Deutscher Bundestag
1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Stenografisches Protokoll
der 9. Sitzung
- Endgültige Fassung* -

1. Untersuchungsausschuss
Berlin, den 26. Juni 2014, 9.30 Uhr
Paul-Löbe-Haus, Europasaal (4.900)
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Prof. Dr. Patrick Sensburg, MdB

Tagesordnung

Tagesordnungspunkt

Öffentliche Anhörung von Sachverständigen (Beweisbeschluss SV-1): *Seite 4*

- Prof. Dr. Michael Waidner
- Dr. Sandro Gaycken
- Frank Rieger

* Hinweis:
Die Korrekturen und Ergänzungen des Sachverständigen Prof. Dr. Michael Waidner (Anlage 1), sind in das Protokoll eingearbeitet.

Deutscher Bundestag
1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Mitglieder des Ausschusses

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

Fraktionsmitarbeiter

CDU/CSU	Bosnjak, Niko Bredow, Lippold von Cossel, Claudia von Feser, Dr. Andreas Hugo, Jasmin Kühnau, Dan
SPD	Ahlefeldt, Johannes von Dähne, Dr. Harald Etzkorn, Irene Geiger, Nicolas Hanke, Christian Diego Hawxwell, Anne Heyer, Christian Olechnowicz, Christin
DIE LINKE.	Lehmann, Dr. Jens Scheele, Dr. Jürgen
BÜNDNIS 90/DIE GRÜNEN	Kant, Martina Leopold, Nils Pohl, Jörn Weinzierl, Dr. Ruth

Deutscher Bundestag
1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Teilnehmer Bundesregierung

Bundeskanzleramt	Bernard, Jan Wolff, Philipp Zygojannis, Dr. Philipp
Auswärtiges Amt	Berkemeier, Gunnar Lehmann, Uta
Bundesministerium des Innern	Akmann, Torsten Darge, Dr. Tobias Gierth, Sonja Hauer, Florian Jacobi, Stephan Weiss, Jochen
Bundesministerium für Verteidigung	Henschen, Elmar Meyer Rahn Rauch, Rüdiger Theis, Björn
Bundesministerium für Wirtschaft und Energie	Rosenberg, Dr. Malte

Teilnehmer Bundesrat

LV Bayern	Luderschmid, Florian
LV Hessen	Steinbach, Arvid Vogel
LV Sachsen	Lang, Julia

(Beginn: 10.45 Uhr)

Vorsitzender Dr. Patrick Sensburg: Meine sehr verehrten Damen und Herren! Ich eröffne die 9. Sitzung des 1. Untersuchungsausschusses der 18. Wahlperiode.

Nach Artikel 44 Absatz 1 des Grundgesetzes erhebt der Untersuchungsausschuss seine Beweise in öffentlicher Verhandlung. Ich stelle fest: Die Öffentlichkeit ist hergestellt. Die Öffentlichkeit und die Pressevertreter darf ich hier an dieser Stelle besonders begrüßen. Ich freue mich, dass Sie da sind und an diesem wichtigen Thema Anteil nehmen und uns unterstützen.

Bevor ich zum eigentlichen Gegenstand der heutigen Sitzung komme, gestatten Sie mir einige Vorbemerkungen - die, die an den Beweiserhebungen bisher teilgenommen haben, kennen diese Vorbemerkungen schon -: Ton- und Bildaufnahmen sind während der öffentlichen Beweisaufnahme grundsätzlich nicht zulässig. Wegen des besonderen öffentlichen Interesses hat der Ausschuss nach § 13 des Untersuchungsausschussgesetzes beschlossen, von der heutigen Sitzung ausnahmsweise eine Videoaufzeichnung durch die Bundestagsverwaltung fertigen zu lassen. Diese wird mit geringem Zeitversatz im Hauskanal des Deutschen Bundestags übertragen. Sonstige Bild-, Ton- oder Filmaufzeichnungen sind nicht zulässig. Entsprechende Geräte sind abzustellen.

Ein Verstoß gegen dieses Gebot kann nach dem Hausrecht des Bundestages nicht nur zu einem dauerhaften Ausschluss von den Sitzungen dieses Ausschusses sowie des ganzen Hauses führen, sondern gegebenenfalls strafrechtliche Konsequenzen nach sich ziehen.

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

> Öffentliche Anhörung von Sachverständigen
> (Beweisbeschluss SV-1)
>
> - Prof. Dr. Michael Waidner
> - Dr. Sandro Gaycken
> - Frank Rieger

Thema der Sachverständigenanhörung ist die - ich zitiere wörtlich aus dem Beweisbeschluss -

> Darlegung der technischen Gegebenheiten im Untersuchungszeitraum bei der Entstehung, Übertragung und Speicherung privater und behördlicher Telekommunikations- und Internetnutzungsdaten aller Art sowie den Zugriffsmöglichkeiten … hierauf, möglichen technischen Konsequenzen aus in der Vergangenheit bekannt gewordenen Angriffen auf staatliche und private Informationsstrukturen im Internet sowie der technischen Möglichkeiten der Abwehr von Datenerfassung auf Vorrat aus Kommunikationsvorgängen (einschließlich Inhalts-, Bestands- und Metadaten) von, nach und in Deutschland durch Nachrichtendienste der Staaten der sog. „Five Eyes“ oder im Auftrag von Nachrichtendiensten der Staaten der sog. „Five Eyes“.

Dazu ganz herzlich begrüßen darf ich unsere Sachverständigen:

Herrn Professor Dr. Michael Waidner. Michael Waidner ist der Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie, Fraunhofer SIT, und zugleich Inhaber des Lehrstuhls für Sicherheit in der Informationstechnik an der Technischen Universität Darmstadt. Seien Sie herzlich begrüßt!

Herrn Dr. Sandro Gaycken, Appointed Director of the NATO SPS Program on National Cyber-security Strategies, Associate Fellow of Oxford University’s Martin College und Senior Fellow at the EastWest Institute. Seien Sie herzlich begrüßt!

Und Herrn Frank Rieger. Frank Rieger ist deutscher Hacker, Sachbuchautor, Technikpublizist, Internetaktivist und einer der Sprecher des Chaos Computer Clubs. Seien Sie herzlich begrüßt!

Heute nicht anwesend sein kann der Sachverständige Christopher Soghoian. Wegen eines Flugzeugschadens war es ihm nicht möglich, die Anreise termingerecht zum Untersuchungsausschuss zu bewerkstelligen. Es ist sehr schade, dass wir Herrn Soghoian heute nicht hören können. Die Obleuterunde hat sich gestern darauf geeinigt, dass wir gegebenenfalls

Herrn Soghoian zu einem späteren Zeitpunkt hören können, weil sicherlich auch sein Statement für den Untersuchungsausschuss von Relevanz sein kann. Und dann überlegen wir, ihn zu einem dann passenden Themenkomplex noch einmal zu hören, und hoffen dann, dass die Flugverbindungen dementsprechend glücklicher verlaufen.

Umso mehr freut es mich, bei den Sachverständigen Frank Rieger begrüßen zu können, und darf mich ganz herzlich bedanken, dass Sie sich so kurzfristig bereit erklärt haben, zur Verfügung zu stehen.

Ich stelle fest, dass die Sachverständigen ordnungsgemäß geladen sind, auch wenn es dann mit so kurzer Frist gewesen ist. Herr Professor Dr. Michael Waidner, Sie haben die Ladung am 28. Mai 2014 erhalten. Herr Dr. Sandro Gaycken, Sie haben die Ladung am 20. Mai 2014 erhalten. Und Herr Frank Rieger, Sie haben die Ladung am 25. Juni 2014 per E-Mail erhalten und sind dankenswerterweise hier. Damit ist die Ladung ordnungsgemäß erfolgt.

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 Aufnahme wird nach Erstellung des Protokolls wieder gelöscht.

Das Protokoll dieser Anhörung wird Ihnen nach Fertigstellung zugestellt. Sie haben, falls dies gewünscht ist, die Möglichkeit, innerhalb von zwei Wochen Korrekturen und Ergänzungen - wo Fehler im Protokoll aus Ihrer Sicht sein sollten - vorzunehmen. Haben Sie hierzu noch Fragen? - Ich sehe, das ist nicht der Fall.

Vor Ihrer Anhörung habe ich Sie zunächst zu belehren. Sie sind als Sachverständige geladen worden. Als Sachverständige sind Sie verpflichtet, die Wahrheit zu sagen. Ihr Gutachten ist unparteiisch und nach bestem Wissen und Gewissen zu erstatten.

Ich habe Sie außerdem auf die Möglichkeit strafrechtlicher Folgen eines Verstoßes gegen die Wahrheitspflicht hinzuweisen. Wer vor dem Untersuchungsausschuss uneidlich falsch aussagt, kann gemäß § 162 in Verbindung mit § 153 des Strafgesetzbuches mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren oder mit Geldstrafe bestraft werden.

Nach § 28 in Verbindung mit § 22 Absatz 2 des Untersuchungsausschussgesetzes können Sie allerdings 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 Ordnungswidrigkeiten auch Disziplinarverfahren. Haben Sie hierzu Fragen? - Ich sehe, das ist nicht der Fall.

Nach diesen notwendigen Vorbemerkungen darf ich Ihnen den geplanten Ablauf kurz darstellen. Zu Beginn haben Sie nach § 28 in Verbindung mit § 24 Absatz 4 des Untersuchungsausschussgesetzes Gelegenheit, zum Beweisthema im Zusammenhang vorzutragen. Zunächst erhält Professor Dr. Michael Waidner das Wort, im Anschluss Herr Dr. Sandro Gaycken und zum Schluss Herr Frank Rieger. Ich bitte Sie dabei, sich jeweils an einen Zeitrahmen von circa 15 Minuten für Ihre Eingangsstatements zu halten. Anschließend haben die Mitglieder des Untersuchungsausschusses Gelegenheit, Nachfragen zu stellen. Dies geschieht dann nach dem Stärkeverhältnis der Fraktionen. Und Sie bekommen danach wieder die Möglichkeit, zu antworten. Haben Sie hierzu Fragen? - Ich sehe, das ist nicht der Fall.

Dann sollten wir uns auch die Möglichkeit geben, an Ihrem Wissen zu partizipieren, und ich darf in die Runde der kurzen Eingangsstatements einsteigen und darf zunächst Herrn Professor Dr. Michael Waidner das Wort für seinen zusammenhängenden Sachverhaltsvortrag geben. Ich darf Ihnen das Wort geben. Bitte schön.

Sachverständiger Prof. Dr. Michael Waidner: Vielen Dank. - Sehr geehrter Herr Vorsitzender! Meine Damen und Herren Abgeordneten! Zunächst möchte ich mich herzlich bedanken für die Einladung zu einer Stellungnahme vor dem NSA-Untersuchungsausschuss, die ich natürlich sehr gerne angenommen habe.

In den Leitfragen des Ausschusses wurden für die Sachverständigen vier Fragenkomplexe definiert, nämlich: Erstens. Wie funktioniert das Abhören Einzelner und vieler? Zweitens. Wie lassen sich aus abgehörten Daten relevante Informationen gewinnen? Drittens. Wie können

Nutzer und Hersteller die Sicherheit verbessern? Viertens. Was kann der Gesetzgeber tun? - In meiner schriftlichen Stellungnahme entsprechen diese vier Komplexe den Abschnitten 2 bis 5. Im Folgenden möchte ich zu jedem Komplex kurz die wichtigsten Punkte herausgreifen.

Zum ersten Fragenkomplex: Wie funktioniert Abhören Einzelner und vieler? Aus technischer Sicht kann ich sagen, dass die Snowden-Dokumente, um die es in diesem Untersuchungsausschuss geht, durchweg plausibel sind. Die dort dargestellten Angriffstechniken entsprechen sozusagen dem Stand der schwarzen Kunst in der Sicherheitsforschung. Sie gehen aber nicht prinzipiell darüber hinaus. In diesem Sinne war die Sicherheitsforschung nicht überrascht von den Techniken, wie sie in den Snowden-Dokumenten dargestellt werden, wohl aber davon, in welchem Umfang sie angewandt wurden.

Nun zu Ihrer Frage, wie abgehört werden kann: Das Internet, auf welches ich mich hier konzentriere, ist mit Abstand das wichtigste Kommunikationsnetz - sowohl für die individuelle Kommunikation wie auch als Backbone für praktisch jede Form der Weitverkehrskommunikation, etwa den internationalen Telefonverkehr.

Zu Beginn des Internets in den 1960er-/1970er-Jahren spielte Sicherheit auf Netzwerkebene keine Rolle. Als Folge ist das Internet bis heute ein ungesichertes Netz. Wer Zugriff auf eine Leitung oder einen Netzknoten hat oder sich verschaffen kann, kann dort auch abhören, und zwar ohne jedes Risiko, dass jemand dies bemerken könnte. Besonders kritisch sind die Stellen und Organisationen, über die ohnehin ein großer Teil des Internetverkehrs läuft, also zum Beispiel die internationalen Telekommunikationsanbieter und die Internet Exchange Points.

Das Internet erlaubt einem Angreifer sogar, gezielt interessante Nachrichten über eigene Systeme umzuleiten. Der Angreifer schaltet sich hierbei zwischen Sender und Empfänger und kann so die Kommunikation als Man in the Middle mitlesen. Beispielsweise wurde so 2013 der Internetverkehr innerhalb der amerikanischen Stadt Denver im Bundesstaat Colorado komplett über einen ISP in Island gelenkt und dort vermutlich auch ausgeleitet. Das Internet hat also, bildlich gesprochen, zahlreiche offene Türen, durch die Kommunikation ausgespäht werden kann. Grundsätzlich effektiver, als Spähangriffe lediglich zu verbieten, ist es, sie technisch auch zu verhindern.

Erfreulicherweise kennt die IT-Sicherheit für das beschriebene Abhörproblem auch schon seit langem die Lösung. In der Fachwelt herrscht Einigkeit darüber, dass Ende-zu-Ende-Verschlüsselung das geeignete Instrument ist, das Internet gegen Abhören zu schützen. Ende-zu-Ende-Verschlüsselung bedeutet, dass Nachrichten vom Sender verschlüsselt werden, dann verschlüsselt durch das Netz laufen und erst beim endgültigen Empfänger wieder entschlüsselt werden. Die Ende-zu-Ende-Verschlüsselung ist allen anderen bekannten Ansätzen deutlich überlegen, selbstverständlich auch dem sogenannten Schengen-Routing oder einer Verschlüsselung nur auf den Verbindungen zwischen Servern.

Die flächendeckende Einführung von Ende-zu-Ende-Verschlüsselung setzt aber eine Investition in Vertrauensinfrastrukturen, sogenannte Public-Key-Infrastrukturen, voraus. Solche PKIs sind erforderlich, um die korrekte Zuordnung eines Schlüssels zu einer Person oder Organisation oder auch zu einem Objekt zu gewährleisten. Dadurch kann man zum Beispiel Man-in-the-Middle-Angriffe durch betrügerisch untergeschobene Schlüssel verhindern. Die flächendeckende Einführung von Ende-zu-Ende-Verschlüsselung halte ich für einen ebenso wichtigen Aspekt der Grundversorgung einer digitalen Gesellschaft wie etwa den Breitbandausbau.

Nun zum zweiten Fragenkomplex: Wie lassen sich aus abgehörten Daten relevante Informationen gewinnen? Zunächst möchte ich kurz erläutern, was man unter Inhalts- und Metadaten versteht. Inhaltsdaten sind all die Daten, um die es in einer Kommunikation eigentlich geht, also etwa Bild- und Tonaufnahmen, E-Mails, Webseiten, Anfragen an Suchmaschinen oder auch die vielen Sensordaten aus der Smart Factory oder dem Smart Home. Alle anderen Daten sind Metadaten, also beispielsweise Adressen, Zeitpunkt, Umfang einer Kommunikation, Standorte, aber auch Hilfsdaten zum schnelleren Suchen wie

Datenbankindizes und automatisch erstellte Annotationen.

In der Praxis verschwimmen die Grenzen zwischen Inhalts- und Metadaten, und spätestens in der Verarbeitung wird diese Unterscheidung bedeutungslos. Mit zwei Beispielen möchte ich dies illustrieren. Beispiel 1: Medien kann man automatisiert annotieren und damit[1] einer effizienten Suche erschließen. Aus Tonaufnahmen kann man automatisiert den gesprochenen Text extrahieren. Aus Bildaufnahmen kann man entsprechend Personen, Orte, teilweise sogar Szenen extrahieren und erkennen. Aus Texten, E-Mails, Webkommentaren kann man die Sprache und diverse Attribute des Sprechenden extrahieren. Aus Inhaltsdaten werden damit Metadaten.

Umgekehrt Beispiel 2: Aus den Verbindungsdaten in sozialen Netzen wie Facebook oder LinkedIn, also aus der Wer-kennt-wen-Beziehung, kann man zu einzelnen Personen Kompetenzen, Vorlieben und Neigungen ableiten und in Profilen speichern. Aus Metadaten werden damit also Inhaltsdaten.

Diese Beispiele zeigen, dass Inhalts- und Metadaten gleichermaßen schützenswert sind. Eine unkontrollierte Auswertung führt zu einem Verlust an Privatsphäre und Vertraulichkeit. Schon das Wissen, dass eine solche Auswertung möglich ist, schränkt die Freiheit und Selbstbestimmung ein. Vorverarbeitungen und Auswertungen, wie ich sie in den beiden Beispielen genannt habe, dürften sich auch in Werkzeugen wie XKeyscore finden. Ähnliches findet man auch in kommerziell verfügbaren Big-Data-Lösungen.

Besonders relevant für alle Sicherheitsanwendungen ist die Big-Data-Analyse von Datenströmen in Realzeit. Das ist auch bekannt als Stream Processing. Das gilt für Nachrichtendienste ebenso wie für die Betrugserkennung und die Erkennung von IT-Sicherheitsproblemen in Firmennetzen. Durch Stream Processing werden viele unterschiedliche Datenströme, etwa Audio, Video, Text, beliebige Sensordaten, gleichzeitig verarbeitet, und zwar eben genauso schnell, wie sie entstehen. Ein Datenanalyst kann diese Ströme in seinem Stream-Processing-Werkzeug zusammenfassen, analysieren, daraus neue Ströme generieren und durch Suche nach bekannten Mustern und Anomalien Alarme erzeugen.

Eine solche Anomalie könnte zum Beispiel darin bestehen, dass anhand von LinkedIn-Daten Mitarbeiter einer Rüstungsfirma identifiziert werden und dabei auffällt, dass diese vermehrt in sozialen Netzen von Reisen in Embargostaaten berichten, was den Verdacht einer Verletzung des Embargos nahelegt, also als ein typisches Beispiel aus dem Nachrichtenkontext.

Jetzt zum dritten Fragenkomplex: Wie können Nutzer und Hersteller die Sicherheit verbessern? Hier möchte ich zwei Punkte ansprechen.

Der erste Punkt betrifft die Kryptografie. Wie eben erläutert, ist die Verschlüsselung das wichtigste technische Hilfsmittel zum Schutz gegen Überwachung im Internet. In den Snowden-Dokumenten werden auch Angriffe auf Kryptografie beschrieben. Es ist mir wichtig, festzustellen, dass keiner dieser Angriffe die Kryptografie an sich betrifft. Nach Aussage von Edward Snowden verfügt auch die NSA nicht über das Wissen und die Mittel, nach dem Stand der Wissenschaft sichere Verschlüsselungsverfahren zu brechen. Angegriffen wurden einzelne Standards und Implementierungen, indem dort Entwurfsfehler ausgenutzt oder Hintertüren eingebaut wurden, und auf diese Problematik möchte ich gleich noch im vierten Komplex zurückkommen.

Mein zweiter Punkt betrifft die System- und Softwaresicherheit. Angesichts der zahlreichen Sicherheitsprobleme heutiger IT und der scheinbar unbegrenzten Fähigkeiten der NSA und anderer Organisationen, in IT-Systeme einzudringen, ist man versucht, IT als hoffnungslos unsicher anzusehen und den Kampf sozusagen aufzugeben. Möchte ein Nachrichtendienst um jeden Preis eine bestimmte Person überwachen oder eine bestimmte Anlage sabotieren, so wird man dies alleine mit Mitteln der IT auch tatsächlich nicht verhindern können. Im Zweifel würde auf klassische Mittel der Überwachung oder Sabotage zurückgegriffen werden, also: Es würde schlicht jemand geschickt werden, der die Überwachung durchführt.

In der IT-Sicherheit geht es aber überhaupt nicht darum, jeden denkbaren und beliebig aufwändigen Angriff zu verhindern. Das Ziel der IT-

1) Protokoll korrigiert, siehe Anlage 1.

Sicherheit ist vielmehr, mit möglichst geringen eigenen Kosten die Kosten des Angreifers möglichst weit nach oben zu treiben. Es geht also nicht darum, Angriffe und Werkzeuge, wie im Katalog der NSA beschrieben, komplett zu verhindern, sondern nur darum, deren Entwicklung und Anwendung so teuer zu machen, dass sie nur sehr selektiv eingesetzt werden können. In diesem Sinne: Auch inkrementelle Fortschritte in der IT-Sicherheit können sich lohnen.

Die wichtigste strukturelle Maßnahme zur Verbesserung der IT-Sicherheit ist, in der Industrie den Übergang von einer primär reaktiven zu einer primär proaktiven Sicherheit zu vollziehen. Reaktive Sicherheit bedeutet, dass man Angriffe auf ein System erkennt und dann möglichst schnell darauf reagiert. Bekannte Beispiele sind Antivirenprogramme oder die Software Patches, die mittlerweile alle großen Softwarehersteller regelmäßig zur Verfügung stellen. Dieser Ansatz ist sehr teuer, und naturgemäß tritt er oft erst dann in Aktion, wenn der Schaden schon passiert ist.

Proaktive Sicherheit bedeutet im Gegensatz dazu, dass man das System von Anfang an richtig absichert, also insbesondere Schwachstellen im Entwurf und in der Implementierung vermeidet. Dieser Ansatz ist als Security and Privacy by Design bekannt und gilt als deutlich effektiver und kostengünstiger als der reaktive Ansatz.

Letztlich braucht man aber beide Ansätze. Das heißt, es geht nicht darum, reaktiv vollständig durch proaktiv zu ersetzen, sondern darum, den Fokus in der Industrie in Richtung proaktiv zu verschieben.

Neben dieser strukturellen Maßnahme braucht es auch Forschung und Entwicklung mit dem Ziel, bessere, sicherheitsfreundlichere IT-Architekturen zu entwickeln. Hier gibt es unterschiedliche Ansätze, teilweise schon sehr nahe am Markt, wie der in Deutschland entwickelte sogenannte L4-Mikrokern, teilweise noch eher im Grundlagenforschungsbereich wie neuartige Techniken zum Rechnen auf verschlüsselten Daten, oder sogenannte „clean slate“-Hardware-/-Software-Architekturen.

Damit zum vierten und letzten Fragenkomplex: Was kann der Gesetzgeber tun? Hier möchte ich Ihnen zehn Empfehlungen geben, die ich jetzt kurz zusammenfasse oder kommentiere.

Empfehlung 1 betrifft die Unterstützung für eine flächendeckende Ende-zu-Ende-Verschlüsselung. Die hierfür notwendige Infrastruktur und der Zugriff auf die notwendige Verschlüsselungssoftware gehören zur Grundversorgung einer digitalen Gesellschaft. Der Gesetzgeber sollte deshalb den Aufbau und den Betrieb Ende-zu-Ende-gesicherter Kommunikationsdienste aktiv fördern. Betreiber von Kommunikationsdiensten sollten dazu verpflichtet werden, entsprechende Angebote zu schaffen.

Mit Empfehlung 2 möchte ich anregen, die Markteinführung von Sicherheitslösungen zu beschleunigen. Die marktgetriebenen Innovationszyklen in der IT-Sicherheit sind deutlich länger als im Rest der Informationstechnologien. Das heißt, der Markt alleine reagiert hier sehr, sehr langsam. Betreiber insbesondere von Cloud-Angeboten sollten deshalb verpflichtet werden, zu jedem Dienst stets auch die nach Stand der Technik sicherste Dienstnutzungsvariante anzubieten.

Mit Empfehlung 3 möchte ich anregen, dass die Massenüberwachung durch Nachrichtendienste und die massenhafte Analyse von Nutzerverhalten durch kommerzielle Anbieter gemeinsam betrachtet werden. Abgesehen davon, dass sie für die Menschen beide gleichermaßen bedeutsam sind, greifen Nachrichtendienste direkt oder indirekt auch auf die Daten der kommerziellen Organisationen zu. Und an der Stelle, muss ich zugeben, ist sicherlich auch noch Forschung und Entwicklung notwendig.

Empfehlung 4 zielt auf den Übergang von einem vorwiegend reaktiven zu einem vorwiegend proaktiven Zugang zur IT-Sicherheit. Der Gesetzgeber sollte die Weiterentwicklung und Umsetzung von Security and Privacy by Design fördern. Dies sollte zunächst die Forschung und Entwicklung entsprechender Werkzeuge und Prozesse umfassen. Forschungs- und Innovationsprojekte, in denen Informationstechnologie entwickelt oder angewandt wird, sollten verpflichtet werden, die Fragen der IT-Sicherheit in angemessenem Maße zu berücksichtigen.

Empfehlung 5 betrifft die Überprüfbarkeit von IT-Sicherheit. Der Gesetzgeber sollte die Voraussetzungen dafür schaffen, dass IT-Produkte hinsichtlich ihrer Sicherheitseigenschaften überprüft werden können. Für Produkte, die in sicherheitskritischen Umgebungen eingesetzt werden, sollten solche Überprüfungen verpflichtend sein. Ohne Überprüfbarkeit kann das verloren gegangene Vertrauen in die IT nicht zurückgewonnen werden. Das gilt insbesondere für IT, die nicht aus Deutschland oder Europa stammt, also nach Stand heute für die überwältigende Mehrheit aller Produkte und Dienstleistungen.

