18. Wahlperiode

Deutscher Bundestag
1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Nur zur dienstlichen Verwendung

Stenografisches Protokoll
der 104. Sitzung
- endgültige Fassung* -

1. Untersuchungsausschuss
Berlin, den 23. Juni 2016, 11.30 Uhr
Paul-Löbe-Haus, Europasaal (4.900)
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Prof. Dr. Patrick Sensburg, MdB

Tagesordnung - Öffentliche Beweisaufnahme

Tagesordnungspunkt

* Hinweis:
Die Korrekturen der Zeugen Andreas Könen (Anlage 1) und Martin Schallbruch (Anlage 2) sind in das Protokoll eingearbeitet.

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Sensburg, Prof. Dr. Patrick Lindholz, Andrea Schipanski, Tankred	Marschall, Matern von Ostermann, Tim, Dr. Wendt, Marian
SPD	Flisek, Christian Mittag, Susanne	Zimmermann, Jens, Dr.
DIE LINKE.	Renner, Martina	Hahn, André, Dr.
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	Ströbele, Hans-Christian

Fraktionsmitarbeiter

CDU/CSU	Allers, Fried-Heye Bredow, Lippold von Fischer, Sebastian D. Puglisi, Livia
SPD	Ahlefeldt, Johannes von Dähne, Dr. Harald Heyer, Christian Olechnowicz, Christin Radau, Linda Schlucke, Lisa Wassermann, Friedrich Weiß, Benjamin
DIE LINKE.	Halbroth, Anneke Martin, Stephan Rom, Katja
BÜNDNIS 90/DIE GRÜNEN	Busold, Christian Kant, Martina Leopold, Nils Pohl, Jörn.

Beauftragte von Mitgliedern der Bundesregierung

Bundeskanzleramt	Jipp, Daniel Kämmerer, Marie Neist, Dennis Pabst, Daniel Pachabeyan, Maria Wolff, Philipp
Auswärtiges Amt	Lehmann, Uta
Bundesministerium der Justiz und für Verbraucherschutz	Unterlöhner, Ulrike, Dr.
Bundesministerium des Innern	Akmann, Torsten Beyer-Pollok, Markus Blidschun, Jürgen Arthur Brandt, Dr. Karsten Darge, Dr. Tobias Hofmann, Christian Hodouschek, Fabian Jurna, Tassilo Matthes, Thomas Meyer, Till Weiss, Jochen
Bundesministerium für Wirtschaft und Energie	Krüger, Philipp-Lennart
Bundesministerium für Verteidigung	Rauch, Rüdiger Theis, Björn
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Kremer, Dr. Bernd

(Beginn: 11.32 Uhr)

Vorsitzender Dr. Patrick Sensburg: Ich eröffne die 104. Sitzung des 1. Untersuchungsausschusses der 18. Wahlperiode.

Ich stelle fest: Die Öffentlichkeit ist hergestellt. Die Öffentlichkeit und die Vertreter der Presse darf ich an dieser Stelle ganz herzlich begrüßen, freue mich, dass Sie auch wieder - vermutlich an einem langen Tag - uns gewogen sind, gute Berichterstattungen aus diesem Ausschuss fabrizieren und uns immer schön begleiten. Seien Sie alle ganz herzlich gegrüßt!

Bevor ich zum eigentlichen Gegenstand der heutigen Sitzung komme, gestatten Sie mir einige Vorbemerkungen.

Ich mache das erst mal andersrum: Erst mal begrüße ich unseren Zeugen. Herr Könen, schön, dass Sie da sind! Ich mache das gleich noch mal, aber das ist ein so langer Text, bevor Sie begrüßt werden. Ich mache das jetzt erst mal vorab. Schön, dass Sie da sind! Ich freue mich, dass Sie diesem Ausschuss zur Verfügung stehen.

Bevor ich zum eigentlichen Gegenstand der heutigen Sitzung komme, gestatten Sie mir einige Vorbemerkungen.

Ton- und Bildaufnahmen sind während der öffentlichen Beweisaufnahme grundsätzlich nicht zulässig. Auch das Wort „grundsätzlich“ werden wir demnächst mal streichen: sind nicht zulässig. Punkt. Ein Verstoß gegen dieses Gebot kann nach dem Hausrecht des Bundestages nicht nur zu einem dauernden Ausschluss von den Sitzungen dieses Ausschusses sowie des ganzen Hauses führen, sondern gegebenenfalls auch strafrechtliche Konsequenzen nach sich ziehen.

Ich rufe den **einzigen Punkt der Tagesordnung** auf:

Zeugenvernehmung

- Andreas Könen
  (Beweisbeschluss Z-124)
- Martin Schallbruch
  (Beweisbeschluss Z-125)
- Dr. Burkhard Even
  (Beweisbeschluss Z-119)

Die Beweisbeschlüsse Z-124 und Z-125 stammen vom 12.05.2016 und der Beweisbeschluss Z-119 stammt vom 25.02.2016. Es wird Beweis erhoben zum Untersuchungsauftrag - Bundestagsdrucksache 18/843 - durch Vernehmung der Zeugen Herrn Könen, Vizepräsident des BSI, Herrn Schallbruch, ehemals BMI, und Herrn Dr. Even, BfV.

Zunächst werden die Zeugen Könen und Schallbruch hintereinander öffentlich vernommen. Im Anschluss findet dann, wenn Bedarf dazu besteht, eine nichtöffentliche Sitzung statt; die findet auf jeden Fall statt bezüglich des Zeugen Dr. Even. Und dann werden sich anschließen, wenn denn Bedarf aufgrund entsprechender Fragen besteht, die nichtöffentlichen, gegebenenfalls eingestuften Vernehmungen der Zeugen Könen und Schallbruch.

Vernehmung des Zeugen
Andreas Könen

Als Erstes begrüßen - und ich habe es ja gerade schon gemacht - darf ich unseren Zeugen Herrn Könen. Ich stelle fest: Der Zeuge ist ordnungsgemäß geladen worden. Herr Könen, Sie haben den Erhalt der Ladung am 14. Juni 2016 bestätigt. Und ich freue mich - ich sage es noch mal -, dass Sie dem Ausschuss für Fragen zur Verfügung stehen.

Einige Formalien habe ich mit Ihnen zu besprechen. Ich habe Sie darauf hinzuweisen, dass die Bundestagsverwaltung eine Tonbandaufnahme dieser Sitzung fertigt. Diese dient ausschließlich dem Zweck, die stenografische Protokollierung dieser Sitzung zu erleichtern.

Das erstellte Protokoll wird Ihnen dann nach Fertigstellung zugesandt. Sie haben dann zwei Wochen Zeit, mögliche Korrekturen oder Ergänzungen vorzunehmen, falls dies gewünscht ist. Die Tonbandaufzeichnung wird danach gelöscht. - Haben Sie hierzu Fragen?

Zeuge Andreas Könen: Herr Vorsitzender, nein, habe ich keine.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Vor Ihrer Anhörung habe ich Sie zunächst zu belehren. Sie sind als Zeuge geladen worden. Als Zeuge sind Sie verpflichtet, die Wahrheit zu sagen. Ihre Aussagen müssen richtig und vollständig sein. Sie dürfen nichts weglassen, was zur Sache gehört, und nichts hinzufügen, was der Wahrheit widerspricht.

Ich habe Sie außerdem auf die möglichen strafrechtlichen Folgen eines Verstoßes gegen diese Wahrheitspflicht hinzuweisen. Wer vor dem Untersuchungsausschuss uneidlich falsch aussagt, kann gemäß § 162 in Verbindung mit § 153 des Strafgesetzbuches mit Freiheitsstrafen von drei Monaten bis zu fünf Jahren oder Geldstrafen bestraft werden. Nach § 22 Absatz 2 des Untersuchungsausschussgesetzes können Sie die Auskunft auf solche Fragen verweigern, deren Beantwortung Sie selbst oder Angehörige im Sinne des § 52 Absatz 1 der Strafprozessordnung der Gefahr aussetzen würde, einer Untersuchung nach einem gesetzlich geordneten Verfahren ausgesetzt zu werden. Dies betrifft neben Verfahren wegen einer Straftat oder Ordnungswidrigkeit auch gegebenenfalls Disziplinarverfahren, wenn das in Betracht kommen sollte.

Sollten Teile Ihrer Aussage aus Gründen des Schutzes von Dienst-, Privat- oder Geschäftsgeheimnissen nur in einer nichtöffentlichen oder eingestuften Sitzung möglich sein, bitte ich Sie um einen Hinweis, damit der Ausschuss dann gegebenenfalls einen Beschluss nach § 14 oder § 15 des Untersuchungsausschussgesetzes fassen kann, also die Sitzung dann in nichtöffentlicher bzw. eingestufter Weise fortführen und Ihnen dann die Fragen stellen kann. - Haben Sie hierzu Fragen?

Zeuge Andreas Könen: Nein, ebenfalls nicht.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Nach diesen notwendigen Vorbemerkungen darf ich Ihnen kurz den Ablauf der heutigen Sitzung vorstellen. Eingangs habe ich Sie zur Person zu befragen. Zu Beginn der Vernehmung zur Sache haben Sie nach § 24 Absatz 4 des Untersuchungsausschussgesetzes Gelegenheit, zum Beweisthema im Zusammenhang vorzutragen, also ein sogenanntes Eingangsstatement abzugeben. Danach werde ich Sie befragen, und im Anschluss erhalten dann die Mitglieder des Ausschusses das Wort für ihre Fragen. Dies geschieht nach dem Stärkeverhältnis der Fraktionen, immer eine Fraktion nach der anderen. - Haben Sie hierzu Fragen?

Zeuge Andreas Könen: Nein.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Dann darf ich Sie nun bitten, sich dem Ausschuss mit Namen, Alter, Beruf und einer ladungsfähigen Anschrift vorzustellen.

Zeuge Andreas Könen: Andreas Könen, geboren am [redacted]1961, demzufolge 55 Jahre alt. Beruf: Diplom-Mathematiker. Zurzeit: Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik. Ladefähige Adresse ist eben die Anschrift genau dieses Bundesamtes: Godesberger Allee 185-187 in Bonn.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Und dann kommen wir jetzt zu dem, was ich gerade schon angekündigt hatte. Sie haben die Gelegenheit, jetzt zu Anfang der Befragung ein sogenanntes Eingangsstatement abzugeben, also zum Beweisgegenstand im Zusammenhang vorzutragen, wenn Sie dies wünschen. Wünschen Sie dies?

Zeuge Andreas Könen: Ja.

Vorsitzender Dr. Patrick Sensburg: Dann haben Sie jetzt das Wort, Herr Könen.

Zeuge Andreas Könen: Ja, sehr geehrter Herr Vorsitzender! Sehr geehrte Damen und Herren Abge-

ordnete! Zunächst möchte ich Ihnen für die Möglichkeit danken, mit einem Eingangsstatement beginnen zu können. Ich möchte Ihnen auch danken, wenn Sie Rücksicht nehmen, dass ich zwischendrin mal vielleicht meine Stimme ein wenig ölen muss. Es ist eine kleine Infektion, die das heute ausgerechnet etwas belastet.

Das Bundesamt für Sicherheit in der Informationstechnik, BSI, ist eine präventiv tätige Sicherheitsbehörde, die sich mit allen Aspekten der Informationssicherheit beschäftigt. Hierzu gehören seit der Gründung des Amtes die Beratung und Unterstützung zu IT-Sicherheit von IT-Infrastrukturen, die Evaluierung und Zertifizierung von IT-Sicherheitsprodukten sowie die Entwicklung und Zulassung von IT-Systemen für die Verarbeitung amtlich geheim gehaltener Informationen.

Wir identifizieren und verfolgen gemeinsam mit der Forschung Trends der IT und gestalten darauf aufbauend gemeinsam mit Wirtschaft und Verwaltung IT-Sicherheitsstandards wie etwa den IT-Grundschutz. Darüber hinaus beobachten wir fortlaufend die IT- und Cybersicherheitslage, detektieren, analysieren und bewerten Angriffe jeglicher Art, darunter oft auch ungewöhnliche, komplexe oder vermeintlich wenig praktikabel erscheinende Angriffsmethoden. Schließlich wehren wir Angriffe auf die IT- und Netzwerkinfrastruktur der Bundesverwaltung ab und kooperieren auf Basis des IT-Sicherheitsgesetzes zum gleichen Zweck auch mit den kritischen Infrastrukturen und vielen anderen Partnern.

Wie Sie wissen, hat sich die IT-Landschaft seit der Gründung des BSI im Jahre 1991 massiv verändert. IT ist mittlerweile in fast allen Geräten des täglichen Lebens zu finden, und bei diesem Trend der fortschreitenden Digitalisierung ist noch lange kein Ende in Sicht. Hinzu kommt eine zunehmende Vernetzung der Systeme, hier vor allem unter dem Stichwort „Internet of Things“. Die Vorteile, die wir als Nutzer solch moderner IT-Systeme haben, zum Beispiel bei der Nutzung unserer geliebten Smartphones zu jeder Zeit an jedem Ort, machen bereits deutlich, dass es kein Zurück geben wird. Wir werden uns daher weiter mit den Gefahren dieser Trends für die IT-Sicherheit beschäftigen müssen; denn gerade eine Kopplung solcher heterogener, zunehmend komplexerer Systeme erhöht die Angriffsfläche, die wir Angreifern bieten.

Lassen Sie mich daher im nächsten Abschnitt zunächst anhand von ausgewählten Beispielen die Bedrohungslage skizzieren, mit der wir im BSI tagtäglich konfrontiert werden:

Die zunehmende Verbreitung von IT-Systemen und die ständige Verbindung mit dem Internet erlaubt es Angreifern, massenhaft Systeme zu scannen und bei Verwundbarkeiten diese Systeme zu übernehmen. Wir beobachten auch bei den Regierungsnetzen eine Vielzahl solcher Scans und allgemeiner Eindringversuche. Während noch vor wenigen Jahren zum Beispiel Portscans und Zugriffsversuche auf einzelne Netzdienste als Angriffsvorbereitung oder sogar als Angriff klassifiziert wurden, wird dies mittlerweile als Hintergrundrauschen verstanden; es ist zum missliebigen Normalfall geworden.

Ein weiteres Massenphänomen ist die Verteilung von Schadsoftware per E-Mail. Dieser Angriffsweg führt nach wie vor die Rangliste an und scheint für Angreifer sehr erfolgversprechend zu sein. Als alternativer Ansatz werden Webseiten- oder Werbebanner-Anbieter im Internet so manipuliert, dass sie anschließend Schadsoftware an alle Besucher verteilen. Wir sprechen hier von Drive-by-Exploits, bei denen noch nicht einmal eine Interaktion des Nutzers erforderlich ist. Es werden automatisiert Schwachstellen im Browser ausgenutzt. Alleine zu diesen Masseninfektionen und möglicherweise für andere Angriffe zu missbrauchenden Systemen senden wir täglich circa 130 000 Mitteilungen an die betroffenen Stellen mit der Bitte um Bereinigung der Systeme bzw. Absicherung der angebotenen Dienste.

Solche Massenangriffe zielen meist auf arglose Nutzer, deren Rechner anschließend oft als Teil eines Botnetzes selbst zum unfreiwilligen Angreifer wird. Wenn man sich einzelne Fälle genauer ansieht, stellt man zudem fest, dass die eingesetzten Angriffswerkzeuge immer professioneller werden. Selbst ohne tiefgehende Kenntnisse ist

es Angreifern mittlerweile möglich, sich Schadsoftware mithilfe sogenannter Exploit-Kits zusammenzubauen. Diese Systeme erlauben mit hoher Modularisierung eine Anpassung an die jeweilige Landessprache des Opfers, lassen den Angreifer wählen, welche Systemkomponenten angegriffen werden sollen und auch was die Schadsoftware beim Opfer anrichten soll - zum Beispiel Bankdaten stehlen oder wichtige Daten des Opfers verschlüsseln. In Untergrundforen werden sogar Support-Dienstleistungen für den Einsatz dieser Systeme sowie Garantien für die Funktion und den Erfolg der Angriffe angeboten. Es sind ein hochprofessioneller Schattenmarkt und eine arbeitsteilige cyberkriminelle Szene entstanden, gegen die wir als BSI gemeinsam mit der Strafverfolgung und vor allem mit der IT-Sicherheitsindustrie präventiv und reaktiv vorgehen müssen.

Die höchste Komplexitätsstufe unter den Angriffsmethoden erreichen aber die sogenannten Advanced Persistent Threats, sogenannte APT. Unter Durchführung einer professionellen Umfelderkundung des Opfers - Stichwort: „Social Engineering“ -, einer Aufklärung der IT-Systeme und -Netze des Opfers sowie der Nutzung von dort vorhandenen Schwachstellen, idealerweise Zero-Day-Exploits, wird versucht, das Angriffsziel mit geeigneter Tarnung präzise zu attackieren und zunächst nachhaltig zu infizieren - Stichwort: „Persistenz“. Angriffe einer solchen Qualität können nur durch hochprofessionelle, technisch extrem versierte Experten ausgeführt werden, die zudem entsprechend organisiert und finanziert sind, etwa als Mitarbeiter von Nachrichtendiensten oder anderen staatlichen Institutionen. Zu APT-Angriffen auch auf deutsche Einrichtungen hat das BSI in jüngerer Vergangenheit mehrfach berichtet und zu deren Bewältigung beigetragen, wie Ihnen selbst bekannt ist.

Nach dieser Einführung zum BSI und zur Bedrohungslage möchte ich nun auf die Aufgabenwahrnehmung des BSI auf der Grundlage des BSI-Gesetzes von 1991 sowie seiner Novellierungen in den Jahren 2009 und 2015 zu sprechen kommen. Im BSI-Errichtungsgesetz von 1991 sind unter anderem folgende Aufgaben für das BSI formuliert: Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik, sowie Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen.

Kryptografische Algorithmen bilden einen wichtigen Grundbaustein für die Sicherheit von Informationstechnik. Die Vertraulichkeit sensibler oder eingestufter Daten ist nur durch den Einsatz von sicheren Verschlüsselungs- und Authentisierungsverfahren zu gewährleisten. Die Entwicklung und Bewertung solcher Verfahren ist seit Gründung des BSI eine seiner Kernkompetenzen. Es gibt eine Reihe von gut untersuchten kryptografischen Verfahren, die nach dem heutigen Stand der Technik als sehr sicher angesehen werden und international als Standard anerkannt sind. Das BSI macht in seinen technischen Richtlinien Empfehlungen bzw. Vorgaben für die Auswahl kryptografischer Verfahren auf Basis dieser Standards. Diese Empfehlungen halten auch einer Überprüfung im Lichte der Snowden-Veröffentlichungen stand. Dennoch unterlaufen bei der Implementierung dieser Verfahren immer wieder beim Hersteller Fehler in der Programmierung durch ungewollte Abstrahlung technischer Komponenten und andere Seitenkanäle, durch die konkrete Verschlüsselungsprodukte dann doch angreifbar werden. Das BSI nutzt zur Aufdeckung solcher Implementierungsfehler als wichtige Instrumente unter anderen die Schwachstellen- und die Seitenkanalanalyse, wie sie im Rahmen von Zertifizierungen nach Common Criteria durchgeführt werden.

Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen bilden bereits, wie erwähnt, seit der Gründung des BSI eine zweite Aufgabe. Mit der Erarbeitung von IT-Sicherheitsstandards, den darauf aufbauenden technischen Richtlinien sowie schließlich Evaluierungen und Zertifizierungen setzt das BSI Maßstäbe für die Qualitätsbewertung von Informationssicherheitsprodukten und -dienstleistungen. Insbesondere trägt das BSI auf diesem Wege dazu bei, den unbestimmten Rechtsbegriff des Standes der Technik zu präzisieren. Die Prüfungs- und Bewer-

tungsmaßstäbe des BSI adressieren dabei so unterschiedliche Bereiche der Informations-, Krypto- und Cybersicherheit wie Hard- und Softwareprodukte - hier: Common-Criteria-Zertifizierung -, Sicherheitsberatung, Auditierung und Pentesting - im Rahmen vor allen Dingen IT-Grundschutzzertifizierung -, Smart Metering und Telematikinfrastruktur, Kryptoprodukte im Rahmen des Geheimschutzes oder auch Geräte gemäß § 27 Absatz 3 TKÜV.

Dabei ist Zertifizierung kein geschützter einheitlicher Begriff, sondern unterliegt so unterschiedlichen Regularien wie BSI-Gesetz § 9, CCRA - das ist Common Criteria Recognition Agreement [sic!] -, ISO 27 000er-Reihe, VSA § 37, TKÜV § 27 oder EnWG. Die Aussagekraft des spezifischen Zertifikats ist dabei im Lichte der jeweiligen Vorschrift zu bewerten. Neben der Weiterentwicklung der gesetzlichen Grundlagen des BSI wurden die Aufgaben durch weitere grundlegende Beschlüsse der Bundesregierung erweitert oder konkretisiert. Hier sind vor allem der Nationale Plan für den Schutz der Informationstechnik [sic!], NPSI, 2005, sowie die beiden Umsetzungspläne für den Bund, 2007, und die kritischen Infrastrukturen, ebenfalls 2007, zu nennen. Über den NPSI wurden zum Beispiel auch die Errichtung des nationalen IT-Lagezentrums und des IT-Krisenreaktionszentrums im BSI initiiert.

Die Erkenntnisse des nationalen IT-Lagezentrums zur Gefährdungslage im Cyberraum in den Jahren 2005 bis 2009 beeinflussten maßgeblich die Novellierung des BSI-Gesetzes 2009. Mit dieser Novellierung erhielt das BSI zum ersten Mal auch operative Verantwortung für die Cybersicherheit der Regierungsnetze. Bereits zu diesem Zeitpunkt wurde eine Meldepflicht auf Bundesebene eingeführt, durch die das BSI als zentrale Meldestelle und IT-Lagezentrum alle relevanten Informationen über Vorfälle bei den Bundesbehörden erhält.

Mit der Cyber-Sicherheitsstrategie aus dem Jahre 2011 rücken Wirtschaft und Bundesländer für das BSI als Zielgruppen in den Fokus. Ergebnisse dieser Strategie sind unter anderem: die Allianz für Cyber-Sicherheit, ACS, zur Zusammenarbeit mit kleinen und mittleren Unternehmen, der Verwaltungs-CERT-Verbund im Rahmen des IT-Planungsrates oder die Einrichtung des Cyber-Abwehrzentrums als zentrale Koordinierungs- und Kooperationsplattform der mit Cybergefährdungen befassten Behörden. Grundlage für alle diese Initiativen ist die Beachtung der jeweiligen Rollen, Aufgaben, Zielsetzungen und - vor allem bei Behörden - Befugnisse der Beteiligten.

Mit dem Inkrafttreten des IT-Sicherheitsgesetzes im Juli vergangenen Jahres und der damit verbundenen Novellierung des BSI-Gesetzes erhielt das BSI nunmehr komplementär zu seinen Aufgaben für die IT-Sicherheit des Bundes Aufgaben und Befugnisse für die IT- und Cybersicherheit der kritischen Infrastrukturen. Dazu gehören, wie Ihnen bekannt, neben der Einführung von Mindeststandards der IT-Sicherheit vor allem auch eine Meldepflicht; insbesondere letztere Maßnahme wird das Ziel einer nationalen Cybersicherheitslage deutlich voranbringen.

Aufgrund der globalen Vernetzung und Digitalisierung ist internationale Zusammenarbeit für Informations-, Krypto- und Cybersicherheit unabdingbar. Für das BSI ist dies aber nicht neu. Ausgehend von den Aufgaben der Gründungszeit in den Bereichen Kryptografie und Zertifizierung, die ich ja bereits dargestellt habe, kooperiert das BSI seit 25 Jahren auf verschiedenen Ebenen mit internationalen Partnern: bilaterale und multilaterale Kooperationen nationaler IT- und Cybersicherheitsbehörden, bilaterale und multilaterale Kooperationen nationaler Computer Emergency Response Teams, sogenannter CERTs, multilaterale Kooperationen der Cybersicherheitsbehörden in der EU, multilaterale Kooperationen der Cybersicherheitsbehörden in der NATO.

Typische Beispiele für die ersten beiden Punkte sind etwa die Kooperationen mit der finnischen Regulierungsbehörde FICORA, die das finnische Regierungs-CERT betreibt, das niederländische National Cyber Security Centre, NCSC, oder die französische Agence nationale de la sécurité des systèmes d'information, also ANSSI, das US-amerikanische Department of Homeland Security, DHS, mit dem US-CERT und dem amerikanischen nationalen IT-Lagezentrum. Im Rahmen

von EU und NATO übernimmt das BSI jeweils im Auftrag des Bundesministeriums des Innern unter Mitwirkung des Bundesministeriums der Verteidigung die Rollen der National Communication Security Authority, NCSA, und National Cyber Defence Authority, NCDA. Im Rahmen dieser Rollen wirkt das BSI mit einer Vielzahl von EU- und NATO-Gremien zusammen. In der Rolle der National Communication Security Authority gestaltet das BSI als eine der technisch führenden Behörden die Eigensicherung der EU-Institutionen und NATO-Institutionen mit. Dies betrifft auch die Absicherung der Vertraulichkeit der Kommunikation bei NATO-Missionen und beim Afghanistan-Einsatz. Gleiches gilt für den Schutz des Cyberraums von EU und NATO in der Rolle „National Cyber Defence Authority“. In beiden Fällen führt diese starke deutsche Beteiligung auch zu einer Stärkung der deutschen Krypto- und Cybersicherheitsindustrie in den jeweiligen Märkten.

Auf US-amerikanischer Seite liegt die Rolle der NCSA bzw. NCDA bei der National Security Agency, NSA, und dort speziell beim Information Security [sic!] Directorate, IAD. Auf britischer Seite werden beide Rollen durch das Government Communications Headquarters, GCHQ, bzw. durch die Communications-Electronics Security Group, CESG, wahrgenommen. Beide direkten Ansprechpartner des BSI sind unmittelbarer Bestandteil des jeweiligen technischen Nachrichtendienstes. Diese Organisationsstruktur findet sich in nahezu allen angelsächsischen und skandinavischen Staaten. Im Zuge ihrer Aufgaben zur Gewährleitung der IT-, Kommunikations- und Cybersicherheit für die US-Streitkräfte und im Rahmen von NATO-Missionen einerseits und der Realisierung einer technisch-strategischen Aufklärung als Nachrichtendienst andererseits muss die NSA ihre zwei Missionen „Information Assurance“ und „Signals Intelligence“ unter einem Dach wahrnehmen. Aus deutscher Sicht führt dies zu einer fehlenden Trennung zwischen den Aufgaben beim Schutz von IT-Infrastrukturen im Gegensatz zur nachrichtendienstlichen Tätigkeit gegen IT-Infrastrukturen. Frankreich und Deutschland haben diese klare Trennung mit der Errichtung der ANSSI und des BSI umgesetzt. Das BSI und seine Mitarbeiter arbeiten im Rahmen ihrer Aufgaben natürlich dennoch mit NSA-IAD zusammen, sind sich der Problematik und notwendigen Abgrenzung deutlich bewusst und nehmen auch gerade deswegen aus Sicht der USA innerhalb von EU und NATO eine starke Position ein.

Meine verehrten Damen und Herren! Im nächsten Teil meines Eingangsstatements möchte ich nun auf die Analyse und Bewertung der Veröffentlichungen durch Edward Snowden durch das BSI zu sprechen kommen. Das BSI hat sich seit den ersten Veröffentlichungen im Juni 2013 kontinuierlich in technischer und sicherheitlicher Weise mit den Dokumenten auseinandergesetzt. Dabei stehen dem BSI nur Dokumente aus denselben öffentlichen Quellen, das heißt insbesondere aus den Medien und dem Internet, zur Verfügung wie der übrigen Öffentlichkeit auch. Hinsichtlich der Authentizität dieser Dokumente herrschen unterschiedliche Auffassungen. Letztlich spielen diese Auffassungen für die Aufgabenwahrnehmung im BSI keine Rolle, da die in den Dokumenten beschriebenen diversen nachrichtendienstlichen Methoden über weite Strecken technisch nachvollziehbar sind und damit reale Gefährdungen konstituieren. Diese Gefährdungen müssen daher in IT-sicherheitlichen Bewertungen in jedem Falle berücksichtigt werden, da diese Methoden nunmehr etwa auch durch Dritte angewendet werden könnten. Dennoch sprechen viele einzelne Indikatoren für eine grundsätzliche Authentizität der Snowden-Dokumente, wie zum Beispiel auch die Agenda meines Gespräches bei der NSA am 23. April 2013, das Sie aus meinen Anmerkungen zu den internationalen Aufgaben des BSI nun bereits einordnen können. Lassen Sie mich daher im Folgenden unsere Bewertung der Dokumente sprachlich ohne die durchgehende Verwendung von Konjunktiven jeweils so formulieren, als handele es sich um authentisches Material.

Die von Snowden veröffentlichten Dokumente beschreiben aus technischer und IT-sicherheitlicher Sicht im Wesentlichen drei Arten von nachrichtendienstlichen Aktivitäten. Erstens. Strategische Aufklärung in Kommunikations-

netzen, zum Beispiel unter dem Stichwort „Upstream“. Individualisierte Angriffe zum Zweiten, zum Beispiel unter dem Kürzel TAO, Tailored Access Operations. Drittens. Schwächung der Sicherheit von IKT-Systemen, zum Beispiel unter dem Stichwort „Bullrun“.

Die strategische Aufklärung umfasst aber alle nachrichtendienstlichen Maßnahmen, die auf passives Abgreifen von Kommunikation auf internationalen Kommunikationsstrecken oder an Kommunikationsknotenpunkten hinauslaufen. Die nachrichtendienstlichen Methoden hierzu waren auch bereits vorher bekannt und Teil der Gefährdungsbewertung des BSI. Die Aktivitäten der NSA in dieser Hinsicht überraschen allerdings hinsichtlich des mengenmäßigen Ausmaßes der Erfassung und hinsichtlich der Dichte der weltweit existierenden Erfassungspunkte. Die durch die strategische Aufklärung gewonnenen Daten werden mittels verschiedener Analysetools ausgewertet und relevante Inhalte herausgefiltert. Hier ist die enge und weitgehende Verknüpfung von Metadaten, also Verkehrsdaten, über viele verschiedene NSA-Programme hinweg auffallend. Die Ergebnisse werden offenbar gerade auch bei der Durchführung von individualisierten Angriffen weiter genutzt. Dies geschieht beispielsweise durch das direkte Abhören von Kommunikation; dort, wo Netzwerke etwa über Funkstrecken geführt werden, zum Beispiel WLAN, Richtfunk bei Mobilkommunikation oder Satellitenverkehre, sind Daten den klassischen Abhörangriffen ausgesetzt. Wir haben die hier deutlich werdenden Gefährdungen, insbesondere der mobilen Kommunikation, in einem ausführlichen Bericht dargestellt, der insbesondere auch die spezielle Situation in Berlin-Mitte berücksichtigt.

Die Abteilung „Tailored Access Operations“ der NSA hat unter anderem die Aufgabe, Endgeräte gezielt zu kompromittieren. Unter dem Begriff „Advanced Network Technology“, ANT, sind manipulierte Geräte aufgelistet und werden inklusive der Nennung der entstehenden Kosten den Mitarbeitern der NSA für die Konzeption von Angriffsoperationen angeboten. Diese Liste trägt daher im BSI den Namen „ANT-Katalog“. Im ANT-Katalog werden hochspezialisierte Formen technischer Manipulationen und Angriffe beschrieben, wie sie im BSI seit langen Jahren diskutiert werden und in vielen Fällen auch als technische Warnungen kommuniziert wurden. Man muss allerdings konstatieren, dass viele dieser Angriffsvarianten von uns und anderen Fachleuten bisher jedoch als unpraktikabel angesehen wurden. Hier haben uns die Veröffentlichungen verdeutlicht, dass wir in nachrichtendienstlichem Umfeld jederzeit mit unüblichen, teuren und vermeintlich unpraktikablen Vorgehensweisen rechnen müssen. Unsere Bereiche der Lauschabwehrprüfung und Hardwareanalyse haben sich bereits hierauf eingestellt.

Zu gezielten Schwächungen der Sicherheit von IKT-Systemen finden sich in den veröffentlichten Dokumenten Beispiele wie die Manipulation von IT-Komponenten, etwa die Manipulation spezifischer Router oder Firewalls aus dem ANT-Katalog, sowie zur grundsätzlichen Beeinflussung von IT und IT-Sicherheitsstandards.

Von besonderer Bedeutung ist aber in einer Gesamtwürdigung, dass die Maßnahmen der strategischen Aufklärung, die Cyberangriffsmethoden gegen individuelle Ziele und die Manipulationen von IT-Technologien technisch und operativ aufeinander abgestimmt sind. Damit sind auch die Gefährdungen, die sich aus den einzelnen Programmen ergeben, letztlich in einer übergreifenden Gefährdungslage zu würdigen und IT-Sicherheitsmaßnahmen entsprechend auszurichten.

Welche möglichen Schutzmaßnahmen hat das BSI aus diesen Erkenntnissen abgeleitet? Und was haben wir konkret unternommen?

Nach Bekanntwerden der Snowden-Veröffentlichungen haben wir unsere gesamten Aktivitäten speziell in der Prävention auf den Prüfstand gestellt. Ein Schutz vor strategischer Aufklärung kann vor allem durch einen umsichtigen Umgang mit persönlichen und beruflichen Daten erreicht werden. Insbesondere durch konsequente oder Ende-zu Ende-Verschlüsselung kann die Vertraulichkeit von Kommunikationsinhalten erreicht werden, durch konsequente Verschlüsselungen von gesamten Kommunikationsstrecken auch ein weitgehender Schutz von Verkehrsdaten. Aus diesem Grunde bieten wir bereits seit Jahren

Empfehlungen, technische Richtlinien, Hilfestellungen und Informationen zu Schutzmaßnahmen an. Wir wollen beispielsweise durch eine Grundverschlüsselung, wie sie zum Beispiel im Regierungsnetz umgesetzt ist, oder Aufklärungskampagnen, zum Beispiel über „BSI für Bürger“, den Schutz erhöhen. Ebenfalls zu nennen sind die BSI-Standards zu Internetsicherheit, die sogenannte ISi-Reihe, und der IT-Grundschutz, der in vielen Organisationen Anwendungen findet. Außerdem haben sich zum Beispiel die deutschen Internetprovider diesen Maßnahmen unter dem Stichwort „E-Mail made in Germany“ angeschlossen.

Zur Absicherung von Daten mit sehr hohem Schutzbedarf, wie zum Beispiel Verschlusssachen, aber auch für den nationalen Personalausweis oder zum Schutz von Daten im Smart Meter werden von uns durch die Entwicklung und den Schutz eigener Algorithmen bzw. eigener Parameter zu bekannten Verfahren zusätzliche Sicherungsebenen eingebaut.

In puncto Mobilfunksicherheit und Spionagebedrohung ist das BSI zum Beispiel für Berlin-Mitte bereits Ende der 90er-Jahre durch wiederholte Warnungen aktiv geworden. Es hat gemeinsam mit den anderen Sicherheitsbehörden Regierung und Parlament wiederholt auf die Spionagegefahr hingewiesen. Mit sicheren Mobiltelefonen und Tablets steht ein ständig wachsendes Angebot an modernen Kommunikationsgeräten zum Schutz der Vertraulichkeit der Kommunikation zur Verfügung. Die Nutzung von Inhouse-Mobilfunkanlagen reduziert die Gefahren des passiven und sogar teilweise des aktiven Abhörens. Wir haben Sofortmaßnahmen abgeleitet, aus denen das Maßnahmenpaket „Sichere Regierungskommunikation“ entstanden ist; dieses beinhaltet über die oben bereits dargestellten Maßnahmen zu Mobiltelefonie unter anderem die erneute Überprüfung der Kommunikationswege im Regierungsviertel, also auch die turnusmäßige Sensibilisierung und Beratung aller Mitarbeiter aller Bundesbehörden.

Meine verehrten Damen und Herren, wie Sie gehört haben, ist das BSI seit 25 Jahren zum Schutz der IT von Verwaltung, Wirtschaft und Bürgern aktiv. Dazu hat sich unsere Behörde seit ihrer Gründung kontinuierlich auf die aktuellen Trends und Entwicklungen in der Informationstechnik eingestellt. Wir haben Informations- und Cybersicherheit als essenzielle Grundlage der Nutzung moderner IT präventiv entwickelt und gefördert. Andererseits haben wir die Bedrohungslage analysiert, jeweils zeitnah gewarnt und die IT-Anwender mit geeigneten Maßnahmen unterstützt. Auch die Veröffentlichungen von Herrn Snowden gehen in diese Bedrohungslage ein, stellen aber dennoch, trotz aller erzeugten Aufmerksamkeit, nur einen Ausschnitt dar.

Um den Schutz für unsere digitalen Infrastrukturen auch zukünftig gewährleisten zu können, möchte ich angesichts der vielfältigen Gefährdungen folgende Grundforderungen in den Raum stellen: Erstens. Förderung vertrauenswürdiger IT und vertrauenswürdiger Hersteller und Anbieter, vor allem für IT-Sicherheitsprodukte und -dienstleistungen. Zweitens. Entwicklung und Implementierung von Cybersicherheitsstandards auf nationaler und europäischer Ebene für alle Felder der Digitalisierung. Drittens. Erstellung einer umfassenden nationalen Cybersicherheitslage durch das BSI, die Sicherheitsbehörden und die Internetwirtschaft. Viertens. Verbesserung der Detektion und Abwehr von Cyberangriffen.

Unser Ziel muss sein, diese Forderungen im kooperativen Ansatz mit IT-Herstellern, -Dienstleistern und -Nutzern umzusetzen, um auch in Zukunft gut auf die Bedrohungslage eingestellt zu sein. - Ich danke für Ihre Aufmerksamkeit.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Herr Könen. - Zumindest was meine Überlegungen zur Frage betrifft, haben Sie unheimlich viel schon in Ihrem Eingangsstatement angesprochen. Meistens ist es ja so, dass man dann trotzdem wieder alle Fragen noch mal stellt. Das probiere ich jetzt zu vermeiden.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Gib doch gleich an die Opposition weiter!)

- Nein. Wenn, würde ich an alle Fraktionen weitergeben, nicht nur an die Opposition. - Ich habe aber ein paar Fragen. Das mache ich regelmäßig so ein bisschen, um Sie noch als Person näher kennenzulernen und den Werdegang. Wir wissen dann, was wir besser fragen können.

Sie haben gesagt, Sie sind Mathematiker; dann stellen wir in der Regel nicht so juristische Fragen. Wenn Sie Jurist sind, ist das hier manchmal ein kleines Staatsexamen. Also von daher kommen so ein paar Fragen sicherlich noch mal zur Vita und zu Ihrem Werdegang. Und ich habe ein paar Punkte - das wird den Kolleginnen und Kollegen sicherlich auch so gehen -, wo ich gerne noch mal in die Tiefe gehen würde.

Einmal zum Werdegang: Sie haben gesagt, Sie haben Mathematik studiert. Nach dem Studium haben Sie dann was gemacht?

Zeuge Andreas Könen: Nach dem Studium habe ich zunächst einmal meinen Wehrdienst abgeleistet. Und nach dem Wehrdienst habe ich dann am 1. Dezember 1988 bei der Zentralstelle für das Chiffrierwesen begonnen; das ist eine Unterabteilung des Bundesnachrichtendienstes, aus der dann eine andere Unterabteilung des Bundesnachrichtendienstes und dann auch - vor allen Dingen personell - der erste Stamm des Bundesamtes für Sicherheit in der Informationstechnik hervorgegangen ist.

Vorsitzender Dr. Patrick Sensburg: Von welchem Jahr reden wir da ungefähr?

Zeuge Andreas Könen: 1988, 1. Dezember.

Vorsitzender Dr. Patrick Sensburg: Genau. Das ist ja da die Gesamtbildung auch vom BSI gewesen ganz allgemein.

Zeuge Andreas Könen: Ja.

Vorsitzender Dr. Patrick Sensburg: Okay. - Im BSI, wie sind Sie da gestartet dann? Also Sie in Person, was haben Sie da gemacht? Also nicht … (akustisch unverständlich)

Zeuge Andreas Könen: Im BSI selber habe ich am 1. Oktober 2006 begonnen als Leiter des dortigen Leitungsstabes. Das habe ich dann über drei Jahre hinweg ungefähr gemacht, um dann im Februar 2009 den Fachbereich „Sicherheit in Kritischen Infrastrukturen und in Anwendungen“ zu übernehmen. Durch eine Umorganisation bin ich dann Fachbereichsleiter für „Koordination und Steuerung“ geworden; das war Mitte Juli 2011. Mit der Übernahme der Abteilungsleitung „Beratung und Unterstützung“ im Dezember 2011 setzte ich dann die Laufbahn innerhalb des BSI fort, und schließlich und endlich am 1. Januar 2013 habe ich die Position des Vizepräsidenten übernommen, die ich ja bis heute einnehme.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Jetzt werden Sie ja heute zu dem Themenkomplex befragt, der Gegenstand unseres Untersuchungsauftrages ist. Und wir haben gehört, dass zum Themenkomplex BSI rund 100 Ordner an betreffenden Beweismaterialien zur Verfügung gestellt sein sollen, ungefähr. Haben Sie sich zur heutigen Sitzung vorbereitet mit diesen Dokumenten? Oder wie haben Sie sich vorbereitet?

Zeuge Andreas Könen: Ja, ich habe mich in der Tat noch einmal mit den Dokumenten beschäftigt, dann insbesondere auch mit den zeitlichen Abläufen, die aus diesen Dokumenten heraus deutlich werden für verschiedene der Themen, die ich auch schon angesprochen habe innerhalb meines Eingangsstatements, und dann basierend auf dem und meiner persönlichen Erfahrung im BSI das Eingangsstatement verfasst.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich glaube, so haben es die meisten Zeugen auch gemacht, wenn ich das richtig sehe.

Sie hatten gesagt, dass nach alledem, was Sie bewerten können - - und Sie müssen nicht jedes Dokument mit jedem Punkt prüfen, sondern Sie prüfen, ich sage mal, Relevanz und vielleicht Gefährdungswahrscheinlichkeiten. Sie haben gesagt, dass die Dokumente, die insbesondere zur Deutschland-Akte von Edward Snowden gehören, aus Ihrer Sicht authentisch sind. Habe ich das richtig wiedergegeben?

Zeuge Andreas Könen: Ja. Die Dokumente sind auf jeden Fall in dem Sinne authentisch, dass sie realisierbare technische Maßnahmen darstellen, realisierbare technische Angriffe, Cyberangriffe und Ähnliches. Das ist der Schluss, zu dem die Analyse unserer Mitarbeiter gekommen ist.

Vorsitzender Dr. Patrick Sensburg: Auf welchen Erkenntnissen und Analysen im Konkreten bezieht sich das? Wie kommen die da drauf? Uns hat zum Beispiel ein anderer Zeuge mal gesagt, das eine Dokument wäre gar kein Originaldokument; das wäre abgetippt von einem Zeitungsjournalisten, einem Redakteur. Da kann man gar nichts machen. Auch der Generalbundesanwalt hat ja seine Ermittlungen eingestellt. Wieso sagen Sie jetzt: „Das ist authentisch“?

Zeuge Andreas Könen: Also, ich sage: Es ist eben authentisch in dem, was an technischen Angriffsmethoden sichtbar wird. Es ist nachvollziehbar, dass diese technischen Angriffsmethoden so durchführbar sind, und es gibt einige Fälle, in denen wir das auch technisch nachvollzogen haben. Wir haben es - auf gut Deutsch - nachgebaut an der Stelle und haben gesehen: Das kann man genau so durchführen, wie es da steht. - Das ist mindestens das Stichwort der technischen Authentizität. Was jedes einzelne Dokument und eine, sagen wir, Authentizität und Unverfälschtheit vom vermuteten Ursprung in irgendeiner NSA-Datenbank über den Weg, den es da in die Hände man weiß ja nicht welcher Leute genommen hat - - und wie Herr Snowden da Dokumente mitgenommen hat, welche Veränderungen dann im Zuge an solchen Dokumenten stattgefunden haben oder ob das, was dann am Ende veröffentlicht wird, in Teilen vielleicht auch Abschriften aus Dokumenten sind, das ist im Einzelnen sehr, sehr schwer nachzuvollziehen. Aber wie ich sagte: Das ist für das BSI nicht der entscheidende Punkt. Es kommt immer auf die Plausibilität dessen an, was dort an Angriff deutlich wird.

Vorsitzender Dr. Patrick Sensburg: Okay. - Also, da ist die Sichtweise einfach eine andere, als wenn man es vergleicht mit dem Generalbundesanwalt, der dann im Endeffekt persönliche Vorwerfbarkeit und Schuld für eine Tat einer Person ermitteln muss. Und bei Ihnen ist es die Plausibilität für eine Gefährdungssituation.

Zeuge Andreas Könen: Ja.

Vorsitzender Dr. Patrick Sensburg: Okay.

Zeuge Andreas Könen: Das einordnen zu können in technische Infrastrukturen, die technische Realisierung im Einzelnen anzuschauen.

Vorsitzender Dr. Patrick Sensburg: Und dann treffen Sie Ihre Maßnahmen oder Empfehlungen.

Zeuge Andreas Könen: Korrekt.

Vorsitzender Dr. Patrick Sensburg: Okay. - Welche Maßnahmen und Empfehlungen haben Sie dann aufgrund dieser Plausibilitätseinschätzung getroffen? Also, was hat das erreicht? Was haben wir im positiven Sinne durch die Veröffentlichungen von Edward Snowden jetzt an Neuerungen?

Zeuge Andreas Könen: Also, vieles habe ich davon ja im Eingangsstatement schon einmal aufgeworfen. Wenn wir noch einmal durch die Hauptangriffsfaktoren durchgehen - eben die strategische Aufklärung auf der einen Seite -, dann haben wir erreicht, dass wir in vielen Nutzungsbereichen, da, wo wir kommunizieren, da, wo wir Daten ablegen auf technischen Geräten, jetzt erstens deutlich sensibler geworden sind, was wir da tun und unter welchem fremden Zugriff das gegebenenfalls geschehen mag oder kommuniziert wird. Entscheidend ist dann auch, entsprechende Verschlüsselungsmaßnahmen ins Feld zu bringen, wenn es um die Vertraulichkeit geht. Da hatte ich bereits erwähnt die Initiativen, die daraus entstanden sind, nicht unbedingt im Bereich der Bundesregierung alleine, sondern - das ist wichtig - auch draußen in der Wirtschaft; das war „E-Mail made in Germany“ auf der einen Seite, das ist aber auch zum Beispiel das, was am Institut von Professor Waidner im Moment mit der Volksverschlüsselung entwickelt wird und das wir sehr intensiv, auch fachtechnisch, begleiten. Das sind dann am Ende auch die Maßnahmen der Verschlüsselung in den Regierungsnetzen, die

wir weiter ausbauen, mehr Behörden in die zentralen Netze der Bundesregierung hineinbringen.

Dann gibt es vor allen Dingen die ganzen Fragestellungen der Cyberangriffe; das ist ja etwas, was wir hier im Parlament an verschiedensten Stellen in Ausschüssen und in anderen Bezügen diskutiert haben: sich mit Cybersicherheitsmaßnahmen genau auf erstens die Detektion von Angriffen auch einzustellen, herauszufinden, dass man unter einer Attacke steht, daraus wieder zu lernen, welche Präventionsmaßnahmen man in Netzen einbauen muss - nicht nur der Regierung, sondern wir geben diese Methoden, wie man das tut, dann auch an die Wirtschaft weiter, insbesondere da, wo dann Telekommunikationsprovider querschnittlich für die gesamte Bevölkerung dann wirken können - - und schließlich und endlich im dritten Bereich, da, wo es um Informationssicherheitsprodukte geht: dass wir noch schärfer darauf schauen, wie diese Produkte gestaltet sind, wie der Hersteller seine Komponenten bezieht, ob er selber vertrauenswürdig ist und ob er dann in der Produktion seiner Geräte letztlich oder Dienstleistungen auch wirklich Komponenten hergibt, die ebenfalls vertrauenswürdig sind, nachvollziehbar, prüfbar sind. Das sind entscheidende Weiterentwicklungen, die wir dann in sehr, sehr vielen Bereichen einfließen lassen.

Es hat also im Grunde grundsätzliche neue Aufstellungen gebracht, es hat strategische Maßnahmen gebracht, und es hat ganz konkrete Schlussfolgerungen gehabt, insbesondere auch im Blick auf die Mobilkommunikation Berlin-Mitte.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Das deckt sich übrigens - ich weiß nicht, ob Sie es in den Protokollen nachvollzogen haben - auch sehr mit den Ausführungen der Experten, die zu den technischen Anforderungen und möglicherweise Forderungen - nicht nur Anforderungen - auch Stellung genommen haben, und dem Wunschkatalog, den wir ihnen abgefragt haben. Also, das deckt sich nach meiner Erinnerung sehr.

Ich habe eine Frage, die sich aus den Zeugenaussagen einiger Zeugen im Vorfeld ergeben hat; da ging es um den Schutz deutscher Kommunikation. Ist es so, dass das BSI die Kommunikation schützt innerhalb der territorialen Grenzen und nicht außerhalb der territorialen Grenzen?

Zeuge Andreas Könen: Also, in einer direkten Wirkung schützt das BSI natürlich unmittelbar die Kommunikation des Bundes, sprich: der Bundesverwaltung; da tun wir exakt das. Wir leiten erstens die Kommunikation über nationale IT-Infrastrukturen und nationale Netzinfrastrukturen, und dort können wir natürlich mit dem jeweiligen Auftragnehmer zusammen den Schutz besonders gut gewährleisten. Da, wo die Kommunikation die Grenzen Deutschlands verlässt, ist es immer noch dann gut, wenn das Kommunikationsequipment, das etwa Bedienstete des Bundes mitführen oder alle anderen, die sich schützen wollen, mitgenommen und genutzt wird. Allerdings muss man klar sagen, dass natürlich auch die direkten Wirkmöglichkeiten des BSI an nationalen Grenzen enden. Aber - dazu bin ich ja auch auf die Kooperationen mit EU und NATO eingegangen - nach meiner Meinung können wir uns in der EU etwa nur wirklich effektiv schützen, wenn wir auch da das gleiche Verständnis von den Sicherheitsmaßnahmen entwickeln, die wir da brauchen. Mit der NIS-Richtlinie ist das jetzt in Teilen für die kritischen Infrastrukturen gegeben, aber da kann ich mir klar mehr vorstellen.

Vorsitzender Dr. Patrick Sensburg: Jetzt noch mal im Konkreten, nicht bezogen auf Regierung etc., sondern auf die Bürgerinnen und Bürger: Wie ist das, wenn ein ausländischer Dienst an der territorialen Grenze zu Deutschland aus dem Glasfasernetz, aus dem Kabel Kommunikation absaugt und da drin ist auch deutsche Kommunikation? Kümmert sich da irgendwer drum? Ist das Sache des BND, des Verfassungsschutzes? Ist ja leider außerhalb Deutschlands. Macht sich das BSI da Gedanken drüber? Also, wer macht sich Gedanken drüber, ob Kommunikation sicher ist oder gegebenenfalls von Dritten außerhalb der territorialen Grenzen abgefangen wird?

Zeuge Andreas Könen: An der Stelle, wo es um zunächst mal das geht, was mir nahe liegt, nämlich das, was das BSI dafür tun kann aus Aufgaben und Befugnissen heraus, ist es so, wie ich

dargestellt habe: Wir müssen dafür sorgen, dass erstens die Personen, die so kommunizieren, sensibilisiert sind und möglichst auch mit entsprechender Software zur Verschlüsselung oder mit Gerät zur Verschlüsselung ausgestattet sind; das ist klar. Wir sind natürlich auch darauf angewiesen - etwa als BSI -, um in der Cyber-Sicherheitslage präzise Aussagen zu treffen, über Deutschland hinaus zu schauen. Wir brauchen Informationen, wie Nachrichtendienste oder auch vor allen Dingen Kriminelle auf Informationen einwirken. Das ist aus meiner Sicht dann eine Aufgabe, die nur durch den Bundesnachrichtendienst erfolgen kann; nur er hat das Instrumentarium, um auch genau diese cybersicherheitlich relevanten Gefährdungen zu detektieren und auch in der Kooperation mit anderen ausländischen Behörden diese Information bereitzustellen und dann natürlich in geeigneter Weise mit dem BSI so zu teilen, dass wir wieder weiter sensibilisieren können und all das machen können, was ich eben schon dargestellt habe. Aber da es sich auf das Ausland bezieht: klar eine Aufgabe des BND.

Vorsitzender Dr. Patrick Sensburg: Okay. - Angriffe in Deutschland. Sie haben ja die TAO genannt. Wie ist die Arbeitsverteilung da? Also sowohl beim direkten Ausforschen von Kommunikation - also das Handy, was konkret attackiert wird - oder beim allgemeinen Abschöpfen beispielsweise durch pfiffige Methoden an einem Knotenpunkt, wo alle sagen: „Das muss doch der Provider, der Betreiber sichern“, ist da irgendwie das BSI involviert? Wenn nicht, wissen Sie, wer da involviert ist?

Zeuge Andreas Könen: Also, um jetzt bei einem deutschen Provider Kommunikation abzusichern? Oder - -

Vorsitzender Dr. Patrick Sensburg: Beide Wege; ich sage mal, einmal der konkrete Angriff auf ein Endgerät - man könnte sich das Kanzlerhandy vorstellen - oder halt das Abgreifen von Daten zum Beispiel an einem Internetknotenpunkt. Da wird uns immer gern gesagt: Ja, das geht gar nicht. Der Betreiber hat da so einen hohen Sicherheitsstandard, den muss er auch gewährleisten. Wenn da irgendwie manipuliert würde, dann wird das sofort gemerkt; da gibt es tausend technische Gründe. - Lässt man es damit bewenden, dass man beispielsweise der Telekom unterstellt, das kriegt die alles raus als Betreiber? Oder irgendeine andere Firma könnte ich jetzt nehmen. Und wie sieht es aus mit dem Handy, zum Beispiel von der Bundeskanzlerin? Wer kümmert sich darum? Ist das ausschließlich der Verfassungsschutz? Ist da das BSI mit der technischen Expertise mit drin? Also, wie läuft da die Arbeitsverteilung? Wie funktioniert so was?

Zeuge Andreas Könen: Gut. Ja, unterscheiden wir zunächst vielleicht zwischen dem, was komplett in der Verantwortlichkeit der Provider liegt. Das ist natürlich das Netz, das die hier national und in der Verknüpfung zu internationalen Netzen aufstellen und anbieten. Da ist es ganz klar, dass die Pflichten, die insbesondere jetzt auch noch mal aus dem IT-Sicherheitsgesetz heraus verschärft worden sind - die gehören zu den kritischen Infrastrukturen - - dass die Sicherungspflichten dort ganz klar bei den Providern liegen und nach unserer Einschätzung da auch sehr weitgehend wahrgenommen werden. Es ist insbesondere aus unserer Erfahrung mit den Dienstleistern, die wir bei den Netzen des Bundes beschäftigen, so, dass da sehr hohe Sicherungsmaßstäbe eingerichtet werden, schon aus der Tatsache heraus, dass dort von den Kommunikationsprovidern ja im eigenen geschäftlichen Interesse erstens Verfügbarkeit gewährleistet werden muss, aber auch Vertraulichkeit, weil natürlich sich keiner der Provider leisten kann, unberechtigte Zugriffe auf dieses Netz zuzulassen. Die unterliegen ja auch an der Stelle sehr deutlichen gesetzlichen Verpflichtungen. Damit ist völlig klar, dass die dort alle eine sehr hohe Sensorik eingerichtet haben, ihre eigenen Netze in entsprechenden Lagezentren sehr genau anschauen, sehr genau und präzise untersuchen und checken, und eine Reihe dieser Provider dann ja auch Teile dieser Infrastruktur beim BSI entsprechend zertifizieren lassen. Wir haben ja etwa das Beispiel von DE-CIX gerade in der Diskussion gehabt; die haben exakt das wahrgenommen, und die sind der größte deutsche Knotenpunkt im Internet.

Darüber hinaus wurden dann Maßnahmen der Streckenverschlüsselung eingerichtet. Komplementär zu dem, was ich eben mit „E-Mail made in Germany“ bezeichnet habe, sind also Vereinbarungen zwischen deutschen Providern geschlossen worden, im Handshake-Verfahren die Kommunikation, die ohnehin innerhalb Deutschlands bleiben soll, dann auch in Tunnelverfahren wie SSL und Ähnlichem zu verschlüsseln. Dafür hat das BSI dann auch entsprechende technische Richtlinien bereitgestellt, um das vergleichbar zu machen.

Kommen wir jetzt zum Schutz von Einzelgeräten. Beim Schutz von Einzelgeräten kommen sehr viele Faktoren zusammen. Erstens, über welche Kommunikationsnetze wird kommuniziert? Für die festen Netze des Internets, des deutschen Teiles am Internet, und auch für die Mobilfunkinfrastruktur gilt ja das, was ich eben gesagt habe: Da ist in erster Linie in der Übertragung natürlich der jeweilige Provider verantwortlich, dass dort keine direkten Zugriffe geschehen.

Zum Zweiten ist es so, dass natürlich dann auf dem Endgerät eine besondere Situation beginnt. Da gibt es zunächst einmal den reinen Kommunikationsanteil, was so landläufig als GSM bezeichnet wird. Da waren in der Vergangenheit große Verbesserungen erforderlich, weil der dort eingerichtete Standard keinerlei Sicherheitsansprüchen - nach modernen Maßstäben von heute sowieso nicht - genügt. Das ist im Wesentlichen mit der Einführung von UMTS und den dort eingeführten neuen internationalen Standards sehr weitgehend geheilt worden. Darüber hinaus muss einem aber immer deutlich bleiben, dass etwa für die Verkehrsdaten dieser Übermittlung solch ein Schutz extrem schwierig wird, weil diese Verkehrsdaten natürlich exakt zu der Kommunikation und Signalisierung, wo diese Kommunikation hingehen muss, genutzt werden müssen, müssen also dem jeweils Berechtigten dann an den entsprechenden Knotenpunkten in offener Form vorliegen. Das ist praktisch mit den heutigen Methoden von Kommunikation nicht anders zu lösen.

Dann kommt das Endgerät selber ins Spiel. Das Endgerät selber stammt heute zu 100 Prozent aus nichtnationaler Produktion. Wir haben keine Produzenten etwa von Mobiltelefonen mehr. Das bedeutet also, in der verwendeten Hardware - und das ist ja auch immer wieder die große Sorge des BSI, wo wir geschützte Kommunikation über solche Geräte abwickeln müssen -, da muss zunächst einmal sehr gründlich hingeschaut werden. Das macht man für gängiges Markengerät natürlich nur dann, wenn entsprechende Sicherheitsvorschriften im Raum sind und wenn man entsprechende Zertifizierungen durchführt, die aber durchaus kostspielig sind und bei kurzlebigen Produkten für den Hersteller unrentabel sind.

Dann geht es weiter: Es geht zu dem, was an Betriebssystemen und Software auf diesen Geräten benutzt wird. All das ist in vielen Fällen sogar öffentlich zugänglich. Man nenne bloß das Beispiel Android. Android ist auf der einen Seite glücklicherweise ein offenes Betriebssystem, in dessen Konstruktion jeder hineinschauen kann. Aber wenn Sie sich genau anschauen, wie Android heute genutzt wird, dann bedeutet das, dass der Open-Source-Kern jeweils über ein sogenanntes Major Release - also, wenn da vorne „4.“-irgendwas steht und „5.“-irgendwas steht - konstant bleibt und damit alle Sicherheitslücken, die darin sind, erst gepatcht werden, wenn sie von „4.“-irgendwas nach „5.“-irgendwas gehen.

So, das heißt, das sind alles Probleme, die man in Betracht ziehen muss - - und dann noch nicht mal die Applikationssicherheit mit betrachtet habe, wo Sie dann auch WhatsApp nutzen oder - - Ich will hier niemanden an die Wand stellen, aber Sie können nennen, was Sie wollen, praktisch von den Applikationen: Jede dieser Applikationen birgt eigene Risiken wieder für Attacken in sich.

Das ist ein großes Spektrum, für das das BSI Empfehlungen bereitstellt, den Unternehmen da nahetritt, wo diese Empfehlungen deutlich missachtet werden und Schwachstellen offensichtlich werden. Im Zweifel warnen wir da auch, wenn keine Kooperation zustande kommt. Aber am Ende, da wo es etwa darauf ankommt, selber den Schutz zu gewährleisten als BSI, wenn es etwa um die sichere Mobilkommunikation der Behörden geht, dann kommt da das Thema Zulassung

ins Spiel, und dann kennen Sie das Problem selber: Was dann zur Verfügung steht, hat natürlich etwas weniger Usability, als man das gerne hätte.

Vorsitzender Dr. Patrick Sensburg: Wenn wir jetzt beim Ausland schon mal angekommen sind - - Frage: Mit welchen Behörden in den USA und in Großbritannien arbeiten Sie zusammen? Sie haben das ja auch schon eben im Eingangsstatement angerissen.

Zeuge Andreas Könen: Ja.

Vorsitzender Dr. Patrick Sensburg: Aber können Sie es etwas konkreter und vollzähliger machen?

Zeuge Andreas Könen: Ja. Um die Landschaft einfach noch mal zu skizzieren: Es ist so, dass dem Bundesministerium des Innern als Gegenüber das Department of Homeland Security gegenübersteht. Dort gibt es tatsächlich keine nachgeordnete Behörde, die direkt unmittelbar für IT-Sicherheit oder Cybersicherheit verantwortlich wäre. Das bedeutet, dass wir da in vielerlei Belangen direkt mit denen zusammenarbeiten, die im DHS - im Ministerium selber - da verantwortlich sind, die etwa für kritische Infrastrukturen die entsprechenden Direktiven geschrieben haben, die der Präsident der Vereinigten Staaten verabschiedet hat zur Sicherheit von kritischen Infrastrukturen. Wir arbeiten mit dem US-CERT zusammen vonseiten unseres nationalen CERTs im BSI; das sind die direkten Kontakte, die wir haben, ergänzt durch Gesprächskontakte, die wir in einigermaßen regelmäßiger Form jährlich wahrnehmen.

Vorsitzender Dr. Patrick Sensburg: So weit USA.

Zeuge Andreas Könen: Das ist die eine Seite; das ist die innenministerielle Seite. Dann wie dargestellt: Im Rahmen der Information-Assurance-Kooperationen der NATO-Staaten arbeiten wir dann mit dem Information Assurance Department [sic!] der National Security Agency zusammen. Das betrifft insbesondere die gesamte Zusammenarbeit in den NATO-Gruppen, die sich mit Informations- und Cybersicherheit beschäftigen, und den entsprechenden Gremienaustausch, der sich da bewegt, ergänzt natürlich durch bilaterale Gespräche, in denen man sich wechselseitig vergewissert, dass man bei modernen Themen auf dem neusten Stand ist, oder auch im Rahmen des sogenannten Common Criteria Recognition Agreements, wo die USA und Großbritannien ebenfalls beide Mitglieder sind und jeweils die NSA bzw. GCHQ die verantwortlichen Partner sind.

Ja, das leitet direkt zur britischen Seite über: Auf der britischen Seite ist es so, dass wir im Grunde sämtliche Gegenüber, mit denen wir im Rahmen dieser Aufgaben CERT und Information Assurance und EU und NATO reden müssen als Behörde, dann innerhalb der GCHQ wiederfinden. Das ist da sehr einheitlich durchgehend strukturiert; dort gibt es praktisch keine anderen wesentlichen Kontakte, die wir wahrnehmen, außer Zufallskontakten im Rahmen von Konferenzen und Ähnlichem.

Vorsitzender Dr. Patrick Sensburg: Okay. - Bei den Softwareprogrammen und Tools, die Sie nutzen: Nutzen Sie XKeyscore?

Zeuge Andreas Könen: Nein.

Vorsitzender Dr. Patrick Sensburg: Oder eine abgewandelte Version?

Zeuge Andreas Könen: Nein. Weder das noch eine abgewandelte Version.

Vorsitzender Dr. Patrick Sensburg: Okay. - Sagen Ihnen die Programme Prism, Tempora oder Boundless Informant etwas?

Zeuge Andreas Könen: Ja. Im Rahmen der Analyse, die wir durchgeführt haben, haben wir uns mit denen beschäftigt. Um es ganz kurz zu skizzieren - -

Vorsitzender Dr. Patrick Sensburg: Kurz den Jahreszeitraum: Wann haben Sie sich damit beschäftigt? Dass wir es einordnen können.

Zeuge Andreas Könen: Praktisch ab Juni 2013; ich glaube - -

Vorsitzender Dr. Patrick Sensburg: Also durch Snowden, -

Zeuge Andreas Könen: Durch Snowden.

Vorsitzender Dr. Patrick Sensburg: - nicht schon vorher.

Zeuge Andreas Könen: Nein.

Vorsitzender Dr. Patrick Sensburg: Okay.

Zeuge Andreas Könen: Vorher waren uns die Begriffe nicht bekannt. Tempora, ähnlich wie Upstream, ist eben ein Programm der strategischen Aufklärung von GCHQ. Dann: Boundless Informant ist ein Tool, mit dem nach meiner Kenntnis - ich habe jetzt die einzelnen Beschreibungen nicht mehr genau im Kopf - - das wesentliche Informationen zu Netzwerk, Infrastrukturen weltweit zusammenträgt. Und Prism seinerseits ist ein Programm, das komplementär zu Tempora und Upstream bei Firmen und Providern entsprechende Daten entgegennimmt.

Vorsitzender Dr. Patrick Sensburg: Letzte Frage voraussichtlich: Was haben Sie da jetzt gemacht, auch eine Plausibilitätskontrolle? Oder haben Sie sich das irgendwie angucken können? Oder - -

Zeuge Andreas Könen: Also an der Stelle, wo es um die strategische Aufklärung geht, die ja rein passiv erfolgt - - für alle diese passiven Komponenten haben wir uns die Folien angeschaut, haben auf Plausibilität geprüft, haben das, was wir etwa über den Verlauf von Netzen wissen, dagegengehalten. Darüber hinaus liegen uns keine konkreten wirklichen Erkenntnisse vor, wie das im Einzelnen abläuft oder wie das im Einzelnen wahrgenommen wird. Das liegt in der Natur der Sache.

Vorsitzender Dr. Patrick Sensburg: Hat man vonseiten des BSI, um, sagen wir mal, den Sachverhalt vollständig rund zu haben, mal bei unseren Diensten nachgefragt, mal im BND, ob die Prism, Tempora oder Boundless Informant oder Upstream kennen? Und was die davon wissen? Da hätte man ja ein Gesamtlagebild erstellt. Ich meine, die Plausibilitätsprüfung in allen Ehren, aber die Frage ist ja jetzt - - Wenn einer Prism hier nutzt, könnte man den ja mal fragen; wenn es so wäre.

Zeuge Andreas Könen: Also, es hat auf der Arbeitsebene dazu Austausch gegeben, allerdings nicht in Form einer irgendwie gearteten geordneten Kooperation, einer Arbeitsgruppe oder Ähnlichem. Das BfV hat von uns dazu technische Informationen erhalten, und auch der BND hat unsere Deutungen dazu in verschiedener Weise zur Kenntnis genommen, aber eine direkte Kooperation dazu: Nein.

Vorsitzender Dr. Patrick Sensburg: Gut. Herzlichen Dank. - Ich wäre insoweit mit meine Fragen erst mal durch. Na, nicht durch, aber ich glaube, jetzt ist die Zeit reif, um das Wort an die Fraktionen abzugeben. Und es beginnt dann in der ersten Fragerunde die Fraktion Die Linke mit ihren Fragen, und es beginnt Frau Kollegin Renner, vermute ich.

Martina Renner (DIE LINKE): Ja, danke, Herr Vorsitzender. - Herr Könen, Sie hatten ja kurz ausgeführt, was Sie im BND gemacht haben. Nur um für uns da sicherzugehen: Mit den hier behandelten Operationen der technischen Aufklärung hatten Sie nie etwas zu tun, also mit den durch den Untersuchungsausschuss besprochenen Operationen.

Zeuge Andreas Könen: Also, meine Tätigkeit im Bundesnachrichtendienst, die, wie gesagt, am 1. Dezember 1988 begonnen hat und am 30. September 2006 endete - - da gibt es zwei große Abschnitte drin: Der erste geht vom Startdatum bis circa Mitte März 2005. Das, was ich dort bearbeitet habe, betrifft den Untersuchungsgegenstand nicht.

Martina Renner (DIE LINKE): Und danach?

Zeuge Andreas Könen: Danach war ich im Leitungsstab des Bundesnachrichtendienstes und war da der Sachgebietsleiter 90AD, der für die damalige Abteilung 2 zuständig war. Dabei sind natürlich auch bei mir Dokumente sichtbar geworden, die hier durchaus zum Untersuchungs-

gegenstand gehören, die auch durch den Bundesnachrichtendienst im Rahmen der verschiedenen Beweisbeschlüsse weitergegeben worden sind. Ich habe mich im Vorfeld erkundigt, und man hat mir dazu Akteneinsicht gewährt, sodass ich einordnen konnte, worum es geht. Das ist über zehn Jahre her.

Martina Renner (DIE LINKE): Okay. Dann müssen wir das jetzt einordnen, weil Sie ja eben ausgeführt haben, bestimmte Gegenstände sind Ihnen durch die Snowden-Dokumente erst bekannt geworden. Aber wenn man zum Beispiel die Operation „Eikonal“ beispielhaft kennen würde aus dem BND, wusste man ja schon vorher, wie da der Hase läuft. Deswegen: Kennen Sie diese Operation „Eikonal“?

Zeuge Andreas Könen: Also, an dieser Stelle muss ich aufgrund der Einstufung der Dokumente, die ich da noch mal im Rahmen der Akteneinsicht zur Kenntnis genommen habe, auf den nichtöffentlichen Teil der Sitzung verweisen.

Martina Renner (DIE LINKE): Also, wir haben hier über „Eikonal“ in einer Ausführlichkeit mit Zeugen gesprochen, dass ich glaube - - Also, hier können alle im Raum wirklich diese Operation mittlerweile schaubildhaft darstellen. Ich glaube nicht, dass das nötig ist, hier auf die eingestufte Sitzung zu verweisen.

Zeuge Andreas Könen: Ja, ich kann die Relation der Dokumente zu „Eikonal“ nicht einordnen.

(Dr. André Hahn (DIE LINKE): Ob Sie sie kennen!)

Martina Renner (DIE LINKE): Ob Sie sie kennen. Ob Sie diese Operation kennen.

Zeuge Andreas Könen: Die Operation kenne ich in der Bezeichnung dann natürlich aus der Presse.

