweite Frage geht an den Sachverständigen Landefeld, ob Sie es nicht auch kurios finden – ich selbst finde, dass ist eine interessante Debatte um Huawei und finde auch, chinesische Konzerne, da sollte man mal einen Blick draufwerfen, was die so zusammenbasteln – und da braucht es einen Katalog, das BSI sitzt da vor allem im Auftrag der Bundesregierung dran, bin ich sehr gespannt, was da für ein Katalog kommen wird. Aber wir haben gleichzeitig immer noch den Status Quo, dass alle Länder dieser Welt an ihren Glasfaserknotenpunkten, also die Verkehrsdaten ziemlich tutto kompletto von einigen Schlaufen ableiten und zumindest den gesamten Datenstrom mit Millionen von Selektoren durchforsten. Das ist mal eine Sicherheitslücke. Vor allen Dingen, die gibt es nicht nur in Frankfurt, sondern in allen Glasfaserknotenpunkten. Huawei-Sabotage ist nochmal eine andere Frage. Aber wie ist das mit diesen Datenabflüssen und Informationsabflüssen, die da stattfinden und ist das nicht ein bisschen eine merkwürdige Diskussion, dass eine – wie ich finde zu Recht – zu thematisierten, aber das andere nicht. Und müssten wir nicht eigentlich auch darüber sprechen, was mit diesen Abgriffen in dieser Pauschalität ist, zumindest in den Rechtstaaten dieser Welt und gilt das dann nicht auch für Hintertüren und ähnliches. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir jetzt zur Beantwortung der Fragen und fangen bei Herrn Dr. Baumgart an.

SV **Dr. Rainer Baumgart** (secunet Security Networks AG, Essen): Es war die Frage, was kann die Wirtschaft tun. So hatten Sie formuliert, glaube ich. Es gibt nicht einfach die Wirtschaft, sondern wir müssen einfach sehen, dass insbesondere bei deutschen Großunternehmen – also ich sage mal DAX-Konzerne – dieses Thema schon eine sehr hohe Sensibilität hat. Und dass diese Unternehmen auch Verantwortlichkeiten festgelegt haben und insbesondere auch, wenn sie international tätig sind – ich sage mal – ihre Assets sehr wohl schützen. Größtenteils mit den gleichen Maßnahmen wie das BSI die auch in Sicherheitsinfrastrukturen des Bundes beispielsweise einsetzt und sich hier auch der gleichen Technologie bedienen. Diese Großunternehmen, die häufig international tätig sind, haben dann gelegentlich Probleme, dass sie gerne starke Verschlüsselung einsetzen möchten, aber im Ausland, insbesondere auch in Asien oder einigen anderen Ländern, blockiert werden diese Technik dann einzusetzen, weil man ihre Kommunikationsinfrastrukturen dann gelegentlich einfach abschaltet oder den Betrieb dieser Sicherheitstechnik nicht genehmigt. Aber das ist noch ein anderes Thema. Also die Wirtschaft der Großunternehmen – würde ich sagen – ist sehr sensibilisiert. Im Mittelstand und insbesondere bei kleinen Unternehmen ist das Gegenteil der Fall. Hier fehlt zum Teil das Wissen, Aufklärung, Verantwortlichkeit, aber auch eine gewisse Investitionsbereitschaft. Das muss man einfach sagen. Es hat sich im Bereich der Betreiber kritischer Infrastrukturen vor einiger Zeit – nur sind das zum Teil auch große Unternehmen muss ich wieder sagen – eine Bereitschaft nach Einführung des IT-Sicherheitsgesetzes, was kritische Infrastrukturbetreiber betrifft, geändert, weil sie müssen. Hier gab es zumindest dann einen ver-

stärkten Anlass auch zu investieren und die Notwendigkeit wird nicht mehr diskutiert. Aber das Gegenteil ist eigentlich im Bereich der mittelständischen Wirtschaft und der kleineren Unternehmen. Hier fehlt Aufklärung. Hier fehlt wahrscheinlich auch ein gewisser Druck. Natürlich gibt es da auch sehr viele Schäden und man weiß gar nicht, was alles für Probleme im eigenen Unternehmen existieren. Aber darüber hinaus, man lebt damit und traut sich nicht zu investieren, weil man glaubt dadurch eventuell wirtschaftliche Nachteile zu haben. Hier fehlt es auch einiges an Erfahrungen umzusetzen, die man in anderen technischen Bereichen schon seit langem hat. Wenn man technische Anlagen betreibt gibt es so etwas wie eine Überwachung. Es gibt Sicherheitsmaßnahmen, die Standard sind, die eingeführt werden. Die werden regelmäßig kontrolliert. Das gilt selbst in den Finanzbereichen. Das gilt bei Compliance und vielen anderen Themen. Im Bereich der IT-Sicherheit ist das oder Cybersicherheit ist das für viele nice to have und auf freiwilliger Basis und wenn man es nicht macht, passiert demjenigen zunächst mal nichts. Und daher könnte Aufklärung und ich meine auch Nachdruck, wie man das vor Jahren schon immer gehabt hat, wenn man den Sicherheitsgurt nicht angelegt hat, passierte nichts und als das plötzlich vor 40 Jahren 10 DM kostete, hatten wir eine hohe Anschnallquote und die Todesfälle gingen zurück. Aber das nur ein Beispiel aus den Erfahrungen in der Industrie.

Abg. **Christoph Bernstiel** (CDU/CSU): Digitaler Sicherheitsgurt.

Digitaler Sicherheitsgurt. Kann man fordern als Minimalmaßnahme. Aber auch die Überwachung, gerade schon genannt, dass Maßnahmen umgesetzt werden und entsprechende Kontrollfunktionen haben in anderen Bereichen in der Vergangenheit sehr wohl erfolgreich geholfen und diese Unternehmen können natürlich auch daraus einen wirtschaftlichen Vorteil ziehen. Das darf man nicht vergessen. Solche Dinge sind nicht unbedingt ein Nachteil. Man hat es in anderen technologischen Bereichen erlebt, wenn die Sicherheit der Produkte besonders hoch war, kann man daraus auch einen Markterfolg generieren. Vielleicht bis hierhin. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Dr. Herpig.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung): Vielen Dank für die Fragen. Ich würde zu allererst auf die Frage von Herrn Hartmann eingehen. Als ein Framing vielleicht zum Anfang. Ich finde es interessant, wir reden hier über ein Stufenmodell des BMI und über einen Referentenentwurf des IT-Sicherheitsgesetzes. Beides übrigens Dokumente, die nicht der Öffentlichkeit zugänglich gemacht worden sind vom Ministerium, sondern geleakt worden sind. Das mal vorweg. Dann die Definition von aktiver Cyberabwehr ist viel größer, als nur dieses Stufe 5-Modell. Das heißt, ein Angriff mit eigenen Bots oder anderen Maßnahmen, um einen Angreiferserver irgendwie auszuschalten. Viele dieser Maßnahmen, die darunter fallen, sind in den Entwürfen zur Harmonisierung des Verfassungsschutzgesetzes, aber auch zum IT-Sicherheitsgesetz 2.0 bereits beinhaltet. Alles so bis unter gleich Stufe 4. Andere Maßnahmen wurden z. B. so auch mit dem IT-Sicherheitsgesetz 2015 implementiert. Dieser sogenannte Walled Garden Approach. Das Telekommunikationsanbietern ermöglicht wird, dass sie, wenn sie Kenntnis davon haben, dass Rechner, die sich in ihrem Netz bewegen, Bots sind, dass sie die aussperren können. Dann wird ihnen eine Webseite angezeigt, sind Teil eines Bot-Netzes, laden sich das runter und sie können sich so desinfizieren. Ansonsten kommen sie nicht mehr ins Internet. Alles Maßnahmen, die unter die große Definition aktive Cyberabwehr fallen. Teilweise Maßnahmen, die wir schon haben. Teilweise welche, die sich in den Gesetzesvorschlägen wiederfinden. Die rote Linie – für mich jetzt mal ganz lapidar gesprochen – ist dort, wo es um sehr invasive Eingriffe in die Vertraulichkeit und die Verfügbarkeit, die Integrität von informationstechnischen Systemen in Deutschland geht. Vor allem dann, wenn – wie vorhin schon gesagt – keine Schutzmaßnahmen ausgebaut werden und wir überhaupt keine Ahnung haben, ob wir diese Maßnahmen überhaupt brauchen oder ob die Sicherheitsbehörden schon über andere Befugnisse Möglichkeiten haben, ähnliche Informationen zu erhalten.

Bei Stufe 5 kommt es nochmal hinzu, dass mir bisher noch niemand sinnvoll darlegen konnte, wie das zu mehr IT-Sicherheit beitragen soll. Es gibt andere Maßnahmen, die weniger invasiv sind, mit denen das gleiche Level an IT-Sicherheit hergestellt werden kann und gegen Angriffe verteidigt werden kann. Von daher würde ich mich darüber freuen, wenn wir da endlich eine öffentliche Diskussion

drüber haben, aber auch eine nuancierte Definition und Diskussion darüber, weil – wie gesagt – wir sprechen über Dokumente, die geleakt worden sind und über die wir keinen öffentlichen Diskurs haben.

Dann zu der Frage, die nicht an mich war, aber ich würde ganz kurz darauf eingehen von Herrn MdB Höferlin. Unabhängigkeit des BSI: Ich glaube eine Unabhängigkeit oder das Herauslösen des BSI aus dem Innenministerium birgt viele Probleme und Herausforderungen, die wir noch gar nicht übersehen können. Deswegen vorhin mein Statement auch eine fachliche Unabhängigkeit. Es gibt da Modelle, wie das Statistische Bundesamt, wo das schon geschehen ist. Es gibt aber auch andere Modelle der Unabhängigkeit wie bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit. Was uns hier wieder fehlt und das habe ich in meinem Eingangsstatement schon erwähnt, ist eine Strategie. Wir haben gar keine Analyse, welche Modelle es gibt. Welche wären sinnvoll? Welche wären nicht sinnvoll? Vielleicht kommen wir am Ende dieser Analyse auch dabei raus, dass keines dieser Modelle auf das BSI passen würde. Aber das wissen wir nicht, sofern wir uns nicht damit beschäftigen.

Und dann die letzte Frage von Frau MdB Domscheit-Berg. Regulierung für höhere Sicherheitsstandards: Ich gehe schon davon aus, dass wir höhere IT-Sicherheit dadurch erreichen, dass wir Standardpasswörter verbieten und einen Updateschutz einführen. Das muss sich natürlich auch mit den wirtschaftlichen Logiken irgendwie arrangieren. Aber ich glaube, wir fangen auch ganz tiefer an. Wenn wir uns den Referentenentwurf des IT-Sicherheitsgesetzes 2.0 angucken, dann ist das IT-Sicherheitskennzeichen nicht mal verpflichtend. Es ein freiwilliges IT-Sicherheitskennzeichen. Das zeigt, wie weit wir von einer Regulierung für Soft- und Hardware entfernt sind. Was es hier braucht ist unter anderem die nuancierte Debatte zu Schwachstellen. Das hilft schon mal sehr viel. Auch vor allem in Hard- und Software, ganz klar. Dazu habe ich an anderer Stelle was gesagt. Aber auch die Stärkung des Verbraucherschutzes und der Aufsichtsbehörden. Laut EU-Regulierung können sie mittlerweile auch schon Bußgelder vergeben. Auch da sollten wir mehr reingucken und die Ressourcen im Bereich Verbraucherschutz aufbauen. Ich glaube, dass ist im IT-Sicherheitsgesetz 2.0 auch bereits erwähnt. Das ist ein wichtiger Vorgang. Wenn wir uns z. B. angucken, die Bundesnetzagentur hat dieses Kinderspielzeug mit der Kamera damals dem Verkehr ziehen lassen. Ich glaube, das ist etwas, wie es sinnvoll funktionieren kann. Daran sollten wir uns orientieren. Und ich glaube, dass ist der Weg, den wir da gehen können. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Dr. Herpig, vielen Dank. Herr Landefeld, bitte.

SV **Klaus Landefeld** (eco – Verband der Internetwirtschaft e. V., Berlin): Der Reihe nach. Der Herr Bernstiel fragte mich – glaube ich – nach Nachschulungsbedarf für Strafverfolger. Wir betreiben als eco sowohl die Internetbeschwerdestelle als auch haben wir verschiedene Projekte, in NRW z. B. SIWEKOS, und dort zeigt sich immer wieder, dass die Strafverfolger eigentlich die Zusammenhänge des Internet, was, wie funktioniert, welche Dienste wo angesiedelt sind, beim wem welche Daten anfallen, also wer überhaupt welche Durchgriffsmöglichkeiten hat – ich sage mal ganz rudimentär – nicht beherrschen. Das haben wir bei Diskussionen mit Europol im BKA nicht so. Die wissen in der Regel was sie tun und haben ganz gute Fachabteilungen. Aber schon bei den Landeskriminalämtern wird es da oft sehr sehr dünn. Und wenn man aber andererseits eine Zuständigkeit bei der Polizei sieht, auch für die Verfolgung hier an der Stelle, und es insbesondere auch um Beweissicherung und ähnliches geht, dann muss doch ein gewisses Basiswissen irgendwo vorhanden sein, damit man einfach auch zeitnah die richtigen Sicherungsanträge an die richtigen Stellen stellt, sonst sind Daten im Zweifelsfall schon wieder gelöscht, die man vielleicht noch hätte bekommen können, auch ohne erweiterte Befugnis oder ohne längere Speicherdauern und ähnliche Geschichten. Es liegt eigentlich nur daran, dass die zuständigen Stellen gar nicht genau wissen, an wen sie herantreten müssen und in welchem Umfang sie wo Daten bekommen können. Das ist das was wir meinen, wenn wir sagen, hier ist dringender Nachschulungsbedarf, dass man auch, wenn man weitere Verantwortlichkeiten da sieht und auch Polizeien dafür verantwortlich macht, Cybersicherheit – es ist ja durchaus auch so, dass die Polizei weiterhin sich da im Bereich Cybersicherheit auch zuständig sieht – dann müssen natürlich auch entsprechende Schulungen und entsprechendes Personal und Res-

sourcen zur Verfügung stehen, um das auch umsetzen zu können.

Dann gab es die Frage nach der Zuständigkeit BSI. Also wir sehen es so, dass für die Funktion des BSI als zentrale Behörde von Cybersicherheit, wenn es in dem Bereich weiter ausgebaut wird, tatsächlich eine Klarstellung erfolgen muss, dass das BSI unabhängig von den Erwägungen anderer Stellen, anderer Sicherheitsbehörden arbeiten kann und auch ausschließlich der Verbesserung der Sicherheit von IT-Systemen und Netzen verpflichtet ist. Das sehen wir in einer Organisation innerhalb des BMI als sehr sehr schwierig gegeben an. Wenn wir in Zukunft als Netzbetreiber dort unsere Software zertifizieren lassen müssen, unsere Betriebssoftware, unsere Hardware zertifizieren lassen müssen, also immer ein permanenter Einblick nicht nur in die verwendete Software, in die verwendeten Systeme, in Schwachstellen von den Systemen und ähnlichem existiert und dann eine Weitergabe, z. B. an eine ZITiS, die im gleichen Geschäftsbereich irgendwo läuft, erfolgen würde oder müsste, dann ist das natürlich sehr sehr schwierig und dann ist man als Netzbetreiber wahrscheinlich auch nicht wirklich bereit, dann eine Zusammenarbeit zu machen. Es ist auch Stand heute nicht so, dass die Zuständigkeit tatsächlich alleine beim BSI ist. Die Sicherheitskonzepte der Netzbetreiber werden momentan mit der Bundesnetzagentur abgestimmt und dort werden auch die Vorgaben gemacht. Auch die Meldepflicht läuft primär Richtung Bundesnetzagentur. Von daher gibt es sowieso schon Doppelzuständigkeiten. Die Frage, wenn man das in eine Stelle packt, sollte man es wahrscheinlich an eine neutrale Stelle tun. Wo das dann genau ist, müsste man gucken. Es müsste eben ein Ministerium sein, dass dann auch entsprechende Kompetenzen hat für Digitalisierung. Ob jetzt ein Vorschlag eines Ministeriums für Digitalisierung oder so was ähnliches je zum Tragen kommt, dass kann ich natürlich nicht beurteilen. Das hat auch damit wenig zu tun. Wir sind als Netzbetreiber auf jeden Fall mit dem BMWI in der Vergangenheit gut gefahren. Das muss man so ausdrücken.