Ohne eine Veröffentlichung der Überprüfungsergebnisse und -details kann der Markt nicht zwischen sehr guter und weniger guter IT-Sicherheit unterscheiden. Folglich können die Hersteller sehr guter IT-Sicherheit hieraus keinen Marktvorteil ableiten. Umgekehrt: Durch die gezielte Förderung von Überprüfbarkeit und die Umsetzung in Beschaffungsrichtlinien können Deutschland und Europa entscheidend Einfluss auf die Technologie- und Marktentwicklung nehmen. Die Überprüfbarkeit von IT-Sicherheit erfordert ein hohes Maß an Forschung und Entwicklung und Investitionen in die Infrastruktur und entsprechende Labore.

Empfehlung 6 hat zum Ziel, die Verbraucher als das schwächste Glied in der Kette der IT-Sicherheit zu unterstützen. Verbraucher benötigen für ihre eigene Cybersicherheit eine aktive Interessensvertretung gegenüber Wirtschaft und Staat.

Empfehlung 7 soll der Gefahr von Sicherheitsstandards mit Hintertüren entgegenwirken. Auf europäischer Ebene sollte eine Organisation identifiziert werden, die für eine eigenständige europäische Standardisierung im Bereich der Cybersicherheit verantwortlich ist.

Die wichtigsten Cybersicherheitsstandards werden heute vom US-amerikanischen NIST entwickelt und dann von internationalen Organisationen in anderen Staaten übernommen. Dieser Prozess birgt stets die Gefahr einer einseitigen Bevorzugung US-amerikanischer politischer und wirtschaftlicher Interessen. Eklatant ist das Beispiel der von der NSA eingebrachten geheimen Hintertür in einem kryptografischen Standard des NIST. Eine intensive, aber eben vollständig transparente und über jeden Verdacht erhabene Standardisierung unter europäischer Kontrolle wäre wünschenswert. Die entsprechenden technischen Kompetenzen sind in Europa und Deutschland vorhanden.

Mit Empfehlung 8 möchte ich anregen, ganz gezielt in die Schaffung von großen europäischen Herstellern von IT und IT-Sicherheit zu investieren. Die Überprüfbarkeit von IT-Sicherheit, wie in Empfehlung 5 genannt, kann helfen, Vertrauen wiederherzustellen. Darüber hinaus ist es aber auch erforderlich, die europäische IT- und insbesondere IT-Sicherheitsindustrie zu fördern. Innovationen in der IT entstehen gemeinhin im Zusammenspiel von exzellenter Forschung und starker forschungsnaher Industrie.

Empfehlung 9 betrifft die Cybersicherheitsforschung in Deutschland. Anwendungs- und Grundlagenforschung sind essenziell für die Cybersicherheit. Hier geht es primär darum, die in Deutschland vorhandenen Forschungskapazitäten zur Cybersicherheit weiter zu bündeln, zu fördern und auszubauen. Aus meiner Sicht als Leiter eines der drei vom BMBF finanzierten Kompetenzzentren zur Cybersicherheitsforschung hat sich das Konzept der Bildung von Zentren sehr bewährt und sollte fortgesetzt und ausgebaut werden.

Inhaltlich wurden bereits strategische Schwerpunkte gesetzt, zum Beispiel das schon erwähnte Security and Privacy by Design, und eine kritische Masse von exzellenten Forscherinnen und Forschern erreicht, die auch international als Schwergewicht wahrgenommen wird.

Eine entsprechende Fokussierung auf Cybersicherheit fehlt leider im Programm Horizon 2020 der EU, und Deutschland sollte sich deshalb intensiv für ein gezieltes Forschungsprogramm zur Cybersicherheit auf europäischer Ebene einsetzen.

Mit Empfehlung 10 - das ist meine letzte Empfehlung - möchte ich schließlich eine bessere Verzahnung von Recht und Technikgestaltung im Bereich der Cybersicherheit anregen. Die Entwicklung auf beiden Seiten, dem Recht einerseits und der sich rasant entwickelnden Technik andererseits, sollte kontinuierlich verfolgt und ihre Verträglichkeit sichergestellt werden. Dadurch soll Investitionssicherheit

erhöht und rechtliche Unsicherheit nach Möglichkeit vermieden werden.

Vielen Dank für Ihre Aufmerksamkeit.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Herr Professor Waidner.

Ich darf nun zu Ihnen, Herr Dr. Gaycken, kommen. Auch bei Ihnen die einführenden Worte in den Themenkomplex. Sie haben das Wort. Bitte schön.

Sachverständiger Dr. Sandro Gaycken: Vielen Dank. - Ich bedanke mich auch für die Einladung vor den Ausschuss. Ich werde nur ein paar ergänzende Bemerkungen machen zu dem, was ich schon in meinem Gutachten geschrieben habe. Ich teile eigentlich auch fast alles, was Herr Waidner gesagt hat. Nur als ergänzende Dinge dazu:

Erst mal als Vorbemerkung zur Bewertung der Aktivitäten der NSA: Zwei Dinge sind da wichtig auseinanderzuhalten aus einer operativen Perspektive. Das eine sind die Fähigkeiten und die Praxis der massenhaften Überwachung. Das andere sind auch die Fähigkeiten der gezielteren Spionage. Das sind also zwei Fähigkeiten, die wir da sehr klar gesehen haben bei der NSA, auch beide sehr unterschiedlich. Es gibt diese unterschiedlichen Divisionen, die sich damit beschäftigen und da in beiden Reichen sehr effizient sind. Da sind die Konsequenzen für uns ganz andere in diesen beiden Bereichen. Die müssen wir also getrennt sehen.

Massenüberwachung: Da geht es natürlich mehr um die Perspektive des Datenschutzes unserer Bürger vor dieser Praxis. Bei der gezielten Spionage geht es natürlich wesentlich eher darum, das als Indikator der allgemeinen Möglichkeiten und Fähigkeiten in diesem Bereich zu verstehen und uns davor in den Bereichen, die Geheimschutz erfordern, und in der Wirtschaft zu schützen.

Denn - das ist jetzt die zweite wichtige Vorbemerkung - wir dürfen nicht vergessen, dass das, was wir jetzt gesehen haben bei der NSA, natürlich nur ein Indikator dafür ist, was viele machen wollen oder alle machen wollen. Wir sind uns ganz sicher, im militärischen Bereich zumindest, dass also auch Russland, China das schon können in dem Umfang, dass also auch Israel das in einem größeren Umfang kann. Frankreich behauptet zumindest, es zu können - hat noch keiner verifiziert. Und viele andere Staaten möchten das gerne können.

Und die NSA haben jetzt auch gute Werbung gemacht natürlich, dass das also alles sehr hocheffizient ist und sich anscheinend lohnt. Von daher müssen wir natürlich davon ausgehen, dass also sehr viele Länder ein sehr umfangreiches Interesse an diesen Fähigkeiten und Möglichkeiten entwickeln bzw. schon entwickelt haben. Wir dürfen also nicht nur auf die USA gucken, sondern müssen sozusagen einen Rundumblick machen und dann auch überlegen, wie andere Länder diese Fähigkeiten strategisch und taktisch bewerten und einsetzen wollen.

Zur ersten Variante, der Massenüberwachung, müssen wir sagen: Das ist schon sehr hoch effizient und sehr ausgebaut. Einerseits ist es natürlich technisch sehr weit ausgebaut. Da ist ja jetzt relativ viel bekannt geworden. Aber wir haben auch viele andere Komponenten, wo es ausgebaut wurde. Ganz wichtig ist natürlich auch zu nennen die rechtliche Kooperation mit Datendienstleistern in den USA. Da gibt es natürlich viel Hin und Her, und die behaupten, sie hätten damit nichts zu tun.

Aber wenn man sich die Sachlage ansieht und die sehr vielen rechtlichen Verfügungen, die ja existieren von der Regierung in die Wirtschaft hinein, die Interesse haben an diesen Daten, dann ist es auch taktisch sehr viel einfacher, über eine Kooperation mit Facebook zum Beispiel an diese Sachen ranzukommen, technisch viel einfacher. Die Schnittstellen sind da, die Kontakte sind da, die rechtlichen Apparate sind da. Also es ist sehr unglaubwürdig von diesen Unternehmen, zu sagen: Es gibt da überhaupt keine Kooperation oder wenn, dann nur so fallbezogen usw. - Das können wir ja auch gar nicht überprüfen. Von daher ist es für uns gut, da mit maximaler Skepsis ranzugehen und diese rechtlichen-wirtschaftlichen Verbindungen auch mit einzubeziehen in die Problemsicht.

Außerdem müssen wir natürlich auch dann verschiedene technische Verfahren und Paradigmen an sich ein bisschen reflektieren. Big Data ist ein Beispiel. Big Data ist einer der großen Kollaborateure bei dieser Massenüberwachung. Big Data wurde überhaupt in den Diensten wesentlich mitentwickelt mit der Absicht, eben

in großen Datenmengen Querverbindungen zu finden, die also eine Repersonalisierung anonymisierter Daten ermöglichen. Von daher ist das also auch was, was wir mit aufnehmen müssen. Denn auch wir sind ja hier dabei, Big Data zu implementieren und zu entwickeln. Das ist also auch was, was man da mit beachten muss.

Im Allgemeinen gehen wir davon aus, dass diese Massenüberwachung ein für Nachrichtendienste nach wie vor interessantes Feld ist. Es gibt zwar geteilte Meinungen inzwischen, und ich hatte auch aus NSA-Kreisen mal gehört, dass diese Metadatenmassenüberwachung gar nicht mehr so effizient ist, weil natürlich auch diese ganzen Bewegungsdatengeschichten - - Wir haben ja bei uns die Vorratsdatenspeicherungsdiskussion auch schon seit ein paar Jahren. Natürlich hören sich die Kriminellen und die Terroristen das auch an, und die wissen also jetzt auch schon seit vier, fünf Jahren, dass sie da sehr vorsichtig sein müssen mit diesen Metadaten/Bewegungsdaten.

Wenn sie mal mit Leuten sprechen, die so Interviews mit diesen Terrorfürsten machen: Die haben also acht, neun Handys, wo die permanent hektisch die Akkus austauschen und die Karten usw. Also, das ist schon noch eine grundlegende Effizienz da, um so den Bodensatz der Angreifer zu finden, die also nicht in der Lage sind, sich technisch gut auszustatten. Aber das Interesse an diesen Massendaten nimmt für diese Variante der Auswertung ein bisschen ab.

Wir sehen aber dafür ein sehr starkes Interesse in Staaten wie Russland und China, diese Technologien sehr viel weiter auszubauen und zu implementieren zu Zwecken der inneren Kontrolle, dass man also da seine Bevölkerung überwachen möchte, Oppositionelle identifizieren möchte. Auch im Nahen und Mittleren Osten sind diese Technologien inzwischen sehr, sehr hip. Und das ist also auch ein Problemfeld, mit dem man sich politisch beschäftigen muss.

Ansonsten ist das natürlich ein interessantes Feld für die Aufklärung, weil da mit verhältnismäßig geringen Kosten und Risiken sehr viele authentische Informationen gewonnen werden können. Das sagen auch viele Dienste gerade bei den gezielteren Aktivitäten: Wenn die sich mit einer menschlichen Quelle treffen, dann erzählt die einem da einen vom Pferd in der Kneipe und man weiß gar nicht, ob das stimmt. Wenn man sich irgendwo reinhackt und da sehr intensiven Einblick hat in die Daten und davon ausgeht, dass die nicht gefälscht sind, dann haben die also eine sehr hohe Authentizität. Und von daher hat man da also eine gute Nachrichtenqualität.

Wir müssen daher von drei Dingen ausgehen, was diese Fähigkeiten der Massenüberwachung und der massenhaften Auswertung angeht. Wir müssen davon ausgehen, dass diese Praxis international weiter ausgebaut wird und dass sie sich stark auf verschiedene Varianten heterogenisieren wird. Da müssen wir dann natürlich auch überlegen, wie wir für einzelne Akteure und bestimmte Opportunitäten, die da existieren, zu möglichen Zielen werden.

Wir müssen auch damit rechnen, dass durch das große internationale Interesse ein großer Markt entstehen wird für diese Varianten von Technologien. Viele davon werden jetzt schon - aus den USA übrigens hauptsächlich - betrieben, teilweise kommen aber auch aus Deutschland einige dieser Technologien. Das ist also auch etwas, was man mit im Blick haben muss. Man kann es also auch technisch nicht mehr eindämmen.

Wenn man jetzt sagt: „Wir wollen diese Technik nicht“, und wir sagen: „Wir schieben da in Deutschland einen Riegel vor“ - was ich selber prinzipiell gut fände -, dann wird das den Marsch der Technik allgemein sozusagen nicht aufhalten, weil sehr viele andere Länder das einfach bauen werden. Einige Staaten werden das auch als wichtiges strategisches Asset ansehen. Das ist also auch wichtig.

Wenn man jetzt versucht, Staaten mit Regulierungen oder mit internationalen Abkommen wieder einzufangen, dann müssen Sie wissen, dass es diesen Staaten jetzt nicht nur irgendwie um Datenschutz geht - ja oder nein -, sondern die sehen das auch als direktes strategisches, geopolitisches Asset - China gegen zum Beispiel die USA und solche Sachen -, dass sie da also diese Fähigkeiten haben und nicht hinterher sein dürfen.

Von daher müssen Sie das also auch in die Kosten-Nutzen-Kalkulation dieser Akteure mit einbeziehen, wenn Sie versuchen wollen, die einzufangen. Die haben also wenig Lust, überhaupt darauf zu verzichten, weil sie das

schon als sehr wesentliches Wirkmittel zum Teil ansehen.

Entsprechend sind die Reaktionen halt eben schwierig. Diplomatische Maßnahmen helfen nur sehr geringfügig. Man kann und sollte sich als Land auch mal gegen diese Praxis international aussprechen. Wir hatten sonst international immer die Amerikaner, die das getan haben, die sich also international auch hingestellt haben und gesagt haben: Es ist wichtig, dass wir das Internet frei halten, dass wir die Bürger nicht total überwachen. - Die sind natürlich jetzt völlig unglaubwürdig geworden.

Wir haben international jetzt auch die Situation, dass viele Staaten denken: Das ist ja total plausibel und rational, das zu tun. - Und da jetzt mit einer Stimme mal wieder nach oben zu kommen, die sagt: „Man braucht es nicht, und es ist auch rechtens und politisch anständig, das nicht zu tun“, wäre also auch empfehlenswert als diplomatische Haltung. Und das hilft dann auch vielen anderen Ländern, das als Alternative anzuerkennen.

Wenn es uns darum gehen muss, eine echte Effizienz hier gegen fremde Überwachung zu erreichen: Die kriegen wir natürlich auf diesem Weg nicht. Also, da müssen wir schon sehr viel stärker werden und stärker reagieren. Da werden Abkommen und Restriktionen sowieso nur unter „like-minded“ Nationen zustande kommen und die anderen gar nicht erst tangieren. Von daher ist da die Effizienz von Anfang an sehr begrenzt.

Deswegen ist auch bei Massenüberwachung das Plädoyer ganz entlang dem, was Michael gesagt hat: für einen echten, harten Schutz über harte technische und organisatorische Maßnahmen, die dieser Praxis also praktische Riegel vorschieben. Der Schutz vor Massenüberwachung lässt sich dabei meiner Meinung nach auf drei Wegen erreichen.

Das eine wurde schon gesagt: die Ende-zu-Ende-Verschlüsselung, wobei hier zwei Dinge sehr wichtig sind. Das eine ist die Zuverlässigkeit des Prozesses, auf dem diese Verschlüsselung generiert wird. Wir haben auch bei der NSA gesehen - und das war auch keine Überraschung; das Brechen von Krypto ist natürlich eines der Kerngeschäfte von Nachrichtendiensten -, wie die sich in diese Standardisierungsgremien reinbewegt haben, wie die auch versucht haben, kryptografische Verfahren so kompliziert zu machen, dass sie gar nicht mehr prüfbar waren. Das ist bei IPsec der Fall. Da gab es von Kryptoexperten, die das prüfen sollten, einige Beschwerden, dass die NSA den Code so kompliziert gemacht hätte, dass man gar nicht wissen kann, was da alles passiert. Das muss also alles gewährleistet sein. Da haben wir aber eigentlich gute Fähigkeiten in Deutschland.

Ganz wichtig ist dann aber halt eben die Laientauglichkeit. Der große Punkt, warum die meisten Leute - mich eingeschlossen zu weiten Teilen - Verschlüsselung überhaupt gar nicht benutzen, ist, dass das einfach furchtbar kompliziert und anstrengend ist und dann die Verbindung nicht klappt. Und dann funktioniert das nicht in der Geschwindigkeit oder irgendwelche solche Sachen. Das ist einfach so furchtbar nutzerfeindlich, dass es im Moment nicht richtig nutzbar ist.

Wenn wir überhaupt gar keine Akzeptanz beim Nutzer dafür einfordern können, dann wird das eben auch nicht implementiert werden. Man muss also, wenn man jetzt an der Kryptografie arbeitet, gar nicht mehr so sehr an der Sicherheit arbeiten, sondern ganz intensiv an der Laientauglichkeit.

Ich halte ebenfalls für sinnvoll eine Souveränität für IT und Daten, also das sogenannte Schengen-Routing. Das ist ja viel in der Kritik. Natürlich kann sich die NSA dann immer noch auf den DE-CIX-Knoten hacken und irgendwelche Sachen machen. Aber dann so massenhaft Daten permanent auszuleiten, wird dann doch erheblich schwieriger, das zu machen. Also rein aus der Sicht der Erhöhung der Sicherheit ist das schon eine ganz gute Maßnahme.

Das ist auch erst mal prima facie kostengünstig. Man muss nur natürlich sehen: Wenn wir jetzt also den Datenverkehr nicht mehr über die dicken Leitungen leiten können, sondern nur noch hausintern in Deutschland leiten, dann ist natürlich die Frage, ob diese Daten die Kapazitäten halten können und ob wir da also nicht unter Umständen recht erhebliche Netzinvestitionen vor uns haben. Ansonsten schafft es aber natürlich Territorialität und eine gewisse Sicherheit.

Ganz wichtig sind dann natürlich auch noch harte gesetzliche Vorgaben für diese internationalen Datendienstleister. Google, Facebook usw.,

die sperren sich jetzt schon mit Händen und Füßen dagegen, dass wir irgendwas von denen wollen, und haben ja auch schon massenhaft Lobbyisten in Berlin ins Feld geschickt. Aber da ist natürlich ein ganz, ganz großes Leck für unsere Privatheit und für unsere privaten Daten. Die einfach aufzufordern, diese Daten hier in Deutschland zu halten und auch nach deutschem Datenschutzrecht zu bedienen, zu benutzen und weiterzuverwerten, das ist auch eine ganz wichtige Maßnahme.

Ich komme dann noch zu der Variante der gezielten digitalen Spionage. Das ist meines Erachtens - das ist eine Privatmeinung - wichtiger eigentlich als die Überwachungsproblematik; denn da erwarten uns härtere realpolitische Schäden. Da geht es vor allem um die Industriespionage, die bei uns auch schon sehr ausgreifend stattfindet. Die Industriespionage hat inzwischen in vielen Fällen das Niveau der NSA erreicht.

Ich will jetzt nicht sagen, dass die USA bei uns spionieren. Sie sind sicherlich nicht der stärkste Akteur in dem Feld. Da gibt es andere, die sehr viel größere Interessen haben und das sehr viel voluminöser machen. Aber die arbeiten auch auf dieser Qualität. Die kommen überall rein. Die können Sicherheit und Detektion ohne jede Probleme umgehen. Und die arbeiten jetzt immer sehr intensiv an der Persistierung ihrer Angriffe. Das heißt, ein solcher Angriff geht in der Regel nicht mehr einmal rein, klaut irgendetwas, geht wieder raus, sondern der geht rein, bleibt dann drei Jahre drinnen und detektiert, lässt sich immer alles schicken, was da passiert - in der Entwicklungsabteilung zum Beispiel -, und wird dann irgendwann entdeckt. Viele Angriffe, die wir jetzt entdeckt haben, sind also wirklich mehrere Monate bis mehrere Jahre in diesen Systemen gewesen.

Das ist natürlich eine große Gefahr für unsere Industrie, und da sind wir leider auch sehr weit entfernt von umsetzbaren veritablen Ansätzen. Da müssen wir auch sagen, dass einfach nur Verschlüsselung hier nicht mehr hilft. Das ist also ein Interesse und ein Angreiferniveau, das wir hier haben - da wird auch auf Hardware-Ebene angegriffen zum Beispiel, da wird angegriffen über geschwächte Standards, über Innentäter ganz viel -, da muss man also sehr viele andere Vektoren noch mitbedenken.

Da muss man also tatsächlich dann sehr tief in die IT gehen, und diese systematischen strukturellen Defizite, die wir dadurch haben, dass wir 40 Jahre die Sicherheit - also eigentlich ja 70 Jahre - in der IT vernachlässigt haben und als Ferner-liefen-Thema behandelt haben, müssen jetzt wieder aufgesetzt werden. Da müssen wir also sehr tief reingreifen.

Da sind auch alle Ansätze, die wir im Moment haben und die im Moment stark propagiert werden, absolut nicht hilfreich - müssen wir ganz klar sagen. Die bieten so eine Basissicherheit in einigen Fällen. Aber - Michael hat das ja auch schon gesagt - diese Detektionsgeschichten zum Beispiel funktionieren alle sehr schlecht. Die reaktiven Ansätze haben sehr schlechte Effizienz.

Da wäre es also klüger - und auch in gewisser Weise eher so im Credo des deutschen Ingenieurs und des deutschen Unternehmertums -, da etwas sorgfältiger drüber nachzudenken, bevor man jetzt lospreschт und irgendwas entwickelt und irgendwas kauft und irgendwas wo ranschraubt. Damit erhöht man unter Umständen nur die Pfadabhängigkeiten auf schlechte Technologien, gibt Ressourcen aus, die man eigentlich besser erst mal für eine Problemsondierung ausgeben sollte.

Wir brauchen also ganz dringend systematische und strategische Ansätze. Ich habe in meinem Gutachten ein paar Ansätze vorgeschlagen, in welche Richtung das gehen könnte. Wir müssen also sehr grundlegend nachdenken. Ganz wichtig ist dabei, als Erstes überhaupt einen Markt für IT-Hochsicherheitsprodukte zu generieren. Das ist der Grund, warum wir diese Produkte nicht haben. Die Ideen gab es immer, die Konzepte gab es immer. Wir haben auch sehr viele gute Fähigkeiten dazu, sehr viele gute Ansätze dazu in Deutschland. Wir können das also machen. Aber es müssen skalierbare Produkte da sein.

Das kann man auf zwei Wegen erreichen: einmal national über harte Standards und harte Haftung, insbesondere jetzt im Bereich Industrie. Wenn die Industrie 4.0 kommt, dann ist für mich ganz klar, dass natürlich die Safety-Anforderungen für Maschinen auch für die IT gelten müssen, die dann da raufgeschraubt wird.

Wir müssen dann halt eben sehen, dass wir ausgehend davon, wenn wir hier sichere Maschinen entwickeln, sichere Computer entwickeln,

das auch als ein Exportprodukt hinbekommen; denn dann haben wir natürlich den Vorteil, dass wir auch die erheblichen Interessen der Großindustrie dahinter mit den entsprechenden Investitionen bekommen.

Im Moment haben wir erhebliche Schwierigkeiten, auch Investitionen im kleineren Millionenbereich überhaupt mal für Start-ups hinzukriegen. Wenn wir also hier die großen Unternehmen begeistern können und auch solide Strategien für Kapitalgeber vorlegen können, dann kriegen wir die erforderlichen Investitionen. Das sind also mehr so zwei- bis dreistellige Millionenbeträge, die da ausgegeben werden müssen. Das wäre eine wichtige Maßnahme.

Das ist also natürlich etwas, was geschehen muss, und das ist auch etwas, wo ganz dringend politischer Handlungsbedarf besteht. - Damit möchte ich es beenden.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für Ihre Ausführungen, Herr Dr. Gaycken. In jedem Skandal steckt auch eine Chance, könnte man vielleicht Ihre letzten Sätze zusammenfassen.

Ich weiß, dass sich auch der Chaos Computer Club mit dem Thema Spionage intensiv, glaube ich, beschäftigt hat. Von daher wäre der letzte Punkt von Dr. Gaycken, glaube ich, eine sehr gute Überleitung zu Ihnen, Herr Rieger. - Ich darf Ihnen das Wort für Ihre einführenden Ausführungen geben. Bitte schön.

Sachverständiger Frank Rieger: Vielen Dank für die Einladung. Wegen der Kurzfristigkeit leider von mir keine schriftliche Stellungnahme. Ich hoffe, Sie haben Verständnis.

Wenn wir uns angucken, worüber wir eigentlich reden, sollten wir uns kurz noch mal vergegenwärtigen, was eigentlich die Auswirkungen von Überwachung sein können. Und da hilft es, kurz einen Blick in die Nachrichten zu werfen. Wenn wir kurz nach Polen gucken, da haben wir gerade eine veritable Regierungskrise, die auf der Basis von publizierten Abhörresultaten passiert und wo wir nicht wissen, wer dahintersteckt. Ob es jetzt die Amerikaner sind, die einen wenig amerikafreundlichen Außenminister destabilisieren wollen, oder die Russen, die die Regierung destabilisieren wollen: Wir wissen es nicht.

Das zeigt sehr deutlich, welche politischen Auswirkungen und welche demokratiegefährdenden Auswirkungen die Existenz von unkontrollierten Abhörsystemen haben kann.

Was haben wir in den letzten Monaten aus den Snowden-Dokumenten gelernt? Wir haben im Wesentlichen gelernt, dass unsere Annahmen über die Natur der digitalen Technologien und des Netzes ein bisschen blauäugig waren. Wir haben jetzt die andere Seite des Januskopfes gesehen. Wir haben gesehen, dass diese Technologien genauso gut, wie sie für Revolutionen in Ägypten oder Ähnliches verwendet werden können, schon seit langem dazu verwendet werden, uns zu überwachen, abzuhören und zu kontrollieren.