Martina Renner (DIE LINKE): Ja, aber Sie kannten Sie unter „Granat“. Oder unter was kannten Sie sie?

Zeuge Andreas Könen: Also - -

Martina Renner (DIE LINKE): Also der Punkt ist, Sie haben gesagt, Sie kennen bestimmte Dinge erst seit den Snowden-Dokumenten, aber wenn wir davon ausgehen, dass man im BND -

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): - mit diesen Operationen, den bilateralen Abgriffen - -

Zeuge Andreas Könen: Ja, also der Begriff „Granat“ sagt mir was, um das klar auf den Punkt zu bringen.

Martina Renner (DIE LINKE): Genau.

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): Dann kennen Sie ja im Grunde - -

Zeuge Andreas Könen: Ich weiß genau das, was in den Dokumenten, die hier abgeben wurden, auch drinsteht, ja. Exakt.

Martina Renner (DIE LINKE): Und kennen Sie auch die Operation „Glotaic“?

Zeuge Andreas Könen: Ja, das ist - - Exakt.

Martina Renner (DIE LINKE): Super.

(Dr. André Hahn (DIE LINKE): Er ist der Erste!)

Super. - Als Sie damals diese Operation zur Kenntnis genommen haben - also, der BND geht als Türöffner für die NSA an das Kabel bzw. an den Internetknoten; es sind ja zwei unterschiedliche Zugänge, einmal „Eikonal“ an den Knoten, dann bei „Glotaic“ ans Kabel -, war Ihnen damals bekannt, dass die Daten an die US-Seite aus diesen Operationen ausgeleitet werden sollen?

Zeuge Andreas Könen: Also, das kann ich jetzt aus meiner Erinnerung nicht mehr präzise nachvollziehen.

Martina Renner (DIE LINKE): Was war denn Sinn dieser Operation in Ihrer Erinnerung?

Zeuge Andreas Könen: Also, ich konnte exakt die Beschreibung, die Sie gegeben haben bezüglich der Technik, bezüglich Paket- bzw. entsprechend … (akustisch unverständlich). Das kann ich nachvollziehen im Moment. Weitere Erinnerungen dazu bzw. - - habe ich nicht.

Martina Renner (DIE LINKE): Haben Sie - -

Vorsitzender Dr. Patrick Sensburg: Jetzt muss ich mal ganz kurz die Bundesregierung fragen: Wie weit ist „Eikonal“ eingestuft? Wenn das nicht eingestuft ist, können wir hier frei drüber reden.

Martina Renner (DIE LINKE): Was soll das denn?

RD Philipp Wolff (BK): Grundsätzlich reden wir natürlich immer noch über eingestufte Dokumente.

Vorsitzender Dr. Patrick Sensburg: Okay, aber das können wir jetzt hier.

RD Philipp Wolff (BK): Ich gehe davon aus, dass Frau Renner das, was sie bisher zitiert hat, natürlich aus der Presse zitiert. Wir haben über „Glotaic“ - -

Vorsitzender Dr. Patrick Sensburg: Ja, bei Frau Renner habe ich kein Problem. Die weiß, was sie macht.

(Vereinzelt Heiterkeit)

Ich frage nur - - Die Aussagen, die dann kommen, damit habe ich das Problem. Herr Könen weiß auch, was er macht, aber - -

RD Philipp Wolff (BK): Vielleicht auch zur Klarstellung, nicht dass das jetzt ein bisschen auseinandergeht: Herr Könen hat ja auch dargestellt, dass er im Leitungsstab tätig war, was natürlich auch bedeutet, Herr Könen war nicht unmittelbar mit der Operation befasst. - Das nur zum Verständnis, wie sein Kenntnisstand ist.

Vorsitzender Dr. Patrick Sensburg: Ich freue mich ja nur, wenn es gesagt werden kann, und will da nicht in Schwierigkeiten kommen.

RD Philipp Wolff (BK): In den Detail- -

Martina Renner (DIE LINKE): Wir hatten ja auch noch gar nicht operativ gefragt. Aber er hat ja gesagt, er wusste auch, wie die technisch aufgesetzt ist, die Operation. Das hat er ja schon ausgeführt, und mich würde eben interessieren mit diesem Wissen - -

RD Philipp Wolff (BK): Er hat gesagt, er hat in einem - - nur um ihn zu zitieren: Dass es um Paketvermittlung geht. Er hat nicht gesagt, er weiß, wie die Operation technisch aufgesetzt ist. Das ist ein großer Unterschied. Nur dass das klargestellt wird. Und wenn es um Details der Operation geht, ist das natürlich weiterhin eingestuft, Frau Renner. Da sind wir uns auch einig.

Martina Renner (DIE LINKE): Wir reden ja jetzt nicht über Details der Operation, sondern wir reden im Moment über die Frage, wenn man mit diesem Wissen aus dem BND ins BSI geht, dass man weiß, es finden solche Operationen am Kabel bzw. am Knoten statt, ob man das dann bei der Frage: „Wie organisiere ich IT-Sicherheit, -

Zeuge Andreas Könen: Genau.

Martina Renner (DIE LINKE): - Netzsicherheit?“, mitgenommen hat oder abgetrennt hat und gesagt hat: „Das war mein früheres Leben; da machen wir jetzt Blitzdings, wie bei „*Men in Black*“, und irgendwie: „Das weiß ich gar nicht mehr, was ich da mitbekommen habe“.

Zeuge Andreas Könen: Man kann das präziser beschreiben. Es ist natürlich durchaus so, dass gerade die Kenntnisse, die man insgesamt gewinnt, wenn man in einem Nachrichtendienst tätig ist, einem auch noch mal deutlich machen, welche Gefährdungen herrschen. Aber wo man eine klare Schere setzt, das ist ganz deutlich, dass man dann das, was man zur Informationssicherheit der Bundesrepublik Deutschland zu tun hat in der neuen Rolle, natürlich auf Basis des tech-

nischen Wissens, was man dazu hat, in der Bewertung von Gefährdungen dann auch bestmöglich umsetzt. Das ist, denke ich, Loyalität unserem Staat gegenüber, dass man das dann genauso wahrnimmt. Die Einordnung der Operationen ist mir auch genau darum exakt in diesem technischen Sinne, wie Sie es geschildert haben, noch bewusst; ich kann Ihnen aber zum Operationellen einmal aufgrund der Einstufung, aber auch andererseits tatsächlich aufgrund des langen Zeitabstandes nichts Genaues mehr benennen, ohne dabei aus der Erinnerung heraus Fehler zu machen.

Martina Renner (DIE LINKE): Und dann bei der Bewertung der Snowden-Dokumente durch das BSI: -

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): - Spielte dann das Wissen um diese Operationen des Bundesnachrichtendienstes eine Rolle? Weil die ja zum Beispiel auch in den Dokumenten erwähnt werden, manchmal unter anderem Namen als im BND, aber eben dort auch vorkommen, und wenigstens, wenn sie nicht als Operationsnamen vorkommen, als generelle Methodik.

Zeuge Andreas Könen: Als konkrete Operationen: Nein. Aber als Methodik - - Das Wissen, was man einmal über Gefährdung erworben hat, das ist natürlich etwas, was man an der Stelle verwenden muss, klar. Und in der Bewertung, dass Operationen an verschiedenen Knotenpunkten stattfinden können und dass es realistisch ist, die Daten auch in der Form dann abzuziehen, natürlich.

Martina Renner (DIE LINKE): Und man hat dann auch gesagt: „Mir ist die Problematik der Selektoren bekannt“? War das - - Also, andersherum angefangen, Herr Könen, bei Ihrem Wissen aus dem BND-Leitungsstab: Wussten Sie, dass NSA-Selektoren in diesen Operationen eine Rolle spielen?

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): Das war Ihnen gänzlich unbekannt.

Zeuge Andreas Könen: Das war mir gänzlich unbekannt.

Martina Renner (DIE LINKE): Telekommunikationsmerkmale, Suchbegriffe vielleicht, dass man es anders labeln irgendwie - -

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): Gar nicht.

Zeuge Andreas Könen: Nein. Nach meiner Erinnerung absolut nicht.

Martina Renner (DIE LINKE): Sie wussten nur: Es werden Daten erfasst.

Zeuge Andreas Könen: Ich wusste - -

Martina Renner (DIE LINKE): Wussten Sie, dass diese in Bad Aibling verarbeitet werden?

Zeuge Andreas Könen: Zu dem Zeitpunkt: Nein. Das ist ebenfalls eine Kenntnis, die ich auch erst über die Presseveröffentlichungen bzw. in der Deutung der Snowden-Veröffentlichungen gewonnen habe.

Martina Renner (DIE LINKE): Und was war Ihr Kenntnisstand, was mit den Daten passiert, wenn Sie nicht wussten, dass sie in Bad Aibling verarbeitet werden? Werden die geroutet zu den Amerikanern? Oder was passiert mit denen?

Zeuge Andreas Könen: Sie meinen, aus dem damaligen Wissensstand heraus?

Martina Renner (DIE LINKE): Aus dem damaligen Wissensstand, also wenn Sie im Leitungsstab hören: „Wir machen jetzt dieses Projekt“. Und was passiert mit den Daten? Was war Ihr Kenntnisstand?

Zeuge Andreas Könen: Also, nach meiner Erinnerung war der Kenntnisstand natürlich der, wie die Verarbeitung innerhalb der heutigen Abteilung TA, damals Abteilung 2, stattfindet, welche Mechanismen dort dann im Einzelnen verwendet werden, technisch und auswertemäßig. Das war

natürlich durch die Kommunikation mit der Abteilung bekannt, klar.

Martina Renner (DIE LINKE): Ja, aber wovon sind Sie ausgegangen, was mit den Daten passiert, die bei der Telekom abgegriffen werden? Was sollte mit denen passieren?

Zeuge Andreas Könen: Die wurden unter den Maßgaben des G-10-Ausschusses entsprechend -

Martina Renner (DIE LINKE): Nein, das ist leider eben nicht so gewesen, nicht?

Zeuge Andreas Könen: - weiterverwertet bzw. -

Martina Renner (DIE LINKE): Und bei „Glotaic“ gar nicht.

Zeuge Andreas Könen: - unter den sonstigen rechtlichen Bedingungen, die der BND hat für seine - -

Martina Renner (DIE LINKE): Ja, leider nicht. Bei „Glotaic“ gab es gar keine G-10-Anordnung und bei „Eikonal“ erst eine sozusagen nachträglich eingeholte.

Zeuge Andreas Könen: Gut. Entzieht sich meiner Kenntnis.

Martina Renner (DIE LINKE): Also -

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir - -

Martina Renner (DIE LINKE): Ja, letzte Frage. Herr Könen, damals - - waren Sie da „Herr Könen“ im BND?

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): Oder dürfen wir nach einem anderen Namen suchen?

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): Es gab immer nur einen Namen; es gibt keinen zweiten.

Zeuge Andreas Könen: Es gab immer nur einen.

Martina Renner (DIE LINKE): Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Dann kommen wir jetzt zur nächsten Fraktion. In dieser ersten Runde ist als zweite Fraktion die Fraktion der SPD dran, und Herr Kollege Flisek beginnt.

Christian Flisek (SPD): Ja, danke, Herr Vorsitzender. - Herr Könen, auch erst mal ein herzliches Willkommen von unserer Seite. - Es ist schon angesprochen worden: Ihre berufliche Laufbahn, die Sie ja vom BND dann zum BSI geführt hat - - und ich möchte das jetzt gar nicht, dass Sie das persönlich nehmen, aber ich frage Sie mal ganz offen: Angesichts der Zuständigkeiten und Aufgabenbereiche dieser beiden Bundesbehörden, sehen Sie das nicht als eigentlich einen Interessengegensatz, den man da irgendwie vergegenwärtigen muss? Wenn man sozusagen einerseits mal, ich glaube, fast 20 Jahre, wie Sie, beim Auslandsnachrichtendienst gearbeitet hat, der eben, sage ich mal, im Rahmen seiner Aufgaben ganz spezifische Erkenntnisinteressen hat, und andererseits man dann sozusagen wechselt in eine Behörde, die für die Integrität und Sicherheit der ganzen Informationstechnik eigentlich eintreten soll und muss, und das mit Sicherheit auch tut, aber - - Ich stelle mir das sehr schwierig vor, sage ich ganz offen.

Zeuge Andreas Könen: Also, das ist eine klare Herausforderung, aber dieser Herausforderung müssen wir uns grundsätzlich stellen, weil die durch die reale Situation selber gegeben ist. Wir brauchen ja gar nicht bei nachrichtendienstlich relevanten Fragestellungen beginnen. Diese Janusköpfigkeit der Fragestellung ergibt sich immer wieder. Wenn Sie auf der einen Seite sich vorstellen, dass Sie natürlich und als allerersten Aufschlag Verkehre verschlüsseln wollen - wir wollen das schützen, was wir als Kommunikation produzieren -, dass aber auf der anderen Seite natürlich auch Kriminalität diese Verschlüsselung nutzt, um ihr eigenes Tun zu beschützen, dass auch Terroristen dies tun, dann ist völlig klar, dass auch in dem Bereich unmittelbar ein Spagat entsteht zwischen der Verpflichtung,

eben wirklich gute und einsetzbare Kryptografie ins Feld zu bringen, im Verhältnis zu dem, was dort die Strafverfolgungsbehörden tun müssen. Das Gleiche gilt in einem Verhältnis des BSI zum Bundesnachrichtendienst oder etwa zum BfV. Da, wo wir darauf angewiesen sind, Erkenntnisse zu erlangen, wie Angriffe aussehen, wenn wir wissen wollen, was sich etwa außerhalb der deutschen Grenzen abspielt, mit welchen Angriffen wir in Zukunft rechnen müssen, dann können wir nur darauf bauen, dass das die Behörde tut, die dafür in Deutschland zuständig ist, und das ist eine klare Zuständigkeitszuordnung für den Bundesnachrichtendienst.

Wie man dann den Schutz gewährleistet, dabei notwendige Informationen etwa den anderen Playern, dem Bundeskriminalamt, dem BfV oder dem BND, so zur Verfügung stellt, dass die für uns diese Gefährdungsaufbereitung leisten können, ohne dabei gleichzeitig neue Gefährdungen zu produzieren, das ist eine deutliche Herausforderung. Gehört sicher -

Christian Flisek (SPD): Das sehe ich auch so.

Zeuge Andreas Könen: - zur Spitze dessen, was man als Business machen muss.

Christian Flisek (SPD): Das sehe ich auch so, dass das eine deutliche Herausforderung ist - - und wir uns natürlich auch hier in diesem Ausschuss, im Rahmen der Empfehlungen, die wir dann abzugeben haben, die Frage stellen, ob das alles so der Weisheit letzter Schluss ist, wenn das beispielsweise - ich habe das auch mit dem Bundesinnenminister de Maizière, als er hier Zeuge war, erörtert - in einem Haus unter einem Hut - - wenn dieser Interessengegensatz - Sie haben das Thema Verschlüsselung angesprochen - da so eklatant vereinigt ist, nicht? Also, verstehen Sie?

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Ich meine, ich frage das jetzt mal auch: Haben Sie das Gefühl, dass das funktioniert, dass man diesen Spagat leisten kann?

Zeuge Andreas Könen: Sie werden es kaum glauben, aber ich denke, dass es funktioniert. Und ich mag Ihnen auch gerne erzählen, warum: Wir haben - Sie haben es zuerst genannt - die schon auch in ähnlicher Hinsicht problematische Schnittstelle zum Bundesnachrichtendienst, wo man sich genau überlegen muss, in welcher Weise man Cybersicherheitszusammenarbeit betreibt. Das hat gar nichts mit Ressorts zu tun; das ist über Ressortgrenzen hinweg. Das heißt, diese Problematik besteht für eine Behörde, die Cybersicherheit und Informationssicherheit machen muss, per se; die existiert unabhängig von der Art, wie ich das zunächst einmal in Ressorts organisiere.

Es wird sehr oft die Frage geäußert, ob das BSI nicht besser unabhängig sein sollte. Ich sage Ihnen ganz klar: An der Stelle braucht man, um als Behörde stark auftreten zu können, um mit Nachdruck auftreten zu können, den Nachdruck eines Ressorts. Das ist für eine völlig unabhängige Stelle aus meiner Sicht aus vielen Gründen - können wir gerne an einer anderen Stelle weiter diskutieren, ist eher eine politische Frage - -

Christian Flisek (SPD): Budgetäre Gründe, oder was meinen Sie?

Zeuge Andreas Könen: Ja, also zum Beispiel - - Es sind ganz einfache Fragen: Wenn man als völlig unabhängige Behörde ein Wachstum benötigt, eine stärkere Einbettung in politische Themen, wenn ein Nachdruck, der einem in einer politischen Einordnung gegeben werden kann - - dann kann da ein Ressortminister in vielen Fällen viel erreichen. Beim Thema Sicherheit gibt es ein klar bezeichnetes Ressort; das ist das Innenministerium, das das Thema „Sicherheit, öffentliche Sicherheit, innere Sicherheit“ gesamt wahrnimmt.

Christian Flisek (SPD): Ja, ich - -

Zeuge Andreas Könen: Da ist das BSI dadurch natürlich auch an einem Ort aufgehoben, der sich präzise mit der Thematik beschäftigt, mit der wir uns da auseinandersetzen.

Christian Flisek (SPD): Ich verstehe das sehr wohl. Nur die Frage ist halt - - Klar, wenn man

sozusagen den Rückhalt eines Ministeriums, eines starken Ministeriums braucht, ist ja die Frage, welche Rolle sozusagen die Arbeit, die Sie machen, auf der Agenda des jeweiligen dann Ministers auch spielt. Und ich sage mal, wenn er in seinem Haus auch natürlich - ich überspitze jetzt mal - Leute hat, die rumlaufen und sagen: „Aus Sicherheitsbehördensicht ist Verschlüsselung des Teufels“, dann ist das natürlich, also nach meinem Empfinden, wenn er dann gleichzeitig die Verantwortung für eine Behörde wie das BSI hat, wo Sie sagen, Sie arbeiten an Volksverschlüsselung usw. - - Das geht irgendwie nicht ganz zusammen. Also, da muss man schon irgendwo schizophren sein, um das irgendwie einigermaßen hinzubekommen.

Zeuge Andreas Könen: Das glaube ich nicht. Ich glaube, man muss gute Mechanismen auch innerhalb eines Ministeriums und einer Behörde entwickeln, sich mit dem Thema auseinanderzusetzen, und das in einer Weise tun, dass man am Ende die Interessen gegeneinander abwägt. Ich würde mir dann, ehrlich gesagt, Gedanken machen, wenn das zusammenfallen würde mit einer irgendwie gearteten Beeinflussung oder irgendetwas, woraus sichtbar würde, dass man uns daran hindern würde, Sicherheit zu produzieren. Das ist nicht der Fall. Wir produzieren Sicherheit, fachlich unabhängig, fachlich mit einem ganz deutlichen Aufschlag. Und wir führen diese Debatte um Quellen-TKÜ, um Onlinedurchsuchung natürlich; aber wir tun das in einem klaren, sichtbaren Prozess und nicht in - -

Christian Flisek (SPD): Gut. - Also, ich halte fest: Sie als Vizepräsident sagen, Sie fühlen sich in den Armen des Bundesinnenministeriums gut aufgehoben und streben nicht nach einer weiteren Unabhängigkeit.

Zeuge Andreas Könen: Nein, es funktioniert offensichtlich.

Christian Flisek (SPD): Okay. - Sie hatten in Ihrem Eingangsstatement bei der Auseinandersetzung, Würdigung mit der Frage „Welche Rolle haben eigentlich die Snowden-Veröffentlichungen, die Dokumente, die Auswertung dieser Dokumente für Ihre eigene Einschätzung gespielt?“ gesagt - korrigieren Sie mich, wenn ich Sie falsch wiedergebe -: „Wir haben vieles grundsätzlich für möglich gehalten, aber dann wiederum eben doch nicht“ - weil Sie es für unpraktikabel gehalten haben, weil beispielsweise der Aufwand für so was viel zu hoch ist - und: „Wir haben nicht gedacht, dass eben das dann tatsächlich auch in der Methodik nachrichtendienstlicher Tätigkeiten anderer Dienste tatsächlich eingesetzt wird und eine Rolle spielt.“

Ich meine, wir haben diese Grundproblematik ja hier im Ausschuss generell, dass, wenn deutsche Dienste mit anderen Diensten kooperieren, sie sozusagen nicht wissen: „Was sind die technischen Fähigkeiten und auch die budgetären Fähigkeiten dieser Dienste eigentlich en détail?“, und man dann sozusagen in diesen Kooperationen beispielweise Daten weitergibt, um ein Beispiel zu nennen, wo man zwar sich irgendwie absichert mit Disclaimern und Zweckbindung, aber am Ende irgendwie vielleicht gar nicht auf dem Bildschirm hat, was da sozusagen dann hinten dran beim anderen für Fähigkeiten existieren und was man dann tatsächlich mit diesen Daten auch machen kann.

Und jetzt wäre meine Frage tatsächlich: Also angesichts ja - - wo Sie sagen: „Diese Analyse der Snowden-Dokumente hat uns noch mal die Augen geöffnet.“ Das waren zwar jetzt nicht Ihre Worte, aber - - „Das hat uns noch mal gezeigt - - Wir haben vieles für möglich gehalten, aber dass es auch tatsächlich dann so stattfindet - - Aha, scheint plausibel zu sein.“ Sie haben sich ja im Gegensatz zu Herrn Maaßen klar dazu geäußert, dass Sie zwar jetzt nicht die Echtheit der Dokumente verifizieren können, aber dass Sie alles, was da ist, für plausibel halten.

Was hat das für Konsequenzen konkret gehabt? Hat man sich da anschließend hingesetzt mit dem Verfassungsschutz, mit dem BND, mit dem Innenministerium und gesagt: „Liebe Leute, das ist sozusagen aus unserer Einschätzung noch mal eine völlig neue Phase, ein neues Stadium; wir haben jetzt doch nicht nur Indizien, sondern Belege dafür, dass hier Fähigkeiten existieren, die wir bisher nicht für praktikabel gehalten haben,

und das bedeutet auch, wir müssen unsere Kooperationen, wir müssen Datenaustausch, ähnliche Dinge, die wir praktizieren, die wir vielleicht so ein bisschen unter dem Schleier des Nichtwissens bisher praktiziert haben, noch mal neu bewerten“? Ist das passiert?

Zeuge Andreas Könen: Also, wir haben tatsächlich, gerade was auch das von mir bereits benannte Beispiel „Sicherheit der Regierungskommunikation“ angeht, daraus gemeinsam mit dem BfV und in dem Fall der Bundespolizei klare Schlüsse gezogen, haben gesagt: Hier hat sich die Bedrohungslage deutlich geändert, und wir müssen die Maßnahmen, die wir schon mal als BSI Anfang der 2000er durchgeführt haben, hier nochmals durchführen, unter dem Gesichtspunkt der neuen Erkenntnisse noch mal neu untersuchen und bewerten. - Das ist ganz konkret passiert.

Christian Flisek (SPD): Wie waren die Reaktionen von den Vorgesetzten da? Weil ich sage es mal so: Bei uns ist es immer so natürlich - - Es gibt so ein „Elefantenargument“; das wandert hier die gesamte Zeit herum.

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Und das ist: Tut bloß nichts, um die Kooperation in Zeiten terroristischer Bedrohungen zu gefährden! Also, alles, was irgendwie getan wird, was für Missstimmungen sorgen könnte bei irgendwelchen wichtigen anderen Diensten: Macht das nicht! Weil irgendwann werden wir da plötzlich abgeschnitten sein, und dann schaut es richtig blöde aus, wenn hier in Deutschland mal was passiert und wir es eigentlich verhindern hätten können, aber eben die Informationen nicht bekommen haben. - Also, ich nenne das deswegen „Elefantenargument“, weil das trampelt alle, jedes andere Argument, jede Debatte, sofort tot. Und sind Sie damit auch konfrontiert worden? Ich meine - -

Zeuge Andreas Könen: Natürlich überlegt man genau, was man mit bestimmten Maßnahmen denn nun auch zum Beispiel in einer solchen genaueren Untersuchung der Sicherheitsinfrastruktur Berlin-Mitte tut. Das ist diskutiert worden, aber zum Beispiel auch unter Fragestellungen: Wenn man hier im Bereich Berlin-Mitte Untersuchungen macht, wie weit stört man auch den Kommunikationsverkehr? Wie weit greift man dann tiefer ein in Strukturen, auch etwa der Botschaften, die hier präsent sind? Das sind entscheidende Fragen, über die wir uns schon Gedanken gemacht haben, wo dann auch entsprechend Bedenken hochkamen. Insgesamt konnte ich das aber nicht feststellen. Es war eher die Frage noch einmal: Wie gehen wir angesichts dessen, was wir jetzt wissen, mit einem technischen Repertoire daran? Wie schaffen wir es, die Kraft eben der Behörden BfV, Bundespolizei und BSI da auf den Punkt zu bringen? - Das sind dann eher Punkte, wo man mit dem Handeln von Behörden als Elefant konfrontiert wird. Das ist aber leider Geschäft.

Christian Flisek (SPD): Dann können Sie mir mal konkrete Änderungen nennen. Was hat sich sozusagen auf der Grundlage dieser Gespräche nach Auswertung der Snowden-Dokumente ganz konkret geändert?

Zeuge Andreas Könen: Ja. Wir haben also ganz klar hier zum Beispiel bei der Sicherheit der Mobilkommunikation erneut nachgefasst, ob die Kommunikation aller Bundesbehörden möglichst über die gesicherten Netze stattfindet. Das ist in hohem Maße gewährleistet worden. Es gab einige, die das noch nicht gemacht haben; die sind dann unter dem Druck dieser Ereignisse mit da hineingenommen worden.

Christian Flisek (SPD): Welche waren das, die das bis dahin so nicht gemacht haben?

Zeuge Andreas Könen: Das habe ich jetzt nicht im Sinn. Wir haben eine Liste erstellt, auf der konkret dann alle draufstanden. Das ist jetzt zu lange her, dass ich jetzt genau jemanden wüsste. Ich würde auch jetzt niemanden blamieren wollen. Aber die sind dann durch den Präsidenten des BSI unmittelbar angeschrieben worden und auch wirklich dann mit Nachdruck gebeten worden, zügig zu migrieren und sich unter den Schutz des IVBB, also des Informationsverbundes Berlin-Bonn, zu begeben.

Wir haben nochmals die Kommunikationswege hier in Berlin selber gecheckt. Wir haben uns angesehen, wie der Auftragnehmer da dann diese Kommunikation realisiert hier. Wir haben geschaut, wo Kabel verlaufen, wo theoretisch nach dem, was uns vorliegt, Kabelzugriffe erfolgen könnten, und haben uns vergewissert, dass das nicht so ist. Wir sind hingegangen, haben verstärkt dann sichere Mobilkommunikation erstens in dem Sinne eingebracht, dass wir - - Sie wissen das: Man klinkt sich über eine Basisstation bei Mobiltelefonie ein. Wir haben dafür gesorgt, dass es eine breitere Struktur von solchen Basisstationen gibt, sodass man mit geringerer Energie kommunizieren kann, was eben auch eine passive Aufklärung etwa deutlich erschwert.

Dann: Die Sensibilisierung der entsprechenden Spitzen der Häuser, genau dieses Wissen, was ich Ihnen dargestellt habe, auch zu kommunizieren, in Handlungsanweisungen für ITSiBes, … (akustisch unverständlich)[1] Sicherheitsbeauftragte, rüberzubringen und damit eben auch die Möglichkeit zu schaffen, jeden einzelnen Mitarbeiter zu erreichen, das ist ebenfalls in einer sehr umfänglichen Kampagne gemacht worden.

Dann haben wir letztlich und endlich natürlich auch noch mal die gesamte Geräteinfrastruktur weiterentwickelt, sprich: Mobiltelefone ins Feld gebracht. Dann durchaus - ich stimme Ihnen absolut zu -: Wir haben uns auch noch mal genau überlegt, wie wir mit Daten umgehen, wie wir am besten Daten so kommunizieren, dass etwa die Information, die wir abgeben, wirklich Cybersicherheitszwecken zugutekommt - das ist etwa Information, mit der man Schadsoftware identifiziert in Netzen -, dass das aber umgekehrt nicht dazu führt, dass wir jemanden, dem wir das in die Hand drücken - - damit umgekehrt Schaden anrichten kann und Angriffe selber produziert - -

Christian Flisek (SPD): Darf ich da gerade einhaken?

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Das sind sozusagen Datenaustausche oder Kooperationen, die Sie als BSI dann im Zweifel haben mit Kooperationsbehörden in anderen Staaten. Wir haben natürlich hier auch noch mal den Fokus auf Austausch von Daten im Rahmen von nachrichtendienstlichen Kooperationen. Also, die Thematik ist natürlich brisant im Rahmen von Drohneneinsätzen beispielsweise. Und hat es da aufgrund dieser Erkenntnisse noch mal zu einer Überprüfung - - Gab es da Zusammenkünfte mit Verfassungsschutz, mit BND, wo man gesagt hat: Liebe Leute, schaut euch das noch mal an! Schaut euch noch mal die Qualität eurer Daten an! Wir haben eventuell hier jetzt eine neue, ich nenne es jetzt mal, Gefährdungslage aus der Perspektive: Was passiert dann beim Empfänger mit diesen Daten? Welche Anreicherungsmöglichkeiten haben die und was - - Also, ist das passiert?

Zeuge Andreas Könen: Also, diese Debatte hat stattgefunden an der Stelle, die Sie benennen. Gerade in der Kooperation mit ausländischen Behörden sind wir natürlich an vielen Stellen ebenfalls auf den Bundesnachrichtendienst angewiesen, da wo der Kontakt eben in der Wahrnehmung ausländischer Kontakte von dort erfolgt. Und diese Sensibilisierung, diese Gespräche haben stattgefunden, initiiert durch die Leitung des BSI bis auf die Arbeitsebene hinunter, die sich konkret mit dem Thema beschäftigen muss. Ja.

Christian Flisek (SPD): Und hat das zu Konsequenzen geführt? Gab es Änderungen in der Art und Weise, wie Daten dann übermittelt worden sind?

Zeuge Andreas Könen: Es gibt einen ganz deutlichen Prüfmechanismus dafür, was wir weitergeben. Der ist auf Basis dessen implementiert worden.

Christian Flisek (SPD): Wie schaut der aus?

Zeuge Andreas Könen: Das sieht so aus, dass der zuständige Bereich - das ist bei uns der Bereich

1) Ergänzung des Zeugen: "[…in Handlungsanweisungen für ITSiBes, also Informationssicherheitsbeauftragte,…]", siehe Anlage 1.

„Internationale Beziehungen“, der das wahrnimmt, dem auch das Cyber-Abwehrzentrum obliegt - in der Kooperation mit den jeweiligen Behördenmitarbeitern Bundesnachrichtendienst das dann im Einzelnen diskutiert. Und das wird einzelfallbezogen angeschaut, welche Relevanz das einzelne Datum hat.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Jetzt müssten wir - -

Christian Flisek (SPD): Schon zu Ende? - Okay.

Vorsitzender Dr. Patrick Sensburg: Ja. Jetzt müssten wir wechseln. - Jetzt kommen wir zur Fraktion von Bündnis 90/Die Grünen, und der Kollege von Notz beginnt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Guten Tag, Herr Könen! - Wir haben ja in den letzten Jahren sehr häufig über die Frage der Unabhängigkeit Ihrer Behörde geredet und haben da einfach unterschiedliche Sichtweisen drauf. Und ich glaube, das können wir hier heute auch nicht lösen.

Ich würde gerne meine Fragen in zwei Abschnitte teilen, einmal Sie zu Ihren Erfahrungen beim Bundesnachrichtendienst befragen und dann zu der Zeit im BSI. Und anknüpfend an die Zeit im Bundesnachrichtendienst und die Fragen von Frau Renner sozusagen: Was war denn Ihr letzter Stand bei der Operation „Eikonal“, als Sie im Oktober 2006 gegangen sind? Was war denn - - War Ihnen bekannt, dass man in Frankfurt an der Glasfaser war mit den Amerikanern?

Zeuge Andreas Könen: In Frankfurt: Ja. Mit den Amerikanern: Nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Sie wussten nicht, dass das mit den Amerikanern zusammen passiert?

Zeuge Andreas Könen: Das kann ich so nicht einordnen, nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Was heißt, das können Sie so nicht einordnen?

Zeuge Andreas Könen: Nach meiner Erinnerung habe ich dazu keine Kenntnis erlangt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also kann es sein, dass das sogar im Bundesnachrichtendienst damals teilweise geheim gehalten worden ist.

Zeuge Andreas Könen: Sie müssen sich das vor allen Dingen so vorstellen, dass ich dann natürlich in der Fähigkeit im Leitungsstab in der Informationsweitergabe zwischen Abteilungen an den Präsidenten tätig war, dass Sie da natürlich auch nicht jedes Dokument wirklich einzeln lesen und im Einzelnen zur Kenntnis nehmen und außerdem aufgrund der Menge auch nicht im Kopf behalten.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das verstehe ich vollständig. Die Frage ist: Ist das eine normale Operation?

Zeuge Andreas Könen: Das kann ich nicht beurteilen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Können Sie nicht beurteilen nach Ihrer Zeit im Bundesnachrichtendienst: Also, es könnte sein, dass der Bundesnachrichtendienst Hunderte solcher Operationen in Deutschland an die Glasfaser - - als Auslandsnachrichtendienst in Deutschland an die Glasfaser geht, automatisiert Daten ausleitet, Herr Könen.

Zeuge Andreas Könen: Dazu müsste ich jetzt irgendwie vermuten oder sonst etwas. Also, da sehe ich jetzt nicht, worauf ich das im Einzelnen begründen sollte.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Na, Sie haben doch einen Erfahrungshorizont. Nach Jahren im Bundesnachrichtendienst haben Sie einen Erfahrungshorizont und können doch sagen, ob das eine alltägliche Operation ist.

Zeuge Andreas Könen: Also, alltäglich war sie sicher nicht, weil definitiv in meinem Gedächtnis ist, dass eben einzeln dann Dokumente dem Präsidenten vorgelegt wurden.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): War Ihnen bekannt, dass das mit einem Auslandsnachrichtendienst zusammen gemacht worden ist?

Zeuge Andreas Könen: Nein. Dass es mit einem Auslandsnachrichtendienst zusammen gemacht wurde: Nein; in der Form, wie Sie die Frage stellen, nicht.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wussten Sie, dass die Technik, Hard- und Software, von einem Auslandsnachrichtendienst kam?

Zeuge Andreas Könen: Nein. Nicht in Erinnerung. Nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Für Sie hätte das auch Bundesnachrichtendienst-inhouse-Entwicklung sein können.

Zeuge Andreas Könen: Ja. Da ich niemals selber in einem der Bereiche tätig war, die mit diesen Vorgängen beschäftigt waren, ist mir das auch nicht aus dem, was ich im Leitungsstab gesehen habe, erkenntlich oder in Erinnerung.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und von Problemen bei dieser Kooperation haben Sie auch nichts gehört? Davon, dass da irgendwie EADS und Eurocopter - -

Zeuge Andreas Könen: Ist mir nicht mehr bewusst, ist mir nicht bewusst. Nein, ich weiß, dass die Kooperation natürlich mit der NSA bestand; aber wie sie sich genau im Rahmen dieser Operation erstreckte und bewegte, kann ich nicht sagen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber Sie wussten, es gab eine Kooperation mit der NSA?

Zeuge Andreas Könen: Das ist klar. Das war offensichtlich ja damals, -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das war klar.

Zeuge Andreas Könen: - da eben auch solche Berichte klar abzuliefern waren jedes Jahr, wie die Kooperationen laufen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber dass es da zu Problemen gekommen ist, dass trotz Echelon oder so - - damit waren Sie nicht vertraut.

Zeuge Andreas Könen: Nein, damit war ich nicht vertraut.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Haben Sie mal was vom Schwachstellenbericht gehört? Sagt Ihnen dieser Begriff was?

Zeuge Andreas Könen: In Bezug auf - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Auf „Eikonal“.

Zeuge Andreas Könen: Nein. Kann ich mich nicht erinnern.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das war auch nach Ihrer Zeit; aber ich dachte, vielleicht hätte man das BSI informiert. - Mit den Snowden-Unterlagen haben Sie sich aber intensiv auseinandergesetzt.

Zeuge Andreas Könen: Haben wir uns im BSI intensiv auseinandergesetzt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja. Dann würde ich Ihnen gerne meine Lieblingsfolie vorlegen, weil ich mich frage - -

Vorsitzender Dr. Patrick Sensburg: Sagst du kurz die Bandnummer? Also, was - - Ist zwar immer die gleiche - ich habe sie auch vor mir -, aber dass wir trotzdem noch mal die Quelle wissen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja. Vielleicht können Sie kurz sagen, was für ein Aktenzeichen da obendrüber steht.

Vorsitzender Dr. Patrick Sensburg: Dann können alle es nachschlagen. Wie gesagt, wir haben alle, glaube ich, ein grobes Bild vor Augen.

Zeuge Andreas Könen: Also, beim Zweiten steht: MAT A Sek-6d_DE, Blatt 8.

Vorsitzender Dr. Patrick Sensburg: Blatt 8.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Könen.

Zeuge Andreas Könen: Bei den anderen ist es nicht erkenntlich.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): So, und hier sind zwei Übersichten, die sich ähneln: „RAMPART-A Typical Operation“ in der „Country X“ mit einem „Access Point A“ und dann einem „Processing Center“. Und der Laie fragt sich, ob das nicht, diese „RAMPART-A Typical Operation“, eine „Typical ‚Eikonal‘“ oder „‚Granat‘ Operation“ ist. Haben Sie diese Akte - -

Zeuge Andreas Könen: Ja.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Die kennen Sie, nicht?

Zeuge Andreas Könen: Ich kenne diese Folien, veröffentlicht - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Haben Sie sich das auch gefragt im Sommer 2013: „Mensch, du, als ich damals im Bundesnachrichtendienst war, ‚Eikonal‘, in Frankfurt an der Glasfaser, in einer Kooperation mit der NSA, könnte es sein, dass wir dieses Secret Comint Network, das hier angezeigt und eingezeichnet ist, dass wir das einfach übersehen haben?“?

Zeuge Andreas Könen: Also, das habe ich mich nicht gefragt. Ich hätte es allenfalls vermuten können. Tatsächlich haben wir uns mit diesen Folien und auch ich persönlich im Jahr 2013 nicht intensiv auseinandergesetzt. Ich weiß, dass ich sie gesehen habe; aber eine weitere Auseinandersetzung damit hat nicht stattgefunden.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, es ist hier - - Also, ich mache Ihnen keinen persönlichen Vorwurf daraus, -

Zeuge Andreas Könen: Ja.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): - weil Behördenleiter, die für Spionageabwehr zuständig sind, sagen, dass sie das noch nie gesehen haben.

Aber jetzt mal ernsthaft: In die BSI-Zeit - - Im Sommer 2013, wenn es darum geht, ob hier Spionage stattfindet, ob hier massenhaft Daten abgegriffen werden in Deutschland, da kommt man nicht auf die Idee, in die Snowden-Folien zu gucken und sich das anzuschauen und zu sagen: „Ach, guck mal, hier gibt es so Operationen ‚RAMPART-A‘, da betreiben die ganz offiziell eine Operation mit einem Partnerland, an der Glasfaser in dem Partnerland; aber irgendwie gibt es dann ein Secret Comint Network, wo heimlich Daten direkt in die USA ausgeleitet werden“? Also, damit hat sich das BSI nicht beschäftigt.

Zeuge Andreas Könen: Also, erstens kann ich jetzt hier aus der Folie nicht erkennen, woraus Sie ziehen „Geheimdaten abgeleitet“; aber das spielt auch gar keine Rolle.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das ziehe ich aus - -

Zeuge Andreas Könen: Ich müsste es einfach vermuten, das haben wir nicht getan. Und da es in dem Moment andere Folien gab, die deutlich wichtiger waren, und ein klarer Bezug zu Informationssicherheitsaufgaben hier nicht gegeben war - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das ist die interessante Frage, ob nicht sozusagen der Bundesnachrichtendienst, Ihr alter Arbeitgeber, Teil einer solchen Operation war. Die Frage kann man sich ja mal stellen. Und ich

komme darauf, dass das ein Secret Comint Network ist, weil das hier dransteht. Das hat die NSA da drangeschrieben, ja? So komme ich darauf.

Sagen Ihnen die Begriffe Site B, Site A, Site C was?

Zeuge Andreas Könen: Nein. Nein, außer dass es hier Bezeichner sind, nicht.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber das ist jetzt für so eine Frage, wo man abgreift, wo man verarbeitet, wo gespeichert wird - - Das kennen Sie so nicht.

Zeuge Andreas Könen: Nein, damit haben wir uns auch nicht auseinandergesetzt, weder ich persönlich - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Nein, kennen Sie diese Begrifflichkeiten?

Zeuge Andreas Könen: Nein, außer in ganz anderen Zusammenhängen - - gibt es natürlich den Begriff „Access Point“ oder „Processing Center“, aber ganz außerhalb dessen, was hier als Folie aus - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber auch dieses Site A, Site B, Site C nicht?

Zeuge Andreas Könen: Nein, nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Weil das scheint also auch - ich muss das so etwas abstrahiert sagen - gängiges Vokabular im Bundesnachrichtendienst zu sein nach meinem Aktenstand. Haben Sie aber nie gehört.

Zeuge Andreas Könen: Nein, also in der Form nie gehört.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Mhm. - Wissen Sie irgendwas über die Beendigung dieser Operationen „Eikonal“ und „Glotaic“?

Zeuge Andreas Könen: Nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Stand nicht zur Diskussion damals, bis 2006? Da gab es keine Schwierigkeiten?

Zeuge Andreas Könen: Also, kann ich mich absolut nicht dran entsinnen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Mhm.

Vorsitzender Dr. Patrick Sensburg: Okay. Jetzt wäre so der Zeitpunkt des Wechselns gekommen. - Und wir kommen jetzt zur nächsten Fraktion. Das ist die CDU/CSU Fraktion. Herr Kollege Schipanski stellt die Fragen.

Tankred Schipanski (CDU/CSU): Ja, Herr Vorsitzender. Vielen Dank. - Herr Zeuge, ebenfalls von unserer Seite ein herzliches Willkommen! - Herr Könen, ein Zeuge, der Herr Dr. Even, der Leiter der Spionageabwehr im BfV, machte hier deutlich, dass es eine enge Zusammenarbeit des BfV und des BSI gab mit Blick auf die Auswertung der Snowden-Folien. Das BSI hätte sich das angeschaut, hätte das bewertet. Der Zeuge Wingerath hat das ebenfalls noch mal deutlich gemacht, dass man sehr regelmäßig, auch vonseiten des BND, zurückgegriffen hat auf die Expertise des BSI. Vielleicht könnten Sie uns diese Zusammenarbeit noch einmal ein Stückchen verdeutlichen. Ist das formalisiert? Gibt es da regelmäßige Treffen? Macht man das nur auf Anfrage? Wie geht das vonstatten?

Zeuge Andreas Könen: Ja, es gibt mehrere Ebenen der Kooperation. Es gibt praktisch zunächst einmal die Zusammenarbeit im Cyber-Abwehrzentrum. Die ist institutionalisiert seit der Existenz. Das BfV ist ja Gründungspartner des Cyber-Abwehrzentrums. Dort arbeitet das BfV ja mit Personal vor Ort im BSI mit. Das ist also eine besonders enge Kommunikationsschnittstelle. Dort finden verschiedene, wöchentliche, wiederkehrende Besprechungen statt, in Rahmen derer Informationen also dann zwischen den Behörden ausgetauscht werden, im Falle von Cybersicherheitsvorfällen dann gegebenenfalls auch gemeinsames Vorgehen abgestimmt wird.

Da das Cyber-Abwehrzentrum noch nicht existierte in der Zeit vor allen Dingen jetzt vor zweitausendund - - jetzt muss ich selber erst mal nachrechnen - elf, ist es natürlich so, dass auch davor schon eine enge fachliche Kooperation bestand, die in ähnlicher Weise diese Informationen ausgetauscht hat.

Wir haben uns dann auch im Zuge der Veröffentlichungen von Herrn Snowden immer wieder ausgetauscht über technische Deutungen dessen, was da sichtbar wurde, in der Regel auf Einzelfallniveau, dann aber auch noch einmal sehr konzertiert in dem Moment, als eben die Gefährdung in Berlin-Mitte deutlich wurde, insbesondere durch die vermutliche Überwachung des Mobiltelefons der Bundeskanzlerin.

Tankred Schipanski (CDU/CSU): Okay. Das heißt, Sie hatten auch vor dem Cyber-Abwehrzentrum faktisch einen institutionalisierten Weg, wie Sie zusammengearbeitet haben. Sie haben sich da regelmäßig getroffen und ausgetauscht.

Zeuge Andreas Könen: Ja, mit 2009 und der Gesetzesänderung insbesondere zum Schutz der Regierungsnetze war das definitiv erforderlich geworden, da ja da das BfV auch genannt ist als der mögliche Partner, der zu involvieren ist, wenn aus unseren Erkenntnissen eventuelle Spionage gegen Deutschland offenbar wird.

Tankred Schipanski (CDU/CSU): Okay. - Und gab es auch mit anderen Behörden solche regelmäßigen Gesprächsrunden, oder primär nur BfV, BND?

Zeuge Andreas Könen: Mit BfV und BND auf jeden Fall. Mit dem Bundeskriminalamt in herausragender Weise für das gesamte Feld der Cyberkriminalität, in einem gewissen Maße auch schon sehr lange mit der Bundespolizei, da, wo vor allen Dingen auch aus dem polizeilichen Umfeld Gefährdungen deutlich werden, und dann darüber hinaus vor allen Dingen mit dem Bundesamt für Bevölkerungs- und Katastrophenschutz in der Zusammenarbeit für die kritischen Infrastrukturen - das BBK ist ja ebenfalls Gründungsmitglied des Cyber-Abwehrzentrums - - und darüber hinaus dann noch verschiedene andere Behörden, die ebenfalls zu diesen Themen beitragen konnten, allerdings nicht ganz auf regelmäßiger Basis.

Tankred Schipanski (CDU/CSU): Okay. - Nun finden sich in den Akten, die uns vorliegen, etliche Vorgänge, in denen das BSI die Veröffentlichung und die Snowden-Dokumente prüft und bewertet. Und teils wurde auch entsprechend Erlass in dem BMI auch berichtet, teils beantwortet das BSI auch Anfragen, etwa auch aus anderen Ländern. Davon, dass dem Ausschuss also keine Akten über Ihre Tätigkeit vorliegen, kann man da also mitnichten sprechen. Gleichwohl ist klar, dass in unseren und sehr umfangreichen Akten nicht sämtliche jemals veröffentlichte Dokumente aus dem Snowden-Fundus mitsamt einer Wertung des BSI zu finden sind. Wie können Sie sich das erklären?

Zeuge Andreas Könen: Das ist Arbeit, die vor allen Dingen auf technischer Ebene stattgefunden hat und die dann in vielen Einzelbewertungen endet, die in dieser Form dann nicht als Bericht zusammengetragen wurden. Berichtet wird im Wesentlichen über die Exzerpte, über die Gesamtbewertungen, über die Maßnahmen, die das BSI zu unternehmen gedenkt. Im Zusammenspiel vor allen Dingen mit dem BMI war das der gängige Weg. Und auf eine Einzelberichterstattung brauchte man an der Stelle auch keinen Wert legen. Das kommt jeweils in den Exzerpten, in den Positionierung der BMI-Berichte deutlich zum Zuge.

Tankred Schipanski (CDU/CSU): Also, das heißt, Sie haben nicht für jede einzelne Folie einen Bericht erstellt und zusammengefasst, technisch geprüft.

Zeuge Andreas Könen: Nein, da gab es keine Anforderung. Nein, nein. Da wurde zusammengefasst, technisch bewertet.

Tankred Schipanski (CDU/CSU): Okay. - Und inwiefern hatte das BSI denn den Auftrag erhalten, wirklich sämtliche Snowden-Dokumente plus entsprechende Berichterstattungen da zu überprüfen und zu sichten?

Zeuge Andreas Könen: Also, das haben wir aus eigenem Antrieb unternommen. Dazu kommen dann jeweilige Erlasse des Bundesinnenministeriums, wenn insbesondere durch neue Veröffentlichungen entsprechend Bedarf bestand, das eben auch in einer BSI-Bewertung zur Kenntnis zu nehmen. Also, ein riesiger, großer Teil ist durch unsere Mitarbeiter auch in Eigenarbeit unmittelbar zur Hand genommen worden, ohne lange aufgefordert zu werden.

Tankred Schipanski (CDU/CSU): Ja, wie kann man sich das vorstellen? Da hat man das in der Presse gelesen und ist der Sache als Mitarbeiter dann nachgegangen?

Zeuge Andreas Könen: Ja, es gab eine Gruppe von Personen, die benannt worden ist, die sich jeweils in den verschiedenen Abteilungen damit beschäftigen sollten. Und wir hatten auch Kollegen, die insbesondere in einem Monitoring dessen, was sich in der Medien- und Presselandschaft tut, dann jeweils die Fachleute darauf hinweisen konnten, ob jeweils wieder Veröffentlichungen dazu erschienen sind.

Tankred Schipanski (CDU/CSU): Ich würde mal ein konkretes Beispiel rausgreifen, um auch mal zu verdeutlichen, wie Ihre Arbeit funktioniert. Anlass waren Presseberichte darüber, dass die NSA und der GCHQ die Verschlüsselungsprotokolle https bzw. SSL/TLS entschlüsseln konnten. Das BSI hat noch am Tage des Erlasses des BMI - das war damals am 6. September 2013 - berichtet, und das BSI kam nach Analyse der Veröffentlichungen zu folgendem Schluss - ich zitiere -:

> Es ist davon auszugehen, dass neben versehentlichen Fehlern auch beabsichtigte Trapdoors in Implementierungen kryptographischer Mechanismen versteckt sind.

Zitat Ende.

Wenn Sie es brauchen, können wir Ihnen den Vorgang auch vorlegen; aber ich denke, -

Zeuge Andreas Könen: Ja.

Tankred Schipanski (CDU/CSU): - Sie kennen sich mit der Thematik entsprechend aus. Könnten Sie jetzt da den Vorgang mal erläutern, wie Sie mit so einer Information umgehen, wie das in Ihrem Hause da bearbeitet wird?

Zeuge Andreas Könen: Also, erstens muss man ganz klar differenzieren zwischen dem, was Sie im ersten Teil Ihrer Frage genannt haben, dem, was bei der Beschäftigung mit http, TLS und SSL herausgekommen ist, und der zitierten generischen Aussage aus unserem Bericht. Also, wir haben grundsätzlich festgestellt, dass in der Gesamtschau der Snowden-Dokumente es sich jeweils so verhält, dass die Kernalgorithmen, die kryptografischen Algorithmen, die heute gängigen Standards und Verfahren zugrunde liegen, auch nach Durchsicht dieser Dokumente im Wesen- - also als sicher zu gelten haben.

Ich möchte ein Beispiel nennen: Das ist etwa das AES-Verfahren; das ist das Verfahren zu Public-Key-Verfahren, was auf elliptischen Kurven beruht. Solche Basisdinge, dazu gibt es keine Aussage der Snowden-Papiere, dass da irgendwelche Angriffe oder Manipulationen gefahren werden.

Dann: Anders verhält es sich - und das ist genau die Aussage des Berichtes - bei der Implementierung solcher Verfahren in konkreter Hard- oder Software. Da ist es auf der einen Seite so, dass aus den Snowden-Papieren deutlich wird, dass sehr konsequent danach gesucht wird, ob Hersteller solche Fehlimplementierungen vorgenommen haben, ob das für die Erfassung der NSA ausbeutbar ist. Solche Schlüsse lassen sich ziehen aus dem, was die Snowden-Dokumente vielfältig zeigen.

Darüber hinaus kommen dann immer wieder Indikatoren, die es vermuten lassen, dass das auch aktiv durch die NSA betrieben wurde. Das ist allerdings an dieser Stelle extrem schwer nachvollziehbar, weil man dazu mehr wissen müsste als das, was in den reinen Papieren steht, nämlich über welche Wege das erfolgt ist. Wenn Sie eine Schwachstelle sehen, können Sie nur mit extremer Mühe feststellen, ob sie absichtlich oder unabsichtlich gesetzt wurde. Fakt ist aber: In den

Implementierungen gibt es Schwachstellen, und diese wurden konsequent ausgenutzt.

Tankred Schipanski (CDU/CSU): War dieses Problem der Implementierung, was Sie gerade beschrieben haben, eine neue Erkenntnis, die Sie durch diese Snowden-Sachen da gewonnen haben, oder war Ihnen das bekannt, aber nicht in dieser Stärke?

Zeuge Andreas Könen: Nein. Wir kennen sehr wohl das Problem, erstens, was aus Qualitätsmanagement bei Herstellern von Hard- und Software entsteht bei kryptografischen Algorithmen. Das ist ja auch der Grund, warum wir immense Aufwände haben, zu zertifizieren, im Rahmen der Zertifizierung dann auch zu evaluieren und genau sicherzustellen, dass die Implementierung dessen, was wir etwa in technischen Richtlinien vorgeben, auch genau so erfolgt. Das ist also ein altbekanntes Problem. Auch die Vermutung, dass es nachrichtendienstliche Tätigkeit gibt, im Rahmen derer solche Fehlimplementierungen dann forciert werden. Auch das ist ganz deutlich immer gewesen. Darum auch der stabile Grundsatz in deutschen Infrastrukturen, möglichst nur entsprechend zertifiziertes oder zugelassenes Gerät einzusetzen, bei dem sowohl Qualitätsmanagement als auch Sicherheitsmanagement stimmen.

Tankred Schipanski (CDU/CSU): In den Akten findet sich eine, ich möchte es mal nennen, reaktive Sprachregelung des BSI, die unter anderem den Hinweis an die Anwender enthält, man möge einen Browser nutzen, der den neuesten, sichersten Standard unterstützt. In einer internen E-Mail kritisiert einer Ihrer Mitarbeiter im BSI diesen Ratschlagt als, ich möchte mal sagen, zu schlicht. Er schreibt an einen Kollegen - ich zitiere -:

> Die Wahrheit ist: Wenn ein Produkt mit Kryptobestandteilen die USA verläßt, hat es das Exportkontrollverfahren durchlaufen, ist damit grundsätzlich nicht mehr sauber und potenziell gefährlich im Hinblick auf die diskutierten Angriffe.

Wir können Ihnen auch das Dokument vorlegen lassen, -

Zeuge Andreas Könen: Ja.

Tankred Schipanski (CDU/CSU): - wenn Sie mögen. Meine Frage ist jetzt: Ist das nur ein besonders meinungsstarker Mitarbeiter, oder entspricht diese Bewertung dieses Mitarbeiters auch Ihrer Einschätzung?

Zeuge Andreas Könen: Also, erstens ist es ein meinungsstarker Mitarbeiter; das kommt schon aus dem Text heraus, und das spiegelt auch genau die Diskussion wider, die wir hatten. Nur, man darf das Kind nicht mit dem Bade ausschütten. Da, wo wir Produkte, auch von US-Herstellern, eben einer sorgfältigen Evaluierung und Zertifizierung unterziehen, das Unternehmen gewissen Vertrauensstandards genügt, die wir auch jeweils einer Zertifizierung voranschicken - - Wenn das Unternehmen im Prozess mit tätig war und diesen Evaluierungsprozess unterstützt hat und am Ende sich die Qualität auf dem jeweils geforderten Zertifikatsniveau bewegt, dann muss man das auch klar konstatieren. Ein pauschales Urteil in der Form, wie es der Kollege dann abgegeben hat, das ist insgesamt dann in einer differenzierten Haltung nicht durchzuhalten. Das muss man klar sagen. Aber es dient natürlich der internen Debatte und ist auch klar bei den Mitarbeitern dann auszusprechen.

Tankred Schipanski (CDU/CSU): Und wenn man das jetzt ein Stückchen weiterdenkt: Hat denn das BSI Erkundigungen eingeholt bei amerikanischen Partnern, Regierungsstellen, Firmen, wie es sich zu diesem Sachverhalt verhält?

Zeuge Andreas Könen: Ja, wir haben das in vielen Einzelthemen getan, wo es sich eben insbesondere bei der Netzsicherheit und der Mobilkommunikationssicherheit in Einzelfällen anbot und diese Hersteller dann etwa auch auf deutschem Boden tätig waren. Wir haben es sehr deutlich angesprochen in Zertifizierungsverfahren. Wir haben da nochmals einen Takt eingefügt, der vor allen Dingen sicherstellen soll, dass die Unternehmen vertrauenswürdig sind, dass sie entsprechende Erklärungen abgeben, dass auch

das, was sie uns an Unterlagen zur Verfügung stellen - - dass das Wissen über die Implementierungen dann auch Nicht-Nachrichtendiensten zugänglich gemacht wird oder erst recht, falls diese Firmen in einer Implementierung des Verfahrens direkt beteiligt sind, dass da auch keinerlei solche Maßnahmen vorgenommen werden. Das gehört heute definitiv dazu, in einer Zertifizierung allemal.

Es ist auch noch weiter so gewesen, dass wir sehr deutliche Gespräche geführt haben mit Herstellern, dann allerdings auch aus noch mehr Ländern, um ganz glasklar unsere Position deutlich zu machen, was wir von einem Hersteller an Vertrauensbasis erwarten. Und in den letzten Jahren hat das auch spürbar zu einer Bewegung geführt. Alleine repräsentiert sich das dadurch, dass unsere Zertifizierung solcher Produkte deutlich zugenommen hat. Die Hersteller sehen den Vorteil einer solchen transparenten Methode.

Tankred Schipanski (CDU/CSU): Okay. - Sie hatten ja vorhin angedeutet, dass wir in Deutschland eigentlich gar nicht mehr diese Hardware teilweise selber herstellen.

Zeuge Andreas Könen: Mhm.

Tankred Schipanski (CDU/CSU): Jetzt noch mal aus Ihrer fachlichen Perspektive her: Müsste man nicht von politischer Seite ein Stückchen eventuell durch Förderprogramme, Ähnliches dafür sorgen, dass deutsche Firmen bei der Eigenentwicklung solcher Produkte wieder viel mehr gefördert werden?

Zeuge Andreas Könen: Definitiv. Also, wir unterstützen das massiv. Sie haben ja auch in meinem Eingangsstatement die Schlussforderungen gehört. Das brauchen wir ganz dringend wieder. Nur, wir müssen auch realistisch sein: Es gibt Technologiesektoren - das Thema Mobiltelefonie war heute schon da -, in denen wir definitiv keine deutschen und oft sogar keine europäischen Hersteller mehr haben. Wir sind darauf angewiesen, dass wir in einer Kompensation mehr Einblick erhalten in die IT und in der Lage sind, eigene IT-Sicherheitsmechanismen dort erfolgreich einzusetzen. Das ist sozusagen die gesamte Prozesskette, die wir da im Auge behalten müssen, und die Möglichkeit, eben dann auch unsere eigenen Sicherheitsvorkehrungen treffen zu können - immer abhängig natürlich auch vom Einsatzgebiet. Es gibt Einsatzgebiete, etwa im Geheimschutz für deutsche Behörden. Da müssen wir definitiv und klar auf deutsche Technologien mit entsprechender Herstellungsgarantie in Deutschland und auch entsprechende Einsatzbedingungen setzen.

Tankred Schipanski (CDU/CSU): Ich möchte noch mal auf die Regierungskommunikation zu sprechen kommen und auf die beiden Netze oder die Netzinfrastruktur, die wir in Deutschland haben: zum einen das IVBB, das andere ist dann der IVBV/BVN sowie das Bund-Länder-Verbindungsnetz. Während das IVBB von der Deutschen Telekom betrieben wird, wurde ja das IVBV/BVN über mehr als zehn Jahre, also mindestens von 2005 bis 2015 -

Zeuge Andreas Könen: Ja.

Tankred Schipanski (CDU/CSU): - von einem US-Unternehmen - Sie wissen es -, Verizon, betrieben. Und im Juni 2014 teilte das BMI mit, die Bundesregierung wolle vor dem Hintergrund der NSA-Affäre die Zusammenarbeit mit dieser Firma schrittweise beenden und zukünftig eine „Infrastruktur mit erhöhtem Sicherheitsniveau“ bereitstellen, die einheitlich durch einen Partner betrieben wird, bei dem - ich zitiere - „auch Krisenregelungen und Eingriffsmöglichkeiten durch den Bund bestehen“. Jetzt würde mich interessieren, was denn die Gründe für die Entscheidung waren, diese Zusammenarbeit mit Verizon zu beenden.

Zeuge Andreas Könen: Zunächst füge ich eine Sache hinzu: Also, die Zusammenarbeit ist noch nicht komplett beendet, die Ablösung läuft weiterhin - um das einfach nicht als falschen Hintergrund im Raum stehen zu lassen.

Aber die Beweggründe sind ganz klar: Mit einem deutschen nationalen Provider für alle diese Netzinfrastrukturen haben wir deutlich bessere Möglichkeiten in der Kooperation mit dem Un-

ternehmen, deutsche Sicherheitsstandards einzufordern, etwa auch das Unternehmen in voller Weise den Forderungen des deutschen Geheimschutzes dann zu unterwerfen und damit auch in einer direkten Zusammenarbeit garantieren zu können, dass das, was beim Auftragnehmer abläuft, ebenfalls unseren Sicherheitsanforderungen genügt. Das ist mit einem Hersteller, der komplett eben sich auf - - sein Angebot auf deutschem Boden hat, der sie auch von einer Zentrale in Deutschland aus verwaltet, unter deutschem Recht deutlich einfacher zu machen als mit einem Unternehmen, das irgendwo im Ausland eine Muttergesellschaft hat, auch wenn es eine Gesellschaft deutschen Rechts ist. Das war der innere Beweggrund.

Diese sicherheitlichen Anforderungen haben wir dann insbesondere bei der Fortschreibung des IVBB hin zu den Netzen des Bundes zum Grundprinzip gemacht und nochmals da auch durchgehend sicherheitlich begründet, warum solch eine nationale Dienstleistung notwendig ist und auch dann schließlich und endlich auch auf EU-Ebene anerkannt wurde.

Tankred Schipanski (CDU/CSU): Lagen denn dem BSI konkrete Hinweise vor, die auf eine Ausleitung von Kommunikation oder eine mit Hilfenahme durch den Netzbetreiber, in dem Fall von Verizon, geführte Telekommunikation durch Nachrichtendienste der Five Eyes, in irgendeiner Art und Weise hingedeutet hätten?

Zeuge Andreas Könen: Nein, Erkenntnisse lagen nicht vor. Alle Unternehmen, die zu dem Zeitpunkt eine zentrale Rolle für die Kommunikation des Bundes spielten, eben die Deutsche Telekom AG, Verizon als zweites und DE-CIX, sind beide - alle drei, Entschuldigung - in einem Brief mehreren Fragen ausgesetzt worden, ob denen selber Erkenntnisse dazu vorliegen, dass solche Zugriffe auf Daten stattfinden oder dass es Wege gibt, diese Zugriffe in irgendeiner Form zu ermöglichen, oder sonstige Vereinbarungen bestehen zur Ausleitung solcher Daten. Alle Unternehmen haben darauf klar geantwortet, dass dies nicht der Fall sei. Und eigene Erkenntnisse, wie gesagt, liegen nicht vor.

Tankred Schipanski (CDU/CSU): Okay. - Das BSI hat nun am 21. August 2013 eine Revision dieses besagten Netzes vorgenommen bei dem entsprechenden amerikanischen Betreiber. Und in einer Unterrichtung aus dem BMI vom 12. Februar 2014 steht nun, dass das BSI, wie Sie das schon gerade formulierten, eigentlich einen positiven Gesamteindruck gewonnen habe. Dieser Eindruck wird aber vom Referat IT 5 des BMI ausdrücklich nicht geteilt, und daher hat das BMI dann eben empfohlen, diese Vertragsbeziehung auch zu beenden. Wie erklären Sie sich das jetzt, dass Sie als BSI ja eigentlich sagen: „Das passt alles“, und jetzt sagt das BMI „Nein, wir machen das trotzdem anders“?

Zeuge Andreas Könen: Also, unsere Bewertung kam aus der fachlichen Betrachtung vor Ort zustande, die nach den Grundsätzen eben einer IS, also Informationssicherheitsrevision, durchgeführt wurde. Alles das, was wir vor Ort, was unsere Mitarbeiter dort vor Ort gesehen haben, entsprach unseren Anforderungen. Also war aus dieser Auseinandersetzung auf dem gängigen Weg der Revision kein anderer Schluss möglich, als dass die Implementierungen unseren Ansprüchen genügen. Wie der Schluss dann im Einzelnen, vielleicht auch noch unter anderen politischen Aufstellungen, bei IT I 5 zustande gekommen ist, das kann ich - - muss ich Sie bitten, das an der Stelle nachzufragen, die diese Entscheidung getroffen hat.

Natürlich ist es klar aus der eben dargestellten grundsätzlichen Erwägung, dass es eben durchaus besser und leichter geht, mit einem deutschen Anbieter alle diese Regularien zu treffen, die vor allen Dingen die Vertrauenswürdigkeit des Unternehmens berühren. Das mag, vermute ich mal, die entscheidende Rolle gespielt haben.

Tankred Schipanski (CDU/CSU): Sie haben am Anfang auch noch mal ein bisschen bei den Motiven erklärt. Aber in der Tat muss man da das BMI fragen; da haben Sie Recht.

Die Bundesregierung - ich würde mich noch mal kurz dem Thema XKeyscore zuwenden, bevor wir durch sind - hat dazu erklärt, dass im Jahr 2011 eine Präsentation dieses Tools XKeyscore

durch den BND stattgefunden hat, bei der auch Mitarbeiter des BSI anwesend waren. Diese Präsentation im Oktober 2011 in Bad Aibling war bereits Gegenstand verschiedener Zeugenbefragungen hier. Waren Sie denn damals mit diesem Thema XKeyscore befasst, oder können aus eigener Wahrnehmung etwas zu diesem Treffen beitragen?

Zeuge Andreas Könen: Also, erstens: An dem Treffen selber habe ich nicht teilgenommen. Zweitens wurde ja im Nachgang darüber durch die Kollegen, die dort vor Ort waren, berichtet. Die Konsequenz, die wir aus der Beschreibung der Kollegen gezogen haben, war die, dass wir gesagt haben, dass das, dieses Tool, für die Aufgaben des BSI keineswegs nutzbringend ist. Das lässt sich auch deutlich erläutern. XKeyscore ist ein Tool, das auf Inhaltsebene selektiert, und unsere Aufgaben erfordern eine Selektion auf Protokollebene, also auf technischer Ebene, nicht da, wo die eigentlichen Nutzdaten transportiert werden. Damit war von vornherein klar, dass dieses Tool für unsere Aufgaben an keiner Stelle nutzbar ist.

Tankred Schipanski (CDU/CSU): Und das hat sich auch bis zum heutigen Zeitpunkt nicht geändert, oder war das BSI in der Folgezeit, nach dieser Präsentation oder Ähnlichem, oder jetzt in jüngster Zeit mit XKeyscore beschäftigt oder hat das geprüft oder zertifiziert oder was auch immer?

Zeuge Andreas Könen: Außerhalb des Untersuchungszeitraumes gibt es tatsächlich eine Anforderung des BfV in dieser Richtung, die aber das BSI jetzt in ganz anderer Weise adressiert, nämlich als Berater in der IT-Sicherheit und im Geheimschutz.

Tankred Schipanski (CDU/CSU): Okay. Da das außerhalb des Untersuchungszeitraumes ist, wollen Sie darauf wahrscheinlich nicht näher eingehen.

Zeuge Andreas Könen: Nein. Also, was ich dazu vielleicht abstrakt hinzufügen kann, um Sie einfach da ein bisschen mitzunehmen, wie das grundsätzlich funktioniert: Es ist natürlich so, dass gerade eben auch wegen der Tatsache, dass viele Technologien in Deutschland nicht mehr eingekauft werden können, deutsche Nachrichtendienste und Polizeien sehr wohl Produkte auch ausländischer Provenienz in vielen Fällen einsetzen. Wenn das in einem Bereich passiert, der dann Geheimschutzbedingungen unterliegt, dann erfolgt das nach § 39 der VSA. Das BSI wird beteiligt, um im Rahmen einer Geheimschutzbewertung diese Installation unter die Lupe zu nehmen, da insbesondere Penetrationstests durchzuführen und sich die Gesamtkonzeption, die IT-Sicherheitskonzepte, die Geheimschutzkonzepte heranzuziehen, genau anzuschauen und auf Basis dieser Prüfung dann eine entsprechende Freigabeempfehlung an den jeweiligen Behördenleiter auszusprechen. Und auf Basis dieser Freigabeempfehlung unter Berücksichtigung weiterer behördenspezifischer Gesichtspunkte kann dann der Behördenleiter die Nutzung dieses Geräts anordnen.

Tankred Schipanski (CDU/CSU): Gut. Dann lassen wir das mal so stehen und machen in der nächsten Runde weiter. Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Dann kommen wir zur zweiten Fragerunde, wenn noch Fragen in öffentlicher Sitzung sind.

(Martina Renner (DIE LINKE): Ja, klar!)

- Ja, weil manche Fragen dann jetzt auch so bisschen den Anklang hatten, dass sie der Zeuge Schallbruch eher beantworten kann, wenn ich es richtig einschätze.

(Martina Renner (DIE LINKE): Ja, aber wir haben erst eine Runde gehabt!)

- Ja, klar. - Frau Kollegin Renner beginnt dann für die Fraktion Die Linke.

Martina Renner (DIE LINKE): Herr Könen, ich war vorhin nicht so schnell mit dem Stift. Könnten Sie mir noch mal im Leitungsstab Ihre Dienststellenbezeichnung nennen?

Zeuge Andreas Könen: Ja. BND-Leitungsstab.

Martina Renner (DIE LINKE): Nein, 90.

Zeuge Andreas Könen: Ja, das ist ja BND-Leitungsstab. 90AD.

Martina Renner (DIE LINKE): 90AD.

Zeuge Andreas Könen: AD.

Martina Renner (DIE LINKE): Das sind Sie, wenn ich hier ins Organigramm gucke.

Zeuge Andreas Könen: Das war ich damals, ja.

Martina Renner (DIE LINKE): Okay, gut. - Und Sie sagten eben, bei der Besprechung in Bad Aibling zu XKeyscore waren Sie nicht dabei. Aber haben Sie sonst mal die Außenstelle Bad Aibling besucht?

Zeuge Andreas Könen: Ich war da mal; aber das war nicht während des Zeitraums im Leitungsstab. Ich war mal in Bad Aibling, ja.

Martina Renner (DIE LINKE): Wann war das?