Dann gab es noch eine Frage von Herrn von Notz zur Einordnung Huawei. Das ist natürlich eine sehr schwierige Frage. Tatsächlich ist es so, dass es hier mehr um eine politische Diskussion geht. Huawei ist Stand heute der Netzbetreiber, der die transparentesten Prozeduren hat. Der seine Software schon auditen lässt von den Betreibern, die es haben. Der ein eigenes Sicherheitszentrum bei den Betreibern aufbaut und auch individuell Software immer nur aus den Modulen zusammenstellt, die man braucht. Wenn ich jetzt sage andere Netzbetreiber aus anderen Ländern haben genau die gleichen rechtlichen Vorschriften – das ist so – dann könnte natürlich theoretisch die gleiche Sicherheitslücke überall existieren. Das hilft aber alles nichts, wenn sie umgangen wird durch administrative oder rechtliche Vorgaben wo es heißt, naja, egal ob euer Netz jetzt sicher ist oder nicht, aber ihr leitet Daten einfach mal aus. Da brauche ich dann keine Schwachstelle. Da habe ich die rechtliche Verpflichtung. Im Prinzip ist es bei Huawei ähnlich. Man sagt, hier ist eine rechtliche Verpflichtung und ihr müsst überhaupt keine Schwachstelle in eurer Software, da muss keine einzige Schwachstelle drin sein, das Netzteam oder der Betreiber beziehungsweise der Hersteller soll auf dem anderen Ende der Welt für eine Ausleitung sorgen in Kenntnis dessen, dass er vielleicht irgendwelche Accounts oder was in seiner Software hat. Ist es dann eine Schwachstelle? Gute Frage. Aber es unterscheidet sich eigentlich nicht davon, dass ich als Netzbetreiber eine Ausleitung vornehmen muss, eben auf Basis meiner eigenen rechtlichen Grundlage. Das ist eine Frage über politische Einflussbereiche und über wer darf was, welche Daten bekomme ich vielleicht in den Zugriff. Da brauchen wir eine gesellschaftliche Diskussion, was zulässig ist, wann was überbordend ist. Diskussionen, wie wir sie jetzt momentan mit dem neuen Verfassungsschutzgesetz sehen, wo dann auf einmal auch im Inland Zugriffsmöglichkeiten auf Daten bestehen und damit im Prinzip eine Legitimierung von der Inlandsausleitung, die auch irgendwo stattfinden würde. Das hilft dann natürlich nicht.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Rieger, bitte.

SV **Frank Rieger** (CCC Berlin e. V.): Die erste Frage war die Frage: Wie macht man das, sicheres Programmieren ausbilden? Das ist relativ einfach, man schafft Lehrmaterial dafür. Das ist kein Hexenwerk, das ist ein Handwerk. Es handelt sich genau um ein Handwerk, wie wenn Sie Buchhaltung lernen. Das heißt, mit entsprechenden Lehrmaterialien – und deren Schaffung sollte einfach passieren, zentral gefördert werden und so strukturiert sein, dass sie

von allen Institutionen frei verwendet werden können – kann man dieses Problem sehr effizient angehen. Das ist aus den Erfahrungen, die wir gemacht haben und wir sind relativ viel in den Schulen unterwegs und bringen Kindern Programmieren bei, ist es sehr einfach. Sobald die einmal verstanden haben, wie ein Buffer-Overflow funktioniert oder wie man stack exploit schreibt, ist das Prinzip dessen, was da passieren kann, in den Köpfen drin und ab da macht man sich da Gedanken drüber, wie man so eine Software baut. Das heißt, die Hürde ist nicht besonders groß, denn es braucht dafür nur Lehrmaterial, das allgemein verfügbar ist und von hoher Qualität, und ganz wichtig, in den Programmiersprachen, die an den verschiedenen Institutionen für das Lehren von Programmieren generell benutzt werden.

Die Frage nach den unmittelbaren Handlungsoptionen – mit drei komme ich nicht aus. Ich denke, wir sollten aufhören an den Symptomen herumzudoktern. Was wir momentan haben, gerade in dem Referentenentwurf jetzt zum IT-Sicherheitsgesetz, ist wieder dieser Versuch drin, zu sagen, wir versuchen irgendwie mit dem Darknet – was auch immer das sein soll – umzugehen und es irgendwie strafbarer zu machen, das Darknet zu benutzen, in der vagen Hoffnung, dass es dazu führen wird, dass die IT-Sicherheit steigen würde. Der kausale Zusammenhang ist nicht so richtig erschließlich. Die Verfügbarkeit von Angriffswerkzeugen hat nicht unbedingt damit zu tun, ob Leute in der Lage sind, einen Tor-Browser zu benutzen, so, das ist ein völlig disjunktes Problem. Sobald man aber anfängt, solche Dinge da rein zu schreiben, hat man einen Großteil der IT-Sicherheitsforscher einfach schlicht gegen sich. Und wir sind in einer Situation, wo wir es nicht – ich sage mal – von Seiten der Politik brauchen können, dass Leute, deren Expertise wir dringend brauchen, um die Probleme zu lösen, sich eher da antagonistisch behandelt fühlen. Das zweite hatte ich schon erwähnt, wir brauchen ein Förderprogramm für sichere Software. Das muss groß sein, wir müssen ganz viele verschiedene Komponenten, die heute überall in den verschiedenen Betriebssystemen, in verschiedenen Softwaresystemen verwendet werden, neu schreiben in sicheren Programmiersprachen, so dass sie auditiert werden können und auch dafür bezahlen. Wir werden da nicht umhin kommen, die Wirtschaft wird es von alleine nicht machen oder wenn, dann nur die Großkonzerne wie Google und Microsoft, wo wir dann hinterher nicht wirklich einen Einblick darin haben, was da passiert.

Die Einrichtung von Strukturen für eine dynamische Zertifizierung von IT-Sicherheit, die ich vorhin schon erwähnt habe, ist eine Sache, die man sehr kurzfristig angehen kann. Wir haben im Bereich KRITIS zum Teil positive Erfahrungen mit diesen branchenspezifischen Sicherheitsanforderungen und dieses Prinzip auszudehnen und zu sagen, wir versuchen möglichst mit allen Teilen der Industrie ins Gespräch zu kommen und z. B. beim BSI oder auch bei einer unabhängigen Institution eine entsprechende Struktur zu schaffen, wo sich diese Branchen drauf festlegen, was der Minimalstandard an IT-Sicherheit ist, den sie fahren, ist eine Sache, die man relativ schnell in die Wege leiten kann. Da gibt es keine großen Hürden.

Ein auch kurzfristig machbares Projekt wäre das Labeling von IT-Produkten. In dem Augenblick, wo da Internet drin ist, muss da eigentlich ein Label drauf, wie bei einer Waschmaschine, wo steht, Update gibt es bis in drei Jahren, und zwar alle drei Monate, und dann kann ich mich als Verbraucher tatsächlich darauf verlassen, dass eine Marktdynamik zugunsten von IT-Sicherheit entsteht. Wir haben das Problem, dass bei der Router TR, das war der erste Versuch in diese Richtung zu gehen, es natürlich einen massiven Widerstand aus der Industrie gab. Das hat niemanden aus der Branche groß überrascht, weil, was das plötzlich passiert ist, dass die Hersteller die Lebenszykluskosten eines Produktes plötzlich anfangen müssen zu kalkulieren, die müssen plötzlich sagen, okay, ich muss diese Kiste, die ich gerade für 100 Euro im Mediamarkt verkauft habe, auch noch die nächsten drei Jahre warten, und plötzlich kostet die 150 Euro. Aber alles andere ist unehrlich, alles andere ist einfach nur Augenwischerei. So ein Label verpflichtend zu machen, einfach nur die Information, wie lange gibt es Updates und wie oft kommen die, ist eine einfache Sache, wo eigentlich auch niemand wirklich ernsthaft gegen argumentieren kann. Deswegen denke ich, das ist ein kurzfristig umsetzbares Projekt. Das ist der Einstieg in eine Produkthaftungsdiskussion und die muss man erstmal anfangen. Die wird natürlich die ganze Industrie in eine Schockstarre versetzen, weil sie bisher nicht gewohnt ist über Haftung nachzudenken. Aber wir brauchen tatsächlich Haftungsregelungen in der Zukunft.

Auch kurzfristig machbar ist tatsächlich die Vertrauenswürdigkeit des BSI zu erhalten oder wieder herzustellen, indem man es nicht mit Aufgaben betraut, die Dienstleistungen für die Strafverfolger sind. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Schönbohm, bitte.

S SV Präs **Arne Schönbohm** (BSI, Bonn): Vielen Dank, Frau Vorsitzende. Ich hatte zwei Fragen, einmal Herr Hartmann zum Thema Frage Hackback und Notwendigkeit. Das BSI ist zuständig für den Schutz der Netze – ich werde gleich Herrn Höferlin noch sagen, wo ich das in meiner Schnellrecherche genau gefunden habe – ich glaube in der Tat, dass es notwendig ist, dass wir dort etwas haben, allein dass man die Möglichkeit hat, wer was wie im Einzelnen macht. Ich denke, da gibt es zurzeit eine Vielzahl von verschiedensten Diskussionen in den entsprechenden Gremien, die man dann auch entsprechend nicht öffentlich, sondern geheim führt. Wenn es dann soweit ist, wird man – glaube ich – auch mit den Punkten in das Parlament oder in die entsprechenden Gremien gehen, aber das ist für uns natürlich als BSI, als nachgeordnete Behörde, dort nicht so sehr das Thema. Aber in der Tat, ich glaube, dass so etwas notwendig ist, allein dass man die Möglichkeit hat. Herr Höferlin, Sie hatten die Frage gestellt, gesetzlicher Auftrag zum Thema der Cyberabwehr, das ist für mich, habe ich jetzt schnell recherchiert, habe ich gefunden in zwei Punkten, Paragraph 1 BSI-Gesetz: Der Bund unterhält ein Bundesamt für Sicherheit und Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene, dann die Begriffsbestimmung danach sagt, die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen. Von entscheidender Bedeutung ist dann der Paragraph 3 Absatz 1 Satz 1, dort heißt es: „Das Bundesamt fördert die Sicherheit in der Informationstechnik.“ In Ordnung und dann: „Hierzu nimmt es folgende Aufgaben wahr.“ Das ist dann der erste Satz: „Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes“ und daraus leiten wir natürlich ab, dass das der gesetzliche Auftrag für die Cyberabwehr, für die Cybersicherheit der der Bundesverwaltung und der Bundesregierung ist.

Abg. **Manuel Höferlin** (FDP): Was verstehen Sie darunter?

SV Präs **Arne Schönbohm** (BSI, Bonn): Ich verstehe immer das, was im Gesetz dort steht, ich bin kein Jurist, aber dort ist – das kann ich gerne vorlesen – die Begriffsbestimmung vom Paragraphen 2, das ist das, was wir darunter auch verstehen.

Vors. **Andrea Lindholz** (CDU/CSU): Abschließend in der Runde, Frau Dr. Sowa.

SVe **Dr. Aleksandra Sowa** (Bonn): Vielen Dank, Frau Domscheit-Berg, für die Frage nach der Schwachstelle Mensch und nach der digitalen Gewalt. Zuerst haben wir die Möglichkeit, auch die Menschen, die sehr jung sind, auf die Nutzung neuer Medien - oder überhaupt an die Konfrontation mit dem Internet - vorzubereiten, indem wir in die Schulen bestimmte Arten von Ausbildung reinbringen. Die Gesellschaft für Informatik hat z.B. ein Curriculum für ein Schulfach Informatik erstellt und das ist unbedingt von anderen Konzepten wie Coding oder Programmieren in den Schulen zu unterscheiden. Denn Informatik als Fach umfasst nicht nur technische Informationen oder technische Kenntnisse, sondern auch gesellschaftliche, philosophische, Aspekte von künstlicher Intelligenz etc., die den Umgang mit den Medien und mit der Technologie ermöglichen. Das ist jetzt besonders wichtig, weil wir uns immer weiter von der Technologie entfernen. Wir können die meisten Geräte, die wir heute nutzen, nicht mal auseinanderbauen, wir kennen ihre Funktionsweise nicht, wir können den Akku in dem Smartphone nicht wechseln und es ist möglich, uns dieses Wissen, diese Gewalt über die Technologie, wieder zurückzuholen, indem wir das Knowhow den Menschen wieder zurückgeben.

Ein Konzept, mit dem man sich auch sehr gut anfreunden kann, ist die Medienkompetenz. Medienkompetenz umfasst nicht nur die informationstechnischen Aspekte, sondern betrachtet auch den Umgang mit den Medien und insbesondere kritischen Umgang mit den Medien: es sollen nicht nur rationales, vernünftiges Denken, aber auch Skeptizismus vermittelt werden. Es ist interessanterweise nicht nur mit dem Fokus politischer Inhalte wichtig, über dem es gerade verstärkt diskutiert wird, es ist ebenfalls wichtig, wenn wir über Produktinformationen sprechen, über Werbung - auch da ist eine skeptische Einstellung oder eine kritische

Validierung sehr, sehr wichtig - gerade was die Sicherheit betrifft.

Neben diesen Konzepten haben wir auch noch die Möglichkeit auf Quick-Wins, wenn wir auf technische Lösungen zurückzugreifen: Anlässlich der Diskussion über das Thema Stalking und individuelle, private Spionage, hat sich kurzfristig das Sicherheitsunternehmen Kaspersky dazu entschlossen, die eigene Antivirus-Software aufzurüsten und um neue sogenannte „Red Flags“ zu ergänzen. Das heißt, es wird auch Alert möglich und es wird jetzt auch als Warnung/Warning ausgewiesen, wenn Spionagesoftware oder Stalking-Software erkannt wird. Was kann dabei die Politik machen? Sie muss sich ganz klar positionieren, ob sie selbst solche Mittel verwenden möchte. Ich spreche hier von Mitteln wie verdeckte Spionage oder Bundestrojaner – das ist, glaube ich, hier das Stichwort. Denn so eine Kaspersky-Anti-Virus-App wird dann vermutlich auch den Staatstrojaner erkennen - und dann wollen wir auch nicht eine Situation erleben, in der die Bundesregierung die Nutzung von Kaspersky-Software verbietet, weil sie ihre eigene Software nicht zu Spionagezwecken einsetzen kann.

Eine andere schnell umsetzbare Möglichkeit, an der sich auch der Staat beteiligen müsste - wenn man es denn so möchte - ist im Kontext von z.B. Netz DG. Wo Hate Speech oder Hasssprache bekämpft werden sollte, wurden z.B. Online-Games ausgeschlossen. Online-Games, besonders die Chatfunktion (Chats) darin, geben viele Möglichkeiten für Angriffe auf junge Menschen, aber auch im Bereich Terrorismus. Chats in Online-Games wurden – es ist mir noch nicht ganz klar warum – aus dem Wirkungsgrad des Netz DG ausgeschlossen. Hier wäre die Möglichkeit z.B. auch – das ist eine Idee vom Berliner Kriminologen Thomas Rüdiger – dass man direkt in dem Spiel eine Polizeidienststelle einrichten kann – da ist die Hürde bei einem Menschen sich direkt im Rahmen eines Spiels zu bewegen und dort einen Stalker oder einen Belästiger zu melden, viel, viel niedriger, als in eine Offline-Welt auszutreten und zur Polizei zu gehen, um eine Anzeige zu erstatten.

Das sind Konzepte, die aktuell schnell umsetzbar sind und diskutiert werden. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Bevor wir in die zweite Runde kommen, habe ich noch einen Hinweis für das Protokoll zu machen. Ich habe in der letzten Obleuterunde für alle Kolleginnen und Kollegen des Ausschusses eine Übersicht über alle hier beschlossenen und durchgeführten und noch durchzuführenden Anhörungen verteilt. Ich weiß nicht, ob sie in allen Büros eingegangen sind, ich empfehle aber mal den Blick in diese Liste.

Wir haben den Antrag zur Anhörung des Antrages der Grünen am 12. Dezember beschlossen. Wir haben die beiden anderen Anträge, eine Anhörung durchzuführen, am 15. März dieses Jahres erhalten, am 20. März beschlossen. Wir führen am 8. April die Anhörung durch. Wir haben seit Beginn des Jahres acht Sitzungswochen gehabt und von diesen acht Sitzungswochen in sechs Sichtungswochen Anhörungen durchgeführt. Wir haben seit Beginn dieses Ausschusses 17 Anhörungen beschlossen und wir haben nur noch eine einzige Anhörung offen, die wir dann in der nächsten Maiwoche absolvieren werden.

Dann kommen wir jetzt in die nächste Fragerunde und mit Blick auf die Uhr – wir haben noch 45 Minuten – können wir auch nochmal so verfahren wie in der ersten Fragerunde. Dann, bitte, Herr Bernstiel.

Abg. **Christoph Bernstiel** (CDU/CSU): Jetzt hätte ich gerne eine Frage an Herrn Schönbohm, und zwar haben wir jetzt schon oft über das IT-Sicherheitskennzeichen diskutiert, was vorgesehen ist im 2. IT-Sicherheitsgesetz und die Wirksamkeit der Freiwilligkeit und der Verbindlichkeit. Mich würde interessieren, Herr Schönbohm, ob Sie nochmal ausführen könnten, was konkret mit diesem IT-Sicherheitskennzeichen verbunden ist, wie es funktionieren soll und auch nochmal zu dieser Frage, die hier immer wieder diskutiert wurde, der angeblichen Unabhängigkeit des BSI. Dieses Misstrauen, was hier teilweise dem BSI gegenüber geäußert wird, das teilen wir natürlich nicht. Vielleicht können Sie da auch nochmal sagen, wie Sie sich das nachher in der Praxis vorstellen, dass Sie nochmal ein bisschen Licht ins Dunkel bringen und in dem Zusammenhang auch nochmal darauf eingehen, auf diese Dynamik, die gefordert wurde, dass gesagt wurde, es gibt jetzt nicht ein starres Zertifikat, das ist dann das Produkt, einmal zertifiziert und dann bleibt das so. Meines Wissens ist es so, dass dann eine regelmäßige Prüfung stattfinden soll. Da

würde ich mich freuen, wenn Sie dazu nochmal etwas sagen könnten. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Haug.