Der grundlegende Konflikt, den wir da gesehen haben in den Ansätzen dessen, was die NSA treibt und auch was die anderen Five-Eyes-Dienste treiben, ist auch ein grundlegender Kulturkonflikt zwischen, sagen wir mal, kontinentaleuropäischen Vorstellungen von Privatsphäre, von Freiheit des Individuums, von der Rolle, die eine Regierung und ihre Dienste haben sollten, und denen, die in angelsächsischen Ländern vorherrschen, die doch eher anderer Ansicht sind.

Da müssen wir uns dann vergegenwärtigen, dass natürlich aber unsere Konzepte von Datenschutz, von Freiheit des Individuums nur so weit reichen, wie wir sie auch durchsetzen können. Das heißt, es geht hier um ganz grundlegende Fragen von Macht, von Souveränität, die unmittelbar verknüpft sind sowohl mit rechtlichen als auch mit technischen Problemen.

Derzeit ist die digitale Souveränität Deutschlands einfach eine Illusion. Wir müssen uns da nicht in die Tasche lügen. Wir können da eigentlich nur sagen: Wir stehen da vor einem großen Scherbenhaufen. Wir haben es auf der anderen Seite zu tun mit Geheimdiensten, die sich eigentlich benehmen - wenn man mal versucht, eine mentale Analogie zu finden; und das ist wichtig, weil man aus dem Verständnis dessen, wie der Gegner denkt, auch Folgerungen darüber ableiten kann, wie er seine technischen Fähigkeiten konzipiert und einsetzt - so ähnlich wie eine Mafia mit einer Rechtsabteilung. Das heißt, wir haben da mit Organisationen zu tun,

die - egal was die technischen oder rechtlichen Hürden sind - versuchen, Wege drum herum zu finden.

Und das Grundkonzept der NSA, was wesentlich ist zum Verständnis dessen, was wir auf der technischen Seite sehen, ist, dass sie alles abhören wollen. Das heißt, sie wollen alle Daten haben, alles sehen, alles erfassen können, um darauf ihre Auswertungen zu fahren. Das ist ein grundlegend anderes Verständnis als das, was wir früher von Geheimdiensten hatten, wo man sagte: Okay, wenn die von irgendwas gehört haben, dann haben die da Leute hingeschickt oder haben mal hier oder da jemanden abgehört. - Sondern wir haben es hier mit der sogenannten Ideologie des Heuhaufens zu tun.

Das sagen auch die NSA-Vertreter selber: Sie wollen einen möglichst großen Heuhaufen haben in der Hoffnung, dass sie darin mehr Nadeln finden, also die Nadeln, die sie dann für das Feindbild - was auch immer gerade das aktuelle ist - halten.

Wenn wir uns die Snowden-Berichterstattung angucken, werden Sie sicherlich auch ein bisschen verwirrt sein von den vielen Dutzenden Codewords, die da immer durch die Gegend jongliert werden, und den verschiedenen Programmen. Dazu sollte man wissen: Diese Codewords wurden genau dazu erfunden, um Leute zu verwirren, die zufällig davon erfahren. Wir sollten uns daher darauf konzentrieren, zu verstehen, was die tatsächlichen technischen Fähigkeiten unabhängig von diesen Codewords sind.

Und was wir gelernt haben, ist, dass es eine vollständige Möglichkeit zur Überwachung jeglicher digitaler Kommunikation, die nicht stark verschlüsselt ist, gibt und wir davon ausgehen müssen, dass dies auch durchgeführt wird. Also, was wir aus den Snowden-Dokumenten sehen: Die Datenmengen, die da erfasst werden - und die auch unter anderem, wie wir jetzt gelernt haben, mithilfe deutscher Dienste erfasst werden -, sind so gigantisch, dass man vor ein paar Jahren noch gesagt hätte: Okay, technisch wird das wohl ein bisschen schwierig. - Aber wir wissen jetzt: Es geht.

Das zeigt auch den wesentlichen Unterschied. Wir werden immer wieder gefragt: Wart ihr denn so als Experten verwirrt darüber, wart ihr erstaunt über die Fähigkeiten der NSA? Und eigentlich ist unisono die Antwort: Nicht über die Fähigkeiten im Detail. Jeder einzelne Angriff - also auch die Fähigkeiten, die schon erwähnt wurden, für gezielte Angriffe oder auch die Möglichkeiten der Massenüberwachung -, jedes einzelne dieser Angriffsmöglichkeitenteile hat keine große Überraschung hervorgerufen. Aber dass die im industriellen Maßstab zur Massenüberwachung des gesamten Planeten eingesetzt werden, das hat uns schon verblüfft. Zum Beispiel Angriffe gegen Verschlüsselung zum Brechen von SSL - der Verschlüsselung, die Sie zum Beispiel für Onlinebanking benutzen - waren bekannt. Wir wussten, dass es Möglichkeiten gibt. Die Implementierungen waren schwach, die PKI-Infrastrukturen sind angreifbar. Aber dass die industrialisiert durchgeführt werden, davon waren wir nicht ausgegangen.

Dass Router angegriffen werden können - die Schaltknoten des Internets -, davon waren wir schon ausgegangen. Aber dass, wie wir jetzt gelernt haben, die NSA 85 000 dieser Router vorsorglich angegriffen hat, um Verkehr ausleiten zu können, damit hatte niemand wirklich gerechnet.

Einer der Punkte, die mir besonders am Herzen liegen, was diese Fähigkeiten angeht - eine der Fragen drehte sich ja um Prism in Ihrer Fragenliste -: Prism ist ja den meisten Deutschen sozusagen das Synonym für diesen NSA-Skandal. Worum es sich dabei aber handelt, ist ein Ausnutzen der Zugänge, die für Strafverfolger, also für gezielte Ermittlungen in Strafverfolgungsfällen, gewährt wurden im Vertrauen darauf, dass sie nicht durch die Dienste missbraucht werden. Das heißt, Prism ist der Zugang, den das FBI bei Internetanbietern bekommen hat, der von der NSA einfach zweitbenutzt wird.

Vor diesem Hintergrund müssen wir uns übrigens auch fragen, was eigentlich mit den Kooperationen ist, die zum Beispiel das Bundeskriminalamt mit dem FBI hat, den Zugängen, die dort gewährt werden, den Datenaustauschen, die dort gewährt werden, im guten Glauben, dass sie für legitime Zwecke der Strafverfolgung verwendet werden, ob auf diese Daten nicht ebenfalls - genau wie die Daten, die der BND mit der NSA teilt - zugegriffen wird.

Die Art und Weise ist - deswegen sagte ich ja: Mafia mit einer Rechtsabteilung -: Man versucht immer, den Weg des geringsten Widerstands zu

finden. Wenn man auf rechtlichem Wege oder auf Kooperationswege nicht zum Ziele kommt - oder auf Bestechungswege -, dann schickt man halt die Techniker los, dann werden halt Kabel angezapft, dann werden Router gehackt, dann werden Wanzen in Computern installiert.

Zur Frage, was wir tun können, also wie wir aus diesem Dilemma herauskommen, dass wir technisch momentan keine Souveränität haben und politisch offensichtlich nur so mäßig vorankommen, was Abkommen und Ähnliches angeht: Da kann ich mich weitgehend meinen Vorrednern anschließen. Wir haben eine große Aufgabe vor uns, was die Technologie angeht. Aber sie ist nicht unlösbar. Mindestens was die Erzielung von technischer Sicherheit gegen die Massenüberwachung angeht, halte ich es für ein durchaus lösbares Problem.

Dazu wird es rechtliche Vorschriften brauchen. Also, Schengen-Routing war zum Beispiel eines dieser Themen - ist nur ein klitzekleiner Baustein, wo es wieder auf die Details ankommt -, Vorschreiben von Ende-zu-Ende-Verschlüsselung. Mit all diesen Dingen kann man sicherlich eine Menge bewegen.

Aber dazu gehört eben auch, tatsächlich deutsche Datensouveränität herzustellen. Momentan ist es immer noch so, dass ein Großteil der Metadaten aus deutschen Mobilfunknetzen nicht in Deutschland verarbeitet wird, sondern von israelischen und amerikanischen Firmen zum Teil im Ausland verarbeitet wird. Das heißt also, wir liefern diese Metadaten - und die sind kritisch, diese Metadaten, wie schon erklärt wurde - quasi frei Haus. Das heißt also, wir müssen auf der rechtlichen Ebene dringend Unternehmen incentivieren, deutsche Daten tatsächlich auch in Deutschland zu halten und auch hier zu verarbeiten.

Was die Empfehlungen angeht zum Thema „Wie kommen wir zu einer sicheren IT-Landschaft, wie können wir Internetanbieter dazu zwingen, europäische Daten in Europa zu lassen?“, schließe ich mich eigentlich im Wesentlichen Professor Waidner an - mit zwei kleinen Unterschieden.

Der eine Unterschied ist: Ich denke, wir werden nicht damit weiterkommen, dass wir wie bisher nur Großforschungseinrichtungen und Großkonzerne weiter mit Geld beglücken. Das ist wichtig für die Grundlagenforschung, das ist wichtig für, sagen wir mal, langfristige Forschung. Aber wenn wir Dinge haben wollen, die möglichst schnell am Markt sind, dann müssen wir uns tatsächlich gerade den kleinen Unternehmen zuwenden.

Und dann müssen wir insbesondere auch Wege finden, staatlicherseits die große Open-Source-Szene, die wir in Deutschland haben, zu fördern. Am meisten ist denen tatsächlich damit geholfen, dass man Audits bezahlt, das heißt also, dass Open-Source-Software wie zum Beispiel OpenSSL - wie wir jetzt gerade gesehen haben: viel kaputter, als jeder angenommen hat - intensiv betrachtet wird, angeguckt wird und Fehler darin gefunden werden. Damit ist denen am meisten geholfen.

Ich denke, wir werden perspektivisch nicht umhinkommen, so was wie eine europäische DARPA zu schaffen, die sich nur um IT-Sicherheit kümmert - wobei das D tatsächlich für Defense im positiven Sinne stehen sollte, nicht für Offensivkapazitäten -, die in der Lage ist, kleine Projekte, schnelle Projekte zu fördern und auch Grundlagenforschung zu sponsern, um dafür zu sorgen, dass wir am Ende im Rahmen eines 10- oder 15-Jahres-Programmes wirklich so was wie eine europäische Informationssouveränität erzielen können.

Was die rechtliche Lage angeht, denke ich, ist es unabdingbar, dass der Staat es wieder schafft, Vertrauen zu schaffen, wenn er sich als Träger des Vertrauens auf der technischen Seite wieder etablieren will. Das Vertrauen ist kaputt, insbesondere auch durch die unregulierte Datenaustauscherei der deutschen Dienste. Da fehlen mir leider so ein bisschen die Worte mittlerweile, was wir da nach und nach lernen, wie da die Prioritäten gesetzt wurden.

Ich denke, dass es zwingend notwendig ist, dass wir, sowohl was die deutschen Behördennetzwerke angeht als auch was den Austausch der Dienste untereinander angeht, das Primat der Politik wiederherstellen, also dass wir da halt tatsächlich die Rolle des Gesetzgebers wieder nach vorne schieben und nicht mehr die Dinge einfach so laufen lassen. - Damit bin ich erst mal am Ende. Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Herr Rieger. - Ich muss ganz ehrlich sagen: Ich bin tief beeindruckt von Ihren

drei Statements, jetzt nicht, weil ich als Jurist die vorherigen Sachverständigen, die juristisch waren - sowohl zum nationalen Recht als auch zum internationalen Recht -, besser verstanden habe als die Techniker, ganz im Gegenteil: weil Sie mit Ihren Statements - und ich habe Sie richtig verstanden, glaube ich - alle drei einen ganz deutlichen perspektivischen Zeig dahin gegeben haben, was gemacht werden kann, was konkret unternommen werden kann, damit wir einerseits mehr Sicherheit in der Kommunikation allgemein, aber auch speziell mit Blick zum Beispiel auf mittelständische Unternehmen, auf unsere Wirtschaft haben.

Ich glaube, das ist ein Punkt, der uns wirklich im Untersuchungsausschuss nachhaltig prägen wird und der sicherlich ein wesentliches Diskussionsthema in den nächsten Monaten sein wird. Wenn man sich das alles mal vor Augen führt, was Sie gerade geschildert haben, dann ist das ein gigantischer Komplex, in dem vielleicht nicht jeder Vorschlag dann irgendwann umgesetzt wird. Aber es ist, glaube ich, sehr deutlich geworden, wie breit die Möglichkeiten sind, zu handeln, aber auch, wie notwendig und wie offen derzeit unsere Kommunikation auf allen Ebenen ist.

Wenn man mit Bürgerinnen und Bürgern spricht, dann kommt sehr oft der Satz: Ich bin doch nicht interessant für irgendwen. Wenn ich per SMS meiner Familie etwas mitteile, geht das doch keinen was an. Aber wenn es einer hört, was soll's? - Und das Gleiche höre ich teilweise bei mittelständischen Betrieben. Also, diese Sensibilität klar zu fixieren, ist, glaube ich, ganz wesentlich, damit diese Schritte, die Sie geschildert haben, dann auch umgesetzt werden können.

Ganz herzlichen Dank für Ihre höchst interessanten Vorträge.

Ich würde jetzt gerne in die Fragerunde einsteigen. Wenn es so ist, dass der Ausschussvorsitzende nicht von seinem Fragerecht zu Anfang Gebrauch macht, was ich an dieser Stelle machen möchte, um direkt den Fraktionen die Möglichkeit geben zu können, zu fragen, dann sieht es so aus, dass wir nach der sogenannten Berliner Runde Zeitbudgets vereinbart haben, in denen die Fraktionen Fraktion nach Fraktion Fragen stellen können. Dann würden Sie die an Sie gestellten Fragen beantworten. Dann ist die nächste Fraktion dran und stellt wieder Fragen.

Hiernach beginnt die Fraktion der CDU/CSU mit 27 Minuten, gefolgt von der Fraktion Die Linke mit 8 Minuten, danach die Fraktion der SPD mit 17 Minuten und dann die Fraktion Bündnis 90/Die Grünen wieder mit 8 Minuten. Nach jeder Fraktion haben Sie die Gelegenheit, die an Sie gestellten Fragen zu beantworten. Danach kann es gegebenenfalls weitere Runden geben, wenn noch Fragen offen sind. Das versuchen wir dann so lange, bis endgültig alle Fragen von Ihnen geklärt worden sind und wir glücklich sind.

Ich darf daher in die erste Fragerunde einsteigen und der Fraktion CDU/CSU für ihre Fragen das Wort geben. - Herr Obmann Kiesewetter.

Roderich Kiesewetter (CDU/CSU): Herzlichen Dank, Herr Vorsitzender. - Und Ihnen drei, meine Herren, Kompliment auch von unserer Seite! Zunächst möchte ich aber unser Bedauern ausdrücken, dass Sie eine Stunde zu warten hatten, und zugleich auch im Namen meiner Fraktion danken, dass wir ein Einvernehmen herstellen konnten, unsere inoffizielle Sitzung zu unterbrechen.

Ich möchte zunächst an Sie, Herr Dr. Gaycken, zwei Fragen stellen, einfach um etwas mehr Verständnis bei Dingen, die ich selber noch nicht verstanden habe, zu finden. Sie haben kurz nach den ersten Enthüllungen betont, die von Snowden offengelegten Missstände seien ein offenes, im Kern langweiliges Geheimnis; das war ja im Sommer letzten Jahres bereits. Was hat Sie zu dieser Einschätzung bewogen, und sehen Sie nach den weiteren Veröffentlichungen das heute auch noch so?

Der zweite Punkt, den Sie gerade in Ihrem Vortrag angesprochen haben: Sie machten in einem Nebensatz die Bemerkung, es gebe Dienste, die größer und voluminöser seien als die NSA. Könnten Sie kurz ausführen, wen Sie meinen?

Dann eine Frage an Herrn Rieger zum Schengen-Routing. Wir haben am 5. Juni eine Anhörung gehabt und unter anderem den Sachverständigen Professor Brown gehört. Er hat in seiner Anhörung gesagt, dass ein Schengen-Routing die europäische Internetbranche mit höheren Kosten bedrohe und damit auch

insgesamt Europa als Innovationsstandort bedrohe. Und der Gewinn an Datensicherheit sei so gering, dass er diese Kosten nicht aufwiege. - Ich sehe das anders. Aber ich würde mich freuen, wenn Sie Argumente hätten, wie man diesem Ansatz begegnen könnte.

Ein weiterer Teil meiner Fragen richtet sich an Sie, Herr Professor Waidner. Zunächst einmal bin ich auch sehr dankbar, dass Sie das Thema Technologie und Marktentwicklung angesprochen haben; das haben ja auch Sie gemacht, Herr Dr. Gaycken. Eine zentrale Frage des Ausschusses heute ist auch, ob die Schilderungen der Überwachungsaktivitäten von Nachrichtendiensten technisch glaubwürdig sind, die auf die von Edward Snowden an die Öffentlichkeit gebrachten Dokumente gestützt werden. Habe ich Sie dabei richtig verstanden: Die entsprechenden Berichte, wie sie etwa von Glenn Greenwald zusammengefasst wurden, schildern Aktivitäten, die alle technisch möglich sind?

Der zweite Punkt geht auch auf einen Teil dessen ein, was Herr Dr. Gaycken gesagt hat. Herr Gaycken hatte Ende des vergangenen Jahres in der Tagespresse den Aufbau einer deutschen IT-Produktion gefordert. Viele neue Hochsicherheitstechnologien seien deutsche Entwicklungen. Sie sehen hier ebenfalls ein Potenzial; Sie haben das ja sehr deutlich gemacht. Was aber muss geschehen, um diese Chancen zu nutzen?

Ich frage das deshalb, weil ich es für äußerst sinnvoll halte, dass von diesem Untersuchungsausschuss Gestaltungsempfehlungen ausgehen, wie wir nicht nur einen eigenen Markt, eine eigene Branche stützen können, sondern wie wir durch ganz konkrete Empfehlungen auch die Sicherheit, auch vielleicht den Aufbau einer IT-Sicherheitsstruktur in Deutschland oder in Europa fördern können.

Meine dritte Frage an Sie, Herr Professor Waidner: Wir haben ja im letzten Jahr gehört, dass auch Private 500 Millionen Metadaten aus Onlinekommunikation bearbeiten könnten; denn diese Metadaten kann man ja nicht verschlüsseln. Sie fordern übereinstimmend mit Dr. Gaycken eine allgemein nutzbare Ende-zu-Ende-Verschlüsselung. Wenn die Aussagekraft von Metadaten aber so groß ist, wie das eben auch heute wieder dargelegt wurde, und diese nicht verschlüsselt werden können, warum kann dann Verschlüsselung überhaupt eine Lösung gegen Massenüberwachung sein? Oder wie muss man Verschlüsselung gestalten, dass sie auch im Bereich der Metadaten nicht eine indirekte Lösung ermöglicht?

Meine vorletzte Frage: Wir haben dieses Schengen-Routing ja vorhin auch schon mal angesprochen. Sie betonen in Ihrem Gutachten, dass bei dieser Maßnahme Erfolg und Ertrag außer Verhältnis stehen. Können Sie die Gründe nochmals erläutern, die Sie zu dieser Einschätzung bewegen? Sie haben das jetzt zwar nicht im Vortrag gesagt, aber in Ihrem Gutachten.

Und mein letzter Punkt, bevor ich an meine Kollegin weitergebe: Wie bewerten Sie Forderungen nach Inselsystemen, also die sogenannte Entnetzung? Tragen solche Systeme zu mehr Sicherheit bei, oder verkomplizieren sie das Ganze? Welche Vor- und Nachteile sehen Sie bei diesen Insellösungen, und wie müssten Andockstellen oder Übergangsstellen gestaltet sein? - Herzlichen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich darf für weitere Fragen Frau Kollegin Lindholz das Wort geben.

Andrea Lindholz (CDU/CSU): Auch von meiner Seite erst mal herzlichen Dank für die wirklich auch für uns oder auch für mich sehr interessanten Ausführungen.

Ich habe eine Frage zunächst an Herrn Waidner. Es geht mir da um die Datenschutzverordnung. Sie hatten sich da im letzten Jahr in der Presse mal differenziert und teilweise kritisch geäußert. Wenn ich jetzt Ihre Stellungnahme lese, verstehe ich das richtig, dass es doch auch jetzt die Empfehlung von Ihnen gibt, hier auf europäischer Ebene weiterzumachen, um damit auch einen wirksamen Impuls zu geben für eine wirksame europäische Datenschutzpolitik?

Ebenso auch meine Frage, die auf diese rechtlichen Grundlagen zielt, an Herrn Dr. Gaycken: Sie hatten in dem Ausschuss Digitale Agenda eher gesagt, dass so weiche Maßnahmen wie Normen und Abkommen nicht unbedingt so zielführend sind. Und jetzt in Ihrem Gutachten haben Sie für uns geschrieben, dass es viele Möglichkeiten gibt, um den unbefugten Datenzugriff einzuschränken. Sie haben

geschrieben „basieren auf wirtschaftlichen, politischen oder rechtlichen Grundlagen oder Maßnahmen“ und haben auch klare rechtliche Bedingungen der nachrichtendienstlichen Kooperation gefordert. Daher meine Frage: Können Sie mir da vielleicht noch mal an einigen Beispielen jetzt erläutern - nur kurz -, was Sie sich darunter konkret vorstellen, und können Sie insbesondere auch noch mal auf die rechtlichen Grundlagen eingehen, ob Sie doch jetzt eher auch solche Maßnahmen für wirksam erachten?

Dann auch von meiner Seite vielleicht noch mal an alle drei Sachverständige die Frage zum Schengen-Routing in aller Kürze: Was würde das eigentlich für so große Firmen wie Google und Facebook konkret bedeuten, wenn wir so was einführen? Bei Herrn Dr. Waidner habe ich es jetzt mittlerweile so verstanden, dass er das Schengen-Routing für gar nicht mehr so sinnvoll erachtet. Aber wenn man das jetzt mal unterstellt: Was würde das bedeuten? Und gibt es da aber auch Risiken? Ist es möglicherweise, wenn man so was einführt, für die Wirtschaft nachteilig? Wie kann sich das unter Umständen da auswirken? Vielleicht können Sie da noch mal konkreter für mich auch drauf eingehen.

Und wenn ich dann sehe, was die NSA zum Beispiel für einen riesigen finanziellen Etat hat, um ihrer Tätigkeit nachzugehen, ist meine Frage: Sie haben auch ausgeführt: Man muss es praktisch technisch so schwer wie möglich machen, überhaupt Daten abzufangen - aktiv -, weil man auf dem Weg auch die Kosten in die Höhe treibt. Eigentlich auch meine Frage an Sie drei: Glauben Sie wirklich, dass das gelingen kann, dass man damit sozusagen den Etat, der den USA zur Verfügung steht, in einer so unmöglichen Höhe nach oben sprengt, dass es uninteressant wird, und dass wir wirklich dauerhaft verhindern können, aktiv verhindern können, dass unsere Daten sozusagen abgefangen werden können? - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Kollege Ostermann, Sie bekommen als Nächster das Wort.

Dr. Tim Ostermann (CDU/CSU): Vielen Dank. - Zunächst einige Fragen an Herrn Professor Waidner. Herr Professor Waidner, Sie sprechen sich aus für allgemein nutzbare Ende-zu-Ende-Verschlüsselung. Habe ich Sie richtig verstanden, dass es dabei entscheidend auf vertrauenswürdige Schlüsselstellen ankommt und dass der Staat hier insbesondere gefordert ist? Darum meine Frage: Was muss der Staat gewährleisten, um das notwendige Vertrauen aufzubauen und zu erhalten, und wie kann die von Ihnen beschriebene Schwachstelle „Anonymisierungsdienste“ überwunden werden?

Dann die zweite Frage. Sie regen an, eine spezielle IT-Sicherheit-Verbraucherschutzorganisation zu installieren. Wäre es da nicht zielführender, anstelle dessen die bestehenden Organisationen, die ja vielfach einen sehr guten Ruf haben und auch eine große Reichweite haben, zu stärken und zu unterstützen von staatlicher Seite?

Dann noch eine dritte Frage an Herrn Professor Waidner. Sie regen an, in Sachen IT-Technologie das Airbus-Konzept zu übertragen. So verstehe ich Sie. Meinen Sie, dass das Bedürfnis nach Datensicherheit und Vertraulichkeit stark genug ist, um die Märkte für solche Branchengrößen bei uns im europäischen Raum zu schaffen?

Dann noch einige Fragen an Herrn Dr. Gaycken. Sie haben gegenüber dem Ausschuss Digitale Agenda, der Sie ja auch schon mal angehört hat, geäußert, dass es Produzenten gibt von IT-Standardprodukten, die gezielt Schwachstellen einbauen würden, und haben dabei das Beispiel Huawei genannt. Welche Schwachstellen weisen die Router auf? Was ist das konkret? Welches Missbrauchspotenzial ist damit verbunden? Wer ist hier konkret gefährdet? Und - Sie fordern ja ein Schengen-Routing - werden dann für ein Schengen-Routing nicht erst mal auch Schengen-Router benötigt, um das effektiv auch ausführen zu können?

Dann noch eine letzte Frage zum Thema Metadaten. Sie sehen ja den taktischen Wert von Metadaten als umstritten an und stellen dann fest, dass gerade auch gefährliche Akteure das Entstehen auswertbarer Metadaten umgehen; Sie haben ja auch ein Beispiel genannt. Verstehe ich Sie insofern richtig, dass Massendatenerfassung eigentlich eine Technologie von gestern ist und dass die Schlauen in Terror und organisierter Kriminalität heute schon in der Lage sind, das zu umgehen?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Als Nächsten habe ich Herrn Kollegen Wendt für seine Fragen.

Marian Wendt (CDU/CSU): Keine.

Vorsitzender Dr. Patrick Sensburg: Da war keine Frage. Okay.