Zeuge Andreas Könen: Kann ich Ihnen beim besten Willen nicht mehr sagen. Ich weiß, dass ich da war, aber nicht mehr, wann.

Martina Renner (DIE LINKE): Was haben Sie dort besucht? Gab es da die JSA schon?

Zeuge Andreas Könen: Das kann ich Ihnen nicht sagen. Da ich nicht ein - - Das spielte da auch in dem Zusammenhang keine Rolle mehr. Ich weiß, dass ich Kollegen des Bundesnachrichtendienstes besucht habe.

Martina Renner (DIE LINKE): Sie haben nicht dort Kollegen der NSA besucht.

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): Ausschließlich waren dort Kollegen - -

Zeuge Andreas Könen: Nach meiner Erinnerung war das ein reines Besprechungsthema in - - Wie gesagt, ist auch außerhalb der Leitungsstabzeit, also in der Zeit davor, die eben nicht vom Untersuchungsgegenstand berührt ist.

Martina Renner (DIE LINKE): Hatten Sie denn in Ihrer Zeit im Leitungsstab mit der NSA zu tun?

Zeuge Andreas Könen: Ich kann jetzt im Einzelnen nicht mehr nachvollziehen, ob ich bei Besuchen entsprechender hochrangiger Personen im Einzelnen anwesend war. Ich weiß nur, dass ich in Begleitung von Präsident, Vizepräsident bei irgendwelchen multilateralen Veranstaltungen NSA-Mitarbeiter gesehen und getroffen habe; aber das ist, wie gesagt, außerhalb des ganzen Themas.

Martina Renner (DIE LINKE): Das Problem: Bei unserer Vorbereitung hatten wir Ihre Dienststellenbezeichnung nicht, -

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): - und deswegen hatten wir keine Möglichkeit, zu sehen, an welchen Aktivitäten Sie teilgenommen haben. Es hätte uns das erleichtert. Wir wussten nur: Leitungsstab.

Bei diesen Terminen, an die Sie sich erinnern mit der NSA, ging es dort auch um SIGINT? Liegt sehr nahe bei 90AD.

Zeuge Andreas Könen: Ja, es war eine größere Konferenz in dem Bereich. Aber, wie gesagt, da ist mir auch das Datum in der Zeitspanne zwischen 2005 und 2006 nicht mehr präzise erinnerlich, dass - - Ja, genau.

Martina Renner (DIE LINKE): Und ging es dort auch um Datenerfassung am Kabel?

Zeuge Andreas Könen: Das kann ich im Einzelnen nicht mehr erinnern. Ich war damals als Begleiter, wenn ich es recht im Sinn habe, eines Vizepräsidenten auf dieser Veranstaltung. Das war etwas - das ist, glaube ich, hier auch schon berührt worden - - SIGINT Seniors Europe heißt

die Gesamtveranstaltung. Aber größeres Veranstaltungsformat; genaue, präzise Tagesordnungspunkte nicht mehr in Erinnerung.

Martina Renner (DIE LINKE): Kennen Sie den Belgacom-Fall?

Zeuge Andreas Könen: Ja. Über den ist ja auch mehrfach schon in anderen Ausschüssen gesprochen worden. Korrekt.

Martina Renner (DIE LINKE): Welche Schlussfolgerungen haben Sie aus diesem Vorgang gezogen hinsichtlich der Frage, inwieweit es durch Five-Eyes-Staaten Angriffe geben könnte auf Kommunikation in Deutschland?

Zeuge Andreas Könen: Also, unsere Bewertung dieses Falles ist technisch erfolgt. Wir haben uns genau eben das, was in einzelnen Veröffentlichungen auch deutlich sichtbar ist, Koinzidenzen zwischen Quellcodes verschiedener Angriffswerkzeuge, ebenfalls angeschaut, und damit wird zumindest deutlich, dass es sich hier um Angreifer handelt, die aus ein und derselben Quelle eben entsprechende Angriffswerkzeuge und Codes schöpfen.

Martina Renner (DIE LINKE): Welche Konsequenz hat man dann daraus gezogen, nachdem man den möglichen Angreifer identifiziert hatte?

Zeuge Andreas Könen: Ja, wir haben ja nicht den möglichen Angreifer identifiziert; wir haben das Angriffswerkzeug untersucht. Den Angreifer zu identifizieren, ist nicht Aufgabe des BSI. Das ist in dem Zusammenhang in der Angreiferermittlung bei Angriffen auf deutsche Infrastruktur Aufgabe des BfV. Ansonsten haben wir natürlich die technischen Rückschlüsse daraus gezogen und haben genau diese Malware und die Strukturen, die da deutlich wurden, genutzt, um das zu blocken und entsprechend abwehren zu können.

Martina Renner (DIE LINKE): Hat dieser Fall bei der Bewertung der Snowden-Dokumente dann auch eine Rolle gespielt?

Zeuge Andreas Könen: Er ist da mit bewertet worden, natürlich. Ich würde jetzt sagen, dass er natürlich eine herausragende Rolle spielt - das haben wir auch mehrfach dargestellt in verschiedenen Gremien -, weil er eben eine sehr ausgefeilte Version eines Advanced Persistent Threat ist, der über sehr, sehr viele verschiedene Ebenen Angriffe verübt. Das kann man durchaus als ein hochprofessionelles Tool bezeichnen.

Martina Renner (DIE LINKE): Gab es andere vergleichbare Vorgänge, die Sie aufgefunden haben?

Zeuge Andreas Könen: Vergleichbare Angriffswerkzeuge?

Martina Renner (DIE LINKE): Mhm.

Zeuge Andreas Könen: Durchaus. Also, im Rahmen der letzten zwei Jahre, was wir da vor allen Dingen gesehen haben oder - -

Martina Renner (DIE LINKE): Ich meine, wir reden hier nur über die Five Eyes. Das muss ich mal vorwegschicken.

Zeuge Andreas Könen: Ja, nein. Also, ich würde sagen, in der Angriffslandschaft haben wir viele gesehen. Es gibt auch noch andere Angriffsmethoden, die wir in den Dokumenten analysiert haben von Snowden. Da sind unterschiedliche Grade und Klassen drin. Das ist sicher ein herausragendes Instrument. Ich könnte jetzt persönlich mich nicht erinnern. Wahrscheinlich gibt es noch anderes Vergleichbares, ja.

Martina Renner (DIE LINKE): Sie haben ja sicherlich verfolgt - - Ich hatte Sie ja vorhin gefragt, ob Sie aus Ihrer BND-Zeit die NSA-Selektorenproblematik kennen. Haben Sie verneint. Aber mittlerweile kennt das BSI ja die NSA-Selektorenproblematik.

Zeuge Andreas Könen: Die Problematik. Die Selektoren kenne ich nicht, und die Problematik kenne ich aus dem Nachvollziehen der politischen Debatte, ja?

Martina Renner (DIE LINKE): Na ja, gut. Es ist ja ein Teil der Selektoren auf WikiLeaks veröffentlicht. Und darunter befinden sich ja auch Telefonnummern aus dem Festnetzbereich des IVBB.

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): Und hat sich das BSI dann mal Gedanken gemacht, wenn ich die NSA-Selektoren benutze aus dem Festnetzbereich des IVBB, auf welchen Datenpool man diese ansetzt, die Selektoren?

Zeuge Andreas Könen: Also, wir haben uns damit auseinandergesetzt, was es bedeutet, wenn ein Nachrichtendienst etwa diese IVBB-Telefonnummern oder andere Kenngrößen als Selektor einsetzt, wie die Bedrohungslage, die sich daraus konstituiert, aussieht. Und das haben wir einer ausführlichen Würdigung unterzogen, auch auf Basis der Daten, die uns daraus klar wurden. Da wird vor allen Dingen deutlich: Ja, damit ist jegliche Kommunikation, die auf diese etwa gewählten Nummern kommt und nicht verschlüsselt ist, natürlich auch wiederum zugänglich. Das ist aber genau das, was wir in vielen Warnszenarien immer wieder predigen. Aber die entscheidende Aussage ist die: Das geht genau bis zur Grenze des IVBB, und es gibt keine Indikatoren, dass hinter den Schutzwällen des IVBB irgendetwas passiert ist. Es ist eine reine Rufnummernselektion.

Martina Renner (DIE LINKE): Sie sagten ja vorhin, die Verizon-Ablösung läuft noch.

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): Wäre das nicht eine Möglichkeit, auf die Daten des IVBB zuzugreifen?

Zeuge Andreas Könen: Nein. Exakt das ist noch, auch im Zuge der bereits von Herrn Schipanski erwähnten Prüfungen, geprüft worden. Da sämtliche Daten des IVBB in dem Moment, wenn sie durch den Provider Verizon transportiert sind, verschlüsselt sind, ist auf die Inhalte der Daten kein Zugriff und da es über Kanäle, also VPNs, transportiert wird, auch keine Sichtbarkeit der direkten Metadaten da, sondern es ist nur der Kanal zu sehen, der von einem Standort Verizon zum nächsten Standort Verizon geht. Und auch die Verschlüsselung obliegt unserer Hoheit.

Martina Renner (DIE LINKE): Und wie sieht das an den Übergabepunkten des IVBB in andere Netze aus?

Zeuge Andreas Könen: Die unterliegen jeweils auch immer dem Schutz, den wir im Rahmen der Gesamtkonstruktion Netze des Bundes konstruiert haben. Das obliegt entweder dem Auftragnehmer unter Anleitung des BSI, aber an der Stelle eben im Wesentlichen des BSI, bis es die Grenze der Netze verlässt, die zu anderen Partnern gehen. Da ist dann auch eine deutliche sicherheitliche Grenze erreicht.

Martina Renner (DIE LINKE): Und bei diesen Übergabepunkten, sind dort auch welche dabei zu US-Provider-Anbietern?

Zeuge Andreas Könen: Nein. Diese Übergabepunkte von IVBB oder BVN finden immer an einem deutschen Standort zum deutschen Teil des jeweiligen Provider-Netzes statt, nicht etwa unmittelbar zu einer Mutter, die sonst wo loziert ist.

Martina Renner (DIE LINKE): Und das war auch immer so, oder ist das jetzt erst so?

Zeuge Andreas Könen: Nein, das war auch immer so. Das war immer deutscher Standort. Es hat niemals eine - oder deutsches Unternehmen oder GmbH in dem Sinne - Übergabe jenseits der Grenzen stattgefunden.

Martina Renner (DIE LINKE): Weil wir fragen uns natürlich, ob es wirklich nur so ist, dass die NSA-Selektoren eingesetzt werden auf Datenpools, die durch Abgriffe von außen mit Kommunikation rein ins IVBB passieren, oder ob es eben auch die Möglichkeit gibt - ist ja auch einer unserer Untersuchungsgegenstände - - inwieweit es sozusagen außerhalb der Kooperation mit dem BND noch eigene Überwachungsmaßnahmen der NSA in Deutschland gegeben hat. Haben Sie diese Frage mal erörtert: „Geht die NSA irgendwo in Deutschland außerhalb von Operation ‚Eikonal' - Nachfolgeprojekt möglicherweise, keine Ahnung, Kooperation an DE-CIX oder was auch immer - irgendwo ans Kabel, alleine, ohne den BND?"?

Vorsitzender Dr. Patrick Sensburg: Das müsste dann die letzte Frage sein.

Zeuge Andreas Könen: Also, außerhalb der Zuständigkeitsbereiche, sprich: Netze des Bundes, könnte ich da nur drüber spekulieren. Dazu haben wir keinerlei Möglichkeit, in irgendwelche Daten hineinzuschauen oder irgendwelche Dinge zu erörtern. Wir haben das natürlich, wie ich schon sagte, in der Abfrage bei der Deutschen Telekom AG, bei Verizon, der deutschen GmbH, und bei DE-CIX genau in den konkreten Fällen erfragt, wie gesagt, mit negativer Antwort. Dort war nichts bekannt. Da müssen wir uns natürlich auf die Aussage verlassen. Wir haben natürlich auch eine permanente Prüfung über Datenabflüsse im IVBB selber und können darum mit wirklich sehr hoher Wahrscheinlichkeit sagen, dass wir keine konzertierten Datenabflüsse aus dem IVBB oder Ähnlichem heraus sehen - da, wo wir das kontrollieren. Nein, es sind immer die typischen Fälle von Cyberangriffen.

Vorsitzender Dr. Patrick Sensburg: Okay. Ganz herzlichen Dank. - Dann kommen wir jetzt in der zweiten Runde zur Fraktion der CDU/CSU. Herr Kollege Schipanski.

Tankred Schipanski (CDU/CSU): Ja, vielen Dank, Herr Vorsitzender. - Herr Zeuge, ich würde noch mal kurz da weitermachen, wo wir vorhin aufgehört haben, bei dieser XKeyscore-Frage. Jetzt hatten wir hier den Leiter der Abteilung 3 im BfV, den Zeugen Berzen, gehabt, der ausdrücklich sagte, dass das BSI seiner Kenntnis nach in Bezug auf die Hardware bei XKeyscore durchaus eingebunden war. Und das wollte ich jetzt Sie einfach noch mal fragen, ob das so stimmt, dass Sie eben mit Blick auf die Hardware da eingebunden waren, bei der Erprobung vielleicht doch irgendwo mitgewirkt haben als BSI.

Zeuge Andreas Könen: Also, wie gesagt, wir haben das System damals, wenn man sich etwa auf diese Vorstellungen bezieht und auf den Zeitraum, in dem wir diesen Kontakt zu XKeyscore überhaupt das erste und einzige Mal in der Form hatten - - haben wir selber keine eigenen Tests durchgeführt, wir haben keine eigene Betrachtung irgendwelcher Hardware oder Software durchgeführt. Wir haben eine reine Präsentation erhalten, wie das System funktioniert, und daraus unsere Schlüsse gezogen.

Tankred Schipanski (CDU/CSU): Und bei der Hardware für G-10-Maßnahmen und so was, müssen Sie das zertifizieren, sich anschauen. Das gab es bei dieser Sache nicht.

Zeuge Andreas Könen: An dem Zeitpunkt nicht. Es mag ja sein, dass der Kollege sich da auf das bezieht, was jetzt akut abläuft.

Tankred Schipanski (CDU/CSU): Also, jetzt akut - das hatten Sie vorhin ja auch dargestellt - machen Sie das ja auch.

Zeuge Andreas Könen: Das hatte ich ja eben skizziert, wie - -

Tankred Schipanski (CDU/CSU): Ja, aber zum damaligen Zeitpunkt bei dieser Besprechung nicht. Und vielleicht meinte ja Herr Berzen eben das, was jetzt gegenwärtig läuft.

Zeuge Andreas Könen: Nein, also das könnte ich jetzt nicht auseinanderhalten. Das ist nicht der Fall gewesen, dass wir uns da mit der Hardware beschäftigt hätten.

Tankred Schipanski (CDU/CSU): Okay. - Dann noch ein ganz anderer Themenbereich, der uns aber hier natürlich auch beschäftigt: Stichwort Geolokalisierung durch Handynummern. Jetzt haben wir hier in dem Ausschuss so zahlreiche Zeugenaussagen zu diesem Thema gehört, welche Arten von personenbezogenen Daten dazu geeignet sein können, eine Lokalisierung von Personen in Gebieten zu ermöglichen, in denen - das ist ja der Aufhänger gewesen - die USA Drohneneinsätze durchführen. Ist Ihnen diese Problematik bekannt oder ein Begriff? Waren Sie damit einmal befasst gewesen?

Zeuge Andreas Könen: Also, die Problematik ist mir natürlich bewusst, da ich ja auch das mit verfolge, was hier diskutiert wird. Aber wir haben entsprechende Anfragen tatsächlich erhalten.

Nur das ist ja ein Gegenstand, der noch jetzt Objekt eines Beweisbeschlusses ist, der von Ihrer Seite aussteht.

Tankred Schipanski (CDU/CSU): Also, die Frage ist doch, ob - -

Vorsitzender Dr. Patrick Sensburg: Dazu Herr Akmann.

MR Torsten Akmann (BMI): Ja, vielen Dank, Herr Vorsitzender. - Herr Könen, ich denke, Sie können schon darstellen, wie da momentan in der Sache Ihr Kenntnisstand ist.

Zeuge Andreas Könen: Ja, gut. - Also, wenn wir über den Kenntnisstand zu Lokalisierung insgesamt reden, dann muss man ganz klar natürlich sagen - da gebe ich Ihnen auch gerne Auskunft zu -, dass sich das BSI damit deutlich beschäftigt hat. Es ist ja so, dass Informationen über Personen nicht nur erlangt werden dadurch, dass man deren Kommunikation im Einzelnen abhört, sondern dass man auch ihre Position bestimmt.

Jetzt gibt es da natürlich mehrere Ebenen: erstens GSM-Lokalisierung selber. Wir haben eine Studie durchgeführt, die im April/Mai 2011 fertig geworden ist, „Schutz mobiler Kommunikation“, in der unter vielen anderen Punkten auch das betrachtet worden ist. Das ist also durch die Fachleute einmal analysiert worden: Wie gut kann man über reine GSM-Signalisierung, die also über die Basisstation und Ähnliches etwa einem Provider zur Verfügung steht, denjenigen lokalisieren, der das Telefon durch die Gegend trägt? Das ist eine ganz klare Sache, die offenbar von der Dichte der Basisstationen in der jeweiligen Region abhängt und damit zu sehr unterschiedlichen Ergebnissen in der Lokalisierung führt.

Legen Sie mich jetzt nicht auf die genauen Zahlen fest. In einsamen Gebieten mögen das einige 10, also 20, 30 Kilometer Ungenauig- - sein, was dann in sehr städtischen, eng bewohnten Gebieten deutlich heruntergeht auf Größenordnungen, die sich irgendwo in 100-Meter-Bereichen bemessen. Ich habe die Studie jetzt selber nie gelesen, sondern beziehe mich auf Informationen. - Das ist die GSM-Ebene.

Natürlich kommen heute in modernen Mobiltelefonen verschiedenste weitere Möglichkeiten dazu, insbesondere wenn das System selber - - Wenn das Telefon ein GPS besitzt, dann kann über diverse Softwarefunktionen, unter anderem auch durch entsprechende Malware, diese Position abgefragt werden und dann nach außen transportiert werden. Das haben wir auch, Herr Hange und ich, in mehreren Gremien immer wieder dargestellt. Da gibt es ein kommerzielles Tool, das etwa solche Ausleitungen vornimmt. Das wird als Malware durch eine dritte Person oder einen Fernangriff auf ein Mobiltelefon installiert und ermöglicht dann Tracking. Dazu gibt es aber mittlerweile Software in Legionen, die solch ein Trecking ermöglicht und damit Personen auch freiwillig völlig nachverfolgbar macht.

Tankred Schipanski (CDU/CSU): Also, das heißt, grundsätzlich sind diese Daten geeignet, zu lokalisieren. - Und jetzt noch mal von Ihrer fachlichen Einschätzung her: Sie haben das jetzt einmal in zwei Ebenen natürlich auch aufgeteilt, diese Studie gewandt. Aber ist das unmittelbar zielgenau möglich, zu orten, um dann auch unter Umständen mit einer dieser beiden Datenströme zu töten?

Zeuge Andreas Könen: Also, die Ortung ist nach heutigem Stand der Technik definitiv, wenn man alle diese Angriffe benutzt, auf wenige Meter möglich, nach dem, was unsere Experten sagen. Allerdings ist es eine sehr diffizile Frage, gerade zu beantworten, zu welchen Daten welche technische Fähigkeit wann wo wer hatte und was zur Verfügung stand.

Tankred Schipanski (CDU/CSU): Wurde das BSI jemals mit dieser fachlichen Bewertung betraut, möchte ich mal sagen? Weil wir haben ja das BfV gehört, die, sagen wir mal, diese Einschätzung, die Sie jetzt vortragen, nicht zwangsläufig so teilen.

Zeuge Andreas Könen: Also, wie gesagt, wir haben uns im Rahmen dieser Studie, die aus vielen Gefährdungsaspekten initiiert war, damit auseinandergesetzt, diese sogenannte „Schutz mobiler Kommunikation“, die es dann - - lag in 2011 vor. Da waren - - Ich weiß nicht genau, wie zu

dem Zeitpunkt das Leistungsspektrum insbesondere der letztgenannten Funktionen war. Dazu müsste ich selber in die Studie hineinschauen.

Tankred Schipanski (CDU/CSU): Okay. Aber diese Studie war bekannt. Aber das BfV oder Ähnliches haben nicht gezielt bei Ihnen angefragt, mal zu sagen: -

Zeuge Andreas Könen: Nein.

Tankred Schipanski (CDU/CSU): - „Wie verhält es sich hier mit den Sachen? Ist das möglich, nicht möglich?“

Zeuge Andreas Könen: Könnte ich jetzt nicht nachvollziehen, ehrlich gesagt.

Tankred Schipanski (CDU/CSU): Das ist Ihnen nicht erinnerlich. Gut. - Dann noch ein weiterer Komplex, der natürlich die Öffentlichkeit sehr berührt hat: das gute Kanzlerinnenhandy. Wir haben ja im Oktober 2013 die Presseberichte; haben Sie alles verfolgt und gesehen. Und nun würde uns da natürlich - - Sie haben im Eingangsstatement ja schon ein bisschen ausgeführt, aber noch mal ein bisschen genauer - - Was hat das BSI denn bezüglich dieses Kanzlerinnenhandys jetzt konkret unternommen, um diesen Vorwürfen nachzugehen?

Zeuge Andreas Könen: Also, wir haben zunächst einmal erst eine Information darüber erhalten am 17. bzw. 18. Oktober. Da ist uns ebendieses Dokument, was vermutlich eine Abschrift von bestimmten Snowden-Informationen darstellt, zugeleitet worden. Wir haben dann zunächst dieses Dokument am 18. einem Plausibilitätscheck unterzogen und festgestellt, dass da durchaus wieder Informationen drauf sind, die als typische Daten einer strategischen Aufklärung gelten können, insbesondere eben mit der Telefonnummer und anderen Indikatoren, die typisch für eine Aufklärung sind.

Dann wurde sehr schnell klar, dass man sich in einer Gesamtschau einmal dieser Bedrohung des konkreten Kanzlerinnenhandys, aber auch dem, was insgesamt aus den Snowden-Dokumenten und früheren Bewertungen unsererseits in der Mobilkommunikation schon bekannt ist - - dass wir uns nochmals genau mit Berlin-Mitte auseinandersetzen müssen. Das habe ich in Teilen ja schon geschildert; das kann man durchaus noch vertiefen.

Der entscheidende Punkt jetzt hier war, dass wir dann angeboten haben, auch entsprechende Prüfungen am Gerät selber vorzunehmen, dass wir mit dem IT-Sicherheitsbeauftragten speziell auch des Kanzleramtes dann gesprochen haben und da auch noch mal entsprechende Leitlinien an die Hand gegeben haben, wie zu verfahren ist und wie Sicherheit möglichst zu gewährleisten ist.

Tankred Schipanski (CDU/CSU): Nun sprechen Sie so elegant in einem deutschen Konjunktiv. Kann ich Ihrer Antwort entnehmen, dass Sie das Handy selbst physisch gar nicht untersucht haben?

Zeuge Andreas Könen: Nein, haben wir nicht.

Tankred Schipanski (CDU/CSU): Also, Sie haben es nicht untersucht.

Zeuge Andreas Könen: Nein.

Tankred Schipanski (CDU/CSU): Wieso ist das unterblieben?

Zeuge Andreas Könen: Das kann ich Ihnen nicht beantworten. Wir haben es angeboten, wie gesagt, haben ja auch in späteren Zusammenhängen solche Untersuchungen angeboten. Aber das Angebot ist nicht angenommen worden.

Tankred Schipanski (CDU/CSU): Okay. - Und dann Ihre Ausführungen, die Sie auch am Anfang taten, jetzt auch mit Blick auf Berlin-Mitte: Sie haben dann eigentlich mehr die Richtung verfolgt: „ Abhören: Was kann da sein? Wie kann das aussehen?“, und Problematik, die Sie vorhin angesprochen haben: Schadsoftware auf einem Gerät. Das konnten Sie gar nicht verifizieren, ob da so etwas vorhanden ist.

Zeuge Andreas Könen: Für den konkreten Fall: Nein. In der abstrakten Würdigung, wie gesagt, erneut Ja.

Tankred Schipanski (CDU/CSU): Okay. - Dann würde mich noch mal interessieren etwas weiter ab, aber schon noch bei dem Thema Kryptohandy. Das haben Sie ja vorhin noch mal ausdrücklich erwähnt, dass das ja an sich eine sichere Sache ist. Und jetzt haben wir in der Presseberichterstattung - das war die *Bild*-Zeitung vom 11.06. diesen Jahres - - hat die *Bild* berichtet über das Handy, Entschuldigung, über die Chinareise der Kanzlerin, und hat darin - -

(Martina Renner (DIE LINKE): Welchen Jahres?)

- Diesen Jahres, ja, 16. Ich komme ja jetzt zu einer Frage. Zu dieser Frage führe ich jetzt ein Stück hin. - Sie haben uns dargestellt, dass dieses Kryptohandy an sich eine sichere Sache ist, und jetzt wird hier behauptet, dass die Chinesen beispielsweise in der Lage sind, auch dieses Kryptohandy, hier steht, „lahmzulegen“. Die sagen nicht, dass man diese Verschlüsselung knackt, aber man kann es lahmlegen. Wie verhält sich das?

(Martina Renner (DIE LINKE): Ist das Untersuchungsgegenstand?)

Ist das möglich, ist das nicht möglich?

(Christian Flisek (SPD): Die Linke macht den Wolff!)

Zeuge Andreas Könen: Also - -

Vorsitzender Dr. Patrick Sensburg: Ich habe es noch nicht ganz mit der Frage - - Wenn Sie noch mal, Kollege Schipanski, noch mal die Frage wieder - -

Tankred Schipanski (CDU/CSU): Also, die Frage ist: Der Zeuge hat vorhin ausgeführt, dass das Kryptohandy eine grundsätzlich sehr sichere Angelegenheit ist. Und jetzt gibt es hier Presseberichte, die sagen: Nein, das ist es nicht. Man kann das lahmlegen wie viele andere Sachen auch. - Und das möchte ich gerne verifiziert haben, ob das so ist oder ob das nicht so ist.

Zeuge Andreas Könen: Also, es ist die Frage, was dieser Artikel, den ich nicht kenne, in der Tat unter „lahmlegen“ versteht. Es ist eine Frage, wie Attacken gegen die Verfügbarkeit wirklich jeglicher Beziehung möglich sind. Da gibt es natürlich grundsätzlich eine ganze riesige Palette. Dass es ganz klar so ist - - Wenn man Ihnen den Zugang alleine zu einer Mobilfunkzelle sperrt, was im Provider absolut einfach ist, dann ist man natürlich ohnehin lahmgelegt.

Man kann auch Kommunikation noch auf verschiedene andere Weise lahmlegen, indem man ganz bestimmte Kanäle ausblendet, indem man dann auch Kommunikation durch Jammer und Ähnliches verhindert, indem man eben die Informationsübertragung vom Mobiltelefon zur Basisstation etwa unmöglich macht. Aber das ist ein sehr weites Spektrum. Wie gesagt, ich kenne diesen Artikel nicht. Ich wüsste jetzt nicht, worauf er sich im Einzelnen bezieht.

Tankred Schipanski (CDU/CSU): Aber letztlich ist es möglich, dass ich auch dieses Kryptohandy - - Das bietet also eigentlich auch keinen hundertprozentigen Schutz.

Zeuge Andreas Könen: Es bietet den entsprechenden Schutz, nur die Kommunikation kommt nicht zustande. Das kann - - Das betrifft aber jedes Gerät, egal ob es krypto ist oder nicht. Für die Kryptofunktionalität, den Schutz der Vertraulichkeit: Da sehe ich keine mir bekannten Informationen, die das infrage stellen würden. Das tut der Artikel in gewisser Weise ja auch nicht. Er drückt es geschickt aus, dass es im Grunde nicht nutzbar sei.

Tankred Schipanski (CDU/CSU): Ja, von daher ging es ja noch mal ein Stück um Ihre fachliche Expertise. - Jetzt noch mal zurück auf das Kanzlerinnenhandy wieder: Sie haben ja erzählt, Ihnen wurden Unterlagen zur Verfügung gestellt bei der Prüfung dieses Kanzlerinnenhandys. Was war das dann da konkret? Wenn Sie das Handy nicht hatten: Was hatten Sie da für Auszüge?

Zeuge Andreas Könen: Was zur Verfügung gestellt wurde, ist genau dieser, wie man es be-

zeichnen mag, Zettel, auf dem bestimmte Grunddaten stehen, die von einem Snowden-Dokument wohl abgeschrieben worden sein sollen. Da steht die Mobilfunknummer drauf, der Name, dann stehen bestimmte sogenannte Target-Kenner drauf. Das deutet darauf hin, dass eben genau diese Daten in einer strategischen Erfassung drin waren. Aber mehr sagt das letztlich nicht aus an der Stelle. Damit ist ein gewisser Anfangsverdacht gegeben einer Überwachung, und das hat eben dann die nachfolgenden Aktionen im BSI inklusive des Angebots einer Analyse des Geräts selber initiiert.

Tankred Schipanski (CDU/CSU): Okay. Und halten Sie es persönlich für plausibel, wie das auf diesem Zettel, auf diesem an- - Das ist ja wohl ein Zettel mit angeblichen NSA-Daten gewesen.

Zeuge Andreas Könen: Ja, also, die Daten sind so plausibel, wie ich das generell für die Dokumente eingeordnet habe. Welche Aktion konkret dann nun da auf nachrichtendienstlicher Seite erfolgt ist, lässt sich natürlich aus dieser reinen Funktionsparameterbeschreibung nicht entnehmen.

Tankred Schipanski (CDU/CSU): Okay. - Dann sind wir erst mal durch.

Vorsitzender Dr. Patrick Sensburg: Okay. Herzlichen Dank. - Dann kommen wir zur nächsten Fraktion, der Fraktion Bündnis 90/Die Grünen. Herr Kollege Ströbele beginnt.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, danke. - Ich fange auch mal hinten wieder an. Haben Sie eine Erklärung dafür, warum das Bundesamt für Verfassungsschutz, zuständig für die Spionageabwehr, hier auch durch einige Herren vertreten als Zeugen, zuletzt durch den Präsidenten, immer noch behauptet, dass man aufgrund der Handydaten eine Person nicht orten kann?

Zeuge Andreas Könen: Also, ich wage jetzt nicht, zu bewerten, was die Zeugen da im Einzelnen ausgesagt haben. Dazu müsste ich den genauen Zusammenhang kennen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, ja.

Zeuge Andreas Könen: Ich hatte ja eben schon angedeutet: Es ist eine diffizile Betrachtung, was zu welchem Zeitpunkt in einer Ortung möglich war.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Nein, heute. Also, bis jetzt, ja.

Zeuge Andreas Könen: Das könnte ich jetzt auch wirklich nicht im Einzelnen nachvollziehen; hatte ich ja auch deutlich gemacht. Insofern kann ich die Aussagen der Kollegen nicht bewerten.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, aber Sie hatten vorhin gesagt, Ihre Erkenntnisse aus diesem Versuch da 2011, die seien auch natürlich allgemein bekannt jetzt in den zuständigen Kreisen.

Zeuge Andreas Könen: Die haben wir dann ab April 2011 zur Verfügung gestellt und kommuniziert.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ja.

Zeuge Andreas Könen: Das ist dann beginnend da der Sachstand einmal der Studie. Von dem Zeitpunkt ab waren natürlich insbesondere auch die Sicherheitsbeauftragten informiert, wie die Gefährdungslage bezüglich Lokalisierungen aussieht.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, wir hatten Herrn Maaßen vor 14 Tagen hier.

Zeuge Andreas Könen: Ja.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Da hat er das immer noch gesagt. - Ja, okay.

Zeuge Andreas Könen: Gut. Lasse es so stehen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): War ja nur ein Versuch. - So ähnlich die

Frage beim Handy der Kanzlerin. Sie haben gesagt, Sie haben sich bereit erklärt, das zu untersuchen, aber von dem Angebot ist kein Gebrauch gemacht worden. - Kann das daran liegen - haben Sie dafür Anhaltspunkte? -, dass man im Kanzleramt aufgrund von anderen Erkenntnissen ohnehin davon ausgegangen ist: „Das stimmt, das ist abgehört worden“?

Zeuge Andreas Könen: Das kann ich Ihnen wirklich nicht sagen. Da müsste ich den Kollegen, der - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ist Ihnen mal gesagt worden, dass - - „Die Sache erübrigt sich, weil wir wissen sowieso, das stimmt - -

Zeuge Andreas Könen: Kann ich Ihnen nicht sagen, ob das der Fall ist oder wie das zustande gekommen ist. Nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Sie haben ja vorhin auch auf die Befragung des Vorsitzenden was zur Plausibilität der Dokumente von Edward Snowden gesagt; gesagt, ja, das sei plausibel, das hätten Sie auf den verschiedenen Wegen überprüft. Kennen Sie eigentlich einen Herrn Heiß und einen Herrn Fritsche im Kanzleramt?

Zeuge Andreas Könen: Ja, sicher, aus den beruflichen Zusammenhängen. Natürlich.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Haben Sie denen eigentlich mal Ihre Erkenntnisse irgendwann mitgeteilt, dass das plausibel ist, dass Ihre Untersuchungen ergeben haben, dass diese Dokumente authentisch sind, jedenfalls dass das - -

Zeuge Andreas Könen: Wir haben das, was sich unserer Meinung nach als Gefährdungslage aus diesem Dokument ergibt, aus der Bewertung ergibt, sehr wohl an vielen Stellen kommuniziert. Wann und zu welchem Zeitpunkt die beiden Personen da in der einen oder anderen Rolle dabei waren, das kann ich jetzt im Moment nicht mehr nachvollziehen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Aber die waren dabei.

Zeuge Andreas Könen: Wir haben das sehr breit und flächendeckend - - Sie waren ja teilweise dann im PKGr auch mit dabei, wenn wir solche Dinge im Nachgang bewertet haben und beschrieben haben. Die Gefährdungslage, die wir daraus ziehen, haben wir sehr breit kommuniziert. Das ist in der Tat richtig.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Gut. - Jetzt komme ich zu dem vierten Punkt. Sie haben das ja geschildert: Bis 2006 waren Sie im Leitungsstab des Bundesnachrichtendienstes und hatten dann auch Kenntnis von „Eikonal“ bzw. „Granat“ und auch von der Nutzung XKeyscore.

Zeuge Andreas Könen: Nein, nein, nein, nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Das hatten Sie nicht?

Zeuge Andreas Könen: XKeyscore ist ein Begriff, der mir erst - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Das haben Sie 2011 dann erst erfahren.

Zeuge Andreas Könen: Ja.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Oho!

Zeuge Andreas Könen: Nein, ich weiß nicht, ob es 2011 war, aber aus den Kontakten, wo wir das erste Mal, wie gerade eben zitiert, in Bad Aibling, wo Mitarbeiter das eben - - eine Darstellung der Fähigkeiten des Gerätes erhalten haben.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, das soll - - Also, Sie sind 2006 dann zum BSI gekommen, und Leiter oder Stellvertreter sollen Sie geworden sein am 1. Januar 2013, glaube ich.

Zeuge Andreas Könen: 13, korrekt.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und danach, März oder so was, sollen diese Besprechungen stattgefunden haben, auch über XKeyscore - kann das sein? -, ob Sie das auch benutzen können oder so.

Zeuge Andreas Könen: Ich meine, die wären etwas früher sogar gewesen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Andreas Könen: Nach meiner Erinnerung, auch jetzt aus dem Aktenstudium, ist mir da eher sogar 2012 im Sinn für ebendieses Treffen und die Bewertungen, die daraus folgen und die klare Aussage: Nein, das ist für das BSI kein geeignetes Instrument.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und nun kommt der Juni 2013 und die ersten Veröffentlichungen, die ja dann jede Woche, jeden Tag manchmal, neue Veröffentlichungen waren aus den Dokumenten von Edward Snowden. Ist Ihnen da nicht die Erinnerung gekommen, plötzlich das Licht aufgegangen? Und dann behauptet plötzlich irgendein fremder Mensch da in Hongkong, dass dieses XKeyscore eingesetzt wurde weltweit, aber insbesondere auch in der Zusammenarbeit mit den Deutschen, wo Sie dann ein Erwachungserlebnis hatten und sagen: Ja, ja, weiß ich ja schon alles, wissen wir ja schon alles. Wir haben ja ausprobiert, und das ist ja tatsächlich was ganz Tolles.

Zeuge Andreas Könen: Also, das sehe ich etwas nüchterner. Natürlich stellt man den Bezug her; das ist völlig klar. Und damit ordnet sich das, was man in so einer kurzen Präsentation im Einzelnen wahrnimmt oder was einem auch sekundär kommuniziert wird, natürlich deutlicher ein. Das ist völlig klar; das ist richtig. Und ich denke, dass man eben doch XKeyscore heute dann umfänglicher und grundlegender bewerten kann.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Also, Sie wussten sofort, als das Wort dann auftaucht - ist ja kein Allerweltswort -: Ja, ja, das ist was.

Zeuge Andreas Könen: Das mit dem Wort war sogar ehrlich noch ein Problem, weil das an einer Stelle sogar mal falsch kommuniziert worden war. Da haben wir dann noch mal geprüft, ob überhaupt dasselbe gemeint war.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Andreas Könen: Es hieß mal in irgendeinem Schriftstück bei uns „XKeystore“, als ob das ein Laden sei. Wie gesagt, also, das war sogar aufgrund des etwas seltsamen Namens erst mal ein Problem.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. Und haben Sie diese Ihre Erkenntnis „Ja, selbstverständlich kennen wir das, das haben wir ja gerade vorgeführt, untersucht, und das wird selbstverständlich eingesetzt beim Bundesnachrichtendienst“ mal weitergegeben, -

Zeuge Andreas Könen: Also, „selbstverständlich eingesetzt - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): - also etwa jetzt auch an die Herren, die ich vorhin genannt habe, oder an den Bundesnachrichtendienst, der wusste es ja eh?

Zeuge Andreas Könen: Ja, es hat ja unmittelbar auch parlamentarische Nachfragen zu dem Thema gegeben.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, genau.

Zeuge Andreas Könen: Und das kann man auch aus den von uns abgegebenen Unterlagen feststellen. Ja, natürlich, das ist kommuniziert worden bis hin zum Untersuchungsausschuss über alle beteiligten Gremien. Und damit war dann natürlich auch deutlich, wie das BSI mit diesen singulären Kontakten da in 2011/12 umgegangen ist.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Also, diese Verantwortlichen im Kanzleramt, beim BND, die wussten -

Zeuge Andreas Könen: Das weiß ich nicht. Da stammen unsere - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): - bei den Veröffentlichungen, was XKeyscore ist. Für die war das jetzt nicht irgendwie ein völliges Fremdwort.

Zeuge Andreas Könen: Das weiß ich nicht. Da die Akten ja vor allen Dingen über das Innenministerium kommuniziert worden sind, ist diese Kommunikation natürlich da gelaufen und umfasst eben genau das, was wir als BSI dazu wahrnehmen und kennen konnten aus - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, nur es liegt nahe, dass Sie das wussten. Warum das trotzdem nicht gleich gesagt wurde: „Ja, wir nutzen das schon lange. Das wissen wir ja, aber das ist gar nicht so böse“ oder so: Wissen Sie nicht, können Sie nicht erklären.

Zeuge Andreas Könen: Das weiß ich nicht genau.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und jetzt komme ich noch mal auf Sie selber als Zeugen. Sie sahen plötzlich diesen Zusammenhang BND-Tätigkeit - -

Vorsitzender Dr. Patrick Sensburg: Ganz kurz. Eine Meldung der Bundesregierung. Herr Wolff. Vielleicht hilft das.

RD Philipp Wolff (BK): Ich will nur ganz kurz - - Herr Ströbele, Sie machen einen Vorhalt. Da hört sich das so an, als sei das bestritten worden. Das ist mitnichten der Fall. Da hat der Zeuge ja auch darauf hingewiesen, dass das in den parlamentarischen Anfragen, was XKeyscore betrifft, natürlich entsprechend thematisiert wurde.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, der Frage gehen wir noch an anderer Stelle nach. Ich wollte ja nur von dem Zeugen hören, was er davon weiß. - Jetzt komme ich also zu Ihnen persönlich noch mal. Sie haben jetzt plötzlich gehört: In der Zeit, als Sie auch eine leitende Stellung im BND gehabt haben, sollen sich Sachen abgespielt haben, bis 2006, was bekannt wurde durch die Snowden-Papiere, was problematisch mindestens sein konnte. Und nun waren Sie auch noch einer von denen, die das alles klären sollten und aufklären sollten, ob das denn stimmt, ob die Dokumente authentisch sind und, und, und. Haben Sie da nicht mal irgendwann gesagt: „Ich bin der Falsche“? Also, Sie kennen das, Bock und Gärtner und so, dass Sie jetzt, einer, der da mit beteiligt war, nun plötzlich prüfen sollten, ob das alles in Ordnung war.

Zeuge Andreas Könen: Also, das unterstellt ja erst mal, dass man sich überhaupt in der Rolle des Bocks da wiederfinden will. Das streite ich also hier massiv ab. Es geht darum, wirklich fachliches Wissen und wirklich unabhängige und präzise Beurteilungsfähigkeit da mit hineinzubringen. Und die wächst genauso, wenn man in einem Bundesnachrichtendienst tätig ist, wenn man da Tätigkeiten und auch verantwortende Tätigkeiten wahrnimmt. Und ich halte es für wesentlich, dass man dieses Wissen, was man für die Sicherheit von Infrastrukturen gewinnt, dann auch wirklich gewinnbringend da einsetzt, aber mit klaren Maßstäben und mit klaren Verantwortlichkeiten, wo man es dann später braucht.

Das hat damit zu tun, dass man da eine Gesamtbeurteilung vornimmt. Und gerade das ist sogar der Nutzen: dass man eben beide Seiten der Medaille sehen kann. Ich finde, das ist vielleicht eher das, was uns insgesamt fehlt: dass wir da genauer hinschauen sollten, um die Fähigkeiten, die wir da haben, so etwas aus mehreren Richtungen beleuchten zu können und ein Gesamtbild Sicherheit herzustellen. Das ist entscheidend. So habe ich mir nicht die Frage gestellt, ob ich mich davon irgendwo zurückziehen sollte, sondern eher die Frage gestellt: Was kann ich persönlich dazu in einer präzisen Beurteilung beitragen, gerade um Sicherheit zu fördern?

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, aber Sie - - Also, es ging ja nicht um irgendeine Expertise, sondern es ging um schwere Vorwürfe - so wurde das jedenfalls allgemein in der Öffentlichkeit aufgefasst, auch von mir - gegenüber dem Bundesnachrichtendienst, dass er in Zusammenarbeit mit der NSA Grundrechte verletzt. Ich sage das jetzt mal ganz allgemein.

Und in dieser Zeit waren Sie auch in Kenntnis der Praktiken in leitender Stellung im Bundesnachrichtendienst. Und nun sind ausgerechnet Sie der Experte, der das untersuchen soll, ob das stattgefunden hat und ob da was Vorwerfbares ist oder so was.

Vorsitzender Dr. Patrick Sensburg: Das wäre dann die letzte Frage in dieser Runde. Aber Herr Könen, Sie können gerne antworten.

Zeuge Andreas Könen: Also, wie gesagt, wenn ich etwas beitragen könnte zu den Einzelvorwürfen, die Sie da genannt haben, und wenn ich ein Zeuge für diese Vorgänge wäre, dann würde ich das hier ganz klar tun. Aber da bringen Sie zwei Dinge immer zusammen: die Auskünfte, die ich vielleicht konkret zu Vorgängen im BND geben könnte - das habe ich eben beantwortet jeweils - und die generischen Fragestellungen einer Bewertung meinerseits, in der Erfahrung, die ich habe, was das Gesamtgefährdungsszenario aus den Snowden-Dokumenten angeht. Da trage ich meinen Teil zu bei; zu dem anderen habe ich gesagt, wie viel ich sagen kann oder nicht sagen kann an der Stelle. Das muss man schon auseinanderhalten.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Dann kommen wir jetzt zur Fraktion der SPD. Herr Kollege Flisek.

Christian Flisek (SPD): Ja, vielen Dank. - Ich würde ganz gerne, Herr Könen, Ihnen einen Vorhalt aus einer E-Mail von Herrn Opfer machen vom 22. Januar 2015. Wenn Sie wollen, kann ich Ihnen das auch vorlegen lassen, damit Sie das mitverfolgen.

Zeuge Andreas Könen: Je nachdem, wie lang es ist.

Christian Flisek (SPD): Na ja. Also, ich lese Ihnen jetzt mal den Abschnitt gerade vor. Das ist MAT A BSI-2n, Blatt 33 bis 34, ist genau am Umbruch. Da heißt es unter anderem:

> Das Risiko hochqualifizierter nachrichtendienstlicher Angriffe ist auf dem Schutzniveau NfD bislang akzeptiert worden.
>
> Um derartige Risiken … abzuwehren, müssten grundsätzlich alle IT-Produkte, also nicht nur die Produkte mit IT-Sicherheitsfunktionen nach VSA, aus vertrauenswürdiger nationaler Produktion kommen und einem Zulassungsprozess auf dem Niveau VS-Vertraulich unterzogen werden. Dies erscheint unter heutigen Voraussetzungen nicht realistisch umsetzbar.

Meine erste Frage wäre jetzt mal: VSA, was ist das?

Zeuge Andreas Könen: Das ist die Verschlusssachenanweisung.

(Zuruf)

Christian Flisek (SPD): Ja. Ich will es von ihm hören, nicht vom Sekretariat. - Können Sie das ausführen?

Zeuge Andreas Könen: Was die Verschlusssachenanweisung ist?

Christian Flisek (SPD): Ja, genau.

Zeuge Andreas Könen: Also, die Verschlusssachenanweisung ist, basierend auf dem Sicherheitsüberprüfungsgesetz, in dem grundsätzlich definiert wird, was Verschlusssachen sind, die Ausführungsbestimmungen des Bundesinnenministeriums über die Handhabung eben genau dieser eingestuften Verschlusssachen. Das erstreckt sich für das BSI insbesondere auf die Pflichten, die da im materiellen Geheimschutz oder IT-Geheimschutz wahrzunehmen sind. Was Herr Opfer beschreibt, ist die Präzisierung der technischen Maßnahmen, die für ein bestimmtes Schutzniveau vorzunehmen sind. Das Zitierte waren die beiden Schutzebenen, der unterste Schutzgrad Verschlusssache-Nur für den Dienstgebrauch, VS-NfD, und das andere war der Verschlusssachengrad VS-V, Verschlusssache-Vertraulich.

Dazu gibt es unter der Voraussetzung, dass der jeweilige Nutzer seine Verschlusssachen sauber klassifiziert nach der Maßgabe des SÜG und der Verschlusssachenanweisung, dann korrespondierende technische Anforderungen, wie das in einer IT- und Kommunikationsumgebung zu gewährleisten ist. Das läuft jeweils darauf hinaus, dass dann entsprechend zugelassenes Gerät zu verwenden ist. Das heißt also, wenn Sie eine Verschlusssache-Nur für den Dienstgebrauch irgendwo dann verschlüsselt etwa speichern wollen auf einem Rechner, dann muss diese Verschlüsselung für den Gebrauch bei VS-NfD zugelassen sein.

Christian Flisek (SPD): Okay.

Zeuge Andreas Könen: So. Der entscheidende Knackpunkt, den Herr Opfer da beschreibt, ist dann der, dass zwischen der Verschlusssache-Nur für den Dienstgebrauch, die eine sehr breit angelegte Verschlusssache ist, die für sehr, sehr viele Dokumente, Sprachinformationen und andere Informationen genutzt wird, und der VS-V-Einstufung eine deutliche Sprunghöhe besteht. Wir haben eine klare Differenzierung, dass wir ab VS-V aufwärts, auch für Geheim und erst recht für Streng Geheim, eben nationale Kryptografien mit nationalen Produkten einsetzen und ein entsprechendes Zulassungsregime in der Abteilung Kryptotechnologie des BSI durchlaufen.

Für die Verschlusssachen-Nur für den Dienstgebrauch wird aber gängiges Gerät und gängige Tools, Software und anderes benutzt, die aus Standardproduktionen von Unternehmen stammen. Zum Beispiel, um ein Mobiltelefon zu erzeugen, müssen Sie eine Plattform hernehmen, die aus nichtdeutscher Produktion ist, wie eben schon geschildert, und dann wird durch geeignete kryptografische Maßnahmen, durch Maßnahmen im Betriebssystem, das Risiko, was auf diese Plattform wirkt, so lange abgesenkt, bis eben ein Gesamtrisiko entsteht, das unter dem Blick auf Verschlusssache-Nur für den Dienstgebrauch tragbar ist. Herr Opfer hätte nun am liebsten, dass auch für diese Ebene genau Technik deutscher Provenienz eingesetzt wird.

Christian Flisek (SPD): Ja.

Zeuge Andreas Könen: Das ist aber aufgrund der Marktgegebenheiten so nicht erreichbar.

Christian Flisek (SPD): Okay. Ich habe das auch so gelesen. Nur eine Frage jetzt mal: Kryptohandys: Gibt es welche aus deutscher Produktion?

Zeuge Andreas Könen: Nein, nicht wenn Sie die Plattform nehmen. Das ist immer ein Gerät ausländischer Provenienz, das entsprechend gehärtet wird.

Christian Flisek (SPD): Also, man kann es nie umsetzen, egal für welche - -

Zeuge Andreas Könen: Das kann man in Mobiltelefonie so nicht umsetzen. Wir wählen einen anderen Weg. Wir schleifen, wie man das fachtechnisch nennt, die Sprache aus dem Gerät heraus, wir übertragen sie auf einer gesicherten Schnittstelle in ein separates Modul, das dann aus deutscher Provenienz stammt, und da wird eine Verschlusssache-Vertraulich-Verschlüsselung eingerichtet. Und dann geht der verschlüsselte Datenstrom über das Gerät letztlich nach außen. Damit ist gewährleistet, dass bis zu dieser Verschlüsselung eben höherwertige Sicherheit entsteht. Aber letztlich ist es dann - -

Christian Flisek (SPD): Und das ist auch mobil nutzbar?

Zeuge Andreas Könen: Das ist mobil nutzbar. Das ist ein Gerät eines bestimmten deutschen Unternehmens, das wir hier auch in der Beratung der letzten zwei Jahre - -

Christian Flisek (SPD): Und das wird auch genutzt?

Zeuge Andreas Könen: Das wird konkret genutzt durch eine Gruppe von Nutzern in einer behördlichen Einrichtung. Die sind Probenutzer. Das ist aber an der Front der Technik.

Christian Flisek (SPD): Ja, also wir - weil der Kollege von Notz natürlich gerade hinweist darauf, dass wir als Obleute natürlich auch Kryptohandys haben - - Den Deutschen Bundestag betrifft das ja nicht, nicht? Da sind Sie - -

Zeuge Andreas Könen: Wir bieten Ihnen das ganz genauso an, ja, natürlich.

Christian Flisek (SPD): Ja, ja, das Angebot wird, glaube ich, vom Deutschen Bundestag bisher abgelehnt.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber von uns nicht!)

- Ja, ja, ein Blackberry, genau. - Also, was ich damit sagen will jetzt mal - -

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Ich möchte mal die Debatte, also die Frage gerade mal aufmachen: Ich meine, aus dieser E-Mail jetzt grundsätzlich mal dokumentiert ist ja doch ein erhebliches Misstrauen gegenüber Herstellern, ich sage das jetzt mal so, ausländischer Provenienz.

Zeuge Andreas Könen: Ja, erst mal gegenüber den Fähigkeiten der Nachrichtendienste, solche Plattformen auszuhebeln.

Christian Flisek (SPD): Ja, genau. Und sozusagen dieses Risiko verschärft sich dann sozusagen aus Sicht jetzt zumindest mal von Herrn Opfer dadurch, dass eben dann auch noch Hardware, Software, wie auch immer, Technik ausländischer Provenienz eingesetzt wird. Und wir kommen aber jetzt zu dem Ergebnis, dass das schlicht - er sagt es ja selber - eben unter den heutigen Voraussetzungen nicht realistisch umsetzbar ist. Wie gehen wir denn damit um?

Zeuge Andreas Könen: Wir gehen damit so um, dass wir da, wo uns entsprechende Technologie aus deutscher oder europäischer Produktion nicht zur Verfügung steht, die entsprechenden zusätzlichen Schutzmaßnahmen hochschrauben - etwas, was für die Nutzer immer unangenehm ist -, dass wir zum Beispiel fordern, dass ein entsprechender Hardwaresicherheitsanker, eine SD-Karte auf gut Deutsch - die schieben Sie dann in das Kryptotelefon hinein - - dass die aus deutscher Produktion von deutschen Unternehmen stammt und dass sich der Lieferant etwa des Mobiltelefons darauf einlassen muss, solche Schnittstellen zur Verfügung zu stellen. Das heißt, wir wirken mehr und mehr auf die Hersteller von Standard-IT-Produkten ein, entsprechende Schnittstellen für nationale oder europäische Sicherheitsmechanismen zu bieten.

Christian Flisek (SPD): Und wie reagieren die darauf?

Zeuge Andreas Könen: Die Bereitschaft, das zu implementieren, hat sich deutlich erhöht während der letzten zwei, drei Jahre.

Christian Flisek (SPD): Das heißt, es sind aber nicht alle gleich Gewehr bei Fuß.

Zeuge Andreas Könen: Nein, es sind nicht alle gleich in der - - Das ist eben ein anstrengendes Geschäft, da auch entsprechend einzuwirken und auch bei den Unternehmen deutlich zu machen, dass Sicherheit etwas ist, womit man eben auch Geld verdienen kann durchaus und was dann eher auch zum Nutzen eines Herstellers sein kann, wenn er das anbieten kann.

Christian Flisek (SPD): Und ich habe Sie richtig verstanden, dass es da, was die Vertrauenswürdigkeit gibt, auch ein abgestuftes System gibt.

Zeuge Andreas Könen: Richtig, ja.

Christian Flisek (SPD): Also, Sie sagen: Da gibt es zwischen, ich sage mal, USA und Deutschland noch mal auch Europäer, die sind noch mal besonders vertrauenswürdiger oder - -

Zeuge Andreas Könen: Ja, wir bewegen uns ja mit dem gemeinsamen Markt in einem besonderen Rechtsraum, -

Christian Flisek (SPD): Ja.

Zeuge Andreas Könen: - sodass ich also auch, gerade was vertragliche Beziehungen zu europäischen Unternehmen angeht und eben auch Vereinbarungen zu Sicherheit in der Informationstechnik und zu Cybersicherheit, deutlich besser

durchkomme und auch mehr Möglichkeiten besitze, bei Verstößen da zu ahnden und dem nachzugehen. Das ist einfach durch die enge Verflechtung der Europäischen Union gegeben.

Christian Flisek (SPD): Also, es würde theoretisch auch für britische Firmen gelten, also zumindest noch bis zum heutigen Tag.

Zeuge Andreas Könen: Es würde theoretisch auch für britische Firmen gelten.

Christian Flisek (SPD): Okay, interessant.

Zeuge Andreas Könen: Bis heute Abend mindestens.

Christian Flisek (SPD): Ja, genau. - Es gibt ein anderes Schreiben von der thüringischen Datenschutzbeauftragten, des thüringischen Datenschutzbeauftragten, in dem wird für die Unterstützung in Sachen CALEA gedankt. Kennen Sie CALEA?

Zeuge Andreas Könen: Also, das ist mir jetzt im - - Ich weiß, dass der Begriff mal vorgekommen ist. Ich kann jetzt nichts damit verbinden.

Christian Flisek (SPD): Das steht für Communications Assistance for Law Enforcement Act.

Zeuge Andreas Könen: Gehört habe ich das schon.

Christian Flisek (SPD): Ich lese Ihnen einfach mal - -

Zeuge Andreas Könen: Wenn Sie mir - - Wenn das ein BSI-relevantes Dokument ist, dann würde - -

Christian Flisek (SPD): Na, ja, das ist ein - - Also, ich habe das gefunden in MAT A BSI-1-6m.pdf, Blatt 121 bis 122. Also, CALEA ist nach meinen Informationen ein amerikanischer Rechtsakt, -

Zeuge Andreas Könen: Ja, aber - -

Christian Flisek (SPD): - der US-Softwarehersteller zum Einbau von Backdoors verpflichtet für amerikanische Dienste. Und der Datenschutzbeauftragte in Thüringen äußert hier die Sorge, dass davon auch eben zum Beispiel US-Verschlüsselungssoftware betroffen sein könnte, die in Deutschland im behördlichen Verkehr eingesetzt wird. - Mein Kollege legt Ihnen das gerade vor.

(Dem Zeugen werden Unterlagen vorgelegt)

Zeuge Andreas Könen: Ja, okay.

Christian Flisek (SPD): Also, Ihnen ist CALEA nicht nur mal untergekommen, ist Ihnen jetzt bekannt?

Zeuge Andreas Könen: Also, diese Anfrage ist jetzt - - nach Zur-Kenntnisnahme erinnere ich mich an die, und wir haben ja hier in dem Antwortschreiben eben zunächst einmal die vom thüringischen Datenschutzbeauftragen vermutete Rolle von CALEA etwas zurechtgerückt und präzisiert. Er spricht ja davon, dass auf Basis von CALEA eben entsprechende Backdoors eingebaut würden. Nach der Aussage unserer Hausjuristen, die mich hier in der Abfassung des Schreibens unterstützt haben, ist es eben nicht so, sondern es ist eine Gesetzgebung, die die entsprechenden Provider dazu anhält, entsprechende Law-Enforcement-Schnittstellen vorrätig zu halten und damit den Zugang für US-amerikanische Behörden bzw. Geheimdienste zu ermöglichen.

Christian Flisek (SPD): Nur Provider?

Zeuge Andreas Könen: Nach dem, was mir damals hier zugearbeitet wurde, ja. Aber wir sind keine durchgehenden Experten für amerikanisches Recht.

Christian Flisek (SPD): Nein, aber Sie sind Experten für die Integrität der deutschen IT-Sicherheitsstruktur.

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Und wenn wir auf deutschen Behördenrechnern massenhaft, sage ich

mal, Windows, Apple OS X, sonst irgendwas installiert haben und darüber kommuniziert wird, auch wenn es nicht eingestuft ist, -

Zeuge Andreas Könen: Ja. Dann dreht es sich ja - -

Christian Flisek (SPD): - dann stellt sich natürlich die Frage schon, wenn es einen Rechtsakt in den USA gibt, der eventuell verpflichtend ist, in der Reichweite hier irgendwelche Backdoors einzubauen - -

Zeuge Andreas Könen: In Verschlüsselungssoftware.

Christian Flisek (SPD): Ja, nicht nur, auch in ganz normaler Software.

Zeuge Andreas Könen: Nein, so steht es ja hier in dem Schreiben auch. Also, hiervon erfasst wäre dann auch Verschlüsselungssoftware amerikanischer Hersteller. Das ist der Grund, warum wir keine Verschlüsselungssoftware fremder Länder für die Verschlüsselung auf Basis VS-NfD nutzen, sondern da nationale Produkte einfordern, weil bei Software ist das kaum nachzuvollziehen.

Christian Flisek (SPD): Aber lassen Sie mich jetzt noch mal eins sicherstellen.

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Also, wenn Sie sagen, wir führen und fordern: Das sind alles Empfehlungen, nicht?

Zeuge Andreas Könen: Nein, mit denen zusammen wird ja gerade bei Verschlüsselung eben im Zusammenhang mit Verschlusssachen-Nur für den Dienstgebrauch auch ein Produkt zugelassen oder mehrere Produkte zugelassen, und die stehen auf den Listen des BSI, die wir den Nutzern zur Verfügung stellen. Und die kann jeder nicht nur aus dem Bund, sondern auch aus den Ländern entsprechend kaufen und installieren.

Christian Flisek (SPD): Und ob er das macht, ist aber seine Entscheidung.

Zeuge Andreas Könen: Bitte?

Christian Flisek (SPD): Ob er das macht, ist seine Entscheidung.

Zeuge Andreas Könen: Ob er das macht, ist seine Entscheidung. Das ist letztlich die Entscheidung auch jedes einzelnen Behördenleiters.

Christian Flisek (SPD): So. Und wie ist denn da die Durchdring- - Also, darum spreche ich - - sage ich: Das, was Sie machen, sind Empfehlungen, -

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): - Angebote.

Zeuge Andreas Könen: Im Bund ist die Durchdringung sehr hoch, weil wir da über entsprechende Rahmenverträge dann diese Produkte bereitstellen und eine absolut hohe Abrufquote vorhanden ist und die Behörden ja dann in dem Moment, wenn es um Verschlusssachen - Nur für den Dienstgebrauch geht, die wirklich auf diesen Rechnern bewegt werden, auch verpflichtet sind - da im Rahmen der VSA sind sie verpflichtet -, dann diese Software einzusetzen.

Christian Flisek (SPD): Das heißt, Herr Könen - korrigieren Sie mich jetzt, wenn ich Ihnen da jetzt was Falsches in den Mund lege -, also, Sie würden sagen: Eine Nutzung, ich sage mal, von US-amerikanischen Hard- und Softwareprodukten, die nicht im Zweifel eine Prüfung durch das BSI durchlaufen haben oder abgewandelt worden sind, ist ein hohes Sicherheitsrisiko in Deutschland.

Zeuge Andreas Könen: Also, in der Pauschalität kann man das natürlich nicht in den Raum stellen. Sie müssen das natürlich gegen die Fragestellung halten: Was müssen Sie schützen? In dem Moment, wenn ich Verschlusssachen schützen muss, deren Verschlusssachengrad höher ist als VS-V, muss ich ganz besondere Maßnahmen anwenden, und dann muss ich in dem Moment, wenn ich Betriebssysteme zum Beispiel ausländischer Provenienz einsetze, über andere Maßnah-

men dafür sorgen, dass etwa eine totale Abschottung des jeweiligen Bereiches existiert und keine Kommunikation. Dann geht es runter, dann muss ich weiter. In dem Moment, wenn ich es für VS-NfD tue, bin ich ja gezwungen - -

Christian Flisek (SPD): Das habe ich alles verstanden, das hatten Sie ja gerade auch schon ausgeführt.

Zeuge Andreas Könen: Ach so. Das heißt, man kann es nur immer in relativer Weise zu dem sehen, was ich gerade mit einer Hard- oder Softwaretechnologie erreichen will. Man muss sich der Gefährdung bewusst sein für seine eigenen Daten. Aber in dem Zusammenhang muss man dann auch die Nutzung dieser jeweiligen Produkte sehen.

Christian Flisek (SPD): Ja, aber diese Relativierung -

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): - der von mir pauschalen Aussage, die Sie jetzt versucht haben, verstehe ich nicht. Entweder die marktgängigen Produkte sind vertrauenswürdig, ja, und ich habe ja auch ein bestimmtes Anspruchsprofil, insbesondere bei der öffentlichen Beschaffung, und das Unternehmen liefert das dann, und es ist vertrauenswürdig, oder es ist nicht vertrauenswürdig. Und wir unterhalten uns ja hier im Ausschuss auch nicht nur über die Kommunikation von Behörden. Wir haben ja den Gesamtblick. Wir haben auch die Bürgerinnen und Bürger im Blick. Wir haben die Unternehmen im Blick. So, und die Frage, die im Raum steht - aus Ihrer Expertise, angesichts dessen, was jetzt hier auch wir vorfinden in Schriftverkehren Ihres Amtes, unter einzelnen Mitarbeitern - - Ich gewinne den Schluss daraus, dass das BSI der Auffassung ist: Marktgängige Produkte der Amerikaner sind für eine sichere, geschützte Kommunikation nicht vertrauenswürdig.

Zeuge Andreas Könen: Also, wie gesagt, diese pauschale Aussage führt nicht wirklich zu einer praktikablen Handhabung der Anfordernisse für alleine den Schutz in den Behörden. Sie können das nur gegeneinanderhalten, wenn Sie Aufwand, Gefährdung und Nutzen gegeneinanderhalten. Wenn es so einfach wäre, dass wir rein die Vertrauenswürdigkeit per se, so wie sie gegeben ist, als alleinigen Maßstab geben, dann müsste man alleine wegen der vielen Angreifbarkeiten, die sich etwa bei der Soft- und Hardware und Betriebssystemen ergeben, praktisch per se darauf verzichten, IT zu nutzen. Vor dieser Entscheidung steht keiner unserer Behördenpartner, sondern man muss es differenzieren.

Christian Flisek (SPD): Entschuldigung, aber - - Nein, nein. Also, ich - -

Zeuge Andreas Könen: Die Vertrauenswürdigkeit für den Einsatz etwa von Verschlüsselung von Betriebssystemprodukten kann natürlich nur gewährleistet werden, wenn in einer Beschaffung, zum Beispiel des Bundes, entsprechende Anforderungen an den Hersteller gerichtet werden. Das tut der Bund. Der Bund richtet genau an die Unternehmen, von denen er so etwas kauft, klare Anforderungen. Ein Stichwort war ja der No-Spy-Erlass, mit dem das noch mal ganz deutlich wurde, dass in solchen Beschaffungen klare Anforderungen an den Hersteller ergehen, dass er etwa deutlich erklärt, dass seine Produkte nicht Daten ausleiten an irgendwelche Dritte - da geht es ja dann nicht nur um Nachrichtendienste, sondern da geht es um die grundsätzliche Frage: „Wohin werden Informationen ausgeleitet?“ - und dass dann definitiv auch entsprechend die - -

Christian Flisek (SPD): Ja, nur jetzt - - Noch mal, Herr Könen, dass er das erklärt - -

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Ja, was soll er denn tun? Ich meine, alle ziehen hier durchs Land und sagen, natürlich halten sie sich an die Marktregeln, in denen sie Geschäfte machen. Was sollen sie denn auch anderes sagen? Aber es ist auch kein Geheimnis, dass es eine Sicherheitsgesetzgebung in den USA gibt, die ihnen genau verbietet, den Unternehmen, genau über das, was sie dort tun müssen in Kooperation mit den eigenen Diens-

ten, auch nur ein Sterbenswort irgendwo zu verlieren. So. Und das ist doch reichlich naiv, diese Ansicht, jetzt zu sagen, einerseits: „Wir haben hier dokumentiert, angeblich gibt es vertrauenswürdige nationale Produktion, und ausländischer Provenienz, das ist eben nicht vertrauenswürdig“, und zu sagen jetzt: „Das kommt immer nur auf die Frage an, welchen Verkehr ich da irgendwie schützen will.“ Entweder ich vertraue diesen Unternehmen, wenn ich ihnen ein Anforderungsprofil gebe, oder nicht. Und das Einzige, was Sie sozusagen dann ja bekommen, ist eine Zusage: Ja, wir sind vertrauenswürdig, wir leiten es nicht aus.

Vorsitzender Dr. Patrick Sensburg: Das wäre dann die letzte Frage.

Zeuge Andreas Könen: Also, wenn es alleine eine Zusage des guten Willens wäre, wäre es zu wenig, aber es ist ja mehr. Es ist eine rechtlich bindende Zusage des Unternehmens.

Christian Flisek (SPD): Ja, ein Rechtsbindungswille ist eine Willenserklärung nach BGB. Könnte zu einer Produkthaftung führen. Ja, toll.

Zeuge Andreas Könen: Sie kann auch strafbewährt sein in dem Moment, wenn eine klare Mitwirkung des Unternehmens erkennbar würde.

Christian Flisek (SPD): Na, wir werden noch mal das vertiefen. Danke erst mal.

Vorsitzender Dr. Patrick Sensburg: Okay. Herzlichen Dank. - Dann kommen wir jetzt zur dritten Fragerunde. Bei der dritten Fragerunde beginnt wieder die Fraktion Die Linke. Frau Kollegin Renner.

Martina Renner (DIE LINKE): Herr Könen, ich habe noch zwei Fragen tatsächlich noch mal zu Ihrer Verwendung im BND. Als Leiter Leitungsstab waren Sie 90AD, habe ich geklärt. Davor waren Sie - -

Zeuge Andreas Könen: Entschuldigung, wenn ich - - Nicht Leiter Leitungsstab. Es ist die Leitung des Sachgebietes 90AD.

Martina Renner (DIE LINKE): Ja, ja. AD, im Leitungsstab. AD dann immer abgekürzt hier, nicht?

Zeuge Andreas Könen: 90A ist der Leitungsstab, 90AD ist das Sachgebiet.

Martina Renner (DIE LINKE): Genau. Alles klar, gefunden auf dem Stempel. - Und davor waren Sie Sachgebietsleiter im Leitungsstab.

Zeuge Andreas Könen: Nein, das ist ja genau die Tätigkeit. Der 90AD - -

Martina Renner (DIE LINKE): Okay. Und davor waren Sie Referent im Leitungsstab.

Zeuge Andreas Könen: Nein, nein.

Martina Renner (DIE LINKE): Auch nicht.

Zeuge Andreas Könen: Ich bin als Leiter des Sachgebietes 90AD im März 2005 in den Leitungsstab des Bundesamtes gekommen.

Martina Renner (DIE LINKE): Und davor hatten Sie mit dem Leitungsstab überhaupt nichts zu tun.

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): Auch nicht mit der Abteilung 2.

Zeuge Andreas Könen: Ich war Mitarbeiter in der Abteilung 2, ja.

Martina Renner (DIE LINKE): Und da im Referat?

Zeuge Andreas Könen: Das war nach damaliger Zählung Unterabteilung 21, heute T3.

Martina Renner (DIE LINKE): Okay. Weil, wie gesagt, wir hatten keine Gelegenheit, Sie in den Akten - -

Zeuge Andreas Könen: Ja.

Martina Renner (DIE LINKE): Und wir haben eine Übersicht mit Referent Leitungsstab, Sachgebietsleiter Leitungsstab, aber das ist alles - -

Zeuge Andreas Könen: Wie gesagt, um das noch mal für Sie deutlich zu machen, also -

Martina Renner (DIE LINKE): Ja, ja, jetzt habe ich - -

Zeuge Andreas Könen: - die Zentralstelle für das Chiffrierwesen wird im Jahr 1991 mit dem BSI-Errichtungsgesetz dann geteilt, mitarbeitermäßig. Ein Teil des Personals geht in das Bundesamt für Sicherheit in der Informationstechnik über, der andere verbleibt als Unterabteilung mit mehreren Nummernänderungen 21 im Bereich.

Martina Renner (DIE LINKE): Okay. Aber wie gesagt, in Bezug auf den Leitungsstab hatten Sie immer nur ein Kürzel: 90AD.

Zeuge Andreas Könen: Ja, korrekt.

Martina Renner (DIE LINKE): Gut, das ist damit auch schon vollständig geklärt. - Und unter diesem Kürzel finde ich Sie ab - -

Zeuge Andreas Könen: Ab circa 15. März 2005.