Abg. **Jochen Haug** (AfD): Dankeschön. Ich habe auch eine Frage an Herrn Schönbohm und zwar einfach nochmal eine konkretisierende Frage. Sie schreiben in Ihrer Stellungnahme, die Anzahl und Qualität der Cyberangriffe auf staatliche und zivile Ziele nimmt eklatant zu und berichten dann von ca. 390.000 neuen Varianten von Schadprogrammen pro Tag. Da wäre meine grundsätzliche Frage, wo denn der Schwerpunkt der Angriffe liegt, das heißt, so etwa aufgeschlüsselt, was die Ziele und die Angreifer sind. Dankeschön.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Haug, vielen Dank. Dann kommen wir zur SPD, Frau Esken.

Abg. **Saskia Esken** (SPD): Vielen Dank, Frau Vorsitzende. Ich will zunächst kommentieren, dass ich sehr froh bin, dass ich von verschiedener Seite gehört habe, dass die IT-Sicherheit als staatliche Aufgabe verstanden werden sollte. Diese Ansicht teile ich, deshalb sind widersprüchliche Vorgehensweisen oder widersprüchliche Haltungen des Staates da auch relativ problematisch und auch wir plädieren für eine strikt defensive Ausrichtung der Cybersicherheitsstrategie der Bundesregierung. Sicherheit, sichere Vorgehensweisen, wie beispielsweise Verschlüsselung oder Anonymität dürfen eben nicht kriminalisiert werden.

Ich habe eine Frage an Herrn Herpig. Herr Herpig, wie beurteilen Sie die Vorschläge und neuen Kompetenz- und Eingriffsbefugnisse im Entwurf des BMI in Bezug auf BfV und BND auf der einen und auf der anderen Seite im IT-Sicherheitsgesetz 2.0 in Bezug auf das Trennungsgebot zwischen polizeilicher und nachrichtendienstlicher Tätigkeit sowie mit Blick auf die immer wieder angemahnte und nie wirklich dargelegte Gesamtschar der Überwachung? Sie hatten auch angeregt, die müsste dann tatsächlich mal erstellt werden. Wer hätte denn möglicherweise den Auftrag, diese zu erstellen?

Und meine andere Frage geht an Herrn Könen. Herr Könen, Herr Herpig hat gesagt, Deutschland sei bei der IT-Sicherheit strategieunfähig, das ist ja eine herbe Aussage …

Vors. **Andrea Lindholz** (CDU/CSU): Herr Könen antwortet hier heute nicht, wir haben eine Sachverständigenanhörung und ich glaube, dass es Kollegen gibt, die auch Herrn Könen heute nicht als Sachverständigen betrachten, insofern bitte ich, Ihre Fragen auch an den Sachverständigen zu richten.

Abg. **Sebastian Hartmann** (SPD): Aber grundsätzlich schon.

Abg. **Saskia Esken** (SPD): Aber grundsätzlich ist die Bundesregierung anwesend, um Fragen beantworten zu können. Und sachverständig ist er auf jeden Fall, das würde ich auch unbedingt unterstreichen.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Also, sachverständig ist er auf jeden Fall.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Könen ist nicht hier, um Fragen zu beantworten. Das können wir in einer Ausschusssitzung unter einem eigenen Tagesordnungspunkt machen, aber wir erweitern jetzt hier nicht die Anhörung. Die zweite Frage geht an welchen Sachverständigen?

Abg. **Saskia Esken** (SPD): Dann geht die zweite Frage auch an den Herrn Herpig. Herr Herpig, Sie hatten ausgeführt, Deutschland sei bei der IT-Sicherheit strategieunfähig. Sie haben uns diese wunderbare Übersicht der Akteure gefertigt, die bei weitem nicht vollständig ist, wenn auch sehr hilfreich. Wer hat denn nun im Sinne dieser Vielfalt der Akteure in der fehlenden Strategien den Hut auf? Sie hatten die Frage gestellt, was macht der Cybersicherheitsrat Deutschland, da meinten Sie sicher nicht den e.V., von dem anderen habe ich tatsächlich auch lange nichts mehr gehört und worin zeigt sich die Arbeit des Cyberabwehrzentrums? Ist da von dem Upgrade auf das Cyberabwehrzentrum Plus tatsächlich zu erwarten, dass die Zusammenarbeit besser klappt oder ist nicht vielmehr das BSI die eine zentrale Cybersicherheitsbehörde und benötigt – wie andere auch schon ausgeführt haben – für diese gesamtgesellschaftlich relevante Arbeit die Unabhängigkeit?

Vors. **Andrea Lindholz** (CDU/CSU): Dann blicke ich jetzt zu Herrn Höferlin.

Abg. **Manuel Höferlin** (FDP): Danke, Frau Vorsitzende, dass Sie zu mir blicken. Wir hatten es auch schon in Anhörungen, dass die Bundesregierung sich geäußert hat, gegen den Protest der Kollegen hier. Vielleicht sollten wir eine einheitliche Regelung finden und nicht nur dann, wenn es passend ist, die Bundesregierung in Anhörungen etwas sagen lassen.

Ich habe auch nochmal eine Frage an Herrn Dr. Herpig, und zwar im Anschluss an das, was Frau Esken gerade schon gesagt hat. Vielleicht nochmal auf den Föderalismus in unserem Land und die Frage, wer hat welche Befugnisse im Bereich Prävention. Also, soll das nationale Cyberabwehrzentrum – wie soll das da geregelt sein aus Ihrer Sicht? Wo gibt es die Herausforderungen, gerade bei einer engeren Zusammenarbeit zwischen Bund und Ländern im Bereich IT-Sicherheit oder dann auch im Bereich der Abwehrmaßnahmen dort? Vielleicht können Sie dazu noch ein bisschen ausholen?

Und die zweite Frage an Herrn Rieger, sie war gerade schon angeklungen, die Frage der Erkennung von Sicherheitslücken in der Sicherheitsforschung. Ich hatte bisher immer den Eindruck, es gäbe viele gute Argumente, die bestehende Gesetzeslage zu Hackerparagraphen etc. endlich mal so zu machen, dass Sicherheitsforschung ordentlich arbeiten kann. Jetzt ist im IT-Sicherheitsgesetz-2.0-Entwurf im Prinzip eine Verschärfung drin. Was bedeutet das genau für die Sicherheitsforschung in Deutschland, wenn wir Werkzeuge, um Sicherheitsforschung durchzuführen, um Sicherheit herzustellen, um die Möglichkeit zu schaffen, Lücken zu entdecken, allein schon die Werkzeuge oder die Nutzung der Werkzeuge unter Strafe stellen? Und was sind Alternativen, die besser funktionieren, vielleicht auch für White Hacker? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Frau Domscheit-Berg, bitte.

Abg. **Anke Domscheit-Berg** (DIE LINKE): Ich habe zunächst eine Frage an Frau Sowa. Ein sehr wichtiges Thema – Unterthema zu dem heutigen Thema – ist das ganze Feld der Kryptographie. Uns wurde von der Bundesregierung in ihrer Cybersicherheitsstrategie 2016 auch versprochen, dass das ein eigenes und natürlich wahnsinnig wichtiges Handlungsfeld sein soll. Ich wüsste jetzt gerne von Ihnen: Wie bewerten Sie die Fortschritte, die zu diesem Thema seitdem passiert sind, insbesondere auch, was benachbarte Politikfelder angeht? Also, z.B. die Entwicklung digitaler Verwaltung. Was macht man da, kann man mit Behörden verschlüsselt kommunizieren, tut man da genug? Und was muss man eigentlich machen, um kryptographische Verfahren besser zu etablieren und zu fördern?

Meine zweite Frage geht an Herrn Rieger und hat zu tun mit einer Sache, die Sie gesagt haben, nämlich dass in der IT-Sicherheit Verteidigung und Angriff nicht miteinander verbunden werden sollten. Das findet natürlich in gewisser Weise tatsächlich aber statt. Wir haben die ZITiS als Hackeragentur auf dem Gelände der Bundeswehr, wir haben eine Cyberagentur, die vom Bundesverteidigungsministerium finanziert wird, im Übrigen als GmbH gegründet und damit einer parlamentarischen Kontrolle vollständig entzogen. Wir haben selbst einen Präsidenten des BSI, Herrn Schönbohm, der auch hier sitzt, der von der Sinnhaftigkeit aktiver Cyberabwehr spricht. Wir haben Stellenausschreibungen, wo Stellen bei Hackeragenturen – staatliche Hackeragenturen wie ZITiS – besser besoldet sind als die z.B. beim BSI, selbst wenn sie vergleichbar sind. Wie bewerten Sie die Konsequenzen in Hinsicht auf sowieso knappe Ressourcen? Was heißt das für die Verteidigung, wenn die besser Bezahlten im Hackerbereich des Staates sind? Welche Risiken ergeben sich für unser aller Sicherheit, auch in Bezug auf eine mangelhafte Möglichkeit der Attribuierung und potentielle Eskalation?

Vors. **Andrea Lindholz** (CDU/CSU): Und den Schluss in der Runde macht Herr von Notz.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Frau Vorsitzende, vielen Dank. Wir haben eben – glaube ich – ein kleines Missverständnis gehabt. Ich bezog mich mit dem einen Jahr auf das Alter unseres Antrags, der ist gerade ein Jahr alt geworden. Der Antrag auf diese Anhörung, der ist erst ein paar Monate alt, also noch relativ frisch. Ich habe noch zwei Fragen. Die erste geht an Herrn Rieger, bezieht sich so ein bisschen darauf, was kann man machen, was relativ schlicht ist. Die Bundesregierung hat – ich weiß gar nicht, ob das der alte GroKo-Vertrag ist oder der neue – diese lustige kleine Phrase da drin stehen oder das BMI kommuniziert das zumindest immer noch so: Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung. Das kommt auch tatsächlich ein bisschen zum Ausdruck. Bei DE-Mail hat man

nicht eine Ende-zu-Ende-Verschlüsselung gemacht, hätte was werden können mit DE-Mail, hat man nicht gemacht, ist jetzt nichts geworden. Und deswegen: Wo/wie könnte man das denn klar gesetzlich entscheiden, dass man hier nicht mit viel Geld ZITiS füttert, dass man mit Quantencomputern Verschlüsselungen hackt, sondern dass Verschlüsselung tatsächlich etwas gilt?

Das andere geht an Herrn Schönbohm, die Frage. Sie haben eben sehr wortreich Ihre Behörde beworben, jetzt stehen Sie aber doch im Weisungsstrang des BMI. Deswegen, ich frage Sie jetzt mal zugespitzt, Herr Präsident: Ihren Sprechzettel hier für die Anhörung, da guckt aber das BMI nicht vorher drüber, was Sie hier sagen? Weil wir so fein unterscheiden, also Sie wissen, ich kämpfe sehr hart für Ihre Unabhängigkeit, aber es würde natürlich helfen, wenn Sie als Präsident auch mal Stellung beziehen, denn das wäre tatsächlich ein wichtiger Baustein. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Die letzte Frage war, ob das BMI auf seinen Sprechzettel schaut, habe ich das richtig verstanden? Dann fangen wir jetzt mit der Beantwortung an in umgekehrter Reihenfolge, beginnend dieses Mal mit Frau Dr. Sowa, bitte.

SVe **Dr. Aleksandra Sowa** (Bonn): Vielen Dank, vielen Dank auch Frau Domscheit-Berg für die Frage zur Kryptographie. Es ist hauptsächlich im wissenschaftlichen Bereich ein Fortschritt zu erkennen, weniger im Nutzungsbereich. Gerade läuft auf der europäischen Ebene ein mehrjähriges Programm zur Postquantum-Kryptographie, unter anderem unter der Führung einer deutschen Wissenschaftlerin, Prof. Dr. Tanja Lange, wo nach Verfahren, nach Methoden recherchiert wird, die – auch wenn wir in der Zukunft, vielleicht in der nahen Zukunft, einen Quantencomputer, einen sehr schnellen Computer zur Verfügung haben – dennoch sichere Verschlüsselungsverfahren, sichere Kryptographie gewährleisten können.

Unabhängig davon, was die Europäische Union in den letzten Jahren gefördert hat, hat das Forschungsministerium ebenfalls – so glaube ich – Anfang diesen Jahres ein Forschungsprojekt zum Thema Postquantum-Kryptographie aufgesetzt. Das Problem ist allerdings, dass in diesem Programm Forscher – auch deutsche Forscher, die nicht in Deutschland forschen, und das sind viele –nicht an den Programmen teilnehmen dürfen. Also, z.B. Frau Prof. Dr. Tanja Lange wird mit Auslauf von ihrem EU-Programm, in Deutschland an dem BMBF-Forschungsprogramm zu Postquantum-Kryptographie vermutlich nicht mitwirken können.

Was die Nutzung von Kryptographie wiederum betrifft, so haben wir das Spannungsfeld– wie Herr von Notz sagte –: mehr Sicherheit durch Verschlüsselung oder mehr Unsicherheit durch Verschlüsselung. Auf der einen Seite ist der Bürger, der seine Anonymität wahren, seine Kommunikation vertraulich/anonym behandeln möchte, auf der anderen der Staat, der durch Auswertung von Kommunikation nach bestimmten Mustern suchen und so eventuell kriminelle oder terroristische Handlungen aufdecken möchte. Und das sind – glaube ich – zwei konträre Trends, die dazu führen, dass es keinen richtigen Fortschritt auf diesem Gebiet gibt. Wir haben immer noch die alten Methoden, die in den neunziger Jahren entwickelt worden sind - ich habe schon Pretty Good Privacy (PGP) erwähnt, als eine der wenigen weitverbreiteten Verschlüsselungsmethoden für E-Mail-Kommunikation. Und wenn Lösungen für Verschlüsselung gefunden werden, dann dienen sie meist nur einer kleinen Organisation. Das heißt, es ist möglich, verschlüsselt innerhalb einer Behörde, innerhalb von einem Unternehmen, zu kommunizieren. Wenn es aber dazu kommt, mit den Bürgern oder mit den Kunden extern verschlüsselt zu kommunizieren - auch z.B. zwischen den Partnern oder wenn die Unternehmen mit externen Kanzleien - sind sie nicht in der Lage, ihre Kommunikation kryptographisch zu sichern, zu verschlüsseln. Und dafür ist vermutlich, außer in der Forschung, tatsächlich mehr Unterstützung für allgemeine Lösungen notwendig, damit sich – vielleicht auch im Rahmen von Privat Public Partnership –, Lösungen wie PGP, die allgemein zugänglich sind, auch über die Grenzen hinweg, etablieren können. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Dann kommen wir nunmehr zu Herrn Schönbohm.

SV Präs **Arne Schönbohm** (BSI, Bonn): Vielen Dank, Herr Vorsitzender. Abgeordneter Bernstiel hat gefragt nach dem Thema IT-Sicherheitskennzeichnung, ob ich das nochmal ein bisschen erklären kann. Es geht hier darum, dass wir ein IT-Sicherheitskennzeichen, bestehend aus einer Herstellererklärung – das ist eines der Themen auch Herr

Rieger, wobei wir auch im Beisein mit dem Chaos Computer Club damals intensiv gesprochen haben, gerungen haben auch, um das einzuführen dementsprechend für die Router, aufgrund des Vorfalls der Deutschen Telekom und das wird ergänzt um eine sogenannte dynamische BSI-Sicherheitsinformation per QR-Code. So, dass man später erkennen kann, wird denn mein Produkt dementsprechend auch geschützt. Ich teile dort die Einschätzung von Herrn Rieger absolut. Es kann nicht angehen, dass Sie eine Waschmaschine oder andere Produkte kaufen und sie bekommen eine sehr detaillierte Information, wie hoch der Stromverbrauch ist und andere Dinge. Aber wie sicher ist das Thema der Informationssicherheit und wie lange werden dann dort auch die Software und andere Punkte gewartet, Updates zur Verfügung gestellt, ist nicht ersichtlich. Und genau dieser Lücke soll eben das das freiwillige IT-Sicherheitskennzeichen entgegen wirken. Das soll eben nicht starr sein, sondern soll auch flexibel überprüft werden. Während Abgeordneter Bernstiel noch nach dem Thema Unabhängigkeit des BSI gefragt hat. Da werde ich gleich darauf antworten im Zusammenhang der Frage von Herrn von Notz – ich soll Stellung beziehen, habe ich verstanden, was ja schon fast ein militärischer Ausdruck ist – um dann das da zu beantworten.

Herr Haug hatte die Frage gestellt: Schwerpunkte der Angriffe nach Zielen und Angriffe letzten Endes. Dort war es – fürs Protokoll –

[Undeutlicher Zwischenruf]

ansonsten dort ist es so. Sie müssen sich vorstellen, die organisierte Kriminalität verdient seit 2009, so eine Studie, mehr Geld mit Cybercrime als mit Drogen. Das heißt, der überwiegende Teil ist organisierte Kriminalität, Hacktivisten, Entschuldigung Idioten usw. alle Möglichen, die man dort findet, ohne dass es despektierlich sein soll. Dann haben Sie eine ganz geringe Anzahl letzten Endes von Angriffen nachrichtendienstlicher Klassifizierung und Qualität. Sie haben gefragt, was heißt das im Bereich der Quantität und Qualität. Dadurch, dass wir jetzt erst anfangen uns zu vernetzen, nehmen natürlich auch die Angriffsmöglichkeiten zu. Die Qualität der IT-Produkte nimmt nicht mit gleichem Maßstab zu. Dadurch gibt es mehr Angriffsmöglichkeiten, die auch wirklich teilweise brutal ausgeführt werden und jüngste Fälle gingen auch gerade wieder durch die Presse. Quantität, weil wir sehen Schwachstellen nicht nur in der Software, sondern eben mittlerweile auch in der Hardware. Das führt zu einer neuen qualitativen und quantitativen Art der Bedrohung, wie wir sie sehen, im Bereich der Informationssicherheit.