Dann darf ich eine Frage im Rahmen der Union anschließen. Das würde, glaube ich, das Zeitkontingent dann am straffesten halten. Herr Dr. Gaycken, Sie haben angesprochen, dass wir im großen Umfang auch von anderen Staaten oder auch von privaten Dritten - das wird man nie so ganz genau feststellen können - das Abgreifen von Daten haben. Also macht es, glaube ich, doch eigentlich Sinn, eher in die Netzsicherheit, in die eigene Datensicherheit zu investieren, weil es macht jetzt keinen großen Sinn mehr, zu unterscheiden: „Wer greift auf meine Daten zu?“, weil man es im Zweifel gar nicht weiß.

Und da würde sich eine zweite Frage anschließen. Sie hatten gesagt, bei Facebook werden Daten gegebenenfalls abgegriffen. Ist es nicht auch vorstellbar, wenn selbst Google oder Facebook sagen: „Wir arbeiten nicht mit der NSA zusammen“, dass sie vielleicht mit privaten, völlig nett aussehenden Unternehmen zusammenarbeiten, die sich vielleicht für Verbraucherdaten interessieren - angeblich für Marktauswertung oder sonst irgendwas -, und diese Zweit-, Dritt-, Viertfirmen, die man sich in einer Kette vorstellen kann, dann wieder irgendwann mit der NSA zusammenarbeiten oder mit Sonstigen, die auf dem Markt sind und sich für Daten interessieren?

Dann kann man natürlich immer sagen: Wir arbeiten nicht mit der NSA oder sonst wem zusammen. - Aber wenn die private Firma, die sich in das Portefeuille geschrieben hat, Verbraucherdaten zu bewerten, dann aber diese Daten wieder an diejenigen weitergibt, die wir nicht wünschen, dann wäre das ganze System natürlich auch perpetuiert.

Also die Frage: Ist Ihnen da etwas bekannt, dass so eine Informationskette besteht? Weil das würde natürlich gerade die große Unternehmen, die immer gesagt haben: „Es ist keine direkte Kommunikation und keine direkte Zusammenarbeit da“, in ein ganz anderes Licht rücken. - Herzlichen Dank.

Ich sehe jetzt vonseiten der Union keine weiteren Fragen mehr. Da alle Sachverständigen auch direkt angesprochen worden sind, würde ich jetzt in der umgekehrten Reihenfolge zu den Wortbeiträgen von eben zuerst Herrn Rieger, dann Herrn Dr. Gaycken und dann Herrn Professor Waidner um ihre Statements, Antworten bitten. - Herr Rieger.

Sachverständiger Frank Rieger: Vielen Dank. - Zur Frage von Herrn Kiesewetter bezüglich der Kosten und Risiken des Schengen-Routings: Das Schengen-Routing kann in allem, was wir diskutieren, nur ein Baustein sein. Es ist halt ein kleines Element, wo wir versuchen, etwas rückgängig zu machen, was durch, sagen wir mal, eine strategische Deregulierungspolitik der Amerikaner entstanden ist.

Sie erinnern sich vielleicht alle noch an die Zeiten, als wir so Vorwahlen vor unseren Telefonnummern gewählt haben, damit wir billiger Ferngespräche führen können. Was es im Wesentlichen war mit dieser Vorwahl: Es wurde eine Vermittlungsstelle in New York angerufen, und diese Vermittlungsstelle in New York hat dann die beiden Anrufe zu Ihrem Ziel und zu Ihnen aufgebaut. Und der Grund dafür war, dass die Amerikaner halt einfach ihr Telekommunikationsnetz so stark dereguliert haben, dass beide Anrufe zusammen viel billiger waren als ein Anruf bei der Deutschen Bundespost.

Und dieses Prinzip besteht zum Teil immer noch. Also Sie haben heute gerade für großvolumige Glasfaserleitungsverbindungen von amerikanischen und britischen Anbietern Preise, wie sie halt am deutschen Markt sonst nicht üblich sind. Allerdings ist der Preisunterschied nicht gigantisch. Also wir reden hier halt von Prozenten, also nicht von Dopplungen oder ähnlichen Dingen.

Zudem haben wir noch das Problem, dass die Deutsche Telekom eine Politik innerhalb von Deutschland pflegt, dass sie gerade mit kleineren Anbietern kein kostenloses sogenanntes Peering ermöglicht. Also normalerweise funktioniert das Internet so, dass Anbieter ähnlicher Größenordnung halt untereinander Leitungen zusammenschalten und sagen: Wir berechnen uns nichts

dafür, jeder trägt seinen Teil der Kosten, und dafür können unsere Kunden kommunizieren.

Die Telekom sagt: „Wir peeren nur - also verbinden uns nur - mit sogenannten Tier-1-Kunden bzw. -Carriern, das heißt also anderen Anbietern in der gleichen Größenordnung“, und will von allen anderen Geld haben. Und das ist eigentlich der Grund dafür, warum dieses Problem überhaupt existiert. Also der Grund, warum so viele deutsche Daten über New York oder über London geleitet werden, die eigentlich in Deutschland bleiben könnten oder im Schengen-Raum bleiben könnten, liegt exakt in dieser Preispolitik.

Dieses Problem zu lösen, wäre eigentlich trivial. Also es ist halt nur ein einfacher regulatorischer Eingriff, der dafür sorgt, dass große Carrier verpflichtet werden, auch Interconnects auf Kostenteilungsbasis mit kleinen Carriern zu schaffen, und dann wäre der Fisch geputzt. Dann wäre halt tatsächlich auch kein - - Also ich sage mal, das Risiko würde sich tatsächlich höchstens - gut, für sie natürlich relevant - im Gewinn der Telekom niederschlagen. Aber damit hätte es sich dann eigentlich auch.

Also die Frage - müssen Sie abwägen - ist natürlich: Welchen Sicherheitsgewinn bringt es? Und, wie gesagt, es handelt sich dabei nur um einen Baustein. Also es handelt sich dabei nur um einen Baustein, der dafür sorgt, dass es nicht mehr ganz so einfach ist, massenweise Kommunikationsdaten mitzunehmen wie zum Beispiel im britischen Tempora-Programm, wo alle Kommunikationsdaten, die durch Großbritannien gehen, für drei bis fünf Tage mitgeschnitten werden.

Wenn man es schafft, die Preispolitik zu beeinflussen und dafür zu sorgen, dass also gerade kleinere Internetunternehmen in Deutschland eben nicht dazu gezwungen werden, die Mondpreise der Telekom für Interconnects zu bezahlen, sind die Innovations- und Preisrisiken tatsächlich völlig überschaubar und managebar. Es wäre also kein großes Risiko. - Ich glaube, damit habe ich Ihre Frage auch schon zum Teil beantwortet.

Zum zweiten Teil Ihrer Frage, Frau Lindholz, was die Kostensteigerung für Massendatenerfassung angeht: Tatsächlich hat Verschlüsselung - ich bin in der Branche seit zehn Jahren tätig - den großen Vorteil, dass sie den Verteidiger bevorzugt. Das ist eine der wenigen Sicherheitstechnologien, wo es so ist, dass wir davon ausgehen können, dass mit relativ geringen Aufwendungen die Aufwendungen des Angreifers überproportional gesteigert werden können.

Das heißt, mit einer Verpflichtung zur Ende-zu-Ende-Verschlüsselung, Eingriffen ins Routing und der Verpflichtung, zum Beispiel Metadaten nicht mehr so lange zu speichern und nicht mehr in so riesigem Umfang zu erfassen, könnten wir relativ problemlos die Kosten so weit hochtreiben, dass auch die NSA mit ihrem 50-Milliarden-Budget sich genau überlegen müsste, wo sie dieses Budget anlegt.

Mit einem Fünfjahreshorizont und mit klugen gesetzgeberischen Eingriffen und klugen technischen Lösungen bin ich da sehr optimistisch, dass man es tatsächlich schaffen kann, die NSA totzurüsten in dem Sinne, dass wir halt einen Vorteil schaffen gegen Metadatenerfassung, gegen Massenüberwachung, der auch mit einer Verdoppelung des Budgets nicht zu schlagen ist. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich hatte ja eben schon gesagt: Das sind unheimlich interessante Vorschläge. Wir werden vielleicht nicht jeden heute eins zu eins umsetzen. Aber die Aussage: „Der Untersuchungsausschuss will die NSA totrüsten“, ich hoffe nicht, dass wir die morgen als Schlagzeile wiederfinden. Aber ganz herzlichen Dank für Ihre interessanten Ausführungen.

Herr Dr. Gaycken, Sie dürfen als Nächster.

Sachverständiger Dr. Sandro Gaycken: Vielen Dank. - Erst mal zur Frage von Herrn Kiesewetter: Die Missstände waren damals ein offenes Geheimnis. In der Community, die wir da hatten, waren einmal diese technischen Schwachstellen alle lange bekannt, zumindest prinzipiell. Da herrschte allerdings auch immer die Perspektive, dass es ein bisschen umständlicher ist, die auszubeuten. Deswegen sehen wir das nicht so bei den Kriminellen. Aber natürlich haben die Nachrichtendienste sich gerne der etwas umständlicheren Dinge bedient, weil sie sich da auch sicher sein konnten, dass da halt eben gar

keiner hingeguckt hat und dass keine Schutzmaßnahmen da waren. Also die waren prinzipiell in der Struktur alle schon bekannt.

Auch die ganzen anderen Missstände in der Wirtschaft - wie man damit umgeht, wie lax man das Thema handhabt, wie man auch mit dem Produktschutz, mit Haftung umgeht -, diese ganzen sehr harten strukturellen Probleme da drunter, die waren alle sehr bekannt.

Wir haben natürlich auch gewusst in der Community, dass die Offensive ganz massiv anbaut und entwickelt. Also wir haben immer gesehen, wann gute Forscher verschwunden sind in irgendwie NSA, DARPA. Plötzlich waren die weg und haben nicht mehr geredet, nicht mehr auf E-Mails geantwortet. Da wussten wir immer: Aha, die arbeiten jetzt für den.

Dann wusste man natürlich auch mit den Fähigkeiten, die die da hingebracht haben, in welche Richtung das da geht. Man hat auch ein bisschen Investitionen gesehen mit Firmen. Die haben ja auch viel kooperiert mit den privaten IT-Unternehmern, speziellen Dienstleistern. Da hat man auch immer schon gesehen, was die sich so anbauen und wofür die sich so interessieren usw.

Dann wurde natürlich auch immer schon gemunkelt und gemauschelt, ob jetzt hier nicht Facebook und Google irgendwelche Schnittstellen - - was da noch alles drüber geht. Wir wussten ja von diesen Schnittstellen für das FBI über den CALEA Act. Aber da war natürlich klar, dass die NSA sich dafür interessiert und es auch macht. Ich meine, es ist die CIA, über die wir hier reden. Es ist schon eine gewaltige und mächtige Intelligence-Organisation, und die hat prinzipiell den Ansatz, dass sie sich nicht irgendwelche Informationen durch die Lappen gehen lässt, wenn die in Amerika rumliegen.

Von daher waren das alles keine Überraschungen. Also auch im Ausmaß waren es nicht so richtig Überraschungen. Natürlich nehmen die alles, was sie kriegen können, und haben die Fähigkeiten, das auch auszuwerten. Das waren Sachen, die alle bekannt waren oder zumindest sehr stark gemutmaßt wurden.

Auch die Missstände, die wir jetzt hier haben, sind in keiner Weise behoben. Da hat sich auch leider - müssen wir sagen - bis jetzt noch gar nichts getan, obwohl wir jetzt schon ein bisschen länger in der Diskussion sind, auch bei den Akteuren, die es eigentlich angeht.

Also die Industrie bemüht sich ein bisschen intensiver jetzt um den Schutz ihres Know-hows. Die haben halt verschiedene Probleme. Die sind durch die NSA natürlich ein bisschen aufgescheucht und bemerken aber auch immer mehr diese starke Industriespionage aus dem Osten in ihren eigenen Systemen und sind jetzt gerade dabei, sich neu aufzustellen, sind aber auch gerade so ein bisschen noch in der strategischen Orientierungsphase, wie sie das machen können, was sie das kostet und wo sie da ansetzen können.

Andere Akteure, die sich eigentlich auch Sorgen darum machen sollten - wie zum Beispiel die Bundeswehr -, stolpern da immer noch rum. Also die Bundeswehr - muss ich mal ganz ehrlich sagen -, die hat es geschafft, von einer schlechten Ausgangssituation in eine miserable Ausgangssituation zu degenerieren mit ihren Versuchen. Kollegen aus dem Ausland, die die Bundeswehr beobachten, sagen immer: Das ist, als würde man einen Autounfall in Zeitlupe sehen.

Da ist viel Bedarf, und da ist vor allen Dingen viel Bedarf jetzt, das Problem nicht nur technisch aufzuzäumen, sondern halt eben auch strategisch zu betrachten, taktisch zu betrachten, ökonomisch zu betrachten und an diese ganzen defizitären Strukturen ranzukommen, die ja in der Vergangenheit immer dafür gesorgt haben, dass immer das Billigste und das Schnellste gekauft wurde und eben nicht das Sichere. Da muss man rangehen, und da ist noch zu wenig passiert.

Bezüglich anderer Dienste und ihrer Interessen: Die unterschiedlichen Dienste haben unterschiedliche Interessen. Und wir müssen bei den USA sehen: Das sind schon noch so - „by and large“ - unsere Freunde und Alliierten und nicht unsere Feinde. Und wir haben aber natürlich andere Regierungen, die - die sind jetzt auch nicht unsere Feinde; aber die Amerikaner haben diesen Begriff „Frenemies“ - schon noch etwas intensiver auch an strategischen Informationen über uns interessiert sind. Die sind rücksichtsloser mit Industriespionage und strategischer Spionage.

Da sind die Interessen natürlich dann auch da, entsprechend stark zu agieren und Dinge zu

tun. Wir sehen die auch immer wieder mal. Das sind dann Sachen, die sehr partikular sind und in der Regel geheim. Aber wir sehen die immer wieder mal. Ansonsten müssen wir halt eben auch davon ausgehen, dass wir die vor allen Dingen deshalb nicht sehen, weil die sehr, sehr gut sind und weil bei denen halt irgendwelche Leute - Whistleblower - auch gar nicht erst an die Öffentlichkeit gelangen.

Zu den Fragen von Frau Lindholz: Die Normen und Abkommen sind international nicht so zielführend. Der Unterschied ist: Recht nach außen oder Recht nach innen. Also, wenn ich jetzt versuchen will, nach außen die USA zu reglementieren in den Auswüchsen ihrer Fernmeldeaufklärung, das ist sehr schwierig, und es wird mir auch nicht so sehr helfen, weil halt eben die Hauptakteure aus Ländern kommen, die sowieso so was nie unterschreiben würden. Auch die USA werden es vermutlich nicht unterschreiben, auch wenn sie auf die Metadaten vermutlich verzichten könnten nach dem, was sie gesagt haben.

Von daher ist das also vermutlich nicht wirksam. Es ist ja auch sowieso schwierig, weil das ja im Feld der internationalen Spionage läuft, das irgendwie zu reglementieren, weil da natürlich auch völkerrechtlich vereinbart ist, dass das also ein relativ rechtsfreier Raum ist. Das kann man politisch eskalieren und sich das wünschen. Aber in Erwartung solider Normen und Abkommen kann man da nicht stehen.

Dann ist es auch schwierig, das Recht zu implementieren über diese sogenannte internationale Internet Governance. Das ist also so ein Bereich, der jetzt gerade viel diskutiert wird und wo es viele Diskussionen gibt. Das sind also verschiedene Gruppen, die sich auf Konferenzen immer wieder treffen und dann über neue Standards im Internet diskutieren.

Da ist aber das Problem, dass da die Ansätze sogenannte Multi-Stakeholder-Ansätze sind. Das bedeutet, dass jeder, der das irgendwie mitgebaut hat und den das interessiert, da mitreden darf. Das führt in der Regel dazu, dass diese Internet-Governance-Geschichten sehr stark von den klassischen IT-Unternehmen okkupiert werden.

Da sind ein paar Diplomaten, die von der Sache nichts verstehen. Und dann sind die ganzen IT-Unternehmen da drin. Und dann sind eine ganze Reihe von Lobbygruppen der IT-Unternehmen da drin und dann noch so ein paar NGOs, die auch ihr Geld irgendwie von den IT-Unternehmen bekommen, und ein paar Wissenschaftler, die von den IT-Unternehmen bezahlt werden.

Und dann haben alle den Eindruck: Das ist ja eine super demokratische Veranstaltung. - Aber die Politiker, die da sind, die haben keine Ahnung. Und die Marschmusik diktiert da sozusagen dann die IT-Industrie, und die hat natürlich kein Interesse, dass wir über die systematischen, strukturellen Schwachstellen bei Cisco, bei Windows, bei Google und Facebook sprechen. Das heißt, die manövrieren das da immer aus.

Von daher sind also diese rechtlichen Maßnahmen in diesem internationalen Bereich sehr, sehr schwierig. Das heißt nicht, dass man das lassen sollte. Gerade im europäischen Raum kann man da sicherlich auch noch mal gucken.

Aber es wäre wichtiger, das Recht nach innen zu wenden und das Recht so zu benutzen, dass man also diese Haftung und Standards so hinbekommt, dass wir also eine bessere technische Grundlage bekommen.

Also Recht ist sehr wichtig, aber halt eben nicht in der Form internationaler Normen oder Abkommen, an die sich dann sowieso keiner hält und die keiner will, sondern als Recht nach innen für Haftung und Standards und für solide, sichere Produkte, die uns dann halt eben diese Basissicherheit einfach liefern.

Da brauchen wir das eben halt, wie gesagt, als initiales Incentive zur Marktentwicklung. Wir können da die Parallele ziehen - Parallelen hinken hier und da -: Autobau ist ja die Parallele mit dem Anschnallgurt. Das wollte auch die Industrie nicht, hat sich auch gesträubt, hat auch gesagt: Das ist irgendwie ein kompetitiver Nachteil. - Inzwischen ist ein sicheres Auto doch etwas, was viele Leute gerne kaufen. Ich habe einen Volvo; ist mir auch lieber als so ein Skoda. Da ist irgendwie dicker Schwedenstahl drum rum, der hat zig Airbags. Das war für mich auch schon ein Argument - ich will jetzt keine Werbung machen und nichts gegen Skoda -, das zu kaufen.

Ich denke, wenn das erst mal da ist, im Markt ist und wir solide Angebote haben - die Risiken werden ja auch immer größer, die gehen ja nicht weg; und es wird auch immer sichtbarer, was da

alles passiert in der IT-Sicherheit -, dann hat man da irgendwann auch einen großen Markt sich erschlossen und einen hohen kompetitiven Vorteil.

Bezüglich Schengen-Routing hatten Sie noch gefragt: Was bedeutet das für Google und Facebook? - Das ist schon sehr schlecht für die. Wir haben hier in Berlin ganz deutlich gemerkt, also wir haben deutlich die Lobbyisten des Silicon Valley gemerkt in den letzten Monaten, die sich ganz erheblich gegen diese Souveränität in Deutschland stemmen, einmal gegen die Vision, dass Deutsche Computer bauen. Da laufen die Lobbyisten immer rum und erzählen uns, wir können das nicht und wir dürfen das nicht und wir sollen uns das mal abschminken. Die haben also schon Angst davor, dass wir das machen, was eigentlich für uns ein guter Indikator ist, dass das wahrscheinlich wirtschaftlich vielversprechend ist.

Wir merken aber erstaunlicherweise auch die Datenunternehmen. Das war so was, was mich ein bisschen überrascht hatte, dass plötzlich also auch Facebook und Google und solche aufgetaucht sind und hier in diese Lobbykisten mit eingestiegen sind, irgendwelche Thinktanks mit instrumentalisiert haben und bezahlt haben und da dann halt eben darauf gedrängt haben, dass man hier dieses Schengen-Routing nicht implementiert. Das heißt also, die haben schon Angst davor, dass ihre Geschäftsmodelle der massiven Datenauswertung ganz erheblich beeinträchtigt werden, wenn diese Daten nicht mehr durch die USA laufen.

Kosten in die Höhe treiben: Darüber habe ich viel nachgedacht, und da gibt es auch viele Kollegen von mir. Ein Freund von mir am MIT beschäftigt sich ganz intensiv damit, wie man diese Kosten-Nutzen-Verhältnisse beeinflussen kann. Das ist natürlich die Idee bei der IT-Hochsicherheit, dass man das nicht absolut unmöglich macht - das wird nicht gehen -, aber dass man es so teuer macht, dass also nur noch die sehr großen Akteure in Einzelfällen das machen können, also im Grunde genommen ein Zurücktreiben der Sicherheitssituation in die 80er-Jahre, wo also nur noch ein Nachrichtendienst mit sehr hohen Mitteln, sehr hohem Willen und Risikobereitschaft in der Lage ist, einzelne Dinge mal zu tun.

Das, denke ich, kann man schon noch machen. Das ist ein bisschen schwierig abzuschätzen, weil auch in der Offensiventwicklung noch sehr viel Raum nach oben ist. Also, was wir gesehen haben bei der NSA, ist noch lange nicht das, was man alles machen könnte. Da muss man also auch ein bisschen strategisch Voraussicht betreiben, zu gucken, was die also noch alles machen können, wenn wir die jetzt auf eine andere Evolution zwingen.

Aber ich denke schon, dass man die Kosten so stark hochtreiben kann, dass zumindest eine große Bandbreite weniger talentierter und ressourcenstarker Akteure prinzipiell rausgeworfen werden und dass die großen Akteure doch auch ganz anders rechnen müssen, wenn sie so was tun.

Zu Herrn Ostermann. Produzenten, die gezielt Schwachstellen einbauen: Dafür haben wir keine Belege. Ich weiß auch nicht, ob man das so nachweisen kann. Die Produkte sind halt voller Schwachstellen. Wir wissen nicht, ob die absichtlich da drin sind oder unabsichtlich. Wir gehen davon aus, dass bei großen IT-Produzenten wie SAP mit 50 000 Entwicklern - wo also jeder, der irgendwie mal eine Tastatur in der Hand gehabt hat, irgendwas dazuschreiben darf - natürlich auch die Dienste Leute einschleusen, die mal dies und das und jenes machen.

Es reichen ja zum Teil sehr kleine Fehler, wenn Sie die also perfide konstruieren. SAP hat 300 Millionen Zeilen Code. Wenn Sie da ein einzelnes Zeichen mal durch ein anderes ersetzen, sodass die Zeile nicht falsch wird, aber eine andere Bedeutung bekommt, dann merkt SAP das nie. Das kriegen Sie über kein Testverfahren heraus. Aber der Dienst hat dann jahrelang weltweit Zugriff auf alle Systeme, die von dem Hersteller hergestellt werden. Von daher ist das schon eine sehr plausible und interessante Geschichte, so was zu tun.

Wir haben ja auch bei der NSA in den Dokumenten - in diesen Black Budget Leaks - gesehen, dass also da eine Abteilung existiert, die ein Budget - mit diesem Projekt GENIE - von 650 Millionen hat, um solche Implantate einzubauen, wobei wir davon ausgehen, dass viele davon halt eben auf der Produktionsebene eingebaut werden.

650 Millionen, um Schwachstellen einzubauen, ist unglaublich viel. Das klingt erst mal wie so eine Hausnummer beim US-Militärbudget; denkt man nicht weiter drüber nach. Aber wenn Sie davon ausgehen, dass es relativ günstig ist, einen Innentäter bei SAP zu finden und anzuwerben, dass Sie da irgendwie kein großes Budget reinstecken müssen, dann ist die Entwicklung von so einer kritischen Schwachstelle vielleicht - wenn Sie das Team sowieso schon im Keller haben - bei 200 000, 300 000. Das heißt, Sie können da also schon erheblich viel bauen, machen, anbauen, implementieren.

Da müssen wir halt davon ausgehen, dass doch ein erheblicher Teil unseres Ökosystems schon sehr nachhaltig verseucht ist. Das sind Sachen, die finden wir nie wieder - niemals. Das kann man sich abschminken, bei diesen komplexen Systemen diese perfiden Schwachstellen zu finden, die die eingebaut haben; das funktioniert nicht. Deswegen auch der Ruf, dass wir da neue Ansätze brauchen, neue IT. Wenn wir nicht von vorne anfangen - - Wir kriegen das nicht mit Flickschusterei von hinten aus hin.

Zur Metadatenerfassung - deswegen auch die Frage -: Wir brauchen also auch Schengen-Router, ganz klar. Also nationale Souveränität in den IT-Produkten ist ganz wichtig und ganz wichtig natürlich auch eine hochsichere Produktion. Wir müssen die behandeln wie strategische Assets und wie Rüstungsgüter. Wir brauchen sicherheitsüberprüftes Personal, harte Sicherheitskonzepte. Ansonsten können wir nie sicher sein, was da drin ist, und können es auch nicht exportieren, weil dann natürlich auch die anderen Nationen nicht wissen, ob dann bei uns nicht doch einer drin war, wenn wir es nicht sicher produziert haben.

Metadatenerfassung, da sagen viele: Wir haben Schwierigkeiten natürlich, da die Effizienz abzuschätzen und die relativen Effizienzen abzuschätzen in der Strafverfolgung. Aber es gibt doch einen relativ hohen Konsens, dass diese Massendatenerfassung - - Also es gibt diese Heuhaufenmentalität - ganz richtig -, dass man sagt: Na ja, da hat man wenigstens ein bisschen was und so ein bisschen ein Anfangsmaterial, mit dem man überhaupt irgendwie arbeiten kann.

Aber gerade die Nachrichtendienste - wir sehen es auch an Veröffentlichungen aus den USA in letzter Zeit -, die arbeiten noch sehr viel intensiver mit gezielten Fähigkeiten. In den USA haben Sie Firmen aus politischen Gründen, die das machen, die also sich bei den bösen Jungs sozusagen reinhacken, zurückhacken. Da muss man natürlich entsprechende rechtliche Abkommen haben oder einen dicken Pelz, dass einem das egal ist. Aber das sind Sachen, die sehr viel effizienter sind. Da kriegt man also sehr viele Informationen.