Martina Renner (DIE LINKE): Gut. - Sie hatten vorhin davon gesprochen, dass die Provider angeschrieben wurden mit einer Fragestellung „Zusammenarbeit mit ausländischen Diensten“ und dass die da alle geantwortet hätten.

Zeuge Andreas Könen: Ja, also, es ging ja im ersten Durchlauf um die Provider, die für den Bund und die Bundesbehörden entsprechende Leistungen zur Verfügung stellen. Das waren die Unternehmen Deutsche Telekom AG, Verizon und DE-CIX.

Martina Renner (DIE LINKE): Und die haben alle, was die Frage „Zusammenarbeit mit ausländischen Diensten“ angeht, ausführlich geantwortet.

Zeuge Andreas Könen: Die haben alle auf diese Fragen geantwortet.

Martina Renner (DIE LINKE): Gut, dann möchte ich Ihnen eine Akte vorhalten. Und das ist MAT A BMI-10, Tagebuchnummer 17/14, Seite 11 f. Also, 11 beginnt das Schriftstück, und 12 wäre dann ein Zettel und eine Anmarkung hier in dem Text. Und dass Sie sich das mal kurz durchlesen und dann mir sagen, ob dann Ihre Aussage von eben so zutreffend ist. Da die eingestuft ist, konnte ich Ihnen das jetzt nicht vorhalten.

(Dem Zeugen werden Unterlagen vorgelegt - Er sowie Vertreter der Bundesregierung nehmen Einblick)

Zeuge Andreas Könen: Also, wo hier genau der orange - - Ja, das ist deswegen zu halten, weil im Nachgang weitere entsprechend eingestufte Informationen gegeben worden sind. Wenn Sie den Gesamtvorgang anschauen, wird das eine komplette Aussage.

Martina Renner (DIE LINKE): Also, dieses Unternehmen sagt dann irgendwas zur Zusammenarbeit mit ausländischen Diensten später aus.

Zeuge Andreas Könen: Es verneint die entsprechend.

Martina Renner (DIE LINKE): Es verneint die?

Zeuge Andreas Könen: Ja, im Sinne - - auf den IVBB bezogen, so wie es hier in der Fragestellung auch vorhanden ist.

Martina Renner (DIE LINKE): Okay, dann müssen wir das noch mal im Aktenverlauf gucken, ob sich das so ergibt. Wir haben nur diese Stelle gefunden. - Ich habe noch eine Frage zu der Break-Problematik aus dem IVBB. Sie sagten vorhin, da ist geklärt worden, dass es an den Übergabepunkten auch keine gibt zu ausländischen Dienstanbietern. Gilt das auch für deutsche Konzerne, die hier als Tochterunternehmen ausländischer Dienstanbieter unterwegs sind? Also, wenn Sie MCI WorldCom Deutschland nennen, meinen Sie, das ist ein deutscher Anbieter, oder ist das für Sie ein US-amerikanischer Anbieter?

Zeuge Andreas Könen: Das ist dann für mich das deutsche Tochterunternehmen, nach deutschem

Recht, eines US-amerikanischen Anbieters, wobei die Verträge eben immer mit dem deutschen Tochterunternehmen geschlossen werden. Und wenn Sie - -

Martina Renner (DIE LINKE): Genau. Und wie sieht es denn in diesem Break - -

Zeuge Andreas Könen: Breakout meint dann ja Folgendes: dass etwa in einer Verkehrssituation, wo eine Übermittlung innerhalb Deutschlands nicht mehr möglich ist, im Netz des jeweiligen Anbieters dann ein Breakout stattfindet in einen anderen Rechtsraum.

Martina Renner (DIE LINKE): Und finden diese Breakouts zu MCI WorldCom Deutschland statt?

Zeuge Andreas Könen: Also, ob solche Breakouts stattgefunden haben tatsächlich im Verlauf des Betriebes, kann ich Ihnen jetzt nicht sagen, da mir dazu keine Informationen vorliegen. Nur, diese Breakouts sind immer in Betracht gezogen worden durch die eben von mir genannte Tunnelverschlüsselung, die dann dazu führt, dass die Informationen, die dann in einem Breakout über fremde Netze fließen, allesamt verschlüsselt sind.

Martina Renner (DIE LINKE): Und wenn ich den Schlüssel habe?

Zeuge Andreas Könen: Wenn man den Schlüssel hat, könnte man es lesen. Der Schlüssel besitzt - -

Martina Renner (DIE LINKE): Wer generiert den Schlüssel eigentlich?

Zeuge Andreas Könen: Bitte?

Martina Renner (DIE LINKE): Wer generiert den Schlüssel?

Zeuge Andreas Könen: Der Schlüssel - - Also, das ist ja immer eine Schlüsselhierarchie. Der letzte konkrete Schlüssel wird in der Maschine erzeugt, mit der er letztlich verschlüsselt wird. Und die Hierarchie: Dafür ist das BSI dann als zentrale Wurzelinstanz zuständig.

Martina Renner (DIE LINKE): Aber es war mir noch mal wichtig, zu klären, dass es eben auch deutsche Tochterunternehmen ausländischer Firmen gibt.

Zeuge Andreas Könen: Es geht immer dann in der präzisen Formulierung um den Vertragspartner, und das ist ein deutsches Tochterunternehmen dann einer US-Firma.

Martina Renner (DIE LINKE): Ich würde Ihnen gerne noch eine andere Akte vorhalten. Das ist MAT A BND-8b. Das ist die Tagebuchnummer 54/14, dort ab Seite 32. Dort geht es um die Problematik, dass Sicherheitstechnik in Deutschland insbesondere an Behörden herangedient werden sollte, die nach Erkenntnis des BND dahin gehend kompromittiert war tatsächlich, dass sie Daten - und es geht um Raumüberwachungssysteme - ausroutet - -

Vorsitzender Dr. Patrick Sensburg: Herr Wolff, bitte.

Martina Renner (DIE LINKE): Ja.

RD Philipp Wolff (BK): Es handelt sich um ein eingestuftes Papier, aus dem kann der Inhalt hier in der Sitzung nicht kundgetan werden.

Martina Renner (DIE LINKE): Okay. - Dann möchte ich nur Sie fragen, ob Sie - Sie können sich das gerne mal ansehen; das ist ab Seite 32 - diesen Inhalt entweder im BND oder später als BSI zur Kenntnis genommen haben und wenn ja, wann. Das geht ja so da allgemein.

(Dem Zeugen werden Unterlagen vorgelegt - Er blättert und liest darin)

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir eine konkrete Vorhaltfrage haben.

Martina Renner (DIE LINKE): Genau. Die Vorhaltfrage war: Seit wann kennen Sie diesen Vorgang, und haben Sie diesen als BND oder als BSI zur Kenntnis genommen? Ist kein Inhalt. Wir hatten ja letztens auch schon das Thema hier gehabt,

dass die GBA sich inzwischen damit beschäftigt usw.; ist ja hier ausführlich erörtert.

Vorsitzender Dr. Patrick Sensburg: Kann ich die Frage so abdrehen: Kennen Sie diesen Vorgang, ist er Ihnen bekannt? Seit wann? Könnte eine konkrete Einordnung eines eingestuften Sachverhalts sein. Ist ja nur eine Erinnerungsstütze, dass ein Zeuge einen Vorhalt, den er sonst nicht kennt, doch wiedererkennt.

Zeuge Andreas Könen: Also, der Vorgang ist mir, so wie er hier liegt, nicht bekannt. Keine Erinnerung, dass mir so etwas je vorgelegen hätte.

Martina Renner (DIE LINKE): Wäre das etwas, was das BSI interessieren würde?

Vorsitzender Dr. Patrick Sensburg: Müssten wir eingestuft fragen dann, glaube ich.

Zeuge Andreas Könen: Also, so schnell man so was eben scannen kann jetzt beim Lesen, sind grundsätzlich immer alle Vorgänge - das wird ja auch aus unserer Auswertung der Snowden-Dokumentation deutlich - interessant, wo Manipulationen stattfinden zur Datenausleitung. Klar, aber - -

Martina Renner (DIE LINKE): Gibt es eine Übereinkunft mit dem BND und dem BfV, wann solche Vorgänge dem BSI zur Kenntnis gebracht werden?

Zeuge Andreas Könen: Also, es gibt keine präzise Einzelvereinbarung zwischen unseren Behörden, sondern es gibt nur die abstrakten Bestimmungen etwa der Verschlusssachenanweisung, dass Erkenntnisse über entsprechende Vorgänge, die Auswirkungen auf die Informationstechnik des Bundes haben, natürlich auch dem BSI zur Kenntnis zu bringen sind, um entsprechende Maßnahmen einzuleiten. Aber nicht - -

Martina Renner (DIE LINKE): Der BSI-Präsident sitzt auch in der Präsidentenrunde?

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): Nein, der ist nicht Teil der Präsidentenrunde.

Zeuge Andreas Könen: Nein, nein.

Martina Renner (DIE LINKE): Dann kann er auf dem Wege auch von so etwas - -

Zeuge Andreas Könen: Also, auf dem Wege nicht. Sondern da ist in der Regel immer eine Einzelaktion der Sicherheitsbehörde erforderlich.

Martina Renner (DIE LINKE): Kennen Sie andere solche Fälle, also dass man etwas kompromittiert und unterjubelt?

Zeuge Andreas Könen: Also, wie gesagt, alleine die Snowden-Vorgänge machen so etwas deutlich.

Martina Renner (DIE LINKE): Nein, faktisch. Also Sie, hatten Sie mal - -

Zeuge Andreas Könen: Wir haben auch faktisch schon natürlich in diversen Zusammenhängen Gerät untersucht, was immer wieder manipuliert worden ist. Das hat aber im Grunde nichts mit diesem Untersuchungsauftrag zu tun, -

Martina Renner (DIE LINKE): Kein Five-Eyes-Bezug.

Zeuge Andreas Könen: - sondern das finden Sie an massiv vielen Stellen, dass Gerät manipuliert wird - bis hin zum Privatmann, der so was versucht.

Martina Renner (DIE LINKE): Ja, ja. Haben Sie auch mal Gerätschaften im BND oder beim BfV dahin gehend untersucht, ob sie manipuliert sind?

Zeuge Andreas Könen: Wir überzeugen uns auf Anforderung auch bei Einzelgerät davon, ob gegebenenfalls Manipulationen vorliegen. Dazu gibt es eine ganze Komponente, die nicht nur Gerät unter die Lupe nimmt, sondern auch Räumlichkeiten. Das ist die Lauschabwehr des BSI, die das natürlich exakt macht und sich auch anschaut.

Martina Renner (DIE LINKE): Und das machen diese auch regelmäßig.

Zeuge Andreas Könen: Ja, die sind ausgebucht. Haben einen Turnus etwa hier auch in Berlin, das genau durchzuführen.

Martina Renner (DIE LINKE): Und wenn Sie US-amerikanische Hard- oder Software untersuchen, was haben Sie da zur Verfügung außer dem Gerät? Handbücher?

Zeuge Andreas Könen: Das kommt auf den Einzelfall an. Wenn wir überhaupt Gerät von Herstellern untersuchen, kommt es immer sehr auf die Zusammenhänge an, in denen das dann vorliegt. Das ist völlig klar. Es geht oft sogar mit Unterstützung des Herstellers, der ein hohes Interesse oft daran hat, Manipulationen zu vermeiden und sein Gerät auch sauber zu halten. Das ist klar.

Martina Renner (DIE LINKE): Bei den Zertifizierungen, wenn es um Gerätschaften geht, die durch einen AND eines Five-Eyes-Landes übergeben wurden, Software oder Hardware, ist es möglich, diese Geräte zu zertifizieren, ohne sie anzusehen?

Zeuge Andreas Könen: Das hängt von der Evaluierungsstufe ab, die eingefordert ist. Auf den niedrigen Evaluierungsstufen findet Blackbox Testing statt, auf den höheren Stufen, nein, da geht es nicht ohne präzises Ansehen der Technik selbst, und auf den extrem hohen Stufen ist im Grunde mathematisch nachweisbar, von der Dokumentation, der Entwicklungsdokumentation, bis zum fertigen Gerät alles nachzuweisen.

Martina Renner (DIE LINKE): Und wer legt fest, welche Stufe jeweils quasi nun nötig ist, also wo - -

Zeuge Andreas Könen: Also, der Hersteller stellt selber einen Antrag beim BSI, auf welcher Stufe er sein Gerät zertifizieren - -

Martina Renner (DIE LINKE): Nein, ich rede jetzt davon, der BND bekommt von der NSA eine Software oder Hardware, und das muss ja durch Sie zertifiziert werden. Was passiert dann? Also, wer legt fest, ob das sozusagen ferngewartet wird, indem man mal irgendwie das Handbuch durchblättert, und wer legt fest, ob man sich auch das Gerät anschaut und mal angeschaltet und vielleicht sogar mal aufschraubt? Wer entscheidet das?

Zeuge Andreas Könen: Ja. Also, jetzt müssen wir erst mal sehr präzise unterscheiden zwischen dem Begriff „Zertifizierung“ und „Zulassung“ und dann noch „Freigabe“. Zertifizierung ist der Vorgang, den wir nach BSI-Gesetz, § 9, Recht der Wirtschaft, anbieten als zentrale Zertifizierungsstelle des BSI gegenüber der Wirtschaft - - und dem Angebot, dieses oder jenes Produkt oder diese oder jene Dienstleistung zu zertifizieren nach unterschiedlichen Maßstäben, wie ich das in meinem Eingangsstatement dargestellt habe.

Dann gibt es den Begriff der Zulassung. Wenn irgendeine Behörde eben Gerät oder Dienstleistungen in ihren entsprechenden IT-Einrichtungen einbringt, dann sind bestimmte Anforderungen zu erfüllen, um das jeweilige VS-Niveau zu wahren. Und in dem Zuge sind dann auch VS-zugelassene Geräte, NfD-zugelassen oder wie auch immer, zu verwenden. Das sind zunächst mal abstrakte - nicht abstrakt - - Aber es sind Prüfungen, die beim BSI am Gerät stattfinden oder wo der Dienstleister eine Dienstleistung entsprechend bewerten lässt. Dann - -

Martina Renner (DIE LINKE): Und bei der Zulassung wird immer auch das Gerät angeschaut, angeschaltet, aufgeschraubt.

Zeuge Andreas Könen: Wenn ein Gerät essenziel nach der VSA und dem entsprechenden § 28 - nach meiner Erinnerung - eben entsprechend zugelassen werden muss, ja, dann werden die höheren Maßstäbe angewendet, dann findet auch eine präzise An- -

Martina Renner (DIE LINKE): Und wenn ein Gerät im Zusammenhang mit Datenerfassung, also Grundrechtseingriffen, eingesetzt werden sollen, ist es - -

Zeuge Andreas Könen: Das sind in der Regel keine Gerätschaften, die dem Regime nach Verschlusssachenanweisung unterliegen, sondern die unterliegen dann entweder dem schon zitierten § 27 der TKÜV, soweit es die Ausleitung bei Providern betrifft, und innerhalb der Liegenschaften etwa einer Sicherheitsbehörde hat der jeweilige Dienststellenleiter zu entscheiden, ob Gerät, das da eingebracht wird, den Schutzanforderungen der VSA gerecht wird. Da gibt es aber kein explizites Zulassungsregime für Gerät.

Kryptoprodukte, das, was zur Verschlüsselung von Strecken eingesetzt wird, das Ganze, was wir auch schon mehrfach heute diskutiert haben: Ja, da muss auch der Behördenleiter entsprechendes Gerät hernehmen, das das BSI zugelassen hat; aber bei diesen Spezialthemen, über die Sie jetzt reden, muss er im Einzelfall entscheiden, ob und wie er das BSI einbezieht.

Vorsitzender Dr. Patrick Sensburg: Und jetzt müssten wir wechseln.

Martina Renner (DIE LINKE): Okay.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Dann kommen wir jetzt zur Fraktion der CDU/CSU. Gibt es da noch Fragen in öffentlicher Sitzung? - Das ist nicht der Fall. - Dann kommen wir zur Fraktion Bündnis 90/Die Grünen. Herr Kollege von Notz beginnt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Herr Könen, diese Ausführungen vorhin bezüglich der Möglichkeiten von Lokalisierungen durch bestimmte Merkmale, sind die mal vom GBA oder der Staatsanwaltschaft Wiesbaden bei Ihnen abgefragt worden?

Zeuge Andreas Könen: Ist jetzt nicht in meiner Erinnerung; aber, wie gesagt, die Anfrage läuft ja noch.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Bitte?

Zeuge Andreas Könen: Ich sagte ja, der Beweisbeschluss ist ja noch in der Finalisierung. Also, mir ist nicht bewusst, dass der GBA das angefragt hat.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Haben Sie sich überhaupt schon mal schriftlich dazu irgendwie gegenüber einer anderen Behörde geäußert?

Zeuge Andreas Könen: In dem Zusammenhang hier mit den Vorgängen, die hier diskutiert werden, nein.

Vorsitzender Dr. Patrick Sensburg: Jetzt muss ich mal kurz dazwischenfragen - ich stoppe auch die Zeit -, vielleicht bin ich der Einzige, der das nicht versteht: Welcher Beweisbeschluss ist in der Finalisierung?

Zeuge Andreas Könen: Der BSI-14 - - ist ja jetzt immer die Rede davon. Das ist der Beweisbeschluss.

Vorsitzender Dr. Patrick Sensburg: Also in der Erfüllung.

Zeuge Andreas Könen: Ja, in der Erfüllung. Entschuldigung, unpräzise Wortwahl.

Vorsitzender Dr. Patrick Sensburg: Ach so, weil finalisiert - - Okay, jetzt habe ich es verstanden. War jetzt am Überlegen, Beweisbeschluss GBA, geht ja nicht.

Zeuge Andreas Könen: Nein, nein, nein.

Vorsitzender Dr. Patrick Sensburg: Dann verstehe ich es. Im Zusammentragen.

Zeuge Andreas Könen: Der BSI-14, der sich auf die Fragen der Lokalisierung richtet und in dem wir gehalten sind, alle Unterlagen dazu zusammenzustellen.

Vorsitzender Dr. Patrick Sensburg: Okay. Ich denke, ich frage lieber, dann weiß ich es zumindest. Wenn es die anderen alle schon vorher wussten, ist ja gut.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): „In der Erfüllung“ klingt so vielversprechend. Bin sehr gespannt, was dann kommt.

(Christian Flisek (SPD): Erfahrungswerte!)

- Ja. - Aber gut. Also, Sie können sich auf jeden Fall nicht erinnern - -

Zeuge Andreas Könen: - - dass der GBA da - - Nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Weil die haben sich ja mit dieser Frage irgendwie beschäftigt, und da auf die Expertise zurückzugreifen, hätte vielleicht ja hilfreich sein können. Na gut.

Als wir vorhin über XKeyscore oder XKeystore - oder ich kaufe XKeyscore im XKeystore; oder Poseidon heißt das ja auch bei anderen Behörden - geredet haben: Wie schätzen Sie denn dieses Instrument ein? Also, wir haben hier gelernt, damit kann man Daten auswerten und erfassen. So. Wenn ich Ihnen das jetzt geben würde auf einem Stick, würden Sie das im BSI in Ihren Rechner stöpseln?

Zeuge Andreas Könen: Na, das ist völlig klar. Nein, Sie reden jetzt über das Gefährdungspotenzial, was von einem - - direkt ausgeht.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich würde gerne wissen, was Sie denken, was das ist. Ich frage Sie mal ganz direkt, -

Zeuge Andreas Könen: Ja.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): - weil ich so wenig Zeit habe, Herr Könen: Könnte es sein, dass das eine Trojanersoftware ist?

Zeuge Andreas Könen: Das ist natürlich im ersten Ansatz niemals auszuschließen -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Andreas Könen: - und gehört zum Prüfspektrum des BSI, wenn das in einer entsprechenden Einrichtung benutzt wird.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Beunruhigt es Sie so wie mich, dass der Bundesnachrichtendienst das in Deutschland an verschiedenen Außenstellen eingesetzt hat?

Zeuge Andreas Könen: Das beunruhigt mich vielleicht nicht so wie Sie, weil ich genau weiß, dass die Kollegen sehr wohl eine entsprechende Sicherheitsbetrachtung durchführen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, da bin ich mir jetzt nicht ganz so sicher. Und wenn Sie da nähere Erkenntnisse haben, wäre mir das sehr recht, wenn Sie mir die zukommen lassen. Also aus unseren Akten geht das schon hervor, dass also zumindest das Bundesamt für Verfassungsschutz sehr unterschiedlich damit umgeht als jetzt der Bundesnachrichtendienst.

Aber um es noch mal auf den Punkt zu bringen: Dieses Instrument XKeyscore, dass das nicht nur Daten verarbeitet oder Daten erfasst, sondern dass das eventuell - ich will jetzt nicht wieder anfangen mit dem Hidden Exit Trail - eine Software ist, die Dinge tut, die man nicht auf den ersten Blick erfasst, wenn man sie sieht, dem würden Sie zustimmen, dass das sein könnte?

Zeuge Andreas Könen: Das ist bei fast jeder Software, die wir verwenden, so, -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Andreas Könen: - dass es sein könnte natürlich bei den heutigen Gegebenheiten, auch den Betriebssystemen mit ihren Schwachstellen, aber auch vor allen Dingen dann, wenn Sie ein Tool wissentlich programmieren. Natürlich kann ich es versuchen - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, gut, Herr Könen, das Relativistische - -

Zeuge Andreas Könen: Was soll ich sagen ohne konkrete Anschauung des jeweiligen Produktes außer einer generellen Aussage?

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also, Sie haben sich XKeyscore nicht angeguckt, nicht beim BND und nicht beim Bundesamt für Verfassungsschutz?

Zeuge Andreas Könen: Ich persönlich nicht. Und unsere Mitar- -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Nein, Sie persönlich - - Ihr Haus natürlich.

Zeuge Andreas Könen: Nein, unser Haus - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, was?

Zeuge Andreas Könen: Ich habe verwiesen auf den Vorgang, der aktuell mit dem Verfassungsschutz läuft, aber außerhalb des Untersuchungszeitraumes liegt, und habe die abstrakte Vorgehensweise geschildert. Alles andere müssten Sie dann - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): So, seit wann prüfen Sie das denn?

Zeuge Andreas Könen: Das sind Fragestellungen, die natürlich im Rahmen - - Wir überprüfen das auf eine Anforderung - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Nein, seit wann, war die Frage, seit wann; das ist zeitlich gemeint.

Zeuge Andreas Könen: Das ist irgendwo seit später als 2014, Mitte. Ich kann es nicht genau sagen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Irgendwo später als 20- -

Zeuge Andreas Könen: Ich kann Ihnen leider nicht so genau sagen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Auf jeden Fall nach unserem Untersuchungszeitraum; das ist das, was Sie mir sagen wollen. Auf jeden Fall, nicht? Also, nichts im Leben ist sicher, was XKeyscore macht. Aber das ist sicher, dass es nicht um Untersuchungszeitraum liegt, ja?

Zeuge Andreas Könen: Da mir die Unterlagen dazu nicht komplett vorliegen, kann ich Ihnen da einfach nicht mal aus gutem Willen präzisere Auskunft geben.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wie bitte?

Zeuge Andreas Könen: Entschuldigung?

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wie bitte? Sie können mir das nicht sagen, weil Ihnen da noch nicht die Akten zusammengestellt worden sind?

Zeuge Andreas Könen: Nein, nein, weil dieses Verfahren noch ein laufendes Verfahren ist.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Welches Verfahren?

Zeuge Andreas Könen: Das, was ich eben abstrakt geschildert habe.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Die Prüfung von XKeyscore.

Zeuge Andreas Könen: In der Prüfung des Einsatzes beim BfV, ja.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, gut; aber wenn Sie sozusagen vor dem Untersuchungszeitraum angefangen haben, das zu untersuchen - -

Zeuge Andreas Könen: Nein - -

Vorsitzender Dr. Patrick Sensburg: Ganz kurze Unterbrechung, Herr Könen, Herr Akmann meldet sich.

MR Torsten Akmann (BMI): Ich glaube, wir können das ein Stück weit abkürzen: Das spielt sich alles nach dem Untersuchungszeitraum ab.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das ist ja praktisch. Das ist ja super. Also, aber unfassbar, echt!

Zeuge Andreas Könen: Ja, Entschuldigung. Nein, um das noch mal -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Andreas Könen: - wirklich deutlich klarzustellen: Die Befassung mit dem Tool selber im Zusammenhang mit einer Installation des Tools bei einer anderen Behörde läuft erst nach Juni/Juli 2014. Vorher haben wir uns mit dem Tool lediglich in diesem genannten Vorstellungstermin in 2012 einmal auseinandergesetzt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und haben Sie dazu irgendwas schriftlich verfasst?

Zeuge Andreas Könen: Ja, das liegt auch dem Untersuchungsausschuss vor, welche Gespräche da gelaufen sind und wie das im Einzelnen dargestellt und von uns bewertet worden ist.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und im Hinblick auf die Software XKeyscore, eingesetzt bei Bundesnachrichtendienst, da prüfen Sie nichts, da gucken Sie sich nichts an, und da haben Sie - -

Zeuge Andreas Könen: Da gibt es keinen laufenden Vorgang, auch keinen von vergangenen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, keinen laufenden Vorgang, auch keinen abgeschlossenen.

Zeuge Andreas Könen: Nein, nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Es gibt keinen Vorgang.

Zeuge Andreas Könen: Nein.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das BSI war mit XKeyscore in den Außenstellen des Bundesnachrichtendienstes -

Zeuge Andreas Könen: Nicht befasst.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): - nicht befasst. Aha.

Zeuge Andreas Könen: Um das - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, gut. Mhm. - So. Sagt Ihnen die Geschichte Belgacom was? Haben wir ja schon kurz darüber gesprochen, sagt Ihnen was.

Zeuge Andreas Könen: Ja.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Können Sie vielleicht kurz umreißen, worum es da geht inhaltlich?

Zeuge Andreas Könen: Also, Belgacom spricht von einem Cyberangriff auf den belgischen Telekommunikationsprovider, in dessen Rahmen eben eine mehrstufige Software installiert worden ist.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Können Sie die Software vielleicht beim Namen nennen?

Zeuge Andreas Könen: Die Software ist in anderen Umständen zum Beispiel als Regin bekannt, ja.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Genau. So, und wer ist Kunde der Belgacom, relevanter Kunde der Belgacom gewesen? Warum war das so eine interessante Geschichte? Bei Snowden heißt das ja, glaube ich, Operation „Socialist“.

Zeuge Andreas Könen: Also, die Kunden sind mir jetzt im Einzelnen nicht bekannt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Europäische Kommission.

Zeuge Andreas Könen: Das ist anzunehmen, dass die - - Aber da kann ich jetzt nur spekulieren.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das ist so. Ja, nein, nein, da braucht man

nicht spekulieren, das ist so, ja? - So, und wo wurde Regin noch eingesetzt? Wo haben Sie sich noch mit Regin befasst in den letzten Jahren?

Zeuge Andreas Könen: Also, wir haben Regin in - - Also, nach meiner Erinnerung sind die weiteren präzisen Aussagen zu diesem Vorgang eingestuft, und für die könnte ich nicht - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich glaube, sie standen alle schon bei *Spiegel Online*.

Zeuge Andreas Könen: Ich könnte Ihnen - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das Bundeskanzleramt, eine Mitarbeiterin aus dem Bundeskanzleramt.

Zeuge Andreas Könen: Also, wir können das natürlich gerne noch mal aufrollen, was wir im Innenausschuss bzw. im Ausschuss Digitale Agenda dazu dargestellt haben. Ähnliche Schadsoftware ist eben festgestellt worden bei einer Mitarbeiterin des Bundeskanzleramtes und da zum Einsatz gekommen, und ähnliche Software - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und in welchem Zusammenhang hat die gearbeitet zum fraglichen Zeitraum? Liegt, glaube ich, ja in unserem Untersuchungszeitraum.

Zeuge Andreas Könen: Mir ist nur ungefähr bekannt, dass die auch im außenpolitischen Bereich eingesetzt war. Präzise das Referat kann ich Ihnen nicht nennen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich habe irgendwo gelesen, dass sie für die Europäische Union zuständig war. Also, Sie wollen sagen, dass Sie die Hintergründe, ob es da ein gezielter Angriff war mit Regin im Hinblick auf EU-Verhandlungen, deutsche EU-Verhandlungen oder so - - das haben Sie nie erwogen, sondern - -

Zeuge Andreas Könen: Das ist etwas, was nicht Aufgabe des BSI ist, dem dann entsprechende andere Behörden nachzugehen haben.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Welche Behörden würden dem nachgehen?

Zeuge Andreas Könen: In dem Falle, wo es sich um einen Angriff auf Deutschland handelt, das BfV und in dem Falle, wenn eventuell Aufklärung in nachrichtendienstlicher Hinsicht zu erwarten ist, BND und wenn Strafbarkeiten vorliegen, das BKA.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und regional, wo haben Sie den Angriff Regin verortet? Waren das die Russen oder die Amerikaner?

Zeuge Andreas Könen: Eine Attribution haben wir nicht vorgenommen, da wir konkrete Angriffe in dieser Weise nicht präzise nachverfolgen konnten, was auch dann wieder nicht unsere Aufgabe war.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das, Herr Könen, sehe ich anders, und es steht meiner Ansicht nach auch in den Akten anders, die leider Geheim sind, und ich kann Ihnen die jetzt nicht vorhalten; aber ich glaube, die Verortung wurde schon himmelsrichtungstechnisch vorgenommen. Können Sie das vielleicht doch noch mal versuchen zu erinnern?

Zeuge Andreas Könen: Also, wie gesagt, es sind Vermutungen dann; aber es sind keine Beweise dafür.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, diese Diskussion kennen wir hier zur Genüge.

Zeuge Andreas Könen: Ja, also, das ist - -

Vorsitzender Dr. Patrick Sensburg: Zumal wenn es in der geheimen Akte steht, wir es so bewerten können oder so einordnen können; sonst würden wir ja schon eine Essenz aus einer Geheimakte hier kundtun.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, genau.

Vorsitzender Dr. Patrick Sensburg: Dafür sind ja dann die eingestuften Sitzungen da.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, genau.

Vorsitzender Dr. Patrick Sensburg: Von daher würde das ja einen Eindruck erwecken, den gerade die Opposition immer bei Zeugen kritisiert, dass sie hier Andeutungen machen, aber dann nicht liefern können, und das machen wir natürlich umgekehrt auch nicht.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich kann liefern, ich kann liefern.

Vorsitzender Dr. Patrick Sensburg: Das haben die Zeugen auch immer gesagt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Da drüben können ja zur sozusagen Abwiegelung falscher Eindrücke Herabstufungen stattfinden. Die Sachen sind sowieso alle presseöffentlich geworden.

Vorsitzender Dr. Patrick Sensburg: Ja, aber das spielt ja juristisch keine Rolle; das wissen wir ja auch.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, häufig sozusagen, ja - -

Vorsitzender Dr. Patrick Sensburg: Hilft nur jetzt nichts. Sollen wir erst mal - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Was hilft Ihnen nichts?

Vorsitzender Dr. Patrick Sensburg: Es hilft nichts, zu sagen: „Das steht alles schon in der Presse“, weil wir das endlos durchdiskutiert haben, dass eine Presseveröffentlichung einen eingestuften Sachverhalt nicht herunterstuft.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, das mag ja sein, trotzdem ist es - - Es gibt - -

Vorsitzender Dr. Patrick Sensburg: Und wenn wir das jedes Mal erwähnen, wird es nicht besser.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wenn ich, Herr Vorsitzender, den Zeugen frage, aus welcher Himmelsrichtung das wohl kommt, und es gibt ganz offene Diskussionen im BSI, was für Kooperationen man beenden müsste oder so, himmelsrichtungsverortet, und er sagt: „Nein, also ich weiß es wirklich nicht“, oder so, dann ist das falsch, ja? Dann kann er sagen: „Ich sage dazu nichts, nicht in öffentlicher Sitzung“, okay, das höre ich mir noch an. Aber er kann nicht sagen: „Nein, ist mir nicht erinnerlich“; dann erweckt er einen falschen Eindruck.

Zeuge Andreas Könen: Nein, das habe ich auch nicht gesagt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und ich kann Ihnen das jetzt vorhalten. Vielleicht will das BMI das zulassen, dass wir das hier kurz öffentlich vorlesen, damit das deutlich wird.

Vorsitzender Dr. Patrick Sensburg: In dieser Runde können wir das nicht mehr machen.

Zeuge Andreas Könen: Ich sage nicht, dass es mir nicht erinnerlich ist, ich sage, -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Sondern was sagen Sie?

Zeuge Andreas Könen: - die Attribution ist nicht mit sicherer technischer Sicherheit durchzuführen. Das ist das, was ich sage.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, die ist nie durchzuführen; die ist nie sicher durchzuführen. Das ist ja einer der Gags bei Cyberangriffen, dass Sie nie eine Sicherheit haben. Aber trotzdem treffen Sie doch eine Zuordnung. Und es ist einfach eine Verwirrung der Öffentlichkeit oder was auch immer. Es ist unzureichend, wenn Sie so antworten, als könnten Sie wirklich nicht sagen, woher das kommt. Im Haus hat es eine klare Zuordnung gegeben, ja? Natürlich hat niemand gesagt, das ist bewiesen. Es sind

viele Sachen auf der Welt nicht bewiesen; aber man sagt trotzdem, es ist - -

Zeuge Andreas Könen: Ja, aber dann, wenn spekuliert wird, muss ich am Ende das Fazit ziehen und das auf den Tisch legen, was ich wirklich dazu sagen kann. Und das mag dann auch Spekulation sein, die an der einen oder anderen Stelle getroffen wird, um inhaltlich weiterzukommen; aber was zählt, ist das Ergebnis. Und das Ergebnis ist klipp und klar das, dass ich die Attribution nicht vornehmen kann und dass ich dazu die Unterstützung dann auch weiterer Bundesbehörden benötige, um die zu erreichen. Es ist ja nicht so, dass man das nicht wollte, sondern das ist einfach - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Nein, diese Bundesbehörden zeigen immer in eine Himmelsrichtung; das ist mir auch schon aufgefallen. Aber sozusagen die Sache bezüglich Regin: Also, meiner Ansicht nach ist das zumindest verfälschend, wenn Sie das so darstellen; denn die Diskussionen bei Ihnen im Haus bezüglich woher so was kommt, sind eindeutig. Und man fragt sich wirklich, warum ein gestandener Beamter wie Sie nicht in der Lage dazu ist, das auch mal zu benennen. Also, die Bundesregierung ist ja auch nicht in der Lage, das zu benennen, sondern es ist sozusagen - - Sobald es an den Punkt geht, wird alles vage und diffus, und man mag nichts sagen. Und wenn das eben irgendwie das Problembewusstsein ist, dann wundert einen gar nichts mehr, ja? Also, ich finde es unerfreulich. Wir müssen es nachher dann in nichtöffentlicher Sitzung im Detail durcharbeiten.

Vorsitzender Dr. Patrick Sensburg: Gut, herzlichen Dank. - Dann kommen wir zur nächsten Fraktion. Das war eine individuelle Bewertung, die sicherlich jedem zusteht. Und die Fraktion der SPD macht jetzt mit Fragen weiter.

Christian Flisek (SPD): Genau. - Ich möchte noch mal so ein bisschen auf das Thema zurückkommen, das wir zuletzt, als ich Sie befragt habe, verlassen haben, also die Rolle der amerikanischen Hersteller von Software und Hardware, und versuche es jetzt mal so, Herr Könen: Auf einer Sitzung des Cyber-Sicherheitsrates im Juli 2013 haben Sie davon berichtet, dass es angeblich bis zu diesem Punkt nach Ihrer Kenntnis 25 sogenannte Hilferufe von deutschen Unternehmen gegeben hätte. Das findet sich in MAT A BMVg-5/3a, Blatt 282 ff. 25 Hilferufe von deutschen Unternehmen! Können Sie uns das mal erläutern?

Zeuge Andreas Könen: Also, diese 25 Hilferufe, die dort zitiert wurden, beziehen sich auf Cyberangriffe, die diese Unternehmen zu erleiden hatten und bei denen das BSI um entsprechenden Ratschlag angegangen wurde.

Christian Flisek (SPD): Was ist das zum Beispiel?

Zeuge Andreas Könen: Das sind typische Fälle, wenn durch eine Schadsoftware entsprechend Rechner übernommen wurden, Daten, wichtige Firmendaten zum Beispiel abfließen, Fragen, wie man das möglichst zügig unterbinden kann. Andere Fragestellungen wären heute, wie man sich gegen Ransomware schützt, Fragen dieser Kategorie.

Christian Flisek (SPD): Und was wurde dann diesen Firmen geraten?

Zeuge Andreas Könen: Also, diese Firmen schildern ja in der Regel konkrete Umstände dessen, was ihnen gerade passiert. Die erhalten dann eine Sofortempfehlung, was sie machen sollen, um den unmittelbaren Schaden abzustellen, und dann weitere Hinweise, wie sie ihre Infrastruktur besser absichern können.

Christian Flisek (SPD): Und seitdem kommen da weitere Hilferufe? Hat sich die Zahl der Hilferufe nach Snowden erhöht?

Zeuge Andreas Könen: Also, im Bereich Cyber erhöht sich die Zahl der Fälle und damit auch die Zahl der Anfragen permanent. Cyberangriffe werden leider Gottes zu einem täglichen Problem, mit dem sich Unternehmen auseinandersetzen müssen, die dann auch durchaus an den verschiedenen Stellen bei uns anfragen, wie man das entsprechend heilen kann.

Christian Flisek (SPD): Ich gehe mal davon aus, eine große Zahl der Unternehmen nutzt Produkte amerikanischer Unternehmen. Äußern Sie sich in dieser Situation dazu, also angesichts ja auch dessen, was es an Schriftverkehr und Einschätzungen zu diesen Fragen und Produkten in Ihrem Hause gibt, gegenüber Unternehmen?

Zeuge Andreas Könen: Wir geben konkrete Hinweise zur Absicherung von Produkten. Da spielt dann letztlich der Hersteller oder die Provenienz keine Rolle.

Christian Flisek (SPD): Also, das ist herkunftsunabhängig.

Zeuge Andreas Könen: Weil einfach das Problem, was in dem Moment im Raum steht, gelöst werden muss. Es beruht auf Schwachstellen des Produktes oder der Konfiguration oder des Netzwerkes oder verschiedenster Anlässe, die da eine Rolle spielen können.

Christian Flisek (SPD): Handelt es sich bei diesen Angriffen denn um Angriffe eher, ich sage mal jetzt, aus einem kriminellen Milieu oder Angriffe auch von Nachrichtendiensten?

Zeuge Andreas Könen: Also, mit einem extrem überwiegenden Anteil handelt es sich um cyberkriminelle Angriffe jeglicher Couleur, auf die wir ja permanent hinweisen.

Christian Flisek (SPD): Aber es gab auch Fälle von Angriffen von Nachrichtendiensten.

Zeuge Andreas Könen: Es gab auch Fälle, bei denen man definitiv gesehen hat, dass die Fähigkeiten des Angreifers extrem hoch sein müssen, sodass also es nahe lag, auch auf Nachrichtendienste oder andere staatliche Institutionen zu schließen.

Christian Flisek (SPD): Konnten Sie da Rückschlüsse ziehen, ob das Nachrichtendienste waren, die in unseren Untersuchungsgegenstand fallen?

Zeuge Andreas Könen: Nein, konnten wir nicht, da wir ja in diesen Fällen eben tatsächlich nicht die weiter dahinter liegenden Attributionsinformationen zur Verfügung haben. Dazu müssten wir entsprechend in Kommunikationsverkehre eingreifen. Diese Möglichkeit haben wir nicht. Darum geben wir solche Fälle dann mit Einverständnis des Unternehmens in der Regel an das Bundeskriminalamt oder das BfV ab.

Christian Flisek (SPD): Und wissen Sie, was dann daraus wird, oder ist das dann bei Ihnen abgeschlossen?

Zeuge Andreas Könen: Ja, das erfahren wir über die Zusammenarbeit im Cyber-Abwehrzentrum dann auch praktisch regelmäßig, weil damit in der Regel noch mal eine unmittelbare Hilfeleistung für das Unternehmen verbunden ist, wo die Behörden zusammenarbeiten.

Christian Flisek (SPD): Gut, dann frage ich ganz konkret: Haben Nachrichtendienste aus den Five-Eyes-Staaten in der Zeit, die Sie überblicken, Angriffe auf deutsche Unternehmen vorgenommen? Gab es Fälle?

Zeuge Andreas Könen: Dazu liegen uns keine Erkenntnisse vor.

Christian Flisek (SPD): Gibt es denn - - Also, wenn Sie sagen, Sie selber haben keine Erkenntnisse, weil Sie die Fälle ja dann ans BKA abgegeben haben, Sie wissen nur, dass es sich wahrscheinlich aufgrund der Fähigkeiten, die dahinter waren, um Nachrichtendienste gehandelt haben muss - - Aber gibt es denn Mutmaßungen, dass es auch Nachrichtendienste der Five-Eyes-Staaten sein könnten?

Zeuge Andreas Könen: Also, nicht konkret, aber natürlich im Zusammenhang etwa mit den Snowden-Papieren, wie gerade eben auch schon diskutiert, klar, natürlich. Wenn eine Schadsoftware in den Snowden-Papieren auftaucht und an anderer Stelle - -

Christian Flisek (SPD): Wenn was auftaucht?

Zeuge Andreas Könen: Wenn eine Schadsoftware in den Snowden-Papieren dargestellt ist und ent-

sprechend dann an anderer Stelle wieder auftaucht, dann muss man sich natürlich fragen, wer überhaupt den Zugriff darauf hat.

Christian Flisek (SPD): Das bedeutet, das BSI hält es auch für - in den Gefährdungspotenzialen, die man so analysiert - möglich, dass Nachrichtendienste der Five-Eyes-Staaten gezielt auch deutsche Unternehmen attackieren.

Zeuge Andreas Könen: Dass die Dienste entsprechende Attacken auch in Deutschland ausüben könnten, also in einer Spekulation, und auf Unternehmen. Möglich ist das. Aber, wie gesagt, es liegen mir keine konkreten Erkenntnisse vor.

Christian Flisek (SPD): Mit welcher Motivation, glauben Sie, würden solche Dienste das machen?

Zeuge Andreas Könen: Das kann ich Ihnen nicht sagen. Da kann ich nicht hineinschauen, ob das - -

Christian Flisek (SPD): Gibt es hierzu einen Austausch mit dem Bundesamt für Verfassungsschutz, insbesondere mit den Leuten, die dort die Spionageabwehr - es sind ja nicht so viele - verantworten?

Zeuge Andreas Könen: Natürlich, im Rahmen des Cyber-Abwehrzentrums findet diese Diskussion statt. Und eine Attribution würde natürlich auch dem BSI in Abwehrmaßnahmen weiterhelfen; aber, wie gesagt - -

Christian Flisek (SPD): Glauben Sie, dass nach Ihrer Einschätzung die deutsche Spionageabwehr im öffentlichen und im privaten Bereich, im unternehmerischen Sektor gut aufgestellt ist?

Zeuge Andreas Könen: Also, insgesamt kann ich das nicht beurteilen, da ich natürlich in die entsprechenden Ämter nicht den Einblick habe. Aber in unseren gemeinsamen Aktionen etwa zum Wirtschaftsschutz und anderen Dingen sieht man, wir haben da noch eine ganze Menge zu tun, definitiv. Wir müssen den Unternehmen hier in Deutschland mehr Schutz zukommen lassen, wir müssen die auch besser aufstellen. Da hapert es an vielen Stellen.

Christian Flisek (SPD): Dann komme ich noch mal wirklich zum Ende meiner letzten Befragung dazu, weil Sie ja sich - - Ich verstehe das im Übrigen, dass man sich dagegen wehrt, so eine pauschale Aussage, wie ich sie vielleicht getätigt habe, zu unterschreiben oder zu bestätigen. Aber dann versuche ich, es zu präzisieren noch mal. Würden Sie denn sagen, dass deutsche Stellen, sage ich jetzt mal, ob das jetzt Behörden sind oder auch Unternehmen, die geschützte Kommunikation betreiben wollen, sei es, weil es sich um eingestufte öffentliche Informationen handelt, sei es, weil es sich beispielsweise um Geschäfts- und Betriebsgeheimnisse handelt - - also, wer so etwas will, dass der sich auf marktgängige Hard- und Software aus US-amerikanischer Provenienz verlassen kann?

Zeuge Andreas Könen: Er sollte sich auf das verlassen, was wir da zertifizieren, weil wir ja die Fähigkeit besitzen, das genauer anzuschauen und dann anhand dessen auch zu bewerten, wann man welches Risiko eingehen kann, definitiv.

Christian Flisek (SPD): Gut, also das bedeutet auch, Sie würden sagen, da einfach ein Produkt von der Stange herzunehmen, um so eine geschützte oder schützenswerte - -

Zeuge Andreas Könen: Nicht, Werte zu schützen. Dabei sollte ich kein Produkt von der Stange hernehmen, sondern sollte ich mich genau informieren, welche Sicherheit damit verbunden ist, und dafür stehen wir halt zur Verfügung.

Christian Flisek (SPD): Und Sie würden schon sagen, dass das bei deutschen und bei europäischen Herstellern dann anders ist oder wäre.

Zeuge Andreas Könen: Ich habe da natürlich bessere Möglichkeiten, diese Sicherheitsmaßnahmen zu bewerten und auch zu einer positiven Beurteilung zu kommen. Das ist definitiv so. Dann müssen Unternehmen aus anderen Ländern, die entsprechende Abkommen etwa nicht besitzen, in der Zertifizierung oder anderen wechselseitigen Aktionen - - die müssen da etwas mehr draufLegen. Das ist ja genau auch der Sinn dessen ge-

wesen, was ich mit den Vertraulichkeitserklärungen und anderen Dingen in den Raum gestellt habe.

Christian Flisek (SPD): Glauben Sie, dass es angesichts der Marktverhältnisse, die wir in diesem Bereich vorfinden, ausreichend ist, wenn ich jetzt mal unterstellen würde, so was wie deutsche Unternehmen - auch natürlich deutsche Bürger, aber ich formuliere das jetzt - - ich spitze das jetzt mal auf den wirtschaftlichen Bereich zu - vor solchen Attacken zu schützen - - Glauben Sie, dass unser bisheriges System da ausreichend ist, was ja ganz im Wesentlichen auf Beratung und Empfehlung hinausläuft?

Zeuge Andreas Könen: Also, dass wir dieses System ausbauen müssen, da bin ich fest von überzeugt.

Christian Flisek (SPD): In welche Richtung denn?

Zeuge Andreas Könen: Wir müssten es stärker ausbauen in der Richtung, dass wir Unternehmen, die zum Beispiel kritische oder sensitive oder personenbezogene Daten verarbeiten, in stärkerer Weise dann auch an die Nutzung solcher geprüfter Sicherheit, geprüfter IT, binden. Das sind klare Anforderungen, die wir zum Beispiel im Rahmen jetzt des IT-Sicherheitsgesetzes bereits für kritische Infrastrukturen stellen. Aber es gibt wesentlich mehr Bereiche der deutschen Wirtschaft, die wir im gleichen Sinne weiter verpflichten sollten, zumal das natürlich auch noch den entsprechenden Marktdruck ergibt, auch so etwas wirklich zu produzieren, und damit wiederum Aussichten für verlässliche Herstellung. Das ist ein total erstrebenswertes Szenario, das zu gewährleisten; aber es kostet natürlich alle Beteiligten auch entsprechende Investitionen.

Christian Flisek (SPD): Und ich frage jetzt noch mal wirklich auch provozierend: Glauben Sie, dass eine Organisation wie das BSI, das selber kooperiert mit anderen Diensten, das unter der Aufsicht eines Bundesinnenministeriums steht, wo auch das Bundesamt für Verfassungsschutz eingeordnet ist, wo man enge Kontakte zum BND hat, glauben Sie, dass diese Organisationsform die geeignete Vertrauensbasis dafür liefert, dass man Unternehmen stärker animiert, vielleicht sogar irgendwann mal gesetzlich verpflichtet, an solchen Maßnahmen stärker teilzunehmen?

Zeuge Andreas Könen: Ja.

Christian Flisek (SPD): Glauben Sie.

Zeuge Andreas Könen: Da bin ich deswegen fest von überzeugt, weil sich das BSI ja nicht alleine in dieser Kooperation manifestiert und definiert - - sondern dass wir weite Bereiche unserer Kapazität unseres Amtes dafür einsetzen, genau für die Felder der Digitalisierung entsprechende Schutzmaßnahmen zu definieren, genau in diese Breite hineinzuwirken, in der das von Ihnen geforderte sichere IT-Equipment auch eingesetzt werden muss, dass wir eine sehr breite Vertrauensbasis da genießen, etwa in der Kooperation zum EnWG, zu Themen jetzt auch des automatisierten Fahrens, dann im gesamten Telematik- und Gesundheitssektor - das sind Themen, wo wir ein hohes Vertrauen genießen -, und dadurch, dass wir auf der anderen Seite Gefährdungen gemeinsam mit den Sicherheitsbehörden präzise untersuchen. Das stellt das nicht infrage, im Gegenteil: Man sieht dadurch eine Gesamtkompetenz des Amtes, die uns auch in dieser Breite nur förderlich ist.

Christian Flisek (SPD): Wer sieht das? Wirtschaftsministerium sieht das?

Zeuge Andreas Könen: Nein, das sehen vor allen Dingen auch die Unternehmen selber, die wir da unterstützen wollen. Das sehen wir ja an der Breite der Ansprache, die auf den verschiedensten Ebenen - Allianz für Cyber-Sicherheit, 1 400 Unternehmen als Mitglieder - zustande kommt.

Christian Flisek (SPD): Okay. - Sie arbeiten ja auch mit dem GCHQ zusammen.

Zeuge Andreas Könen: Ja, im Rahmen der EU- und NATO-Kooperation, korrekt.

Christian Flisek (SPD): Wenn wir uns jetzt nur mal so angucken, was wir so bekommen haben, dann sind sozusagen die Akten, die wir haben in

Bezug auf diese Zusammenarbeit, doch erheblich mehr als alles andere. Würden Sie sagen - also, wenn man das jetzt mal als eine Referenz für die Qualität und Quantität der Zusammenarbeit nimmt -, dass man sagt, man arbeitet verstärkt mit britischen, in dem Fall GCHQ und mit dem Office of Cyber Security and Information Assurance zusammen - verstärkt, als man das mit Amerikanern tut?

Zeuge Andreas Könen: Das kann ich jetzt nicht nachvollziehen, woher Sie den Eindruck gewinnen.

Christian Flisek (SPD): Nur von der Menge der Akten her.

Zeuge Andreas Könen: Von der Menge der Akten. Nun zeigen die Akten einen Ausschnitt aus der BSI-Kooperation. Ich würde das jetzt nicht - -

Christian Flisek (SPD): Ich hoffe, einen vollständigen, zumindest wenn es untersuchungsgegenständlich ist.

Zeuge Andreas Könen: Also, Untersuchungsgegenstand ist vollständig.

Christian Flisek (SPD): Ja, ich meine, wir hatten schon Gründe, daran auch zu zweifeln.

Zeuge Andreas Könen: Nein, das ist durchaus nicht - -

Christian Flisek (SPD): Na ja, aber wenn ich jetzt mal unterstelle, es ist ein vollständiger Ausschnitt, -

Zeuge Andreas Könen: Ja. Nein, es ist ein Ausschnitt - -

Christian Flisek (SPD): - zumindest ein vollständiger Ausschnitt der Kooperation zwischen 2001 und 2013 in Bezug auf alle Five-Eyes-Staaten, dann komme ich zum Ergebnis, Sie arbeiten vor allen Dingen mit den Briten zusammen. Und das ist falsch?

Zeuge Andreas Könen: Das sehe ich absolut nicht so, weil die Gesamtzusammenarbeit natürlich mit den Briten da stärker herausragt, wo es um die EU-Kooperation geht. Dadurch entsteht natürlich auch einfach eine stärkere zeitliche Präsenz, wo man in Gremien zusammenarbeitet. Aber das würde ich jetzt nicht in einer absoluten Wichtung sehen. Es ist immer eine Frage auch der Wichtigkeit für die Fragen der Informations- und Cybersicherheit, und die USA als eine starke produzierende Nation sind natürlich für das BSI von herausragender Bedeutung.

Christian Flisek (SPD): Sie haben ja gesagt, dass sozusagen die Europäer da einen gewissen, irgendwie einen anderen noch mal Vertrauensvorschuss im Zweifel genießen als die Amerikaner.

Zeuge Andreas Könen: Mhm.

Christian Flisek (SPD): Das heißt, wenn wir jetzt auch über Großbritannien reden: Ist Ihnen bekannt, dass zum Beispiel bei der GCHQ die NSA und andere eventuell im huckepack sind?

Zeuge Andreas Könen: Also, davon gehe ich grundsätzlich aus, nicht zuletzt natürlich aufgrund der Zusammenarbeit, die jetzt deutlich wird, über die aber in den vergangenen Jahrzehnten irgendwo immer Klarheit bestand. Das ist ja auch in anderen Veröffentlichungen, etwa zu Echelon, schon deutlich geworden. Das heißt, davon geht man aus. Allerdings, wie gesagt, in Ihrer Wichtung kann ich es nicht nachvollziehen, zumal auch in Europa ganz andere für uns im Mittelpunkt stehen, die noch deutlich herausragende Rollen einnehmen. Selbst die Niederlande und Schweden haben für uns in der direkten Kooperation etwa in der EU deutlich herausragendere Stellen, mal ganz zu schweigen von Frankreich. Das ist klar.

Christian Flisek (SPD): Ja. Ich frage deswegen, weil wir auf unserer Reise mit dem Ausschuss in die USA ein Gespräch hatten mit einem ehemaligen NSA-Mitarbeiter namens Robert Lee, der heute in einem Thinktank arbeitet, nämlich der New America Foundation, und der also gesagt hat, dass die NSA durchaus Fragen der Cyber Security an die britischen Partner verstärkt outsourct.

Zeuge Andreas Könen: Mhm, gut. Ich kann nur feststellen, dass beide Behörden entsprechende Kompetenz besitzen, und könnte jetzt nicht so präzise differenzieren zwischen dem, was der eine im Einzelnen kann und der andere nicht.

Christian Flisek (SPD): Ja, aber ist Ihnen dieses Outsourcing bekannt?

Zeuge Andreas Könen: Nein.

Christian Flisek (SPD): Da haben Sie gar keine Anhaltspunkte für?

Zeuge Andreas Könen: Nein.

Christian Flisek (SPD): Kennen Sie auch nicht?

Zeuge Andreas Könen: Wie die bilaterale Kommunikation oder der Austausch da läuft, das ist mir nicht bekannt.

Christian Flisek (SPD): Aber Sie würden trotzdem festhalten, dass die Briten nach wie vor dann irgendwie trotzdem aufgrund - Sie haben das angesprochen - des engeren Rechtsraums, in den sie eingebunden sind, und der damit verbundenen - irgendwie - Sanktionsmöglichkeiten vertrauenswürdiger sind.

Zeuge Andreas Könen: Ja. Es ist entscheidend für die Zusammenarbeit etwa mit britischen Unternehmen, da, wo die als Anbieter oder Produzenten auftreten, dass die sich in einem entsprechenden Rechtsraum befinden mit den entsprechenden Marktvorschriften. Das sind natürlich Grundlagen, auf denen man dann eine Zusammenarbeit leichter aufbauen kann als etwa dann, wenn man nur unter generellen - meinetwegen - WTO-Regularien oder anderen internationalen Regularien steht.

Christian Flisek (SPD): Ja, gut. Unser Eindruck hier in der Arbeit ist, ich sage mal: Wenn wir den Preis an den unkooperativsten Five-Eyes-Staat vergeben würden, dann würden wir den wahrscheinlich - - wäre Großbritannien ein heißer Kandidat.

Zeuge Andreas Könen: Insofern - - Es ist ja durchaus so, dass ich den Eindruck, den Sie gewonnen haben, dass es eine besonders starke Kooperation mit GCHQ gibt, nicht nachvollziehen kann. Ich sehe es wirklich auf gleichem Niveau.

Und auf der anderen Fragestellung, wie gesagt, „Was können wir in einer EU-Kooperation gewinnen?“, stehen für mich wirklich die EU-Gesichtspunkte im Mittelpunkt, da, wo ich etwa in einer Gesetzesinitiative vonseiten der EU-Kommission und Ähnlichem mit - - Da treffe ich natürlich mit britischen Kollegen zusammen. Aber das ist dann ähnlich einzuordnen, als würde ich mit französischen, niederländischen oder anderen reden, mit denen wir ganz bestimmte cybersicherheitliche Vorgehensweisen teilen.

Vorsitzender Dr. Patrick Sensburg: Okay. Wir müssten jetzt wieder wechseln.

Christian Flisek (SPD): Das geht immer so schnell. - Danke.

Vorsitzender Dr. Patrick Sensburg: Wir kommen in die nächste Fragerunde. Die nächste Fragerunde beginnt wieder Die Linke. Wir müssen so ein bisschen auf die Zeit gucken - vielleicht kriegen wir das irgendwie hin -, weil wir noch weitere Zeugen haben. - Frau Kollegin Renner.

Martina Renner (DIE LINKE): Ja, kriegen wir hin. - Ich würde gerne noch mal wissen: Bei dieser Bewertung der Snowden-Files - - Sie sagten eingangs, da saßen auch oder kooperierten auch BfV, BND und BSI. Wer jeweils war daran beteiligt? Also, wer - -

Zeuge Andreas Könen: In der Bewertung der Snowden-Dokumente, dass - -

Martina Renner (DIE LINKE): Ja. Wer vom BND, wer vom BfV und wer vom - -

Zeuge Andreas Könen: Nein, das haben wir ja, jede Behörde für sich, zunächst einmal in der Bewertung vorgenommen und uns dann entsprechend darüber auf Arbeitsebene in der Bewertung ausgetauscht. Wer jetzt jeweils da die Kontakt- und Ansprechpartner in den verschiedenen

Behörden waren, kann ich bis auf wenige Ausnahmen nicht aufzählen. Natürlich ist Dr. Even als der Leiter der entsprechenden Abteilung für mich ein Ansprechpartner gewesen, und aufseiten des Bundesnachrichtendienstes war es dann der jeweils verantwortliche Abteilungsleiter, zu dem Zeitpunkt Herr Pauland.

Martina Renner (DIE LINKE): Pauland?

Zeuge Andreas Könen: Pauland.

Martina Renner (DIE LINKE): Pauland. - Und darüber gibt es auch Unterlagen, oder waren das in der Regel mündliche - -

Zeuge Andreas Könen: Das waren in der Regel mündliche Gespräche als TOP im Rahmen üblicher Jours fixes, also regelmäßiger Austausche.

Martina Renner (DIE LINKE): Gab es dann auch nach 2013 Besuche beim BND, also jenseits von Fragen Zertifizierung -

Zeuge Andreas Könen: Ja, mhm.

Martina Renner (DIE LINKE): - oder Zulassung, um sich bestimmte Dinge zeigen und erklären zu lassen?

Zeuge Andreas Könen: In welchem Zusammenhang jetzt?

Martina Renner (DIE LINKE): Snowden-Dokumente.

Zeuge Andreas Könen: Snowden-Dokumente. - Nein, nicht dass es mir bewusst wäre, dass also aus Anlass von Snowden-Dokumenten und dem, was da offensichtlich geworden ist, spezifische Besuche stattgefunden hätten. Es gibt die regelmäßige Zusammenarbeit mit dem BND auch aus dem Cyber-Abwehrzentrum heraus, in dann bilateraler Fortsetzung. Aber dass es jetzt im Rahmen der Snowden-Dokumente erfolgt sei, ist mir nicht bewusst. Nein.

Martina Renner (DIE LINKE): Ich habe noch eine Frage, weil wir ja kurz - ich war es nicht - - ein anderer Kollege vorhin, ich glaube, sogar der Herr Schipanski, Sie gefragt hat zu den Möglichkeiten der Geolokalisation via verschiedener Methoden, -

Zeuge Andreas Könen: Mhm.

Martina Renner (DIE LINKE): - Triangulation und Ähnliches. Was weiß denn das BSI zur Ortung von Personen via mobiler IMSI-Catcher zum Beispiel an Drohnen?

Zeuge Andreas Könen: Zum Beispiel?

Martina Renner (DIE LINKE): An Drohnen, IMSI-Catcher - -

Zeuge Andreas Könen: Also, zu Letzterem, an Drohnen: -

Martina Renner (DIE LINKE): Gar nicht?

Zeuge Andreas Könen: - keine Erkenntnisse. Natürlich, wenn Sie einen IMSI-Catcher nutzen, sind Sie unmittelbar in der Zelle, in der sich derjenige, dessen Mobiltelefon Sie einfangen, auch bewegt. Und in dem Moment, wenn er dann entsprechend über den IMSI-Catcher kommuniziert, haben Sie natürlich die gesamten GSM-Daten oder sogar Applikationsdaten zur Verfügung.

Martina Renner (DIE LINKE): Ist das BSI in dem Zeitraum, den Sie überblicken oder zu dem Sie Aussagen machen können, mal von irgendeiner anderen Behörde oder einer Ministeriumsstelle dahin gehend befragt worden, wie Geolokalisation von Drohnen stattfindet, funktioniert?

Zeuge Andreas Könen: Von Drohnen: Nein, -

Martina Renner (DIE LINKE): Nie?

Zeuge Andreas Könen: - kenne ich keinen Vorgang zu.

Martina Renner (DIE LINKE): Also, da hat Sie weder mal der BND, das BfV, das Auswärtige Amt -

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): - das BMI -

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): - oder sonst irgendjemand - -

Zeuge Andreas Könen: Nein.

Martina Renner (DIE LINKE): Und hätten Sie dazu was sagen können?

Zeuge Andreas Könen: Also, wie ich sagte: In der spezifischen Anbindung an die Drohnenthematik nicht. Zur technischen grundsätzlichen Frage von Lokalisierbarkeit, wie ich es auch eben dargestellt hatte, ausgehend etwa von dieser Studie, hätten wir uns natürlich äußern können.

Martina Renner (DIE LINKE): Okay. Gut. Ich habe jetzt erst mal auch keine Fragen mehr. Danke, Herr Könen.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. Dann kommen wir jetzt zur Fraktion der SPD. - Hier waren keine Fragen mehr; so habe ich es wahrgenommen. - Dann sind wir bei Bündnis 90/Die Grünen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Dazu wollte ich auch eine Frage stellen, was die Kollegin zuletzt gefragt hat. Sie haben ja vorhin mal erwähnt, dass Sie hier genau verfolgen, was wir hier so treiben, also was hier im Untersuchungsausschuss diskutiert wird, was die Zeugen sagen, was davon in der Zeitung steht, sage ich mal. Haben Sie denn nicht mitbekommen, dass wir hier einen ehemaligen Drohnenpiloten lange befragt haben und dass der erklärt hat, wie das geht, also dass man das auf der Grundlage von Telefonnummern mit so einem IMSI-Catcher, der an der Drohne selber ist und dann die Daten nach USA zurückgibt - - und dann werden die genutzt, um dann die Zielerkennung einzuleiten.

Zeuge Andreas Könen: Also, ich habe einiges zum Untersuchungsausschuss gelesen in der Presse, klar, aber zu dieser speziellen Thematik tatsächlich nicht.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ist das Ihnen möglich, so was - - dieser Frage mal nachzugehen? Also, das ist hier so gesagt worden, und wir sind jetzt dabei, das zu verifizieren.

Zeuge Andreas Könen: Also, die grundsätzlichen technischen - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Aber Sie haben ja vorhin gesagt, allein die Telefonnummer würde ja schon ausreichen - oder die Handydaten, sagen wir mal so.

Zeuge Andreas Könen: Also, die präzise Aussage, was wann ausreicht, um zu lokalisieren, hatte ich ja in den Zusammenhang gestellt, was zu welchem Zeitpunkt jeweils möglich war. Natürlich können wir uns zur Technik von IMSI-Catchern äußern und dazu, was an Lokalisierungsdaten über solch ein Gerät dann abgeleitet werden kann. Wie das im Zusammenhang etwa dann mit diesem spezifischen fliegenden Gerät steht und den dann eventuell noch nötigen sonstigen Maßnahmen - - ist das eher schwierig, da das nicht zu unseren Anwendungszenarien gehört.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Also, wenn Sie so ein Ding sehen würden, könnten Sie sagen, es funktioniert, oder nicht?

Zeuge Andreas Könen: Das weiß ich nicht; das müsste ich den Kollegen überlassen, die da fachlich versiert sind.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. - Eine letzte Frage: Sie haben hier geschildert, dass Sie von „Eikonal“ bzw. „Granat“ gehört haben, und Sie haben ja danach auch wiederum mitbekommen, dass uns das sehr intensiv hier beschäftigt hat, lange Artikel in der *Süddeutschen Zeitung* und so. Haben Sie das zum Anlass genommen, Sie oder Ihr Amt, mal der Frage nachzugehen: „Wie wird eigentlich oder wie wurde und vielleicht wie wurde auch danach in Frankfurt an dem Knoten, an dem Kabel ausgeleitet? Wie wird das gemacht? Wie wurde das gemacht, und wie sicher ist das?“, weil Sie ja für die Überprüfung durchaus zuständig sind solcher

Ausleitungsgeschichten, wenn ich das richtig sehe.

Zeuge Andreas Könen: Also, wir sind diesem Fall nicht nachgegangen, und die Zuständigkeit in der Prüfung solchen Equipments nach TKÜV § 27 bezieht sich ja auf eine Vorabprüfung.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Aha. - Da können Sie auch nicht sagen, ob - also 2008 irgendwann soll das beendet worden sein - das danach noch weiterläuft in der Auswertung.

Zeuge Andreas Könen: Nein, da wir im praktischen Einsatz der entsprechenden Ausleitungsgerätschaften nicht involviert sind, können wir dazu auch keine Aussagen treffen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. Haben Sie auch nicht versucht, -

Zeuge Andreas Könen: Nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): - zu prüfen, also: Wie geht das? Wie sicher ist das, und können da andere mitlesen oder -hören oder Daten aufnehmen?

Zeuge Andreas Könen: Also, abgesehen davon, dass es nicht zu unserem Auftrag gehört, ist es nicht beauftragt worden und ist auch mit den Schwierigkeiten des Zugangs in dem Moment versehen, der ja nach TKÜV eben dem BSI auch gar nicht zu gewähren wäre.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. Gut. Danke.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich nutze den Rest gerne. - Noch mal ganz kurz zu XKeyscore. Wird das nach Ihrer Kenntnis heute noch eingesetzt von deutschen Behörden?

Zeuge Andreas Könen: Nein, nach meiner Erkenntnis - - „Noch eingesetzt“? Ich kann weder zum vergangenen Einsatz noch zum jetzigen - -

Vorsitzender Dr. Patrick Sensburg: Da meldet sich Herr Akmann, weil es wahrscheinlich nicht mehr Untersuchungszeitraum ist, was heute eingesetzt wird, richtig?

MR Torsten Akmann (BMI): Ja, das ist nicht im Untersuchungszeitraum.

Vorsitzender Dr. Patrick Sensburg: Dem würde ich zustimmen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, das interessiert mich völlig unabhängig, als Parlamentarier, von diesem Untersuchungsausschuss, ob eben die Software, die Herr Könen so angestrengt prüft mit seinem Haus jetzt seit vielen, vielen Monaten, weil es wahrscheinlich eine Trojanersoftware ist, beim Bundesnachrichtendienst weiter eingesetzt wird. Vielleicht kann das Bundeskanzleramt uns da kurz alle entwarnen, oder? - Nein. Na, gut. Das habe ich mir gedacht.

(Christian Flisek (SPD): Wollen Sie nicht!)

- Nein, es bleibt offen, es bleibt offen. Herr Könen prüft noch; es liegt außerhalb des Untersuchungszeitraums.

RD Philipp Wolff (BK): Sie haben es ja selber schon gesagt. Wenn Sie es allgemein als Parlamentarier interessiert, dann steht es Ihnen natürlich völlig frei, eine entsprechende Frage zu stellen, aber nicht im Rahmen des UA.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Werde ich tun, versprochen! Die Antworten kann ich mir ungefähr vorstellen, und in der Vergangenheit waren sie ab und zu auch nicht das Papier wert, auf dem sie dann in der Geheimschutzstelle lagen, wenn ich das mal so sagen darf.

Vorsitzender Dr. Patrick Sensburg: Sehr despektierliche Sichtweise auf die Bundesregierung. So gehen wir hier gar nicht miteinander um.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich glaube, das kann man in der Rückschau mit einigem Recht einfach mal sagen.

Vorsitzender Dr. Patrick Sensburg: Ich verwahre mich immer gegen Kritik gegenüber diesem Ausschuss. Deswegen kann ich es natürlich umgekehrt auch nicht gut finden, wenn man so miteinander umgeht.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Natürlich kannst du das, du bist eben Parlamentarier.

Vorsitzender Dr. Patrick Sensburg: Nein, das eine ist mir wichtig, weil ich hier der Vorsitzende bin. Aber trotzdem freue ich mich natürlich, wenn wir so nicht miteinander umgehen, dass wir nicht sagen, das, was der andere macht, ist das Papier nicht wert, auf dem es steht.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich habe gesagt, es gab Fälle, bei denen war das so; da standen einfach falsche Sachen. Aber ich werde das gerne noch mal nachfragen.

So. Ich wollte noch mal bezüglich der Erkenntnislage des BSI im Hinblick auf die Belgacom nachforschen. Jetzt ist es ja so: Sie haben gesagt, man könnte das nicht zuordnen und mit Sicherheit nicht sagen, wo es herkommt. Vorhin haben Sie ja gesagt, dass diese Snowden-Dokumente schon authentisch sind, wenn ich Sie richtig verstanden habe am Anfang.

Zeuge Andreas Könen: Soweit es die technischen Aussagen betrifft, ist es weitgehend plausibel -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Genau.

Zeuge Andreas Könen: - und wohl auch authentisch.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Genau. - Jetzt gibt es hier eine von *The Intercept* veröffentlichte Folie, 13.12.2014, da haben die das veröffentlicht. Es geht um die Operation „Belgacom“, Operation „Socialist“. Da steht ganz klar ein GCHQ-Bezug drauf. Vielleicht können Sie da einmal draufgucken und das bestätigen. Das sind ja Original-GCHQ-Unterlagen, und so haben Sie die ja bestimmt auch angeguckt.