Schwerpunkte der Angriffe nach Zielen und Angreifern: Es wird all das angegriffen, womit man relativ einfach viel Geld verdienen kann. Wo es viele Daten gibt. Aber es werden auch die Lieferanten des Hauptziels letzten Endes angegriffen, um sich frühzeitig in Systeme einzubetten. Wer steckt dahinter? Das ist – glaube ich – gerade deutlich geworden. Ich glaube, eine Attribution nach bestimmten Ländern macht nur begrenzt Sinn und dafür sind wir auch nicht zuständig, sondern das ist eines der Themen, wofür das Bundesamt für Verfassungsschutz und der Bundesnachrichtendienst zuständig sind.

Herr von Notz hat mich gebeten, Stellung zu beziehen zum Thema Unabhängigkeit des BSI. Ich fühle mich eigentlich ganz wohl – und ich beziehe gerne Stellung für Sie – aber wir sind eine fachlich, technisch, wissenschaftliche Behörde. Das ist so, wie es auch im BSI-Gesetz drinsteht. Jetzt ist es so, natürlich arbeiten wir sehr partnerschaftlich und eng auch mit den anderen Bundesoberbehörden zusammen. Ja und ich saß auch gerade zusammen bei „Deutschland sicher im Netz“ und neben mir saß der BKA-Präsident Münch und wir haben darüber gesprochen, wie kann man das Thema Informationssicherheit voranbringen. So wie er auch in der realen Welt den Einbruchschutz voranbringt. Und das ist ein Thema, wo wir uns relativ wohl und gut fühlen. Die Frage ist immer die und das ist ja das, was bei Ihnen dahintersteht. Es gibt immer so ein Gefühl, auch teilweise bei den Sachverständigen, nach dem Motto, dort werden irgendwelche Schwachstellen an irgendwen weitergegeben. Jetzt bin seit gut drei Jahren in diesem Amt und dieser Funktion. Ich bin noch nie irgendwo gehindert worden dafür zu sorgen, eine Schwachstelle schnell zu schließen. Die Herausforderung ist eher …

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Das wäre ja auch mal eine Meldung wert.

SV Präs **Arne Schönbohm** (BSI, Bonn): Ja, ja klar. Ich weiß. Ist ja öffentlich. Alles klar. Aber die Herausforderung, die wir haben, ist doch eher, dass

wenn wir auch darauf die Hard- und Software-Hersteller hinweisen, die Schwachstellen eben nicht so schnell, wie es eigentlich sein müsste, teilweise geschlossen werden. Das ist doch eher die Herausforderung, die wir haben. Und ich glaube, wir sollten uns hier auf die wesentlichen Themen konzentrieren und ich fühle mich in der jetzigen Phase – so wie wir gerade alle zusammenarbeiten – sehr, sehr wohl.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Aber wenn Sie die Auffassung hätten, Hackbacks sind des Teufels, können Sie das sagen als Präsident? Im Weisungsstrang Fach- und Rechtsaufsicht des BMI. Können Sie das sagen?

SV Präs **Arne Schönbohm** (BSI, Bonn): Natürlich kann ich das sagen. Die Frage ist, wie oft ich das sagen kann. Aber ich kann es schon sagen.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Rieger.

SV **Frank Rieger** (CCC Berlin e. V.): Die Frage von Herrn Höferlin zum Thema Hacker-Paragraphenverschärfung und die Auswirkungen auf die Sicherheitsforschung. Schon der erste Hacker-Tool-Paragraph hat verheerende Auswirkung gehabt. Wir waren an einem Versuch beteiligt, diese Paragraphensammlung vor dem Bundesverfassungsgericht eingrenzen zu lassen. Wenn man diese Paragraphen anfasst, lohnt es sehr, die Klageabweisungsbegründung zu lesen, weil die bezieht sich im Wesentlichen darauf, dass die Begründung der damals beschlossenen Paragraphen klar sagt, dass es sich um mehr oder minder Ausnahmetatbestände handelt. Also um welche, die benutzt werden, wenn zusätzlich zu anderen ohnehin schon vorgekommenen Straftaten noch Hackertools benutzt wurden. Was wir jetzt gerade in diesem Referentenentwurf beim IT-Sicherheitsgesetz sehen, geht darüber hinaus. Das heißt, die Wahrscheinlichkeit ist relativ groß, dass es in Karlsruhe – und wir werden es auf jeden Fall angreifen, da können Sie sicher sein – dass es in Karlsruhe möglicherweise nicht durchgehen wird. Das heißt, da sollte man – glaube ich – nochmal eine gründliche verfassungsmäßige Abwägung treffen. Die psychologischen Auswirkungen auf die Branche sind wenig überraschend ziemlich verheerend. Wir haben – wie gesagt – schon beim ersten Paragraphen ein klares Empfinden bekommen von dem Sicherheitsvorschlag, dass sie gesagt haben, „ja Gott, also mit einem Staat, der mich bestrafen will, weil ich irgendwie einen Hackingtool auf meiner Platte habe, will ich nichts zu tun haben. Warum sollte ich dem irgendwie helfen? Warum soll ich dem irgendwie irgendeinen Gefallen tun? Dann gehe ich doch lieber los und verkaufe meine Exploits. Weil strafbar ist es ja dann ohnehin.“ So und diesen Eindruck sollte man tunlichst nicht noch verschärfen, sondern im Gegenteil eher versuchen, die Hand auszustrecken und zu sagen, okay, wir müssen das Problem gemeinschaftlich lösen. Deswegen kann ich da nur dringlich von abraten, diesen, genau wie bei diesen Versuchen da jetzt Darknet-Paragraphen ins IT-Sicherheitsgesetz reinzuschreiben beziehungsweise dieser Entwurf vom Bundesrat. Auch der führt genau zu so einem antagonistischen Gefühl bei Leuten, die eigentlich guten Willens sind. Die eigentlich eher sagen, „okay, wir können dieses Problem auch gerne zusammen lösen.“

Zur Frage von Frau Domscheit-Berg. Auseinanderhalten von Defense und Offense, was insbesondere die Behörden angeht. Herr Herpig hat es schon sehr schön und sehr deutlich gesagt. Wir haben momentan ein wildes Verantwortungsnebeneinander, um es freundlich zu formulieren, was auch mit einer großen Konkurrenz um Personal einhergeht. Das heißt also, wir haben viele Behörden, die um denselben relativ kleinen potentiellen Mitarbeiterpool konkurrieren. Menschen, die sowohl was von der Technologie verstehen als auch Willens sind, für den Staat zu arbeiten. Das ist in der Branche nicht so häufig. Und wenn, dann geht man wahrscheinlich eher zum BSI, weil man da noch eher sich sagen kann, man tut hier was Gutes. Wir haben diese Situation, dass verschiedenste Behörden, die unklar positioniert sind, wie jetzt z. B. diese neue Agentur, wo einerseits die öffentliche Wahrnehmung und auch die Aufgabenbeschreibung sagt, okay, wir entwickeln hier Angriffswerkzeuge für die Sicherheitsbehörden, was im nächsten Atemzug wieder umfänglich bestritten wird. Wissen Sie, wenn Sie einen Bewerber haben, der sich denkt, okay, ich kann mal für eine Behörde arbeiten, ich verstehe was davon, der wird nicht zu einer Behörde gehen wo ihm nicht klar ist, was da eigentlich passiert und welche Aufgabenstellungen ihm da gestellt werden und in welche Gewissenskonflikte er da kommt. Und wir sollten nicht übersehen, dass wir in der Branche eine Menge Leute haben, die durchaus ein Gewissen haben und die lieber was machen wollen, wo sie ihre Lebenszeit

nicht mit der Entwicklung von Angriffswerkzeugen für den Staat verbringen. Das heißt, dieses Nebeneinander, diese Unklarheit der Aufgabenteilung und die Durchmischung von Kompetenzen, die sich gerade abzeichnet, sind auch verheerend für die Personalgewinnung. Das ist vollkommen klar.

Zur Frage Sicherheit trotz Verschlüsselung von Herrn von Notz: Wir haben die Situation in Deutschland, dass die momentane deutsche Kryptopolitik immer noch auf den Eckpunkten der deutschen Kryptopolitik aus den 90ern beruht. Das heißt, ein klares Bekenntnis zur Verschlüsselung, was gelegentlich auch wiederholt wird, was auch durch das Urteil des Bundesverfassungsgerichts für digitale Selbstverteidigung gestärkt ist. Das heißt, eigentlich haben wir in Deutschland eine Position, die sagt: Verschlüsselung, Hintertüren einbauen, ist keine Politik dieses Landes und das heißen wir auch ausdrücklich gut, weil Verschlüsslung eines der wenigen Mittel ist, die wir haben, um uns tatsächlich gegen alle möglichen Formen von Cyberangriffen wirksam zu schützen im Sinne von den Datenverlust zu verhindern und Spionage zu verhindern oder zumindest sehr viel schwerer zu machen. Es würde – glaube ich – der Branche, dem Land und auch der Wahrnehmung sehr gut tun, wenn diese Position nochmal ausdrücklich bestärkt und bekräftigt werden würde von Seiten der Politik, von Seiten des Parlaments, wenn man sagen würde, okay, es handelt sich eben nicht nur um Eckpunkte, die nicht unbedingt Gesetzesrang haben, sondern um ein klar beschlossenes Gesetz in dem steht, Verschlüsselung ist wichtig, jeder hat das Recht auf Verschlüsselung und der Staat steht dahinter, dass seine Bürger möglichst gut verschlüsseln.

Diese Frage, wie man mit den Begehrlichkeiten der Strafverfolger umgeht, also was irgendwie das Eindringen in Systeme mit Verschlüsselung angeht, mit Trojanern, mit Hintertüren wie auch immer, ist eine extrem komplexe Diskussion, wo die Frage „ist es denn notwendig“, also gibt es nicht auch mildere Mittel, haben wir nicht in der Regel auch noch andere Möglichkeiten, diese Probleme zu lösen, hinlänglich in den Urteilen des Verfassungsgerichts diskutiert wurde und der Regel dort auch beantwortet wurde. Weil gesagt wurde, ein Trojaner-Einsatz ist mitnichten das mildeste Mittel, die Risiken sind groß, die Nebenwirkungen sind groß und wir haben meistens auch andere Möglichkeiten. Das heißt also, wenn wir über diese Trojaner-Diskussion reden, lohnt es tatsächlich auch wirklich mit den Praktikern einer Strafverfolgung zu reden, die sehr oft sagen, okay, häufig genug brauchen wir es nicht, weil wir andere Mittel und Methoden haben, mit denen wir zum Erfolg kommen können. Wir haben nur leider nicht das Personal. Wir haben nur nicht die Ausbildung. Wir haben nicht die Ressourcen das zu tun. An der Frage, wo wir einen Trojaner-Einsatz über Bürgerrechte vs. Personalausstattung reden, sollte die Entscheidung ganz klar Richtung Bürgerrechte fallen. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir kommen nunmehr zu Herrn Dr. Herpig.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung): Ganz kurz vorweg. Mit Blick an Herrn MdB von Notz und Herrn Schönbohm. Im BSI-Gesetz steht meines Erachtens eben nicht drin, dass das BSI wissenschaftlich unabhängig arbeitet. Das steht im Gesetz vom Statistischen Bundesamt. Vielleicht wäre das ganz interessant, das mal zu erwägen, das dort aufnehmen zu lassen.

Und zu Herrn MdB Bernstiel: Das ist eben kein Misstrauen gegenüber dem BSI, sondern es ist ein Misstrauen gegenüber dem BMI und meistens darauf begründet – ist schon ein paar Jahre her – aber im Erlass des Innenministeriums damals an das BSI, das Bundeskriminalamt bei der Konzeption beziehungsweise eigentlich bei der Absicherung des Bundes-Trojaners/Quellen-TKÜ/Online-Durchsuchung zu unterstützen. Ich lasse das mal unbewertet. Ich sage nur, wo es herkommt.

Abg. **Christoph Bernstiel** (CDU/CSU): Ja, aber zu welchem Zweck? Der ist nicht das Ziel. Das ist eine völlig falsche Einschätzung.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung): Ich lasse es – wie gesagt – unkommentiert. Ich will jetzt nur nochmal darauf hinweisen, wo es herkommt.

Dann hatte Frau MdB Esken zu den Eingriffsbefugnissen Bundesverfassungsschutz, Bundesnachrichtendienst und was noch im IT-Sicherheitsgesetz 2.0 erwähnt wird, gesagt, es ist schwer zu bewerten aus dem Grund, weil die Gesamtschau der Überwachung einfach fehlt. Wir haben sie nicht. Wir können nicht beurteilen, also ich kann nicht beurteilen, ob das notwendig ist das auszubauen oder nicht. Ich will nicht – wie gesagt – ich will nicht

von vornherein annehmen, dass es nicht notwendig ist. Aber ich weiß es eben nicht. Und ich glaube, das kann niemand beurteilen. Auch die zuständigen Stellen können es nicht beurteilen. Und gleichzeitig sehen wir aber – und das können wir sehen – dass die Schutzmechanismen nicht ausgebaut werden. Wir sprechen da wieder von dem Schutz des Kernbereichs privater Lebensführung. Aber wie das umgesetzt wird ist vollkommen unklar. Vielleicht reden wir mal über konkrete Maßnahmen, wie z. B. dürfen bestimmte Sensoren, wie die Kamera oder das Mikrofon, nicht aktiviert werden auf diesen Geräten, wenn man eben in die Wohnung eintritt. GPS ist relativ genau, 1 m bis 3 m. Dann können wir vielleicht nicht abgrenzen, ob es das Schlafzimmer ist, aber dann wird es die ganze Wohnung sein. Aber darüber müssen wir diskutieren. Das tun wir aber nicht. Das heißt, wir haben keine neuen Schutzmaßnahmen, keine neuen Kontrollmaßnahmen, aber wir wollen eine Ausweitung der Überwachung ohne zu wissen, ob wir diese Überwachung brauchen. Was soll ich dazu sagen?

Federführung sehe ich hier beim Bundesministerium des Innern, für Bau und Heimat. Herr Könen, korrigieren Sie mich, wenn ich da falsch liege. Aber so einen Gesamtschutz zu erstellen, würde da liegen. Ich biete auch in der Kapazität, wie ich das kann, meine Unterstützung an. Das bringt mich auch zu der Frage, wer hat eigentlich den Hut auf? Wie gesagt, es gilt das Primat des Zivilen in der deutschen Cybersicherheitspolitik und IT-Sicherheitspolitik und damit hat für mich das Bundesministerium des Innern, für Bau und Heimat hier ganz klar den Hut auf.

Fragestellung Cyberabwehrzentrum Plus. Brauchen wir das überhaupt? Kann das das BSI nicht regeln? Ich glaube, das Cyberabwehrzentrum Plus oder das Cyberabwehrzentrum erfüllt einen sehr, sehr wichtigen Punkt hier in Deutschland. Es bringt auf operativer Ebene, genau wie der Cybersicherheitsrat das auf strategisch-politischer Ebene macht, alle Fäden irgendwo zusammen. Im Cyberabwehrzentrum können sich die Expertinnen und Vertreterinnen der verschiedenen Behörden, die sich mit Cybersicherheit in Deutschland beschäftigen, also auch der Verfassungsschutz und der Bundesnachrichtendienst oder der Militärische Abschirmdienst, zu aktuellen Fällen austauschen. Es gilt auch dort das Trennungsgebot. Das Trennungsgebot wird auch dort meines Wissens nach eingehalten. Von daher ist es eine sehr, sehr wichtige Kooperationsplattform. Es ist aufgrund der technischen Expertise wichtig, die nur im Bundesamt für Sicherheit in der Informationstechnik vorliegt, dass das Cyberabwehrzentrum weiterhin beim BSI auch tätig ist.

Abg. **Saskia Esken** (SPD): Das jetzt – Entschuldigung Herr Dr. Herpig – das ist jetzt Theorie gewesen, oder? Praktisch leistet das Cyberabwehrzentrum diese Aufgaben nicht, die Sie jetzt gerade aufgezählt haben.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung): Das sind die Aufgaben des Cyberabwehrzentrums.

Abg. **Saskia Esken** (SPD): Ja, ja. In der Theorie.

SV **Dr. Sven Herpig** (Stiftung Neue Verantwortung): Ich habe nicht im Cyberabwehrzentrum gearbeitet. Ich kann es in der Realität nicht beurteilen.

Das bringt mich dann genau genommen zum Übergang zu dem Punkt von Herrn MdB Höferlin. Präventive Befugnis des Cyberabwehrzentrums, Zusammenarbeit Bund/Länder: Ja, die Länder müssen eingebunden werden im Cyberabwehrzentrum und jede dieser Institutionen agiert im Rahmen seiner ihm zustehenden Befugnisse. Das ist jetzt schon theoretisch so, dass die Behörden dort agieren, das Cyberabwehrzentrum agiert nicht. Es hat keine exekutiven Befugnisse, weil es hat keine operativen Funktionen in dem Sinne. Sondern die Behörden bringen eben dort ihre eigenen Befugnisse ein und arbeiten im Rahmen ihrer Befugnisse, tauschen dort Informationen aus und kooperieren dort, um verschiedene Vorfälle zu bearbeiten. Das vielleicht auch als Schluss und damit auch den Einlass von Frau MdB Esken. Deswegen brauchen wir auch ein Einrichtungsgesetz für das Cyberabwehrzentrum, damit wir wissen, wer dort mit wem kommuniziert, wie die Befugnisse dort aufgeteilt sind, um das alles Mal transparent aufzustellen. Das klärt auch die Frage nach der Ländereinbindung. Vielen Dank.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Wir haben jetzt noch 13 Minuten. Das heißt, es bestünde die Möglichkeit für eine kurze letzte Nachfragerunde. Jetzt schaue ich mal, gibt es bei der CDU/CSU Wünsche? SPD?