Das wird dann noch ergänzt durch Human Intelligence, also ganz klassische Aufklärungsarbeit. Da sind die Informationen so gut, dass die also wirklich sehr effizient sind, sehr ausführbar und „actionable“ Sachen produzieren.

Von daher würde ich auch empfehlen, für unsere Strafverfolgungsbehörden und Nachrichtendienste gezielte Fähigkeiten da aufzubauen. Das ist also was, was datenschutzmäßig völlig in Ordnung ist - da muss ich eben keine Massenüberwachung machen - und was gleichzeitig für die Strafverfolgung und Aufklärung sehr viel effizienter ist. Möchte ich also sehr empfehlen. Kostet aber natürlich ein bisschen was und ist auch ein bisschen komplizierter.

Herr Sensburg, zu Ihren Fragen: Ich teile absolut Ihre Einschätzung, dass man große Schwierigkeiten hat, die Akteure zu identifizieren. Das Problem ist auch nach wie vor nicht gelöst. Wir sehen so ein paar neue Ansätze aus den USA, wo sie also nachweisen wollen, dass sie schon in der Lage sind, die „bad guys“ auch zu identifizieren. Aber das sind „lucky shots“, und man denkt auch, dass das „one hit wonder“ sind.

Man hat jetzt diese chinesischen Einheiten zum Beispiel, die Industriespionage machen, auch nur deshalb identifizieren können, weil die sehr schlampig waren in ihrer „operational security“ und sich also nicht viel Mühe gegeben haben, sich zu tarnen. Da gibt es sehr viel höhere, bessere Standards. Sie können übrigens bemerken, dass wir noch nie die Russen irgendwo erwischt haben, obwohl wir davon ausgehen, dass die sehr aktiv sind. Die sind einfach so gut, dass wir die nicht sehen. Das ist also so was, was da natürlich eine Rolle spielt.

Das heißt, wir wissen also nie genau, wer uns da angreift. Von daher müssen wir also eine IT-

Sicherheitsstrategie fahren, die unabhängig davon ist, ob wir diese Attribution und diese Identifikation jemals hinbekommen. Unabhängig von dieser Frage eine Strategie zu bauen, bedeutet natürlich, passive technische Sicherheit zu bauen in einem entsprechenden Maß.

Mit den Firmen, privaten Unternehmen, die die Metadaten kaufen: Das kann natürlich sein. Ich selber habe das nicht gehört. Wenn das existieren würde, wäre das auch topsecret und nur in sehr kleinen Kreisen bekannt, weil natürlich alles, was so sehr sensibel für die Unternehmen ist, da auch nur auf sehr kleiner Basis, mit sehr wenigen Leuten gemacht wird normalerweise. Das ist also schwer, da reinzukommen.

Aber wir sehen natürlich ganz klar, dass es viele Interaktionen mit privaten Akteuren gibt - auch in vielen anderen Ländern. Zwei große Probleme will ich Ihnen mal nennen - da gibt es auch übrigens harten politischen Handlungsbedarf für Sie -:

Das eine sind PR-Firmen, die also angeheuert werden von Nachrichtendiensten oder mit denen man kooperiert, um sogenannte Information Operations zu fahren. Die gehen also in fremde Länder in diese sozialen Medien - Twitter, Facebook usw. -, die haben da Identitäten angelegt über Jahre. Die agieren digital also sehr glaubwürdig in bestimmten Communitys als Aktivisten oder als irgendwas, und die können dann auf Auftrag Kampagnen fahren, irgendwelche Meinungen beeinflussen.

Bekannte von mir in der SecDev Group in Kanada - das ist so eine Sicherheitsfirma - beobachten zum Beispiel diese Information Operations, und die haben sehr viele Indikatoren zum Beispiel für Aktivitäten in Südamerika, wo also vor bestimmten Abstimmungen oder im Rahmen politischer Prozesse plötzlich sehr stark synchronisiert gezielte Nachrichten gestreut wurden in sozialen Medien in Ländern, wo das Grundvertrauen in die staatlichen Medien sehr gering ist, wo man also denkt, dass das Internet die Wahrheit eher verbreitet als die anderen Medien, und wo man dann also sehr genau beobachten konnte, wie die Meinungsströme gesteuert wurden. Immer wenn was in eine Richtung ging, die denen nicht passte, haben die da neue Sachen gestreut und Informationen und „Guck dir mal die Studie von diesem Institut an“. Das war dann einfach nur irgendeine Webseite, wo so eine gefakte Studie dran war. Das ist also ein großes Problem, wo private Akteure eine große Rolle spielen.

Ein anderes größeres Problem sind auch viele Hackerfirmen, international, vor allem im Moment im asiatischen Raum, die sich als Söldner andienen und Hacks in militärischer Qualität an Akteure verkaufen, die das von sich aus nicht produzieren können. Wir wissen, dass da Leute mit Koffern voller Bargeld antanzen und denen sagen: „Ich möchte gerne einen Hack auf die und die Strukturen und so weit, dass ich dann nur noch draufdrücken muss“, und dann geht das. Die verkaufen das und sind unbeobachtet. Das wäre also so was, was man doch dringend mal unter Beobachtung stellen müsste.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für Ihre Ausführungen. - Herr Professor Waidner, ich darf Ihnen das Wort geben.

Sachverständiger Prof. Dr. Michael Waidner: Vielen Dank. - Also zunächst zu den Fragen von Herrn Kiesewetter:

Sie hatten ja am Anfang gefragt, wie meine Aussage dazu zu verstehen ist, dass die Aussagen in den Snowden-Dokumenten glaubwürdig sind. Das ist natürlich eine sehr gute Frage. Was ich damit meinte, ist: Diese Snowden-Dokumente, wenn Sie sich die angucken, haben alle ein bisschen den Charakter von sozusagen einem Katalog; sagen wir es mal so. Es werden viele tolle Dinge beschrieben - teilweise direkt. Also es gibt diesen einen Katalog von „targeted“ Techniken, es gibt viele andere Dokumente, die einfach nur Schulungsdokumente beschreiben oder Klassifikationen beschreiben.

Also in diesem Sinne kann ich sagen, was wir gemacht haben: Wir haben uns diese Liste mal angeguckt, die man generieren kann, und haben überlegt: Könnte es etwas geben, angriffstechnisch, was dem entspricht? Und die Antwort ist durchweg: Ja. Also in diesem Sinne ist das, was da steht, glaubwürdig implementierbar, und teilweise ist es ja auch ziemlich naheliegend, wie man es implementieren würde.

Viele der Angriffe, die beschrieben sind, haben wir ja auch tatsächlich im realen Leben

schon gesehen. Einen habe ich zitiert: Das war diese berühmte Umleitung über Island. Nichts gegen Island; ich glaube, Island hatte damit nichts zu tun. Aber da gibt es viele Beispiele dieser Art.

Wir haben auch mal geguckt beispielsweise: Kann man tatsächlich SSL-Implementierungen korrumpieren? Da gibt es eine Group in Großbritannien; die hat sehr ausführlich darüber geforscht. Da kann man sehr viel nachlesen bei denen. Wir haben auch mal geguckt: Kann man DNS - also nicht DNSSEC, sondern DNS pur - missbrauchen? Gibt es tatsächlich im wilden, echten Internet den Fall, dass hin und wieder mal DNS-Anfragen falsch beantwortet werden? Auch das haben wir experimentell nachgewiesen.

Also das passiert alles tatsächlich, kann man alles realisieren. In diesem Sinne halte ich das alles für sehr, sehr glaubwürdig.

Ihre nächste Frage ist richtig schwierig, muss ich sagen. Sie haben gefragt - sinngemäß -: Was muss geschehen, damit in Deutschland und Europa ein Markt entsteht? Ich halte das eigentlich wirklich für die wichtigste Frage sogar, weil ich denke, da ist eine Gelegenheit. So ein Markt entsteht typischerweise ja nicht, sondern da ist ein Markt. Und die Frage ist: Wie kann man diesen Markt bedienen, wie kann man ihn gestalten, sodass er für uns eine Möglichkeit ist?

Ich möchte ganz kurz einschieben: Frank Rieger hat, glaube ich, mich in die Ecke geschoben, ich würde[2] nur Großforschung und die Großindustrie fördern. Dem ist natürlich nicht so. Natürlich braucht man sehr viele innovative KMUs, um neue Technologien zu erzeugen. Von daher: Alles, was ich sage, gilt auch für die KMUs.

Ich denke, uns fehlt allerdings tatsächlich auch ein großer Hersteller; darauf komme ich aber gleich zurück. Danach hat auch jemand von Ihnen gefragt.

Wie würde man so einen Markt generieren? Wie gesagt: Zum einen: Das Grundbedürfnis nach IT-Sicherheit existiert. Die Frage ist: Wie kann man es so gestalten, dass man es erstens bedienen kann - und dass wir es bedienen können, also „wir“: Europa, Deutschland? Was dafür, glaube ich, ganz essenziell ist, ist, dass man an der Stelle vernünftige Standards schafft, die zu mehr Sicherheit führen. Deswegen habe ich so viel Wert darauf gelegt, dass man europäische Standards schafft, die über alle Zweifel erhaben sind.

Wichtig ist: Wer Standards schafft, hat typischerweise einen Technologievorteil - typischerweise. Wenn Sie sich angucken, wie Standards gemacht werden: Heutzutage werden Standards selten in den großen ISOs gemacht, von den nationalstaatlichen Organisationen, sondern Standards werden von Firmen getrieben, die sich davon Vorteile versprechen, und die haben die auch.

Damit man diese Vorteile umsetzen kann, ist es wiederum wichtig, denke ich, dass man erstens die Technologien schafft - deswegen ist Forschung so wichtig, deswegen ist Entwicklung so wichtig -, aber auch, dass man in der Vergabe von Aufträgen der öffentlichen Hand beispielsweise oder durch Haftungsfragen sicherstellt, dass wirklich auch diese Dinge eingesetzt werden müssen.

Ich hatte ja erwähnt, dass tatsächlich erstaunlich wenig passiert, wenn man alleine dem Markt die IT-Sicherheit überlässt. Ich habe jetzt die Zahlen nicht hier, aber sinngemäß: Selbst bei solchen elementaren Dingen wie Firewalls, wo man jetzt wirklich sagen würde: „Sie helfen vielleicht nicht furchtbar viel, aber sie helfen ein bisschen was“, selbst da gibt es[3] so was wie 15 Prozent aller Unternehmen ohne Firewalls, also ohne Netzwerk-Firewall. Das zeigt sozusagen: Da werden Innovationen nicht so schnell angenommen wie üblicherweise.

Die Innovationsgeschwindigkeit kann man, wie gesagt, erhöhen durch Vergaberichtlinien, also dass einfach Standards, die gesetzt werden, von der öffentlichen Hand auch umgesetzt werden müssen, und durch Dinge wie Gefährdungshaftung, was jetzt nicht mein Thema ist; ich bin ja Techniker, kein Jurist. Aber ich denke auch, da könnte man einiges tun, um die Sachen voranzubringen.

Der zweite Teil, den ich erwähnen wollte, ist: Wir müssen auch schauen - und da ist ein Riesenmarkt für Europa -, dass wir die Produkte, die nicht in Europa hergestellt werden, trotzdem verwenden können. Ich bin ein großer Verfechter

2) vgl. Anmerkung des Sachverständigen, siehe Anlage1 .

3) Protokoll korrigiert, siehe Anlage 1.

davon, dass es einen Riesenmarkt geben kann für uns. Aber wir werden nie unabhängig werden von Technologie aus anderen Ländern. Das Problem ist einfach zu groß, und ich denke, wir müssen daran denken: Wir sind eine exportorientierte Nation. Wenn wir uns von dem Rest der Welt abkoppeln, ist das, glaube ich, nicht sehr vorteilhaft für unsere Wirtschaft. Also wir wollen international Dinge integrieren können.

An der Stelle muss man investieren in die Fähigkeit, zu überprüfen, und auch das ist wiederum ein großer Markt. Also wenn Sie beispielsweise mit potenziellen Anwendern im Nahen Osten reden oder sonst wo - also in manchen Gegenden dieser Welt -, die die gleichen Probleme haben wie wir: Ich glaube, die würden voller Freude Produkte aus Deutschland, aus Europa nehmen und Testmethoden, wenn wir sagen: Nach diesen Methoden können wir darauf vertrauen, dass, wenn wir Produkte integrieren, die sozusagen hinreichend okay sind. - Gut, also soweit vielleicht mal zu diesem Punkt.

Die nächste Frage war von Herrn Kiesewetter, wie Ende-zu-Ende-Verschlüsselung einzuschätzen ist - gegeben, dass es ja auch noch Metadaten gibt und andere Dinge. Da muss man ganz klar sagen: Ende-zu-Ende-Verschlüsselung ist das Mittel der Wahl gegen Massenüberwachung durch Abhören auf Leitungen in Netzknoten - also alles, was zwischen den Enden passiert.

Es gibt darüber hinaus natürlich Metadaten, die fallen trotzdem an. Also einfach: Wer redet mit wem? Da sieht man trotzdem die klassischen Verbindungsdaten. Auch dagegen kann man sich schützen. Das habe ich in meinem Gutachten ein bisschen erläutert. Da gibt es Mechanismen wie das berühmte Tor-Netz, oder in Deutschland gab es mal eine Entwicklung JonDo - die gibt es immer noch -, die leider nicht so stark geworden ist wie Tor. Da kann man viel tun. Da muss man einfach mehr investieren, um diese Technologien, die es gibt, hoch zu skalieren, sodass man sie wirklich breit verwenden kann.

Ich liebe diese Technologien, also ich würde das stark unterstützen. Aber fairerweise muss man natürlich sagen: Sehr viele Metadaten fallen einfach an den Endpunkten an. Also wenn ich voller Freude ein soziales Netz verwende und dort alle meine Daten hinterlege, dann hilft mir die ganze Ende-zu-Ende-Verschlüsselung nichts, weil das Ende ist ja genau das, was die Daten dann verarbeitet und eventuell weiterreicht. Kurz und gut: Ende-zu-Ende-Verschlüsselung ist ein sehr wichtiges Element, aber nicht das einzige Element, um das es geht.

Dann hatten ja verschiedene von Ihnen Fragen zum Schengen-Routing, und ich bin, glaube ich, an dieser Stelle wahrscheinlich der skeptischste von uns - vielleicht; weiß ich nicht. Was ich sagen wollte, ist: Schengen-Routing ist für sich betrachtet ein Element, was etwas nützt. Also sozusagen: Wenn natürlich Daten nicht freiwillig zu demjenigen fließen, der sie aber abhören möchte, dann ist das erst mal eine gute Sache. Schengen-Routing ist keine Kleinigkeit. Man muss etliche Dinge ändern. Ich habe ja in meinem Beispiel gezeigt: Man kann leicht ohne Änderungen Daten einfach umlenken - ob jetzt Schengen-Routing da ist oder nicht. Also man muss es technisch durchsetzen.

Es wird sicherlich erfordern, dass man Kapazitäten ändert. Also die dicken Leitungen sind heute halt eben nicht nur innerhalb von Europa, sondern teilweise auch außerhalb. Was ich eben gerne anregen würde, ist, dass man einfach mal guckt: Was sind die effizienten Methoden?

Schengen-Routing hilft gegen die gleiche Art von Angriffen, gegen die Ende-zu-Ende-Verschlüsselung hilft. Längerfristig ist Ende-zu-Ende-Verschlüsselung die deutlich wirksamere. Man müsste einfach mal vergleichen sozusagen. Wenn ich jetzt anfange, Hunderte von Millionen Euro zu investieren: Wo investiere ich die? Darum geht es mir eigentlich.

Sie hatten auch gefragt: Was bringen Inselösungen, also diese berühmten VIP-Netze oder losgelösten Regierungsnetze oder was auch immer? Das hängt sehr davon ab, was man darunter versteht. Es gibt extreme Vorstellungen, dass man sagt, man macht komplett getrennte Netze und getrennte Leitungen, die nur über sichere - also über auch baulich sichere - Verbindungen geführt werden. Das hat sich in der Praxis nie durchgesetzt. Es gab auch schon ähnliche Gedanken beispielsweise in den USA, mal ein eigenes Regierungsnetz zu machen. Es ist horrend teuer, und es verkennt, glaube ich, den Witz an einem Netz, nämlich, dass man kommunizieren kann.

Es ist auch so: Insellösungen kann man auch implementieren durch so was wie bestimmte Sicherheits-Policies - die kennen Sie wahrscheinlich alle aus eigener Erfahrung -, dass man Dinge klassifiziert in „Topsecret“, „Secret“ usw. Das hat man auch in der Wirtschaft am Anfang probiert. Alle diese Dinge sind kläglich gescheitert.

Also im Endeffekt: Die Ausnahmen sind immer stärker als die Regel. Unterklassifikationen kommen häufig vor. Die Übergänge zwischen diesen Netzen werden sehr, sehr häufig vorkommen. Von daher kann ich nur abraten, über Insellösungen in diesem Sinne nachzudenken - also nachdenken sollte man immer - und sie dann auch wirklich zu tun.

Insellösungen im Sinne von Virtual Private Networks oder ähnlichen Dingen gibt es natürlich, werden auch verwendet, sind nützlich. Man muss sie nur richtig implementieren und entsprechend absichern.

So, ich hoffe, ich habe Ihre Fragen alle korrekt mitgeschrieben gehabt.

Frau Lindholz hatte eine Frage zur Datenschutz-Grundverordnung der EU. An der Stelle muss ich klar sagen: Ich finde das eines der besten Dinge, die dem Datenschutz in Europa passiert sind - aus verschiedenen Gesichtspunkten. Man kann auch Dinge kritisieren - darauf komme ich gleich zurück -, aber das Prinzip erst mal, dass es so eine Datenschutz-Grundverordnung gibt, ist eine sehr, sehr gute Sache. Für die Wirtschaft bedeutet das eine Vereinheitlichung; das ist sehr, sehr positiv. Für die Verbraucher bedeutet es ebenfalls eine deutliche Vereinheitlichung im internationalen Verkehr; auch das ist eine sehr, sehr gute Sache.

Ich denke, die Sorgen, dass die Grundverordnung, wie sie sich langsam abzeichnet, das deutsche Datenschutzniveau absenken würde, halte ich persönlich für übertrieben, und auf jeden Fall sehe ich, dass die positiven Dinge deutlich überwiegen. Also darüber kann man gerne ausführlich reden, aber das ist eine sehr, sehr gute Sache.

Was man halt auch sehen muss, ist: Die Datenschutz-Grundverordnung wird nicht das Einzige sein, was das Problem löst. Also wir hatten ja, glaube ich, alle drei gesagt, dass im Endeffekt Technik das Einzige ist, was wirklich nicht kor-rumpierbar ist. Alle Gesetze sind prinzipiell nur so gut wie das System darum herum, was es sicherstellt. Das gilt auch für die Datenschutz-Grundverordnung. Jetzt glaube ich nicht, dass die EU gerade untergeht oder so was in der Art, aber sozusagen Gesetze sind nicht die einzige Lösung.

Im Detail gibt es auch Kleinigkeiten. Es gibt Fragen, wie beispielsweise: Wie realisiere ich einen „consent“, der sehr, sehr breit sehr, sehr oft vorkommen muss? Das ist ein bekanntes Problem, was man nicht gut im Griff hat. Dadurch, dass man es in ein Gesetz reinschreibt, wird es immer noch nicht besser gelöst. Also da gibt es noch sehr viele Forschungsfragen, die man angehen muss.

Dann hatten Sie uns alle gefragt zu Schengen-Routing: Was bedeutet das für Google? Was sind die Risiken für die Wirtschaft? Das hat ja teilweise Sandro Gaycken schon beantwortet.

Google und andere mögen nervös darauf reagieren. Fairerweise bedeutet das für Google natürlich einfach überhaupt nichts, weil, wie gesagt, wenn das Schengen-Routing ganz sicher meine Daten bis zur Grenze der Europäischen Union oder des Schengen-Raumes leitet, aber dann zu den Servern von Google, dann habe ich an dieser Stelle nichts gewonnen. Das ist, wie gesagt, auch eine der Schwachstellen des Schengen-Routings. Das Internet ist global, wir wollen global kommunizieren, und ich bin genauso besorgt über meine Daten, die ins Nicht-Schengen-Ausland gehen, wie über die, die im Schengen-Raum bleiben.

Für die Wirtschaft ist es eine Frage, die ich vorhin schon angesprochen habe. Man muss einfach eine vernünftige Kalkulation machen. Also man muss gucken: Was kostet es, Kapazitäten aufzubauen? Wenn Kapazitäten aufgebaut werden müssten im großen Umfang, muss die irgendjemand bezahlen. Das wird sich sicherlich auf die Wirtschaft auswirken. Wie groß diese Auswirkung ist, kann ich nicht beantworten. Aber das müsste man einfach nüchtern analysieren.

Dann die Frage: Können wir die NSA sozusagen totrüsten? Meine Antwort wäre eigentlich ziemlich genau die gleiche wie die von Frank Rieger. Bei Dingen wie kryptografiebasierten Lösungen - Ende-zu-Ende-Verschlüsselung gegen Überwachung durch die NSA - ist die Antwort klar Ja. Also ich kann das Sicherheitsniveau so weit nach oben treiben, dass ich ein beliebig

hohes Budget mit einem beliebig großen Faktor einfach ausschöpfen kann.

Wenn es um gezielte Angriffe geht - also diese berühmten APTs -, ist es wirklich so, wie ich es vorhin versucht habe zu sagen. Man kann einzelne Personen nie hundertprozentig schützen. Das ist keine Frage von Technik, weil im Endeffekt kann ich immer jemanden mit dem berühmten Klempnerkasten schicken, der einfach eine Wanze einbaut. Dagegen kann ich jetzt persönlich relativ wenig machen.

Was ich sicherlich machen kann, ist, dass ich Angriffe, wie sie in den Katalogen, die von Snowden veröffentlicht worden sind, beschrieben sind, deutlich verteuern kann. Also ich kann sozusagen dafür sorgen, dass das Budget, was heute vielleicht ausreicht, um, sagen wir mal, 10 000 Personen oder 100 000 Personen zu überwachen, dann vielleicht nur noch ausreicht, um vielleicht 1 000 oder 10 000 zu überwachen. Das kriege ich hin.

Dauerhaft - das war ein Teil Ihrer Frage - wird so was nie sein. Also Menschen machen Fehler. Wir können die Fehlerrate reduzieren. Es wird immer neue IT-Sicherheitsangriffe geben. Wir müssen immer gucken, dass wir weiter vorangehen. Also in diesem Sinne ist es ein dauernder Wettstreit zwischen Angreifern und Verteidigern.

Auch bei der Kryptografie - haben Sie schon gesehen -: Die Empfehlungen zu Schlüssellängen werden regelmäßig upgedatet. Also was früher sicher war, wie 1 024 Bit bei RSA, gilt heute nicht mehr als so furchtbar sicher, und die Empfehlungen gehen eher Richtung 3 000. Es gibt auch Empfehlungen Richtung 10 000 und noch größeren Schlüssellängen. Also diese Art von Wachstum, die man bei der Kryptografie klar sieht, wird es überall geben.

So, ich hoffe, ich habe alle Ihre Fragen beantwortet.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für die Beantwortung der Fragen.

Sachverständiger Prof. Dr. Michael Waidner: Gut, ich habe noch Herrn Ostermann.

Vorsitzender Dr. Patrick Sensburg: Okay, Entschuldigung.

Sachverständiger Prof. Dr. Michael Waidner: Wenn Sie mir noch ganz kurz zuhören.

Vorsitzender Dr. Patrick Sensburg: Natürlich.

Sachverständiger Prof. Dr. Michael Waidner: Oder Sie dürfen mir zuhören; Sie dürfen auch was anderes tun. - Herr Ostermann hatte gefragt, was der Staat tun muss, um Ende-zu-Ende-Verschlüsselung zu unterstützen, und wie man Public-Key-Infrastrukturen einrichten kann, wie man Anonymisierungsdienste einrichten kann. An der Stelle denke ich: Für den Staat geht es weniger darum, dass er selbst diese Infrastrukturen zur Verfügung stellt. Das ist sicherlich eine Option, aber ich denke, es geht eher darum, dass man, wie bei anderen Dienstleistungen auch, die Voraussetzungen dafür schafft, dass diese Dienstleistungen entstehen, sodass man im Markt auch eine gewisse Wahl hat.

Ich würde jetzt nicht sagen, das BSI soll als neue Aufgabe bekommen: „Jetzt macht eine PKI für die Republik“, sondern es müssen Richtlinienstandards geschaffen werden, es müssen Incentives geschaffen werden, und es muss eine Verpflichtung bestehen, dass sozusagen bis in den letzten Winkel des Odenwalds eine PKI sozusagen zur Verfügung steht, genauso wie in den letzten Winkeln des Odenwalds ein Breitbandnetz zur Verfügung stehen soll.

Das Gleiche gilt auch für Anonymisierungsdienste. Wenn wir so was haben wollen wie anonyme Kommunikation als ein Grunddienst, der da sein muss, dann müssen die entsprechenden Infrastrukturen da sein. Wichtig ist immer an der Stelle: Die Infrastrukturen sind das, was wirklich Geld kosten wird. Also sozusagen: Es ist wichtig, E-Mail-Programme zu haben, die verschlüsseln, Chat-Programme zu haben usw. Das ist aber nicht das wirklich Schwierige oder das wirklich Teure. Das Teure ist die Infrastruktur, die ausgerollt werden muss.

Dann hatten Sie gefragt, welche Organisation gemeint ist oder wer das mit dem Verbraucherschutz machen könnte. Natürlich ist es so: Die existierenden Verbraucherschutzorganisationen können diese Rolle übernehmen. Ich sage jetzt also nicht, wir müssen da eine ganz neue Organisation gründen.