(Dem Zeugen werden Unterlagen vorgelegt)

So, und jetzt noch mal die Frage vor dem doch sehr, sehr nahe liegenden Verdacht, dass der GCHQ hier bei dieser Operation „Belgacom“ mit Regin infiltriert hat, um EU-Kommunikation, Verhandlungen, auch aus dem Bundeskanzleramt abzuhören und mitzuschneiden - darüber reden wir ja; deswegen war Ihre Behörde auch so tief involviert in diese Fragen, weil das sind ja relevante Vorgänge -: Hat es Diskussionen darüber gegeben, ob diese gemeinsamen Treffen, diese Kooperations- und Absprachedinge, die man auch mit dem GCHQ beim BSI hatte, ob die noch Sinn machen, ob das Vertrauensverhältnis noch gegeben ist, ob das so eigentlich alles okay ist?

Zeuge Andreas Könen: Diese Diskussionen hat es geben, natürlich.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und mit welchem Ausgang?

Zeuge Andreas Könen: Mit dem klaren Ausgang, dass wir den Verpflichtungen, den wir im EU- und NATO-Rahmen nachkommen müssen, auch nachkommen, dass wir aber sonstige Kontakte auf ein Minimum beschränken.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Glauben Sie, dass Großbritannien ähnlich reagiert hätte im umgekehrten Fall?

Zeuge Andreas Könen: Das kann ich nicht beurteilen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, das stimmt wahrscheinlich.

Zeuge Andreas Könen: Das ist sehr schwer zu sagen, wie die Behörden - -

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Hat man darüber mal mit dem GCHQ gesprochen? Hat man das mal thematisiert und gesagt: „Leute, wir haben diese Folien hier, ich bin etwas enttäuscht heute Morgen“, oder?

Zeuge Andreas Könen: Also, das hat man gemacht, ganz klar. Aber ich glaube, einer der anderen Zeugen hat es schon gesagt: Was einem entgegenkommt, ist weder Bestätigung noch sonstige Aussagen; es ist professionelles Verhalten der Kollegen. Und dann gehen Sie mit dem gleichen Unsicherheitsgrad nach Hause, mit dem Sie reingekommen sind.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich verstehe.

Vorsitzender Dr. Patrick Sensburg: Okay. Jetzt gucke ich mal in die Reihen der Fraktionen. - Ich sehe hier keine Fragen mehr, die in öffentlicher Sitzung beantwortet werden können. Ich habe aber festgestellt, es sind doch einige in nichtöffentlicher oder eingestufter Sitzung. Wir müssen daher folgenden Beschluss fassen - ich schlage daher folgenden Beschlussvorschlag vor -:

Für die weitere Vernehmung des Zeugen Herrn Könen am heutigen Tag wird die Öffentlichkeit gemäß § 14 Absatz 1 Nummer 4 des Untersuchungsausschussgesetzes ausgeschlossen, weil besondere Gründe des Wohls des Bundes entgegenstehen.

Wer dem so zustimmen kann, bitte ich um das Handzeichen. - Herzlichen Dank. Gegenstimmen? - Enthaltungen? - Damit ist dies so einstimmig beschlossen.

Herr Könen, ganz herzlichen Dank. So schlagartig geht das. Dann sind wir am Ende der öffentlichen Vernehmung. Wir würden jetzt die anderen Zeugen hören und kommen dann in die nichtöffentliche Vernehmung. Das kann ein bisschen dauern. Aber wir würden das gerne heute noch mit Ihnen machen, weil ich habe schon wahrgenommen, es gibt Fragen. Richtig oder nicht? - Ich frage mal in die Runde. Opposition?

(Martina Renner (DIE LINKE): Ja!)

- Okay. Danke. Gut. Eine Fraktion reicht ja. Also, es gibt Fragen im nichtöffentlichen Teil. Von daher bitte ich Sie, sich bereitzuhalten. Wir müssen gucken, wann wir da sind. Es kommen ja auch gleich noch einige namentliche Abstimmungen. Ganz herzlichen Dank insoweit, Herr Könen.

So, ich bitte, jetzt den nächsten Zeugen in den Sitzungssaal zu geleiten. Das ist der Zeuge Schallbruch. Ich denke, das wird so knapp fünf Minuten dauern. Fünf Minuten unterbrechen wir jetzt die Sitzung. Dann kann jeder mal so ein bisschen sich ausschütteln auf den Sitzen, ein Getränk holen, und dann machen wir in fünf bis zehn Minuten weiter.

Die Sitzung ist unterbrochen.

(Unterbrechung von 15.39 bis 15.52 Uhr)

Vorsitzender Dr. Patrick Sensburg: Die unterbrochene Sitzung des 1. Untersuchungsausschusses wird fortgesetzt, und ich darf unseren nächsten Zeugen begrüßen.

Vernehmung des Zeugen Martin Schallbruch

Herr Schallbruch, ich freue mich, dass Sie da sind und dem Ausschuss für viele Fragen sicherlich Rede und Antwort stehen.

Ich stelle fest: Der Zeuge ist ordnungsgemäß geladen. Herr Schallbruch, Sie haben den Erhalt der Ladung am 14. Juni 2016 bestätigt.

Ich habe Sie darauf hinzuweisen, dass die Bundestagsverwaltung eine Tonbandaufnahme der Sitzung fertigt. Diese dient ausschließlich dem Zweck, die stenografische Aufzeichnung der Sitzung zu erleichtern. Die Tonbandaufnahme wird nach Erstellung des Protokolls dann auch gelöscht, und Sie haben 14 Tage Zeit, dann Ergänzungen oder Korrekturen an dem Protokoll vorzunehmen, wenn dies nötig sein sollte. - Haben Sie hierzu Fragen?

Zeuge Martin Schallbruch: Nein, Herr Vorsitzender.

Vorsitzender Dr. Patrick Sensburg: Danke schön. - Herr Schallbruch, vor Ihrer Anhörung habe ich Sie zunächst zu belehren.

Sie sind als Zeuge geladen worden. Als Zeuge sind Sie verpflichtet, die Wahrheit zu sagen. Ihre Aussagen müssen richtig und vollständig sein. Sie dürfen nichts weglassen, was zur Sache gehört, und nichts hinzufügen, was der Wahrheit widerspricht.

Ich habe Sie außerdem auf die möglichen strafrechtlichen Folgen eines Verstoßes gegen die Wahrheitspflicht hinzuweisen. Wer vor dem Untersuchungsausschuss uneidlich falsch aussagt, kann gemäß § 162 in Verbindung mit § 153 des Strafgesetzbuches mit Freiheitsstrafen von drei Monaten bis zu fünf Jahren oder mit Geldstrafe bestraft werden.

Nach § 22 Absatz 2 des Untersuchungsausschussgesetzes können Sie die Auskunft auf solche Fragen verweigern, deren Beantwortung Sie selbst oder Angehörige im Sinne des § 52 Absatz 1 der Strafprozessordnung der Gefahr aussetzen würde, einer Untersuchung nach einem gesetzlich geordneten Verfahren ausgesetzt zu werden. Dies betrifft neben Verfahren wegen einer Straftat oder Ordnungswidrigkeit auch gegebenenfalls Disziplinarverfahren, wenn dies in Betracht kommen sollte.

Sollten Teile Ihrer Aussage aus Gründen des Schutzes von Dienst-, Privat- oder Geschäftsgeheimnissen nur in einer nichtöffentlichen oder eingestuften Sitzung möglich sein, bitte ich Sie um einen Hinweis, damit der Ausschuss dann gegebenenfalls einen Beschluss nach § 14 oder § 15 des Untersuchungsausschussgesetzes fassen kann, also die Sitzung in nichtöffentlicher oder eingestufter Weise fortsetzen kann, sodass man Ihnen dann die entsprechenden Fragen stellen kann und Sie auch dann antworten können. - Haben Sie hierzu Fragen?

Zeuge Martin Schallbruch: Nein, keine Fragen.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Nach diesen notwendigen Vorbemerkungen darf ich Ihnen den geplanten Ablauf noch einmal kurz darstellen. Eingangs habe ich Sie zur Person zu befragen. Zu Beginn der Vernehmung zur Sache haben Sie gemäß § 24 Absatz 4 des Untersuchungsausschussgesetzes die Gelegenheit, zum Beweisthema im Zusammenhang vorzutragen, also ein sogenanntes Eingangsstatement abzugeben. Danach werde ich Ihnen Fragen stellen. Danach erhalten die Fraktionen die Möglichkeit, ihre Fragen zu stellen, immer eine Fraktion nach der anderen mit ihren Mitgliedern.

Wenn keine weiteren Fragen mehr sind, darf ich Sie nun bitten, sich zu Beginn der Ausführungen dem Ausschuss einmal mit Namen, Alter, Beruf und einer ladungsfähigen Anschrift vorzustellen.

Zeuge Martin Schallbruch: Mein Name ist Martin Schallbruch. Ich bin geboren am [redacted] 1965 und bin Wissenschaftler und stellvertretender Direktor eines Forschungsinstituts hier in Berlin.

Als ladungsfähige Anschrift können Sie das Bundesministerium des Innern, Alt-Moabit 140 in 10557 Berlin, verwenden.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich frage nur einmal ergänzend - „Wissenschaftler“: Welche Wissenschaft? Weil das ein weites Feld ist.

Zeuge Martin Schallbruch: Ich bin Informatiker, und mein wissenschaftliches Feld ist auf der Schnittstelle von Informationstechnik und Recht.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich hatte es eben gesagt: Wenn Sie dies möchten, hätten Sie zu Anfang die Gelegenheit zu einem sogenannten Eingangsstatement, also im Zusammenhang zum Beweisgegenstand Ausführungen zu machen, ohne dann eben von den Ausschussmitgliedern unterbrochen zu werden. - Wünschen Sie das?

Zeuge Martin Schallbruch: Ja, davon würde ich gerne Gebrauch machen, Herr Vorsitzender.

Vorsitzender Dr. Patrick Sensburg: Dann haben Sie jetzt das Wort.

Zeuge Martin Schallbruch: Ja, vielen Dank. - Herr Vorsitzender! Sehr geehrte Damen und Herren Abgeordnete! Ich habe in dem Untersuchungszeitraum zwischen Februar 2002 und dem Ende des Untersuchungszeitraums im Bundesministerium des Innern die Aufgabe eines IT-Direktors wahrgenommen und einen Stab geleitet, der im Jahre 2008 zu einer Abteilung umgewandelt wurde. Meine Zuständigkeit erstreckte sich auf Fragen der Netzpolitik, der Digitalisierungspolitik, des IT-Einsatzes in der öffentlichen Verwaltung, der IT- und der Cybersicherheit. Bei der IT- und Cybersicherheit kam mir die Rolle der Fachaufsicht über das Bundesamt für Sicherheit in der Informationstechnik zu.

Sie haben mich geladen zum gesamten Untersuchungsgegenstand. Der Untersuchungsauftrag enthält unter anderem die Fragestellung, sehr allgemein zu Strategien und Konzepten zur IT-Sicherheit, speziell gegen Datenabfluss, Stellung zu nehmen, mit dem Schwerpunkt auch auf dem IT-System des Bundes. Deshalb würde ich gerne in meiner Einführungsbemerkung zur IT-Sicherheit und den Maßnahmen, die in diesem Bereich im Untersuchungszeitraum ergriffen worden sind, Stellung nehmen.

Vielleicht eine Vorbemerkung zu der Materie der IT-Sicherheit, wie sie sich in dem gesamten Zeitraum entwickelt hat: Wir haben in diesem Zeitraum eine sehr hochkomplexe, an Komplexität Jahr für Jahr zunehmende Problematik der IT-Sicherheit erlebt. Das kam daher, dass zum einen die Informationstechnik sich weiter ausdifferenziert hat, komplexer ausgestaltet hat: Mobilisierung, Virtualisierung, Produktvielfalt, Vernetzung. Es kommt daher, dass die Qualität der Informationstechnik sich über die letzten 10, 15 Jahre nicht wirklich gebessert hat, also die Qualität der Software- und Hardwareprodukte, dass die Abhängigkeit von Staat, Gesellschaft, Wirtschaft von Informationstechnik im gleichen Zeitraum immens zugenommen hat, dass sich eine komplexe Bedrohungslage entwickelt hat, in der viele Player aus dem Bereich der Kriminalität - Konkurrenzausspähung usw. usf. -, auch nachrichtendienstliche Akteure, militärische Akteure das Thema IT- und Cyberangriffe für sich entdeckt haben.

Die Verantwortung für IT-Sicherheit kann kein Akteur allein herstellen, weder Hersteller von Systemen noch Nutzer noch der Staat. Die Lösung der Probleme der IT-Sicherheit erfordert immer ein Zusammenwirken unterschiedlichster Akteure. Und eines der großen Probleme bei der IT-Sicherheit, mit dem ich im gesamten Zeitraum befasst war, war das Verhältnis zwischen IT-Sicherheit auf der einen und Nutzbarkeit und Innovation auf der anderen Seite. IT-Sicherheit behindert immer ein Stück weit die Nutzbarkeit von Systemen, verlangsamt Innovationen. Ein Smartphone, was[2] sicher ist, alles kryptiert - das Gerät kryptiert die Verbindungen, kryptiert die Mails -,

2) Richtigstellung des Zeugen: "[das]", siehe Anlage 2.

ist nicht so einfach zu benutzen, nicht so sehr „at a fingertip“, wie das viele Nutzer gewohnt sind.

Hinzu kommt, dass die IT-Sicherheit ein Stück weit immer der Geschwindigkeit der IT-Innovationen hinterherläuft, weil viele Hersteller und Anwender IT-Sicherheit nicht von Anfang an in die Systeme hineinplanen, sondern IT-Sicherheit zusätzlich hinzugekauft werden muss.

Ich würde gerne speziell zur IT-Sicherheit der Bundesverwaltung ein paar Aussagen machen. Die Behörden des Bundes sind in großem Umfang abhängig von der Funktionsfähigkeit ihrer Informationstechnik. Kaum eine Behörde kann ohne funktionierende Informationstechnik ihre Aufgabe noch wirklich wahrnehmen. Seit etwa dem Jahr 2004 haben wir in der Bundesverwaltung eine stetige Zunahme an Zahl und Art und Komplexität von Angriffen auf die IT-Systeme erlebt: Spam-Angriffe, Denial-of-Service-Attacks, Trojaner, Hackerangriffe usw. usf. Oftmals war und ist auch aus heutiger Sicht nicht ganz erkennbar, wer Ursprung oder Urheber dieser Angriffe war.

In dem Zusammenhang kann ich auch gleich an dieser Stelle sagen, dass mir, was die IT der Bundesverwaltung angeht, kein Fall bekannt geworden ist, der sich eindeutig auf beispielsweise Nachrichtendienste aus den hier in Rede stehenden Five-Eyes-Staaten zurückführen ließe. Die Bundesverwaltung mit ihrer IT bietet zunehmende Angriffsflächen, weil sie mehr IT einsetzt - mobile Geräte, Cloud-Services usw. usf. - und weil der Einsatz der IT immer komplizierter wird.

Für die Sicherheit der IT im Bund wie auch für die IT insgesamt sind grundsätzlich die Ressorts selbst verantwortlich. Das BMI hat für die IT der Bundesverwaltung eine koordinierende Rolle. Das Ergebnis dieser Eigenverantwortung der Ressorts ist eine weit zersplitterte IT-Landschaft des Bundes. 2013 gab es hierzu eine Erhebung: 119 Rechenzentren, über 1 200 Serverräume, 40 unterschiedliche Netze. Im Hinblick auf die IT-Sicherheit führt das zu unterschiedlichen IT-Sicherheitsvorkehrungen in den einzelnen Behörden, die nur dort einheitlich sind, wo sie typischerweise einheitlich finanziert sind, zum Beispiel - prominentestes Beispiel vielleicht - bei den Regierungsnetzen, IVBB und anderen Regierungsnetzen, die ressortübergreifend vom BMI bereitgestellt werden.

Es hat im gesamten Untersuchungszeitraum einen immerwährenden Druck des BMI auf die Bundesministerien gegeben, mehr für die Sicherheit in ihren Behörden zu tun auf allen Ebenen. Es gab zu diesem Thema Kabinettsbefassungen, Staatssekretärsbesprechungen, diverse Sensibilisierungsveranstaltungen, Präsentationen in Staatssekretärsrunden, und in praktisch jeder Sitzung des Rats der IT-Beauftragten der Bundesministerien wurden Fragen der IT-Sicherheit seit Anfang 2008 adressiert.

Lassen Sie mich nun die wesentlichen Maßnahmen im Untersuchungszeitraum zur IT-Sicherheit aufzählen. Ich möchte fünf Maßnahmenbereiche nennen:

Erstens. Auf der politisch-strategischen Ebene hat die Bundesregierung im Jahre 2005 mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen eine erste IT-Sicherheitsstrategie vorgelegt, die die Bundesverwaltung betraf, aber darüber hinaus auch Fragen der Internetsicherheit, Erweiterung der Aufgaben des BSI, Technologiepolitik. Dieser nationale Plan war auch Beginn einer engeren Zusammenarbeit mit Unternehmen im Bereich der kritischen Infrastruktur. 2009 wurde das BSI-Gesetz novelliert, und das BSI erhielt zusätzliche Befugnisse für die Kontrolle der Sicherheit der IT des Bundes, aber auch zusätzliche Aufgaben im Bereich der Unterstützung von Unternehmen und Warnung der Bürger.

Im Jahre 2011 wurde die bis heute gültige Cyber-Sicherheitsstrategie des Bundes beschlossen, die ressortübergreifend zustande gekommen ist und als wesentliches Umsetzungsgremium einen Cyber-Sicherheitsrat eingerichtet hat, den es seit 2011 gibt, in dem diese Fragen ressortübergreifend auf Staatssekretärsebene und auch mit der Wirtschaft diskutiert werden. Die Cyber-Sicherheitsstrategie 2011 hat einen sehr starken Fokus

auf die Sicherheit der kritischen Infrastrukturen gelegt.

Zweiter Maßnahmenbereich: die Sicherheit der IT des Bundes. Vor 2007/2008 gab es keine ressortübergreifenden Vorgaben für die IT-Sicherheit der Bundesbehörden, nur Empfehlungen von BSI und BMI. Im Jahre 2007 hat das Bundeskabinett den sogenannten Umsetzungsplan Bund beschlossen, eine erste verbindliche IT-Sicherheitsleitlinie für alle Bundesbehörden. Damit wurden in jeder Behörde ein IT-Sicherheitsmanagement eingerichtet, Sicherheitsbeauftragte benannt, Sicherheitskonzepte erstellt. Seitdem müssen Vorfälle gemeldet werden an das BSI, und es werden jährliche Ampelberichte erstellt.

Mit dem Umbau der IT-Steuerung des Bundes, der Einrichtung eines IT-Rats des Bundes und der Einrichtung eines Beauftragten für Informationstechnik im BMI wurde ab 2008 dann die Möglichkeit geschaffen, dass auf ressortübergreifender Ebene auch Beschlüsse gefasst werden zur IT-Sicherheit im IT-Rat. Und es gab da, wie ich eben schon erwähnt habe, in den zweimonatlichen Sitzungen praktisch jede Sitzung die Thematisierung von Sicherheitsthemen. Es gab auch zu verschiedenen Sicherheitsvorfällen Sondersitzungen.

Ein Kernthema der IT-Sicherheit des Bundes war im gesamten Zeitraum die Sicherheit der Regierungsnetze. Die zentrale Infrastruktur IVBB für die Bundesregierung wurde permanent erweitert und gehärtet. Immer dann, wenn praktisch neue technische Angriffsformen bekannt wurden, wurde der IVBB vom BSI entsprechend geprüft, und wir haben dann sehr häufig als BMI eine Nachbeauftragung gemacht, um zusätzliche Sicherheitsmaßnahmen zu ergreifen. Seit 2009 hat das BSI auf Basis des novellierten Gesetzes dann automatische Schadsoftware-Erkennungssysteme installiert, die auch Datenabflüsse unter anderem verhindern.

Auch dank des Drucks des Haushaltsausschusses des Deutschen Bundestages gibt es seit 2011 eine Konsolidierung der Netze in eine gemeinsame Netzplattform, sodass alle Bundesbehörden - nicht nur die an den IVBB angeschlossenen Bundesbehörden - auf das gleiche hohe Sicherheitsniveau gezogen[3] werden sollen.

Ein weiterer Bereich, den ich, was die Sicherheit der IT des Bundes angeht, erwähnen will, ist die mobile Kommunikation. Spätestens um 2004/05 herum, als die ersten Smartphones in den Einsatz kamen - die ersten Geräte waren Blackberrys, die im Business-Bereich Verbreitung fanden -, gab es eine Beschäftigung des BSI und anderer Sicherheitsbehörden mit Fragen der Sicherheit von mobilen Geräten. Es gab seit 2005 Warnungen an die Bundesressorts, mobile Geräte nicht oder nur eingeschränkt einzusetzen, und wir haben im Hinblick auf die Bedenken, die wir aus technischer Sicht gegen die Architektur der Kommunikation der Geräte hatten, 2007 begonnen, ein sicheres Smartphone zu entwickeln, was[4] der Bundesregierung und auch dem Deutschen Bundestag im Übrigen zur Verfügung gestellt werden sollte. Es gab ab 2007 Pilotprojekte, und zwischen 2009 und 2011 wurden 10 000 Geräte - Smartphones und Kryptotelefone - für den Bund aus zentralen Mitteln beschafft.

Der dritte Maßnahmenbereich, den ich erwähnen möchte, ist die IT-Sicherheit in Wirtschaft und Gesellschaft. Die zunehmenden Angriffe betrafen naturgemäß nicht nur die Verwaltung, sondern, wie Sie den Lageberichten des BSI jährlich entnehmen können, auch Unternehmen und jeden Einzelnen; ich sage nur: Phishing-Attacken. Das BMI hat darauf reagiert durch einen Ausbau vor allen Dingen der BSI-Angebote im Bereich der Beratung, Zertifizierung, Prüfung, Warnung, die Einrichtung eines Bürger-CERTs, aber auch durch eine intensivere Kooperation mit Wirtschaftsunternehmen bei der IT-Sicherheit.

Beginnend mit dem IT-Gipfel, den die Bundeskanzlerin 2006 eingerichtet hat, gab es eine ganze Reihe von solchen Initiativen. Ich möchte nur nennen die Gründung des Vereins „Deutschland

3) Richtigstellung des Zeugen: "[gebracht]", siehe Anlage 2.

4) Richtigstellung des Zeugen: "[das]", siehe Anlage 2.

sicher im Netz“, mit dessen Hilfe sehr viele Weiterbildungsangebote in Schulen, für den Mittelstand, für bestimmte Gruppen bereitgestellt wurden, Fernsehspots und Ähnliches oder das Anti-Botnet-Beratungszentrum - was auch[5] eine Initiative der Wirtschaft ist[6], mit Unterstützung des Bundes -, was[7] Betroffenen Hilfe gibt, wenn sie in ein Botnetz geraten.

Oder ich will erwähnen - das hat möglicherweise auch Herr Könen bereits erwähnt - die Allianz für Cyber-Sicherheit, die das BSI gemeinsam mit BDI und BITKOM gegründet hat, die dem Wissenstransfer, dem Know-how-Austausch über IT-Sicherheit und „Wie kann man Sicherheitsvorfällen begegnen?“ dient.

Ein wesentlicher Bereich, was die IT-Sicherheit in Wirtschaft und Gesellschaft angeht, waren seit jeher die kritischen Infrastrukturen. Seit 2007 gibt es eine institutionalisierte Zusammenarbeit zwischen den Bundesministerien und den kritischen Infrastrukturen im sogenannten Umsetzungsplan KRITIS, mit gemeinsamen Sicherheitsstandards, gemeinsamen Gremien und auch Informationsaustauschen. Das hat beispielsweise dazu geführt, dass auch Unternehmen aus den KRITIS-Branchen an der ersten cyberbezogenen Krisenübung 2011 teilnahmen. Und seit 2012 ist durch weitergehende Assessments, die wir durchgeführt haben im Bereich der kritischen Infrastrukturen, die Vorbereitung getroffen worden für den Entwurf eines IT-Sicherheitsgesetzes, der 2013 dann[8] in das parlamentarische Verfahren ging, wegen der Diskontinuität aber dann ja[9] erst diese Wahlperiode abgeschlossen werden konnte.

Der vierte Maßnahmenbereich, den ich erwähnen möchte, ist der Ausbau der behördlichen Strukturen zur IT-Sicherheit. Das BSI - ich hatte es schon erwähnt - ist in den letzten 15 Jahren ganz erheblich ausgebaut worden: von 250, 300 Mitarbeitern 2002 auf 570, 600 etwa zum Ende des Untersuchungszeitraums. Gleichzeitig hat das BSI die Breite seiner Beschäftigung mit der Thematik erheblich erhöht, was die Techniken angeht, aber auch, was die Anwendungsbereiche angeht, wenn Sie an die Sicherheit von Energienetzen denken, an die Sicherheit im Gesundheitswesen, die Gesundheitstelematik. Das sind alles Themen, die das BSI zusätzlich aufgenommen hat.

Auf deutschen Vorschlag wurde 2002/2003 in Europa eine vergleichbare europäische Einrichtung gegründet, die ENISA. Seit 2009 gibt es ja[10] auch einen deutschen Direktor der ENISA. Die ENISA hat sich sehr intensiv darum bemüht, die Sicherheitsniveaus der EU-Mitgliedstaaten anzugleichen und zum Beispiel CERT-Informationen auszutauschen.

Mit der Cyber-Sicherheitsstrategie 2011 hat sich der Bund dann entschieden, unter Federführung des BSI ein Cyber-Abwehrzentrum einzurichten, in dem alle mit Cyberfragen beschäftigten Sicherheitsbehörden zusammenwirken, um gemeinsame Lagebeurteilungen vorzunehmen und sich über zu treffende Maßnahmen im Rahmen der jeweiligen Zuständigkeiten abzustimmen.

Der fünfte und letzte Maßnahmenbereich, den ich erwähnen möchte, ist die Förderung vertrauenswürdiger Informationstechnik, die Förderung von IT-Sicherheitstechnik. Das ist aus meiner Sicht eine zentrale Fragestellung für präventive IT-Sicherheit. Wir haben in Deutschland eine sehr leistungsstarke, aber eher klein- und mittelständisch geprägte IT-Sicherheitswirtschaft. Wir haben allerdings nur winzige Teile der im praktischen Einsatz befindlichen IT, die tatsächlich auch Sicherheitszertifikate hat, die tatsächlich belastbar geprüft ist. Wir haben eine hohe Abhängigkeit von ausländischen IT-Herstellern und naturgemäß immer die Möglichkeit, dass IT-Produkte, die man einkauft auf dem

5) Richtigstellung des Zeugen: "[streichen der Worte „was auch“]", siehe Anlage 2.
6) Richtigstellung des Zeugen: "[streichen des Wortes „ist“]", siehe Anlage 2.
7) Richtigstellung des Zeugen: "[statt was, das]", siehe Anlage 2.
8) Richtigstellung des Zeugen: "[streichen des Wortes „dann“]", siehe Anlage 2.
9) Richtigstellung des Zeugen: "[streichen der Worte „dann ja“]", siehe Anlage 2.
10) Richtigstellung des Zeugen: "[streichen des Wortes „ja“]", siehe Anlage 2.

Weltmarkt, Backdoors enthalten, Schwachstellen enthalten, von geringer Qualität sind.

Hinzu kommt, dass die Technologieentwicklung ganz allgemein im Augenblick sehr stark vom sogenannten Consumer-Markt getrieben ist, das heißt von der schnellen Weiterentwicklung von Geräten für den Endkunden und weniger von der Entwicklung von Technik für Sicherheitsbereiche. Aus diesen Gründen hat das BMI im gesamten Untersuchungszeitraum eine ganze Reihe von Maßnahmen zur Förderung vertrauenswürdiger Informationstechnik durchgeführt. Das BSI hat beispielsweise Entwicklungsprojekte für Kryptogeräte durchgeführt; einige hatte ich schon erwähnt. Wir haben eine intensivere Nachfragebündelung des Bundes und auch Sammelbeschaffung durch das BSI erreicht, sodass durch diese größere Nachfrage auch für die Unternehmen eine stabilere wirtschaftliche Situation erreicht werden kann. Die Unternehmen wurden bei Auslandsvertrieb unterstützt, beispielsweise bei Kryptogeräten in neuen EU-Mitgliedstaaten.

Wir haben uns darum bemüht, bei Vergaben im Bereich der Bundesverwaltung hohe Anforderungen an die IT-Sicherheit zu stellen - im Rahmen des, sage ich mal[11], europarechtlich Möglichen jeweils -, aber auch die vorhandenen Ausnahmegenehmigungen im europäischen Vergaberecht zu erhalten. Es gab in dem Untersuchungszeitraum mindestens zwei Bemühungen von europäischer Seite, die Ausnahmevorschriften für Sicherheitsvergaben enger zu fassen und uns hier weiter einzuschränken; dagegen haben wir uns regelmäßig auch erfolgreich gewehrt.

Im Rahmen der Novellierung des Außenwirtschaftsgesetzes hat das BMI sich dafür eingesetzt, dass auch Kryptounternehmen unter das Außenwirtschaftsgesetz fallen, und es gab mehrere Fälle, in denen die Übernahme von Unternehmensanteilen durch ausländische Erwerber durch das Bundeswirtschaftsministerium gemeinsam mit dem BMI untersagt oder nur unter Auflagen genehmigt wurde.

Wir haben Initiativen gefördert wie „E-Mail made in Germany“ für den sicheren, verschlüsselten E-Mail-Austausch zwischen deutschen Providern. Es gibt Sicherheitspartnerschaften mit einer ganzen Reihe von IT-Sicherheitsunternehmen, und das BMI hat gemeinsam mit dem BMBF zwei IT-Sicherheitsforschungsprogramme - 2008 und 2013, glaube ich - beschlossen und durchgeführt, mit denen zusätzliche IT-Sicherheitstechnik gefördert wurde.

Ich möchte im abschließenden Teil meiner Eingangsbemerkungen die zusätzlichen Maßnahmen darstellen, die wir nach Veröffentlichung der Snowden-Dokumente durchgeführt haben. Ich möchte persönlich vorwegschicken: Ich habe mir etliche von diesen Dokumenten angeguckt[12] - natürlich bei weitem nicht alle, sondern auch nur einen Teil - und habe mir auch Gedanken darüber gemacht und viel darüber gelesen. Mich haben bei diesen Dokumenten die Methodenvielfalt und der Umfang des Einsatzes der Techniken durchaus überrascht, sehr überrascht, auf der anderen Seite aber auch mich darin bestätigt, dass der Einsatz von Kryptotechnologie und vertrauenswürdiger IT ein Schlüssel für sichere und vertrauenswürdige Kommunikation ist, völlig egal, wer der jeweilige Angreifer auf diese Kommunikation ist.

Nach Bekanntwerden der Snowden-Veröffentlichungen haben wir in fünf Bereichen Aktivitäten in meinem Zuständigkeitsbereich entfaltet:

Das ist erstens im Bereich der Aufklärung, dort vor allen Dingen mit der Zielrichtung, die Provider, die vertraglich mit dem Bund gebunden sind, daraufhin zu überprüfen, inwieweit sie mit den Daten so umgehen und mit ihren Verpflichtungen so umgehen, wie es im Vertrag vorgesehen ist. Da wurden die Provider entsprechend angesprochen durch das BMI oder das BSI, je nachdem, wer den Vertrag geführt hat, und es wurden in einzelnen Fällen auch Revisionen durchgeführt. Wir haben durch diese Aufklärungsmaßnahmen keine Erkenntnisse gewinnen

11) Richtigstellung des Zeugen: "[streichen der Worte „sage ich mal“]", siehe Anlage 2.

12) Richtigstellung des Zeugen: "[angeschaut statt angeguckt]", siehe Anlage 2.

können, die belegen, dass es entsprechende Maßnahmen der Five-Eyes-Staaten gegen die jeweiligen deutschen Regierungsnetze gab, die in den Verträgen abgebildet waren.

Wir haben uns zweitens sehr intensiv mit einer weiteren Absicherung der Regierungskommunikation beschäftigt. Das BSI hat die Leitungsverbindungen überprüft. Einige Behörden wurden zusätzlich auf den IVBB geschwenkt. Es wurden zentrale Server für kryptierte Mobilverbindungen aufgesetzt, damit die Nutzer es noch leichter haben, zu kryptieren; sie konnten auch vorher schon kyptiert telefonieren, aber damit es noch ein bisschen einfacher fällt. Es gab Sensibilisierungsveranstaltungen für auch hochrangige Bundesbedienstete und zusätzliche Gerätebeschaffungen von Kryptogerären aus zentralen Mitteln.

Wir haben drittens die Thematik, die in den Snowden-Dokumenten niedergelegt ist, umfassend in den zuständigen Gremien - IT-Rat des Bundes, IT-Planungsrat mit den Ländern und auch Cyber-Sicherheitsrat - diskutiert und mit den jeweiligen Partnern besprochen.

Es gab viertens im September 2013 einen runden Tisch „IT-Sicherheitstechnik“ gemeinsam mit der Wirtschaft, einer ganzen Reihe von Verbänden und Unternehmen - auch andere Ressorts waren daran beteiligt -, wo wir einen Katalog entwickelt haben von weiter zu fördernden Maßnahmen, zum Beispiel Förderung der IT-Konsolidierung im Bund, um dazu einheitlicher nachfragen zu können, weiterer Ausbau des BSI, neues IT-Sicherheitsforschungsprogramm, Erweiterung der IT-Sicherheit auf neue Anwendungsfelder wie Energy und Health, Programme zur Förderung von der IT-Sicherheit bei KMU. Das waren Ergebnisse dieses runden Tisches.

Und wir haben fünftens im Bereich der vertraglichen und Vergabeentscheidungen zusätzliche Vertragsklauseln aufgenommen in die Musterverträge - EVB-IT - und auch in Einzelverträge mit einzelnen IT-Unternehmen, die ihnen zusätzliche vertragliche Verpflichtungen auferlegten, zu melden, wenn sie ausländischen Nachrichtendiensten Daten übergeben müssen oder wenn sie bestimmten Verpflichtungen unterliegen, damit der Bund dann davon Gebrauch machen kann, zu sagen: Das Unternehmen können wir jetzt nicht mehr weiter beauftragen.

Und wir haben auch in einigen konkreten Vergabeverfahren uns für nationale Lösungen entschieden. Ich selbst habe mich sehr intensiv bemüht, in einer schwierigen Abstimmung mit der EU-Kommission die Vergabe der Netze des Bundes freihändig an einen deutschen Anbieter durchführen zu können und dafür das Plazet der EU-Kommission zu bekommen, was am Ende gelungen ist.

Abschließend möchte ich in wenigen Worten noch einmal zusammenfassen, dass wir in dem gesamten Untersuchungszeitraum eine komplexer gewordene Bedrohungslage erlebt haben, sowohl was Angreifer und Motive angeht als auch vor allen Dingen was Technik und Anwendung der IT angeht, und uns versucht haben, bei der IT-Sicherheitspolitik immer auf das einzustellen, was technisch an Angriffen möglich ist.

Das erforderte immer eine Mischung aus technischen, organisatorischen und rechtlichen Maßnahmen. Zentrale Punkte - auch durchaus umstrittene Punkte immer im Bund -: die stärkere Konsolidierung von Netzen und die Informationstechnik, ein konsequenter Einsatz von Sicherheitstechnik auch durch die Bediensteten, eine engere Zusammenarbeit zwischen Wirtschaft und Staat und zuletzt - das habe ich ja sehr deutlich gemacht - eine sehr starke Förderung von vertrauenswürdiger IT, über die man belastbare Sicherheitsaussagen machen kann. - Vielen Dank.

Stellvertretende Vorsitzende Susanne Mittag: Ja, schönen Dank. - Dann geht es gleich mit der ersten Befragungsrunde los. CDU/CSU, Herr Wendt.

Marian Wendt (CDU/CSU): Ja, vielen Dank, Frau Mittag. - Herr Schallbruch, schönen guten Tag! Willkommen im Ausschuss! Vielen Dank für Ihre Ausführungen - auch noch mal auch grundsätzlicher Art - zur IT-Sicherheit, auch für die nötige Sensibilisierung; das ist ja neben dem konkreten Untersuchungsgegenstand auch ein Thema, mit

dem sich der Untersuchungsausschuss und natürlich der Bundestag an sich beschäftigen. Von daher auch vielen Dank meinerseits - - der sich in dem Thema engagiert, für diese grundsätzlichen Ausführungen zur IT-Sicherheit.

Herr Schallbruch, Sie waren ja von 2002 bis zum Februar dieses Jahres IT-Direktor im Bundesinnenministerium. Vielleicht könnten Sie noch mal konkret Ihre Aufgabenstellung darstellen, auch vielleicht gerade im Zeitabriss, wie sich die Aufgabe verändert hat. Zwischen 2002 und 2016 gab es ja nicht nur verschiedene Ereignisse - wie Snowden - politischer Art; es gab verschiedene wechselnde Regierungen auch, die natürlich verschiedene Zielvorgaben hatten, und auch natürlich die Technik war sicherlich eine ganz andere 2002. Vielleicht wenn Sie das noch mal als Abriss Ihrer Aufgabe und auch in dieser Agenda darstellen könnten?

Zeuge Martin Schallbruch: In der Anfangszeit, als der IT-Stab im Bundesinnenministerium gegründet worden ist und ich die Leitung übernommen habe, war die Zuständigkeit im Wesentlichen beschränkt auf Koordinierung der IT des Bundes und Fachaufsicht über das BSI. Und die wesentlichen politischen Initiativen zu diesem Zeitpunkt gingen in die Richtung der Digitalisierung der Behörden: dass Behörden überhaupt das Internet nutzen, dass erste E-Government-Projekte durchgeführt wurden, ein erstes Portal errichtet wurde, also noch weit von dem entfernt, was wir heute haben, eine Digitalisierung der Behörden zu fördern.

Die ersten Jahre meiner Tätigkeit in dieser Funktion habe ich in der Bundesverwaltung vor allen Dingen für Digitalisierung geworben. Wenn ich das mal von[13] rückwärts betrachte: Die letzten fünf Jahre in dieser Funktion habe ich innerhalb der Regierung vor allen Dingen vor bestimmten Digitalisierungen gewarnt und für Sicherheit geworben. Also, da hat sich der Blickwinkel ein Stück weit geändert, weil in dem Maße, in dem die Behörden die digitale Technik eingesetzt haben, aber auch darüber hinaus wir uns insbesondere im Bereich der Infrastrukturen davon abhängig gemacht haben, die Verantwortung für Sicherheitsfragen in meiner subjektiven Wahrnehmung in meiner Aufgabenerfüllung eine immer größere Rolle gespielt hat, weil die Behörden zu irgendeinem Zeitpunkt - Mitte[14] so ungefähr 2005/06/07 - die Digitalisierung ihrer Behörden ein Stück weit als eigene Aufgabe auch angenommen haben, aber die Sicherheit, wie ich im Eingangsstatement schon gesagt habe, immer ein kleines Stück hinterherhängt, weil sie zusätzlich gekauft werden muss.

Was in den letzten Jahren zusätzlich eine große Rolle gespielt hat, war die Frage: Wo und wie kann der Staat eigentlich IT-Sicherheit irgendwie[15] gewährleisten in einem Umfeld, in dem die meisten Dienstleister irgendwie[16] global sind und wir uns bei dem, was wir alle - Sie auch alle - als IT einsetzen, von globaler Technologie abhängig machen, wo man mit deutscher Gesetzgebung oder nicht mal mit deutschen Forschungsprogrammen keine großen Einflüsse drauf ausüben kann? Das hat eine immer größere Rolle gespielt. Deshalb habe ich diese Verantwortung für vertrauenswürdige IT auch so in den Mittelpunkt meiner Ausführungen gestellt.

Marian Wendt (CDU/CSU): Hatten Sie während Ihrer Zeit auch Kontakte zum BND oder BfV - regelmäßig, unregelmäßig? -, also Arbeitskontakte?

Zeuge Martin Schallbruch: Also, zum BND unregelmäßig wie wahrscheinlich zu allen Behörden der Bundesverwaltung - ich war ja für die IT der gesamten Bundesverwaltung zuständig -, zum BfV natürlich regelmäßig. Das BfV ist eine Behörde des Geschäftsbereichs des Bundesinnen-

13) Richtigstellung des Zeugen: "[streichen des Wortes „von“]", siehe Anlage 2.
14) Richtigstellung des Zeugen: "[Streichen des Wortes „Mitte“]", siehe Anlage 2.
15) Richtigstellung des Zeugen: "[streichen des Wortes „irgendwie“]", siehe Anlage 2.
16) Richtigstellung des Zeugen: "[streichen des Wortes „irgendwie“]", siehe Anlage 2.

ministeriums, wo regelmäßig Behördenleiterbesprechungen stattfinden, an denen ich auch teilgenommen habe.

Marian Wendt (CDU/CSU): Welchen Inhalts waren die regelmäßigen Kontakte zum BfV? Ging es da nur um die Digitalisierung, oder um was für konkrete Anlässe ging es da? Vielleicht auch Cybersicherheit, IT-Sicherheit?

Zeuge Martin Schallbruch: Die meisten Jahre waren die regelmäßigen Kontakte die gleichen Kontakte, wie ich sie auch zum Statistischen Amt oder Bundesverwaltungsamt gepflegt habe; das heißt, es ging um die IT-Ausstattung der Behörde, um Digitalisierung, Haushaltsfragen und Ähnliches. In den letzten Jahren, seit der Cyber-Sicherheitsstrategie 2011, haben die Kontakte natürlich auch die Zusammenarbeit im Bereich der Cybersicherheit betroffen, weil das BSI, was[17] meiner Fachaufsicht unterstand, die federführende Behörde war für das Cyber-Abwehrzentrum und das BfV eine beteiligte Behörde war. Insofern hatten die Kontakte dann häufig damit zu tun: „Wie funktioniert die Zusammenarbeit der Behörden im Cyber-Abwehrzentrum oder bei Cybervorfällen?“, ähnlich wie bei BKA oder Bundespolizei auch.

Marian Wendt (CDU/CSU): Was haben Sie da festgestellt inhaltlicher Art? Wie hat sich die Cybersicherheitslage verändert? Woher kommen Angriffe als Beispiel? Sie haben ja sicherlich auch darüber geredet jetzt, wie sich die Lage verändert hat, wer eine Bedrohung darstellt, wo wir nachsteuern müssen, wo wir vielleicht Experten brauchen. Was hat sich da inhaltlich geändert?

Zeuge Martin Schallbruch: Das ist eine sehr weit gehende Frage. Um sie ordentlich zu beantworten, muss ich das ein bisschen aufteilen. Technisch hat sich die Bedrohungslage erheblich ausdifferenziert, aber einfach wegen der Ausdifferenzierung der Informationstechnik. Wenn Sie viele mobile Geräte einsetzen, Cloud-Services oder Ähnliches, dann ergeben sich da neue Angriffsformen.

Marian Wendt (CDU/CSU): Klar.

Zeuge Martin Schallbruch: Was die Motivlage angeht, haben sich über viele Jahre vier, fünf typische Motivlagen herausgestellt: allgemeine Kriminalität, organisierte Kriminalität, nachrichtendienstliche Aktivitäten, politisch motivierte Aktivitäten. Also, ich kann mich auch erinnern an Cyberangriffe gegen Systeme des Bundes, die offenbar im Kontext standen mit politischen Protestaktionen, und sicherlich auch militärische Aktionen, die wir jetzt nicht erlebt haben, aber über die ich Berichte gelesen habe.

Marian Wendt (CDU/CSU): Und wenn Sie den Punkt „Nachrichtendienstliche Angriffe“ herausstellen, wo, würden Sie einordnen, kamen erstens natürlich die Angriffe her? Das interessiert uns natürlich auch sehr oft, die Frage: Wie hat sich die Situation vielleicht verändert? Gab es da vor Snowden mehr, gab es nach Snowden weniger? Das wäre ja so eine Vermutung vielleicht. Wie würden Sie das ungefähr einschätzen?

Zeuge Martin Schallbruch: Es gibt ja regelmäßige Berichte des BSI an den Innenausschuss des Deutschen Bundestages über die bei den Regierungsnetzen festgestellten Angriffe, und die zeigen eigentlich, dass die Anzahl der Angriffe stetig zunimmt. Ich habe nicht in Erinnerung, dass das irgendwie sich verändert hat rund um Snowden.

Marian Wendt (CDU/CSU): Also nur im Bereich nachrichtendienstlicher Angriffe, nicht die gesamten fünf Punkte.

Zeuge Martin Schallbruch: Die Attribution von Angriffen ist meistens unmöglich oder jedenfalls sehr, sehr schwierig. Es ist nicht so, dass man bei einem Angriff typischerweise in der Lage ist, zu irgendeinem Zeitpunkt sagen zu können: Nun können wir sicher sein, dass der Angriff von diesem oder jenem Urheber ausgeht. - Ich habe aus

17) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.

den Unterlagen, die mir vorgelegt worden sind, wahrgenommen, dass Angriffe Nachrichtendiensten zugeschrieben wurden, wenn sie einen bestimmten technischen Professionalisierungsgrad sozusagen überschritten haben.

Für die Zuordnung von Angriffen zu Nachrichtendiensten im Übrigen ist das BSI nicht zuständig, und mithin bin ich auch nicht zuständig gewesen. Insofern habe ich dazu keine Erkenntnisse. Aber dass ab einem bestimmten Professionalisierungsgrad man aufgrund der Veröffentlichungen, die es gibt, eher davon ausgehen kann, dass es einen nachrichtendienstlichen Hintergrund gab, das ist etwas, was mir berichtet wurde. Aber eine wirkliche Zuordnung zu einem konkreten Nachrichtendienst kenne ich aus eigentlich keinem einzigen Fall.

Marian Wendt (CDU/CSU): Okay. - Die Sicherheit der IT-Infrastruktur und auch der Schutz der Kommunikation deutscher Bürger, deutscher Behörden und auch der deutschen Wirtschaft ist ja bereits längeres Thema, auch im BMI. Bereits im Jahre - - Anfang 2006 formuliert ja der IT-Stab seine entsprechenden Ziele, und dort finden sich bereits Ziele wie die Erarbeitung einer IT-Sicherheitsstrategie, die Verbesserung der IT-Sicherheit in der Bundesverwaltung sowie die Förderung nationaler Sicherheitslösungen. Sie hatten das ja auch so ein bisschen angedeutet: nationale Anbieter, nationale IT-Lösungen. Könnten Sie das noch mal ausführen, welche konkreten Schritte Sie hier gemeinsam mit Ihren Kollegen unternommen haben und welche gesteckten Ziele man erreichen wollte und auch vielleicht jetzt, zehn Jahre danach, erreicht hat?

Zeuge Martin Schallbruch: In der Tat: Diese Zielplanung, die Sie da referenzieren, an die ich mich so ungefähr erinnere, ist überwiegend angegangen worden, was die Strategie angeht - das hatte ich eben erwähnt - und auch was die Verbesserung der IT-Sicherheit in der Bundesverwaltung angeht. Ergebnis war der Kabinettsbeschluss Umsetzungsplan Bund 2007.

Was die Förderung der vertrauenswürdigen nationalen IT-Sicherheitslösungen angeht, habe ich eben einige Maßnahmen ja schon aufgezählt: 2007/08 wurden Sicherheitskooperationen mit einigen Unternehmen geschlossen. Das BSI hat die Anzahl der - - oder hat die[18] Entwicklungsprojekte mit nationalen Anbietern erhöht. Wir haben in bestimmten Bereichen der IT des Bundes auf nationale Lösungen gesetzt. An mehreren Stellen wurde bei Vergabeverfahren eine entsprechende Vorgabe gemacht, soweit das vergaberechtlich möglich war. Und wir haben uns bemüht, die nationalen Anbieter im Bereich der IT-Sicherheit zu fördern, also bei zum Beispiel Export oder auch bei Schutz vor Übernahmen durch ausländische Anbieter. Das waren so wesentliche Maßnahmen, die wir in diesem Bereich ergriffen haben.

Marian Wendt (CDU/CSU): Ebenfalls im Jahr 2006 informierte ja das BMI gemeinsam mit BfV, BND und BSI den Chef des Bundeskanzleramtes, damals der heutige Innenminister de Maizière, über die Sicherheitslage in der Informations- und Kommunikationstechnik. Thema waren hierbei unter anderem ein erheblicher Informationsbedarf und fehlendes Problembewusstsein von Entscheidungsträgern in der Bundesverwaltung, die Sensibilisierung privater Unternehmen, die Verbesserung der Vertrauenswürdigkeit der Anbieter von Produkten und Dienstleistungen im staatlichen Bereich sowie die unter Sicherheitsaspekten zentrale Bedeutung nationaler Anbieter im Sicherheitsbereich. Also, das war vor zehn Jahren. Die Themen kommen ja immer wieder hoch, wie wir sehen. Und Sie waren damals als Vertreter des BMI bei dieser Besprechung im Kanzleramt anwesend. Können Sie sich an diese Besprechung erinnern? - Also, wir haben auch das Ergebnisprotokoll. Wir können es auch vorlegen, aber vielleicht - -

Zeuge Martin Schallbruch: Also, nicht mehr ganz genau -

Marian Wendt (CDU/CSU): Nein, klar.

18) Richtigstellung des Zeugen: "[streichen von „oder die“]", siehe Anlage 2.

Zeuge Martin Schallbruch: - an jedes Detail, aber so grob kann ich mich an die Besprechung erinnern, ja.

Marian Wendt (CDU/CSU): Okay. - Was war der Hintergrund dieses Treffens? Waren Sie da - - Haben Sie das maßgeblich mit initiiert? Waren Sie da nur beigeladen? Waren Sie Unterstützer? Woher gab es - - Was war der konkrete Anlass oder Auslöser?

Zeuge Martin Schallbruch: Daran kann ich mich nicht mehr ganz genau erinnern. Ich weiß allerdings, dass es einen Vorlauf gab, der darin bestand, dass wir Ende 2005/Anfang 2006 die Hausleitung des BMI damals über die Lage informiert haben, und nach meiner Erinnerung ging die Initiative für dieses Treffen auf den damaligen Sicherheitsstaatssekretär des BMI zurück, der das angeregt hat, dass man mal[19] so eine Besprechung macht, um das auch mal[20] ressortübergreifend zu besprechen.

Marian Wendt (CDU/CSU): Und gab es dafür einen konkreten Anlass? Gab es ein aktuelles Szenario, eine Bedrohung, einen konkreten Fall, wo Daten abgeflossen sind, wo man angegriffen wurde beispielsweise? Oft ist man ja auch in der Politik nur reaktiv. Oder war es einfach ein Lagebild, was sich ergeben hatte: „Und wir müssen uns da mal treffen und die Entscheidungsträger auf höherer Ebene sensibilisieren“?

Zeuge Martin Schallbruch: Also, es gab keinen konkreten Anlass nach meiner Erinnerung.

Marian Wendt (CDU/CSU): Okay.

Zeuge Martin Schallbruch: Auch: Soweit ich mich erinnere, hat die Präsentation, die damals gegeben wurde, das Thema auch umfassend abgebildet, von Netzsicherheit bis zu sicheren Geräten, von Fragen der Betroffenheit der Wirtschaft bis zu Fragen der Mitarbeiter der Bundesregierung. Also, das war ein ganz breites Thema, und das war ja damals der Beginn einer Wahlperiode, wo es darum ging - Anfang 2006 muss das gewesen sein -, -

Marian Wendt (CDU/CSU): Ja.

Zeuge Martin Schallbruch: - was in dieser Wahlperiode - - welche Aktivitäten da von der Bundesregierung auf diesem Feld ergriffen werden. Insofern war das eher so eine Strategiebesprechung.

Marian Wendt (CDU/CSU): Und - wir springen, kommen ein bisschen nach vorne - im September 2012, also noch weit vor den Snowden-Veröffentlichungen, richteten Sie im IT-Stab des BMI eine organisatorisch unselbstständige Projektgruppe „Gesellschaft für IuK-Sicherheitsinfrastruktur“ - in Klammern: „PG GSI“ - ein. Könnten Sie uns da erläutern, was da der Anlass war oder die Ursache?

Zeuge Martin Schallbruch: Ja, das ist ein bisschen komplizierter zu erläutern. Wir haben uns als Bundesregierung Ende, ich glaube, 2008/2009 ungefähr oder als Bundesinnenministerium, muss man sagen, entschieden, eine Initiative zu starten, die Netze der Bundesregierung, alle Netze aller Bundesbehörden zu konsolidieren, weil der IVBB eben nur Ministerien, wichtige Behörden und Ähnliches abdeckt.

Diese Konsolidierung wurde dann vom Haushaltsausschuss des Bundestages - ich glaube, es muss 2011 gewesen sein - beschlossen und unterstützt. Wir haben dann eine Strategie entwickelt: Wie würden wir uns denn eigentlich angesichts der Cybersicherheitslage die Regierungsnetze der Zukunft vorstellen? Ein wesentlicher Eckpfeiler diese Strategie war, dass wir einen vertrauenswürdigen nationalen Partner brauchen, einen nationalen Provider, mit dem wir längerfristig zusammenarbeiten können, um nicht abhängig zu sein von schwer kontrollierbaren ausländischen Zulieferungen.

19) Richtigstellung des Zeugen: "[streichen des Wortes „mal“]", siehe Anlage 2.

20) Richtigstellung des Zeugen: "[streichen des Wortes „mal“]", siehe Anlage 2.

Ergebnis davon war, dass wir diese Projektgruppe eingerichtet haben, die Möglichkeiten geprüft haben, eine Gesellschaft zu gründen zwischen dem Bund und einem nationalen Provider, die auf Dauer den Betrieb der Regierungsnetze betreut.

Marian Wendt (CDU/CSU): Ähnlich wie vielleicht die BDBOS mit Alcatel Lucent oder - -

Zeuge Martin Schallbruch: Gut, das ist - -

Marian Wendt (CDU/CSU): Vergleichbar oder - -

Zeuge Martin Schallbruch: Nicht wirklich vergleichbar, weil es da mehr so um technischen Betrieb geht, nicht um Verantwortung. Die Verantwortung für den[21] Betrieb liegt außerhalb meiner Zuständigkeit, weil ja das Digitalfunknetz liegt bei der BDBOS selbst.[22]

Die Idee dieser Gesellschaft war, dass dort auch die Verantwortung für den Betrieb übernommen wird. Eine Gesellschaft, bei der der Bund dann auch zum Beispiel in einem Not- und Krisenfall hätte eintreten können, die Gesellschaft übernehmen, wo aber nicht Beamte, sage ich mal, für innovative Netztechnologien allein zuständig sind, sondern man bei einem Provider, der mehr Erfahrung hat, mit dabei ist.

Aber das ist ein schwieriges Unterfangen, eine solche Gesellschaft zu gründen für so viele Netze und alle Bundesbehörden. Deshalb wurde dafür eine Projektgruppe eingerichtet. Dieses Vorhaben ist nicht zu Ende verfolgt worden, aber auch noch nicht ganz, sage ich mal, abgeschlossen, weil nach der Planung, die mir jetzt auf dem letzten Kenntnisstand bekannt ist, das noch eine Option ist, darüber aber dann wiederum im Haushaltsausschuss des Bundestages entschieden werden wird.

Marian Wendt (CDU/CSU): Genau. - Deswegen möchte ich überleiten zu einem nächsten Themenkomplex, der die Netze des Bundes betrifft. Die heutige Regierungskommunikation stützt sich ja - Sie hatten schon in Teilen ausgeführt - im Wesentlichen auf die beiden Netzinfrastrukturen IVBB, Informationsverbund Berlin-Bonn, und IVBV-BVN, Informationsverbund der Bundesverwaltung, sowie das Bund-Länder-Verbindungsnetz DOI. Während das IVBB von der Deutschen Telekom betrieben wurde, wird, wurde das zweite Netz, IVBV, über mehr als zehn Jahre vom US-Unternehmen MCI bzw. Verizon betrieben. Und im Juni 2014 teilte das BMI mit, die Bundesregierung wolle vor dem Hintergrund der NSA-Affäre die Zusammenarbeit mit der Firma Verizon im Bereich IVBB - - IVBV, also dem zweiten Netz, schrittweise beenden und zukünftig eine Infrastruktur mit erhöhtem Sicherheitsniveau bereitstellen, die einheitlich durch einen Partner betrieben wird, bei dem - ich zitiere - „auch Krisenregelungen und Eingriffsmöglichkeiten durch den Bund bestehen“. Sie hatten das ja eben so leicht angedeutet bei der vorhergehenden Frage.

Was waren erst mal aus Ihrer Sicht die Entscheidungsgründe für die Zusammenarbeit mit Verizon?

Zeuge Martin Schallbruch: Dass es eine europaweite Ausschreibung gab und Verizon diese Ausschreibung 2003, glaube ich, etwa gewonnen hat.

Marian Wendt (CDU/CSU): Ja. Gut. - Da haben sie dann zehn Jahre den Betrieb geführt. Und gab es aus Ihrer Sicht vor dem Hintergrund der NSA-Affäre - das ist eine allgemeine Formulierung - einen konkreten Anlass, dass Sie sagen: „Da gab es Datenabflüsse von der MCI/Verizon aus dem Netz des Bundes“? Gab es Fragen, Dinge oder Anhaltspunkte, die eine Unzuverlässigkeit des Partners - - ja, die dafür - - da, wo es Anhaltspunkte gab - - Gab es Anhaltspunkte dafür, an der - - für die Unzuverlässig- -

Zeuge Martin Schallbruch: Es gab keine Erkenntnisse über Datenabflüsse. Bei Verizon wurde eine

21) Richtigstellung des Zeugen: "[„diesen“ statt „den“]", siehe Anlage 2.

22) Richtigstellung des Zeugen: "[weil das Digitalfunknetz bei der BDBOS liegt]", siehe Anlage 2.

Revision durchgeführt, und da sind keine Erkenntnisse festgestellt worden. Aber unsere Überlegungen zur zukünftigen Strategie für die Netze des Bundes haben eingeschlossen, dass wir Datenabflüsse auch ausschließen wollten. Durch die Beauftragung eines Unternehmens, was[23] eine deutsche Niederlassung eines US-Unternehmens ist und was[24] Bestandteil einer globalen Infrastruktur dieses Unternehmens ist, haben Sie immer die Situation, dass, sage ich mal[25], kritische Steuerungseinrichtungen nicht in Deutschland sind, naturgemäß. Selbst wenn die ganze Kommunikation nur über Deutschland geleitet wird, ist bei einem solchen Unternehmen typischerweise auch ein Einfluss von außen nicht völlig auszuschließen. Und wir haben uns 2014 dafür entschieden, dass wir diesen Einfluss von außerhalb Deutschlands auf die Infrastrukturen ausschließen wollten und das, was beim IVBB jetzt schon stattfindet, für alle Teilnehmer von Netzen des Bundes für die Zukunft ermöglichen wollten, und aus diesem Grunde gesagt: Wir wollen diesen separaten Vertrag nicht mehr fortführen. Ist ja keine irgendwie[26] Sonderkündigung oder so was gewesen, sondern wir haben gesagt: Wir wollen diesen Vertrag nicht mehr fortführen, sondern die Teilnehmer aus diesem Vertrag in die allgemeine NdB-Infrastruktur überführen, die dann von der Telekom betrieben wird.

Marian Wendt (CDU/CSU): Dem Ausschuss liegt ein Dokument vor, VS-NfD. Da geht es im Jahr 2003, wo Bedenken vorgetragen wurden - - Oder gab es denn die Fragestellung, ob es Bedenken gibt der Zusammenarbeit zwischen Bundesregierung - - und ob die Regierungskommunikation über dieses MCI laufen sollte? Damals wurde festgestellt, dass das BMI diese Bedenken in den Bereich der Spekulation zurückweist und dass dem BND keine Erkenntnisse vorlagen, dass dort möglicherweise Datenabflüsse ins Ausland stattfinden könnten, so wie sie - - was vielleicht Ursache war, um 2014 die Verträge nicht zu verlängern. Was ist dazwischen passiert? Also, vielleicht können Sie das noch mal - - Welche Erkenntnisse - - Gab es konkret Anlässe, wo Sie sagen, zwischen 2003: „Wir haben keine Anhaltspunkte, wir können da vollkommen vertrauen, wir machen die europaweite Ausschreibung, Verizon bekommt das“ und dann mit einmal - mit einmal nicht, aber zehn Jahre sind natürlich ein Zeitraum - 2014 die Entscheidung: „Wir wollen national zurückholen und die Gefahr der Abflüsse entsprechend minimieren“?

Zeuge Martin Schallbruch: Also, zu dem Dokument 2003 kann ich mich nicht äußern. Das müssten Sie mir bitte vorlegen. Ich kann aber zu 2014 vielleicht noch mal ausführen.

Das war keine Entscheidung, die sich gegen ein bestimmtes Unternehmen richtete oder die die Erfahrungen in der Zusammenarbeit mit diesem Unternehmen zum Gegenstand hatte, sondern die die Architektur der IT-Systeme des Bundes betraf. Wir haben uns auch in Kenntnis natürlich der Snowden-Unterlagen entschieden, dass wir das Risiko, dass wir ein global operierendes Unternehmen mit wesentlichen Steuerungseinrichtungen außerhalb Deutschlands mit der Regierungskommunikation beauftragen, nicht mehr eingehen wollen.

Im Jahre, ich glaube, 2000 oder 2001 hat die EU-Kommission gegen die Bundesrepublik Deutschland ein Vertragsverletzungsverfahren eingef- - also[27] durchgeführt wegen der freihändigen Vergabe des IVBB. Die Bundesrepublik Deutschland hat eine Einstellung dieses Verfahrens erreichen können durch die Zusicherung, zukünftig alle weiteren Netzvergaben in europaweiter Ausschreibung zu machen. Das wurde[28] - - 2003 hat es zu der Vergabe an Verizon geführt.

23) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.
24) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.
25) Richtigstellung des Zeugen: "[streichen von „sage ich mal“]", siehe Anlage 2.
26) Richtigstellung des Zeugen: "[streichen von irgendwie]", siehe Anlage 2.
27) Richtigstellung des Zeugen: "[streichen von „eingef also“]", siehe Anlage 2.
28) Richtigstellung des Zeugen: "[streichen von „das wurde“]", siehe Anlage 2.

Wir haben es 2014 erreicht - ich erwähnte das eben schon - durch schwierige Verhandlungen mit der EU-Kommission, dass wir für die gesamten Netze des Bundes eine freihändige Vergabe an die Deutsche Telekom mit Zustimmung der EU-Kommission möglich machen konnten, und aus diesem Grunde stand uns auch diese Option zur Verfügung. Insofern, das höhere Risiko wollten wir nicht mehr tragen, und wir hatten die vergaberechtliche Option. Und das beides zusammen hat zu der Entscheidung 2014 geführt, unabhängig von dem 2003er-Vermerk, den ich jetzt nicht erinnerlich habe.

Marian Wendt (CDU/CSU): Also, 2014 war sozusagen Sicherheit vor freiem Wirtschaftsverkehr, würde man sagen. Da hat man die Sicherheitsinteressen vorgebracht, und aufgrund dessen - -

Zeuge Martin Schallbruch: Genau.

Marian Wendt (CDU/CSU): Und wenn Sie sagen - - Wenn Sie von höheren Risiken sprechen, welche Risiken waren das ganz konkret? Also, Ihnen wurde das ja vorgelegt. Das wurde ja sicherlich nicht nur allgemein sicherlich erwähnt und so über den Daumen gepeilt und sich nur auf die Snowden-Dokumente, die irgendwo öffentlich standen, Bezug genommen, sondern es muss ja eventuell auch konkrete Anlässe gegeben haben, die Sie auch der EU-Kommission vorgelegt haben, wahrscheinlich was Sie dazu bewegt, was rechtfertigt, dass wir hier die Sicherheitsinteressen vorbringen und die sozusagen eine freie Vergabe notwendig machen.

Zeuge Martin Schallbruch: Die entscheidende Frage, die man dann oder die wir beantworten mussten, war: Können wir bei einem wettbewerblichen Vergabeverfahren die hohen Sicherheitsanforderungen, die wir haben, gewährleisten? Und das haben wir mit Nein beantwortet, was damit zusammenhängt, dass wir im Laufe vieler Jahre jetzt die Erkenntnisse gewonnen haben, dass eine stärkere Virtualisierung und Vermaschung von Infrastrukturen stattgefunden hat. Ich will mal ein Beispiel nennen, dass Provider beispielsweise weltweite Netze betreiben, diese Netze zwar auch lokale Rechenzentren haben und auch lokale Netzknoten haben, dass es aber zum Beispiel übergreifende Systeme gibt, die Storage-Management machen, wo Follow-the-sun-mäßig irgendwelche Überprüfungen in Asien stattfinden oder Ähnliches. Das heißt, man hat eine andere technische Struktur, und wenn man ein Netz bauen möchte, was[29] man auf einem Vertraulichkeitsniveau VS-NfD haben möchte, und man möchte gleichzeitig ausschließen, dass Einrichtungen steuernd auf dieses Netz einwirken, die außerhalb Deutschlands sind, dann kann man nicht mehr, sagen wir mal[30], europaweit ausschreiben, sondern dann muss man zu einem Provider gehen, wo man entsprechenden Einfluss auch auf alle Steuerungseinrichtungen, die auf dieses Netz einwirken können, hat. Das war, sagen wir mal[31], die wesentliche Erkenntnis, die dann dazu geführt hat, dass wir eine andere Sicherheitsbewertung und dann auch eine andere vergaberechtliche Bewertung vorgenommen haben.

Marian Wendt (CDU/CSU): Ich bin da auch inhaltlich bei Ihnen, wie gesagt, dass man das auch macht und dass das mit Sicherheit auch vor die Warenverkehrsfreiheit und Wirtschaftsfreiheit gehen muss. Für mich stellt sich halt die Frage, dass gewisse Erkenntnisse doch in 2000 eigentlich schon da waren, auch im BMI. Ich darf da vielleicht mal aus einem Vermerk vom 15. Februar 2006 zitieren - das ist MAT A BMI 7-1g_2.pdf, Blatt 76; wir haben ja die Akten anschließend; ich zitiere -:

> Mit der Bezugsvorlage wurde Herrn Minister in einem eingestuften Papier darüber berichtet, dass mit einem massiven Anstieg der (nachrichtendienstlichen) Gefahrdung durch ausländische IT/TK-Unternehmen gerechnet werden

29) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.

30) Richtigstellung des Zeugen: "[streichen von „sage ich mal“]", siehe Anlage 2.

31) Richtigstellung des Zeugen: "[streichen von „sage ich mal“]", siehe Anlage 2.

> muss. Es kann nicht ausgeschlossen werden, dass Firmen an Schlüsselpositionen gezielt Personal und Technik einsetzen, um Informationen auszuspähen und die Verfügbarkeit des Systems zu stören.

Das ist Ende des Zitats. - Gleichwohl wurden die bestehenden Verträge mit der Firma MCI bzw. Verizon nicht gekündigt. Auch die dringende Empfehlung, die Verträge nach dem Ende der regulären Vertragslaufzeit 2008 im Jahr keinesfalls zu verlängern, wurde offenkundig - ja, klar - nicht befolgt, nicht gefolgt, und erst vor dem Hintergrund der Ereignisse um 2013, ohne dem ein gewisses höheres Gewicht beizumessen, entschied sich ja das BMI 2014, die Verträge auslaufen zu lassen mit Verizon. Vielleicht können Sie da noch mal die Situation darstellen. War das ein Kampf? Wie muss man sich das ungefähr vorstellen, wenn es unter den Fachleuten schon die Einschätzung damals gab: „Es gibt diese Angriffe, es gibt die Gefährdung der IT-Sicherheit des Bundes“, und dass man trotzdem sagt: „Hier gilt die EU-Vorgabe“? Man hat vielleicht Angst vor der Kommission, vor einem Verfahren, und man hat da die Bedenken abgewiegelt? Vielleicht können Sie das mal beschreiben, wie das damals war.

Stellvertretende Vorsitzende Susanne Mittag: Das wäre jetzt die letzte Frage, -

Marian Wendt (CDU/CSU): Die letzte Frage, genau.

Stellvertretende Vorsitzende Susanne Mittag: - weil wir dann zur namentlichen Abstimmung müssen.

Zeuge Martin Schallbruch: Okay. - Also, zu dem konkreten Dokument - das müssen Sie mir vorlegen - kann ich mich jetzt nicht äußern. Ich bin auch nicht sicher, ob das nicht eingestuft ist.

Aber zu dem Sachverhalt vielleicht noch mal, soweit ich mich erinnere. Mir sind immer wieder Hinweise zugekommen, dass eine Zusammenarbeit ausländischer IT-Unternehmen mit Nachrichtendiensten nicht ausgeschlossen werden kann, sage ich mal in allgemeiner Form, Nachrichtendienste unterschiedlicher Provenienz.

Gleichzeitig sind in diesem konkreten Fall, aber auch in den meisten anderen Fällen nie - -

(Dem Zeugen werden Unterlagen vorgelegt)

Marian Wendt (CDU/CSU): Genau, das Dokument wird Ihnen jetzt gezeigt, aber es ist, glaube ich, von dem Kernwert der Aussage - -

Zeuge Martin Schallbruch: Ich würde es jetzt erst mal allgemein stellen, -

Marian Wendt (CDU/CSU): Ja, genau.

Zeuge Martin Schallbruch: - und wenn ich es dann noch lesen sollte, dann müssten Sie es mir sagen. Dann kann ich vielleicht meine Aussage noch mal konkretisieren.

Sind mir nie so harte justiziable Fakten vorgelegt worden, die es rechtfertigen würden, einen Vertrag mit einem Provider wegen Unzuverlässigkeit zu kündigen. Man kann nicht, wenn man in einem normalen Vergabeverfahren einen Vertrag vergeben hat, wenn man dann Hinweise darauf bekommt, dass möglicherweise ein Unternehmen mit einem ausländischen Nachrichtendienst zusammenarbeitet, das zum Grund nehmen, einen Vertrag zu kündigen. Man kann bei der nächsten Vergabe sich darum bemühen - -

Marian Wendt (CDU/CSU): Auch wenn die Sicherheitsinteressen der Bundesrepublik Deutschland dem entgegenstehen? Ich meine, Sie sind ja nicht irgendwer, Sie sind ja das Bundes- -

Zeuge Martin Schallbruch: Na ja, wenn das justiziable, auch gegenüber dem jeweiligen Vertragspartner vorzeigbare und auch vor Gericht vorzeigbare Fakten sind. Das war aber in diesem Fall nicht so. Solche Fakten haben wir nicht gehabt.

Insofern ist das mehr eingeflossen in eine allgemeine Sicherheitsbewertung. Das hat dazu geführt, dass wir sehr darauf gedrängt haben, dass von der Möglichkeit, alle Daten zu verschlüsseln,

die es ja im IVBV gibt, und zwar nicht durch diesen Anbieter, sondern das Kryptomanagement hat ja der Deutsche Wetterdienst gemacht, also durch eine staatliche Behörde - - von dieser Möglichkeit Gebrauch gemacht wird, damit der Anbieter, auch der Anbieter nicht in der Lage ist, auf die Daten zuzugreifen.