Abg. **Saskia Esken** (SPD): Vielleicht kann Herr Könen jetzt die Fragen beantworten?

MDg **Andreas Könen** (BMI): Ich würde es aus Gleichberechtigungsgründen nicht machen wollen. Ich beantworte Ihnen die Fragen in einer anderen Veranstaltung sehr gerne, aber hier würde ich es einfach nicht machen, weil das ist als Expertenanhörung ausgelegt und ich bin nicht als Experte benannt. Also insofern, nein.

Stv. Vors. **Jochen Haug** (AfD): Dankeschön. Ich sehe bei der FDP, bei den LINKEN und bei den GRÜNEN auch keine Fragewünsche mehr. Dann bedanke ich mich bei allen Experten für Ihr Kommen und für das Erteilen Ihrer Auskünfte und schließe die Sitzung um 15:48 Uhr. Dankeschön.

Schluss der Sitzung: 15:48 Uhr

Andrea Lindholz, MdB
Vorsitzende

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 A

Stiftung Neue Verantwortung

Sachverständigenstellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema "IT-Sicherheit"

Die folgende Stellungnahme bezieht sich vor allem auf die Drucksachen 19/1328 (IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern" vom 21.03.2018), 19/7698 (Antrag "Digitalisierung ernst nehmen - IT-Sicherheit stärken" vom 12.02.2019) und 19/7705 (Antrag "Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors" vom 13.02.2019) aber auch auf die aktuellen Gesetzes- und Policy-Entwicklungen der Bundesregierung, wie dem IT-Sicherheitsgesetz 2.0, dem Gesetz zur Harmonisierung des Verfassungsschutzrechts, dem nationalen Schwachstellenmanagement, der Aktiven Cyberabwehr, einer Umorganisation des Cyber-Abwehrzentrums und der Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik.

[1] SNV-Profil: Dr. Sven Herpig
Sachverständigenstellungnahme für den Bundestagsausschuss für Inneres und Heimat am 08.04.2019 von Dr. Sven Herpig, SNV.

Die zukünftige Cybersicherheitspolitik in Deutschland sollte auf folgenden Kernaspekten basieren, um ein gleichermaßen hohes Maß an Freiheit wie auch an IT-Sicherheit gewährleisten zu können:

1. Strategische Planung und Umbau der nationalen Cybersicherheitsarchitektur[2] um Redundanzen und Friktionen zu vermeiden sowie um ein hohes Maß an Sicherheit durch Prävention, Detektion, Reaktion und Repression herzustellen. Hierbei sollte unbedingt die strikte Trennung zwischen zivilem und militärischem Bereich sowie von Nachrichtendiensten und Strafverfolgern beachtet und eine stärkere Unabhängigkeit des Bundesamts für Sicherheit in der Informationstechnik von Bundesministerium des Innern, für Bau und Heimat geprüft werden.

2. Erhöhen der Resilienz des nationalen IT-Ökosystems mit Fokus auf den Umgang mit Schwachstellen in Hardware, Software und Online-Dienstleistungen (u.a. IT-Sicherheitskennzeichen, Patch-Bereitstellung, Zwei-Faktor-Authentisierung[3] und Einführen eines nationalen Schwachstellenmanagements[4]).

3. Erhöhung der Schutzmaßnahmen[5] von Individuen und Institutionen gegenüber invasiver staatlicher Überwachungsmaßnahmen (u.a. Online-Durchsuchung und Quellen-TKÜ), Überarbeitung entsprechender Kontrollmechanismen[6] und Stärkung der Transparenz über den staatlichen Einsatz solcher Maßnahmen.

4. Erarbeitung einer umfassenden "whole-of-government"-Strategie zum repressiven Umgang mit Cyberoperationen; von der Entwicklung eines gemeinsamen (internationalen) Attributionsverständnisses bis zur Verknüpfung mit entsprechenden (u.a. nachrichtendienstlichen, politischen und wirtschaftlichen) Gegenmaßnahmen im Rahmen internationaler Normen. Hierbei ist ein differenzierter Diskurs zur "Aktiven Cyberabwehr"[7] unerlässlich.

5. Verbesserung der Fachkräfteausbildung und -weiterbildung im Bereich der IT-Sicherheit und innovative Maßnahmen zum (Ein-)Binden entsprechender Fachkräfte im öffentlichen Dienst[8]; auch mit Hinblick auf die Strategieentwicklung Deutschlands.

---

[2] Sven Herpig und Clara Bredenbrock: Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum
[3] Jan-Peter Kleinhans: Mehr IoT-Sicherheit in der EU
[4] Sven Herpig: Schwachstellen-Management für mehr Sicherheit
[5] Sven Herpig: A Framework for Government Hacking in Criminal Investigations
[6] Thorsten Wetzling: Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BND) sowie weiterer Vorlagen
Thorsten Wetzling: Nachrichtendienstkontrolle in Deutschland und Europa jetzt vorantreiben!
[7] Sven Herpig: Hackback ist nicht gleich Hackback
[8] Julia Schuetze: Warum dem Staat IT-Sicherheitsexpert:innen fehlen

Im Einzelnen

Ad 1. Eine Übersicht zur deutschen Cybersicherheitsarchitektur mit Kurzanalyse des Cyber-Abwehrzentrums wurde am 1. April 2019 von der Stiftung Neue Verantwortung veröffentlicht.[9]

Ad 1. Die Digitalisierung als Querschnittsaufgabe erfordert die direkte Zusammenarbeit der für IT-Sicherheit zuständigen Stelle, hier das Bundesamt für Sicherheit in der Informationstechnik (BSI), mit den Bedarfsträger:innen, u.a. Ministerien, Institutionen innerhalb der Bundesländer, der Industrie aber auch Institutionen mit verfassungsrechtlicher Unabhängigkeit. Gleichzeitig wird spätestens seit Verabschiedung der Cybersicherheitsstrategie für Deutschland 2016 eine starke Konvergenz öffentlicher Sicherheit (u.a. auch durch den Einsatz von Hacking-Werkzeugen) und IT-Sicherheit vorangetrieben. Um einen singulären Fokus des BSI auf IT-Sicherheit zu wahren und eine entsprechende vertrauenswürdige und effektive Zusammenarbeit mit anderen staatlichen und nicht-staatlichen Stellen zu gewährleisten, sollten verschiedene Modelle der Unabhängigkeit des BSI vom Bundesministerium des Innern, für Bau und Heimat (BMI) geprüft werden. Hierbei steht vor allem die Frage der Fachaufsicht im Vordergrund. Modelle die als Vorbild dienen könnten wären u.a. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) oder das statistische Bundesamt. Grundkonsens muss hierbei sein, dass die Behörde nicht aufgeteilt wird, da die bestehenden Synergien elementar zu ihrer Funktionsfähigkeit beitragen.

Ad 1. Die seit Jahren diskutierte Umorganisation der Cyber-Abwehrzentrums (Cyber-AZ) sollte umgehend umgesetzt werden. Hierbei ist es wichtig, dass zusätzlich zu den bestehenden Verwaltungsvereinbarungen der im Cyber-AZ vertretenen Behörden eine Rechtsgrundlage über die Zusammenarbeit geschaffen wird. Dort muss u.a. geregelt sein, welche Kommunikationspflichten den einzelnen Behörden gegenüber dem Cyber-AZ zukommen sollen. Weiterhin ist eine Einbindung der Länder erforderlich. Eine institutionelle Anbindung des Cyber-AZ beim BSI ist u.a. aufgrund der dort existierenden technischen Fachkenntnisse und artverwandten Strukturen (CERT-Bund, Nationalem IT-Lagezentrum, Lagezentrum und IT-Krisenreaktionszentrum) unerlässlich. Eine Angliederung an den militärischen Bereich (z. B. an die Bundeswehr) wäre kontraproduktiv, genauso wie eine Aufweichung des Trennungsgebots zwischen Nachrichtendiensten und Strafverfolgern.

Ad 1. Die immer komplexer werdende Cybersicherheitsarchitektur in Deutschland braucht einen "Masterplan". Während ein gewisses natürliches Wachstum der Behörden und Strukturen in den ersten Jahren der deutschen Cybersicherheitspolitik verständlich ist, ist es – auch aufgrund der begrenzten Ressourcen wie IT-Fachkräften – notwendig, einen kohärenten Plan vorzulegen, wie z.B. der Nationale Pakt für Cybersicherheit (s. Koalitionsvertrag[10]) oder das Deutsche Institut für Internationale Cyber-Sicherheit (s. Cyber-Sicherheitsstrategie

[9] Sven Herpig und Clara Bredenbrock: Cybersicherheitspolitik in Deutschland. Akteure, Aufgaben und Zuständigkeiten. Im Fokus: Das Cyber-Abwehrzentrum

[10] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD

für Deutschland 2016[11]) eingebunden werden sollen. Nur so kann dem Aufbau von Parallelstrukturen entgegengewirkt und die vorhandenen Ressourcen effizient genutzt werden. Dies beinhaltet auch klare Zuständigkeiten, Kooperation und Kommunikation von Bundes- und Landesebene (s. Gründung des Landesamts für Sicherheit in der Informationstechnik in Bayern). Eine Militarisierung des Bereichs Cybersicherheit in Deutschland – u.a. durch geographische Angliederung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) an das Forschungsinstitut Cyber Defense (CODE) oder das gemeinsame Betreiben der Agentur für Innovation in der Cybersicherheit – sollte strikt vermieden werden. Seit 1991 ist Cybersicherheit in Deutschland eine zivile Domäne, die militärische Aufgabe im Cyberraum muss daher auf den Schutz der eigenen Systeme und mandatierte Einsätze von Cyber-Wirkmitteln begrenzt bleiben. Für Cybersicherheit in Deutschland hat weiterhin das Primat des Zivilen in den zivil-militärischen Beziehungen zu gelten.

Ad 2. Ein:e hochranginge:r Vertreter:in des zuständigen BMI bezeichnete Schwachstellen 2018 als "die Seuche der modernen IT". Nur wenn diesem Zustand entschieden entgegengewirkt werden kann, kann die IT-Sicherheit in Deutschland signifikant erhöht werden. Dem Bereich der "bekannten" Schwachstellen, die in weit mehr als 90% der Exploits zum Einsatz kommen[12], gilt es daher, besondere Aufmerksamkeit zu widmen. Dies geht über Schwachstellen in Computern und Smartphones hinaus und betrifft den gesamten Sektor des Internets-der-Dinge (u.a. Smart Home und Connected Cars). Die Marktüberwachung und Verbraucherschutzbehörden müssen ertüchtigt werden, um überhaupt IT-Sicherheit einfordern und Produkte/Unternehmen überprüfen zu können. Eine Kennzeichnungspflicht allein schafft nicht unmittelbar mehr IT-Sicherheit. Standardisierung, Zertifizierung und Marktüberwachung müssen immer gemeinsam betrachtet werden[13], da sie voneinander abhängen.

Im Bereich der "unbekannten" Schwachstellen sollte die Bundesregierung „Bug Bounty“-Projekte für Programme (z.B. EU-Fossa[14]) unterstützen[15] und ein rechtlich verankertes, behördenübergreifendes und transparentes Schwachstellenmanagementmodell einführen. Ein Referenzmodell wurde durch die Zusammenarbeit von internationalen Expert:innen erstellt, im August 2018 von der Stiftung Neue Verantwortung veröffentlicht und dem Bundesministerium des Innern, für Bau und Heimat vorgestellt.[16] Um diese Puzzleteile zusammenzuführen, wäre es ggf. hilfreich, ein umfassendes nationales Konzept zur Verringerung von Schwachstellen mit konkreten Maßnahmen zu erarbeiten und dann zu implementieren.

[11] Bundesministerium des Innern: Cyber-Sicherheitsstrategie für Deutschland 2016
[12] Sven Herpig: Schwachstellen-Management für mehr Sicherheit
[13] Jan-Peter Kleinhans: Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit
[14] Sebastian Grüner: EU erweitert Bug-Bounty-Programm für Open-Source-Software
[15] Fraktion der FDP im Bundestag: Digitalisierung ernst nehmen - IT-Sicherheit stärken
[16] Sven Herpig: Schwachstellen-Management für mehr Sicherheit

Ad 2. Zwei weitere Grundvoraussetzungen um die IT-Sicherheit in Deutschland nachhaltig zu erhöhen, sind die Bekräftigung und Förderung der Maßnahmen aus den Eckpunkten der Kryptopolitik 1999 und das Vorantreiben und die Förderung von Multifaktorauthentifizierung bei Dienstleistungen wie E-Mails und sozialen Medien.

Ad 3. Im aktuellen Referentenentwurf zum "Gesetz zur Harmonisierung des Verfassungsschutzrechts" werden die Befugnisse zum Eingriff in informationstechnische Systeme durch das Bundesamt für Verfassungsschutz und den Bundesnachrichtendienst ausgeweitet, ohne ihnen entsprechende Schutz- und Kontrollmaßnahmen für Individuen und Institutionen entgegenzustellen. Dies folgt der Ausweitung entsprechender Befugnisse und Aufgaben des BKA aus 2017. Die vom Bundesverfassungsgericht angemahnte Gesamtschau der Überwachung[17] ist hier dringend geboten. Die Gesamtschau müsste Kontrolleur:innen zum Zeitpunkt der Erfordernis- und Zulässigkeitsprüfung auch in praktischer Weise zur Verfügung stehen. Auch wenn einer bedarfs- und lagenangepassten Ausweitung der Aufgaben und Befugnisse im Allgemeinen (!) nichts entgegensteht, so ist ein weiterer staatlicher Ausbau von invasiven Eingriffen in informationstechnische Systeme ohne empirische Evidenz des Bedarfs und Identifikation weißer Flecken bei der Arbeit von Nachrichtendiensten und Strafverfolgern höchst problematisch. Hierbei gilt es, auch vergangene Operationen von Strafverfolgern und Nachrichtendiensten (z.B. NSU, Anis Amri) von unabhängiger Stelle daraufhin zu analysieren, ob das Fehlen aktuell geforderter Befugnisse ausschlaggebend für den Verlauf der Ermittlungen war. Die Bundesregierung versprach im Koalitionsvertrag bereits die "gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" bei Ausweitung der Befugnisse der Sicherheitsbehörden[18]. Mögliche technische und rechtliche Schutzmaßnahmen gegen Quellen-TKÜ und Online-Durchsuchung (Oktober 2018)[19] sowie Beispiele für gute Rechtsnormen und innovative Kontrollpraxis/-instrumente gegen nachrichtendienstliche Überwachung (März 2019)[20] wurden von der Stiftung Neue Verantwortung erarbeitet.

Ad 4. Der Bundesregierung fehlt aktuell eine kohärente und umfassende Strategie, wie politisch auf Cyberoperationen zu reagieren ist. Eine solche Strategie muss u. a. gemeinsame, international harmonisierte Attributionsstandards, eine kohärente Kommunikationsstrategie und ein allgemeingültiges Verständnis von "Aktiver Cyberabwehr" (bekannt auch als "Hackbacks") enthalten. Schwerwiegender ist jedoch das Fehlen eines "whole-of-government"-Ansatzes von der IT-Sicherheitstrinität (Prävention, Detektion, Reaktion) über Attribution und ggf. aktive Cyber-Abwehr bis hin zur Verknüpfung mit unterschiedlichen politischen Reaktionen inkl. nachrichtendienstlicher Gegenmaßnahmen, wirtschaftlichen oder finanziellen Sanktionen, politischen Sanktionen uvm. Das eine solche Strategie fehlt, ist auch in der Zusammenarbeit mit Partnern (gemeinsame

[17] Fraktion der SPD im Bundestag: Positionspapier der AG Inneres und der AG Digitale Agenda
[18] Bundesregierung: Koalitionsvertrag zwischen CDU, CSU und SPD
[19] Sven Herpig: A Framework for Government Hacking in Criminal Investigations
[20] Thorsten Wetzling und Kilian Vieth: Massenüberwachung bändigen. Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich

Attribution oder Implementierung von gemeinsamen Maßnahmen im Rahmen der Cyber Diplomacy Toolbox/ eines Sanktionsregimes) hinderlich.

Ad 4. Aktive Cyber-Abwehr ist ein Überbegriff verschiedener Maßnahmen, die politisch, rechtlich und technisch äußerst unterschiedlich zu bewerten sind. Äußerst problematisch sind hierbei unter anderem Eingriffe in informationstechnische Systeme in Deutschland. Einen Überblick über entsprechende Maßnahmen hat die Stiftung Neue Verantwortung im Juli 2018 vorgelegt.[21] Einige Maßnahmen nach dieser Definition sind bereits legitimiert (z.B. "Walled Garden"-Maßnahmen für Internet Service Provider durch das IT-Sicherheitsgesetz 2015), andere sollen gerade durch die Harmonisierung des Verfassungsschutzgesetzes (Einsatz von Hacking-Werkzeugen zur Attribution) und durch das IT-Sicherheitsgesetz 2.0 (u.a. Anweisungsbefugnis gegenüber Providern zur Datenlöschung oder Datenumleitung) eingeführt werden. Das Fehlen einer nuancierten (öffentlichen) Debatte zu den verschiedenen Maßnahmen inklusive Bestandsaufnahme sowie das Fehlen einer Einbettung in die nicht-vorhandene deutsche Strategie zum politischen Umgang mit Cyberoperationen (s. vorheriger Absatz) kann und wird zu Problemen in unbekanntem Ausmaß führen. Welche Rolle der Bundeswehr im Rahmen der Cyberabwehr zukommt, ist nicht abschließend geklärt. Auch ist es beim aktuellen Vorgehen unmöglich hervorzusehen, ob die wenigen Ressourcen, die in Deutschland vorhanden sind (IT-Fachkräftemangel) aktuell effizient investiert werden.