Was eben wichtig ist, ist: Es muss weiter hinausgehen über das, was heute da ist. Also Verbraucher sind wirklich das schwächste Glied. Da muss wirklich massiv für Verbraucher Lobbying gemacht werden für sichere Angebote. Es müssen Dinge bereitgestellt werden, wie beispielsweise Infrastruktur für die Verbraucher usw., es müssen Tools entwickelt werden, es muss vielleicht auch ein bisschen gesteuert werden, was in der Forschung passiert. Das geht weit über das hinaus, was heute von Verbraucherschutzorganisationen gemacht wird. Aber die könnten das natürlich tun. Es geht auch weit hinaus über das, was beispielsweise vom BSI gemacht wird, wie „BSI für Bürger“. - Also da gibt es gute Ansätze, aber sie reichen bei Weitem und lange nicht aus.

Dann hatten Sie gefragt nach dem berühmten Airbus-Modell für IT-Sicherheit. Dazu möchte ich zwei Sachen sagen:

Zum einen: Der Markt für so etwas ist wirklich da, denke ich. Also ich denke, der IT-Sicherheitsmarkt ist international ein attraktiver Markt. Die internationalen Player sind Firmen wie Cisco, HP, IBM, Symantec - lauter gutklingende Namen aus den USA. Es ist einer der am schnellsten wachsenden Märkte, und ich denke, wir haben eben einen eklatanten Vorteil an dieser Stelle, den wir einfach nur nutzen müssen. Also der Markt ist definitiv da, und mit den Maßnahmen, die ich vorhin geschildert habe - also Dingen wie eben Standards, Standards auch durchsetzen in der öffentlichen Beschaffung, über Haftungsfragen nachdenken -, kann man diesen Markt auch deutlich nach oben ziehen.

Jetzt: Airbus steht natürlich für das große Megaunternehmen und nicht für die kleinen KMUs. An der Stelle geht es mir eigentlich darum: Also, IT-Sicherheit in Europa ist zurzeit ein sehr zersplitterter Markt. Es gibt viele tolle Firmen. Auch in Deutschland gibt es - mit TeleTrusT gibt es einen Verband; ich weiß gar nicht, wie viele Mitglieder der mittlerweile hat; es müssen Hunderte sein - eine sehr, sehr reichhaltige Landschaft. Die machen alle tolle Sachen.

Meiner Erfahrung nach ist es einfach so: Diese IT-Sicherheitsfirmen tun sich sehr, sehr schwer, im internationalen Kontext erfolgreich zu sein, also ins Ausland zu verkaufen. Es gibt dann einmal einen französischen Markt, einen deutschen Markt, einen UK-Markt. Wir müssen diesen Firmen irgendwie helfen, international agieren zu können: also keine deutschen Standards, weg von diesen Spezialstandards, die man nur in Deutschland verkaufen kann und sonst nirgends, hin zumindest mal zu europäischen Standards oder am besten zu internationalen Standards. Das ist eine Sache. Das hilft KMUs und den Airbussen gleichzeitig. Deshalb glaube ich, dass wir so was brauchen wie einen Airbus für IT-Sicherheit. Das liegt einfach daran: Also, wir brauchen ja nicht nur tolle Standards und Vorschriften, dass man da was kaufen kann, sondern es muss ja auch jemanden geben, der das Zeug wirklich produzieren kann.

Es gibt sehr viele Diskussionen dazu, dass man solche Dinge machen möchte wie vertrauenswürdige Plattformen, also eine vertrauenswürdige Plattform für Industrie 4.0 beispielsweise, was Herr Gaycken vorhin angesprochen hatte. Das kann man sehr schnell tun, wenn man die Ressourcen da reinsteckt. Also, die Innovationszyklen in der IT unterschätzt man oft. Das sind so was wie vier, fünf Jahre; dann hat man so was. Das ist nicht lange; aber es ist eine horrende Investition, die über die Kraft von einzelnen KMUs hinausgeht. Deswegen denke ich, man braucht einen Zusammenschluss von mehreren. Ob das jetzt, wie Airbus, der Zusammenschluss der ganzen europäischen Industrie ist, weiß ich nicht - eher unwahrscheinlich -, ob es eine Föderation ist, also eine Stiftung oder eine Genossenschaft oder so was, dazu kann ich nicht viel sagen. Aber es gibt Mechanismen, die kritischen Maße zusammenzuziehen, die man braucht, um wirklich sichere Systeme zu bauen.

Abschließend möchte ich nur ganz kurz zur Ehrenrettung der SAPs und aller anderen Firmen, die Sandro die ganze Zeit als schlechtes Beispiel genommen hat, sagen: Also, natürlich ist es nicht so, dass jeder Entwickler in einer Firma, der eine Tastatur hat, jeden beliebigen Code ändern kann. Es ist in der Tat so, dass es so was wie 300 Millionen Zeilen[4] gibt und mehrere 10 Millionen Zeilencodes[4] in allen großen Programmen. Dementsprechend kann man hochrechnen: mehrere Tausend Schwachstellen, die man

4) Protokoll korrigiert, siehe Anlage 1.

ausnutzen kann. Aber es hat sehr, sehr viel schon stattgefunden.

Ich möchte auch mal positiv erwähnen: Also, seitdem wir uns mit diesem Thema beschäftigen - Security and Privacy by Design - und seit den NSA-Enthüllungen ist die Bereitschaft gerade bei großen Firmen wie SAP, Prozesse einzuführen, um die Qualität nach oben zu treiben, Kontrollen einzuführen, gerade auch mit Open Source Code besser umzugehen und so, dramatisch nach oben gegangen. Also, es gibt furchtbar viel zu tun; aber man darf nie in Pessimismus verfallen. Das hilft niemandem. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ich glaube, jetzt sind alle Fragen beantwortet, und auch alle Kollegen nicken. Es wäre schon fast bizarr, wenn die NSA dazu beigetragen hätte, dass sich hier ein dementsprechend großer Markt entwickelt, dass sich „Security like in Germany“ oder europäische Standards entwickeln. Allein wenn man mal sich vorstellt, welches volkswirtschaftliche Volumen die Vorschläge, die gerade diskutiert werden, haben, dann kann man, glaube ich, erkennen, wie groß dieses Thema ist. Also, ich finde das unheimlich beeindruckend.

Ich möchte jetzt zur nächsten Fraktion kommen und Ihnen, liebe Kolleginnen und Kollegen von der Fraktion Die Linke, Gelegenheit geben, Fragen zu stellen. Frau Obfrau Renner.

Martina Renner (DIE LINKE): Danke, Herr Vorsitzender. - Mein Dank natürlich zuerst auch mal an Sie, meine Herren Sachverständige, auch für Ihre schriftliche Zuleitung der Gutachten.

Ich will am Anfang eine allgemeine Frage stellen und dann zu vier technischen Details einzelne Fragen noch mal an Sie richten.

Die allgemeine Frage schließt sich an eine Eingangsbemerkung von Professor Waidner an. Er sagte, er will referieren zum Stand der Schwarzen Kunst bei der Überwachung des Internets. Was mich so umtreibt, ist eigentlich: Wie halte ich denn die Hexenmeister der Schwarzen Kunst von dem fern, was Sie dann jetzt alle an möglichen technischen, politischen und rechtlichen Schlussfolgerungen formuliert haben, Ende-zu-Ende-Verschlüsselung und all dem, was wir hier diskutieren? Ich frage das vor dem Hintergrund vieler Einzelbefunde, die wir ja auch in den letzten Wochen und Monaten in der Presse gesehen haben, die wir in den Akten sehen, die wir diskutieren.

Eine Behörde, die zum Beispiel mit diesen Fragen befasst ist - das BSI, das Bundesamt für die Sicherheit in der IT-Technik -, kooperiert mit der NSA. Wir hatten die letzten Tage - ich würde es fast so sagen - den Skandal, dass eines der Unternehmen, die schon sehr lange im Verdacht stehen, ich sage mal, Schnittstellen für Geheimdienste zur Verfügung zu stellen - Verizon -, nicht nur den Bundestag zum Teil bedient, sondern auch Landtage und Bundesbehörden. Sie sprachen davon, Herr Rieger, Experten wechselten die Seiten. Oder: Herr Gaycken sagte, der Dienst sei auch in der Lage, zum Beispiel in Firmen Leute einzuschleusen, und dann nannten Sie SAP. Das Beispiel war ja beliebig. Es ging ja nicht um SAP, sondern insgesamt um die Problematik.

Das heißt, wie halte ich die Hexenmeister der Schwarzen Kunst von alledem fern, was wir hier diskutieren, was unser aller IT-Sicherheit - der Bürger und Bürgerinnen, der Unternehmen, der Exekutive, der Parlamente - erhöhen würde? Da sehe ich noch nicht wirklich Licht am Ende des Tunnels, weil anscheinend haben diese Dienste ja vielfältige technische wie personelle wie finanzielle Möglichkeiten, jede dieser sozusagen Vorkehrungen und Ansätze zu unterlaufen, zu unterminieren.

Die vier technischen Fragen beziehen sich zum einen auf diese Schnittstellen bei Telekommunikationsanbietern, die geschaffen wurden, um dann auch unter Richtervorbehalt Strafverfolgungsbehörden den Zugang zu Telekommunikationsdaten zu verschaffen. Sie sprachen vorhin davon - Herr Rieger führte das auch aus -, dass diese Schnittstellen eben auch für die nachrichtendienstliche Informationsbeschaffung genutzt werden können. Ich würde mal ganz gerne wissen, wie das genau passiert.

Dann wurde ein bisschen andiskutiert, dass es durchaus ja technische Möglichkeiten geben könnte, dem einen Riegel vorzuschieben. Ich frage mich allerdings, wie Sie dies beurteilen vor dem Hintergrund, dass wir ja nicht nur auf nationaler Ebene, sondern auch im internationalen Rahmen eine zunehmende Kooperation der Strafverfolgungsbehörden mit

den Geheimdiensten haben, bis hin zu gemeinsamen Datenbanken und Ähnlichem. Also, selbst wenn es technisch möglich ist, diese Schnittstellen dichtzumachen: Wird das nicht durch das alles, was wir mittlerweile an Kooperation in dem Bereich haben, dann wieder fortlaufend irgendwie ausgehebelt? Und: Wie sehen Sie eigentlich die Forderung, dass man Bürger und Bürgerinnen über diese Zugriffsmöglichkeiten bei den Telekommunikationsanbietern informieren müsste und zum Beispiel auch Nutzer, die Gegenstand solcher Maßnahmen geworden sind, im Nachgang zu diesen Datenerhebungen informiert?

Dann ein Thema, das auch die letzten Tage eine Rolle spielte, Stichwort „Glasfaserkabel“, also Codename „Warp Drive“, diese gemeinsame Operation von NSA, BND und drittem Partner, den wir noch nicht kennen. Ich würde gerne wissen, was Sie zu dieser Funktionsweise des Abgreifens von Daten von Glasfaserkabeln wissen. Also, welche Abhör- und Überwachungsmöglichkeiten gibt es für Dienste, Lichtwellenleiter abzuhören, die Daten abzugreifen? Ist es möglich, lediglich einzelne beschaltete Fasern eines Glasfaserkabels abzuhören und so weit internationale Übertragungswege länderbezogen auszuwerten? Oder ist es eher so, dass der Geheimdienst erst mal alles erfasst, was auf diesem Kabel transportiert wird, und im zweiten Schritt dann zum Beispiel die Daten ausfiltert? Ist zum Beispiel das Abhören von solchen Seekabeln eigentlich möglich, ohne dass der Betreiber der Infrastruktur das merkt? Da sind Sie meine technischen Experten, die mir vielleicht so eine Frage beantworten können.

Herr Gaycken hat das jetzt auch in seinen Ausführungen noch mal erwähnt, aber auch in seiner schriftlichen Stellungnahme: Er hat davon gesprochen, dass es unbemerkte Zugriffe auf Kommunikationssysteme geben kann durch die NSA - er hat da insbesondere drei Programme erwähnt, TAO, GENIE - und dass es bei der NSA auch das Vorhaben gibt, sozusagen Modifikationen an der Linux Mastercopy vorzunehmen. Bei GENIE haben Sie vorhin noch mal gesagt: Da gibt es auch den ganzen monetären Rahmen, der da bekannt ist. Mich würde interessieren: Wie sieht die Praxis dieses Programms aus? Wie funktioniert das?

Können Sie uns zum Zweiten erklären, welche Auswirkungen die Manipulationsaktivitäten der NSA an der Linux Mastercopy haben können für die Nutzer und Nutzerinnen? Bislang dachte ich - da das ja eine Open-Source-Programmierung ist -, dass das eher eine sichere Komponente ist. Wie ist jetzt sozusagen diese neue Entwicklung dort einzuschätzen?

Wenn ich noch eine Minute habe - ich gucke mal Richtung Vorsitzender -, dann würde ich gern noch was fragen zur Infizierung von Endgeräten mit Malware und Fernsteuerung durch Malware. Bereits im März 2014 ist in den Medien und auch in Internetblogs berichtet worden, dass die NSA mittels des Einsatzes zweier Programme Systeme und Endnutzergeräte beispielsweise durch Übermittlung einer gefälschten Facebook-Anmeldeseite mit Malware infizieren kann.

Jetzt ist die Frage, jetzt nicht konkret zu diesem, sondern mal mit Blick auf die Bundesrepublik - der Bundesnachrichtendienst hat schon lange vor, seit 2006, wie wir wissen, einen Bundestrojaner zu entwickeln usw. usf. und ist in dem Zusammenhang auch im Austausch mit der NSA -: Welche Konsequenzen ziehen Sie daraus, dass Programme wie der Bundestrojaner auch in der Lage sind, auf infizierten Endgeräten belastete, gefälschte Dateien oder Dokumente abzulegen, mit denen Spähangriffe gegen Endnutzer nachträglich legitimiert werden können? Und - ganz konkret -: Wie sind vor diesem Hintergrund und angesichts der Überwachungsaffäre aus Ihrer Sicht die Pläne der deutschen Sicherheitsbehörden, die wir jetzt auch gerade kürzlich diskutiert haben, zu bewerten, die sozialen Netzwerke systematisch abzuhören? Sie wissen ja: Da gibt es ja durchaus auch finanzielle Forderungen aus den Behörden, gerade für den Bereich Aufwüchse zu generieren, damit man dort, in dem Bereich soziale Netzwerke, insbesondere Facebook, aktiv werden kann. - Das wären so meine Fragen, die mehr dann auf diese technischen Seiten hinweisen würden. - Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für die Fragen. - Bevor ich den Sachverständigen das Wort gebe, zwei Hinweise:

Wir haben den Versorgungswagen hier kurz in den Saal geholt. Jemand, der sich versorgen will, kann das jetzt im Laufe der laufenden Sitzung machen. Dann geht der Versorgungswagen wieder raus, sodass auch Sie, meine Damen und Herren von der Galerie, sich draußen vor dem Sitzungssaal ausreichend mit Getränken und Speisen versorgen können, ohne dass wir die Sitzung dafür unterbrechen müssen.

Zweitens. Weil gerade über Twitter die Meldung kam, es wäre das Twittern aus dieser Sitzung nicht zugelassen: Das ist nicht richtig. Ich habe gerade, von Anfang an, gesagt, dass Bild-, Ton- und Filmaufzeichnungen nicht gestattet sind. Wir haben bereits in den ersten Sitzungen ganz klar gesagt, dass journalistische Berichte, aber auch Twittern aus der Sitzung möglich sind, nur eben nicht als Ton- und Bildaufnahme. Aber ganz herzlichen Dank, dass Sie so Anteil an dieser Sitzung nehmen! Ich bitte dann aber, doch auch richtig zu twittern. Sie können es natürlich auch nicht richtig twittern; aber wenn, sollten Sie es richtig machen. Das ist dann sicherlich ein höherer Erklärungswert. Ganz herzlichen Dank hierfür!

Ich darf nun den Sachverständigen zur Beantwortung der Fragen von Frau Kollegin Renner und insgesamt von der Fraktion Die Linke das Wort geben. Ich würde jetzt wieder in der Reihenfolge, wie wir begonnen haben, anfangen mit Ihnen, Professor Waidner.

Sachverständiger Prof. Dr. Michael Waidner: Vielen Dank. - Sie haben richtig schwierige Fragen gestellt, muss ich sagen.

Also, die erste Frage geht ja in die Richtung: Was kann man tun, um sozusagen organisatorische Sicherheit herzustellen? Also, was passiert sozusagen, wenn die bösen Jungs eigentlich auf der guten Seite sind? Das war, glaube ich, Ihre Frage. Das ist natürlich eines der größten Probleme, auch im kommerziellen Bereich. Also, die Dunkelzahlen sind da sehr, sehr hoch. Aber typischerweise sagt man: Mindestens 50 Prozent aller seriösen Angriffe involvieren Innentäter. Innentäter kann man prinzipiell nicht vermeiden; das ist überhaupt keine Frage. Also, jeder von Ihnen könnte ein Innentäter sein und hätte wahrscheinlich einigen Einfluss.

Was man gegen Innentäter tun kann, ist, dass man relativ massiv originellerweise Überwachungstechnologien einsetzt, um zu beobachten, was jemand, der sehr große Privilegien hat, tut, während er sie ausnutzt. Da gibt es relativ umfangreiche Forschungsprogramme. Das ist bei uns nicht ganz so ausgeprägt. In den USA gab es dazu sehr, sehr große Programme. Ob die jetzt effektiv sind oder nicht, kann ich Ihnen leider nicht sagen; aber das ist auf jeden Fall das, was man technisch machen kann. Ansonsten sind es tatsächlich auch einfach solche Dinge wie: Sie müssen in der IT-Sicherheitsbranche beispielsweise ordentliche Gehälter bezahlen; Sie müssen den Leuten vernünftige Incentives geben. Es ist zum großen Teil eine ethische Frage, wie man sich verhält. All diese allgemeinen Dinge, die man an dieser Stelle sagen und sich denken kann, treffen tatsächlich zu; aber es ist ein großes, großes Problem an dieser Stelle.

Zu den eher technischen Fragen, wie man Glasfasern überwacht und ähnliche Dinge, würde ich auf meinen Kollegen Frank Rieger verweisen, der vorhin schon in unserer Vorbesprechung, während Sie sich vorbesprochen haben, ausführlich gute Ideen dazu hatte. Was ich sagen kann, ist, dass ich nicht denke, dass man ein Glasfaserkabel, wie es ja berichtet worden ist, überwachen kann, ohne dass derjenige, der das Glasfaserkabel betreibt, dies merkt, in dem Umfang, wie es berichtet worden ist. Also, man kann einzelne Glasfasern, die hier im Gebäude sind, problemlos überwachen. Ich denke, bei Unterseekabeln halte ich es für relativ unwahrscheinlich, dass man das überwachen kann, ohne dass die Betreiber etwas davon mitbekommen.

Ihre beiden abschließenden Fragen gingen ja eher so in die Richtung: Was sind die Risiken von Überwachungstechnologien, die so überhaupt noch diskutiert werden, wie eben Quellenüberwachung durch Staats- oder Bundestrojaner - wie immer man sie nennen möchte - oder die Überwachung von sozialen Netzen? Also, technisch gesehen: Zunächst mal kann ich zur Überwachung von sozialen Netzen natürlich nicht sehr viel sagen, weil das sind öffentliche Daten, die man natürlich ausnutzen kann. Dagegen kann man technisch relativ wenig tun.

Ich kann Ihnen meine Meinung anbieten, die da wäre, dass ich, wenn ich in einem sozialen Netz unterwegs bin, eine gewisse Vorstellung

davon habe, was mit meinen Daten passiert. Dazu gehört normalerweise nicht, dass irgendwelche Überwachungsbehörden meine sozialen Daten ausnutzen. Also, man verletzt die Erwartungshaltung der Nutzer, was ich persönlich jetzt nicht okay finde. Technisch kann ich nichts dagegen tun. Es ist kein Problem, so etwas zu machen.

Zum Problem Bundestrojaner und „Kann ich mit einem Trojaner Dinge auf einem Rechner hinterlegen, die hinterher Anlass bieten würden, was anderes zu tun?“. Da ist die Antwort natürlich ganz klar: Ja, natürlich. Also, wenn ich einen Trojaner habe, einen universellen Trojaner auf einer Plattform, der auf dieser Plattform alles tun kann, was der Benutzer auch tun könnte, dann kann der natürlich dort auch alle möglichen seltsamen Dinge tun. Es gab da in Deutschland ja heftige Diskussionen dazu, ob ein Bundestrojaner eine zulässige Methode ist oder nicht und welche Risiken damit verbunden sind. Ich denke, alle Risiken, die damals diskutiert worden sind, gelten natürlich heute noch genauso, wie sie damals gegolten haben.

Also, ein Bundestrojaner - das ist ein schlechtes Wort - oder ein Trojaner zur Überwachung hat nur dann sozusagen einen halbwegs seriösen Sinn, wenn er upgedatet werden kann. Das heißt, ich kann einen Bundestrojaner oder ein trojanisches Pferd zur Überwachung eigentlich nur dann mit gutem Gewissen betreiben, wenn ich in der Lage bin, die Fehler, die ich unvermeidlich gemacht haben werde, auch wieder zu beheben. Damit kann ich natürlich ein trojanisches Pferd immer auch beliebig ausbauen. Also, sozusagen das Risiko ist nicht zu überschätzen. Technisch kann ich von daher wiederum nur sagen: Ein trojanisches Pferd ist immer eine schlechte Idee, genauso wie eine Schwachstelle auszunutzen immer eine schlechte Idee ist. Also, die sichersten Plattformen sind eben einfach die Plattformen, die sicher sind, keine trojanischen Pferde enthalten, nicht leicht korrum-pierbar sind, keine Schwachstellen haben. Wenn man als Hersteller von einer Schwachstelle erfährt, dann sollte man sie typischerweise eben fixen und nicht in irgendeiner Form zur Ausnutzung freigeben. - Vielen Dank von meiner Seite.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Damit darf ich Herrn Dr. Gaycken jetzt das Wort geben.

Sachverständiger Dr. Sandro Gaycken: Vielen Dank. - Ich möchte zu Anfang noch mal kurz SAP in Schutz nehmen. Das war jetzt natürlich nur das Beispiel sozusagen; viele Firmen sind noch viel schlechter, gerade auch Oracle; nicht dass mich hier irgendjemand verklagt. Und es stimmt natürlich, dass SAP sich auch viel Mühe gegebenen hat in der letzten Zeit, seine Missstände zu beheben. - Das also nur kurz vorweg.

Jetzt zur Frage: Wie halte ich die NSA und andere Nachrichtendienste davon fern, irgendwie diese Prozesse zu infiltrieren? Einmal zur Frage der Kooperation mit der NSA durch unsere Bundesbehörden: Da spricht natürlich jetzt für mich erst mal nichts dagegen. Das sind ja immer noch unsere Freunde und Alliierten. Und wenn wir uns irgendwie darauf einigen, dass wir in bestimmten strategischen Zielen uns einig sind und da unsere Fähigkeiten ergänzen wollen, Kooperationen machen wollen, dann sollen wir das gerne tun. Wir müssen nur natürlich bei diesen Kooperationen darauf achten, dass die rechtlichen Rahmenbedingungen klar sind. Das heißt, wir müssen die auch gerade für diese neuen technischen Möglichkeiten noch mal genau revidieren und klar definieren, was das eigentlich bedeutet, was die dürfen und wo sie es dürfen. Dann müssen wir natürlich auch die parlamentarischen Kontrollgremien in eine Lage bringen, dass sie auch mit ihrer Expertise das dann beurteilen können, was da passiert. Da sehe ich noch große Defizite und große Probleme.

Das war übrigens auch bei der NSA eines der Basisprobleme. Da hatte ich mal gesprochen mit jemandem, der im Senat für diese Kontrollgremien mit zuständig war, und der hat gesagt: Das ist unsere Schuld. - Die haben sofort gesehen, dass das ein riesiger strategischer Schaden für die USA ist, für die Wirtschaft genauso wie für das Ansehen und Kooperationen usw., und haben gesagt: Wir hätten das verhindern müssen. Die NSA hat sozusagen nur ihren Job gemacht - maximale Nachrichtengewinnung -, und die Kontrollgremien haben es aber nicht verstanden, waren auch total überarbeitet von diesen riesigen Stapeln, haben

das dann von da nach da geschoben und haben gesagt: Macht mal; wird schon okay sein. - Das darf natürlich nicht passieren. Das heißt, wir müssen auch die Kontrollgremien dazu bringen, dass die das verstehen, dass die notfalls auch externe Expertise dazuholen, die auch diese rechtlichen, strategischen Dimensionen mit bedenken kann, und dass die das dann halt eben auch regelmäßig kontrollieren und vorher rechtlich genau und verständlich und eindeutig definieren.

Zur Unterminierung durch Innentäter: Wenn wir jetzt natürlich auch dazu übergehen, Hochsicherheitskonzepte zu bauen und zu entwickeln und auch Hochsicherheits-IT zu entwickeln und uns auch durch Maßnahmen dieser Überwachung zu entziehen, müssen wir damit rechnen, dass verschiedene Nachrichtendienste ein hohes Interesse haben, Innentäter sehr früh einzuschleusen. Das heißt, wir müssen da also auch mit einer Spionageabwehrperspektive rangehen, wenn wir diese Prozesse anfangen. Und gerade auch wenn wir in die industrielle Implementierung gehen, müssen wir das von Anfang an auf einem Ü-3-Level machen und das vernünftig machen und da eine sehr hohe Sicherheit einziehen: in der Konzeption, in der Entwicklung, in der Implementierung. Da darf es gar keine Diskussion geben, weil sonst ist das sofort wieder weg.