Marian Wendt (CDU/CSU): Okay.

Zeuge Martin Schallbruch: Dass 2008 nicht gekündigt worden ist, lag daran, dass das technisch nicht möglich war. Also, zu dem damaligen Zeitpunkt gab es die Infrastruktur, in die jetzt gerade die entsprechenden Anbieter[32], Teilnehmer migriert werden, noch nicht.

Marian Wendt (CDU/CSU): Okay. - Dann vielen Dank, und dann machen wir dann später weiter.

Stellvertretende Vorsitzende Susanne Mittag: Gut, dann wäre die Runde auch beendet gewesen.

Marian Wendt (CDU/CSU): Genau.

Stellvertretende Vorsitzende Susanne Mittag: Dann machen wir jetzt eben eine Pause, und wir gehen zur namentlichen Abstimmung. Ich bitte dann alle, flott wiederzukommen,

(Martina Renner (DIE LINKE): Genau, flott! Keine Umwege!)

damit wir wieder einsteigen können, weil wir noch zwei haben. - Danke schön.

(Unterbrechung von 16.47 bis 17.12 Uhr)

Vorsitzender Dr. Patrick Sensburg: So, sollen wir wieder? - Ich gucke mal so in die Runde. Es sind zwar noch nicht alle da, aber alle Fraktionen sind vertreten.

Okay, die unterbrochene Sitzung des 1. Untersuchungsausschusses wird fortgesetzt. Es war die Befragung durch die CDU/CSU-Fraktion abgeschlossen, und jetzt kommen wir in der ersten Runde, wo der Vorsitzende keine Fragen gestellt hat, zur Fraktion Die Linke, und Frau Kollegin Renner stellt die Fragen, wenn ich es richtig sehe. Right? - Gut.

Martina Renner (DIE LINKE): Herr Schallbruch, auch von mir herzlich willkommen! - Ich würde Sie gerne fragen: Es gibt ja auch im Bereich der IT-Sicherheit eine Kooperation mit den USA; Sie haben es ja selbst genannt. Homeland Security als Partnerbehörde spielt da sicherlich eine Rolle.

Sie waren auch selbst Teilnehmer eines Treffens im März 2004, und da ging es auch um Schutz kritischer Infrastruktur und Strategien und Erfahrungsaustausch usw. War Ihnen zu dem Zeitpunkt bekannt, dass es auch Operationen der US-Dienste in Deutschland gab, bei denen Daten in Deutschland - in Deutschland - erfasst wurden und ausgewertet wurden?

Zeuge Martin Schallbruch: Nein, war mir nicht bekannt.

Martina Renner (DIE LINKE): Gab es insgesamt bei diesem Erfahrungsaustausch im Vorfeld Überlegungen, dass man dort auch ein gewisses Maß an Vorsicht walten lassen muss?

Zeuge Martin Schallbruch: Der Erfahrungsaustausch, den Sie ansprechen, war zwischen dem BMI und dem ganz neu gegründeten Department of Homeland Security oder - ich weiß gar nicht, ob das schon „Department“ hieß - Office of Homeland Security, jedenfalls einem neu eingerichteten Ministerium, und der Inhalt des Erfahrungsaustauschs war nach meiner Erinnerung der Schutz kritischer Infrastrukturen. Es ging also nicht um die Sicherheit der IT-Systeme der Regierungen, sondern es ging um die Frage nach meiner Erinnerung: Was für Anforderungen stellt man an die Betreiber von Infrastrukturen?

32) Richtigstellung des Zeugen: "[streichen von „Anbieter“]", siehe Anlage 2.

Martina Renner (DIE LINKE): Okay. - Also, es ging nicht um den Schutz von Behörden oder Regierungseinrichtungen oder Bürgern und Bürgerinnen vor Zugriffen.

Zeuge Martin Schallbruch: Nein, nein.

Martina Renner (DIE LINKE): Gab es dann irgendwann mal später in der Kooperation auch mit US-amerikanischen Stellen solche Überlegungen, dass man auch Skepsis an den Tag legen muss?

Zeuge Martin Schallbruch: Ich kann mich nicht daran erinnern, dass wir in der Kooperation mit den Vereinigten Staaten solche Überlegungen angestellt haben, Skepsis an den Tag zu legen. Die Vereinigten Staaten waren für uns wichtige Partner bei der IT- und Cybersicherheit. Allerdings haben alle Kooperationsgespräche, an die ich mich erinnern kann, immer den Fokus gehabt: Wie kann man eigentlich IT-Sicherheitsmaßnahmen verbessern? Welche zusätzlichen Anforderungen kann man stellen? Wie kann man Informationen über Angriffe austauschen? Und so weiter und so fort.

Martina Renner (DIE LINKE): Okay.

Zeuge Martin Schallbruch: Wir haben zu keinem Zeitpunkt - insofern, das würden Sie vielleicht als Skepsis werten - in diesen Kooperationen Informationen beispielsweise über unsere Sicherheitsmaßnahmen für unsere Regierungsnetze mit den Amerikanern ausgetauscht.

Martina Renner (DIE LINKE): Ich frage das vor dem Hintergrund, dass der *Spiegel* in seiner Ausgabe 49/2014 unter der Überschrift „Fern bedient“ auf einen Vorgang in 2005 abstellt, bei dem der Bundesnachrichtendienst Technik analysiert, Überwachungsanlagen zur Raumüberwachung, also inklusive Kamera, Mikrofonen und Sensorik, und dort feststellt, dass diese Technik, die durch einen US-Anbieter auf den deutschen Markt unter Preis drängt und insbesondere versucht, Geschäfte mit Behörden und Sicherheitseinrichtungen abzuschließen, etwas ganz anderes tut, als sie vorgibt, nämlich dass sie so konfiguriert ist, dass sie, selbst wenn der Nutzer sie ausschaltet oder den Bewegungsmelder deaktiviert, Daten routet an US-Seite. Und das ist ein Vorgang, der, so laut *Spiegel,* im BND 2005 analysiert wurde, untersucht wurde und auch in der Präsidentenrunde besprochen werden sollte. Das wäre ja Anlass gewesen, insbesondere wenn diese Technik hier, so wie es im *Spiegel* heißt, zielgerichtet an Kunden wie Ministerien, Sicherheitsbehörden usw. - - untergeschoben zu werden, dass man sich das dann genauer anguckt mit Blick auf Ihre Aufgabe, IT-Sicherheit der Behörde. Also, kennen Sie diesen Vorgang aus 2005?

Zeuge Martin Schallbruch: Also, an diesen Vorgang kann ich mich nicht erinnern. Ich kann mich aber an vergleichbare Vorgänge erinnern, die aber, glaube ich, nicht 2005 waren, in denen wir Hinweise bekommen haben, dass bestimmte Anbieter versuchen, Produkte in sicherheitsrelevante Bereiche zu bringen, bei denen es Bedenken des BND gab wegen zum Beispiel dem Hintergrund des Anbieters oder Bedenken des BSI wegen der Architektur, nach dem Motto: Der Anbieter kann mit dieser Software oder Hardware bestimmte Informationen abgreifen.

In solchen Fällen haben wir typischerweise Warnungen in die Bundesverwaltung gegeben, dass man solche Systeme nicht einsetzt, seit 2007, seit der Zusammenarbeit mit den kritischen Infrastrukturen, auch in Richtung kritischer Infrastrukturen.

Insofern, um noch mal auf die Skepsis zurückzukommen, gibt es - -

Martina Renner (DIE LINKE): Ich will - -

Zeuge Martin Schallbruch: Ja.

Martina Renner (DIE LINKE): Wir müssen immer gucken, dass wir hier nicht so ins Allgemeine kommen. Uns interessieren die Nachrichtendienste der Five Eyes und nicht alles das, was es noch Schlimmes in der Welt gibt. Warum das möglicherweise von Interesse ist, wenn man mit der US-Seite kooperiert - - Dieser Bericht des

BND war damals überschrieben, also hier laut Spiegel:

> Nachrichtendienstliche Aufklärung deutscher Behörden und Hochtechnologieunternehmen durch US-Nachrichtendienste mithilfe von Sicherheitstechnik zur Raumüberwachung.

Also, hier wusste man, wer der Täter ist, und das war 2005. Wie ist man mit so etwas umgegangen, wenn der BND zu solchen Erkenntnissen kommt?

Zeuge Martin Schallbruch: An diesen Vorgang kann ich mich nicht erinnern. Aber man ist mit so etwas so umgegangen, dass man dann gesagt hat: Wir wollen dieses Produkt in den entsprechenden sicherheitsrelevanten Bereichen nicht einsetzen.

Martina Renner (DIE LINKE): Mhm. - Und dass man sich mal diese Methodik ansieht hinsichtlich der Frage: „Könnte es da noch anderes geben?“? Also, das muss dann ja auch eine Rolle spielen, nicht nur dieses Produkt sozusagen nicht dann sozusagen noch zu bewerten oder zuzulassen, sondern man muss sich ja dann etwas grundsätzlichere Gedanken machen, wenn sozusagen ein sogenannter befreundeter Dienst so etwas unternimmt hier in Deutschland, ob es dort sozusagen darüber hinaus eine strategische Ausrichtung bei solchen Unternehmungen gibt oder ob das ein Einzelfall ist.

Zeuge Martin Schallbruch: Also, ich kenne diesen einen Vorgang, wie gesagt, nicht. Aber das BSI hat für alle kritischen Infrastrukturbereiche oder kritischen IT-Bereiche der Bundesverwaltung ständig die Sicherheit überprüft und überlegt: An welchen Stellen kommen hier welche Produkte zum Einsatz? Wo müssen wir vertrauenswürdige nationale Produkte einsetzen? Wo müssen wir, sagen wir mal, genauer hingucken? Wo müssen wir auf Zertifizierung bestehen und wo nicht?

Wenn wir Erkenntnisse bekommen haben - und da kenne ich durchaus verschiedene Fälle -, dass Produkte fragwürdig sind, dann hat das immer dazu geführt, dass eine Sicherheitsbewertung durchgeführt worden ist: Wo werden die bei uns eingesetzt, und können wir die noch weiter einsetzen?

Beispielsweise Smartphones eines bestimmten Herstellers wurden von BND und BSI als fragwürdig angesehen. Wir haben die Bundesverwaltung gewarnt. Wir haben gesagt: Wir wollen die nicht mehr einsetzen. Wir haben eine Alternative entwickelt. Das ist die normale Vorgehensweise gewesen.

Im Übrigen war ich für Fragen der Spionageabwehr, das heißt für, sagen wir mal, das Gesamtbild der Tätigkeit einzelner anderer Nachrichtendienste, innerhalb des BMI nicht zuständig.

Martina Renner (DIE LINKE): Vor dem Hintergrund - Sie sind ja schon zur MCI WorldCom/Verizon-Problematik gefragt worden -: Wieso ist dieser Vorgang bis heute, Verizon vollständig als kooperierenden Diensteanbieter auszuschließen, nicht abgeschlossen?

Zeuge Martin Schallbruch: Also, ich kann jetzt nur bis 2014 dazu Stellung nehmen. Die Entscheidung ist ja erst 2014 getroffen worden, Verizon als Diensteanbieter abzulösen, und das ist nichts, was man so tun kann, wie man jetzt den Bezug von - was weiß ich - Getränken oder so - - einfach morgen einen anderen Provider beauftragen kann, sondern das geht dann um Tausende von Standorten und Liegenschaften in ganz Deutschland, an denen man die jeweilige Technik austauschen muss, und jeder dieser Standorte muss einzeln geschwenkt werden. Das heißt, da muss jemand hin und muss da irgendwie den Standort erst mal aufnehmen. Dann muss geplant werden, und dann wird ein Projekt aufgesetzt, und man schafft dann irgendwie[33] drei Standorte pro Woche oder Ähnliches. Also, das ist ein sehr aufwendiges technisches Projekt,

33) Richtigstellung des Zeugen: "[streichen von „irgendwie“]", siehe Anlage 2.

wenn man angesichts der heutigen Anforderungen an elektronische Kommunikation die Kommunikation in der Fläche in ganz Deutschland von einem Provider auf einen anderen schwenkt.

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir wechseln in dieser Runde.

Martina Renner (DIE LINKE): Okay. Machen wir dann nachher weiter.

Vorsitzender Dr. Patrick Sensburg: Genau, geht ja gleich wieder weiter. - Wir kommen jetzt zur Fraktion der SPD, und es beginnt mit Fragen Kollege Flisek.

Christian Flisek (SPD): Danke, Herr Vorsitzender. - Herr Schallbruch, guten Tag! - Ich würde mal so gern einsteigen: Sie haben im Sommer/Spätsommer 2013 Vorschläge bei den Koalitionsverhandlungen gemacht für, ich sage jetzt mal, allgemein Verbesserungen im Bereich der IT-Sicherheit in Deutschland. Was haben Sie damals für Bedarfe oder Defizite im Bereich der IT-Sicherheit in Deutschland erkannt, wo Sie sagen: „Das muss eigentlich oder hätte in einen Koalitionsvertrag eingehen müssen“? Welche Vorschläge waren das?

Zeuge Martin Schallbruch: Ich kann mich nicht mehr an alle Vorschläge erinnern, die ich gemacht habe, weil ich ja für die Abteilung, für die gesamte Abteilung zuständig war und wir zu allen Fragen der Digitalisierung Vorschläge gemacht haben.

Christian Flisek (SPD): Ja.

Zeuge Martin Schallbruch: Das waren Dutzende von Einzelvorschlägen.

Im Bereich der IT-Sicherheit war ein ganz entscheidender Punkt die Förderung vertrauenswürdiger Informationstechnik, das heißt Fortsetzung von Forschungsprogrammen, Erleichterungen von Regelungen im Vergaberecht, vertrauenswürdige nationale Provider zu beauftragen, Ausweitung des Anwendungsbereichs der Zertifizierung des BSI. Regelungen im Außenwirtschaftsgesetz waren nach meiner Erinnerung von den Vorschlägen umfasst. Ein ganz wichtiger Vorschlag, der sich im Koalitionsvertrag nicht durchgesetzt hat, aber dann später, war die Konsolidierung der IT des Bundes bei einem Dienstleister, um dort einheitliche und höhere Sicherheitsmaßnahmen ergreifen zu können und nicht so viele Angriffsflächen zu bieten. Auch die Konsolidierung der Netze des Bundes war nach meiner Erinnerung vorgeschlagen. Dann haben wir eine ganze Reihe Vorschläge gemacht im Bereich kritischer Infrastrukturen, IT-Sicherheitsgesetz, was ja dann auch im Koalitionsvertrag aufgenommen worden ist, Sensibilisierung der Bürgerinnen und Bürger. Förderung „Deutschland sicher im Netz“ war aus meine Erinnerung ein Vorschlag, den wir gemacht haben. Also, viel mehr Erinnerungen habe ich jetzt nicht mehr, was jetzt konkrete Vorschläge waren.

Christian Flisek (SPD): Und Sie haben das ja mal angedeutet: Was waren Dinge, die jetzt nicht Eingang gefunden haben, wo Sie aber sagen: „Das ist eigentlich ein Bedarf, ein Defizit, der nach wie vor sehr akut besteht“?

Zeuge Martin Schallbruch: Also, sehr intensiv bemüht hatte ich mich um eine Aussage zur Konsolidierung der IT der Bundesverwaltung. Das ist eine Zeit lang auch in den Entwürfen drin gewesen und hat dann am Ende nicht Eingang gefunden.

Christian Flisek (SPD): Was hätte das konkret bedeutet, Konsolidierung?

Zeuge Martin Schallbruch: Dass man den IT-Betrieb der Bundesbehörden, Hunderter von Bundesbehörden bei einem Dienstleister konzentriert, dass man damit - natürlich nicht in einem Rechenzentrum; jetzt haben wir 119 Rechenzentren - - Ich würde mir dann einen Dienstleister vorstellen, der natürlich in Deutschland vielleicht fünf Rechenzentren betreibt, also hohe Redundanz, aber eben mit einem hohen einheitlichen Sicherheitsniveau für alle Behörden und auch der Möglichkeit, dass - was Frau Abgeordnete Renner eben angesprochen hat -, wenn zum Beispiel eine Sicherheitsbewertung für ein Pro-

dukt zu dem Ergebnis führt: „Da haben wir Zweifel, weil zum Beispiel der Hersteller übernommen worden ist von einem anderen Hersteller“, man es dann für die ganze Bundesverwaltung sehr schnell austauschen kann.

Heute ist es so: Wir haben in der Fläche eine sehr heterogene Landschaft und brauchen für einen solchen Austausch sehr lange.

Christian Flisek (SPD): Und diese sehr heterogene Landschaft in der Fläche, die Sie jetzt gerade angesprochen haben, ist etwas, was sozusagen im - ich nenne das jetzt mal - Wildwuchs über Jahre sich so ergeben hat, weil jeder eigentlich unkoordiniert das gemacht hat, was er für richtig gehalten hat.

Zeuge Martin Schallbruch: Ja, genau.

Christian Flisek (SPD): Das heißt, eine Konsolidierung - - Oder ich frage jetzt mal andersrum: Warum, glauben Sie, ist das denn dann gescheitert? Sie sagen: Das ist dann aus dem Koalitionsvertrag rausgeflogen. - War das ein Widerstand der einzelnen Ressorts, die gesagt haben: „Wir lassen uns da nicht reinfuhrwerken und reinbestimmen in unsere eigene IT-Infrastruktur“?

Zeuge Martin Schallbruch: Ich war ja nicht Teilnehmer der Koalitionsverhandlungen, und insofern kann ich nicht sagen, warum es da nicht aufgenommen worden ist von den Politikern, die den Koalitionsvertrag verhandelt haben. Aber ich kann nur aus der Perspektive eines Regierungsbeamten berichten, dass es genau so ist, wie Sie beschreiben: Es gibt einen immerwährenden Widerstand der Ressorts in dem gesamten Zeitraum, auf den sich der Untersuchungsauftrag erstreckt, gegen die Konsolidierung der IT bei einem Dienstleister wegen der Befürchtung, dass man dann nicht die IT-Leistungen zu dem Preis bekommt, wie man sie gerne haben möchte.

Christian Flisek (SPD): Und das war dann wahrscheinlich auch der Grund, warum - - Sie sind ja sozusagen - ich nenne das mal so - der Architekt eines CIO-Konzepts des Bundes, also Chief Information Officer. Sie haben mal vorgeschlagen, glaube ich, dass jedes Ressort eine solche Person nennen soll und das Ganze unter dem Dach eines Bundes-CIO dann steht. Und dieses Konzept ist ja auch nicht umgesetzt worden, und das sind ähnliche Gründe. Also, sozusagen die Nickeligkeiten zwischen den Ressorts haben da doch eine ganz starke Wirkung.

Zeuge Martin Schallbruch: Ja, im Grundsatz trifft das zu, was Sie vortragen. Umgesetzt worden ist das Konzept schon, was 2007 wesentlich von mir entwickelt worden ist, aber eben sehr schwach. Die Ressorts haben IT-Beauftragte eingerichtet, zentrale, und es gibt einen IT-Beauftragten der Bundesregierung, dem aber wegen der Ressorthoheit aus Artikel 65 Grundgesetz keine Entscheidungsbefugnisse zugedacht wurden, sondern eben die Leitung eines Gremiums, was dann ressortübergreifend einstimmig entscheiden muss. Und es gibt auch kein zentrales Budget für die IT des Bundes, sondern die Budgets liegen in den Bundesministerien.

Ein Stück weit ist das in den letzten Monaten geändert worden, aber das liegt außerhalb des Untersuchungszeitraums.

Christian Flisek (SPD): Wenn man mal eine Bestandsaufnahme von dieser Situation macht, vor der wir stehen - also ich sage jetzt noch mal den Begriff „so etwas gewachsener Wildwuchs“ -, nach Ihrer Einschätzung was bedeutet das denn für die Sicherheit der dort verarbeiteten, gespeicherten Daten? Haben wir zum Beispiel, wenn man sich die ganze Landschaft vor Augen hält, Daten, die beispielsweise auch auf US-Servern liegen können?

Zeuge Martin Schallbruch: Ich kann das nicht ausschließen, dass es innerhalb der Bundesverwaltung Behörden gibt, die Dienste nutzen, wo Daten auf US-Servern liegen. Es gibt eben bis heute noch keine, sagen wir mal, zentrale Steuerung der gesamten IT, wo an einer Stelle die Information verfügbar ist: Wo sind welche Daten? Auf was für Servern? Mit welchen Produkten werden sie verarbeitet? Und so weiter und so

fort. Das ist das Resultat einer, sage ich mal[34], unkonsolidierten Landschaft.

Allerdings gibt es Bereiche in der Bundesverwaltung - das muss man erwähnen -, in denen man frühzeitig konsolidiert hat, und das sind die Netze. Das hängt mit dem Regierungsumzug zusammen. Viele Staaten in der Welt haben kein einheitliches Regierungsnetz, wie es die Bundesrepublik Deutschland hat. Bei meinen Kontakten in den Vereinigten Staaten, die Frau Abgeordnete Renner eben erwähnt hat, habe ich beispielsweise gelernt, dass dort eines der größten Sicherheitsprobleme ist, dass sie ungefähr 2 000 Übergänge aus ihren Regierungsnetzen ins Internet haben, während hier die Bundesregierung in Bonn und in Berlin jeweils zwei Übergänge hat. Die vier kann man natürlich ganz anders sichern, als wenn man 2 000 hat. Also, Teile der Landschaft sind schon ganz gut konsolidiert, aber die Rechenzentren in ihrer Vielfältigkeit harren noch der Konsolidierung.

Christian Flisek (SPD): Und hat sich denn da in der Bewertung nach Snowden, wenn man das jetzt mal als eine Zäsur sieht, was da im Sommer 2013 passiert ist, irgendwas verändert? Ist man dort mal stärker tätig geworden? Wir haben ja dann auch den Vorfall des Kanzlerinnenhandys gehabt, wo wir alle ja nur gesagt haben: „Das ist allenfalls die Spitze eines Eisbergs“, jetzt ganz symbolisch. Aber eigentlich geht es ja da um die große Masse der IT-Infrastruktur und der Sicherheit, die davon betroffen ist. Hat sich da gravierend was verändert nach Snowden?

Zeuge Martin Schallbruch: Also, ich überblicke ja den gesamten Zeitraum seit 2002 und kann sagen: Es hat sich seit Snowden gravierend etwas verändert. Es gibt Beschlüsse über die IT-Konsolidierung der gesamten Bundesverwaltung, sukzessive soll das in einen Dienstleister reingehen[35]. Es gibt einen harten Beschluss zur Konsolidierung aller Netze. Es gibt einen vor 2013 noch ganz schwachen, jetzt sehr starken Druck aus dem Haushaltsausschuss des Bundestages, der diesen Prozess steuert und vierteljährlich, glaube ich, Bericht bekommt zu dem Thema. Das heißt - -

Christian Flisek (SPD): Druck inwiefern? Was machen die Kollegen da?

Zeuge Martin Schallbruch: Die üben Druck aus auf die Bundesministerien, das BMI federführend und dahinter die Bundesministerien, die Konsolidierung der IT voranzutreiben und regelmäßig über die Fortschritte zu berichten.

Christian Flisek (SPD): Okay.

Zeuge Martin Schallbruch: Auch die Mittel dafür sind bereitgestellt worden, umfassend, aber immer mit Auflagen versehen und mit Berichten, dass auch tatsächlich ein Fortschritt messbar ist. Und dass dieser Druck aus dem Parlament entstanden ist, geht nach meinem Eindruck auch auf die Snowden-Veröffentlichungen zurück.

Das Zweite, was ich nennen will: Es gibt eine sehr viel größere Akzeptanz bei den Beschaffern im Bund, die Möglichkeiten, die das Vergaberecht bietet, in sicherheitskritischen Bereichen auch nationale vertrauenswürdige Lösungen einzusetzen, auch auszunutzen. Jeder Beschaffer geht ja ein Risiko ein, wenn er sagt: Ich nehme jetzt hier die Ausnahmevorschrift § 100 GWB irgendwie und sage: Das ist sicherheitskritisch. - Das Risiko, dass er dann vor Gericht gezogen wird und verliert oder dass es ein Vertragsverletzungsverfahren gegen Deutschland gibt - - Diese Risikobereitschaft ist gestiegen. Auch das führe ich auf die Snowden-Veröffentlichungen zurück.

Christian Flisek (SPD): Das heißt, es werden bei den Ausschreibungen verstärkt - vielleicht können Sie das noch mal quantifizieren - dann Anforderungen formuliert, die auf, ich sage mal, eine nationale Lösung hinsteuern.

Zeuge Martin Schallbruch: Quantifizieren kann ich das nicht, weil es keine zentrale Beschaffungsorganisation für die Bundesverwaltung gibt

34) Richtigstellung des Zeugen: "[streichen von „sage ich mal“]", siehe Anlage 2.

35) Richtigstellung des Zeugen: "[statt „reingehen“ „verlagert werden“ siehe Anlage 2.

und das BMI hier nur, sagen wir mal[36], Handreichungen gibt, Musterverträge usw. Aber in all diesen Regelungen sind inzwischen Klauseln drin[37], die manche ausländischen Anbieter nicht akzeptieren können und deshalb auf Gebote verzichten. Mir sind vielmehr Einzelfälle bekannt geworden in meiner Tätigkeit, in denen eine freihändige Vergabe durchgeführt worden ist und durchaus auch in manchen Fällen vor Gericht sich dann durchgesetzt hat.

Christian Flisek (SPD): Wie sind da die Reaktionen von, ich sage mal, den Lobbyisten der US-Unternehmen, die davon betroffen sind?

(Dr. André Hahn (DIE LINKE): Die sind not amused!)

Zeuge Martin Schallbruch: Nach den Snowden-Veröffentlichungen habe ich selbst auch und haben auch die Kollegen in meinem Bereich und auch das Bundesinnenministerium insgesamt natürlich sehr viel deutlicher hingeschaut und sehr viel deutlicher gemacht, dass wir bei amerikanischen Unternehmen genauer hinschauen müssen. Das hat zu einem - wie soll ich mal sagen? - sehr starken Anstieg von Lobbydruck geführt - das kann man nicht verkennen - von amerikanischen Unternehmen, weil die Vertrauenswürdigkeit amerikanischer Unternehmen insgesamt ein Stück weit infrage gestellt wurde, es dazu ja auch Presseberichte gab. Die Reaktion der Unternehmen war unterschiedlich. Manche haben sich darauf eingestellt und haben beispielsweise begonnen, Kooperationen mit deutschen IT-Sicherheitsunternehmen zu suchen, um vertrauenswürdige deutsche Produkte zur Absicherung ihrer Lösungen einzusetzen. Da kenne ich einige Beispiele.

Manche Unternehmen haben in Deutschland Infrastrukturen errichtet, Rechenzentren. Manche Unternehmen haben die sogar deutschen Unternehmen praktisch zur Verfügung gestellt, sodass juristisch die Daten nicht bei einem amerikanischen Unternehmen gespeichert sind. Also, es gibt da auch in der Sache einige Unternehmen, die große Fortschritte gemacht haben in der Zeit, die hier in Rede steht, bei der Erhöhung der Vertrauenswürdigkeit ihrer Leistungen.

Christian Flisek (SPD): Also konkret jetzt mal, ohne dass wir jetzt hier Werbung machen wollen oder so: Aber zum Beispiel jetzt eine Vereinbarung, die Microsoft mit der Deutschen Telekom geschlossen hat, sodass man sich darauf verständigt hat, die Speicherung von europäischen Kommunikationsdaten auf Servern innerhalb der EU sicherzustellen, und wo dann EU-Unternehmen sozusagen als Sachwalter und Datenspeicher des US-Konzerns fungieren - - Das sind solche Fortschritte beispielsweise, oder?

Zeuge Martin Schallbruch: Ich habe solche Lösungen im Untersuchungszeitraum gefordert von den Unternehmen und habe natürlich jetzt davon gehört, dass das auch inzwischen erste Unternehmen umsetzen.

Christian Flisek (SPD): Halten Sie das für vertrauenswürdig, so was?

Zeuge Martin Schallbruch: „Vertrauenswürdig“ ist kein absoluter Begriff. Das erhöht die Vertrauenswürdigkeit. In der IT-Sicherheit können Sie beispielsweise mit einem Innentäter immer sehr leicht -

Christian Flisek (SPD): Okay.

Zeuge Martin Schallbruch: - auch alles, was an Vertrauen da ist, schon wieder zerstören. Es erhöht die Vertrauenswürdigkeit, weil die Datenspeicherung eben vollständig auch in deutschem Rechtsraum stattfindet. Und das ist schon ein guter Schritt, und ich habe wahrgenommen, dass das ja auch von vielen Unternehmen, Unternehmenskunden inzwischen auch nachgefragt wird, nicht nur von der Regierung.

Christian Flisek (SPD): In der vorletzten Woche war eine Tagung bei der Stiftung Wissenschaft und Politik, und da hat ein US-amerikanischer

36) Richtigstellung des Zeugen: "[streichen von „sagen wir mal“]", siehe Anlage 2.

37) Richtigstellung des Zeugen: "[streichen von „drin“]", siehe Anlage 2.

Referent darauf hingewiesen, dass Deutschland innerhalb der EU eine sehr zentrale Rolle als Internet-Backbone einnimmt innerhalb der EU, etwa vergleichbar durchaus wie die USA, insbesondere im Hinblick auf Kommunikationsverkehre, ich sage mal, aus Nahost. Und wir wissen ja alle, dass dieser Kommunikationsverkehr - haben wir uns sehr gut mit auseinandergesetzt bei den Kooperationsprojekten des BND im Rahmen oder im Kontext der Terrorismusbekämpfung - wichtig und auch begehrt ist. Jetzt frage ich Sie aber: Gibt es aus Ihrer Sicht besondere Schutzvorkehrungen, die notwendig wären in Deutschland gerade aufgrund dieser strategischen Position als bedeutender Internet-Backbone, um den Schutz der Privatsphäre hier und auch den Schutz von Betriebs- und Geschäftsgeheimnissen von Unternehmen in Deutschland angemessen zu schützen?

Zeuge Martin Schallbruch: Ja, ganz einfach: Verschlüsseln.

(Martina Renner (DIE LINKE): Ja!)

Ich meine - -

Christian Flisek (SPD): Ja, mich freut das immer, wenn ich das aus dem Hause des Bundesinnenministers höre.

Zeuge Martin Schallbruch: Ich bin nicht im Hause des Bundesinnenministers, aber habe das auch schon zu meiner Zeit im Hause des Bundesinnenministers gesagt: Verschlüsseln aller Daten und Kommunikationsverkehre. So einfach ist das.

Das ist natürlich in der praktischen Umsetzung sehr schwierig, aber man kann in allen Bereichen - jeder Einzelne, jedes Unternehmen, jede Behörde - sehr viel mehr tun noch und kann einfach weitere Verkehre verschlüsseln. Dafür stehen vernünftige Verfahren zur Verfügung, die auch sicher sind.

Christian Flisek (SPD): Und Verschlüsseln heißt auch Verschlüsseln. Da hat kein anderer einen Schlüssel für.

Zeuge Martin Schallbruch: So verstehe ich das, Verschlüsseln.

(Martina Renner (DIE LINKE): So war das gedacht!)

Christian Flisek (SPD): Genau. - Das bedeutet - - Jetzt auch mal bezogen auf Ihre Zeit im Innenministerium die Frage gestellt: Wie ist denn das Haus mit solchen sehr unterschiedlichen Zielsetzungen, die ja alle unter einem Dach vereinigt waren, also einerseits natürlich schon die Begehrlichkeiten der Sicherheitsbehörden und Nachrichtendienste, da irgendwie dann doch für den Fall aller Fälle den Schlüssel irgendwie in den Händen zu halten, und andererseits die Anforderung, die IT-Infrastruktur zu konsolidieren und die Integrität sicherzustellen - - Wie ist man denn mit diesem Zielkonflikt unter einem Dach umgegangen?

Zeuge Martin Schallbruch: Man hat das intensiv diskutiert. Ich kann mich aus der Zeit, in der ich da Verantwortung getragen habe, an bestimmt vier, fünf Grundsatzdiskussionen bis hoch zur Ministerebene über diese Frage erinnern. Beginnt 2002, und immer wieder wurden - -

Christian Flisek (SPD): Wer war damals - - Sagen Sie nur, wer da - - mit wem - - mit welchen Ministern Sie da gesprochen haben.

Zeuge Martin Schallbruch: Mit Herrn Schily, mit Herrn Schäuble, mit Herrn de Maizière. Bei Herrn Friedrich kann ich mich nicht erinnern, ob im Zeitraum der Amtszeit von Herrn Friedrich diese Diskussion war. Aber bei den drei Ministern jedenfalls kann ich mich erinnern. Und es wurden dann die Argumente von beiden Seiten gehört, und am Ende hat sich die Linie durchgesetzt, für die ich mich auch starkgemacht habe, dass wir in Deutschland keine Kryptoregulierung einführen.

Christian Flisek (SPD): Bei allen drei Ministern war das gleichermaßen so.

Zeuge Martin Schallbruch: Ja.

Christian Flisek (SPD): Das ist ja - - Nach meiner Kenntnis, ich sage mal, ist das letzte offizielle Dokument, das ich zur Kryptopolitik kenne, glaube ich, ein einseitiges Dokument irgendwie aus dem Jahr 1999. Seitdem gibt es sozusagen ja irgendwie keine Aktualisierung, oder? Ist das richtig?

Zeuge Martin Schallbruch: Da gibt es keine Aktualisierung. Die Diskussion ging immer darum: Wollen wir die Kryptoeckpunkte von 1999 bestätigen oder nicht? Und das Ergebnis war immer: Wir wollen sie bestätigen.

Es gibt jetzt aber auch nicht wirklich die Notwendigkeit, dass ein Bundesministerium Dokumente produziert, dass sie zu irgendeinem Thema kein Gesetz machen. Insofern ist es bei dieser Linie, 99er-Linie, geblieben bis heute.

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir wechseln.

Christian Flisek (SPD): Ja, dann wechseln wir.

Vorsitzender Dr. Patrick Sensburg: Genau. - Dann geht es zur Fraktion von Bündnis 90/Die Grünen, und Herr Kollege von Notz fängt an.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Guten Tag, Herr Schallbruch! - Um das vielleicht ein bisschen zu konkretisieren: Können Sie sich noch dran erinnern, was für Diskussionen stattgefunden haben im Sommer 2013 mit den Snowden-Veröffentlichungen bei Ihnen?

Zeuge Martin Schallbruch: Sicher nicht an alle, weil es waren sehr viele.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber wie war denn so die Stimmung? War man völlig aus den Latschen? Oder hat man gesagt: „Ja, gedacht haben wir es uns eigentlich schon immer“?

Zeuge Martin Schallbruch: Ich würde mal sagen: In der Mitte zwischen Ihren beiden Positionen. Weil[38] ich persönlich kann über mich sprechen und das, was ich in meinem Verantwortungsbereich wahrgenommen habe: Ich bin davon ausgegangen, dass die ausländischen Nachrichtendienste hinter vielen Cyberangriffen möglicherweise stecken und sich intensiv darauf vorbereiten, auch den Cyberraum zu nutzen für Angriffe. Und so weiter und so fort.

Ich bin nicht davon ausgegangen oder ich habe nicht erwartet gehabt zu dem damaligen Zeitpunkt, dass das Ausmaß der technischen Vorbereitungen, auch der technischen Maßnahmen, die sozusagen von der NSA laut den Snowden-Dokumenten vorbereitet worden sind, so gewaltig ist. Also, das hat mich auch als Techniker, sage ich mal[39], überrascht. Auch die verschiedenen Stoßrichtungen, mit denen da technische Maßnahmen konzipiert wurden, um in fremde Systeme einzudringen, war nichts, was ich in diesem Ausmaß erwartet hätte.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und dass Teil dieser Kooperationen, die es da gab, teilweise ein deutscher Nachrichtendienst auch war? War das bei Ihnen so bekannt, dass der Bundesnachrichtendienst so eng kooperiert auch in Deutschland mit den Five Eyes, oder hat das auch überrascht?

Zeuge Martin Schallbruch: Also, über die Kooperationen des Bundesnachrichtendienstes mit anderen Nachrichtendiensten war mir in meiner gesamten Dienstzeit nichts bekannt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also „Eikonal“, „Glotaic“, solche Sachen hat man nie was von gehört.

Zeuge Martin Schallbruch: Nein, war mir nicht bekannt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja. - Haben Sie von diesem Belgacom-Fall

38) Richtigstellung des Zeugen: "[streichen von „Weil“]", siehe Anlage 2.

39) Richtigstellung des Zeugen: "[streichen von „sage ich mal“]", siehe Anlage 2.

auch erst aus den Snowden-Unterlagen erfahren, oder - -

Zeuge Martin Schallbruch: Ich kann mich nicht mehr ganz genau erinnern, aber ich glaube, ich habe von diesem Fall früher erfahren, weil das BSI mit diesem Fall befasst war und das BSI dazu berichtet hat.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und können Sie das mal für uns einordnen, wie man damals da von deutscher Behördenseite draufgeguckt hat auf diesen Belgacom-Fall?

Zeuge Martin Schallbruch: Bei mir ist vor allen Dingen angekommen, was das BSI, was[40] ja da ein Stück weit eingebunden war in die Analyse, berichtet hat über die Art und Weise, wie dieser Angriff erfolgt ist, welche auch ausgefeilten Methoden verwendet wurden, um dort in das System einzudringen. Und das hat mich natürlich in dem Maße interessiert, als für uns klar war: Wir müssen prüfen, ob wir bei unseren Regierungsnetzen gegen vergleichbare Angriffe ausreichend geschützt sind. Das hat das BSI dann auch getan und ist zu dem Ergebnis gekommen, dass das im Grundsatz so ist. Allerdings[41] bei jedem einzelnen Vorfall, den man zur Kenntnis bekommen hat - wir haben auch andere Vorfälle aus dem Ausland zur Kenntnis bekommen -, hat das BSI eigentlich in der Regel immer seine Abwehrsysteme noch mal ein Stück weit erweitert, neue Signaturen eingepflegt oder neue Mechanismen danach programmiert. Ich kann mich nicht mehr genau erinnern, aber es kann sein, dass das auch im Belgacom-Fall so war.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Trotzdem hat sich da im Nachhinein rausgestellt, dass auch Mitarbeiterinnen und Mitarbeiter des Bundeskanzleramts offensichtlich mit ganz ähnlichen Instrumenten angegriffen worden sind um das Jahr 2012 herum.

Zeuge Martin Schallbruch: Ich glaube, der Vorgang ist eingestuft, oder?

(Der Zeuge wendet sich an Vertreter der Bundesregierung)

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Er stand auf *Spiegel Online.*

MR Torsten Akmann (BMI): Sie können da, wenn Sie da was zu wissen, abstrakt was zu sagen. Sonst ist er eingestuft, in der Tat.

Zeuge Martin Schallbruch: Ich kann jedenfalls - - Abstrakt kann ich sagen, dass mir in der Tat neben dem Belgacom-Fall andere Fälle zur Kenntnis gebracht worden sind, wo vergleichbare Angriffstechniken verwendet wurden, weil das auch eine der Tätigkeiten des BSI war, sich anzuschauen: „Mit welchen Angriffswerkzeugen wurden unter Ausnutzung welcher Angriffsvektoren dort welche Ergebnisse erzielt?“, weil das natürlich für die Schutzaufgabe des BSI von besondere Bedeutung war. Und da gab es eben auch andere Fälle, bei denen vergleichbare Angriffswerkzeuge mir zur Kenntnis gegeben wurden.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Genau. - Also, es heißt ja - ich kann es - - ich weiß es ja auch nicht, aber ich habe das jetzt so wahrgenommen im Nachhinein -, dass eben in beiden Fällen Regin eine Rolle spielt. Und diese Software ist ja irgendwie zuordnenbar nach den Snowden-Unterlagen, und zwar als Software, als Instrument des GCHQ. Und deswegen frage ich mich sozusagen: Ab welchem Zeitpunkt ist man von Bundesregierungsseite ausgegangen - ich sage es mal überspitzt -: „Der Feind in meinem Bett“? Also, ab wann hat man so überlegt, dass vielleicht die Leute, mit denen man sehr eng kooperiert, vielleicht auch Teil des Sicherheitsproblems sind, das man hat? Und was bedeutet das eigentlich in der Konsequenz für die Kooperationen, die man laufen hat?

40) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.

41) Richtigstellung des Zeugen: "[einfügen „:“]", siehe Anlage 2.

Ja, jetzt bin ich der Erste, der irgendwie so Zwänge und so auch versteht. Aber hat man das nicht an irgendeiner Stelle dann auch diskutiert?

Vorsitzender Dr. Patrick Sensburg: Dazu die Bundesregierung. Herr Akmann.

MR Torsten Akmann (BMI): Vielen Dank, Herr Vorsitzender. - Ich will nicht groß unterbrechen. Wenn es darum geht, wer es war: Das ein eingestufter Vorgang. Der kann nur in nichtöffentlicher Sitzung hier behandelt werden. - Danke.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wer was war? Regin jetzt?

(MR Torsten Akmann (BMI): Ja, Sie hatten vorhin schon mal danach gefragt!)

- Ja, ich habe ja diese *Intercept*-Folie vorgelegt. Da steht, dass das der GCHQ war. Das ist eine öffentliche Folie. Soll ich die jetzt noch - - Wir haben eine Folie für Sie, Herr Schallbruch.

Vorsitzender Dr. Patrick Sensburg: Die Folie können wir vorlegen. Nur den Sachverhalt können wir daran nicht diskutieren.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Bitte?

Vorsitzender Dr. Patrick Sensburg: Die Folie können wir natürlich vorlegen. Aber den Sachverhalt können wir danach nicht diskutieren, weil der eingestuft ist.

(Dem Zeugen werden Unterlagen vorgelegt)

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also, das hat der *Intercept* am 13.12.2014 veröffentlicht. Das liegt außerhalb unseres Untersuchungszeitraums, ist aber nur die Veröffentlichung. Die Folie ist natürlich älter.

Zeuge Martin Schallbruch: Also, ich kenne das Dokument nicht und kann es, ehrlich gesagt, auch nicht wirklich beurteilen, ob dieses Dokument irgendetwas beweist. Ich will aber versuchen, Ihre Frage zu beantworten.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Martin Schallbruch: Ich persönlich bin seit der Veröffentlichung der Snowden-Folien davon ausgegangen, dass man es nicht ausschließen kann, dass andere Nachrichtendienste auch aus den Five-Eyes-Staaten, aber auch andere Nachrichtendienste - die Snowden-Folien sind ja auch eine Anleitung für Nachrichtendienste - derartige Angriffe auf unsere Regierungsnetze durchführen, dass man es nicht ausschließen kann. Insofern habe ich versucht und da auch sehr viel Zeit drauf verwandt, die Maßnahmen zum Schutz der Infrastrukturen in Deutschland so zu erweitern, dass man auch diese Art Angriffe abwehren kann und dass man darauf vernünftig vorbereitet ist.

Ich habe mich nicht mit der Frage beschäftigt, weil ich nicht zuständig war und dazu auch keine eigenen Quellen hatte: Wie wahrscheinlich ist es denn tatsächlich, dass solche Angriffe von einem bestimmten Urheber kommen?

Was die Kooperation angeht, so ist die Kooperation mit den Vereinigten Staaten oder mit unseren europäischen Partnern im Bereich der Cybersicherheit von großer Bedeutung. Wir tauschen dort Informationen aus über sehr schwerwiegende Fälle auch von beispielsweise Wirtschaftsspionage, bei denen wir ganz andere Vermutungen haben, was der Urheber sein könnte, aber auch das in der Regel nicht beweisen können. Und diese Kooperation habe ich - und da bin ich seit der Veröffentlichung der Snowden-Folien natürlich noch ein bisschen misstrauischer - nicht bezogen auf Art und Umfang der Sicherheitsmaßnahmen, die wir in unseren Infrastrukturen betreiben. Wir haben schon seit Veröffentlichung der Snowden-Unterlagen eine sehr viel nationalere Beschaffung und Kryptopolitik betrieben als vorher.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das verstehe ich. Und Sie sind ja jetzt

sozusagen fürs BMI hier. Wir haben aber die letzten Monate eben sehr viel auch im Hinblick auf den Bundesnachrichtendienst diskutiert. Und was ich mich eben immer frage, ist, ob es da nicht einen Widerspruch gibt zwischen der Kooperation und dem Datenaustausch und dem gemeinsamen An-die-Glasfaser-Gehen und ebendiesem Grundvertrauen, was es dafür eigentlich braucht.

Ich würde auch immer zustimmen: Es braucht eigentlich internationale Kooperationen in solchen Fragen, und so bin ich ein total pragmatischer Mensch. Aber wenn so eine Zäsur da eintritt und man feststellt, ich sage jetzt mal - da können Sie vielleicht auch noch was zu sagen -, dass man eben bei der Software XKeyscore, die man einsetzt, bis heute offensichtlich nicht sicher ist, ob das nicht ein gigantomanisches Trojanerprogramm ist und man das bis heute irgendwie prüft, obwohl es jahrelang in Deutschland eingesetzt wurde von deutschen Nachrichtendiensten - - Ich meine, das ist doch irgendwie eine krasse Geschichte. Und deswegen - -

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir in der Zeit noch eine krasse Antwort hinkriegen, bevor die Zeit abgelaufen ist.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, ich müsste in der Zeit erst mal eine Frage hinbekommen.

Vorsitzender Dr. Patrick Sensburg: Ich fand die schon gut bis jetzt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja. - Antworten Sie doch einfach spontan, was Ihnen dazu einfällt, Herr Schallbruch.

(Heiterkeit)

Zeuge Martin Schallbruch: Als Erstes: XKeyscore kenne ich nicht.

Zweitens. Die Frage, mit welchen Staaten man kooperiert, ist zunächst mal eine politische Frage. Und die Kooperation mit den Vereinigten Staaten von Amerika auf dem Feld der Cybersicherheit war politisch erwünscht und gefördert, und ich habe da auch zugeraten, das zu tun, weil wir da auch wichtige Erkenntnisse ausgetauscht haben. Und aus diesem Grunde habe ich diese Kooperation auch betrieben, aber eben in dem wie eben schon beschriebenen eingeschränkten Maß, dass es immer auch nationale Sicherheitsinteressen gibt, die man dann auch mit Kooperationspartnern nicht teilen kann.

Vorsitzender Dr. Patrick Sensburg: Okay. - Jetzt kommen wir zur zweiten Runde. Es beginnt wieder die Fraktion der CDU/CSU. Der Kollege Wendt.

Marian Wendt (CDU/CSU): Ja, vielen Dank. - Wir haben jetzt verschiedene Bereiche schon abgearbeitet. Es kam vorhin auch das Thema des sogenannten Kanzlerinnenhandys, des Verdachts des Abhörens des Kanzlerinnenhandys. Am 23. Oktober 2013 berichtet ja *Spiegel Online,* dass das Handy der Bundeskanzlerin möglicherweise von der NSA überwacht worden sei. Bereits einen Tag später richtete der Generalbundesanwalt eine Erkenntnisanfrage dazu an den Präsidenten des BSI. Diese Anfrage beantwortete der BSI-Präsident am 8. November gleichen Jahres, es lägen dem BSI keine über die Presseberichterstattungen hinausgehenden Erkenntnisse vor. Ich zitiere:

> Teile der in der Presse dargestellten Erkenntnisse wurden dem BSI jedoch einige Tage vor Veröffentlichung mit der Bitte um Bewertung der Plausibilität zur Verfügung gestellt.

Die Frage: Dieses Schreiben - - Inwieweit waren Sie in diesen Vorgang eingebunden als Fach- und Dienstaufsicht? Ging das Schreiben an den BSI-Präsidenten vom Generalbundesanwalt auch über Ihren Tisch?

Zeuge Martin Schallbruch: Das Schreiben ging nicht über meinen Tisch. Das habe ich aber sicher nachrichtlich bekommen. Ich kenne den Vorgang.

Marian Wendt (CDU/CSU): Okay. - Von wem wurden dem BSI denn die in der Presse dargestellten Erkenntnisse mit der Bitte um Bewertung der Plausibilität zur Verfügung gestellt?

Zeuge Martin Schallbruch: Von mir. Ich habe vom Bundeskanzleramt eine entsprechende Anfrage bekommen mit der Bitte, das BSI zu befassen, die Erkenntnisse zu plausibilisieren, das an das BSI weitergegeben, und das BSI hat dann diese Plausibilisierung vorgenommen.

Marian Wendt (CDU/CSU): Und was war die Antwort an Sie aus Ihrer Erinnerung? Sie müssen das ja dann weitergeleitet haben. Oder was haben Sie als Antwort weitergeleitet?

Zeuge Martin Schallbruch: Nein, ich habe die Antwort - - Also, das BSI hat dann in der Folge unmittelbar mit dem Bundeskanzleramt kommuniziert, weil das BSI einen gesetzlichen Beratungsauftrag gegenüber jeder Bundesbehörde hat, und den jeweiligen Geheimschutzbeauftragten informiert. Ich habe das sozusagen nur vermittelt. Aber die Erkenntnis des BSI war, dass das BSI das für plausibel hält, aber es kein Beleg ist.

Marian Wendt (CDU/CSU): Würden Sie persönlich dieser Meinung, dieser Auffassung auch folgen?

Zeuge Martin Schallbruch: Ja, absolut.

Marian Wendt (CDU/CSU): Okay. - Vor dem Hintergrund der Berichte über das Kanzlerinnenhandy legte das BSI dann mit Datum vom 5. November gleichen Jahres eine allgemein gehaltene Darstellung zu den Angriffsmöglichkeiten auf die mobile Regierungskommunikation unter dem Titel „Bewertung Angriffsvektoren“ vor. Darin werden verschiedene Angriffsmethoden bei mobilen Kommunikationsmitteln analysiert und hinsichtlich technischer Machbarkeit und praktischer Einsatzwahrscheinlichkeit bewertet. Es gibt dazu auch ein Dokument, das wir Ihnen gerne vorlegen wollen. Das ist MAT A BSI-1-6g, Blatt 40 ff. und ist VS-NfD klassifiziert. Ich lasse Ihnen das kurz mal vorlegen.

(Dem Zeugen werden Unterlagen vorgelegt)

Ist Ihnen bekannt?

Zeuge Martin Schallbruch: Das ist mir bekannt.

Marian Wendt (CDU/CSU): Ja. - Was waren - - Also, Sie sind mit diesem Vorgang vertraut auch demzufolge, oder ist Ihnen das nur allgemein bekannt?

Zeuge Martin Schallbruch: Nein, also mit dem Vorgang bin ich vertraut.

Marian Wendt (CDU/CSU): Gut. - Was waren die wesentlichen Ergebnisse dieser BSI-Analyse?

Zeuge Martin Schallbruch: Unmittelbar nach den Berichten über das sogenannte Kanzlerhandy haben wir das BSI gebeten, die Angriffsvektoren, die es für die Überwachung eines Handys gibt, aufzuschreiben und herauszufinden: Welche Angriffsvektoren sozusagen gibt es, und was für Schutzmaßnahmen kann man dann ergreifen?

Das BSI hat dann nach meiner Erinnerung fünf Angriffsvektoren identifiziert, also sozusagen Datennetz, mit IMSI-Catcher, in einem fremden Mobilfunknetz usw., also wie man die Kommunikation, die über ein Handy geführt wird, abgreifen kann, und hat Gegenmaßnahmen vorgeschlagen: Ende-zu-Ende-Verschlüsselung, Indoor-Anlagen, Verzicht auf DECT-Telefonie usw.

Wir haben das dann im Bundesinnenministerium umgewandelt in etwas, was wir, ich glaube, „Schutzprogramm Regierungskommunikation“ nannten - oder so ähnlich. Das heißt, wir haben daraus ein Programm gemacht, was[42] zusätzliche Maßnahmen und auch zusätzliche Investitionen in die Sicherheit der Regierungskommunikation umfasste.

Marian Wendt (CDU/CSU): Und damit war auch sichergestellt, dass alle fünf Vektoren, sage ich mal so, auch abgedeckt waren.

Zeuge Martin Schallbruch: Sicherstellen kann man das nicht. Ich fange mal an mit dem ersten

42) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.

Vektor. Wenn jetzt jemand, der ein Kryptohandy hat, dieses Kryptohandy nicht benutzt, sondern irgendwie über eine offene Leitung kommuniziert oder das Gespräche persönlich führt oder Ähnliches, da kann man mit Technik nichts gegen machen. Oder wenn ich den fünften Vektor nehme, den Zugriff auf Geräte in ausländischen Mobilfunknetzen: Können wir auch nur sehr schwer beeinflussen.

Insofern sind das alles risikoreduzierende Maßnahmen gewesen, die wir da vorgeschlagen haben und die dann auch gebilligt worden sind.

Marian Wendt (CDU/CSU): Sie haben dann eine Analyse vorgelegt. Gab es aufgrund der Analyse auch einen Maßnahmenplan? Sie hatten das ja vorhin skizziert: Es gab es dann mehr Kryptohandys. Das ist ja auch immer die Frage, die sich mir stellt: Umgang damit. Wurde das auch genutzt aus Ihrer Sicht heraus?

Der Mensch ist ja das Hauptproblem, wenn es um Fragen der IT-Sicherheit immer wieder geht - natürlich, klar. Er muss die Dinge auch nutzen, und eine hundertprozentige Sicherheit gibt es ja nicht; das ist uns auch klar. Wir versuchen, uns diesen 100 irgendwo anzunähern durch verschiedene Maßnahmen. Inwieweit hat das, sage ich mal, so zu einem Veränderungsprozess innerhalb der Bundesregierung geführt von Mitarbeitern?

Wir haben das auch im Bundestag selber; da nehme ich uns auch nicht aus. Klar, man ist manchmal leichtsinnig mit gewissen Sachen, sicherlich auch mit Passwörtern und Ähnlichem, was es alles gibt. Inwieweit würden Sie sagen - - Gab es erst einen Maßnahmenplan konkret? Wie tief sah der aus? Also, sagte der: „Alle Abteilungsleiter kriegen ein Kryptohandy oder bestimmte Bereiche“? Wie tief ging das ungefähr? Und wie ist dann der Erfolg gewesen aus Ihrer Sicht?

Zeuge Martin Schallbruch: Es gab einen Maßnahmenplan, den das Bundesinnenministerium gemacht hat, der dann irgendwo um den Zeitraum November/Dezember 2013 herum vom damaligen Minister gebilligt wurde, auch zusätzliche Investitionen vorsah, der aber im Wesentlichen die Bereitstellung zusätzlicher Geräte, Server, Indoor-Anlagen oder Ähnliches vorsah. Allerdings liegt es in der Verantwortung der Ressorts und der einzelnen Behörden, festzulegen, welche Bediensteten solche Geräte bekommen. Das ist nichts, was das BMI zentral machen kann, sondern das muss dezentral entschieden werden. Es gibt Behörden, in denen also bis runter Referatsleiterebene alle solche Geräte haben, völlig egal, wo sie arbeiten. Und es gibt andere, wo nur in wesentlichen sicherheitsrelevanten Bereichen Kryptogeräte eingesetzt werden.

Die Nutzung ist dann noch mal eine andere Frage. Ich habe wahrgenommen, dass wir in den Jahren 2007 bis 2012, in denen wir uns bemüht haben, sichere Smartphones, sage ich mal, an die Frau und an den Mann zu bringen, einen ziemlichen Gegenwind hatten. Aus den Ressorts gab es immerzu Aussagen wie: „Das funktioniert nicht so gut wie ein iPhone, die Akkulaufzeit ist zu gering, es ist zu umständlich und usw. usf.“, was in der Tat so ist bei speziell abgesicherten Geräten. Dieser starke Widerstand ist nach 2013, glaube ich, ein Stück weit gewichen, und wir haben jetzt doch eine höhere Akzeptanz für gesicherte Kryptogeräte.

Marian Wendt (CDU/CSU): In der gleichen Analyse, die mir vorliegt, wird auch zu möglichen Angriffsmöglichkeiten, speziell zur Platzierung von passiven Empfangsantennen, sich geäußert. Ich darf zitieren:

> Diese Angriffsmethode wird als sehr wahrscheinlich angesehen.
>
> Begründung:
>
> Mit verborgenen Richtantennen an wenigen zentral gelegenen Standorten (z. B. ausländischen Botschaften) kann die Mobilkommunikation in Berlin-Mitte nahezu flächendeckend massenhaft abgehört werden. Die gezielte Überwachung ausgewählter Personen ist bei Kenntnis der Mobilfunknummer möglich, ohne dass dies messtechnisch nachweisbar wäre.

Ende des Zitats.

Die Analyse erinnert ja an die immer wiederkehrenden Berichte über auffällige Aufbauten auf den Botschaftsgebäuden Russlands, Großbritanniens, USA usw. Und dazu heißt es weiter in dem Bericht - Zitat -:

> Insbesondere in der Nähe von Orten mit hoher Aufenthaltswahrscheinlichkeit ...

von Regierungsvertretern

> (BK-Amt, Bundestag)

- obwohl der Bundestag natürlich keine Regierungsvertretung ist, möchte ich anmerken -

> und der Nähe zu exterritorialen Gebäuden ist der Einsatz eines Breitbandempfängers eine Angriffmethode, die … keinerlei Spuren hinterlässt, … nahezu nicht nachweisbar zu installieren ist und … eine hohe Mitschnittquote aufweist.

War Ihnen, der Sie mit der Fachaufsicht über das BSI betraut waren, das Ausmaß bekannt vorher schon?

Zeuge Martin Schallbruch: Die Möglichkeiten waren ja immer schon bekannt, ja, bestimmt schon seit 2002/2003, schätze ich mal, und hat auch immer Eingang gefunden in unsere Argumentation gegenüber den Ressorts. Sie haben eben gefragt nach der Veranstaltung für den Chef des Bundeskanzleramts im Mai 2006.

Marian Wendt (CDU/CSU): Genau.

Zeuge Martin Schallbruch: Da wurde das auch vorgetragen, und eine der Folgen war beispielsweise, dass wir dann Sensibilisierungsveranstaltungen durchgeführt haben, zum Beispiel für Büroleiter von Ministern und Ähnliches, um darauf hinzuweisen, dass, wenn man mit ungeschützten Telefonen kommuniziert, dann nicht ausgeschlossen werden kann, dass durch eine passive Empfangseinrichtung - sei es irgendwo stationär oder auch eine mobile Einrichtung - diese Kommunikation mitgeschnitten werden kann. Diese Möglichkeit war mir bekannt, und jeder, der kein Kryptotelefon einsetzt, muss eben damit rechnen, dass diese Möglichkeit besteht.

Marian Wendt (CDU/CSU): Also, das ist interessant, weil diese gleiche Analyse - - Wir hatten ja schon verschiedene Zeugen sitzen. Auch das BfV zum Beispiel kommt natürlich zu den gleichen Bewertungen. Wenn Sie sagen, Sie haben bereits seit 2002/2003 darauf hingewiesen, und als Sie eben ausführten, zwischen 2007 und 2012 war man wenig offen für die verbesserte Sicherung der Kommunikation, dann gibt einem das natürlich schon zu bedenken und Fragestellungen einfach, ja. Hat Sie das nicht demotiviert, -

Zeuge Martin Schallbruch: Na ja.

Marian Wendt (CDU/CSU): - wenn Sie natürlich wissen, die Gefahren bestehen und es wird nicht so recht auf Sie gehört?

Zeuge Martin Schallbruch: „Demotiviert“ ist in dem Zusammenhang keine Kategorie, die ich irgendwie relevant finde, sondern mich hat das dazu motiviert, das Bemühen zu verstärken, auch vernünftige Lösungen anzubieten. Ich habe mich sehr intensiv um die Weiterentwicklung von sicheren Smartphones beispielsweise gekümmert, damit die Akzeptanz vergrößert werden kann, weil man schon sagen muss: Die Nutzung von Sicherheitseinrichtungen erreicht man nur dann, wenn ein Stück weit Einsicht da ist und wenn auch irgendwas zur Verfügung steht, was auch alltagstauglich ist. Und wenn man als viel beschäftigter Beamter, Politiker ständig kommunizieren muss, dann muss man auch ein vernünftiges Gerät im Einsatz haben, und die Sicherheitslösungen sind eben mit Komforteinbußen verbunden. Insofern war meine Motivation mehr, in diese Richtung da noch besser zu werden.

Marian Wendt (CDU/CSU): Also kann man schon sagen, dass Ihre Warnungen schon - - also dass man nicht sagen kann, dass erst in der Bundesregierung der erste Gedanke kam mit Herrn Snowden: „Oh, wir müssen jetzt was für die IT-

Sicherheit und den nachrichtendienstlichen Abgriff tun“, sondern den Fachleuten und vielen Ebenen war schon vorher weit bekannt, und Snowden war vielleicht noch mal dieser öffentliche Aufschrei, sage ich mal so, mehr nicht, so eine Art letzter Anstoß. Oder wie kann man das vielleicht urteilen?

Zeuge Martin Schallbruch: Genau so würde ich das beschreiben.

Marian Wendt (CDU/CSU): Ja, okay. - Ich habe meinen letzten Bereich. Herr Vorsitzender, wir müssen da ja wieder weiter. - Die Bundesregierung hat ja - Sie haben es auch beschrieben - in den letzten Jahren sowohl auf nationaler als auch auf internationaler Ebene viel für den Schutz der Privatsphäre bewegt. Es ist unter anderem auf deutsche Initiative zurückzuführen, dass mehrere VN-Resolutionen verabschiedet und das Mandat eines VN-Sonderberichterstatters für das Recht auf Privatsphäre geschaffen wurde. Wie würden Sie das beurteilen, die Ergebnisse dessen, die Initiativen? Und wo wurden wirklich echte Verbesserungen erreicht?

Zeuge Martin Schallbruch: Das liegt ganz überwiegend außerhalb meiner Zuständigkeit.

Marian Wendt (CDU/CSU): Okay.

Zeuge Martin Schallbruch: Ich habe nur zugeliefert, was die deutschen Vorschläge angeht, weil ich überzeugt war und auch durch eigene Aktivitäten auf internationaler Ebene mich dafür eingesetzt habe, dass wir zu stärkeren globalen Standards für vertrauenswürdige Informationstechnik kommen müssen, die sicherstellen, dass wir auch ein offenes, benutzbares, innovationsoffenes, freies Internet auf Dauer erhalten können. Also, an diesen Initiativen habe ich mich mit meiner Abteilung eigentlich immer beteiligt, aber das war typischerweise nicht in meiner Federführung.

Marian Wendt (CDU/CSU): Okay, gut. - Dann danke ich Ihnen. Die Unionsfraktion hat dann erst mal keine weiteren Fragen. Wir danken für die Befragung und sehen uns sicherlich an der einen oder anderen Stelle zum Thema „IT-Sicherheit“ bestimmt wieder.

Vorsitzender Dr. Patrick Sensburg: Danke schön. - Dann kommen wir jetzt zur nächsten Fraktion, der Fraktion Die Linke, und Frau Kollegin Renner stellt die Fragen.

(Martina Renner (DIE LINKE): Wir haben erst mal keine weiteren Fragen mehr!)

- Herzlichen Dank. - Dann kommen wir zur Fraktion der SPD.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Die SPD hat auch keine Fragen!)

Herr Kollege?

(Christian Flisek (SPD): Keine Fragen!)

Dann sind wir bei der Fraktion Bündnis 90/Die Grünen, und der Kollege Ströbele hat noch Fragen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. - Herr Schallbruch, benutzen Sie eigentlich ein Kryptohandy immer?

Zeuge Martin Schallbruch: Ich habe immer ein Kryptohandy benutzt in der Zeit, in der ich im BMI tätig war, für meine dienstlichen Geschäfte, und jetzt als Wissenschaftler an der Hochschule wird mir kein Kryptohandy zur Verfügung gestellt.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und wenn Sie sich umgeschaut haben im Bundesinnenministerium: Was schätzen Sie, wie viel Prozent sind Ihrem Rat gefolgt?

Zeuge Martin Schallbruch: Ich kann da keine Schätzung abgeben. Ich weiß nur, dass wir im Bundesinnenministerium doch eine hohe Anzahl

Kryptohandys - ich glaube, 200 bis 250 - ausgegeben haben und dass ich auch wichtige Kommunikation - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): 250 im Innenministerum.

Zeuge Martin Schallbruch: In der Größenordnung - - und dass ich auch meine wesentlichen Kommunikationspartner in der Tat auch darüber erreichen konnte.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. - Haben Sie nur ein Kryptohandy gehabt, oder haben Sie auch bestimmte Gespräche mit dem normalen Handy oder mit einem Nicht-Kryptohandy geführt?

Zeuge Martin Schallbruch: Das Gerät, was[43] im BMI im Einsatz war und auch in anderen Bundesministerien - es gibt da verschiedene Linien -, ist ein abgesichertes Smartphone, was[44] mein einziges dienstliches Gerät war, mit dem also die Kommunikation der E-Mails, also zum Beispiel der Zugriff auf die dienstlichen E-Mails, auf den dienstlichen Kalender, auf die dienstlichen Adressen, immer verschlüsselt ist und mit dem auch dienstliche Gespräche kryptiert geführt werden konnten, ich aber auch in der Lage war, ein Gespräch mit einem Partner, der kein Kryptogerät hat, offen zu führen. Insofern ist das kein Gerät, was[45] nur kryptiert kommunizieren kann, sondern das können Sie für alle Zwecke einsetzen. Und wenn Sie dann eben eine kryptierte Kommunikation führen wollen, dann können Sie dieses Gerät eben, wenn Ihr Partner auch so ein Gerät hat, dafür benutzen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, das war aber nicht meine Frage. Meine Frage war eigentlich, ob Sie daneben auch ein anderes Handy, also normal oder jedenfalls nicht Krypto - - Weil wir wissen ja von der Kanzerin - jedenfalls liest man das in der Zeitung -, dass sie auch ein Kryptohandy hat, und trotzdem hat sie mit dem Nicht-Kryptohandy telefoniert.

(Dr. André Hahn (DIE LINKE): Ja, das ist das Problem!)

Zeuge Martin Schallbruch: Da ich mit dem dienstlichen Gerät keine privaten Gespräche führen kann, habe ich natürlich auch ein privates Gerät gehabt.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ah ja. - Und gibt es da fließende Grenzen, also vom Inhalt, was Sie da kommunizieren?

Zeuge Martin Schallbruch: Die Kryptogeräte oder die Kryptokommunikation ist ja für die Fälle notwendig, in denen man VS-NfD-Inhalte austauscht.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Martin Schallbruch: Es ist ja nicht für jedes dienstliche Gespräch so, dass man kryptiert kommunizieren muss. Und insofern ist, sagen wir mal, eigentlich die Bedeutung - - Oder man weiß eigentlich in der Regel, was ein bedeutendes Gespräch ist, was[46] man dann eben auch kryptiert führen sollte.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, aber wir haben ja gehört, der Mensch ist das Problem. Ihr Rat, Kryptohandys - - oder Ende-zu-Ende zu verschlüsseln, gilt doch für alle, oder nur für Sie und das Bundesinnenministerium?

Zeuge Martin Schallbruch: Das gilt für alle, und ich kann nur das aufnehmen, was Sie gesagt haben: Der Menschen ist das Problem. Wir wissen alle, dass viele Leute unkryptiert kommunizieren und dass wir - -

43) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.
44) Richtigstellung des Zeugen: "[statt „was“ „Es war“]", siehe Anlage 2.
45) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.
46) Richtigstellung des Zeugen: "[„das“ statt „was“]", siehe Anlage 2.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, wahrscheinlich 99 Prozent.

Zeuge Martin Schallbruch: Wahrscheinlich 99 Prozent. - Und jedes kryptiert geführte Gespräch und jede kryptierte E-Mail sind eine Verbesserung. Insofern kann man die IT-Sicherheit sehr einfach verbessern, indem man nämlich in der tagtäglichen Benutzung öfter auf kryptierte Kommunikation zurückgreift.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und wie viele waren das jetzt für die ganze Bundesregierung? Gehört bei den Bundesorganen auch der Bundestag dazu?

Zeuge Martin Schallbruch: Nein, der Bundestag ist bei der Beschaffung seiner Informationstechnik selbstständig. Ich weiß nicht, ob der Bundestag solche Geräte beschafft hat. Er kann die Rahmenverträge nutzen, die die Bundesregierung geschlossen hat für den gesamten Bund. Der Bund hat aus dem IT-Investitionsprogramm im Zeitraum 2009 bis 2011, ich glaube, ungefähr 5 000 Kryptosmartphones und 4 500 Kryptotelefone beschafft und an Bundesbehörden ausgegeben.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Weil, ich meine, ich halte mich ja häufig hier im Bundestag auf, und wenn ich die Kollegen sehe, habe ich eigentlich noch nie einen mit einem Kryptohandy telefonieren sehen.

Zeuge Martin Schallbruch: Ja, aber das, Herr Abgeordneter, liegt möglicherweise daran, dass man die Geräte nicht mehr unbedingt erkennt. Also, das aktuell verbreitetste Gerät -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Sie können ja mal hier rumgucken.

Zeuge Martin Schallbruch: - aus der Blackberry-X10-Reihe sieht nicht viel anders aus wie so ein Samsung oder iPhone. Also, das würden Sie jetzt auf die Entfernung - - Wenn es bei mir hier läge, würden Sie nicht erkennen, ob das ein solches Gerät ist oder ein anderes.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Jetzt habe ich noch eine andere Frage. Waren Sie auch befasst mit der Sicherheit von Daten, die nach außen an ausländische, also an andere Staaten, an fremde Mächte weitergegeben werden?

Zeuge Martin Schallbruch: Nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Das war nicht Ihr Gebiet.

Zeuge Martin Schallbruch: Das war nicht mein Gebiet.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Also dass die sicher sind und so oder dass - -

Zeuge Martin Schallbruch: Damit war ich nicht befasst, nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Okay. - Danke.

Vorsitzender Dr. Patrick Sensburg: So, jetzt schaue ich mal in die Runde. Das würde genau passen von der Zeit. Wenn im öffentlichen Teil keine Fragen mehr sind, dann können wir noch schnell einen Beschluss fassen und dann dann zur Abstimmung gehen. Ich schlage folgenden Beschluss vor:

Für die weitere Vernehmung des Zeugen Schallbruch am heutigen Tag wird die Öffentlichkeit gemäß § 14 Absatz 1 Nummer 4 des Untersuchungsausschussgesetzes ausgeschlossen, weil besondere Gründe des Wohls des Bundes entgegenstehen.

Wer dem so zustimmen kann, den bitte ich um das Handzeichen. - Herzlichen Dank. Gegenstimmen? - Enthaltungen?