Ad 5. IT-Fachkräfte sind die wichtigsten Ressourcen, um IT in Deutschland abzusichern. Ihre Ausbildung, Weiterbildung und effizienter Einsatz sind neben den genannten technischen und politischen Rahmenbedingungen die Grundvoraussetzung für mehr IT-Sicherheit. Gleichzeitig übernimmt der Staat vermehrt Aufgaben im Bereich staatliche IT-Sicherheitsvorsorge. Ideen diesbezüglich hat die Stiftung Neue Verantwortung im Februar 2018 vorgelegt[22].

Ad 5. Im Hinblick auf den effizienten Einsatz der vorhandenen Fachkräfte wäre es daher notwendig, die Cyber-Sicherheitsstrategien aus den Jahren 2011 und 2016 zu evaluieren. Es gibt keine Erkenntnisse, ob diese Strategien erfolgreich waren oder nicht. Dies ist aber auch eine Grundvoraussetzung für die Verabschiedung weiterer politischer und legislativer Maßnahmen im Bereich der IT-Sicherheit in Deutschland.

[21] Sven Herpig: Hackback ist nicht gleich Hackback
[22] Julia Schuetze: Warum dem Staat IT-Sicherheitsexpert:innen fehlen

Fazit

Zusammenfassend muss gesagt werden, dass in der deutschen Cybersicherheitspolitik gleichzeitig eine gewisse Strategieunfähigkeit (u. a. politischer Umgang mit Cyberoperationen, Entwicklung der Cybersicherheitsarchitektur), ein Fehlen empirischer Evidenz (u. a. Evaluation der Cybersicherheitsstrategien, Gesamtschau der Überwachung), eine Vernachlässigung der notwendigen Anpassung von Schutz- und Kontrollmaßnahmen (u. a. gegenüber Quellen-TKÜ und Online-Durchsuchung) und ein Mangel an Ressourcen (Fachkräfte) vorliegen.

Staatliche Aufgaben und Befugnissen getreu dem Motto "besser haben als brauchen" zu erweitern, ist höchst problematisch und führt zusammen mit den vorher genannten Herausforderungen zu falschen Prioritäten und ggf. zu weniger, anstatt mehr IT-Sicherheit; definitiv aber zu einem ineffizientem Einsatz der vorhandenen Ressourcen und einem grundlosen Ausbau repressiver Maßnahmen. Umso schlimmer ist es dann, wenn Befugnisse erweitert werden, ohne die Ressourcen und Instrumente der Kontrolle entsprechend anzupassen.

An dieser Stelle sollte jedoch nicht außer Acht gelassen werden, dass verschiedene politische und rechtliche Maßnahmen, auch im internationalen Vergleich, als positiv zu bewerten sind. Hier zählen u. a. das bisherige Primat des Zivilen bei Cybersicherheit, Aufbau und Rolle des Bundesamts für Sicherheit in der Informationstechnik (inkl. CERT-Bund, Nationalen IT-Lagezentrum und Cyber-Abwehrzentrum), IT-Sicherheitsstandards und Meldepflichten für kritische Infrastrukturen, sehr gut ausgebildete IT-Spezialist:innen sowie eine (begrenzte) öffentliche Debattenkultur und Gesprächsbereitschaft der Verantwortlichen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 B

Stellungnahme zu den Anträgen:

19/7698: Digitalisierung ernst nehmen – IT-Sicherheit stärken,
19/7705: Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors, und
19/1328: IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

Berlin, 4. April 2019

Die Digitalisierung ist in Deutschland und Europa auf dem Vormarsch. Immer mehr Geräte enthalten IT oder sind über Datenverbindungen mit dem Netz verbunden. Schätzungen des BMVI auf Grundlage des IT-Netzwerkausrüsters Cisco gehen davon aus, dass die Zahl vernetzter Geräte bis 2020 auf ca. 800 Millionen in Deutschland allein steigen wird. Schätzungen verschiedener Netzbetreiber gehen von insgesamt zwischen 35 Mrd. und 50 Mrd. vernetzten Geräten weltweit in den 2020ern aus. Mit der zunehmenden Vernetzung von IT-Systemen und der Übernahme immer neuer Funktionen und Aufgaben in immer mehr Einsatzgebieten kommt IT eine ständig wachsende Bedeutung zu. Mit diesem Wachstum steigt auch die Relevanz der Sicherheit dieser Systeme für alle Beteiligten. Der Themenkomplex der IT-Sicherheit wird deshalb von Staat, Wirtschaft und Gesellschaft zunehmend als relevantes Handlungsfeld der Politik gesehen.

Die Veröffentlichung der Cybersicherheitsstrategien von 2011 und 2016, das IT-Sicherheitsgesetz von 2015 und dessen Ergänzung im Jahr 2017, sowie die vom Bundesministerium für Verteidigung gestartete Initiative zum Cyber- und Informationsraum zeigen nur einige Ansätze dafür, wie die Bundesregierung mit diesen Bedrohungen umgeht.

Der Internetwirtschaft kommt im Rahmen dieser Überlegungen in mehrerlei Hinsicht wachsende Bedeutung zu. Zum einen bietet und liefert sie die Infrastrukturen und Dienste, die die digitale Welt ausmachen und ist damit Treiber der voranschreitenden Digitalisierung sind. Gleichzeitig kann sie Angriffsziel und Opfer von Angriffen werden, sie spielt damit eine Schlüsselrolle bei der Gestaltung von IT-Sicherheit in Deutschland.

Die Debatte um die Ausgestaltung von IT-Sicherheit hat sich in den vergangenen Jahren weiter differenziert und adressiert sowohl operative

Fragen zu konkreten Maßnahmen der IT-Sicherheit, als auch in zunehmendem Maße die dahinterliegenden Strukturen und Maßgaben. Beide werden in den zur Debatte stehenden Anträgen entsprechend gewürdigt. eco – Verband der Internetwirtschaft e.V. sieht in den folgenden Bereichen weiteren Diskussions- und Erörterungsbedarf:

(IT-)Sicherheitsarchitektur:
Die jüngsten Vorfälle wie die Doxing Attacke gegen Bundestagsabgeordnete, aber auch die allgemeine Entwicklung der Sicherheitsinstitutionen in Deutschland mit der Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) werfen die Frage nach der „organisatorischen Fitness“ der deutschen Sicherheitsbehörden für digitale Sicherheitslagen auf. Im Zentrum der Überlegungen steht immer wieder das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Eine zentrale Forderung, die auch in den drei vorliegenden Anträgen herausgearbeitet wird, ist die Unabhängigkeit des BSI und dessen Herauslösung aus dem Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat (BMI). Zentral an dieser Stelle ist, dass das BSI unabhängig von anderen Behörden arbeiten sollte und sich so alleine auf eine Förderung der IT Sicherheit statt deren Unterwanderung fokussieren kann.

Dies gilt umso mehr für Wechselwirkungen mit der ebenfalls im Geschäftsbereich des BMI betriebenen ZITiS. Beide Institutionen haben unterschiedliche Aufgaben, die möglicherweise zueinander in ein Spannungsverhältnis geraten könnten, wenn eine Stelle Schwachstellen sammeln, prüfen und deren Behebung einleiten soll, die andere möglicherweise jedoch Schwachstellen ausnutzt, um im Auftrag von Ermittlungsbehörden und Geheimdiensten in IT-Systeme einzudringen. Es ist offensichtlich, dass sich diese Gemengelage unterschiedlicher Aufgaben diametral gegenübersteht.

Es bedarf für die Funktion des BSI als zentrale Behörde für Cybersicherheit einer Klarstellung dahingehend, dass die Arbeit des BSI unabhängig von den Erwägungen anderer Stellen und Sicherheitsbehörden erfolgt und ausschließlich der Verbesserung der Sicherheit von IT-Systemen und Netzen verpflichtet ist.

Alle davon abweichenden Maßgaben schwächen die Rolle des Amtes und das Vertrauen in digitale Dienste. Im Sinne einer stringenten Digitalisierung ist dies

nicht hilfreich, da so letzten Endes auch das Vertrauen in staatliche Behörden und deren Zuverlässigkeit untergraben wird. Die Festschreibung des BSI als obere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern wird dem möglicherweise aufgrund der vorgetragenen Vorbehalte nicht mehr gerecht.

In diesem Licht steht auch die Arbeit des Nationalen Cyberabwehrzentrums (NCAZ). Als Koordinierungsstelle für die IT-Abwehr steht es sowohl direkt durch die Zusammenarbeit mit dem BfV als auch durch die Zusammenarbeit mit weiteren Geheimdiensten und Ermittlungsbehörden vor der Frage, welchen Beitrag es zur Verbesserung der IT-Sicherheit leisten soll. Das Beispiel des groß angelegten Hacks auf das Auswärtige Amt und das Bundesverteidigungsministerium unterstreichen grundsätzlich, dass es neben der Arbeit des BSI auch in allen anderen Verfassungsorganen eine proaktive Auseinandersetzung mit dem Thema und darüber hinaus auch der Austausch über organisationsübergreifende Ereignisse sinnvoll sein kann.

In diesem Kontext wird immer wieder auch die Forderung nach einer Neuzuordnung des BSI in den Geschäftsbereich eines noch zu schaffenden Bundesministeriums für Digitales diskutiert. Ein solches Ministerium hat durchaus den Vorteil, der bestehenden Zersplitterung bei der Regulierung von Netzen und Diensten entgegenzuwirken, wenn der entsprechende fachliche Zuschnitt korrekt erfolgt. Je nach Themenschwerpunkt hat man bei zentralen Fragen der Digitalisierung mit bis zu vier verschiedenen Bundesministerien zu tun, die sehr unterschiedliche, teilweise widersprüchliche Ziele verfolgen. Aber auch bei einer solchen Neuzuordnung muss der Grundsatz gelten, dass das BSI in seiner Arbeit unabhängig sein muss und über etwaig bestehende Zweifel, die durch die Zusammenarbeit mit Sicherheitsbehörden entstehen, erhaben sein muss. Da das hier in Rede stehende Digitalministerium aller Voraussicht nach keine geheimdienstlichen Aufgaben übernimmt, wären die Zweifel, die derzeit in Bezug auf das BMI im Zusammenhang mit ZITiS bestehen, ausgeräumt.

Zuletzt sei noch auf die Ausstattung und Ausrüstung von Polizeibehörden eingegangen. Diese müssen dringend sowohl personell als auch technisch besser ausgestattet sein und für die Herausforderungen der Strafverfolgung im Netz besser geschult werden. Die Erfahrungen, die eco in Workshops mit Strafverfolgern und Ermittlungsbehörden gemacht hat, zeigen, dass hier noch dringender Informations- und Nachschulungsbedarf besteht. Inwieweit eine organisatorische Umgestaltung der Ermittlungsarbeit in Form einer Bündelung bestimmter Arbeiten bei den Zentralen Anlaufstellen für Cybercrime (ZACs)

hilfreich sein kann, kann nicht abschließend beurteilt werden. Zu überlegen ist hierbei, ob es darüber hinaus nicht auch sinnvoll wäre, wenn grundsätzlich eine Verbreiterung der IT-Kompetenzen von Polizeibeamten erfolgen würde.

Strukturelle Verbesserung der IT-Sicherheit:
Eine maßgebliche Frage ist der Umgang mit Schwachstellen, über die öffentliche Stellen Kenntnis erlangen. Derzeit gibt es keine klaren Maßgaben, wie mit solchen Schwachstellen umgegangen wird. Grundsätzlich sollten solche Schwachstellen den Unternehmen mitgeteilt werden, in deren Systemen oder Produkten sie bestehen. Wenn Behörden Sicherheitslücken in IT-Systemen für sich behalten, bspw. um besser mit Hilfe eigener Software Überwachungsmaßnahmen durchzuführen oder um gezielt schädliche Systeme oder Akteure ausschalten zu können (Hackback), schädigt dies das Vertrauen von Nutzerinnen und Nutzern in die Verwendung dieser Dienste. Es gefährdet zudem auch deren Sicherheit. Es ist daher dringend angezeigt, dass alle staatlichen Stellen ihnen bekannte Sicherheitslücken zwingend melden und zwecks einer Schließung derselben in die Datenbank bekannter Sicherheitslücken (CVS) überführen müssen.

Eine entsprechende Meldepflicht wurde bereits mit dem IT-Sicherheitsgesetz (IT-SG) den Betreibern kritischer Infrastrukturen (KRITIS) auferlegt und mit dem NIS-Richtlinien-Anpassungsgesetz von 2017 auf Betreiber von Clouddiensten und Onlinemarktplätze ausgeweitet. Staatliche Stellen stehen aus Sicht des eco hier ebenso in der Pflicht, Ihren Teil zur Verbesserung der IT-Sicherheit aller Beteiligten zu leisten

Dies wirft auch die Frage auf, wie mit Software verfahren wird, die zur Ausspähung von Informationen auf Endgeräten von Nutzern durch Ermittlungsbehörden und Geheimdienste (Staatstrojaner) eingesetzt wird.

Zwar bieten Staatstrojaner gegenüber der flächendeckenden, anlasslosen Vorratsdatenspeicherung den Vorteil, dass sie zumindest theoretisch zielgerichtet eingesetzt werden können, auch wenn sich hier die Frage nach einer möglichen nicht intendierten Weiterverbreitung stellt. Ihre Einsatzszenarien werfen jedoch eine Reihe grundlegende Fragestellungen auf, die bis heute nicht geklärt wurden.

Diese Ermittlungswerkzeuge müssen auf den Endgeräten der Zielpersonen installiert werden. Hierzu liegen keine Erkenntnisse vor, wie genau dies geschieht. Das wirft die Frage auf, ob und inwieweit hier möglicherweise

schadhafte Auswirkungen durch die Ausnutzung von Sicherheitslücken in Kauf genommen werden, über die Ermittlungsbehörden und Geheimdienste verfügen. Zahlreiche weitere Sicherheitsmaßnahmen, wie beispielsweise die Stärkung der Verschlüsselung von Diensten, würden so untergraben.

Der Einsatz von Verschlüsselung ist ein zentraler Baustein für mehr Sicherheit in digitaler Kommunikation. Ihr Einsatz sollte daher auf keinen Fall durch Regelungen zur Bereitstellung von „Generalschlüsseln“ durch Betreiber von Diensten oder durch vorgegebene Übergabe- und Ausleitungsschnittstellen untergraben werden. Die Praxis zeigt zudem, das derartige Schlüssel in keinem Fall dauerhaft geheim gehalten werden können.

Auf dem Markt befinden sich verschiedene offen zugängliche Verschlüsselungslösungen, sowie Dienste, die eigene Verschlüsselungstechnologien zum Einsatz bringen. Eine Festlegung auf eine bestimmte Verschlüsselungstechnologie oder einen bestimmten Standard durch den Staat, bspw. bei Ausschreibungen, sollte kritisch geprüft werden und mit Blick auf die dynamischen Entwicklungen im Markt eher zurückgestellt werden.

Die Problematik unterschiedlicher – tendenziell gleichwertiger – Sicherheitslösungen stellt sich auch bei der Frage der Anerkennung von Normen und Standards mit Bezug auf IT-Sicherheit. Die Debatte um die TR-Router des BSI und deren Akzeptanz bei TK-Unternehmen und Kabelnetzbetreibern mit eigenen Standards einerseits, sowie den Herstellern der Geräte andererseits zeigt, dass Normierung im Sinne einer einheitlichen Definition von zwingend einzuhaltenden technischen Standards und Spezifikationen in der bisherigen Form u.U. nicht zielführend ist.

Auch die Verpflichtung zur Veröffentlichung des Quellcodes unter einer bestimmten öffentlichen Lizenz (Open Source) ist nicht zwingend und ausschließlich mit einer Verbesserung der IT-Sicherheit verbunden, wenngleich es im Prinzip zu einer Verbesserung des Sicherheitsniveaus beitragen kann, wenn der Quellcode einer Überprüfung zugänglich ist und so nachvollzogen werden kann. Dies ermöglicht allerdings zugleich auch, dass Schwachstellen in Quellcodes von allen Akteuren, auch böswilligen, identifiziert und ausgenutzt werden können. Es sollte daher grundsätzlich im Ermessen von Entwicklern und Herstellern liegen, wie sie ihre Software lizenzieren wollen und mit wem sie für welche Zwecke ihren Quellcode teilen wollen. Escrow-Verfahren mit beschränktem Zugang, wie Beispielsweise im derzeitigen IT-Sicherheitsgesetz für das BSI vorgesehen, können hier ebenfalls zum Einsatz kommen.