Zum Abgreifen von Glasfaserkabeln hätte ich ein bisschen eine andere Meinung als Michael. Also, wir wissen - das ist auch schon lange bekannt und auch öffentlich bekannt -, dass zum Beispiel in Portugal, wo ja einige dieser Kabel ankommen, so aufgereiht entlang der Kabelstrecke verschiedene Botschaften unterschiedlicher Länder stehen. Das ist natürlich nicht, weil die Aussicht so schön ist, sondern weil die Kabel darunter liegen. Da ist es also rational, dass die sich da unten im Keller durchbuddeln und dann da an diese Kabel rangehen, die Daten spiegeln und auslesen. Das merkt die Telekom nicht. Die merken vielleicht mal kurz irgendwie so eine Verzögerung. Die wissen natürlich, die Telekom-Provider, dass es Botschaften auf ihren Kabelstrecken gibt. Die sind ja auch nicht blöd und können sich auch denken, was die da machen im Keller. Aber das geht, und das merkt man im laufenden Betrieb eigentlich nicht, solange die nicht irgendwelche gravierenden Fehler machen und den Kaffee drüberkippen, und dann ist der Datenverkehr für Europa weg oder so was; aber das passiert denen eigentlich nicht.

Dann noch zu den gezielten Aktivitäten: Das ist natürlich eine sehr gefährliche und schwierige Geschichte. Wir wissen, dass die NSA, aber auch viele andere Nachrichtendienste darauf eigentlich im Moment ihr Hauptgewicht legen. Also, ein paar der Informationen von Snowden sind ja auch ein bisschen veraltet. Wir wissen jetzt halt - oder vermuten das aufgrund der Aufstellungen, die wir so gesehen haben -, dass man doch sehr stark rübergegangen ist in diese stärker gezielten Aktivitäten und dass man auch das IT-Ökosystem versucht möglichst früh zu infiltrieren - in der Herstellung, Produktion -, an Stellen zu infiltrieren, die sehr gut skalieren, ja, also Produkte, die überall im Gebrauch sind, Produkte, bei denen sich Angriffe, Schwachstellen sehr schwer detektieren lassen, oder Produkte, die halt in speziellen Kontexten, wie zum Beispiel in der iranischen Atomproduktion, eine Rolle spielen, dass man da irgendwie relativ früh reinkommt. Da ist man also sehr interessiert und sehr umfangreich auch in der Lage. Da spielen natürlich auch die klassischen nachrichtendienstlichen Fähigkeiten der Infiltration, der Manipulation eine ganz entscheidende Rolle, die da also mit diesen Cyberfähigkeiten sozusagen kombiniert werden. Das ist also auch so eine Kombination, die noch nicht so richtig bedacht ist, wo alleine technische Maßnahmen halt auch nicht helfen.

Das Projekt GENIE hatte ich schon erwähnt. Es ist da sehr indikativ. Da passiert sehr, sehr viel, was wir überhaupt nicht wieder einholen können. Natürlich gibt es dann auch Interessen an solchen Sachen wie der Linux Mastercopy. Na klar haben die ein Interesse, Linux zu infiltrieren. Eine Mastercopy, das ist so die eine Version, von der dann alle anderen abgezogen werden; das ist natürlich eine ideale Skalierung. Also, man muss bei diesen Schutzmaßnahmen, wenn man die implementiert, halt eben auch immer sehen: Wo würde der Angreifer ansetzen, um eine maximale Skalierung und Wirkung mit minimalen Mitteln zu erreichen? Das sind eben gerade diese Basisstrukturen. Wir arbeiten aber in der IT-Sicherheit, im Schutz, eigentlich immer ganz außen, an der Peripherie, an den vielen kleinen

Endpunkten, ohne dass wir diese strukturellen Kernpunkte mal adressieren.

Auch die Open-Source-Sicherheit, muss ich sagen, bringt natürlich für gezielte Aktivitäten von Nachrichtendiensten keinen Gewinn; das muss ich ganz klar so sagen. Na klar sind die wesentlich besser in der Sicherheit bzw. sind weniger verwundbar als kommerzielle Projekte; aber das gilt auch nur für Kernprojekte in der Open-Source-Community. Wenn das dann irgendwie in die Peripherie geht und das ist irgend so ein Open-Source-Geschraube, wo drei Leute mal dran rumbasteln, sind die dann in der Regel noch wesentlich schlechter als kommerzielle Sachen und haben ja auch keine Prozesse drin, um das zu evaluieren. Die Kernprojekte sind sicherer als die kommerziellen Kernprojekte, aber nicht sicher genug, um eine Infiltration und auch eine nachhaltige und mehrfache Infiltration durch Nachrichtendienste zu verhindern.

Dann zum Schluss zur Frage, ob mit Bundestrojanern und solchen Sachen auch belastende Beweise hinterlegt und gefälscht werden können: Na klar, kein Problem. Man muss eine Einzelfallbetrachtung sicherlich machen, was die da tun können, ob die dazu in der Lage sind. Aber das ist prinzipiell das Problem: Digitale Beweise haben eine sehr schlechte Beweiskraft. Das ist also auch ein Grundproblem in der digitalen Forensik. Wenn also die Möglichkeit besteht, dass da irgendwie jemand draufschreiben kann, der sich Zugriff verschafft hat, dann können Sie die Sachen eigentlich schon nicht mehr so richtig gerichtsfest verwerten. Deswegen gilt auch bei vielen Forensikern und auch in der Aufklärung normalerweise das Credo, dass man diese Dinge nur benutzt, um Indizien für die weitere Aufklärung zu finden, aber nicht, um gerichtsharte Indizien zu finden.

Also, viele verwenden solche Sachen. Die hacken sich bei einem Gegner rein; aber die wissen genau, dass das, was sie dann da finden, nicht gerichtsfest verwertbar ist. Von daher interessiert die das gar nicht, sondern die wollen dann nur Beweise sammeln, wo sie die dann finden können, wo sie vielleicht härtere Beweise sammeln können. Oder die machen halt solche Sachen, wie die USA das jetzt machen, über die Firmen, dass sie einfach Berichte publizieren über solche Angriffe auf chinesische Einheiten. Dann sind sie sozusagen nicht haftbar als Staat gegenüber der chinesischen Regierung für irgendwelche Falschbehauptungen und können es aber trotzdem ein bisschen eskalieren.

Zu den Anträgen und Ideen, die sozialen Netzwerke jetzt intensiver abzuhören, möchte ich eigentlich nur das wiederholen, was ich vorhin schon gesagt habe: Ich halte die Ausbildung gezielter Fähigkeiten in den Diensten und Strafverfolgungsbehörden für kriminalistisch und aufklärerisch wesentlich effizienter, und die sind gleichzeitig datenschutzsensibel. Von daher sollte man vielleicht, bevor man solche Fässer aufmacht, erst mal die Gesamtmenge der Mittel evaluieren - das ist meines Erachtens noch nicht so richtig geschehen -, sich auch mal ansehen mit anderen Experten oder anderen Regierungen: „Was haben die so ausgebildet an gezielten Fähigkeiten, wie benutzen die das, wie sinnvoll ist es?“, und dann sollte man vielleicht eher solche Sachen anbauen und sich damit weiterentwickeln, als jetzt die Massenüberwachung weiter auszubauen. - Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Herr Dr. Gaycken. - Dann kommen wir zu Ihnen, Herr Rieger. Ich darf Sie um Ihre Antworten bitten.

Sachverständiger Frank Rieger: Frau Renner, zur Frage: Wie schafft man es, diesen Sumpf aufzuräumen und die Hexenmeister fernzuhalten? Ich stimme da tatsächlich Herrn Gaycken nicht zu. Eine klassische Sicherheitsüberprüfung bringt uns da gerade ganz wenig, weil wir mit solchen Sicherheitsüberprüfungen möglicherweise Leute finden können, die halt, sagen wir mal, von östlichen oder chinesischen Diensten bezahlt werden, uns zu infiltrieren, aber sicherlich keine Leute, die, sagen wir mal, von Verbündeten geschickt werden.

Viel eher sollten wir darauf dringen, dass wir die Prozesse, mit denen Software entwickelt wird, sowohl im Hochsicherheitsbereich als auch im allgemeinen Softwarebereich, so sicher machen, dass wir möglichst wenige Probleme bekommen. Also, wenn wir uns mal angucken: „Wo kommt der Großteil unserer Probleme her?“, ist es einfach schlechte Software. Diese Fehler in dieser Software werden absichtlich eingebaut. Das ist das, was man heutzutage Backdoors

nennt. Wenn Sie jetzt so einen Source Code analysieren und einen Binary analysieren, wo eine Hintertür drin ist, dann ist es also nicht so, dass es dann da schreit: „Ich bin eine Hintertür!“, sondern es sind halt eigentlich immer - also alles, was ich bisher gesehen habe, mit ganz wenigen Ausnahmen - Fehler, also Schlampereien, Sachen, die so kleine Modifikationen sind, dass man denken kann: Okay, könnte ein Fehler sein; vielleicht hat er es nur nicht besser gewusst. - Deswegen gibt es ja diesen sogenannten Begriff der „bugdoor“, also die Zusammenziehung aus „backdoor“ und „bug“. Was dagegen hilft, sind tatsächliche Audits, das heißt also, sicherzustellen, dass die Software, die wir einsetzen, die Software, die wir entwickeln, auch die Software, die wir neu fördern, tatsächlich angeguckt wird.

Was wir dazu brauchen, ist leider ein bisschen länger. Wir brauchen zum einen in der Ausbildung von unseren Informatikern die Herausbildung dieser Fähigkeiten: dass die halt lernen, einen Code zu lesen, dass die lernen, Binaries zu analysieren, dass die auch lernen, sicher zu programmieren - das findet derzeit nicht statt; das ist eine große Herausforderung für die Informatikausbildung oder überhaupt für die Ausbildung an den Universitäten und an den FHs von allen Leuten, die irgendwie programmieren; es müssen halt nicht Informatiker sein, es können auch Maschinenbauer sein -, und dass die lernen, eben Schwachstellen im Code zu finden. Das ist eine herausbildbare Fähigkeit. Man muss es halt nur tatsächlich verpflichtend vorschreiben in den Ausbildungscurricula.

Erst wenn wir da sind - das heißt also, wir halt eine möglichst breite Vielfalt von Leuten haben, die Source Codes angucken können, also tatsächlich über die Fähigkeit verfügen, Hintertüren, Schwachstellen oder ein Gemisch von beidem zu finden -, können wir tatsächlich die Sicherheit dramatisch erhöhen, und dann können wir damit auch die Hexenmeister fernhalten, weil in dem Augenblick, wo wir Überprüfbarkeit zu einem wesentlichen Ziel auch des Designs machen – also, wenn wir tatsächlich auch Produkte so designen und Software so designen, dass sie gut überprüfbar sind -, sinken zum einen die Kosten und sinkt zum anderen die Wahrscheinlichkeit, dass man da solche Probleme drinhat. Da kann man relativ früh mit anfangen in der Informatikausbildung, schon in den Schulen teilweise, und man kann es auch über gesetzliche Standards relativ einfach abbilden.

Wie gesagt, von Sicherheitsüberprüfungen halte ich da an dieser Stelle nicht viel. Ich kenne zu viele Firmen, die sicherheitsüberprüfte Mitarbeiter hatten, die sich dann doch als irgendjemand anders herausstellten. Also da gibt es nicht so viel zu holen. Deswegen: Lieber auf Öffentlichkeit setzen, lieber auf Überprüfbarkeit durch alle setzen und anfangen, die Standards zu verbessern und auch die Ausbildung zu verbessern.

Zur Frage: Wie werden Schnittstellen, die bei Anbietern für Strafverfolger eingeräumt wurden, von Geheimdiensten genutzt? Wir müssen da in der Berichterstattung zwei grundsätzliche Dinge unterscheiden. Wir haben in Deutschland die Situation, dass Schnittstellen für Strafverfolger und auch für die Dienste immer von der Rechtsabteilung des Anbieters geprüft werden. Das heißt also, wenn heute zum Beispiel die Polizei zur Telekom geht und sagt: „Wir hätten gerne von diesem bösen Jungen den Telefonanschluss abgehört“, dann guckt da die Rechtsabteilung von der Telekom zumindest schon mal drüber: „Ist das irgendwie rechtlich alles stimmig?“, und schaltet dann eben diesen Anschluss. Wenn so eine Anfrage von den Diensten kommt, ist die Überprüfung beschränkt auf formale Korrektheit. Das heißt, ob jetzt der BND einen Anschluss überwachen möchte für seine Freunde bei der NSA oder für seine eigenen Zwecke, ist schwierig herauszufinden. Am Ende landet es dann in der G-10-Kommission; die muss halt entscheiden, ob das rechtmäßig ist. In welchem Umfang das stattfindet, kann ich nicht sagen.

In anderen Ländern ist es anders, auch in anderen europäischen Ländern. Da ist es so, dass die Dienste und auch die Polizeibehörden sich selbst die Abhörschnittstellen schalten. Das heißt, der Anbieter bekommt davon gar nichts mit. Das ist natürlich eine Situation, die wesentlich gravierender ist als in Deutschland, wo wir zumindest irgendwie noch so ein bisschen Eindämmung da drin haben. Was die sonstigen Daten angeht, also wo es nicht um Abhören geht, sondern zum Beispiel um die Kooperation oder Ermittlung von Biometriedaten

oder die Übermittlung von Personenbewegungsdaten, die ja in großem Umfang in Kooperation mit den Amerikanern im Strafverfolgungsbereich stattfindet - muss ich leider sagen -, müssen wir nach dem, was wir jetzt wissen, davon ausgehen, dass die direkt in Fort Meade bei der NSA landen - also, ich kann mir nichts anderes vorstellen - oder dass die zumindest einen direkten Zugriff auf die Daten haben, die da ausgetauscht werden. Und da ist tatsächlich nur auf rechtlichem Weg eine Einschränkung möglich. Das heißt, wir sollten da weggehen von der massenweisen Übermittlung hin zu einer gezielten Einzelfallübermittlung, wo auch tatsächlich Leute dafür bezahlt werden, hinzugucken, ob es eigentlich plausibel ist, dass diese Daten zum Beispiel für Terrorismus angefordert werden und nicht für Industriespionage.

Die Informationspflicht nach solchen Zugriffen, auch von Nachrichtendiensten auf Daten, auf Kommunikationsverbindungen: Ich bin ein großer Freund davon, die so weit wie möglich zu gestalten, das heißt also, möglichst viel zu informieren, einfach um die demokratische Kontrolle dieser Maßnahmen aufrechtzuerhalten. Je mehr Leute tatsächlich persönliche Betroffenheit von solchen Maßnahmen erfahren oder in ihrer Verwandtschaft oder Bekanntschaft erfahren, desto stärker wird nachgefragt, desto mehr Presseberichterstattung gibt es und desto mehr demokratische Kontrolle dieser Maßnahmen findet statt. Ich weiß, das ist natürlich immer eine heikle Abwägung gerade insbesondere in Strafverfolgungsfragen bezüglich Ermittlungstaktik. Aber selbst wenn es zwei, drei Jahre später stattfindet, halte ich es trotzdem für angemessen, in jedem einzelnen Fall, auch zum Beispiel bei einer Funkzellenabfrage, tatsächlich die Tatsache zu übermitteln, um einfach die gesellschaftliche Diskussion und die Einbalancierung dieser Maßnahmen am Leben zu halten.

Zu den technischen Fragen: Glasfasern können, ohne dass der Anbieter was davon mitbekommt, wenn er nicht absichtlich genau hinsieht, angezapft werden. Es gibt dazu drei wesentliche Verfahren:

Das eine Verfahren, das einfachste, ist in der sogenannten Kopfstation, das heißt also da, wo die Fasern zum Beispiel aus dem Meer kommen und landen oder wo sie von Überlandstrecken in Rechenzentren eingespeist werden. Dort sind die Daten relativ einfach abzugreifen, zumal es dort in der Regel sogar vorgesehene Schnittstellen gibt, mit denen man sich auf eine Faser einkoppeln kann, ohne dass der Verkehr auf dieser Faser gestört wird, und zwar einfach für Zwecke der Fehlerbehebung und der Analyse, ob diese Leitung einfach in Ordnung ist.

Die zweite Möglichkeit - die ist etwas aufwendiger - ist, die sogenannten Repeater anzugreifen. So eine Faser hat eine begrenzte Reichweite. So nach 50, 60 Kilometern muss normalerweise das Signal erneuert werden. Das heißt, da sitzt dann so ein Stück Elektronik dazwischen, sowohl unter Wasser als auch über Land, wo das Lichtsignal, was auf der einen Seite reinkommt, wieder verstärkt wird und auf der anderen Seite wieder ausgeleitet wird. An dieser Stelle ist auch ein Eingriff relativ problemlos möglich. Wir wissen aus Berichten von ehemaligen amerikanischen Geheimdienstmitarbeitern, die sogar auch in der Literatur zu finden sind, dass die Amerikaner diese Fähigkeiten eigentlich schon seit Anfang der 60er-Jahre hatten, damals noch für Kupferkabel, und dass sie die für Fasern weiterentwickelt haben. Es gibt glaubwürdige Berichte darüber, dass die USS Jimmy Carter, also ein Atom-U-Boot, spezifisch für solche Zwecke umgerüstet wurde, also dass die tatsächlich genau diesen Zweck des Abhörens von Glasfaserkabeln als einen Haupteinsatzzweck hat. An Land ist die Sache natürlich noch um vieles einfacher.

Wenn das alles nicht gelingt, also wenn man weder an den Kopfstationen noch an den Repeater rankommt, gibt es immer noch die Möglichkeit, mit sogenannten Biegekopplern zu arbeiten. Das ist ein bisschen heikler. Dazu muss man die Faser aufpulen, also die äußere Umhüllung abmachen, und dann biegt man die Fasern in einen bestimmten Radius, und dann kommt so ein ganz kleines bisschen Licht an der Seite raus. Also, durch eine Faser „bounct“ das Licht so wie durch ein Rohr durch. Wenn man es ein bisschen biegt, kommt da Licht an der Seite raus, der sogenannte Biegekoppler. Sie können sich hier im Museum für Telekommunikation das Exemplar angucken, das die Staatssicherheit benutzt hat, um den Verkehr nach Westberlin abzuhören. Also so alt ist die Technologie, und

die Stasi hatte sie auch schon, sehr instruktiv, sehr einfaches Gerät. Kann man machen, sieht man aber, wenn man die Dämpfung auf der Faser sozusagen beobachtet: Wie verhält sich das Signal? Wenn man da sehr aufmerksam hinsieht, kann man möglicherweise sehen, dass da was passiert. Deswegen wird das halt nur verwendet, wenn man keine anderen Möglichkeiten hat; geht aber im Prinzip.

Zur Frage: Können die Geheimdienste Fasern einzeln abhören, entsprechend Ländern, sage ich mal, sortiert? Es gibt tatsächlich einige wenige Fasern, also Interkontinentalfasern, die von Land zu Land gemietet werden, aber in der Regel haben Sie da Mischverkehre drauf. Also, das heißt, typischerweise ist es so, dass der Verkehr nicht einzeln separierbar ist, dass Sie sagen können: Okay, auf dieser Faser ist jetzt nur der Verkehr von Dänemark nach Großbritannien. - Selbst wenn dem so wäre, muss man bedenken, dass die NSA ja gerne immer redundant abhört. Das heißt, die macht auf der einen Seite einen Vertrag mit dem BND, um an einen bestimmten Verkehr zu kommen, und dann filtert der BND die deutschen Daten raus, und dann machen sie auf der anderen Seite einen Vertrag mit den Briten oder mit den Dänen, und die filtern die deutschen Daten natürlich nicht raus - aber das ist derselbe Verkehr, der da rauskommt -, sondern die filtern nur die dänischen oder britischen Daten raus. Erst am Ende kommen sie immer an die Gesamtheit der Daten. Das heißt, an dieser Stelle anzusetzen, hilft halt nicht wirklich.

Es gibt in der Literatur auch hinreichend Belege dafür, auch von anderen NSA-Whistleblowern, nicht nur Herrn Snowden, dass die NSA typischerweise immer, wenn sie in einem Land nicht zum Zuge kommt oder nationaler Verkehr ausgefiltert wird, sie in ein anderes Land geht, wo dieser Verkehr ebenfalls langkommt, um dann noch den Rest zu bekommen. Wie gesagt, die wollen alles haben und halten sich halt immer nur quasi als Dekoration an die nationalen Gegebenheiten.

Zur Frage „gezieltes Trojanisieren und Fälschung von Beweisen“: Wir hatten in diesem Haus schon mehrere hinlängliche Diskussionen über diese Frage der Trojaner, über Bundestrojaner. Wir hatten das Urteil des Verfassungsgerichts dazu. Das heißt also, die Materie ist hinreichend bekannt. Die Frage, ob man im geheimdienstlichen Bereich mit so was arbeiten kann, kann man lange diskutieren. Sicherlich ist es besser, sagen wir mal so, gezielte Methoden zu verwenden, die eines hohen Aufwands bedürfen und dementsprechend auch seltener eingesetzt werden, als eine Massenüberwachung durchzuführen. Als datenschutzrechtlich unproblematisch würde ich sie trotzdem nicht bezeichnen, zum einen weil man mit einem Trojaner einen vollständigen Zugriff auf alle Inhalte eines Computers bekommt und eben auch Beweismittel problemlos dort platzieren kann.

Das heißt, es ist tatsächlich ein Mittel, das wirklich nur im alleräußersten Notfall eingesetzt werden sollte. Wie wir am Beispiel des Bundestrojaners gesehen haben, arbeiten die entsprechenden Hersteller und Dienststellen da auch eher meistens sehr schlampig. Das heißt also, dass halt die datenschutzrechtliche Absicherung eines solchen Vorgehens auch sehr problematisch ist. Natürlich ist es im geheimdienstlichen Bereich, wo es halt nicht um Beweiserhebung geht, sondern nur um Indizienerhebung, einfacher als im strafrechtlichen Bereich, wo wir halt am Ende Beweise sehen wollen. Trotzdem würde ich jetzt davon absehen, das als Allheilmittel anzupreisen, sondern als möglicherweise im Einzelfall einsetzbares Werkzeug, aber sicherlich nicht als etwas, das im großen Maßstab angewendet werden sollte.

Was die Analyse sozialer Netze angeht, wo der BND ja dann Geld haben wollte: Die Problematik da ist natürlich, dass man immer argumentieren kann: Die Daten sind ja sowieso da draußen, also die Leute geben sie ja freiwillig preis. - Allerdings muss man da sagen: mit einer anderen Erwartungshaltung. Das heißt also, die Erwartung, die einem zum Beispiel von Facebook vermittelt wird, ist, dass nur meine Freunde sehen können, was ich in meiner Timeline poste. Wenn wir als Dienst aber in der Lage sind, den gesamten Verkehr dort mitzuschneiden und zu analysieren und alle Verbindungen nachzuvollziehen, entsteht dadurch ein Lebensprofil. Wir haben das Urteil des Verfassungsgerichts zur Vorratsdatenspeicherung, das eben exakt solche Erstellungen von Lebensprofilen auf der Basis von großflächiger

Datenerhebung als äußerst problematisch deklariert.

Insofern würde ich das in diesem Kontext betrachten, ob man deutschen Diensten so was gestatten sollte. Wie halt die entsprechenden rechtlichen Rahmenbedingungen dafür aussehen, sollte sich exakt eben genau an dieser Möglichkeit zur Lebensprofilerstellung orientieren, genau wie bei allen anderen Metadaten übrigens, also sowohl bei Mobilfunkdaten als auch sozialen Mediadaten, Internetnutzungsdaten. Es geht eigentlich immer genau um diese Lebensprofile und um die Frage: Wie viel sollen Behörden über das Leben des Einzelnen wissen können? Und sie können eigentlich genau alles wissen.

Die Frage stellt sich natürlich genauso auch bei den Unternehmen, die diese sozialen Dienste betreiben. Meiner Meinung nach sollten wir hier zum Beispiel dahin kommen, dass wir sagen: Wir brauchen eine Kartellregulierung, die eingreift, wenn ein Unternehmen zu viel Prozent der Daten meines Lebens hat. Wenn dann Google quasi 90 Prozent der Daten meines Lebens hat, weil ich ihre Autos fahre usw. usf., dann müsste man da wohl eingreifen. Ähnlich sollte man es wahrscheinlich auch bei Behörden handhaben. In dem Augenblick, wo die zu viel über einzelne Personen wissen können, muss man da wohl einschreiten. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. Ich sehe, die Fragen sind beantwortet. - Eine Zwischenfrage.

Roderich Kiesewetter (CDU/CSU): Ich hätte eine Verständnisfrage, eine ganz kurze Zwischenfrage, wenn es gestattet ist, Herr Vorsitzender, ganz kurz nur. Das wäre sehr nett.

Vorsitzender Dr. Patrick Sensburg: Ja, klar.

Roderich Kiesewetter (CDU/CSU): Sie sagten gerade, Herr Rieger, in einem Nebensatz, der BND filtere deutsche Daten aus dem Glasfasernetz heraus. Könnten Sie das nochmal erläutern?

Sachverständiger Frank Rieger: Wir haben ja aus der Presseberichterstattung gelernt, dass der Bundesnachrichtendienst am DE-CIX Verkehr ausleitet. Er ist ja dazu auch im Rahmen der strategischen Fernmeldeüberwachung berechtigt, das mit bis zu 20 Prozent der deutschen Auslandsbandbreite zu tun, und er muss dabei ja, wie wir jetzt auch wissen, deutsche Daten ausfiltern. Wir haben jetzt aus den neuesten Snowden-Dokumenten gelernt, weil er im Inland nicht tätig werden darf, mit welchen kruden Methoden das passiert, also dass im Wesentlichen nur alles nach de-Domain weggefiltert wird und ein paar namentlich bekannte Domainnamen von anderen Unternehmen und Organisationen, die dann rausgelassen wurden, bevor sie halt an die Amerikaner weitergeleitet wurden. Dieses Vorgehen, dass man sagt: „Okay, der jeweilige Auslandsdienst darf Inlandsdaten eigentlich nicht auswerten, außer im begründeten Einzelfall“, wird dort versucht, sage ich mal so, dem Sinn nach grob zu implementieren, aber das ist natürlich im Einzelfall, gerade in so einem internationalen Netz wie dem Internet, sehr schwierig nachzuvollziehen. Wenn ich irgendwie von meiner E-Mail-Adresse, die endet auf rieger.org - - Der Server steht in Deutschland, das hätte trotzdem nichts geholfen, meine Daten wären trotzdem in der BND-Erfassung gelandet.