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wollen wir ihn Geheim hören? - Martina Renner (DIE LINKE): Ihn nicht! - Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ihn nicht!)

- Will ihn keiner Geheim hören? Eingestuft? - Nein? - Dann ist der Beschluss trotzdem schön, rechtlich richtig, aber wird nicht umgesetzt. Mit anderen Worten: Ich bedanke mich bei Ihnen ganz herzlich dafür, dass Sie uns Rede und Antwort gestanden haben, so gut und so offen, dass wir anscheinend keine nichtöffentliche oder eingestufte Sitzung mehr brauchen, und wünsche Ihnen einen schönen Nachmittag. Danke, dass Sie bei uns waren.

Die Sitzung ist unterbrochen für die nächste namentliche Abstimmung. Wir sehen uns dann im üblichen Sitzungssaal für nichtöffentlich oder Geheim wieder.

An die Öffentlichkeit: Ganz herzlichen Dank, dass Sie bei uns waren. Die nächsten Zeugen werden nichtöffentlich vernommen. Damit ist für Sie bei ungefähr 30 Grad draußen jetzt Feierabend. Wir machen hier in gekühlten Räumen noch ein bisschen weiter. Danke, dass Sie da waren. Schönen Feierabend für Sie!

Bei uns geht es gleich nach Umzug weiter im üblichen Sitzungssaal mit dem Zeugen Dr. Even.

(Schluss des Sitzungsteils Zeugenvernehmung, öffentlich: 18.12 Uhr - Folgt Sitzungsteil Zeugenvernehmung, Geheim)

ANLAGE 1

Mitarbeiter16 PA25

Von:	Könen, Andreas <[redacted]@bsi.bund.de>
Gesendet:	Mittwoch, 13. Juli 2016 12:56
An:	Georgii Harald PA25
Cc:	PA25 1.Untersuchungsausschuss 18.WP Postfachaccount PA25; [redacted] GPUntersuchungsausschuss
Betreff:	Korrektur des Stenographischen Protokolls der 104. Sitzung, öffentlicher Teil

Sehr geehrter Herr Georgii,

nach Durchsicht des Stenographischen Protokolls der 104. Sitzung, öffentlicher Teil, möchte ich Ihnen wie telefonisch angekündigt, lediglich eine Ergänzung meinerseits mitteilen:

Auf der Seite 26, linke Spalte, findet sich im 2. Absatz eine Stelle meiner Aussage, die für die Stenographen unverständlich blieb. Dies möchte ich in folgender Weise ergänzen:
" ... in Handlungsanweisungen für ITSiBes, also Informationssicherheitsbeauftragte, ..."

Weitere Korrekturwünsche habe ich nicht, den nicht-öffentlichen Teil kommentiere ich in einer weiteren Email.

Mit freundlichen Grüßen

Andreas Könen

Bundesamt für Sicherheit in der Informationstechnik (BSI) Vizepräsident

Godesberger Allee 185 -189
53175 Bonn

Postfach 20 03 63
53133 Bonn

Telefon: +49 (0)228 99 9582 [redacted]
Telefax: +49 (0)228 99 10 9582 [redacted]
E-Mail [redacted]@bsi.bund.de
Internet:
www.bsi.bund.de
www.bsi-fuer-buerger.de

ANLAGE 2

DSI DIGITAL SOCIETY INSTITUTE BERLIN

esmt ESMT European School of Management and Technology

ESMT GmbH · Schlossplatz 1 · 10178 Berlin

Deutscher Bundestag
1. Untersuchungsausschuss
06. Juli 2016
664 5503-04

Martin Schallbruch
Ministerialdirektor a.D.
Deputy Director of DSI Berlin
Senior Researcher for
Cyber Innovation and Regulation

Phone: +49 30 21231-[redacted]
Fax: +49 30 21231[redacted]
[redacted]@esmt.org

Herrn
Harald Georgii
Leiter Sekretariat PA 25
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

Berlin, 5. Juli 2016

Betr.: Stenografisches Protokoll der 104. Sitzung des 1. Untersuchungsausschusses
hier: Korrekturen und Ergänzungen

Bezug: Ihr Schreiben – PA 25 – 5503 – vom 28. Juni 2016

Sehr geehrter Herr Georgii,

vielen Dank für die Übersendung des Stenographischen Protokolls. Anbei erhalten Sie meine Korrekturen und Ergänzungen.

Für Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

Martin Schallbruch

ESMT
European School of Management and Technology GmbH
Schlossplatz 1
10178 Berlin
Phone: +49 30 21231-0
Fax: +49 30 21231-9

Branch office
Schloss Gracht
Fritz-Erler-Str. 1
50374 Erftstadt
Phone: +49 2235 405-204
Fax: +49 2235 405-235

Inforaquest@esmt.org
www.esmt.org

Chairman of the Supervisory Board:
Prof. Dr. Clemens Börsig

Managing Directors:
Prof. Jörg Rocholl, PhD (President)
Georg Garlichs (CFO)

Register court:
Berlin-Charlottenburg, HRB 87005
Bank information: Deutsche Bank AG
Acc.: 077 304 400, BC: 100 700 00
IBAN DE91 1007 0000 0077 3044 00
BIC DEUT DEBB

VAT-Id.: DE814050117

18. Wahlperiode

Deutscher Bundestag

1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Nur zur dienstlichen Verwendung

Stenografisches Protokoll
der 104. Sitzung
- vorläufige Fassung* -

1. Untersuchungsausschuss
Berlin, den 23. Juni 2016, 11.30 Uhr
Paul-Löbe-Haus, Europasaal (4.900)
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Prof. Dr. Patrick Sensburg, MdB

Tagesordnung - Öffentliche Beweisaufnahme

Tagesordnungspunkt

* Hinweis:
Die Stenografischen Protokolle über die Vernehmung von Zeugen und Sachverständigen werden grundsätzlich weder vom Ausschuss noch von den jeweiligen Zeugen oder Sachverständigen redigiert bzw. korrigiert. Zeugen und Sachverständigen wird das Stenografische Protokoll über ihre Vernehmung regelmäßig mit der Bemerkung zugesandt, dass sie Gelegenheit haben, binnen zwei Wochen dem Ausschusssekretariat Korrekturwünsche und Ergänzungen mitzuteilen. Etwaige Korrekturen und Ergänzungen werden sodann durch das Sekretariat zum Zwecke der Beifügung zum entsprechenden Protokoll verteilt.

Vorsitzender Dr. Patrick Sensburg: Die unterbrochene Sitzung des 1. Untersuchungsausschusses wird fortgesetzt, und ich darf unseren nächsten Zeugen begrüßen.

Vernehmung des Zeugen Martin Schallbruch

Herr Schallbruch, ich freue mich, dass Sie da sind und dem Ausschuss für viele Fragen sicherlich Rede und Antwort stehen.

Ich stelle fest: Der Zeuge ist ordnungsgemäß geladen. Herr Schallbruch, Sie haben den Erhalt der Ladung am 14. Juni 2016 bestätigt.

Ich habe Sie darauf hinzuweisen, dass die Bundestagsverwaltung eine Tonbandaufnahme der Sitzung fertigt. Diese dient ausschließlich dem Zweck, die stenografische Aufzeichnung der Sitzung zu erleichtern. Die Tonbandaufnahme wird nach Erstellung des Protokolls dann auch gelöscht, und Sie haben 14 Tage Zeit, dann Ergänzungen oder Korrekturen an dem Protokoll vorzunehmen, wenn dies nötig sein sollte. - Haben Sie hierzu Fragen?

Zeuge Martin Schallbruch: Nein, Herr Vorsitzender.

Vorsitzender Dr. Patrick Sensburg: Danke schön. - Herr Schallbruch, vor Ihrer Anhörung habe ich Sie zunächst zu belehren.

Sie sind als Zeuge geladen worden. Als Zeuge sind Sie verpflichtet, die Wahrheit zu sagen. Ihre Aussagen müssen richtig und vollständig sein. Sie dürfen nichts weglassen, was zur Sache gehört, und nichts hinzufügen, was der Wahrheit widerspricht.

Ich habe Sie außerdem auf die möglichen strafrechtlichen Folgen eines Verstoßes gegen die Wahrheitspflicht hinzuweisen. Wer vor dem Untersuchungsausschuss uneidlich falsch aussagt, kann gemäß § 162 in Verbindung mit § 153 des Strafgesetzbuches mit Freiheitsstrafen von drei Monaten bis zu fünf Jahren oder mit Geldstrafe bestraft werden.

Nach § 22 Absatz 2 des Untersuchungsausschussgesetzes können Sie die Auskunft auf solche Fragen verweigern, deren Beantwortung Sie selbst oder Angehörige im Sinne des § 52 Absatz 1 der Strafprozessordnung der Gefahr aussetzen würde, einer Untersuchung nach einem gesetzlich geordneten Verfahren ausgesetzt zu werden. Dies betrifft neben Verfahren wegen einer Straftat oder Ordnungswidrigkeit auch gegebenenfalls Disziplinarverfahren, wenn dies in Betracht kommen sollte.

Sollten Teile Ihrer Aussage aus Gründen des Schutzes von Dienst-, Privat- oder Geschäftsgeheimnissen nur in einer nichtöffentlichen oder eingestuften Sitzung möglich sein, bitte ich Sie um einen Hinweis, damit der Ausschuss dann gegebenenfalls einen Beschluss nach § 14 oder § 15 des Untersuchungsausschussgesetzes fassen kann, also die Sitzung in nichtöffentlicher oder eingestufter Weise fortsetzen kann, sodass man Ihnen dann die entsprechenden Fragen stellen kann und Sie auch dann antworten können. - Haben Sie hierzu Fragen?

Zeuge Martin Schallbruch: Nein, keine Fragen.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Nach diesen notwendigen Vorbemerkungen darf ich Ihnen den geplanten Ablauf noch einmal kurz darstellen. Eingangs habe ich Sie zur Person zu befragen. Zu Beginn der Vernehmung zur Sache haben Sie gemäß § 24 Absatz 4 des Untersuchungsausschussgesetzes die Gelegenheit, zum Beweisthema im Zusammenhang vorzutragen, also ein sogenanntes Eingangsstatement abzugeben. Danach werde ich Ihnen Fragen stellen. Danach erhalten die Fraktionen die Möglichkeit, ihre Fragen zu stellen, immer eine Fraktion nach der anderen mit ihren Mitgliedern.

Wenn keine weiteren Fragen mehr sind, darf ich Sie nun bitten, sich zu Beginn der Ausführungen dem Ausschuss einmal mit Namen, Alter, Beruf und einer ladungsfähigen Anschrift vorzustellen.

Zeuge Martin Schallbruch: Mein Name ist Martin Schallbruch. Ich bin geboren am 30.09.1965 und bin Wissenschaftler und stellvertretender Direktor eines Forschungsinstituts hier in Berlin.

Als ladungsfähige Anschrift können Sie das Bundesministerium des Innern, Alt-Moabit 140 in 10557 Berlin, verwenden.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich frage nur einmal ergänzend - „Wissenschaftler“: Welche Wissenschaft? Weil das ein weites Feld ist.

Zeuge Martin Schallbruch: Ich bin Informatiker, und mein wissenschaftliches Feld ist auf der Schnittstelle von Informationstechnik und Recht.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich hatte es eben gesagt: Wenn Sie dies möchten, hätten Sie zu Anfang die Gelegenheit zu einem sogenannten Eingangsstatement, also im Zusammenhang zum Beweisgegenstand Ausführungen zu machen, ohne dann eben von den Ausschussmitgliedern unterbrochen zu werden. - Wünschen Sie das?

Zeuge Martin Schallbruch: Ja, davon würde ich gerne Gebrauch machen, Herr Vorsitzender.

Vorsitzender Dr. Patrick Sensburg: Dann haben Sie jetzt das Wort.

Zeuge Martin Schallbruch: Ja, vielen Dank. - Herr Vorsitzender! Sehr geehrte Damen und Herren Abgeordnete! Ich habe in dem Untersuchungszeitraum zwischen Februar 2002 und dem Ende des Untersuchungszeitraums im Bundesministerium des Innern die Aufgabe eines IT-Direktors wahrgenommen und einen Stab geleitet, der im Jahre 2008 zu einer Abteilung umgewandelt wurde. Meine Zuständigkeit erstreckte sich auf Fragen der Netzpolitik, der Digitalisierungspolitik, des IT-Einsatzes in der öffentlichen Verwaltung, der IT- und der Cybersicherheit. Bei der IT- und Cybersicherheit kam mir die Rolle der Fachaufsicht über das Bundesamt für Sicherheit in der Informationstechnik zu.

Sie haben mich geladen zum gesamten Untersuchungsgegenstand. Der Untersuchungsauftrag enthält unter anderem die Fragestellung, sehr allgemein zu Strategien und Konzepten zur IT-Sicherheit, speziell gegen Datenabfluss, Stellung zu nehmen, mit dem Schwerpunkt auch auf dem IT-System des Bundes. Deshalb würde ich gerne in meiner Einführungsbemerkung zur IT-Sicherheit und den Maßnahmen, die in diesem Bereich im Untersuchungszeitraum ergriffen worden sind, Stellung nehmen.

Vielleicht eine Vorbemerkung zu der Materie der IT-Sicherheit, wie sie sich in dem gesamten Zeitraum entwickelt hat: Wir haben in diesem Zeitraum eine sehr hochkomplexe, an Komplexität Jahr für Jahr zunehmende Problematik der IT-Sicherheit erlebt. Das kam daher, dass zum einen die Informationstechnik sich weiter ausdifferenziert hat, komplexer ausgestaltet hat: Mobilisierung, Virtualisierung, Produktvielfalt, Vernetzung. Es kommt daher, dass die Qualität der Informationstechnik sich über die letzten 10, 15 Jahre nicht wirklich gebessert hat, also die Qualität der Software- und Hardwareprodukte, dass die Abhängigkeit von Staat, Gesellschaft, Wirtschaft von Informationstechnik im gleichen Zeitraum immens zugenommen hat, dass sich eine komplexe Bedrohungslage entwickelt hat, in der viele Player aus dem Bereich der Kriminalität - Konkurrenzausspähung usw. usf. -, auch nachrichtendienstliche Akteure, militärische Akteure das Thema IT- und Cyberangriffe für sich entdeckt haben.

Die Verantwortung für IT-Sicherheit kann kein Akteur allein herstellen, weder Hersteller von Systemen noch Nutzer noch der Staat. Die Lösung der Probleme der IT-Sicherheit erfordert immer ein Zusammenwirken unterschiedlichster Akteure. Und eines der großen Probleme bei der IT-Sicherheit, mit dem ich im gesamten Zeitraum befasst war, war das Verhältnis zwischen IT-Sicherheit auf der einen und Nutzbarkeit und Innovation auf der anderen Seite. IT-Sicherheit behindert immer ein Stück weit die Nutzbarkeit von Systemen, verlangsamt Innovationen. Ein Smartphone, ~~was~~ das sicher ist, alles kryptiert - das Gerät kryptiert die Verbindungen, kryptiert die Mails -, ist nicht so einfach zu benutzen, nicht so sehr „at a fingertip“, wie das viele Nutzer gewohnt sind.

Hinzu kommt, dass die IT-Sicherheit ein Stück weit immer der Geschwindigkeit der IT-Innovationen hinterherläuft, weil viele Hersteller und Anwender IT-Sicherheit nicht von Anfang an in

die Systeme hineinplanen, sondern IT-Sicherheit zusätzlich hinzugekauft werden muss.

Ich würde gerne speziell zur IT-Sicherheit der Bundesverwaltung ein paar Aussagen machen. Die Behörden des Bundes sind in großem Umfang abhängig von der Funktionsfähigkeit ihrer Informationstechnik. Kaum eine Behörde kann ohne funktionierende Informationstechnik ihre Aufgabe noch wirklich wahrnehmen. Seit etwa dem Jahr 2004 haben wir in der Bundesverwaltung eine stetige Zunahme an Zahl und Art und Komplexität von Angriffen auf die IT-Systeme erlebt: Spam-Angriffe, Denial-of-Service-Attacks, Trojaner, Hackerangriffe usw. usf. Oftmals war und ist auch aus heutiger Sicht nicht ganz erkennbar, wer Ursprung oder Urheber dieser Angriffe war.

In dem Zusammenhang kann ich auch gleich an dieser Stelle sagen, dass mir, was die IT der Bundesverwaltung angeht, kein Fall bekannt geworden ist, der sich eindeutig auf beispielsweise Nachrichtendienste aus den hier in Rede stehenden Five-Eyes-Staaten zurückführen ließe. Die Bundesverwaltung mit ihrer IT bietet zunehmende Angriffsflächen, weil sie mehr IT einsetzt - mobile Geräte, Cloud-Services usw. usf. - und weil der Einsatz der IT immer komplizierter wird.

Für die Sicherheit der IT im Bund wie auch für die IT insgesamt sind grundsätzlich die Ressorts selbst verantwortlich. Das BMI hat für die IT der Bundesverwaltung eine koordinierende Rolle. Das Ergebnis dieser Eigenverantwortung der Ressorts ist eine weit zersplitterte IT-Landschaft des Bundes. 2013 gab es hierzu eine Erhebung: 119 Rechenzentren, über 1 200 Serverräume, 40 unterschiedliche Netze. Im Hinblick auf die IT-Sicherheit führt das zu unterschiedlichen IT-Sicherheitsvorkehrungen in den einzelnen Behörden, die nur dort einheitlich sind, wo sie typischerweise einheitlich finanziert sind, zum Beispiel - prominentestes Beispiel vielleicht - bei den Regierungsnetzen, IVBB und anderen Regierungsnetzen, die ressortübergreifend vom BMI bereitgestellt werden.

Es hat im gesamten Untersuchungszeitraum einen immerwährenden Druck des BMI auf die Bundesministerien gegeben, mehr für die Sicherheit in ihren Behörden zu tun auf allen Ebenen. Es gab zu diesem Thema Kabinettsbefassungen, Staatssekretärsbesprechungen, diverse Sensibilisierungsveranstaltungen, Präsentationen in Staatssekretärsrunden, und in praktisch jeder Sitzung des Rats der IT-Beauftragten der Bundesministerien wurden Fragen der IT-Sicherheit seit Anfang 2008 adressiert.

Lassen Sie mich nun die wesentlichen Maßnahmen im Untersuchungszeitraum zur IT-Sicherheit aufzählen. Ich möchte fünf Maßnahmenbereiche nennen:

Erstens. Auf der politisch-strategischen Ebene hat die Bundesregierung im Jahre 2005 mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen eine erste IT-Sicherheitsstrategie vorgelegt, die die Bundesverwaltung betraf, aber darüber hinaus auch Fragen der Internetsicherheit, Erweiterung der Aufgaben des BSI, Technologiepolitik. Dieser nationale Plan war auch Beginn einer engeren Zusammenarbeit mit Unternehmen im Bereich der kritischen Infrastruktur. 2009 wurde das BSI-Gesetz novelliert, und das BSI erhielt zusätzliche Befugnisse für die Kontrolle der Sicherheit der IT des Bundes, aber auch zusätzliche Aufgaben im Bereich der Unterstützung von Unternehmen und Warnung der Bürger.

Im Jahre 2011 wurde die bis heute gültige Cyber-Sicherheitsstrategie des Bundes beschlossen, die ressortübergreifend zustande gekommen ist und als wesentliches Umsetzungsgremium einen Cyber-Sicherheitsrat eingerichtet hat, den es seit 2011 gibt, in dem diese Fragen ressortübergreifend auf Staatssekretärsebene und auch mit der Wirtschaft diskutiert werden. Die Cyber-Sicherheitsstrategie 2011 hat einen sehr starken Fokus auf die Sicherheit der kritischen Infrastrukturen gelegt.

Zweiter Maßnahmenbereich: die Sicherheit der IT des Bundes. Vor 2007/2008 gab es keine ressortübergreifenden Vorgaben für die IT-Sicherheit der Bundesbehörden, nur Empfehlungen von

BSI und BMI. Im Jahre 2007 hat das Bundeskabinett den sogenannten Umsetzungsplan Bund beschlossen, eine erste verbindliche IT-Sicherheitsleitlinie für alle Bundesbehörden. Damit wurden in jeder Behörde ein IT-Sicherheitsmanagement eingerichtet, Sicherheitsbeauftragte benannt, Sicherheitskonzepte erstellt. Seitdem müssen Vorfälle gemeldet werden an das BSI, und es werden jährliche Ampelberichte erstellt.

Mit dem Umbau der IT-Steuerung des Bundes, der Einrichtung eines IT-Rats des Bundes und der Einrichtung eines Beauftragten für Informationstechnik im BMI wurde ab 2008 dann die Möglichkeit geschaffen, dass auf ressortübergreifender Ebene auch Beschlüsse gefasst werden zur IT-Sicherheit im IT-Rat. Und es gab da, wie ich eben schon erwähnt habe, in den zweimonatlichen Sitzungen praktisch jede Sitzung die Thematisierung von Sicherheitsthemen. Es gab auch zu verschiedenen Sicherheitsvorfällen Sondersitzungen.

Ein Kernthema der IT-Sicherheit des Bundes war im gesamten Zeitraum die Sicherheit der Regierungsnetze. Die zentrale Infrastruktur IVBB für die Bundesregierung wurde permanent erweitert und gehärtet. Immer dann, wenn praktisch neue technische Angriffsformen bekannt wurden, wurde der IVBB vom BSI entsprechend geprüft, und wir haben dann sehr häufig als BMI eine Nachbeauftragung gemacht, um zusätzliche Sicherheitsmaßnahmen zu ergreifen. Seit 2009 hat das BSI auf Basis des novellierten Gesetzes dann automatische Schadsoftware-Erkennungssysteme installiert, die auch Datenabflüsse unter anderem verhindern.

Auch dank des Drucks des Haushaltsausschusses des Deutschen Bundestages gibt es seit 2011 eine Konsolidierung der Netze in eine gemeinsame Netzplattform, sodass alle Bundesbehörden - nicht nur die an den IVBB angeschlossenen Bundesbehörden - auf das gleiche hohe Sicherheitsniveau ~~gezogen~~ werden sollen.

Ein weiterer Bereich, den ich, was die Sicherheit der IT des Bundes angeht, erwähnen will, ist die mobile Kommunikation. Spätestens um 2004/05 herum, als die ersten Smartphones in den Einsatz kamen - die ersten Geräte waren Blackberrys, die im Business-Bereich Verbreitung fanden -, gab es eine Beschäftigung des BSI und anderer Sicherheitsbehörden mit Fragen der Sicherheit von mobilen Geräten. Es gab seit 2005 Warnungen an die Bundesressorts, mobile Geräte nicht oder nur eingeschränkt einzusetzen, und wir haben im Hinblick auf die Bedenken, die wir aus technischer Sicht gegen die Architektur der Kommunikation der Geräte hatten, 2007 begonnen, ein sicheres Smartphone zu entwickeln, ~~was~~ der Bundesregierung und auch dem Deutschen Bundestag im Übrigen zur Verfügung gestellt werden sollte. Es gab ab 2007 Pilotprojekte, und zwischen 2009 und 2011 wurden 10 000 Geräte - Smartphones und Kryptotelefone - für den Bund aus zentralen Mitteln beschafft.

Der dritte Maßnahmenbereich, den ich erwähnen möchte, ist die IT-Sicherheit in Wirtschaft und Gesellschaft. Die zunehmenden Angriffe betrafen naturgemäß nicht nur die Verwaltung, sondern, wie Sie den Lageberichten des BSI jährlich entnehmen können, auch Unternehmen und jeden Einzelnen; ich sage nur: Phishing-Attacken. Das BMI hat darauf reagiert durch einen Ausbau vor allen Dingen der BSI-Angebote im Bereich der Beratung, Zertifizierung, Prüfung, Warnung, die Einrichtung eines Bürger-CERTs, aber auch durch eine intensivere Kooperation mit Wirtschaftsunternehmen bei der IT-Sicherheit.

Beginnend mit dem IT-Gipfel, den die Bundeskanzlerin 2006 eingerichtet hat, gab es eine ganze Reihe von solchen Initiativen. Ich möchte nur nennen die Gründung des Vereins „Deutschland sicher im Netz“, mit dessen Hilfe sehr viele Weiterbildungsangebote in Schulen, für den Mittelstand, für bestimmte Gruppen bereitgestellt wurden, Fernsehspots und Ähnliches oder das Anti-Botnet-Beratungszentrum - ~~was auch~~ eine Initiative der Wirtschaft ist, mit Unterstützung des Bundes -, ~~was~~ Betroffenen Hilfe gibt, wenn sie in ein Botnetz geraten.

Oder ich will erwähnen - das hat möglicherweise auch Herr Könen bereits erwähnt - die Allianz für Cyber-Sicherheit, die das BSI gemeinsam mit BDI und BITKOM gegründet hat, die dem Wissens-

transfer, dem Know-how-Austausch über IT-Sicherheit und „Wie kann man Sicherheitsvorfällen begegnen?“ dient.

Ein wesentlicher Bereich, was die IT-Sicherheit in Wirtschaft und Gesellschaft angeht, waren seit jeher die kritischen Infrastrukturen. Seit 2007 gibt es eine institutionalisierte Zusammenarbeit zwischen den Bundesministerien und den kritischen Infrastrukturen im sogenannten Umsetzungsplan KRITIS, mit gemeinsamen Sicherheitsstandards, gemeinsamen Gremien und auch Informationsaustauschen. Das hat beispielsweise dazu geführt, dass auch Unternehmen aus den KRITIS-Branchen an der ersten cyberbezogenen Krisenübung 2011 teilnahmen. Und seit 2012 ist durch weitergehende Assessments, die wir durchgeführt haben im Bereich der kritischen Infrastrukturen, die Vorbereitung getroffen worden für den Entwurf eines IT-Sicherheitsgesetzes, der 2013 ~~dann~~ in das parlamentarische Verfahren ging, wegen der Diskontinuität aber ~~dann ja~~ erst diese Wahlperiode abgeschlossen werden konnte.

Der vierte Maßnahmenbereich, den ich erwähnen möchte, ist der Ausbau der behördlichen Strukturen zur IT-Sicherheit. Das BSI - ich hatte es schon erwähnt - ist in den letzten 15 Jahren ganz erheblich ausgebaut worden: von 250, 300 Mitarbeitern 2002 auf 570, 600 etwa zum Ende des Untersuchungszeitraums. Gleichzeitig hat das BSI die Breite seiner Beschäftigung mit der Thematik erheblich erhöht, was die Techniken angeht, aber auch, was die Anwendungsbereiche angeht, wenn Sie an die Sicherheit von Energienetzen denken, an die Sicherheit im Gesundheitswesen, die Gesundheitstelematik. Das sind alles Themen, die das BSI zusätzlich aufgenommen hat.

Auf deutschen Vorschlag wurde 2002/2003 in Europa eine vergleichbare europäische Einrichtung gegründet, die ENISA. Seit 2009 gibt es ~~ja~~ auch einen deutschen Direktor der ENISA. Die ENISA hat sich sehr intensiv darum bemüht, die Sicherheitsniveaus der EU-Mitgliedstaaten anzugleichen und zum Beispiel CERT-Informationen auszutauschen.

Mit der Cyber-Sicherheitsstrategie 2011 hat sich der Bund dann entschieden, unter Federführung des BSI ein Cyber-Abwehrzentrum einzurichten, in dem alle mit Cyberfragen beschäftigten Sicherheitsbehörden zusammenwirken, um gemeinsame Lagebeurteilungen vorzunehmen und sich über zu treffende Maßnahmen im Rahmen der jeweiligen Zuständigkeiten abzustimmen.

Der fünfte und letzte Maßnahmenbereich, den ich erwähnen möchte, ist die Förderung vertrauenswürdiger Informationstechnik, die Förderung von IT-Sicherheitstechnik. Das ist aus meiner Sicht eine zentrale Fragestellung für präventive IT-Sicherheit. Wir haben in Deutschland eine sehr leistungsstarke, aber eher klein- und mittelständisch geprägte IT-Sicherheitswirtschaft. Wir haben allerdings nur winzige Teile der im praktischen Einsatz befindlichen IT, die tatsächlich auch Sicherheitszertifikate hat, die tatsächlich belastbar geprüft ist. Wir haben eine hohe Abhängigkeit von ausländischen IT-Herstellern und naturgemäß immer die Möglichkeit, dass IT-Produkte, die man einkauft auf dem Weltmarkt, Backdoors enthalten, Schwachstellen enthalten, von geringer Qualität sind.

Hinzu kommt, dass die Technologieentwicklung ganz allgemein im Augenblick sehr stark vom sogenannten Consumer-Markt getrieben ist, das heißt von der schnellen Weiterentwicklung von Geräten für den Endkunden und weniger von der Entwicklung von Technik für Sicherheitsbereiche. Aus diesen Gründen hat das BMI im gesamten Untersuchungszeitraum eine ganze Reihe von Maßnahmen zur Förderung vertrauenswürdiger Informationstechnik durchgeführt. Das BSI hat beispielsweise Entwicklungsprojekte für Kryptogeräte durchgeführt; einige hatte ich schon erwähnt. Wir haben eine intensivere Nachfragebündelung des Bundes und auch Sammelbeschaffung durch das BSI erreicht, sodass durch diese größere Nachfrage auch für die Unternehmen eine stabilere wirtschaftliche Situation erreicht werden kann. Die Unternehmen wurden bei Auslandsvertrieb unterstützt, beispielsweise bei Kryptogeräten in neuen EU-Mitgliedstaaten.

Wir haben uns darum bemüht, bei Vergaben im Bereich der Bundesverwaltung hohe Anforderungen an die IT-Sicherheit zu stellen - im Rahmen

des, ~~sage ich mal~~, europarechtlich Möglichen jeweils -, aber auch die vorhandenen Ausnahmegenehmigungen im europäischen Vergaberecht zu erhalten. Es gab in dem Untersuchungszeitraum mindestens zwei Bemühungen von europäischer Seite, die Ausnahmevorschriften für Sicherheitsvergaben enger zu fassen und uns hier weiter einzuschränken; dagegen haben wir uns regelmäßig auch erfolgreich gewehrt.

Im Rahmen der Novellierung des Außenwirtschaftsgesetzes hat das BMI sich dafür eingesetzt, dass auch Kryptounternehmen unter das Außenwirtschaftsgesetz fallen, und es gab mehrere Fälle, in denen die Übernahme von Unternehmensanteilen durch ausländische Erwerber durch das Bundeswirtschaftsministerium gemeinsam mit dem BMI untersagt oder nur unter Auflagen genehmigt wurde.

Wir haben Initiativen gefördert wie „E-Mail made in Germany“ für den sicheren, verschlüsselten E-Mail-Austausch zwischen deutschen Providern. Es gibt Sicherheitspartnerschaften mit einer ganzen Reihe von IT-Sicherheitsunternehmen, und das BMI hat gemeinsam mit dem BMBF zwei IT-Sicherheitsforschungsprogramme - 2008 und 2013, glaube ich - beschlossen und durchgeführt, mit denen zusätzliche IT-Sicherheitstechnik gefördert wurde.

Ich möchte im abschließenden Teil meiner Eingangsbemerkungen die zusätzlichen Maßnahmen darstellen, die wir nach Veröffentlichung der Snowden-Dokumente durchgeführt haben. Ich möchte persönlich vorwegschicken: Ich habe mir etliche von diesen Dokumenten ~~angeguckt~~ angeschaut - natürlich bei weitem nicht alle, sondern auch nur einen Teil - und habe mir auch Gedanken darüber gemacht und viel darüber gelesen. Mich haben bei diesen Dokumenten die Methodenvielfalt und der Umfang des Einsatzes der Techniken durchaus überrascht, sehr überrascht, auf der anderen Seite aber auch mich darin bestätigt, dass der Einsatz von Kryptotechnologie und vertrauenswürdiger IT ein Schlüssel für sichere und vertrauenswürdige Kommunikation ist, völlig egal, wer der jeweilige Angreifer auf diese Kommunikation ist.

Nach Bekanntwerden der Snowden-Veröffentlichungen haben wir in fünf Bereichen Aktivitäten in meinem Zuständigkeitsbereich entfaltet:

Das ist erstens im Bereich der Aufklärung, dort vor allen Dingen mit der Zielrichtung, die Provider, die vertraglich mit dem Bund gebunden sind, daraufhin zu überprüfen, inwieweit sie mit den Daten so umgehen und mit ihren Verpflichtungen so umgehen, wie es im Vertrag vorgesehen ist. Da wurden die Provider entsprechend angesprochen durch das BMI oder das BSI, je nachdem, wer den Vertrag geführt hat, und es wurden in einzelnen Fällen auch Revisionen durchgeführt. Wir haben durch diese Aufklärungsmaßnahmen keine Erkenntnisse gewinnen können, die belegen, dass es entsprechende Maßnahmen der Five-Eyes-Staaten gegen die jeweiligen deutschen Regierungsnetze gab, die in den Verträgen abgebildet waren.

Wir haben uns zweitens sehr intensiv mit einer weiteren Absicherung der Regierungskommunikation beschäftigt. Das BSI hat die Leitungsverbindungen überprüft. Einige Behörden wurden zusätzlich auf den IVBB geschwenkt. Es wurden zentrale Server für kryptierte Mobilverbindungen aufgesetzt, damit die Nutzer es noch leichter haben, zu kryptieren; sie konnten auch vorher schon kyptiert telefonieren, aber damit es noch ein bisschen einfacher fällt. Es gab Sensibilisierungsveranstaltungen für auch hochrangige Bundesbedienstete und zusätzliche Gerätebeschaffungen von Kryptogerären aus zentralen Mitteln.

Wir haben drittens die Thematik, die in den Snowden-Dokumenten niedergelegt ist, umfassend in den zuständigen Gremien - IT-Rat des Bundes, IT-Planungsrat mit den Ländern und auch Cyber-Sicherheitsrat - diskutiert und mit den jeweiligen Partnern besprochen.

Es gab viertens im September 2013 einen runden Tisch „IT-Sicherheitstechnik“ gemeinsam mit der Wirtschaft, einer ganzen Reihe von Verbänden und Unternehmen - auch andere Ressorts waren daran beteiligt -, wo wir einen Katalog entwickelt haben von weiter zu fördernden Maßnahmen, zum Beispiel Förderung der IT-Konsolidierung im Bund, um dazu einheitlicher nachfragen zu

können, weiterer Ausbau des BSI, neues IT-Sicherheitsforschungsprogramm, Erweiterung der IT-Sicherheit auf neue Anwendungsfelder wie Energy und Health, Programme zur Förderung von der IT-Sicherheit bei KMU. Das waren Ergebnisse dieses runden Tisches.

Und wir haben fünftens im Bereich der vertraglichen und Vergabeentscheidungen zusätzliche Vertragsklauseln aufgenommen in die Musterverträge - EVB-IT - und auch in Einzelverträge mit einzelnen IT-Unternehmen, die ihnen zusätzliche vertragliche Verpflichtungen auferlegten, zu melden, wenn sie ausländischen Nachrichtendiensten Daten übergeben müssen oder wenn sie bestimmten Verpflichtungen unterliegen, damit der Bund dann davon Gebrauch machen kann, zu sagen: Das Unternehmen können wir jetzt nicht mehr weiter beauftragen.

Und wir haben auch in einigen konkreten Vergabeverfahren uns für nationale Lösungen entschieden. Ich selbst habe mich sehr intensiv bemüht, in einer schwierigen Abstimmung mit der EU-Kommission die Vergabe der Netze des Bundes freihändig an einen deutschen Anbieter durchführen zu können und dafür das Plazet der EU-Kommission zu bekommen, was am Ende gelungen ist.

Abschließend möchte ich in wenigen Worten noch einmal zusammenfassen, dass wir in dem gesamten Untersuchungszeitraum eine komplexer gewordene Bedrohungslage erlebt haben, sowohl was Angreifer und Motive angeht als auch vor allen Dingen was Technik und Anwendung der IT angeht, und uns versucht haben, bei der IT-Sicherheitspolitik immer auf das einzustellen, was technisch an Angriffen möglich ist.

Das erforderte immer eine Mischung aus technischen, organisatorischen und rechtlichen Maßnahmen. Zentrale Punkte - auch durchaus umstrittene Punkte immer im Bund -: die stärkere Konsolidierung von Netzen und die Informationstechnik, ein konsequenter Einsatz von Sicherheitstechnik auch durch die Bediensteten, eine engere Zusammenarbeit zwischen Wirtschaft und Staat und zuletzt - das habe ich ja sehr deutlich gemacht - eine sehr starke Förderung von vertrauenswürdiger IT, über die man belastbare Sicherheitsaussagen machen kann. - Vielen Dank.

Stellvertretende Vorsitzende Susanne Mittag: Ja, schönen Dank. - Dann geht es gleich mit der ersten Befragungsrunde los. CDU/CSU, Herr Wendt.

Marian Wendt (CDU/CSU): Ja, vielen Dank, Frau Mittag. - Herr Schallbruch, schönen guten Tag! Willkommen im Ausschuss! Vielen Dank für Ihre Ausführungen - auch noch mal auch grundsätzlicher Art - zur IT-Sicherheit, auch für die nötige Sensibilisierung; das ist ja neben dem konkreten Untersuchungsgegenstand auch ein Thema, mit dem sich der Untersuchungsausschuss und natürlich der Bundestag an sich beschäftigen. Von daher auch vielen Dank meinerseits - - der sich in dem Thema engagiert, für diese grundsätzlichen Ausführungen zur IT-Sicherheit.

Herr Schallbruch, Sie waren ja von 2002 bis zum Februar dieses Jahres IT-Direktor im Bundesinnenministerium. Vielleicht könnten Sie noch mal konkret Ihre Aufgabenstellung darstellen, auch vielleicht gerade im Zeitabriss, wie sich die Aufgabe verändert hat. Zwischen 2002 und 2016 gab es ja nicht nur verschiedene Ereignisse - wie Snowden - politischer Art; es gab verschiedene wechselnde Regierungen auch, die natürlich verschiedene Zielvorgaben hatten, und auch natürlich die Technik war sicherlich eine ganz andere 2002. Vielleicht wenn Sie das noch mal als Abriss Ihrer Aufgabe und auch in dieser Agenda darstellen könnten?

Zeuge Martin Schallbruch: In der Anfangszeit, als der IT-Stab im Bundesinnenministerium gegründet worden ist und ich die Leitung übernommen habe, war die Zuständigkeit im Wesentlichen beschränkt auf Koordinierung der IT des Bundes und Fachaufsicht über das BSI. Und die wesentlichen politischen Initiativen zu diesem Zeitpunkt gingen in die Richtung der Digitalisierung der Behörden: dass Behörden überhaupt das Internet nutzen, dass erste E-Government-Projekte durchgeführt wurden, ein erstes Portal errichtet wurde, also noch weit von dem entfernt, was wir heute haben, eine Digitalisierung der Behörden zu fördern.

Die ersten Jahre meiner Tätigkeit in dieser Funktion habe ich in der Bundesverwaltung vor allen Dingen für Digitalisierung geworben. Wenn ich das mal ~~von~~ rückwärts betrachte: Die letzten fünf Jahre in dieser Funktion habe ich innerhalb der Regierung vor allen Dingen vor bestimmten Digitalisierungen gewarnt und für Sicherheit geworben. Also, da hat sich der Blickwinkel ein Stück weit geändert, weil in dem Maße, in dem die Behörden die digitale Technik eingesetzt haben, aber auch darüber hinaus wir uns insbesondere im Bereich der Infrastrukturen davon abhängig gemacht haben, die Verantwortung für Sicherheitsfragen in meiner subjektiven Wahrnehmung in meiner Aufgabenerfüllung eine immer größere Rolle gespielt hat, weil die Behörden zu irgendeinem Zeitpunkt - ~~Mitte~~ so ungefähr 2005/06/07 - die Digitalisierung ihrer Behörden ein Stück weit als eigene Aufgabe auch angenommen haben, aber die Sicherheit, wie ich im Eingangsstatement schon gesagt habe, immer ein kleines Stück hinterherhängt, weil sie zusätzlich gekauft werden muss.

Was in den letzten Jahren zusätzlich eine große Rolle gespielt hat, war die Frage: Wo und wie kann der Staat eigentlich IT-Sicherheit ~~irgendwie~~ gewährleisten in einem Umfeld, in dem die meisten Dienstleister ~~irgendwie~~ global sind und wir uns bei dem, was wir alle - Sie auch alle - als IT einsetzen, von globaler Technologie abhängig machen, wo man mit deutscher Gesetzgebung oder nicht mal mit deutschen Forschungsprogrammen keine großen Einflüsse drauf ausüben kann? Das hat eine immer größere Rolle gespielt. Deshalb habe ich diese Verantwortung für vertrauenswürdige IT auch so in den Mittelpunkt meiner Ausführungen gestellt.

Marian Wendt (CDU/CSU): Hatten Sie während Ihrer Zeit auch Kontakte zum BND oder BfV - regelmäßig, unregelmäßig? -, also Arbeitskontakte?

Zeuge Martin Schallbruch: Also, zum BND unregelmäßig wie wahrscheinlich zu allen Behörden der Bundesverwaltung - ich war ja für die IT der gesamten Bundesverwaltung zuständig -, zum BfV natürlich regelmäßig. Das BfV ist eine Behörde des Geschäftsbereichs des Bundesinnenministeriums, wo regelmäßig Behördenleiterbesprechungen stattfinden, an denen ich auch teilgenommen habe.

Marian Wendt (CDU/CSU): Welchen Inhalts waren die regelmäßigen Kontakte zum BfV? Ging es da nur um die Digitalisierung, oder um was für konkrete Anlässe ging es da? Vielleicht auch Cybersicherheit, IT-Sicherheit?

Zeuge Martin Schallbruch: Die meisten Jahre waren die regelmäßigen Kontakte die gleichen Kontakte, wie ich sie auch zum Statistischen Amt oder Bundesverwaltungsamt gepflegt habe; das heißt, es ging um die IT-Ausstattung der Behörde, um Digitalisierung, Haushaltsfragen und Ähnliches. In den letzten Jahren, seit der Cyber-Sicherheitsstrategie 2011, haben die Kontakte natürlich auch die Zusammenarbeit im Bereich der Cybersicherheit betroffen, weil das BSI, ~~was~~ meiner Fachaufsicht unterstand, die federführende Behörde war für das Cyber-Abwehrzentrum und das BfV eine beteiligte Behörde war. Insofern hatten die Kontakte dann häufig damit zu tun: „Wie funktioniert die Zusammenarbeit der Behörden im Cyber-Abwehrzentrum oder bei Cybervorfällen?“, ähnlich wie bei BKA oder Bundespolizei auch.

Marian Wendt (CDU/CSU): Was haben Sie da festgestellt inhaltlicher Art? Wie hat sich die Cybersicherheitslage verändert? Woher kommen Angriffe als Beispiel? Sie haben ja sicherlich auch darüber geredet jetzt, wie sich die Lage verändert hat, wer eine Bedrohung darstellt, wo wir nachsteuern müssen, wo wir vielleicht Experten brauchen. Was hat sich da inhaltlich geändert?

Zeuge Martin Schallbruch: Das ist eine sehr weit gehende Frage. Um sie ordentlich zu beantworten, muss ich das ein bisschen aufteilen. Technisch hat sich die Bedrohungslage erheblich ausdifferenziert, aber einfach wegen der Ausdifferenzierung der Informationstechnik. Wenn Sie viele mobile Geräte einsetzen, Cloud-Services oder Ähnliches, dann ergeben sich da neue Angriffsformen.

Marian Wendt (CDU/CSU): Klar.

Zeuge Martin Schallbruch: Was die Motivlage angeht, haben sich über viele Jahre vier, fünf typische Motivlagen herausgestellt: allgemeine Kriminalität, organisierte Kriminalität, nachrichtendienstliche Aktivitäten, politisch motivierte Aktivitäten. Also, ich kann mich auch erinnern an Cyberangriffe gegen Systeme des Bundes, die offenbar im Kontext standen mit politischen Protestaktionen, und sicherlich auch militärische Aktionen, die wir jetzt nicht erlebt haben, aber über die ich Berichte gelesen habe.

Marian Wendt (CDU/CSU): Und wenn Sie den Punkt „Nachrichtendienstliche Angriffe" herausstellen, wo, würden Sie einordnen, kamen erstens natürlich die Angriffe her? Das interessiert uns natürlich auch sehr oft, die Frage: Wie hat sich die Situation vielleicht verändert? Gab es da vor Snowden mehr, gab es nach Snowden weniger? Das wäre ja so eine Vermutung vielleicht. Wie würden Sie das ungefähr einschätzen?

Zeuge Martin Schallbruch: Es gibt ja regelmäßige Berichte des BSI an den Innenausschuss des Deutschen Bundestages über die bei den Regierungsnetzen festgestellten Angriffe, und die zeigen eigentlich, dass die Anzahl der Angriffe stetig zunimmt. Ich habe nicht in Erinnerung, dass das irgendwie sich verändert hat rund um Snowden.

Marian Wendt (CDU/CSU): Also nur im Bereich nachrichtendienstlicher Angriffe, nicht die gesamten fünf Punkte.

Zeuge Martin Schallbruch: Die Attribution von Angriffen ist meistens unmöglich oder jedenfalls sehr, sehr schwierig. Es ist nicht so, dass man bei einem Angriff typischerweise in der Lage ist, zu irgendeinem Zeitpunkt sagen zu können: Nun können wir sicher sein, dass der Angriff von diesem oder jenem Urheber ausgeht. - Ich habe aus den Unterlagen, die mir vorgelegt worden sind, wahrgenommen, dass Angriffe Nachrichtendiensten zugeschrieben wurden, wenn sie einen bestimmten technischen Professionalisierungsgrad sozusagen überschritten haben.

Für die Zuordnung von Angriffen zu Nachrichtendiensten im Übrigen ist das BSI nicht zuständig, und mithin bin ich auch nicht zuständig gewesen. Insofern habe ich dazu keine Erkenntnisse. Aber dass ab einem bestimmten Professionalisierungsgrad man aufgrund der Veröffentlichungen, die es gibt, eher davon ausgehen kann, dass es einen nachrichtendienstlichen Hintergrund gab, das ist etwas, was mir berichtet wurde. Aber eine wirkliche Zuordnung zu einem konkreten Nachrichtendienst kenne ich aus eigentlich keinem einzigen Fall.

Marian Wendt (CDU/CSU): Okay. - Die Sicherheit der IT-Infrastruktur und auch der Schutz der Kommunikation deutscher Bürger, deutscher Behörden und auch der deutschen Wirtschaft ist ja bereits längeres Thema, auch im BMI. Bereits im Jahre - - Anfang 2006 formuliert ja der IT-Stab seine entsprechenden Ziele, und dort finden sich bereits Ziele wie die Erarbeitung einer IT-Sicherheitsstrategie, die Verbesserung der IT-Sicherheit in der Bundesverwaltung sowie die Förderung nationaler Sicherheitslösungen. Sie hatten das ja auch so ein bisschen angedeutet: nationale Anbieter, nationale IT-Lösungen. Könnten Sie das noch mal ausführen, welche konkreten Schritte Sie hier gemeinsam mit Ihren Kollegen unternommen haben und welche gesteckten Ziele man erreichen wollte und auch vielleicht jetzt, zehn Jahre danach, erreicht hat?

Zeuge Martin Schallbruch: In der Tat: Diese Zielplanung, die Sie da referenzieren, an die ich mich so ungefähr erinnere, ist überwiegend angegangen worden, was die Strategie angeht - das hatte ich eben erwähnt - und auch was die Verbesserung der IT-Sicherheit in der Bundesverwaltung angeht. Ergebnis war der Kabinettsbeschluss Umsetzungsplan Bund 2007.

Was die Förderung der vertrauenswürdigen nationalen IT-Sicherheitslösungen angeht, habe ich eben einige Maßnahmen ja schon aufgezählt: 2007/08 wurden Sicherheitskooperationen mit einigen Unternehmen geschlossen. Das BSI hat die Anzahl der - - oder hat die Entwicklungsprojekte mit nationalen Anbietern erhöht. Wir haben in bestimmten Bereichen der IT des Bundes auf nationale Lösungen gesetzt. An mehreren Stellen

wurde bei Vergabeverfahren eine entsprechende Vorgabe gemacht, soweit das vergaberechtlich möglich war. Und wir haben uns bemüht, die nationalen Anbieter im Bereich der IT-Sicherheit zu fördern, also bei zum Beispiel Export oder auch bei Schutz vor Übernahmen durch ausländische Anbieter. Das waren so wesentliche Maßnahmen, die wir in diesem Bereich ergriffen haben.

Marian Wendt (CDU/CSU): Ebenfalls im Jahr 2006 informierte ja das BMI gemeinsam mit BfV, BND und BSI den Chef des Bundeskanzleramtes, damals der heutige Innenminister de Maizière, über die Sicherheitslage in der Informations- und Kommunikationstechnik. Thema waren hierbei unter anderem ein erheblicher Informationsbedarf und fehlendes Problembewusstsein von Entscheidungsträgern in der Bundesverwaltung, die Sensibilisierung privater Unternehmen, die Verbesserung der Vertrauenswürdigkeit der Anbieter von Produkten und Dienstleistungen im staatlichen Bereich sowie die unter Sicherheitsaspekten zentrale Bedeutung nationaler Anbieter im Sicherheitsbereich. Also, das war vor zehn Jahren. Die Themen kommen ja immer wieder hoch, wie wir sehen. Und Sie waren damals als Vertreter des BMI bei dieser Besprechung im Kanzleramt anwesend. Können Sie sich an diese Besprechung erinnern? - Also, wir haben auch das Ergebnisprotokoll. Wir können es auch vorlegen, aber vielleicht - -

Zeuge Martin Schallbruch: Also, nicht mehr ganz genau -

Marian Wendt (CDU/CSU): Nein, klar.

Zeuge Martin Schallbruch: - an jedes Detail, aber so grob kann ich mich an die Besprechung erinnern, ja.

Marian Wendt (CDU/CSU): Okay. - Was war der Hintergrund dieses Treffens? Waren Sie da - - Haben Sie das maßgeblich mit initiiert? Waren Sie da nur beigeladen? Waren Sie Unterstützer? Woher gab es - - Was war der konkrete Anlass oder Auslöser?

Zeuge Martin Schallbruch: Daran kann ich mich nicht mehr ganz genau erinnern. Ich weiß allerdings, dass es einen Vorlauf gab, der darin bestand, dass wir Ende 2005/Anfang 2006 die Hausleitung des BMI damals über die Lage informiert haben, und nach meiner Erinnerung ging die Initiative für dieses Treffen auf den damaligen Sicherheitsstaatssekretär des BMI zurück, der das angeregt hat, dass man ~~mal~~ so eine Besprechung macht, um das auch ~~mal~~ ressortübergreifend zu besprechen.

Marian Wendt (CDU/CSU): Und gab es dafür einen konkreten Anlass? Gab es ein aktuelles Szenario, eine Bedrohung, einen konkreten Fall, wo Daten abgeflossen sind, wo man angegriffen wurde beispielsweise? Oft ist man ja auch in der Politik nur reaktiv. Oder war es einfach ein Lagebild, was sich ergeben hatte: „Und wir müssen uns da mal treffen und die Entscheidungsträger auf höherer Ebene sensibilisieren"?

Zeuge Martin Schallbruch: Also, es gab keinen konkreten Anlass nach meiner Erinnerung.

Marian Wendt (CDU/CSU): Okay.

Zeuge Martin Schallbruch: Auch: Soweit ich mich erinnere, hat die Präsentation, die damals gegeben wurde, das Thema auch umfassend abgebildet, von Netzsicherheit bis zu sicheren Geräten, von Fragen der Betroffenheit der Wirtschaft bis zu Fragen der Mitarbeiter der Bundesregierung. Also, das war ein ganz breites Thema, und das war ja damals der Beginn einer Wahlperiode, wo es darum ging - Anfang 2006 muss das gewesen sein -, -

Marian Wendt (CDU/CSU): Ja.

Zeuge Martin Schallbruch: - was in dieser Wahlperiode - - welche Aktivitäten da von der Bundesregierung auf diesem Feld ergriffen werden. Insofern war das eher so eine Strategiebesprechung.

Marian Wendt (CDU/CSU): Und - wir springen, kommen ein bisschen nach vorne - im September 2012, also noch weit vor den Snowden-Veröffentlichungen, richteten Sie im IT-Stab des BMI eine

organisatorisch unselbstständige Projektgruppe „Gesellschaft für IuK-Sicherheitsinfrastruktur" - in Klammern: „PG GSI" - ein. Könnten Sie uns da erläutern, was da der Anlass war oder die Ursache?

Zeuge Martin Schallbruch: Ja, das ist ein bisschen komplizierter zu erläutern. Wir haben uns als Bundesregierung Ende, ich glaube, 2008/2009 ungefähr oder als Bundesinnenministerium, muss man sagen, entschieden, eine Initiative zu starten, die Netze der Bundesregierung, alle Netze aller Bundesbehörden zu konsolidieren, weil der IVBB eben nur Ministerien, wichtige Behörden und Ähnliches abdeckt.

Diese Konsolidierung wurde dann vom Haushaltsausschuss des Bundestages - ich glaube, es muss 2011 gewesen sein - beschlossen und unterstützt. Wir haben dann eine Strategie entwickelt: Wie würden wir uns denn eigentlich angesichts der Cybersicherheitslage die Regierungsnetze der Zukunft vorstellen? Ein wesentlicher Eckpfeiler diese Strategie war, dass wir einen vertrauenswürdigen nationalen Partner brauchen, einen nationalen Provider, mit dem wir längerfristig zusammenarbeiten können, um nicht abhängig zu sein von schwer kontrollierbaren ausländischen Zulieferungen.

Ergebnis davon war, dass wir diese Projektgruppe eingerichtet haben, die Möglichkeiten geprüft haben, eine Gesellschaft zu gründen zwischen dem Bund und einem nationalen Provider, die auf Dauer den Betrieb der Regierungsnetze betreut.

Marian Wendt (CDU/CSU): Ähnlich wie vielleicht die BDBOS mit Alcatel Lucent oder - -

Zeuge Martin Schallbruch: Gut, das ist - -

Marian Wendt (CDU/CSU): Vergleichbar oder - -

Zeuge Martin Schallbruch: Nicht wirklich vergleichbar, weil es da mehr so um technischen Betrieb geht, nicht um Verantwortung. Die Verantwortung für den Betrieb liegt außerhalb meiner Zuständigkeit, weil ja das Digitalfunknetz liegt bei der BDBOS selbst. < >

Die Idee dieser Gesellschaft war, dass dort auch die Verantwortung für den Betrieb übernommen wird. Eine Gesellschaft, bei der der Bund dann auch zum Beispiel in einem Not- und Krisenfall hätte eintreten können, die Gesellschaft übernehmen, wo aber nicht Beamte, sage ich mal, für innovative Netztechnologien allein zuständig sind, sondern man bei einem Provider, der mehr Erfahrung hat, mit dabei ist.

Aber das ist ein schwieriges Unterfangen, eine solche Gesellschaft zu gründen für so viele Netze und alle Bundesbehörden. Deshalb wurde dafür eine Projektgruppe eingerichtet. Dieses Vorhaben ist nicht zu Ende verfolgt worden, aber auch noch nicht ganz, sage ich mal, abgeschlossen, weil nach der Planung, die mir jetzt auf dem letzten Kenntnisstand bekannt ist, das noch eine Option ist, darüber aber dann wiederum im Haushaltsausschuss des Bundestages entschieden werden wird.

Marian Wendt (CDU/CSU): Genau. - Deswegen möchte ich überleiten zu einem nächsten Themenkomplex, der die Netze des Bundes betrifft.

Die heutige Regierungskommunikation stützt sich ja - Sie hatten schon in Teilen ausgeführt - im Wesentlichen auf die beiden Netzinfrastrukturen IVBB, Informationsverbund Berlin-Bonn, und IVBV-BVN, Informationsverbund der Bundesverwaltung, sowie das Bund-Länder-Verbindungsnetz DOI. Während das IVBB von der Deutschen Telekom betrieben wurde, wird, wurde das zweite Netz, IVBV, über mehr als zehn Jahre vom US-Unternehmen MCI bzw. Verizon betrieben. Und im Juni 2014 teilte das BMI mit, die Bundesregierung wolle vor dem Hintergrund der NSA-Affäre die Zusammenarbeit mit der Firma Verizon im Bereich IVBB - - IVBV, also dem zweiten Netz, schrittweise beenden und zukünftig eine Infrastruktur mit erhöhtem Sicherheitsniveau bereitstellen, die einheitlich durch einen Partner betrieben wird, bei dem - ich zitiere - „auch Krisenregelungen und Eingriffsmöglichkeiten durch den Bund bestehen". Sie hatten das ja eben so leicht angedeutet bei der vorhergehenden Frage.

Was waren erst mal aus Ihrer Sicht die Entscheidungsgründe für die Zusammenarbeit mit Verizon?

Zeuge Martin Schallbruch: Dass es eine europaweite Ausschreibung gab und Verizon diese Ausschreibung 2003, glaube ich, etwa gewonnen hat.

Marian Wendt (CDU/CSU): Ja. Gut. - Da haben sie dann zehn Jahre den Betrieb geführt. Und gab es aus Ihrer Sicht vor dem Hintergrund der NSA-Affäre - das ist eine allgemeine Formulierung - einen konkreten Anlass, dass Sie sagen: „Da gab es Datenabflüsse von der MCI/Verizon aus dem Netz des Bundes“? Gab es Fragen, Dinge oder Anhaltspunkte, die eine Unzuverlässigkeit des Partners - - ja, die dafür - - da, wo es Anhaltspunkte gab - - Gab es Anhaltspunkte dafür, an der - - für die Unzuverlässig- -

Zeuge Martin Schallbruch: Es gab keine Erkenntnisse über Datenabflüsse. Bei Verizon wurde eine Revision durchgeführt, und da sind keine Erkenntnisse festgestellt worden. Aber unsere Überlegungen zur zukünftigen Strategie für die Netze des Bundes haben eingeschlossen, dass wir Datenabflüsse auch ausschließen wollten. Durch die Beauftragung eines Unternehmens, ~~was~~ das eine deutsche Niederlassung eines US-Unternehmens ist und ~~was~~ Bestandteil einer globalen Infrastruktur dieses Unternehmens ist, haben Sie immer die Situation, dass, ~~sage ich mal,~~ kritische Steuerungseinrichtungen nicht in Deutschland sind, naturgemäß. Selbst wenn die ganze Kommunikation nur über Deutschland geleitet wird, ist bei einem solchen Unternehmen typischerweise auch ein Einfluss von außen nicht völlig auszuschließen. Und wir haben uns 2014 dafür entschieden, dass wir diesen Einfluss von außerhalb Deutschlands auf die Infrastrukturen ausschließen wollten und das, was beim IVBB jetzt schon stattfindet, für alle Teilnehmer von Netzen des Bundes für die Zukunft ermöglichen wollten, und aus diesem Grunde gesagt: Wir wollen diesen separaten Vertrag nicht mehr fortführen. Ist ja keine ~~irgendwie~~ Sonderkündigung oder so was gewesen, sondern wir haben gesagt: Wir wollen diesen Vertrag nicht mehr fortführen, sondern die Teilnehmer aus diesem Vertrag in die allgemeine NdB-Infrastruktur überführen, die dann von der Telekom betrieben wird.

Marian Wendt (CDU/CSU): Dem Ausschuss liegt ein Dokument vor, VS-NfD. Da geht es im Jahr 2003, wo Bedenken vorgetragen wurden - - Oder gab es denn die Fragestellung, ob es Bedenken gibt der Zusammenarbeit zwischen Bundesregierung - - und ob die Regierungskommunikation über dieses MCI laufen sollte? Damals wurde festgestellt, dass das BMI diese Bedenken in den Bereich der Spekulation zurückweist und dass dem BND keine Erkenntnisse vorlagen, dass dort möglicherweise Datenabflüsse ins Ausland stattfinden könnten, so wie sie - - was vielleicht Ursache war, um 2014 die Verträge nicht zu verlängern. Was ist dazwischen passiert? Also, vielleicht können Sie das noch mal - - Welche Erkenntnisse - - Gab es konkret Anlässe, wo Sie sagen, zwischen 2003: „Wir haben keine Anhaltspunkte, wir können da vollkommen vertrauen, wir machen die europaweite Ausschreibung, Verizon bekommt das“ und dann mit einmal - mit einmal nicht, aber zehn Jahre sind natürlich ein Zeitraum - 2014 die Entscheidung: „Wir wollen national zurückholen und die Gefahr der Abflüsse entsprechend minimieren“?

Zeuge Martin Schallbruch: Also, zu dem Dokument 2003 kann ich mich nicht äußern. Das müssten Sie mir bitte vorlegen. Ich kann aber zu 2014 vielleicht noch mal ausführen.

Das war keine Entscheidung, die sich gegen ein bestimmtes Unternehmen richtete oder die die Erfahrungen in der Zusammenarbeit mit diesem Unternehmen zum Gegenstand hatte, sondern die die Architektur der IT-Systeme des Bundes betraf. Wir haben uns auch in Kenntnis natürlich der Snowden-Unterlagen entschieden, dass wir das Risiko, dass wir ein global operierendes Unternehmen mit wesentlichen Steuerungseinrichtungen außerhalb Deutschlands mit der Regierungskommunikation beauftragen, nicht mehr eingehen wollen.

Im Jahre, ich glaube, 2000 oder 2001 hat die EU-Kommission gegen die Bundesrepublik Deutschland ein Vertragsverletzungsverfahren ~~eingef- -~~

also durchgeführt wegen der freihändigen Vergabe des IVBB. Die Bundesrepublik Deutschland hat eine Einstellung dieses Verfahrens erreichen können durch die Zusicherung, zukünftig alle weiteren Netzvergaben in europaweiter Ausschreibung zu machen. Das wurde -- 2003 hat es zu der Vergabe an Verizon geführt.

Wir haben es 2014 erreicht - ich erwähnte das eben schon - durch schwierige Verhandlungen mit der EU-Kommission, dass wir für die gesamten Netze des Bundes eine freihändige Vergabe an die Deutsche Telekom mit Zustimmung der EU-Kommission möglich machen konnten, und aus diesem Grunde stand uns auch diese Option zur Verfügung. Insofern, das höhere Risiko wollten wir nicht mehr tragen, und wir hatten die vergaberechtliche Option. Und das beides zusammen hat zu der Entscheidung 2014 geführt, unabhängig von dem 2003er-Vermerk, den ich jetzt nicht erinnerlich habe.

Marian Wendt (CDU/CSU): Also, 2014 war sozusagen Sicherheit vor freiem Wirtschaftsverkehr, würde man sagen. Da hat man die Sicherheitsinteressen vorgebracht, und aufgrund dessen - -

Zeuge Martin Schallbruch: Genau.

Marian Wendt (CDU/CSU): Und wenn Sie sagen - - Wenn Sie von höheren Risiken sprechen, welche Risiken waren das ganz konkret? Also, Ihnen wurde das ja vorgelegt. Das wurde ja sicherlich nicht nur allgemein sicherlich erwähnt und so über den Daumen gepeilt und sich nur auf die Snowden-Dokumente, die irgendwo öffentlich standen, Bezug genommen, sondern es muss ja eventuell auch konkrete Anlässe gegeben haben, die Sie auch der EU-Kommission vorgelegt haben, wahrscheinlich was Sie dazu bewegt, was rechtfertigt, dass wir hier die Sicherheitsinteressen vorbringen und die sozusagen eine freie Vergabe notwendig machen.

Zeuge Martin Schallbruch: Die entscheidende Frage, die man dann oder die wir beantworten mussten, war: Können wir bei einem wettbewerblichen Vergabeverfahren die hohen Sicherheitsanforderungen, die wir haben, gewährleisten?

Und das haben wir mit Nein beantwortet, was damit zusammenhängt, dass wir im Laufe vieler Jahre jetzt die Erkenntnisse gewonnen haben, dass eine stärkere Virtualisierung und Vermaschung von Infrastrukturen stattgefunden hat. Ich will mal ein Beispiel nennen, dass Provider beispielsweise weltweite Netze betreiben, diese Netze zwar auch lokale Rechenzentren haben und auch lokale Netzknoten haben, dass es aber zum Beispiel übergreifende Systeme gibt, die Storage-Management machen, wo Follow-the-sun-mäßig irgendwelche Überprüfungen in Asien stattfinden oder Ähnliches. Das heißt, man hat eine andere technische Struktur, und wenn man ein Netz bauen möchte, was man auf einem Vertraulichkeitsniveau VS-NfD haben möchte, und man möchte gleichzeitig ausschließen, dass Einrichtungen steuernd auf dieses Netz einwirken, die außerhalb Deutschlands sind, dann kann man nicht mehr, sagen wir mal, europaweit ausschreiben, sondern dann muss man zu einem Provider gehen, wo man entsprechenden Einfluss auch auf alle Steuerungseinrichtungen, die auf dieses Netz einwirken können, hat. Das war, sagen wir mal, die wesentliche Erkenntnis, die dann dazu geführt hat, dass wir eine andere Sicherheitsbewertung und dann auch eine andere vergaberechtliche Bewertung vorgenommen haben.

Marian Wendt (CDU/CSU): Ich bin da auch inhaltlich bei Ihnen, wie gesagt, dass man das auch macht und dass das mit Sicherheit auch vor die Warenverkehrsfreiheit und Wirtschaftsfreiheit gehen muss. Für mich stellt sich halt die Frage, dass gewisse Erkenntnisse doch in 2000 eigentlich schon da waren, auch im BMI. Ich darf da vielleicht mal aus einem Vermerk vom 15. Februar 2006 zitieren - das ist MAT A BMI 7-1g_2.pdf, Blatt 76; wir haben ja die Akten anschließend; ich zitiere -:

> Mit der Bezugsvorlage wurde Herrn Minister in einem eingestuften Papier darüber berichtet, dass mit einem massiven Anstieg der (nachrichtendienstlichen) Gefährdung durch ausländische IT/TK-Unternehmen gerechnet werden muss. Es kann nicht ausgeschlossen werden, dass Firmen an

> Schlüsselpositionen gezielt Personal und Technik einsetzen, um Informationen auszuspähen und die Verfügbarkeit des Systems zu stören.

Das ist Ende des Zitats. - Gleichwohl wurden die bestehenden Verträge mit der Firma MCI bzw. Verizon nicht gekündigt. Auch die dringende Empfehlung, die Verträge nach dem Ende der regulären Vertragslaufzeit 2008 im Jahr keinesfalls zu verlängern, wurde offenkundig - ja, klar - nicht befolgt, nicht gefolgt, und erst vor dem Hintergrund der Ereignisse um 2013, ohne dem ein gewisses höheres Gewicht beizumessen, entschied sich ja das BMI 2014, die Verträge auslaufen zu lassen mit Verizon. Vielleicht können Sie da noch mal die Situation darstellen. War das ein Kampf? Wie muss man sich das ungefähr vorstellen, wenn es unter den Fachleuten schon die Einschätzung damals gab: „Es gibt diese Angriffe, es gibt die Gefährdung der IT-Sicherheit des Bundes“, und dass man trotzdem sagt: „Hier gilt die EU-Vorgabe“? Man hat vielleicht Angst vor der Kommission, vor einem Verfahren, und man hat da die Bedenken abgewiegelt? Vielleicht können Sie das mal beschreiben, wie das damals war.

Stellvertretende Vorsitzende Susanne Mittag: Das wäre jetzt die letzte Frage, -

Marian Wendt (CDU/CSU): Die letzte Frage, genau.

Stellvertretende Vorsitzende Susanne Mittag: - weil wir dann zur namentlichen Abstimmung müssen.

Zeuge Martin Schallbruch: Okay. - Also, zu dem konkreten Dokument - das müssen Sie mir vorlegen - kann ich mich jetzt nicht äußern. Ich bin auch nicht sicher, ob das nicht eingestuft ist.

Aber zu dem Sachverhalt vielleicht noch mal, soweit ich mich erinnere. Mir sind immer wieder Hinweise zugekommen, dass eine Zusammenarbeit ausländischer IT-Unternehmen mit Nachrichtendiensten nicht ausgeschlossen werden kann, sage ich mal in allgemeiner Form, Nachrichtendienste unterschiedlicher Provenienz.

Gleichzeitig sind in diesem konkreten Fall, aber auch in den meisten anderen Fällen nie - -

> (Dem Zeugen werden Unterlagen vorgelegt)

Marian Wendt (CDU/CSU): Genau, das Dokument wird Ihnen jetzt gezeigt, aber es ist, glaube ich, von dem Kernwert der Aussage - -

Zeuge Martin Schallbruch: Ich würde es jetzt erst mal allgemein stellen, -

Marian Wendt (CDU/CSU): Ja, genau.

Zeuge Martin Schallbruch: - und wenn ich es dann noch lesen sollte, dann müssten Sie es mir sagen. Dann kann ich vielleicht meine Aussage noch mal konkretisieren.

Sind mir nie so harte justiziable Fakten vorgelegt worden, die es rechtfertigen würden, einen Vertrag mit einem Provider wegen Unzuverlässigkeit zu kündigen. Man kann nicht, wenn man in einem normalen Vergabeverfahren einen Vertrag vergeben hat, wenn man dann Hinweise darauf bekommt, dass möglicherweise ein Unternehmen mit einem ausländischen Nachrichtendienst zusammenarbeitet, das zum Grund nehmen, einen Vertrag zu kündigen. Man kann bei der nächsten Vergabe sich darum bemühen - -

Marian Wendt (CDU/CSU): Auch wenn die Sicherheitsinteressen der Bundesrepublik Deutschland dem entgegenstehen? Ich meine, Sie sind ja nicht irgendwer, Sie sind ja das Bundes- -

Zeuge Martin Schallbruch: Na ja, wenn das justiziable, auch gegenüber dem jeweiligen Vertragspartner vorzeigbare und auch vor Gericht vorzeigbare Fakten sind. Das war aber in diesem Fall nicht so. Solche Fakten haben wir nicht gehabt.

Insofern ist das mehr eingeflossen in eine allgemeine Sicherheitsbewertung. Das hat dazu geführt, dass wir sehr darauf gedrängt haben, dass von der Möglichkeit, alle Daten zu verschlüsseln, die es ja im IVBV gibt, und zwar nicht durch diesen Anbieter, sondern das Kryptomanagement hat ja der Deutsche Wetterdienst gemacht, also

durch eine staatliche Behörde - - von dieser Möglichkeit Gebrauch gemacht wird, damit der Anbieter, auch der Anbieter nicht in der Lage ist, auf die Daten zuzugreifen.

Marian Wendt (CDU/CSU): Okay.

Zeuge Martin Schallbruch: Dass 2008 nicht gekündigt worden ist, lag daran, dass das technisch nicht möglich war. Also, zu dem damaligen Zeitpunkt gab es die Infrastruktur, in die jetzt gerade die entsprechenden Anbieter-Teilnehmer migriert werden, noch nicht.