Robuster Rechtsrahmen für IT-Sicherheit:
In der Gesamtschau stellt sich die Frage, wie ein Rechtsrahmen für IT-Sicherheit auszugestalten wäre. Der Schutz personenbezogener Daten nimmt hierbei eine besondere Stellung ein.

Mit der Datenschutz-Grundverordnung (DSGVO) hat die Europäische Union bereits einen Rechtsrahmen gestaltet und auch Maßgaben für mehr (IT-)Sicherheit in den Verordnungstext einfließen lassen. Sie implizieren, dass Datenverarbeitung auch unter „sicheren“ Rahmenbedingungen geschehen muss und bietet im Verbund mit den vorliegenden Regelungen zur IT-Sicherheit hohe Anforderungen an Anbieter von Diensten und Produkten. Zwar wäre hier noch eine Überprüfung der Einheitlichkeit der Meldewege und –pflichten zu überprüfen, um Dopplungen bei den Meldepflichten zu vermeiden. Grundsätzlich ist dieser Rechtsrahmen jedoch geeignet.

Inwieweit eine zusätzliche europäische Regelung zur Vertraulichkeit elektronischer Kommunikation einen Beitrag leisten kann, muss an dieser Stelle offenbleiben. Eine Regelung, die, analog zum deutschen Fernmeldegeheimnis, die Vertraulichkeit von Kommunikationsinhalten während des Datentransfers sicherstellt, könnte auf europäischer Ebene für Klarheit sorgen. Sinnvoll wäre hier den Regelungsbedarf zu prüfen und die bestehende Regulierung robust umzusetzen, ehe weitere Regelungen getroffen werden.

Vor dem Hintergrund der Bedeutung des Schutzes personenbezogener Daten und datensparsamer Ansätze bei Ermittlungen und bei staatlichem Handeln ist es auch wegen des massiven Eingriffs in die Vertraulichkeit der Kommunikation von Bürgerinnen und Bürgern dringend erforderlich, dass die Vorratsdatenspeicherung abgeschafft wird.

Darüber hinaus stellt sich die Frage, wie das oben beschriebene Spannungsverhältnis zwischen Ermittlungsbehörden und Geheimdiensten auf der einen Seite und Institutionen zur Stärkung von IT-Sicherheit auf der anderen Seite sinnvoll aufgelöst werden kann. Derzeit ist zu beobachten, dass zahlreiche, oftmals kritisch zu bewertende, Maßnahmen insbesondere im Geheimdienstbereich mit Verweis auf die Handlungsfähigkeit der Behörden nachträglich legalisiert werden. Dies war bei der Novelle des letzten Gesetzes über den Bundesnachrichtendienst Ende 2016 und auch bei dem jetzt bekannt gewordenen Entwurf eines Gesetzes zur Harmonisierung des

Verfassungsschutzrechts der Fall, welcher durch eine Änderung des Verfassungsschutzgesetzes sowie des BND-Gesetzes die Möglichkeiten der Dienste erneut deutlich ausweiten soll. Außer Acht gelassen werden dabei allerdings die negativen Auswirkungen auf das Vertrauen und die Integrität in Telekommunikation und digitale Dienste.

Darüber hinaus und je nach Angriffsvektor der Ermittlungsbehörden wirft dies auch die Frage auf, ob für die Durchführung der Maßnahmen nicht ein größeres Sicherheitsrisiko für die Allgemeinheit erzeugt und billigend in Kauf genommen wird, als in einer digitalisierten Gesellschaft akzeptabel.

Zu beobachten ist zudem, dass immer häufiger eine eigentlich originär staatliche Verantwortung auf Betreiber von Diensten und Netzen übertragen wird. Dies geschieht sowohl auf europäischer Ebene mit der derzeit diskutierten „Verordnung zur Verhinderung der Verbreitung terroristischer Online-Inhalte“ als auch in Deutschland beispielsweise mit dem vom Bundesrat diskutierten „Anti-Darknet-Gesetze“.

Beiden ist gemein, dass sie oftmals sehr unspezifische Anforderungen an Betreiber von Diensten und Netzen stellen, somit also einen recht frühen Übergang der Verantwortung implizieren könnten bei einer weiten Interpretation und Auslegung. Diese Verschärfungen des Strafrechts im IT-Bereich halten wir für nicht sinnvoll, da sie den problematischen Einsatz technisch nur bedingt tauglicher Maßnahmen wie Uploadfilter erfordern und zudem auch eine konsistente und proaktive Überwachung von Nutzern und deren Aktivitäten im Netz bedingen oder zumindest zur Folge haben. Dies ist sowohl aus bürgerrechtlicher Sicht als auch aus technischer Sicht nicht sinnvoll.

Die Verantwortung für Ereignisse im Netz mit Sicherheits- oder Strafrechtsrelevanz kann sinnvoll nur für solche Fälle zugeschrieben werden, die im Verantwortungs- und Einflussbereich des jeweiligen Akteurs stehen. Dies gilt sowohl für Fragen der proaktiven Kontrolle und Überwachung von Nutzern, die strikt abzulehnen ist, als auch für die Haftung für etwaig bestehende IT-Sicherheitslücken, die oftmals nur vom Hersteller der jeweiligen Software oder des jeweiligen Produkts bzw. der jeweiligen Komponente sinnvoll adressiert werden kann.

In beiden Fällen ist eine pauschale Zuweisung und Verlagerung der Verantwortung an einen Akteur, der gesamtschuldnerisch für alle Aktivitäten seiner Nutzer aber auch seiner Geschäftspartner in der Pflicht steht, nicht

sinnvoll darstellbar.

Unbeschadet davon kann im Fall der IT-Sicherheit darüber nachgedacht werden, in welchen Fällen eine Konkretisierung der bestehenden Haftungsregeln sinnvoll ist, so beispielsweise zur besseren Adressierung einer möglichen Fahrlässigkeit im Rahmen der Herstellerhaftung., Dies könnte exemplarisch wie im bestehenden Haftungsrecht für einen Mangel in IT-Systemen dargestellt werden, die per definitionem ebenfalls nie komplett fehlerfrei sein können.

Eine Haftung von Plattformbetreibern, Hostern oder Telekommunikationsunternehmen für die Handlungen von Nutzern, die über die in der e-Commerce Richtlinie definierten Maßgaben hinausgehen, und wie sie jetzt schon teilweise mit dem Netzwerkdurchsetzungsgesetz (NetzDG) und den dazu gehörigen Bußgeldleitlinien eröffnet worden sind, lehnen wir ab.

Sie illustrieren ebenfalls die Übertragung von Verantwortung der genannten Akteure für das Verhalten von Nutzern und nehmen Ermittlungsbehörden und Justiz aus der Verantwortung. Wir halten mit Blick auf die Maßgaben des Rechtsstaats und der geteilten Verantwortung daher die Neudefinition bestehender Probleme durch digitale Technologien für nicht sinnvoll.

Fazit:
Deutschland ist – auch geprägt durch europäische Debatten – vor die Frage gestellt, wie es seine Digitalisierung weiter vorantreiben möchte. Derzeit bestehen sowohl auf gesetzlicher als auch auf organisatorischer und operativer Ebene Spannungsgefüge zwischen verschiedenen Interessen. Im Sinne eines offenen und resilienten Internets bzw. einer darauf ausgerichteten Internet-Governance sollte daher darauf geachtet werden, dass das Interesse der Allgemeinheit für sichere und vertrauenswürdige Dienste und Kommunikation immer Vorrang vor den Interessen individueller Akteure für den Zugang zu IT-Systemen oder Endgeräten haben sollte. Weiterhin sollten Behörden, die diese Sicherheit und Integrität sicherstellen und ggf. auch regulieren sollen, unabhängig agieren können und nicht in diesem Spannungsgefüge sich diametral gegenüberstehender Aufgaben agieren, da dies am Ende die Glaubwürdigkeit aller Akteure nachhaltig beschädigt.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 C

Stellungnahme
des Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI),
Herr Arne Schönbohm

zu den Anträgen der Fraktion der FDP (19/7698) „Digitalisierung ernst nehmen – IT-Sicherheit stärken", der Fraktion DIE LINKE (19/7705) „Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors" und der Fraktion BÜNDNIS 90/DIE GRÜNEN (19/1328) „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern"

im Rahmen der Öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 8. April 2019.

Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Bundestagsabgeordnete,

ich bedanke mich ganz herzlich für die Einladung als Sachverständiger und möchte nun gern auf einige Punkte der vorliegenden Anträge eingehen:

Die Anzahl und Qualität der Cyber-Angriffe auf staatliche und zivile Ziele nimmt eklatant zu. Auch die kritischen Infrastrukturen sind verstärkt im Fokus der Angreifer. Die hohe Dynamik bei der Weiterentwicklung von Schadprogrammen (ca. 390.000 neue Varianten pro Tag!) und Angriffswegen, die steigende Betroffenheit durch ein „Smart-Everything" sowie die zunehmende Angriffsintensität verdeutlicht die Verletzlichkeit von IT-Systemen und digitalen Infrastrukturen in einer zunehmend vernetzen Welt. In Anbetracht der erhöhten Gefährdungslage und der zunehmenden Digitalisierung von Staat, Wirtschaft und Gesellschaft ist Informations- und Cyber-Sicherheit zur Voraussetzung für das Gelingen der Digitalisierung geworden. Wenn wir auch in Zukunft einen starken und sicheren Standort Deutschland haben wollen, müssen wir mehr in Informations- und Cyber-Sicherheit investieren. Auch der Staat muss im Bereich Cyber-Sicherheit verstärkt aktiv werden.

Als die nationale Cyber-Sicherheitsbehörde gestaltet das BSI auf der Basis seines gesetzlichen Auftrags Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Der auch im Koalitionsvertrag von CDU, CSU und SPD festgelegte geplante Ausbau des BSI sowie die Weiterentwicklung des IT-Sicherheitsgesetzes einschließlich neuer Befugnisse und Möglichkeiten des BSI zum Schutz der IT-Systeme des Bundes sind wichtige Schritte, die nun konsequent umgesetzt werden müssen. Das BSI, die einzige

Bundesbehörde mit klarem gesetzlichen Auftrag zur Cyber-Abwehr, muss angesichts der dynamischen Gefährdungslage auch in den kommenden Jahren weiterhin substantiell verstärkt werden. Die Gewährleistung von Cyber-Sicherheit als Voraussetzung für eine gelungene Digitalisierung erfordert eine ständige Überprüfung von Prozessen, Befugnissen und Zuständigkeiten. Das BSI soll als neutrale Beratungsstelle in Fragen der IT-Sicherheit für Bund, Länder, Unternehmen und Bürgerschaft gestärkt werden. Auch eine Ausweitung der präventiven Aufsichtsbefugnisse wird angestrebt: Unternehmen und Hersteller von IT-Produkten, die wie kritische Infrastrukturen von besonderem nationalen Interesse sind, sollen hierbei stärker in die Pflicht genommen werden.

Die zunehmende Digitalisierung bietet für den Einzelnen, die Gesellschaft als Ganzes sowie den Wirtschaftsstandort Deutschland viele Chancen. Den auch damit einhergehenden Herausforderungen muss proaktiv und verhältnismäßig begegnet werden. Sei es die Sicherheit unserer Smart-Home-Systeme, die in einem direkten Zusammenhang mit der physischen Sicherheit unserer Wohnung steht, oder die Gewährleistung des Verbraucherschutzes in der digitalen Welt. Durch die Stärkung präventiver Sicherheitsmaßnahmen sowie die geplante Einführung eines IT-Sicherheitskennzeichens werden Anwender künftig besser geschützt und Verbrauchern mehr Orientierung geboten. Diese Aufgaben übernimmt das BSI als die zentrale Stelle für Zertifizierung und Standardisierung.

Im Bereich der Künstlichen Intelligenz festigt das BSI seine Rolle als Thought Leader beispielsweise durch die Einrichtung des Kompetenzzentrums KI und bündelt darin die bereits vorhandene Expertise.
Gewonnene Erkenntnisse stellt das BSI in seiner Eigenschaft als neutrales Kompetenzzentrum für die IT-Sicherheit allen Ressorts zur Verfügung. Auf Grund dieser Querschnittsfunktion ist das BSI eine Behörde von besonderer Bedeutung. Auch künftig soll das BSI zentrale Anlaufstelle für alle Fragen der IT-Sicherheit in der Digitalisierung sein. Beispiele für die Unterstützung der Ressorts sind die IT-Sicherheitsberatung (aller Ressorts), die elektronische Gesundheitskarte (BMG), das Smart Meter (BMWi), sowie das Autonome Fahren (BMVI).

Durch seine integrierte Wertschöpfungskette der Cyber-Sicherheit identifiziert das BSI unter anderem mit Hilfe der Schadsoftware-Erkennungssysteme Angriffskampagnen und Lücken in bestehenden Systemen. Die daraus abgeleiteten Warnungen adressieren Bund, Länder, Kommunen, KRITIS-Betreiber, die Wirtschaft und die Bevölkerung. Im Jahr 2018 hat das BSI über

16 Millionen Warnmails an deutsche Netzbetreiber versendet, um auf Gefahrensituationen aufmerksam zu machen. Die gewonnenen Erkenntnisse fließen in die Zertifizierung und Zulassung neuer Produkte ein. Eine sachgerechte Aufgabenerledigung und damit die Gewährleistung und Stärkung der Cyber-Sicherheit der Bundesrepublik Deutschland kann nur im Rahmen der bestehenden Bündelung und Vernetzung von Cyber-Sicherheitsexpertise innerhalb des BSI erfolgen.

Das BSI hat eine gesamtgesellschaftliche Verantwortung inne. Dies spiegelt sich auch in den im Koalitionsvertrag neu festgelegten Aufgabenbereichen wie digitaler Verbraucherschutz, Beratung für Wirtschaft und KMUs, sowie Beratungs- und Unterstützungsangebote für die Länder wider. Letzteres ist essentiell, um einer Fragmentierung im Bereich Cyber-Sicherheit entgegenzuwirken. Für die Sicherheit der Bundesrepublik Deutschland und ihrer Länder besteht die gemeinsame Verantwortung, durchgehend ein qualitativ hohes, einheitliches und angemessenes Cyber-Sicherheitsniveau sicherzustellen. Dem BSI als tragende Säule der Cyber-Sicherheitsarchitektur in Deutschland kommt dabei eine zentrale Stellung und Verantwortung in Zusammenarbeit mit den Ländern zu. So konnten in den vergangenen zwei Jahren bereits mit neun Bundesländern Absichtserklärungen für engere Kooperationen abgeschlossen werden. Auch der globalen Herausforderung Informationssicherheit stellt sich das BSI durch aktive Mitarbeit in Gremien sowie durch bi- und multilaterale Zusammenarbeit mit anderen Staaten. Das BSI übernimmt für die Bundesrepublik zahlreiche Rollen und Funktionen auch bei EU und NATO.

Die Stärkung der Cyber-Sicherheit in Deutschland erfordert zudem einen ganzheitlichen Ansatz, der die verschiedenen Gefährdungen im Cyberraum wie Spionage, Ausspähungen, Terrorismus und Cyber-Crime zusammenführt. Vor diesem Hintergrund soll die operative Zusammenarbeit aller im nationalen Cyber-Abwehrzentrum beteiligten Behörden weiter optimiert sowie Schutz- und Abwehrmaßnahmen besser koordiniert werden. Ziel ist ein noch schnellerer Informationsaustausch, damit einhergehende zügige Bewertungen sowie sich daraus ableitende konkrete Handlungsempfehlungen.

Letzten Endes sind robuste und vertrauenswürdige Netzinfrastrukturen wie 5G Grundlage der Digitalisierung in Deutschland. Gemeinsames Ziel aller beteiligten Akteure ist eine sichere Infrastruktur für den Mobilfunk der Zukunft, wobei Sicherheitseigenschaften der verschiedenen

Netzbereiche herstellerneutral gestaltet und die Sicherheit des Gesamtnetzes somit unabhängig vom jeweiligen Hersteller gewährleistet werden kann.

Der Deutsche Bundestag hat das BSI in den Haushalten 2018 und 2019 bereits mit einer großen Zahl an neuen Stellen ausgestaltet – dafür herzlichen Dank.
Die Gewährleistung und Verbesserung der IT-Sicherheit der Bundesrepublik Deutschland ist eine gesamtgesellschaftliche Aufgabe. Zur Realisierung dessen benötigen sowohl Unternehmen als auch Behörden qualifiziertes und motiviertes Personal. Als beliebtester Arbeitgeber im öffentlichen Dienst für IT-Absolventen gelingt dem BSI nach wie vor, geeignete Fachkräfte anzuwerben, dies verdeutlicht auch unsere Besetzungsquote von 95 Prozent zu Ende 2018.

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich auf Ihre Fragen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)255 D

Stellungnahme

Dr. Aleksandra Sowa
Datenschutzbeauftragte, Datenschutzauditor in und Buchautorin, u. a. „Digital Politics“

zu den Anträgen der Fraktion DIE LINKE (19/7705) „Umsetzung effektiver Maßnahmen für digitale Sicherheit statt Backdoors“ der Fraktion der FDP (19/7698) „Digitalisierung ernst nehmen – IT-Sicherheit stärken“ und der Fraktion BÜNDNIS 90/DIE GRÜNEN (19/1328) „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern“.

im Rahmen der Öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 8. April 2019.

Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Bundestagsabgeordnete,

ich bedanke mich für die Einladung als Sachverständi ge und möchte zu den o. g. Anträgen wie folgt Stellung beziehen:

IT-Sicherheit stärken, Freiheit erhalten, Privatsphäre stärken, effektive Maßnahmen einführen, hinreichende Ressourcen bereitstellen, Ende -zu-Ende-Verschlüsselung als Recht gewährleisten: Tolle Anträge mit guten Ideen, Lösungsansätzen und Vorschlägen, wie man IT -Sicherheit – diese „Achillesferse des Informationszeitalters“ [1] – in Deutschland und Europa stärken solle.

Vielen Dank dafür.

Ein Déjà-vu-Effekt setzt dennoch ein: B ackdoor, Recht auf Verschlüsselung, Hackbacks und die Rolle der Bundeswehr bei all dem, Cyber-Abwehr und die Ausgründung (oder Neugründung) einer unabhängigen Behörde mit Zuständigkeit Digitales u nd/oder IT-Sicherheit, Überwachungs-Software und ihre Exporte – all das ist schon einmal da gewesen. Oder gar mehrmals. Seit mehr als 20 Jahren wird debattiert, Argumente und Gegenargumente werden ausgetauscht, Experten angehört und Lösungen vorgeschlagen: ob im Virtuellen Ortsverein, der Möglichkeiten des Internets für die politische Arbeit erproben wollte, in der Enquete -Kommission, ob anlässlich der Beinahe-Verhaftung von Phil Zimmermann, Erfinder von Pretty Good Privacy, PGP, wegen illegaler Exporte von Verschlüsselungs -Software, zu den Stellungnahmen namhafter Kryptologen und IT -Sicherheitsexperten zu Backdoor (u. a. mit dem Paper: *Keys und Doormats*[2]) oder zuletzt anlässlich des Widerstandes von Apple, den US -Behörden Zugriff auf das iPhone des San-Bernardino-Attentäters einzuräumen.

Das Ziel des Krieges sei Sieg – und nicht die Fortsetzung von Kriegsoperationen, klärte Sun Tzu auf. Um es mit dem chinesischen Krieg sherrn zu halten:

Der Bundestag wird endlich entscheiden müssen!

Denn dafür, wo Deutschland in den nächsten Jahren zu dem wichtigsten Thema steht, egal , ob es um Digitalisierung, Industrie 4.0 oder lernende Algorithmen und Künstliche Intelligenz geht – dafür, wie sich Deutschland zu dem Thema IT-Sicherheit positioniert, wird der Gesetzgeber verantwortlich sein.

[1] BT Drs 19/7698, S. 1.
[2] https://www.schneier.com/academic/paperfiles/paper -keys-under-doormats-CSAIL.pdf (7.7.2015).

1. „Anonymes Surfen – das brauche man nicht in einer Demokratie“, erklärte der Innensekretär Günter Krings der *Süddeutsche Zeitung*[3] . Das Gegenteil davon ist richtig: Gerade in einem freien Land, in einer Demokratie, braucht man Anonymität im Internet – nicht weniger als im Allgemeinen. Nicht ohne Grund sind die Wahlen in einer Demokratie anonym. Anonymität – ob in trauter Heimarbeit oder mit hilfe moderner Technologien – darf kein Luxus sein. Anonymität ist legitim. Sie ist … vollkommen normal.

   Tatsächlich können Straftaten in Computernetzen „nur vermieden werden, wenn die Vertraulichkeit der Kommunikation mittels sicherer Verschlüsselung gewährleistet ist “[4]. Dies wurde bereits im Jahr 1998 im Schlussbericht der Enquete-Kommission festgehalten.

   Während es technisch und organisatorisch relativ einfach ist, kompatible, verschlüsselte E-Mail-Kommunikation in kleinen, autarken Organisationen wie Unternehmen oder Behörden zu implementieren, sind die Etablierung und Einführung von Lösungen, die ganze Gesellschaften umfassen, weit weniger trivial. Die von Phil Zimmermann erfundene Pretty Good Privacy (PGP) ist ein Beispiel für Technologie, die relativ verbreitet und relativ nutzerfreundlich sowie weitgehend kostenlos ist. Damit Technologien wie diese zum Masseneinsatz kommen, erfordert es Unterstützung und Förderung. Ja, es wird Geld kosten. Ja, es wird Förderung bedürfen. Und ja, Politik und Staat müssen beteiligt sein.

   Diese IT-Sicherheit, die Verschlüsselung, so liest und hört man, die Schaffung sicherer Kommunikationskanäle, der Integrität und Vertraulichkeit der Informationen – das alles kostet Geld und ist im Grunde genommen unnötig – und wenn etwas passiert, kann man immerhin eine Anzeige erstatten. Man lebe letztendlich in einem Rec htsstaat.

   So einfach verhält es sich nicht.

   Politik muss involviert sein, forderte der Silicon -Valley-Aktivist Mat Ceglowski. Politik muss involviert sein, um Lösungen wie Ende-zu-Ende-Verschlüsselung zu gewährleisten, die jedermann zugänglich sind – und auf die man vertrauen kann. Erstens muss die Prämi sse Privacy-as-a-Right und Security-as-a-Right heißen – und nicht etwa Privacy- oder Security-as-a-Service. Zweitens ist eine **konsequente** Positionierung hinsichtlich der Frage der Backdoors – Hintertüren – erforderlich:

   Die Fraktion der FDP fordert,
   „sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme auszusprechen;
   den Einsatz von sogenannten Backdoors zu verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken abzulehnen“ [5].
   Dies sind zweifelsohne gute Vorschläge. Möglicherweise aber nicht hinreichend: Sie schließen bspw. Unterbeauftragung u nd/oder Outsourcing an privatwirtschaftliche Organisationen/Unternehmen nicht aus.

[3] https://www.sueddeutsche.de/digital/tor -netzwerk-darknet-demokratie-1.4363329.
[4] BT Drs. 13/1104. 1998. Schlussbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft*) zum Thema Deutschlands Weg in die Informationsgesellschaft, http://dip21.bundestag.de/dip21/btd/13/110/1311004.pdf, S. 16 (172) .
[5] BT Drs. 19/5764.

Dezidierter:

Die Forderung der Fraktion DIE LINKE lautet, *„den Einsatz von Staatstrojanern zu unterbinden und Sicherheitslücken wie Backdoors oder Zero -Day-Exploits weder zu nutzen noch anzuschaffen“*[6].

Noch besser: deren Einsatz zu sanktionieren. Wie? Hierbei kann man sich von der DSGVO inspirieren lassen.

2. „Ist ein Land, in dem man nicht zwischen Tor und Bundestrojaner wählen darf, noch frei ?“, fragte einer der Internet-Diskussionsteilnehmer anlässlich des *SZ*-Statements von Günter Krings.

   IT-Sicherheit hilft zweifellos auch Kriminellen . Technologien wie Ende-zu-Ende-Verschlüsselung oder starke Kryptogra fie können gewiss auch Terroristen nutzen. Aber keine IT-Sicherheit bedeutet für alle Nichtkriminellen mehr Kriminalität. Insofern gefährdet ein Staat, der vermeintliche Sicherheit vor IT -Sicherheit setzt, seine Schutzfunktion gegenüber den Bürgern.

   Um des Weltfriedens willen ist es vermutlich viel wichtiger, sichere Plattformen für die Kommunikation zu besitzen, als wenn gelegentlich ein Krimineller nicht geschnappt werden kann. Im Fall eines begründeten Verdachts kann die Ermittlungsbehörde immer noch auf die Kommunikation des Verdächtigen zugreifen – im hinreichend begründeten Verdachtsfall und unter hinreichender Beachtung der Rechteabwägung.

   Auch wenn es im Einzelfall gute Gründe geben kann, eine (vorhandene) Hintertür zu nutzen , spricht aus der gesamtgesellschaftlichen Perspektive alles dagegen . Da wäre zuerst die Frage, für wen die Hintertüren geschaffen w erden sollten und wer (und wann) Zugriff darauf erhalten sollte. Nur für die Regierungen des Herstellerlandes? Oder sollen importierte Produkte mit Backdoors für die Sicherheitsbehörden des jeweiligen Importlandes ausgestattet werden? Wie stellt man sicher, dass der Zugriff auf Backdoors nicht weitergegeben wird? Der US-Sicherheitsguru Bruce Schneier konstatierte Folgendes: Wenn man Hintertüren einbaut oder für etwaige Gegenangriffe offenhält, sollte man dafür sorgen, dass nur die „guten Jungs“ sie nutzen, und zwar nur dann, wenn sie es sollen. Die Welt wäre allerdings viel sicherer, wenn es sie gar nicht gäbe. [7]

   Und da wir zwar im Informationszeitalter, aber zugleich auch in einer Ära sehr niedriger Effizienz der Regierungen leben, hätten Unternehmen zahlreiche Möglichkeiten, solch e nationalen Regulierungen zur Backdoor-Pflicht zu umgehen und bspw. ihren Standort nach Indien zu verlegen (die meisten Geräte werden ohnehin in Asien gefertigt, inklusive Software). Kunden würden ggf. den Erwerb nichtdeutscher Produkte vorziehen. Denn: Wer kauft schon gerne ein Produkt mit eingebauter Backdoor?

   Stattdessen fordert das B undeskriminalamt (B KA) wieder neue Gesetze: TOR, Darknet, „eigene Strafbarkeit“ für Administratoren und Moderatoren der als „illegal“ bezeichneten

[6] BT Drs. 19/7705.
[7] https://www.schneier.com/blog/archives/2011/10/fbi -sponsored_b.html (letzter Zugriff: 5.3.2018).

Plattformen etc.[8] Wer aber die IT-Sicherheit einer vermeintlichen Sicherheit opfert, erntet nicht Sicherheit, sondern Kriminalität. Mehr Kriminalität. Es ist bedauerlich, dass sich diese banale Erkenntnis auch nach über 20 Jahren der damaligen Enquete noch immer nicht als Allgemeingut durchgesetzt hat. Nichts daran ist falsch. Im Gegenteil. Auch aus diesem Grund ist die Herauslösung des BSI aus dem BMI in der Tat vordringlich – wie es zuvor die Herauslösung des BSI aus dem BND war.

3. Bisweilen erwecken das politische Sinnieren über den Cyber-Krieg und das Ersinnen fantastischer digitaler Gegenangriffsszenarien gegen Hacker aus fernen Ländern den Eindruck, von anderen, viel gewichtigeren Problemen abzulenken: „Zu lange hat die Bundesregierung die im Mittelpunkt stehenden Fragen der IT-Sicherheit der Selbstregulierung der Wirtschaft überlassen und eine Politik verfolgt, die die Interessen von Sicherheitsbehörden vor den effektiven Schutz von Grundrechten und sichere digitale Angebote stellt“[9], kritisiert die Fraktion Bündnis 90/Die Grünen in ihrem Antrag. Ein lässiger Umgang mit IT-Sicherheit, veraltete Technologien, keine Kontrollen und kaum Sanktionen gegen notorische Sicherheitssünder (vgl. u. a. § 14 BSIG[10]) sind das Ergebnis. Dass ein digitaler Gegenschlag im Notfall tatsächlich „wirken“ würde, ist noch nicht erwiesen, obwohl es auch darauf ankommt, welches Ergebnis die Bundesregierung als „wirksam“ bezeichnet.

   Unterschiedlich gehen die Fraktionen mit dem Problem der Attribution um:

   Die Fraktion BÜNDNIS 90/DIE GRÜNEN schlägt die Einrichtung einer unabhängigen Organisationseinheit zur „*Bewertung einer etwaigen Zurechenbarkeit von Angriffen* “ vor.

   Die Fraktion der FDP fordert: „*Die Bundesregierung soll […] die weitere Prüfung zur Schaffung einer rechtlichen Grundlage für Hack Backs umgehend einstellen .*“

   Die Forderung der Fraktion DIE LINKE geht am weitesten: Die Bundesregierung solle „*sogenannte Hackbacks durch staatliche Institutionen “* ausschließen und ächten.

   Statt Strategien für Kriege der Zukunft zu entwickeln, sollten Unternehmen und Behörden ihre Systeme und Netzwerke angemessen – gemäß dem Stand der Technik – absichern, in Firewalls und Perimeter-Sicherheit und in gut ausgebildete sowie erfahrene Spezial isten investieren, damit externe Angreifer nicht mehr mit gewohnter Nonchalance in die Systeme eindringen können. Und nicht auf den Hinweis der Geheimdienste warten, ob sie eventuell doch Opfer einer Cyber-Attacke geworden sind.

   Im Zeitalter sinkender Effektivität der Regierungen sind freiwillige Verpflichtungen kaum eine Alternative zu verpflichtenden Standards, Mindestanforderungen oder obligatorischen Zertifizierungen. An der Hochschule für Telekommunikation Leipzig (H fTL) arbeitet Frau Prof. Sabine Radomski an methodischen Grundlagen und einer Definition quantifizierbarer Qualitätsbegriffe für ein IT-Gütesiegel für Software-Sicherheit (Definition von objektiven, messbaren Indikatoren, Metriken) in Bezug auf die Sicherheit von Anfang an. Denn: Die Sache beginnt am Beginn.

---

[8] Vogt, Dr., Sabine 2017. „Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus“ der Kriminellen?“. In: Die Kriminalpolizei Nr. 2/2017, S. 4–7.

[9] BT-Drucksache 19/1328, Antrag *IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern.* 21.3.2018 (http://dipbt.bundestag.de/dip21/btd/19/013/1901328.pdf).

[10] BSI-Gesetz, https://www.buzer.de/gesetz/8987/a193775.htm (letzter Zugriff 3.5.2018).

Die steigende Komplexität der Systeme ist der größte Feind der Sicherheit. In einer aktuellen Studie der Gesellschaft für Informatik e. V., „*Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren* "[11], wurden zwei zentrale Methoden identifiziert, die die Transparenz algorithmischer Entscheidungen „signifikant erhöhen": Testing und Audit .[12] Damit diese effektiv eingesetzt werden können, fehlen noch ge eignete Standards, die den Bewertungen und Prüfungen zugrunde gelegt werden können. Neben den gesetzlichen Grundlagen, so das Ergebnis der Studie, fehlen an vielen Stellen Standards oder die konsequente Legitimation relevanter Instrumente wie Prüfungen, Te sts oder Zertifikate durch den Gesetzgeber.

Die Einführung genereller Meldepflichten[13] für Sicherheitsvorfälle nach dem Vorbild der DSGVO – für alle Branchen und Organisationen, unabhängig von der Größe und ob der Vorfall einmalig ist – ist sehr interessant und kann als eine Ergänzung detektiver IT-Sicherheit für u. a. bessere Transparenz dienen – wobei Transparenz hier als eine notwendige Bedingung der Prüfbarkeit und Kontrolle gesehen wird.

Fazit:

Ein „schlüssiges Konzept einer einheitlichen Strategie für mehr digitale Sicherheit" [14] wird im Antrag der Fraktion DIE LINKE gefordert. Tatsächlich verhält es sich mit den Vorschlägen und Lösungsansätzen zur IT-Sicherheit ein wenig wie in dem Dürrenmattschen Hörspiel *Herkules und der Stall des Augias:*

EINE STIMME:
Bilden wir eine Oberkommission!
ALLE:
Beschlossen schon: Wir bilden eine Oberkommission! [15]

Digitalministerium, ZITIS, CAZ, BSI, Ausgründung oder Neugründung, Zentralisierung der Kompetenzen kontra Dezentralisierung, mit mehr oder weniger Kompetenzen und Ressourcen – der Bundestag wird eine grundsätzliche Entscheidung treffen müssen: Möchte man weiterhin Technologien fördern, die Überwachung, Lebens- und Arbeitskontrolle stärken – oder möchte man in Technologien investieren, die neue Lebens- und Arbeitsentwürfe ermöglichen, Freiheit und Demokratie stärken – und so seine Schutzfunktion gegenüber den Bürgern ausfüllen.

Dafür ist es notwendig, die richtige Perspektive zu wählen und die Strategie für IT-Sicherheit danach auszurichten. Wenn man beispielsweise die Sicherheit in einem selbstfahrenden Auto aus der Perspektive des Fahrers gestaltet, sieht das Ergebnis anders aus, als wenn man die Sicherheit aus der Perspektive der Fußgänger und/oder Radfahrer modelliert. Nichts anderes gilt für die IT-Sicherheit.

Der deutsche Politologe Thomas Meyer warnte davor, die tatsächlichen absoluten Grundrechte wie die Freiheit mit Rechten von instrumentellem Wert, wie etwa Sicherheit, zu verwechseln:

[11] Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e. V. (GI). 2018. Technische und rechtliche Betrachtungen algo rithmischer Entscheidungsverfahren (Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen). Berlin: Oktober 2018, S. 6.
[12] Ebenda, S. 7.
[13] Hanßen, H. und Sowa, A. 2018. „Meldepflichten nach DSG-VO, ITSiG und NIS-Richtlinie". In <*kes*> 4/2018 (36), S. 74–78.
[14] BT Drs. 19/7705.
[15] Dürrenmatt, F. 1964, „Herkules und der Sta ll des Augias" (4. Auflage), Arche Zürich, S. 47.

„Der relative Wert der Sicherheit verkehrt sich in eine substanzielle Gefahr, sobald er den Rang der wirklichen Grundrechte usurpiert oder gar diese übertreffen soll.“ [16]

[16] Meyer, T. 2013. „Falsche Sicherheit – Die Verwirrung der Begriffe“. In: *Neue Gesellschaft – Frankfurter Hefte* 9/2013, S. 14, http://www.frankfurter-hefte.de/upload/Archiv/2013/Heft_09/PDF/2013-09_meyer.pdf.