Marian Wendt (CDU/CSU): Okay. - Dann vielen Dank, und dann machen wir dann später weiter.

Stellvertretende Vorsitzende Susanne Mittag: Gut, dann wäre die Runde auch beendet gewesen.

Marian Wendt (CDU/CSU): Genau.

Stellvertretende Vorsitzende Susanne Mittag: Dann machen wir jetzt eben eine Pause, und wir gehen zur namentlichen Abstimmung. Ich bitte dann alle, flott wiederzukommen,

(Martina Renner (DIE LINKE): Genau, flott! Keine Umwege!)

damit wir wieder einsteigen können, weil wir noch zwei haben. - Danke schön.

(Unterbrechung von 16.47 bis 17.12 Uhr)

Vorsitzender Dr. Patrick Sensburg: So, sollen wir wieder? - Ich gucke mal so in die Runde. Es sind zwar noch nicht alle da, aber alle Fraktionen sind vertreten.

Okay, die unterbrochene Sitzung des 1. Untersuchungsausschusses wird fortgesetzt. Es war die Befragung durch die CDU/CSU-Fraktion abgeschlossen, und jetzt kommen wir in der ersten Runde, wo der Vorsitzende keine Fragen gestellt hat, zur Fraktion Die Linke, und Frau Kollegin Renner stellt die Fragen, wenn ich es richtig sehe. Right? - Gut.

Martina Renner (DIE LINKE): Herr Schallbruch, auch von mir herzlich willkommen! - Ich würde Sie gerne fragen: Es gibt ja auch im Bereich der IT-Sicherheit eine Kooperation mit den USA; Sie haben es ja selbst genannt. Homeland Security als Partnerbehörde spielt da sicherlich eine Rolle.

Sie waren auch selbst Teilnehmer eines Treffens im März 2004, und da ging es auch um Schutz kritischer Infrastruktur und Strategien und Erfahrungsaustausch usw. War Ihnen zu dem Zeitpunkt bekannt, dass es auch Operationen der US-Dienste in Deutschland gab, bei denen Daten in Deutschland - in Deutschland - erfasst wurden und ausgewertet wurden?

Zeuge Martin Schallbruch: Nein, war mir nicht bekannt.

Martina Renner (DIE LINKE): Gab es insgesamt bei diesem Erfahrungsaustausch im Vorfeld Überlegungen, dass man dort auch ein gewisses Maß an Vorsicht walten lassen muss?

Zeuge Martin Schallbruch: Der Erfahrungsaustausch, den Sie ansprechen, war zwischen dem BMI und dem ganz neu gegründeten Department of Homeland Security oder - ich weiß gar nicht, ob das schon „Department" hieß - Office of Homeland Security, jedenfalls einem neu eingerichteten Ministerium, und der Inhalt des Erfahrungsaustauschs war nach meiner Erinnerung der Schutz kritischer Infrastrukturen. Es ging also nicht um die Sicherheit der IT-Systeme der Regierungen, sondern es ging um die Frage nach meiner Erinnerung: Was für Anforderungen stellt man an die Betreiber von Infrastrukturen?

Martina Renner (DIE LINKE): Okay. - Also, es ging nicht um den Schutz von Behörden oder Regierungseinrichtungen oder Bürgern und Bürgerinnen vor Zugriffen.

Zeuge Martin Schallbruch: Nein, nein.

Martina Renner (DIE LINKE): Gab es dann irgendwann mal später in der Kooperation auch

mit US-amerikanischen Stellen solche Überlegungen, dass man auch Skepsis an den Tag legen muss?

Zeuge Martin Schallbruch: Ich kann mich nicht daran erinnern, dass wir in der Kooperation mit den Vereinigten Staaten solche Überlegungen angestellt haben, Skepsis an den Tag zu legen. Die Vereinigten Staaten waren für uns wichtige Partner bei der IT- und Cybersicherheit. Allerdings haben alle Kooperationsgespräche, an die ich mich erinnern kann, immer den Fokus gehabt: Wie kann man eigentlich IT-Sicherheitsmaßnahmen verbessern? Welche zusätzlichen Anforderungen kann man stellen? Wie kann man Informationen über Angriffe austauschen? Und so weiter und so fort.

Martina Renner (DIE LINKE): Okay.

Zeuge Martin Schallbruch: Wir haben zu keinem Zeitpunkt - insofern, das würden Sie vielleicht als Skepsis werten - in diesen Kooperationen Informationen beispielsweise über unsere Sicherheitsmaßnahmen für unsere Regierungsnetze mit den Amerikanern ausgetauscht.

Martina Renner (DIE LINKE): Ich frage das vor dem Hintergrund, dass der *Spiegel* in seiner Ausgabe 49/2014 unter der Überschrift „Fern bedient" auf einen Vorgang in 2005 abstellt, bei dem der Bundesnachrichtendienst Technik analysiert, Überwachungsanlagen zur Raumüberwachung, also inklusive Kamera, Mikrofonen und Sensorik, und dort feststellt, dass diese Technik, die durch einen US-Anbieter auf den deutschen Markt unter Preis drängt und insbesondere versucht, Geschäfte mit Behörden und Sicherheitseinrichtungen abzuschließen, etwas ganz anderes tut, als sie vorgibt, nämlich dass sie so konfiguriert ist, dass sie, selbst wenn der Nutzer sie ausschaltet oder den Bewegungsmelder deaktiviert, Daten routet an US-Seite. Und das ist ein Vorgang, der, so laut *Spiegel*, im BND 2005 analysiert wurde, untersucht wurde und auch in der Präsidentenrunde besprochen werden sollte. Das wäre ja Anlass gewesen, insbesondere wenn diese Technik hier, so wie es im *Spiegel* heißt, zielgerichtet an Kunden wie Ministerien, Sicherheitsbehörden usw. - - untergeschoben zu werden, dass man sich das dann genauer anguckt mit Blick auf Ihre Aufgabe, IT-Sicherheit der Behörde. Also, kennen Sie diesen Vorgang aus 2005?

Zeuge Martin Schallbruch: Also, an diesen Vorgang kann ich mich nicht erinnern. Ich kann mich aber an vergleichbare Vorgänge erinnern, die aber, glaube ich, nicht 2005 waren, in denen wir Hinweise bekommen haben, dass bestimmte Anbieter versuchen, Produkte in sicherheitsrelevante Bereiche zu bringen, bei denen es Bedenken des BND gab wegen zum Beispiel dem Hintergrund des Anbieters oder Bedenken des BSI wegen der Architektur, nach dem Motto: Der Anbieter kann mit dieser Software oder Hardware bestimmte Informationen abgreifen.

In solchen Fällen haben wir typischerweise Warnungen in die Bundesverwaltung gegeben, dass man solche Systeme nicht einsetzt, seit 2007, seit der Zusammenarbeit mit den kritischen Infrastrukturen, auch in Richtung kritischer Infrastrukturen.

Insofern, um noch mal auf die Skepsis zurückzukommen, gibt es - -

Martina Renner (DIE LINKE): Ich will - -

Zeuge Martin Schallbruch: Ja.

Martina Renner (DIE LINKE): Wir müssen immer gucken, dass wir hier nicht so ins Allgemeine kommen. Uns interessieren die Nachrichtendienste der Five Eyes und nicht alles das, was es noch Schlimmes in der Welt gibt. Warum das möglicherweise von Interesse ist, wenn man mit der US-Seite kooperiert - - Dieser Bericht des BND war damals überschrieben, also hier laut Spiegel:

> Nachrichtendienstliche Aufklärung deutscher Behörden und Hochtechnologieunternehmen durch US-Nachrichtendienste mithilfe von Sicherheitstechnik zur Raumüberwachung.

Also, hier wusste man, wer der Täter ist, und das war 2005. Wie ist man mit so etwas umgegangen, wenn der BND zu solchen Erkenntnissen kommt?

Zeuge Martin Schallbruch: An diesen Vorgang kann ich mich nicht erinnern. Aber man ist mit so etwas so umgegangen, dass man dann gesagt hat: Wir wollen dieses Produkt in den entsprechenden sicherheitsrelevanten Bereichen nicht einsetzen.

Martina Renner (DIE LINKE): Mhm. - Und dass man sich mal diese Methodik ansieht hinsichtlich der Frage: „Könnte es da noch anderes geben?"? Also, das muss dann ja auch eine Rolle spielen, nicht nur dieses Produkt sozusagen nicht dann sozusagen noch zu bewerten oder zuzulassen, sondern man muss sich ja dann etwas grundsätzlichere Gedanken machen, wenn sozusagen ein sogenannter befreundeter Dienst so etwas unternimmt hier in Deutschland, ob es dort sozusagen darüber hinaus eine strategische Ausrichtung bei solchen Unternehmungen gibt oder ob das ein Einzelfall ist.

Zeuge Martin Schallbruch: Also, ich kenne diesen einen Vorgang, wie gesagt, nicht. Aber das BSI hat für alle kritischen Infrastrukturbereiche oder kritischen IT-Bereiche der Bundesverwaltung ständig die Sicherheit überprüft und überlegt: An welchen Stellen kommen hier welche Produkte zum Einsatz? Wo müssen wir vertrauenswürdige nationale Produkte einsetzen? Wo müssen wir, sagen wir mal, genauer hingucken? Wo müssen wir auf Zertifizierung bestehen und wo nicht?

Wenn wir Erkenntnisse bekommen haben - und da kenne ich durchaus verschiedene Fälle -, dass Produkte fragwürdig sind, dann hat das immer dazu geführt, dass eine Sicherheitsbewertung durchgeführt worden ist: Wo werden die bei uns eingesetzt, und können wir die noch weiter einsetzen?

Beispielsweise Smartphones eines bestimmten Herstellers wurden von BND und BSI als fragwürdig angesehen. Wir haben die Bundesverwaltung gewarnt. Wir haben gesagt: Wir wollen die nicht mehr einsetzen. Wir haben eine Alternative entwickelt. Das ist die normale Vorgehensweise gewesen.

Im Übrigen war ich für Fragen der Spionageabwehr, das heißt für, sagen wir mal, das Gesamtbild der Tätigkeit einzelner anderer Nachrichtendienste, innerhalb des BMI nicht zuständig.

Martina Renner (DIE LINKE): Vor dem Hintergrund - Sie sind ja schon zur MCI WorldCom/Verizon-Problematik gefragt worden -: Wieso ist dieser Vorgang bis heute, Verizon vollständig als kooperierenden Diensteanbieter auszuschließen, nicht abgeschlossen?

Zeuge Martin Schallbruch: Also, ich kann jetzt nur bis 2014 dazu Stellung nehmen. Die Entscheidung ist ja erst 2014 getroffen worden, Verizon als Diensteanbieter abzulösen, und das ist nichts, was man so tun kann, wie man jetzt den Bezug von - was weiß ich - Getränken oder so - - einfach morgen einen anderen Provider beauftragen kann, sondern das geht dann um Tausende von Standorten und Liegenschaften in ganz Deutschland, an denen man die jeweilige Technik austauschen muss, und jeder dieser Standorte muss einzeln geschwenkt werden. Das heißt, da muss jemand hin und muss da irgendwie den Standort erst mal aufnehmen. Dann muss geplant werden, und dann wird ein Projekt aufgesetzt, und man schafft dann ~~irgendwie~~ drei Standorte pro Woche oder Ähnliches. Also, das ist ein sehr aufwendiges technisches Projekt, wenn man angesichts der heutigen Anforderungen an elektronische Kommunikation die Kommunikation in der Fläche in ganz Deutschland von einem Provider auf einen anderen schwenkt.

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir wechseln in dieser Runde.

Martina Renner (DIE LINKE): Okay. Machen wir dann nachher weiter.

Vorsitzender Dr. Patrick Sensburg: Genau, geht ja gleich wieder weiter. - Wir kommen jetzt zur Fraktion der SPD, und es beginnt mit Fragen Kollege Flisek.

Christian Flisek (SPD): Danke, Herr Vorsitzender. - Herr Schallbruch, guten Tag! - Ich würde mal so gern einsteigen: Sie haben im Sommer/Spätsommer 2013 Vorschläge bei den Koalitionsverhandlungen gemacht für, ich sage jetzt mal, allgemein Verbesserungen im Bereich der IT-Sicherheit in Deutschland. Was haben Sie damals für Bedarfe oder Defizite im Bereich der IT-Sicherheit in Deutschland erkannt, wo Sie sagen: „Das muss eigentlich oder hätte in einen Koalitionsvertrag eingehen müssen"? Welche Vorschläge waren das?

Zeuge Martin Schallbruch: Ich kann mich nicht mehr an alle Vorschläge erinnern, die ich gemacht habe, weil ich ja für die Abteilung, für die gesamte Abteilung zuständig war und wir zu allen Fragen der Digitalisierung Vorschläge gemacht haben.

Christian Flisek (SPD): Ja.

Zeuge Martin Schallbruch: Das waren Dutzende von Einzelvorschlägen.

Im Bereich der IT-Sicherheit war ein ganz entscheidender Punkt die Förderung vertrauenswürdiger Informationstechnik, das heißt Fortsetzung von Forschungsprogrammen, Erleichterungen von Regelungen im Vergaberecht, vertrauenswürdige nationale Provider zu beauftragen, Ausweitung des Anwendungsbereichs der Zertifizierung des BSI. Regelungen im Außenwirtschaftsgesetz waren nach meiner Erinnerung von den Vorschlägen umfasst. Ein ganz wichtiger Vorschlag, der sich im Koalitionsvertrag nicht durchgesetzt hat, aber dann später, war die Konsolidierung der IT des Bundes bei einem Dienstleister, um dort einheitliche und höhere Sicherheitsmaßnahmen ergreifen zu können und nicht so viele Angriffsflächen zu bieten. Auch die Konsolidierung der Netze des Bundes war nach meiner Erinnerung vorgeschlagen. Dann haben wir eine ganze Reihe Vorschläge gemacht im Bereich kritischer Infrastrukturen, IT-Sicherheitsgesetz, was ja dann auch im Koalitionsvertrag aufgenommen worden ist, Sensibilisierung der Bürgerinnen und Bürger. Förderung „Deutschland sicher im Netz" war aus meine Erinnerung ein Vorschlag, den wir gemacht haben. Also, viel mehr Erinnerungen habe ich jetzt nicht mehr, was jetzt konkrete Vorschläge waren.

Christian Flisek (SPD): Und Sie haben das ja mal angedeutet: Was waren Dinge, die jetzt nicht Eingang gefunden haben, wo Sie aber sagen: „Das ist eigentlich ein Bedarf, ein Defizit, der nach wie vor sehr akut besteht"?

Zeuge Martin Schallbruch: Also, sehr intensiv bemüht hatte ich mich um eine Aussage zur Konsolidierung der IT der Bundesverwaltung. Das ist eine Zeit lang auch in den Entwürfen drin gewesen und hat dann am Ende nicht Eingang gefunden.

Christian Flisek (SPD): Was hätte das konkret bedeutet, Konsolidierung?

Zeuge Martin Schallbruch: Dass man den IT-Betrieb der Bundesbehörden, Hunderter von Bundesbehörden bei einem Dienstleister konzentriert, dass man damit - natürlich nicht in einem Rechenzentrum; jetzt haben wir 119 Rechenzentren - - Ich würde mir dann einen Dienstleister vorstellen, der natürlich in Deutschland vielleicht fünf Rechenzentren betreibt, also hohe Redundanz, aber eben mit einem hohen einheitlichen Sicherheitsniveau für alle Behörden und auch der Möglichkeit, dass - was Frau Abgeordnete Renner eben angesprochen hat -, wenn zum Beispiel eine Sicherheitsbewertung für ein Produkt zu dem Ergebnis führt: „Da haben wir Zweifel, weil zum Beispiel der Hersteller übernommen worden ist von einem anderen Hersteller", man es dann für die ganze Bundesverwaltung sehr schnell austauschen kann.

Heute ist es so: Wir haben in der Fläche eine sehr heterogene Landschaft und brauchen für einen solchen Austausch sehr lange.

Christian Flisek (SPD): Und diese sehr heterogene Landschaft in der Fläche, die Sie jetzt gerade angesprochen haben, ist etwas, was sozusagen im - ich nenne das jetzt mal - Wildwuchs über Jahre sich so ergeben hat, weil jeder eigentlich unkoordiniert das gemacht hat, was er für richtig gehalten hat.

Zeuge Martin Schallbruch: Ja, genau.

Christian Flisek (SPD): Das heißt, eine Konsolidierung - - Oder ich frage jetzt mal andersrum: Warum, glauben Sie, ist das denn dann gescheitert? Sie sagen: Das ist dann aus dem Koalitionsvertrag rausgeflogen. - War das ein Widerstand der einzelnen Ressorts, die gesagt haben: „Wir lassen uns da nicht reinfuhrwerken und reinbestimmen in unsere eigene IT-Infrastruktur"?

Zeuge Martin Schallbruch: Ich war ja nicht Teilnehmer der Koalitionsverhandlungen, und insofern kann ich nicht sagen, warum es da nicht aufgenommen worden ist von den Politikern, die den Koalitionsvertrag verhandelt haben. Aber ich kann nur aus der Perspektive eines Regierungsbeamten berichten, dass es genau so ist, wie Sie beschreiben: Es gibt einen immerwährenden Widerstand der Ressorts in dem gesamten Zeitraum, auf den sich der Untersuchungsauftrag erstreckt, gegen die Konsolidierung der IT bei einem Dienstleister wegen der Befürchtung, dass man dann nicht die IT-Leistungen zu dem Preis bekommt, wie man sie gerne haben möchte.

Christian Flisek (SPD): Und das war dann wahrscheinlich auch der Grund, warum - - Sie sind ja sozusagen - ich nenne das mal so - der Architekt eines CIO-Konzepts des Bundes, also Chief Information Officer. Sie haben mal vorgeschlagen, glaube ich, dass jedes Ressort eine solche Person nennen soll und das Ganze unter dem Dach eines Bundes-CIO dann steht. Und dieses Konzept ist ja auch nicht umgesetzt worden, und das sind ähnliche Gründe. Also, sozusagen die Nickeligkeiten zwischen den Ressorts haben da doch eine ganz starke Wirkung.

Zeuge Martin Schallbruch: Ja, im Grundsatz trifft das zu, was Sie vortragen. Umgesetzt worden ist das Konzept schon, was 2007 wesentlich von mir entwickelt worden ist, aber eben sehr schwach. Die Ressorts haben IT-Beauftragte eingerichtet, zentrale, und es gibt einen IT-Beauftragten der Bundesregierung, dem aber wegen der Ressorthoheit aus Artikel 65 Grundgesetz keine Entscheidungsbefugnisse zugedacht wurden, sondern eben die Leitung eines Gremiums, was dann ressortübergreifend einstimmig entscheiden muss. Und es gibt auch kein zentrales Budget für die IT des Bundes, sondern die Budgets liegen in den Bundesministerien.

Ein Stück weit ist das in den letzten Monaten geändert worden, aber das liegt außerhalb des Untersuchungszeitraums.

Christian Flisek (SPD): Wenn man mal eine Bestandsaufnahme von dieser Situation macht, vor der wir stehen - also ich sage jetzt noch mal den Begriff „so etwas gewachsener Wildwuchs" -, nach Ihrer Einschätzung was bedeutet das denn für die Sicherheit der dort verarbeiteten, gespeicherten Daten? Haben wir zum Beispiel, wenn man sich die ganze Landschaft vor Augen hält, Daten, die beispielsweise auch auf US-Servern liegen können?

Zeuge Martin Schallbruch: Ich kann das nicht ausschließen, dass es innerhalb der Bundesverwaltung Behörden gibt, die Dienste nutzen, wo Daten auf US-Servern liegen. Es gibt eben bis heute noch keine, sagen wir mal, zentrale Steuerung der gesamten IT, wo an einer Stelle die Information verfügbar ist: Wo sind welche Daten? Auf was für Servern? Mit welchen Produkten werden sie verarbeitet? Und so weiter und so fort. Das ist das Resultat einer, sage ich mal, unkonsolidierten Landschaft.

Allerdings gibt es Bereiche in der Bundesverwaltung - das muss man erwähnen -, in denen man frühzeitig konsolidiert hat, und das sind die Netze. Das hängt mit dem Regierungsumzug zusammen. Viele Staaten in der Welt haben kein einheitliches Regierungsnetz, wie es die Bundesrepublik Deutschland hat. Bei meinen Kontakten in den Vereinigten Staaten, die Frau Abgeordnete Renner eben erwähnt hat, habe ich beispielsweise gelernt, dass dort eines der größten Sicherheitsprobleme ist, dass sie ungefähr 2 000 Übergänge aus ihren Regierungsnetzen ins Internet haben, während hier die Bundesregierung in Bonn und in Berlin jeweils zwei Übergänge hat. Die vier kann man natürlich ganz anders sichern, als wenn man 2 000 hat. Also, Teile der Landschaft sind schon ganz gut konsolidiert, aber die Rechenzentren in ihrer Vielfältigkeit harren noch der Konsolidierung.

Christian Flisek (SPD): Und hat sich denn da in der Bewertung nach Snowden, wenn man das jetzt mal als eine Zäsur sieht, was da im Sommer 2013 passiert ist, irgendwas verändert? Ist man dort mal stärker tätig geworden? Wir haben ja dann auch den Vorfall des Kanzlerinnenhandys gehabt, wo wir alle ja nur gesagt haben: „Das ist allenfalls die Spitze eines Eisbergs", jetzt ganz symbolisch. Aber eigentlich geht es ja da um die große Masse der IT-Infrastruktur und der Sicherheit, die davon betroffen ist. Hat sich da gravierend was verändert nach Snowden?

Zeuge Martin Schallbruch: Also, ich überblicke ja den gesamten Zeitraum seit 2002 und kann sagen: Es hat sich seit Snowden gravierend etwas verändert. Es gibt Beschlüsse über die IT-Konsolidierung der gesamten Bundesverwaltung, sukzessive soll das in einen Dienstleister ~~reingehen~~ hineingehen. Es gibt einen harten Beschluss zur Konsolidierung aller Netze. Es gibt einen vor 2013 noch ganz schwachen, jetzt sehr starken Druck aus dem Haushaltsausschuss des Bundestages, der diesen Prozess steuert und vierteljährlich, glaube ich, Bericht bekommt zu dem Thema. Das heißt - -

Christian Flisek (SPD): Druck inwiefern? Was machen die Kollegen da?

Zeuge Martin Schallbruch: Die üben Druck aus auf die Bundesministerien, das BMI federführend und dahinter die Bundesministerien, die Konsolidierung der IT voranzutreiben und regelmäßig über die Fortschritte zu berichten.

Christian Flisek (SPD): Okay.

Zeuge Martin Schallbruch: Auch die Mittel dafür sind bereitgestellt worden, umfassend, aber immer mit Auflagen versehen und mit Berichten, dass auch tatsächlich ein Fortschritt messbar ist. Und dass dieser Druck aus dem Parlament entstanden ist, geht nach meinem Eindruck auch auf die Snowden-Veröffentlichungen zurück.

Das Zweite, was ich nennen will: Es gibt eine sehr viel größere Akzeptanz bei den Beschaffern im Bund, die Möglichkeiten, die das Vergaberecht bietet, in sicherheitskritischen Bereichen auch nationale vertrauenswürdige Lösungen einzusetzen, auch auszunutzen. Jeder Beschaffer geht ja ein Risiko ein, wenn er sagt: Ich nehme jetzt hier die Ausnahmevorschrift § 100 GWB irgendwie und sage: Das ist sicherheitskritisch. - Das Risiko, dass er dann vor Gericht gezogen wird und verliert oder dass es ein Vertragsverletzungsverfahren gegen Deutschland gibt - - Diese Risikobereitschaft ist gestiegen. Auch das führe ich auf die Snowden-Veröffentlichungen zurück.

Christian Flisek (SPD): Das heißt, es werden bei den Ausschreibungen verstärkt - vielleicht können Sie das noch mal quantifizieren - dann Anforderungen formuliert, die auf, ich sage mal, eine nationale Lösung hinsteuern.

Zeuge Martin Schallbruch: Quantifizieren kann ich das nicht, weil es keine zentrale Beschaffungsorganisation für die Bundesverwaltung gibt und das BMI hier nur, ~~sagen wir mal~~, Handreichungen gibt, Musterverträge usw. Aber in all diesen Regelungen sind inzwischen Klauseln ~~drin~~, die manche ausländischen Anbieter nicht akzeptieren können und deshalb auf Gebote verzichten. Mir sind vielmehr Einzelfälle bekannt geworden in meiner Tätigkeit, in denen eine freihändige Vergabe durchgeführt worden ist und durchaus auch in manchen Fällen vor Gericht sich dann durchgesetzt hat.

Christian Flisek (SPD): Wie sind da die Reaktionen von, ich sage mal, den Lobbyisten der US-Unternehmen, die davon betroffen sind?

(Dr. André Hahn (DIE LINKE): Die sind not amused!)

Zeuge Martin Schallbruch: Nach den Snowden-Veröffentlichungen habe ich selbst auch und haben auch die Kollegen in meinem Bereich und auch das Bundesinnenministerium insgesamt natürlich sehr viel deutlicher hingeschaut und sehr viel deutlicher gemacht, dass wir bei amerikanischen Unternehmen genauer hinschauen müssen. Das hat zu einem - wie soll ich mal sagen? - sehr starken Anstieg von Lobbydruck geführt - das kann man nicht verkennen - von amerikanischen Unternehmen, weil die Vertrauenswürdigkeit

amerikanischer Unternehmen insgesamt ein Stück weit infrage gestellt wurde, es dazu ja auch Presseberichte gab. Die Reaktion der Unternehmen war unterschiedlich. Manche haben sich darauf eingestellt und haben beispielsweise begonnen, Kooperationen mit deutschen IT-Sicherheitsunternehmen zu suchen, um vertrauenswürdige deutsche Produkte zur Absicherung ihrer Lösungen einzusetzen. Da kenne ich einige Beispiele.

Manche Unternehmen haben in Deutschland Infrastrukturen errichtet, Rechenzentren. Manche Unternehmen haben die sogar deutschen Unternehmen praktisch zur Verfügung gestellt, sodass juristisch die Daten nicht bei einem amerikanischen Unternehmen gespeichert sind. Also, es gibt da auch in der Sache einige Unternehmen, die große Fortschritte gemacht haben in der Zeit, die hier in Rede steht, bei der Erhöhung der Vertrauenswürdigkeit ihrer Leistungen.

Christian Flisek (SPD): Also konkret jetzt mal, ohne dass wir jetzt hier Werbung machen wollen oder so: Aber zum Beispiel jetzt eine Vereinbarung, die Microsoft mit der Deutschen Telekom geschlossen hat, sodass man sich darauf verständigt hat, die Speicherung von europäischen Kommunikationsdaten auf Servern innerhalb der EU sicherzustellen, und wo dann EU-Unternehmen sozusagen als Sachwalter und Datenspeicher des US-Konzerns fungieren - - Das sind solche Fortschritte beispielsweise, oder?

Zeuge Martin Schallbruch: Ich habe solche Lösungen im Untersuchungszeitraum gefordert von den Unternehmen und habe natürlich jetzt davon gehört, dass das auch inzwischen erste Unternehmen umsetzen.

Christian Flisek (SPD): Halten Sie das für vertrauenswürdig, so was?

Zeuge Martin Schallbruch: „Vertrauenswürdig" ist kein absoluter Begriff. Das erhöht die Vertrauenswürdigkeit. In der IT-Sicherheit können Sie beispielsweise mit einem Innentäter immer sehr leicht -

Christian Flisek (SPD): Okay.

Zeuge Martin Schallbruch: - auch alles, was an Vertrauen da ist, schon wieder zerstören. Es erhöht die Vertrauenswürdigkeit, weil die Datenspeicherung eben vollständig auch in deutschem Rechtsraum stattfindet. Und das ist schon ein guter Schritt, und ich habe wahrgenommen, dass das ja auch von vielen Unternehmen, Unternehmenskunden inzwischen auch nachgefragt wird, nicht nur von der Regierung.

Christian Flisek (SPD): In der vorletzten Woche war eine Tagung bei der Stiftung Wissenschaft und Politik, und da hat ein US-amerikanischer Referent darauf hingewiesen, dass Deutschland innerhalb der EU eine sehr zentrale Rolle als Internet-Backbone einnimmt innerhalb der EU, etwa vergleichbar durchaus wie die USA, insbesondere im Hinblick auf Kommunikationsverkehre, ich sage mal, aus Nahost. Und wir wissen ja alle, dass dieser Kommunikationsverkehr - haben wir uns sehr gut mit auseinandergesetzt bei den Kooperationsprojekten des BND im Rahmen oder im Kontext der Terrorismusbekämpfung - wichtig und auch begehrt ist. Jetzt frage ich Sie aber: Gibt es aus Ihrer Sicht besondere Schutzvorkehrungen, die notwendig wären in Deutschland gerade aufgrund dieser strategischen Position als bedeutender Internet-Backbone, um den Schutz der Privatsphäre hier und auch den Schutz von Betriebs- und Geschäftsgeheimnissen von Unternehmen in Deutschland angemessen zu schützen?

Zeuge Martin Schallbruch: Ja, ganz einfach: Verschlüsseln.

(Martina Renner (DIE LINKE): Ja!)

Ich meine - -

Christian Flisek (SPD): Ja, mich freut das immer, wenn ich das aus dem Hause des Bundesinnenministers höre.

Zeuge Martin Schallbruch: Ich bin nicht im Hause des Bundesinnenministers, aber habe das auch schon zu meiner Zeit im Hause des Bundesinnenministers gesagt: Verschlüsseln aller Daten

und Kommunikationsverkehre. So einfach ist das.

Das ist natürlich in der praktischen Umsetzung sehr schwierig, aber man kann in allen Bereichen - jeder Einzelne, jedes Unternehmen, jede Behörde - sehr viel mehr tun noch und kann einfach weitere Verkehre verschlüsseln. Dafür stehen vernünftige Verfahren zur Verfügung, die auch sicher sind.

Christian Flisek (SPD): Und Verschlüsseln heißt auch Verschlüsseln. Da hat kein anderer einen Schlüssel für.

Zeuge Martin Schallbruch: So verstehe ich das, Verschlüsseln.

(Martina Renner (DIE LINKE): So war das gedacht!)

Christian Flisek (SPD): Genau. - Das bedeutet - - Jetzt auch mal bezogen auf Ihre Zeit im Innenministerium die Frage gestellt: Wie ist denn das Haus mit solchen sehr unterschiedlichen Zielsetzungen, die ja alle unter einem Dach vereinigt waren, also einerseits natürlich schon die Begehrlichkeiten der Sicherheitsbehörden und Nachrichtendienste, da irgendwie dann doch für den Fall aller Fälle den Schlüssel irgendwie in den Händen zu halten, und andererseits die Anforderung, die IT-Infrastruktur zu konsolidieren und die Integrität sicherzustellen - - Wie ist man denn mit diesem Zielkonflikt unter einem Dach umgegangen?

Zeuge Martin Schallbruch: Man hat das intensiv diskutiert. Ich kann mich aus der Zeit, in der ich da Verantwortung getragen habe, an bestimmt vier, fünf Grundsatzdiskussionen bis hoch zur Ministerebene über diese Frage erinnern. Beginnt 2002, und immer wieder wurden - -

Christian Flisek (SPD): Wer war damals - - Sagen Sie nur, wer da - - mit wem - - mit welchen Ministern Sie da gesprochen haben.

Zeuge Martin Schallbruch: Mit Herrn Schily, mit Herrn Schäuble, mit Herrn de Maizière. Bei Herrn Friedrich kann ich mich nicht erinnern, ob im Zeitraum der Amtszeit von Herrn Friedrich diese Diskussion war. Aber bei den drei Ministern jedenfalls kann ich mich erinnern. Und es wurden dann die Argumente von beiden Seiten gehört, und am Ende hat sich die Linie durchgesetzt, für die ich mich auch starkgemacht habe, dass wir in Deutschland keine Kryptoregulierung einführen.

Christian Flisek (SPD): Bei allen drei Ministern war das gleichermaßen so.

Zeuge Martin Schallbruch: Ja.

Christian Flisek (SPD): Das ist ja - - Nach meiner Kenntnis, ich sage mal, ist das letzte offizielle Dokument, das ich zur Kryptopolitik kenne, glaube ich, ein einseitiges Dokument irgendwie aus dem Jahr 1999. Seitdem gibt es sozusagen ja irgendwie keine Aktualisierung, oder? Ist das richtig?

Zeuge Martin Schallbruch: Da gibt es keine Aktualisierung. Die Diskussion ging immer darum: Wollen wir die Kryptoeckpunkte von 1999 bestätigen oder nicht? Und das Ergebnis war immer: Wir wollen sie bestätigen.

Es gibt jetzt aber auch nicht wirklich die Notwendigkeit, dass ein Bundesministerium Dokumente produziert, dass sie zu irgendeinem Thema kein Gesetz machen. Insofern ist es bei dieser Linie, 99er-Linie, geblieben bis heute.

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir wechseln.

Christian Flisek (SPD): Ja, dann wechseln wir.

Vorsitzender Dr. Patrick Sensburg: Genau. - Dann geht es zur Fraktion von Bündnis 90/Die Grünen, und Herr Kollege von Notz fängt an.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Guten Tag, Herr Schallbruch! - Um das vielleicht ein bisschen zu konkretisieren: Können Sie sich

noch dran erinnern, was für Diskussionen stattgefunden haben im Sommer 2013 mit den Snowden-Veröffentlichungen bei Ihnen?

Zeuge Martin Schallbruch: Sicher nicht an alle, weil es waren sehr viele.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Aber wie war denn so die Stimmung? War man völlig aus den Latschen? Oder hat man gesagt: „Ja, gedacht haben wir es uns eigentlich schon immer"?

Zeuge Martin Schallbruch: Ich würde mal sagen: In der Mitte zwischen Ihren beiden Positionen. Weil ich persönlich kann über mich sprechen und das, was ich in meinem Verantwortungsbereich wahrgenommen habe: Ich bin davon ausgegangen, dass die ausländischen Nachrichtendienste hinter vielen Cyberangriffen möglicherweise stecken und sich intensiv darauf vorbereiten, auch den Cyberraum zu nutzen für Angriffe. Und so weiter und so fort.

Ich bin nicht davon ausgegangen oder ich habe nicht erwartet gehabt zu dem damaligen Zeitpunkt, dass das Ausmaß der technischen Vorbereitungen, auch der technischen Maßnahmen, die sozusagen von der NSA laut den Snowden-Dokumenten vorbereitet worden sind, so gewaltig ist. Also, das hat mich auch als Techniker, sage ich mal, überrascht. Auch die verschiedenen Stoßrichtungen, mit denen da technische Maßnahmen konzipiert wurden, um in fremde Systeme einzudringen, war nichts, was ich in diesem Ausmaß erwartet hätte.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und dass Teil dieser Kooperationen, die es da gab, teilweise ein deutscher Nachrichtendienst auch war? War das bei Ihnen so bekannt, dass der Bundesnachrichtendienst so eng kooperiert auch in Deutschland mit den Five Eyes, oder hat das auch überrascht?

Zeuge Martin Schallbruch: Also, über die Kooperationen des Bundesnachrichtendienstes mit anderen Nachrichtendiensten war mir in meiner gesamten Dienstzeit nichts bekannt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also „Eikonal", „Glotaic", solche Sachen hat man nie was von gehört.

Zeuge Martin Schallbruch: Nein, war mir nicht bekannt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja. - Haben Sie von diesem Belgacom-Fall auch erst aus den Snowden-Unterlagen erfahren, oder - -

Zeuge Martin Schallbruch: Ich kann mich nicht mehr ganz genau erinnern, aber ich glaube, ich habe von diesem Fall früher erfahren, weil das BSI mit diesem Fall befasst war und das BSI dazu berichtet hat.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Und können Sie das mal für uns einordnen, wie man damals da von deutscher Behördenseite draufgeguckt hat auf diesen Belgacom-Fall?

Zeuge Martin Schallbruch: Bei mir ist vor allen Dingen angekommen, was das BSI, was ja da ein Stück weit eingebunden war in die Analyse, berichtet hat über die Art und Weise, wie dieser Angriff erfolgt ist, welche auch ausgefeilten Methoden verwendet wurden, um dort in das System einzudringen. Und das hat mich natürlich in dem Maße interessiert, als für uns klar war: Wir müssen prüfen, ob wir bei unseren Regierungsnetzen gegen vergleichbare Angriffe ausreichend geschützt sind. Das hat das BSI dann auch getan und ist zu dem Ergebnis gekommen, dass das im Grundsatz so ist. Allerdings bei jedem einzelnen Vorfall, den man zur Kenntnis bekommen hat - wir haben auch andere Vorfälle aus dem Ausland zur Kenntnis bekommen -, hat das BSI eigentlich in der Regel immer seine Abwehrsysteme noch mal ein Stück weit erweitert, neue Signaturen eingepflegt oder neue Mechanismen danach programmiert. Ich kann mich nicht mehr genau erinnern, aber es kann sein, dass das auch im Belgacom-Fall so war.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Trotzdem hat sich da im Nachhinein raus-

gestellt, dass auch Mitarbeiterinnen und Mitarbeiter des Bundeskanzleramts offensichtlich mit ganz ähnlichen Instrumenten angegriffen worden sind um das Jahr 2012 herum.

Zeuge Martin Schallbruch: Ich glaube, der Vorgang ist eingestuft, oder?

(Der Zeuge wendet sich an Vertreter der Bundesregierung)

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Er stand auf *Spiegel Online*.

MR Torsten Akmann (BMI): Sie können da, wenn Sie da was zu wissen, abstrakt was zu sagen. Sonst ist er eingestuft, in der Tat.

Zeuge Martin Schallbruch: Ich kann jedenfalls - - Abstrakt kann ich sagen, dass mir in der Tat neben dem Belgacom-Fall andere Fälle zur Kenntnis gebracht worden sind, wo vergleichbare Angriffstechniken verwendet wurden, weil das auch eine der Tätigkeiten des BSI war, sich anzuschauen: „Mit welchen Angriffswerkzeugen wurden unter Ausnutzung welcher Angriffsvektoren dort welche Ergebnisse erzielt?“, weil das natürlich für die Schutzaufgabe des BSI von besondere Bedeutung war. Und da gab es eben auch andere Fälle, bei denen vergleichbare Angriffswerkzeuge mir zur Kenntnis gegeben wurden.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Genau. - Also, es heißt ja - ich kann es - - ich weiß es ja auch nicht, aber ich habe das jetzt so wahrgenommen im Nachhinein -, dass eben in beiden Fällen Regin eine Rolle spielt. Und diese Software ist ja irgendwie zuordnenbar nach den Snowden-Unterlagen, und zwar als Software, als Instrument des GCHQ. Und deswegen frage ich mich sozusagen: Ab welchem Zeitpunkt ist man von Bundesregierungsseite ausgegangen - ich sage es mal überspitzt -: „Der Feind in meinem Bett“? Also, ab wann hat man so überlegt, dass vielleicht die Leute, mit denen man sehr eng kooperiert, vielleicht auch Teil des Sicherheitsproblems sind, das man hat? Und was bedeutet das eigentlich in der Konsequenz für die Kooperationen, die man laufen hat?

Ja, jetzt bin ich der Erste, der irgendwie so Zwänge und so auch versteht. Aber hat man das nicht an irgendeiner Stelle dann auch diskutiert?

Vorsitzender Dr. Patrick Sensburg: Dazu die Bundesregierung. Herr Akmann.

MR Torsten Akmann (BMI): Vielen Dank, Herr Vorsitzender. - Ich will nicht groß unterbrechen. Wenn es darum geht, wer es war: Das ein eingestufter Vorgang. Der kann nur in nichtöffentlicher Sitzung hier behandelt werden. - Danke.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wer was war? Regin jetzt?

(MR Torsten Akmann (BMI): Ja, Sie hatten vorhin schon mal danach gefragt!)

- Ja, ich habe ja diese *Intercept*-Folie vorgelegt. Da steht, dass das der GCHQ war. Das ist eine öffentliche Folie. Soll ich die jetzt noch - - Wir haben eine Folie für Sie, Herr Schallbruch.

Vorsitzender Dr. Patrick Sensburg: Die Folie können wir vorlegen. Nur den Sachverhalt können wir daran nicht diskutieren.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Bitte?

Vorsitzender Dr. Patrick Sensburg: Die Folie können wir natürlich vorlegen. Aber den Sachverhalt können wir danach nicht diskutieren, weil der eingestuft ist.

(Dem Zeugen werden Unterlagen vorgelegt)

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also, das hat der *Intercept* am 13.12.2014 veröffentlicht. Das liegt außerhalb unseres Untersuchungszeitraums, ist aber nur die Veröffentlichung. Die Folie ist natürlich älter.

Zeuge Martin Schallbruch: Also, ich kenne das Dokument nicht und kann es, ehrlich gesagt,

auch nicht wirklich beurteilen, ob dieses Dokument irgendetwas beweist. Ich will aber versuchen, Ihre Frage zu beantworten.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Martin Schallbruch: Ich persönlich bin seit der Veröffentlichung der Snowden-Folien davon ausgegangen, dass man es nicht ausschließen kann, dass andere Nachrichtendienste auch aus den Five-Eyes-Staaten, aber auch andere Nachrichtendienste - die Snowden-Folien sind ja auch eine Anleitung für Nachrichtendienste - derartige Angriffe auf unsere Regierungsnetze durchführen, dass man es nicht ausschließen kann. Insofern habe ich versucht und da auch sehr viel Zeit drauf verwandt, die Maßnahmen zum Schutz der Infrastrukturen in Deutschland so zu erweitern, dass man auch diese Art Angriffe abwehren kann und dass man darauf vernünftig vorbereitet ist.

Ich habe mich nicht mit der Frage beschäftigt, weil ich nicht zuständig war und dazu auch keine eigenen Quellen hatte: Wie wahrscheinlich ist es denn tatsächlich, dass solche Angriffe von einem bestimmten Urheber kommen?

Was die Kooperation angeht, so ist die Kooperation mit den Vereinigten Staaten oder mit unseren europäischen Partnern im Bereich der Cybersicherheit von großer Bedeutung. Wir tauschen dort Informationen aus über sehr schwerwiegende Fälle auch von beispielsweise Wirtschaftsspionage, bei denen wir ganz andere Vermutungen haben, was der Urheber sein könnte, aber auch das in der Regel nicht beweisen können. Und diese Kooperation habe ich - und da bin ich seit der Veröffentlichung der Snowden-Folien natürlich noch ein bisschen misstrauischer - nicht bezogen auf Art und Umfang der Sicherheitsmaßnahmen, die wir in unseren Infrastrukturen betreiben. Wir haben schon seit Veröffentlichung der Snowden-Unterlagen eine sehr viel nationalere Beschaffung und Kryptopolitik betrieben als vorher.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das verstehe ich. Und Sie sind ja jetzt sozusagen fürs BMI hier. Wir haben aber die letzten Monate eben sehr viel auch im Hinblick auf den Bundesnachrichtendienst diskutiert. Und was ich mich eben immer frage, ist, ob es da nicht einen Widerspruch gibt zwischen der Kooperation und dem Datenaustausch und dem gemeinsamen An-die-Glasfaser-Gehen und ebendiesem Grundvertrauen, was es dafür eigentlich braucht.

Ich würde auch immer zustimmen: Es braucht eigentlich internationale Kooperationen in solchen Fragen, und so bin ich ein total pragmatischer Mensch. Aber wenn so eine Zäsur da eintritt und man feststellt, ich sage jetzt mal - da können Sie vielleicht auch noch was zu sagen -, dass man eben bei der Software XKeyscore, die man einsetzt, bis heute offensichtlich nicht sicher ist, ob das nicht ein gigantomanisches Trojanerprogramm ist und man das bis heute irgendwie prüft, obwohl es jahrelang in Deutschland eingesetzt wurde von deutschen Nachrichtendiensten - - Ich meine, das ist doch irgendwie eine krasse Geschichte. Und deswegen - -

Vorsitzender Dr. Patrick Sensburg: Jetzt müssten wir in der Zeit noch eine krasse Antwort hinkriegen, bevor die Zeit abgelaufen ist.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, ich müsste in der Zeit erst mal eine Frage hinbekommen.

Vorsitzender Dr. Patrick Sensburg: Ich fand die schon gut bis jetzt.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja. - Antworten Sie doch einfach spontan, was Ihnen dazu einfällt, Herr Schallbruch.

(Heiterkeit)

Zeuge Martin Schallbruch: Als Erstes: XKeyscore kenne ich nicht.

Zweitens. Die Frage, mit welchen Staaten man kooperiert, ist zunächst mal eine politische Frage. Und die Kooperation mit den Vereinigten Staaten von Amerika auf dem Feld der Cybersicherheit war politisch erwünscht und gefördert,

und ich habe da auch zugeraten, das zu tun, weil wir da auch wichtige Erkenntnisse ausgetauscht haben. Und aus diesem Grunde habe ich diese Kooperation auch betrieben, aber eben in dem wie eben schon beschriebenen eingeschränkten Maß, dass es immer auch nationale Sicherheitsinteressen gibt, die man dann auch mit Kooperationspartnern nicht teilen kann.

Vorsitzender Dr. Patrick Sensburg: Okay. - Jetzt kommen wir zur zweiten Runde. Es beginnt wieder die Fraktion der CDU/CSU. Der Kollege Wendt.

Marian Wendt (CDU/CSU): Ja, vielen Dank. - Wir haben jetzt verschiedene Bereiche schon abgearbeitet. Es kam vorhin auch das Thema des sogenannten Kanzlerinnenhandys, des Verdachts des Abhörens des Kanzlerinnenhandys. Am 23. Oktober 2013 berichtet ja *Spiegel Online,* dass das Handy der Bundeskanzlerin möglicherweise von der NSA überwacht worden sei. Bereits einen Tag später richtete der Generalbundesanwalt eine Erkenntnisanfrage dazu an den Präsidenten des BSI. Diese Anfrage beantwortete der BSI-Präsident am 8. November gleichen Jahres, es lägen dem BSI keine über die Presseberichterstattungen hinausgehenden Erkenntnisse vor. Ich zitiere:

> Teile der in der Presse dargestellten Erkenntnisse wurden dem BSI jedoch einige Tage vor Veröffentlichung mit der Bitte um Bewertung der Plausibilität zur Verfügung gestellt.

Die Frage: Dieses Schreiben - - Inwieweit waren Sie in diesen Vorgang eingebunden als Fach- und Dienstaufsicht? Ging das Schreiben an den BSI-Präsidenten vom Generalbundesanwalt auch über Ihren Tisch?

Zeuge Martin Schallbruch: Das Schreiben ging nicht über meinen Tisch. Das habe ich aber sicher nachrichtlich bekommen. Ich kenne den Vorgang.

Marian Wendt (CDU/CSU): Okay. - Von wem wurden dem BSI denn die in der Presse dargestellten Erkenntnisse mit der Bitte um Bewertung der Plausibilität zur Verfügung gestellt?

Zeuge Martin Schallbruch: Von mir. Ich habe vom Bundeskanzleramt eine entsprechende Anfrage bekommen mit der Bitte, das BSI zu befassen, die Erkenntnisse zu plausibilisieren, das an das BSI weitergegeben, und das BSI hat dann diese Plausibilisierung vorgenommen.

Marian Wendt (CDU/CSU): Und was war die Antwort an Sie aus Ihrer Erinnerung? Sie müssen das ja dann weitergeleitet haben. Oder was haben Sie als Antwort weitergeleitet?

Zeuge Martin Schallbruch: Nein, ich habe die Antwort - - Also, das BSI hat dann in der Folge unmittelbar mit dem Bundeskanzleramt kommuniziert, weil das BSI einen gesetzlichen Beratungsauftrag gegenüber jeder Bundesbehörde hat, und den jeweiligen Geheimschutzbeauftragten informiert. Ich habe das sozusagen nur vermittelt. Aber die Erkenntnis des BSI war, dass das BSI das für plausibel hält, aber es kein Beleg ist.

Marian Wendt (CDU/CSU): Würden Sie persönlich dieser Meinung, dieser Auffassung auch folgen?

Zeuge Martin Schallbruch: Ja, absolut.

Marian Wendt (CDU/CSU): Okay. - Vor dem Hintergrund der Berichte über das Kanzlerinnenhandy legte das BSI dann mit Datum vom 5. November gleichen Jahres eine allgemein gehaltene Darstellung zu den Angriffsmöglichkeiten auf die mobile Regierungskommunikation unter dem Titel „Bewertung Angriffsvektoren“ vor. Darin werden verschiedene Angriffsmethoden bei mobilen Kommunikationsmitteln analysiert und hinsichtlich technischer Machbarkeit und praktischer Einsatzwahrscheinlichkeit bewertet. Es gibt dazu auch ein Dokument, das wir Ihnen gerne vorlegen wollen. Das ist MAT A BSI-1-6g, Blatt 40 ff. und ist VS-NfD klassifiziert. Ich lasse Ihnen das kurz mal vorlegen.

(Dem Zeugen werden Unterlagen vorgelegt)

Ist Ihnen bekannt?

Zeuge Martin Schallbruch: Das ist mir bekannt.

Marian Wendt (CDU/CSU): Ja. - Was waren - - Also, Sie sind mit diesem Vorgang vertraut auch demzufolge, oder ist Ihnen das nur allgemein bekannt?

Zeuge Martin Schallbruch: Nein, also mit dem Vorgang bin ich vertraut.

Marian Wendt (CDU/CSU): Gut. - Was waren die wesentlichen Ergebnisse dieser BSI-Analyse?

Zeuge Martin Schallbruch: Unmittelbar nach den Berichten über das sogenannte Kanzlerhandy haben wir das BSI gebeten, die Angriffsvektoren, die es für die Überwachung eines Handys gibt, aufzuschreiben und herauszufinden: Welche Angriffsvektoren sozusagen gibt es, und was für Schutzmaßnahmen kann man dann ergreifen?

Das BSI hat dann nach meiner Erinnerung fünf Angriffsvektoren identifiziert, also sozusagen Datennetz, mit IMSI-Catcher, in einem fremden Mobilfunknetz usw., also wie man die Kommunikation, die über ein Handy geführt wird, abgreifen kann, und hat Gegenmaßnahmen vorgeschlagen: Ende-zu-Ende-Verschlüsselung, Indoor-Anlagen, Verzicht auf DECT-Telefonie usw.

Wir haben das dann im Bundesinnenministerium umgewandelt in etwas, was wir, ich glaube, „Schutzprogramm Regierungskommunikation“ nannten - oder so ähnlich. Das heißt, wir haben daraus ein Programm gemacht, was zusätzliche Maßnahmen und auch zusätzliche Investitionen in die Sicherheit der Regierungskommunikation umfasste.

Marian Wendt (CDU/CSU): Und damit war auch sichergestellt, dass alle fünf Vektoren, sage ich mal so, auch abgedeckt waren.

Zeuge Martin Schallbruch: Sicherstellen kann man das nicht. Ich fange mal an mit dem ersten Vektor. Wenn jetzt jemand, der ein Kryptohandy hat, dieses Kryptohandy nicht benutzt, sondern irgendwie über eine offene Leitung kommuniziert oder das Gespräche persönlich führt oder Ähnliches, da kann man mit Technik nichts gegen machen. Oder wenn ich den fünften Vektor nehme, den Zugriff auf Geräte in ausländischen Mobilfunknetzen: Können wir auch nur sehr schwer beeinflussen.

Insofern sind das alles risikoreduzierende Maßnahmen gewesen, die wir da vorgeschlagen haben und die dann auch gebilligt worden sind.

Marian Wendt (CDU/CSU): Sie haben dann eine Analyse vorgelegt. Gab es aufgrund der Analyse auch einen Maßnahmenplan? Sie hatten das ja vorhin skizziert: Es gab es dann mehr Kryptohandys. Das ist ja auch immer die Frage, die sich mir stellt: Umgang damit. Wurde das auch genutzt aus Ihrer Sicht heraus?

Der Mensch ist ja das Hauptproblem, wenn es um Fragen der IT-Sicherheit immer wieder geht - natürlich, klar. Er muss die Dinge auch nutzen, und eine hundertprozentige Sicherheit gibt es ja nicht; das ist uns auch klar. Wir versuchen, uns diesen 100 irgendwo anzunähern durch verschiedene Maßnahmen. Inwieweit hat das, sage ich mal, so zu einem Veränderungsprozess innerhalb der Bundesregierung geführt von Mitarbeitern?

Wir haben das auch im Bundestag selber; da nehme ich uns auch nicht aus. Klar, man ist manchmal leichtsinnig mit gewissen Sachen, sicherlich auch mit Passwörtern und Ähnlichem, was es alles gibt. Inwieweit würden Sie sagen - - Gab es erst einen Maßnahmenplan konkret? Wie tief sah der aus? Also, sagte der: „Alle Abteilungsleiter kriegen ein Kryptohandy oder bestimmte Bereiche“? Wie tief ging das ungefähr? Und wie ist dann der Erfolg gewesen aus Ihrer Sicht?

Zeuge Martin Schallbruch: Es gab einen Maßnahmenplan, den das Bundesinnenministerium gemacht hat, der dann irgendwo um den Zeitraum November/Dezember 2013 herum vom damaligen Minister gebilligt wurde, auch zusätzliche Investitionen vorsah, der aber im Wesentlichen die Bereitstellung zusätzlicher Geräte, Server, Indoor-Anlagen oder Ähnliches vorsah. Allerdings liegt es in der Verantwortung der Ressorts und der einzelnen Behörden, festzulegen, welche Bediensteten solche Geräte bekommen. Das ist nichts, was das BMI zentral machen kann, sondern das muss dezentral entschieden werden. Es

gibt Behörden, in denen also bis runter Referatsleiterebene alle solche Geräte haben, völlig egal, wo sie arbeiten. Und es gibt andere, wo nur in wesentlichen sicherheitsrelevanten Bereichen Kryptogeräte eingesetzt werden.

Die Nutzung ist dann noch mal eine andere Frage. Ich habe wahrgenommen, dass wir in den Jahren 2007 bis 2012, in denen wir uns bemüht haben, sichere Smartphones, sage ich mal, an die Frau und an den Mann zu bringen, einen ziemlichen Gegenwind hatten. Aus den Ressorts gab es immerzu Aussagen wie: „Das funktioniert nicht so gut wie ein iPhone, die Akkulaufzeit ist zu gering, es ist zu umständlich und usw. usf.", was in der Tat so ist bei speziell abgesicherten Geräten. Dieser starke Widerstand ist nach 2013, glaube ich, ein Stück weit gewichen, und wir haben jetzt doch eine höhere Akzeptanz für gesicherte Kryptogeräte.

Marian Wendt (CDU/CSU): In der gleichen Analyse, die mir vorliegt, wird auch zu möglichen Angriffsmöglichkeiten, speziell zur Platzierung von passiven Empfangsantennen, sich geäußert. Ich darf zitieren:

> Diese Angriffsmethode wird als sehr wahrscheinlich angesehen.
>
> Begründung:
>
> Mit verborgenen Richtantennen an wenigen zentral gelegenen Standorten (z. B. ausländischen Botschaften) kann die Mobilkommunikation in Berlin-Mitte nahezu flächendeckend massenhaft abgehört werden. Die gezielte Überwachung ausgewählter Personen ist bei Kenntnis der Mobilfunknummer möglich, ohne dass dies messtechnisch nachweisbar wäre.

Ende des Zitats.

Die Analyse erinnert ja an die immer wiederkehrenden Berichte über auffällige Aufbauten auf den Botschaftsgebäuden Russlands, Großbritanniens, USA usw. Und dazu heißt es weiter in dem Bericht - Zitat -:

> Insbesondere in der Nähe von Orten mit hoher Aufenthaltswahrscheinlichkeit ...

von Regierungsvertretern

> (BK-Amt, Bundestag)

- obwohl der Bundestag natürlich keine Regierungsvertretung ist, möchte ich anmerken -

> und der Nähe zu exterritorialen Gebäuden ist der Einsatz eines Breitbandempfängers eine Angriffmethode, die ... keinerlei Spuren hinterlässt, ... nahezu nicht nachweisbar zu installieren ist und ... eine hohe Mitschnittquote aufweist.

War Ihnen, der Sie mit der Fachaufsicht über das BSI betraut waren, das Ausmaß bekannt vorher schon?

Zeuge Martin Schallbruch: Die Möglichkeiten waren ja immer schon bekannt, ja, bestimmt schon seit 2002/2003, schätze ich mal, und hat auch immer Eingang gefunden in unsere Argumentation gegenüber den Ressorts. Sie haben eben gefragt nach der Veranstaltung für den Chef des Bundeskanzleramts im Mai 2006.

Marian Wendt (CDU/CSU): Genau.

Zeuge Martin Schallbruch: Da wurde das auch vorgetragen, und eine der Folgen war beispielsweise, dass wir dann Sensibilisierungsveranstaltungen durchgeführt haben, zum Beispiel für Büroleiter von Ministern und Ähnliches, um darauf hinzuweisen, dass, wenn man mit ungeschützten Telefonen kommuniziert, dann nicht ausgeschlossen werden kann, dass durch eine passive Empfangseinrichtung - sei es irgendwo stationär oder auch eine mobile Einrichtung - diese Kommunikation mitgeschnitten werden kann. Diese Möglichkeit war mir bekannt, und jeder, der kein Kryptotelefon einsetzt, muss eben damit rechnen, dass diese Möglichkeit besteht.

Marian Wendt (CDU/CSU): Also, das ist interessant, weil diese gleiche Analyse - - Wir hatten ja

schon verschiedene Zeugen sitzen. Auch das BfV zum Beispiel kommt natürlich zu den gleichen Bewertungen. Wenn Sie sagen, Sie haben bereits seit 2002/2003 darauf hingewiesen, und als Sie eben ausführten, zwischen 2007 und 2012 war man wenig offen für die verbesserte Sicherung der Kommunikation, dann gibt einem das natürlich schon zu bedenken und Fragestellungen einfach, ja. Hat Sie das nicht demotiviert, -

Zeuge Martin Schallbruch: Na ja.

Marian Wendt (CDU/CSU): - wenn Sie natürlich wissen, die Gefahren bestehen und es wird nicht so recht auf Sie gehört?

Zeuge Martin Schallbruch: „Demotiviert" ist in dem Zusammenhang keine Kategorie, die ich irgendwie relevant finde, sondern mich hat das dazu motiviert, das Bemühen zu verstärken, auch vernünftige Lösungen anzubieten. Ich habe mich sehr intensiv um die Weiterentwicklung von sicheren Smartphones beispielsweise gekümmert, damit die Akzeptanz vergrößert werden kann, weil man schon sagen muss: Die Nutzung von Sicherheitseinrichtungen erreicht man nur dann, wenn ein Stück weit Einsicht da ist und wenn auch irgendwas zur Verfügung steht, was auch alltagstauglich ist. Und wenn man als viel beschäftigter Beamter, Politiker ständig kommunizieren muss, dann muss man auch ein vernünftiges Gerät im Einsatz haben, und die Sicherheitslösungen sind eben mit Komforteinbußen verbunden. Insofern war meine Motivation mehr, in diese Richtung da noch besser zu werden.

Marian Wendt (CDU/CSU): Also kann man schon sagen, dass Ihre Warnungen schon - - also dass man nicht sagen kann, dass erst in der Bundesregierung der erste Gedanke kam mit Herrn Snowden: „Oh, wir müssen jetzt was für die IT-Sicherheit und den nachrichtendienstlichen Abgriff tun", sondern den Fachleuten und vielen Ebenen war schon vorher weit bekannt, und Snowden war vielleicht noch mal dieser öffentliche Aufschrei, sage ich mal so, mehr nicht, so eine Art letzter Anstoß. Oder wie kann man das vielleicht urteilen?

Zeuge Martin Schallbruch: Genau so würde ich das beschreiben.

Marian Wendt (CDU/CSU): Ja, okay. - Ich habe meinen letzten Bereich. Herr Vorsitzender, wir müssen da ja wieder weiter. - Die Bundesregierung hat ja - Sie haben es auch beschrieben - in den letzten Jahren sowohl auf nationaler als auch auf internationaler Ebene viel für den Schutz der Privatsphäre bewegt. Es ist unter anderem auf deutsche Initiative zurückzuführen, dass mehrere VN-Resolutionen verabschiedet und das Mandat eines VN-Sonderberichterstatters für das Recht auf Privatsphäre geschaffen wurde. Wie würden Sie das beurteilen, die Ergebnisse dessen, die Initiativen? Und wo wurden wirklich echte Verbesserungen erreicht?

Zeuge Martin Schallbruch: Das liegt ganz überwiegend außerhalb meiner Zuständigkeit.

Marian Wendt (CDU/CSU): Okay.

Zeuge Martin Schallbruch: Ich habe nur zugeliefert, was die deutschen Vorschläge angeht, weil ich überzeugt war und auch durch eigene Aktivitäten auf internationaler Ebene mich dafür eingesetzt habe, dass wir zu stärkeren globalen Standards für vertrauenswürdige Informationstechnik kommen müssen, die sicherstellen, dass wir auch ein offenes, benutzbares, innovationsoffenes, freies Internet auf Dauer erhalten können. Also, an diesen Initiativen habe ich mich mit meiner Abteilung eigentlich immer beteiligt, aber das war typischerweise nicht in meiner Federführung.

Marian Wendt (CDU/CSU): Okay, gut. - Dann danke ich Ihnen. Die Unionsfraktion hat dann erst mal keine weiteren Fragen. Wir danken für die Befragung und sehen uns sicherlich an der einen oder anderen Stelle zum Thema „IT-Sicherheit" bestimmt wieder.

Vorsitzender Dr. Patrick Sensburg: Danke schön. - Dann kommen wir jetzt zur nächsten Fraktion, der Fraktion Die Linke, und Frau Kollegin Renner stellt die Fragen.

(Martina Renner (DIE LINKE): Wir haben erst mal keine weiteren Fragen mehr!)

- Herzlichen Dank. - Dann kommen wir zur Fraktion der SPD.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Die SPD hat auch keine Fragen!)

Herr Kollege?

(Christian Flisek (SPD): Keine Fragen!)

Dann sind wir bei der Fraktion Bündnis 90/Die Grünen, und der Kollege Ströbele hat noch Fragen.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. - Herr Schallbruch, benutzen Sie eigentlich ein Kryptohandy immer?

Zeuge Martin Schallbruch: Ich habe immer ein Kryptohandy benutzt in der Zeit, in der ich im BMI tätig war, für meine dienstlichen Geschäfte, und jetzt als Wissenschaftler an der Hochschule wird mir kein Kryptohandy zur Verfügung gestellt.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und wenn Sie sich umgeschaut haben im Bundesinnenministerium: Was schätzen Sie, wie viel Prozent sind Ihrem Rat gefolgt?

Zeuge Martin Schallbruch: Ich kann da keine Schätzung abgeben. Ich weiß nur, dass wir im Bundesinnenministerium doch eine hohe Anzahl Kryptohandys - ich glaube, 200 bis 250 - ausgegeben haben und dass ich auch wichtige Kommunikation - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): 250 im Innenministerum.

Zeuge Martin Schallbruch: In der Größenordnung - - und dass ich auch meine wesentlichen Kommunikationspartner in der Tat auch darüber erreichen konnte.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja. - Haben Sie nur ein Kryptohandy gehabt, oder haben Sie auch bestimmte Gespräche mit dem normalen Handy oder mit einem Nicht-Kryptohandy geführt?

Zeuge Martin Schallbruch: Das Gerät, ~~was~~ das im BMI im Einsatz war und auch in anderen Bundesministerien - es gibt da verschiedene Linien -, ist ein abgesichertes Smartphone, ~~was~~ das mein einziges dienstliches Gerät ~~war~~ ist, mit dem also die Kommunikation der E-Mails, also zum Beispiel der Zugriff auf die dienstlichen E-Mails, auf den dienstlichen Kalender, auf die dienstlichen Adressen, immer verschlüsselt ist und mit dem auch dienstliche Gespräche kryptiert geführt werden konnten, ich aber auch in der Lage war, ein Gespräch mit einem Partner, der kein Kryptogerät hat, offen zu führen. Insofern ist das kein Gerät, ~~was~~ das nur kryptiert kommunizieren kann, sondern das können Sie für alle Zwecke einsetzen. Und wenn Sie dann eben eine kryptierte Kommunikation führen wollen, dann können Sie dieses Gerät eben, wenn Ihr Partner auch so ein Gerät hat, dafür benutzen.

H das

H Es war das

H das

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, ja, das war aber nicht meine Frage. Meine Frage war eigentlich, ob Sie daneben auch ein anderes Handy, also normal oder jedenfalls nicht Krypto - - Weil wir wissen ja von der Kanzerin - jedenfalls liest man das in der Zeitung -, dass sie auch ein Kryptohandy hat, und trotzdem hat sie mit dem Nicht-Kryptohandy telefoniert.

(Dr. André Hahn (DIE LINKE): Ja, das ist das Problem!)

Zeuge Martin Schallbruch: Da ich mit dem dienstlichen Gerät keine privaten Gespräche führen kann, habe ich natürlich auch ein privates Gerät gehabt.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ah ja. - Und gibt es da fließende Grenzen, also vom Inhalt, was Sie da kommunizieren?

Zeuge Martin Schallbruch: Die Kryptogeräte oder die Kryptokommunikation ist ja für die Fälle notwendig, in denen man VS-NfD-Inhalte austauscht.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja.

Zeuge Martin Schallbruch: Es ist ja nicht für jedes dienstliche Gespräch so, dass man kryptiert kommunizieren muss. Und insofern ist, sagen wir mal, eigentlich die Bedeutung - - Oder man weiß eigentlich in der Regel, was ein bedeutendes Gespräch ist, ~~was~~ das man dann eben auch kryptiert führen sollte.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, aber wir haben ja gehört, der Mensch ist das Problem. Ihr Rat, Kryptohandys - - oder Ende-zu-Ende zu verschlüsseln, gilt doch für alle, oder nur für Sie und das Bundesinnenministerium?

Zeuge Martin Schallbruch: Das gilt für alle, und ich kann nur das aufnehmen, was Sie gesagt haben: Der Menschen ist das Problem. Wir wissen alle, dass viele Leute unkryptiert kommunizieren und dass wir - -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ja, wahrscheinlich 99 Prozent.

Zeuge Martin Schallbruch: Wahrscheinlich 99 Prozent. - Und jedes kryptiert geführte Gespräch und jede kryptierte E-Mail sind eine Verbesserung. Insofern kann man die IT-Sicherheit sehr einfach verbessern, indem man nämlich in der tagtäglichen Benutzung öfter auf kryptierte Kommunikation zurückgreift.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Und wie viele waren das jetzt für die ganze Bundesregierung? Gehört bei den Bundesorganen auch der Bundestag dazu?

Zeuge Martin Schallbruch: Nein, der Bundestag ist bei der Beschaffung seiner Informationstechnik selbstständig. Ich weiß nicht, ob der Bundestag solche Geräte beschafft hat. Er kann die Rahmenverträge nutzen, die die Bundesregierung geschlossen hat für den gesamten Bund. Der Bund hat aus dem IT-Investitionsprogramm im Zeitraum 2009 bis 2011, ich glaube, ungefähr 5 000 Kryptosmartphones und 4 500 Kryptotelefone beschafft und an Bundesbehörden ausgegeben.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Weil, ich meine, ich halte mich ja häufig hier im Bundestag auf, und wenn ich die Kollegen sehe, habe ich eigentlich noch nie einen mit einem Kryptohandy telefonieren sehen.

Zeuge Martin Schallbruch: Ja, aber das, Herr Abgeordneter, liegt möglicherweise daran, dass man die Geräte nicht mehr unbedingt erkennt. Also, das aktuell verbreitetste Gerät -

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Sie können ja mal hier rumgucken.

Zeuge Martin Schallbruch: - aus der Blackberry-X10-Reihe sieht nicht viel anders aus wie so ein Samsung oder iPhone. Also, das würden Sie jetzt auf die Entfernung - - Wenn es bei mir hier läge, würden Sie nicht erkennen, ob das ein solches Gerät ist oder ein anderes.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Jetzt habe ich noch eine andere Frage. Waren Sie auch befasst mit der Sicherheit von Daten, die nach außen an ausländische, also an andere Staaten, an fremde Mächte weitergegeben werden?

Zeuge Martin Schallbruch: Nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Das war nicht Ihr Gebiet.

Zeuge Martin Schallbruch: Das war nicht mein Gebiet.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Also dass die sicher sind und so oder dass - -

Zeuge Martin Schallbruch: Damit war ich nicht befasst, nein.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Okay. - Danke.

Vorsitzender Dr. Patrick Sensburg: So, jetzt schaue ich mal in die Runde. Das würde genau passen von der Zeit. Wenn im öffentlichen Teil keine Fragen mehr sind, dann können wir noch schnell einen Beschluss fassen und dann dann zur Abstimmung gehen. Ich schlage folgenden Beschluss vor:

Für die weitere Vernehmung des Zeugen Schallbruch am heutigen Tag wird die Öffentlichkeit gemäß § 14 Absatz 1 Nummer 4 des Untersuchungsausschussgesetzes ausgeschlossen, weil besondere Gründe des Wohls des Bundes entgegenstehen.

Wer dem so zustimmen kann, den bitte ich um das Handzeichen. - Herzlichen Dank. Gegenstimmen? - Enthaltungen?

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wollen wir ihn Geheim hören? - Martina Renner (DIE LINKE): Ihn nicht! - Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Ihn nicht!)

- Will ihn keiner Geheim hören? Eingestuft? - Nein? - Dann ist der Beschluss trotzdem schön, rechtlich richtig, aber wird nicht umgesetzt. Mit anderen Worten: Ich bedanke mich bei Ihnen ganz herzlich dafür, dass Sie uns Rede und Antwort gestanden haben, so gut und so offen, dass wir anscheinend keine nichtöffentliche oder eingestufte Sitzung mehr brauchen, und wünsche Ihnen einen schönen Nachmittag. Danke, dass Sie bei uns waren.

Die Sitzung ist unterbrochen für die nächste namentliche Abstimmung. Wir sehen uns dann im üblichen Sitzungssaal für nichtöffentlich oder Geheim wieder.

An die Öffentlichkeit: Ganz herzlichen Dank, dass Sie bei uns waren. Die nächsten Zeugen werden nichtöffentlich vernommen. Damit ist für Sie bei ungefähr 30 Grad draußen jetzt Feierabend. Wir machen hier in gekühlten Räumen noch ein bisschen weiter. Danke, dass Sie da waren. Schönen Feierabend für Sie!

Bei uns geht es gleich nach Umzug weiter im üblichen Sitzungssaal mit dem Zeugen Dr. Even.

(Schluss des Sitzungsteils Zeugenvernehmung, öffentlich: 18.12 Uhr - Folgt Sitzungsteil Zeugenvernehmung, Geheim)