Vorsitzender Dr. Patrick Sensburg: Okay. Ganz herzlichen Dank. - Jetzt möchte ich aber der Fraktion der SPD das Wort geben, um ihre Fragen zu stellen. Herr Obmann, Herr Flisek, Sie haben das Wort.

Christian Flisek (SPD): Danke, Herr Vorsitzender. - Ich würde bei dem, was Sie jetzt, Herr Rieger, zum Schluss ausgeführt haben auf die Fragen des Kollegen Kiesewetter, noch mal direkt ansetzen wollen. In der Tat haben wir, was unsere eigenen Dienste betrifft, rechtliche Vorgaben - Sie haben es zitiert -, zum einem im G-10-Gesetz, dass höchstens 20 Prozent der jeweiligen Übertragungskapazität der Überwachung ausgewertet werden dürfen im Rahmen der strategischen Kommunikationsüberwachung. Und Sie haben natürlich auch erwähnt, dass der BND beispielsweise Reindaten, die im deutschen Verkehr anfallen zwischen deutschen Staatsbürgern, eben überhaupt nicht überwachen darf. Das heißt, ich habe auf der einen Seite eine Kapazitätsbegrenzung, und ich habe auf der anderen Seite ein Filterproblem, und ich habe

auch, ich sage mal, ein architektonisches Problem mit der Organisation, wie deutsche Geheimdienste organisiert sind, nämlich dass man sagt: „Die setzen immer noch an dem Gegensatz von Inland und Ausland auf“, wo ich ein Fragezeichen mal setzen möchte, ob das in Zeiten jetzt auch einer digitalen globalen Massenkommunikation - noch mal, das Beispiel habe ich schon mal genannt -, wo irgendwelche E-Mails, die von Berlin von mir aus nach München in Deutschland verschickt werden - - wo ich mir nicht sicher sein kann, über welche Wege die eigentlich gehen.

Daher meine Frage: Diese Kapazitätsbegrenzung, das sind ja rechtliche Vorgaben, die sozusagen versuchen, die Grundrechte zu übersetzen in einfaches Recht, in einfache gesetzliche Vorgaben für die Arbeit der Geheimdienste. Wie bewerten Sie diese Art, gesetzgeberisch überhaupt tätig zu werden, aus Ihrer IT-Sicht, aus Ihrem IT-technischen Sachverständnis heraus? Wobei ich jetzt die Frage nicht nur an den Herrn Rieger, sondern auch an die beiden anderen Sachverständigen gerne richten würde. Also, noch mal die Frage: Kapazitätsbegrenzung 20 Prozent, geht das überhaupt heutzutage, macht es überhaupt Sinn, so rechtlich zu arbeiten, um Grundrechte zu verwirklichen, und auf der anderen Seite auch die Filterproblematik, ist das überhaupt möglich? Sie, Herr Rieger, haben ja gerade auch von kruden Methoden gesprochen in dem Zusammenhang, Stichwort eben, dass man zum Beispiel irgendwie Sprache oder de-Domains als Parameter verwendet, die eben überhaupt nichts im Zweifel dann aussagen über die Art der Kommunikation, die dahinter steht.

Mich würde mal eines auch noch vorab interessieren. Wenn ich mir angucke: Das Selbstverständnis von Organisationen wie der NSA ist es, eine globale Informationsvorherrschaft zu erzielen und dann vielleicht auch zu halten. Der Eindruck drängt sich ja auf, dass wir hier auch so eine Art globales IT-Wettrüsten haben. Wir reden auch wenig über Russland oder China. Wir wissen nicht, was da eigentlich vorgeht. Meine Frage wäre jetzt mal: Wenn man sich das anschaut angesichts auch der Zahlen, die wir sehen, wie sehr sich Informationen in unserer Welt eigentlich - - wie schnell sich die Zahl der Informationsmenge verdoppelt, permanent, ist so etwas wie ein Full Take aus Ihrer technischen Perspektive überhaupt denkbar? Ist es dann am Ende auch handelbar? Mich würde mal tatsächlich interessieren, dass Sie darstellen - vielleicht kann das einer von Ihnen machen; ich möchte die Frage da jetzt nicht an alle drei richten -: Wie wird aus einem noch so großen Heuhaufen wirklich eine Nadel? Einfach um das mal verständlich nachvollzogen zu bekommen: Wenn der Heuhaufen wächst, wächst, wächst, vielleicht sind da tatsächlich ein paar Nadeln drin, aber wie funktioniert das technisch nach dem Stand der Technik, so wie wir das derzeit kennen?

Ich hätte Fragen noch mal zum Thema, wie wir uns strategisch hier aufstellen. In der Tat, ein relevanter Markt für sichere IT-Produkte wurde, glaube ich, von Ihnen dreien insgesamt als ein strategisches Ziel für Deutschland bzw. Europa identifiziert. Ich möchte auch noch mal den Akzent darauf legen, dass wir natürlich dort als Gesetzgeber eventuell vor allen Dingen im vergaberechtlichen Bereich was tun könnten, weil die IT-Beschaffung der öffentlichen Hand in der Tat ein relevanter Markt aus meiner Sicht ist. Ich meine, es ist ja kein Zufall, dass unsere öffentlichen Nachfrager, wenn man so will, IT-Dienstleistungen und IT-Produkte sich beschaffen auch vor allen Dingen von amerikanischen Anbietern, US-amerikanischen Anbietern. Ich unterstelle ja da jetzt nicht irgendwelche Verschwörungen, sondern das hat eben im gegenwärtigen Vergaberecht seine Gründe. Sehen Sie eventuell eine Gefahr darin, wenn wir mit unseren Standards so hoch gehen, zum Beispiel über das Vergaberecht, dass es am Ende vielleicht gar keine Anbieter mehr geben könnte, also dass wir sozusagen in so eine Art Henne-Ei-Dilemma kommen könnten? Da würde ich gerne eine Einschätzung von Ihnen bekommen, weil das ist ja ein strategisches Ziel, wie wir das lösen könnten.

Und eine Einschätzung hätte ich auch noch mal ganz gerne von Ihnen in Bezug auf die ja von Ihnen als sehr wichtig oder als eine Säule erkannte Peer-to-Peer-Verschlüsselung, die ja sehr oft, ich sage mal, an fehlendem Know-how oder vielleicht auch an fehlender Disziplin scheitert, aber vielleicht auch an fehlender Usability, also dass wir einfach noch nicht so die Produkte haben, die am Ende aller Tage es dem Nutzer wirklich einfach machen, im Alltag so

etwas umzusetzen. Wie bewerten Sie da die Entwicklungen derzeit, und besteht dort Nachholbedarf?

Ich möchte noch einmal zu sprechen kommen auf die Rolle der großen IT- und Internetkonzerne der Vereinigten Staaten mit den dortigen Geheimdiensten. Wenn ich mit denen spreche, sagen die: Na ja, die Anfragen, diese individualisierten Anfragen, die wir eigentlich von allen Geheimdiensten weltweit irgendwie erhalten und von allen Sicherheitsbehörden, die finden sich in sogenannten „transparency reports“, die kann man lesen. Da wird nicht Ross und Reiter genannt, aber wir haben Statistiken, wie viele Informationen wir an welche Dienste in welchen Ländern wie oft geben. Ich sage mal: Das ist sicherlich aus meiner Sicht - und da würde ich Sie bitten, eine Einschätzung abzugeben, ob wir da richtig liegen - nur die unterste Stufe. Es gibt auf der zweiten Stufe offensichtlich eine strukturelle Zusammenarbeit dieser Firmen mit Geheimdiensten, die auch allesamt durch entsprechende Geheimhaltungsvereinbarungen begleitet sind, sodass wir offiziell auch in diesen Transparency Reports darüber nichts lesen.

Ich glaube, es gibt jetzt sogar noch eine dritte Stufe, die darüber hinaus geht, und das war auch der Grund, warum sich diese Firmen empört an das Weiße Haus gewandt haben. Sie haben festgestellt, dass sie zusätzlich noch gegebenenfalls auch Opfer von Attacken werden. Diese Nachrichten, die uns da erreicht haben, da hätte ich auch gerne von Ihnen noch mal eine Einschätzung, ob diese Darstellung plausibel ist oder ob das nicht vielleicht doch auch ein Stück weit eine Inszenierung sein kann, eine inszenierte Empörung.

Ich würde ganz gerne auch noch mal einen Akzent setzen auf das Thema Wirtschaftsspionage. Wir haben von den Vereinigten Staaten gehört, dass das, was man dort tut, allein sicherheitsrechtlich motiviert sei, nicht sozusagen diene, um irgendwelche Betriebs-, Geschäftsgeheimnisse oder Sonstiges auszuspähen. Ich sage halt: Allein mir fehlt der Glaube daran, und ich rede jetzt auch wieder nicht von Russland oder China. Da würde mich mal wirklich interessieren, ob es Erkenntnisse bei Ihnen gibt, dass tatsächlich auch vonseiten dieser Behörden die Infrastruktur, die dort zur Verfügung steht, entweder direkt oder mittelbar zu Zwecken der Wirtschaftsspionage genutzt wird. Ich meine, dass ist für ein exportorientiertes Land, für Deutschland, besonders wichtig. Wir haben bei uns sehr viele sogenannte Hidden Champions, das sind Firmen, die mit unglaublichen Investitionen im Bereich Forschung und Entwicklung es schaffen, immer wieder ein Stück weit die Nase in ihrem kleinen Stück, wo sie tätig sind, weltweit vorne zu haben, um auch Weltmarktführer zu werden. Wenn diese Investitionen irgendwann nicht mehr in Schutzrechte münden können, weil eben solche Geheimnisse vorher ausspioniert werden, dann ist das eine Achillesferse für unsere deutsche Wirtschaft.

Herzlichen Dank. - Die Kollegin Mittag hat noch eine weitere Frage.

Vorsitzender Dr. Patrick Sensburg: Deswegen gebe ich der Kollegin Mittag das Wort.

Susanne Mittag (SPD): Das ist nett, danke. - Ich habe nur noch eine ergänzende Frage. Wir haben jetzt von der Bevölkerung gesprochen, wo Daten abgefischt werden, von Firmen. Ich habe eine Frage zu Infrastruktur, zu risikobehafteter Infrastruktur, seien es jetzt nun Gasfirmen, seien es jetzt Elektrizitätsfirmen, die auch grenzüberschreitend arbeiten, ob da Kenntnisse bestehen - und die Frage stelle ich an alle drei Sachverständigen -, ob die eben auch zielgerichtet angegangen werden, wenn die Kenntnisse bestehen, mit welcher Zielrichtung, und ob auch Sicherheitsbehörden - jetzt nicht hier im Bundestag; darüber brauchen wir jetzt erst mal nicht mehr zu reden - - aber sagen wir mal auf Landes- oder kommunalen Ebenen, ob da, sagen wir mal, kommunale Strukturen auch irgendwo im Fokus stehen, stehen könnten, um, sagen wir mal, Kenntnisse zu erlangen.

Vorhin hatten Sie noch gesagt - ich weiß jetzt nicht, wer es gewesen ist -, die Umsetzung, sagen wir mal, um eine vergrößerte Sicherheit und rechtliche Bestimmung hinzukriegen - - 10, 15 Jahre, wenn es denn so wäre mit meiner Frage. Was wären denn dann für Möglichkeiten aus der Sicht, sagen wir mal, die ersten Schritte eher umzusetzen und nicht zu sagen: „Wir müssen auf irgendein Ergebnis noch zehn Jahre warten, selbst wenn wir mit der Umsetzung flott anfangen“, aber dass man sagt: „Erste Eckpunkte

kann man ja vermutlich in den ersten ein, zwei, drei Jahren setzen“? Das würde mich schon interessieren. - Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich würde jetzt wieder in der gegenläufigen Reihenfolge beginnen, deswegen mit Ihnen, Herr Rieger. Ich darf Sie um die Beantwortung der Fragen bitten.

Sachverständiger Frank Rieger: Vielen Dank. - Zu den Fragen von Herrn Flisek: die Bewertung der Kapazitätsbegrenzung nach strategischer Fernmeldeüberwachung. Ich halte die, ehrlich gesagt, für Augenwischerei, weil in dem Augenblick, wo man sich anguckt, wie die Kapazitäten sind - und die Definition ist ja nicht „Prozent des Verkehrs“, sondern „Prozent der Kapazitäten“ -, dann sehen wir, dass die deutschen Auslandsverbindungen im Peak maximal zur Hälfte ausgelastet sind. Das heißt also, das ist halt wirklich schon die Spitze, weil jeder vernünftige Telekommunikationskonzern wird spätestens dann Kapazitäten nachbauen, wenn er zwischendurch mal sieht, dass er zwei Drittel Auslastung auf den Fasern hatte. Das heißt also, im Schnitt, also im Tagesschnitt, können die, wenn man jetzt mal Spam und Pornografie abzieht, allen relevanten Verkehr mitlesen; na ja, muss man ja tun, ich meine, das ist wahrscheinlich der uninteressante Teil. Das heißt also, die können im Zweifel allen relevanten Verkehr mitlesen und auswerten. Deswegen halte ich diese Definition für ungeeignet.

Die Frage „Was ist denn eigentlich der Sinn und Zweck von strategischer Fernmeldeüberwachung, und wie ist die dementsprechend auszugestalten?“, ist eine längere Diskussion, die man auch ausführlich führen sollte und möglichst auf der Basis von Fakten, insbesondere was irgendwie den Nutzen angeht. Da sind wahrscheinlich die Mitglieder der G-10-Kommission in einer besseren Position, zu diskutieren, um mal sagen: Was kommt denn da eigentlich raus? Welche Erkenntnisse sind denn daraus zu ziehen? Wie viel Prozent des Verkehrs muss man dafür auswerten? Gibt es möglicherweise bessere Mittel und Wege, zu denselben Erkenntnissen zu gelangen, als jetzt so eine 20-Prozent-plus-Keywords-Regelung? Oder braucht man es möglicherweise gar nicht, weil man sagt: „Okay, da ist sowieso so wenig zu holen, gerade an den deutschen Außenverkehrsstellen, dass man auch darauf verzichten kann“, es sei denn, man braucht es eben als Handelsgut auf dem internationalen Geheimdienstbasar? Was so ein bisschen meine Vermutung ist, ist, dass tatsächlich ein Großteil dieser Überwachungskapazitäten des BND in Deutschland bzw. an deutschen Grenzen halt auch deswegen vorgehalten wird, damit sie was zum Bieten haben und zum Tauschen.

Die effektive Filterung nach, sagen wir mal, deutschen Inhalten ist schwierig, weil, wie Sie richtig sagen, wir sind ein internationales Netz. Wir nutzen internationale Dienste von rings um den Planeten, und deutsche Bürger da rauszuhalten, ist eine hochgradig schwierige Angelegenheit. Das technisch zu lösen, ist vermutlich maximal die Hälfte des Problems, die andere Hälfte ist rechtlich und organisatorisch. Und wie die angesichts der mangelhaften politischen Kontrolle der Dienste zu realisieren ist, weiß ich nicht, kann ich gerade einfach schlicht nicht sagen.

Die technische Frage: Ist Full Take möglich? Wir wissen ja: Tempora, das Programm der Briten, speichert zwischen drei und fünf Tage sämtlichen Internetverkehr, der durch Großbritannien geht, der irgendwie relevant ist, also minus Spam und Pornografie. Die Kapazitäten, die sie da aufgebaut haben, sind jetzt nicht utopisch. Ich habe vor mehreren Jahren mal angefangen, eine Kalkulation zu machen: Was würde es kosten, sämtliche Telefonate in Deutschland zu speichern? Und es sind nur ein paar Millionen pro Jahr.

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

- Ja, Inhaltsdaten. - Also wenn Sie alle Telefonate in Deutschland die ganze Zeit abhören würden, da kommen nur so ein paar Petabyte Daten zusammen. Das heißt also, die Datenmenge wächst zwar jedes Jahr, aber die Speicherkosten fallen dramatisch. Wir sind bei so etwas wie 35 Millionen Euro oder so; das sind dann die reinen Speicherkosten. Das heißt, so ein Full Take ist tatsächlich möglich, was selektive Daten angeht.

Ein Full Take des gesamten Internets zur gesamten Zeit ist momentan, glaube ich, nicht unbedingt für den gesamten Planeten möglich. Aber ich sage mal, es ist auch die Frage, wo man da als Geheimdienst, also als Angreifer, seine Ressourcen investiert, und von einem Full Take von bestimmten Ländern wissen wir, dass der passiert, also auch von Telefonverbindungen, auch von Internetverbindungen. Wir wissen auch, dass einzelne Länder, insbesondere im Nahen Osten, interne Full-Take-Kapazitäten haben. Das heißt, die speichern einfach alles, also komplett einmal alle Telefonate. Die speichern, wer wann welche Webseite besucht hat, die speichern die Inhalte von Kommunikation. Das heißt, es passiert tatsächlich; es ist halt keine Chimäre.

Das Filtern des Heuhaufens ist ein Prozess. Ich versuche mal, den zu erklären. Die Dienste strukturieren ihre Informationen traditionell so in drei Dinge: Das eine ist „data“, das sind die Rohdaten; „informations“ sind destillierte Informationen, aus denen man schon mal Dinge ersehen kann; und Intelligence, das sind Erkenntnisse, die definiert sind als: Da kann man was mit anfangen, da kann man Aktionen draus ableiten. Das kann man sich so vorstellen wie einen mehrstufigen Filterprozess.

Im ersten Schritt werden aus den gesamten Daten zwei Ströme abgeleitet. Der eine sind sogenannte „strong selectors“, das heißt also, Daten, wo man zu Personen, wo man irgendeinen Anhaltspunkt hat: Namen, Orte, Telefonnummern, E-Mail-Adressen, IP-Adressen, irgendetwas. Die werden komplett mitgenommen.

Zum anderen gibt es verhaltensbasierte und stichwortbasierte Ausleitungen, wo man sagt: Leute, die *Spiegel Online* aus Pakistan sich angucken, sind möglicherweise verdächtig, oder Leute, die nach bestimmten Keywords suchen, sind verdächtig, oder Kombinationen von bestimmten technischen Parametern. Also nehmen wir mal an, der benutzt Tor, und von derselben IP-Adresse haben wir E-Mail-Verkehr. Die werden mitgenommen. Das ist halt so ein Filtersystem. Das ist das, was XKeyscore tut. Dafür ist XKeyscore gut. Das ist in der Lage, komplexe Filterkriterien zu definieren und sich auszudenken und die auch weiterzuentwickeln, um aus diesen riesigen Mengen von Metadaten und Full-Take-Daten eine Kombination von Erkenntnissen zu erzielen.

Zwangsläufig haben Sie dabei eine riesige Menge Beifang. Also selbst, wenn Sie sich halt an die rechtlichen Rahmenbedingungen halten würden, haben Sie zwangsläufig dabei eine riesige Menge an „false positives“, die einfach nichts mit dem eigentlichen Ziel der Überwachung zu tun haben.

Vorsitzender Dr. Patrick Sensburg: Darf ich einmal ganz kurz reingehen? Das mache ich sonst nicht, nur des Verständnisses halber, weil Sie auch der Experte sind. XKeyscore: Ich hatte bisher den Eindruck - korrigieren Sie mich -, dass XKeyscore nicht der Staubsauger aus dem Netz ist, sondern das bereits Gespeicherte dementsprechend nach bestimmten Suchmöglichkeiten gefiltert und dann ausgewiesen wird. Bitte erklären Sie es noch mal so, dass wir es detailliert verstehen, nicht dass falsche Eindrücke entstehen. Sie können mich gerne korrigieren, nur dass wir alle hinterher auf dem Stand sind, dass wir auch wissen, was es wirklich macht, weil jetzt hatte ich gerade den Eindruck gewonnen, XKeyscore wäre die Software, die die Daten aus dem Netz punktuell rauszieht. Ich hatte, wie gesagt, bisher das Verständnis, dass ein bestehender Datensatz dann gefiltert wird nach den jeweiligen Suchalternativen, die ich bei XKeyscore nutzen kann. Wenn Sie das noch mal darstellen können? Ich glaube, das ist sinnvoll, dass ich hier nachfrage, damit wir alle die Kenntnisse haben.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Stand auf meinem Zettel!)

Manche haben vielleicht die Erkenntnis, aber mir reicht es, wenn ich hinterher schlau bin.

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

Sachverständiger Frank Rieger: XKeyscore dient tatsächlich der Vereinheitlichung der vielen Datenquellen. In den NSA-Termini gibt es die sogenannten SIGADs. Das sind also die

Anzapfpunkte im Netz, aus denen Daten, also sowohl Full-Take-Daten als auch Metadaten oder was auch immer möglich ist, gewonnen werden, die in große Datenbanken fließen. XKeyscore ist das System, mit dem man Filter auf diese Daten konfigurieren kann, und zwar so, dass man fortan alles, was mit diesen Keywords zu tun hat, bekommt, aber auch, dass man rückwärts gucken kann in die Metadaten, die schon gespeichert sind, und in die kurzzeitig gespeicherten Full-Take-Daten, die da sind, um entsprechend dieser Keywords Sachen zu bekommen.

Wenn Sie sich die User Interfaces angucken, ist es so: Ein Analyst konfiguriert sich da seinen Satz von Filtern und bekommt jeden Morgen in die Inbox oder fortlaufend in die Inbox die Ergebnisse aus diesen Filterungen, und die können, wie gesagt, beliebig komplex sein. Die werden auch tatsächlich **- -** Das ist auch sehr interessant: Diese Filter funktionieren zum einen auf den bereits gespeicherten Metadaten und den Full-Take-Daten, aber werden auch gezielt nach vorne gepusht, dahin, wo die Daten angezapft werden, also um diese Daten höher zu priorisieren. Das heißt also, Daten, die auf XKeyscore-Filterungen matchen, werden dann halt nicht mehr weggeworfen. Das ist auch ein wichtiger Punkt. Die landen dann halt immer in den Archiven. Das heißt, XKeyscore ist tatsächlich die Filterschicht über den vielen verschiedenen Anzapfstellen, die aus verschiedensten Quellen die Daten in die Datenbanken bringen. Soweit verständlich?

Vorsitzender Dr. Patrick Sensburg: Aber greift auf die Datenbank zu als Algorithmus quasi, was es aus der Datenbank in dem Moment abgezapft hat? Also, es kann nicht das Netz durchsuchen, sondern es durchsucht die angezapften Daten an den verschiedenen Anzapfpunkten durch? Es geht mir jetzt nur um das technische Verständnis.

Sachverständiger Frank Rieger: Ich versuche, es mal so zu erklären. Sie haben zum einen so was wie einen Zwischenspeicher - das ist so was wie Tempora -, wo Sie halt das Internet für drei bis fünf Tage einfach zwischenspeichern. Sie haben zum anderen Metadatenspeicher - da gibt es verschiedene Codenamen -, wo halt gespeichert wird, wer wann kommuniziert mit wem. Und dann haben Sie die Anzapfstellen, die den Live-Verkehr durchsuchen. Und XKeyscore kann eben all diese Dinge auf einmal benutzen.

Das können Sie sich so vorstellen: Die strategische Fernmeldeüberwachung des BND filtert ja nach bestimmten Stichworten, oder es sind nicht nur einfache Stichworte, sondern halt komplexere Ausdrücke. Die können Sie mit so was wie XKeyscore konfigurieren, Sie können aber auch gleichzeitig sehen, welche schon passenden Sachen haben wir schon in den Datenbanken dazu. Es kann sozusagen beides. Die Macht dieses Werkzeuges liegt eben darin, dass es eben nicht nur auf einer Datenbank sucht, sondern eben auf allem, was die NSA hat an der Stelle.

Vorsitzender Dr. Patrick Sensburg: Danke.

Sachverständiger Frank Rieger: Diese Filterung des Heuhaufens hat am Ende immer wieder das Ziel, dass man einzelne Personen identifiziert. Es geht immer um Menschen, also darum, dass man Leute identifiziert und die wiederum dann mit so einer Art Strong Selectors versieht, das heißt also, dafür sorgt, dass deren Daten, deren Kommunikation immer komplett mitgeschnitten wird, wenn die als interessant identifiziert wurden - das ist das Ende sozusagen des Filtertrichters so ein bisschen -, und von denen halt vor allen Dingen auch Lebensprofile erstellt werden können. Darum geht es vor allen Dingen bei der Metadatenspeicherung. Das ist ganz wichtig.

Die Metadaten - das ist vielleicht so ein bisschen untergegangen heute - sind deswegen so wichtig, weil man sie automatisiert verarbeiten kann. Die muss sich niemand anhören, die muss niemand per Hand auswerten, sondern die können halt automatisch zu Lebensprofilen, zu Aufenthaltswahrscheinlichkeiten - - Eines dieser Programme war zum Beispiel Co-Traveler, wo sie versucht haben, anhand der Metadaten festzustellen, wer reist mit wem, also teilweise sehr intime Details.

Nächste Frage von Herrn Flisek war: Können wir denn eigentlich einen Markt schaffen, also zum Beispiel mit dem IT-Vergaberecht? Was sind eigentlich die Probleme mit den Dienstleistern, die wir insbesondere aus den USA haben? Ich denke schon, dass es geht. Wir können sicherlich mit einer Steuerung der öffentlichen

Vergabepolitik schon deutsche Dienstleister bevorzugen, und wir sind durchaus auch in der Lage, mit dem doch relativ substanziellen öffentlichen IT-Markt auch deutsche Dienstleister, sagen wir mal, ein bisschen aufzupäppeln. Wie das europarechtlich funktioniert, weiß ich nicht. Ist nicht mein Expertisengebiet.

Sagen wir mal, rein technisch ist es schon so, dass die Fragen „Welche IT-Aufträge müssen denn zwingend extern verarbeitet werden? Wie viel Outsourcing muss denn eigentlich sein in den Behörden? Ist es nicht möglicherweise notwendig, auch mal wieder eigene IT-Kompetenzen in Behörden aufzubauen?“ aus meiner Sicht klar zu beantworten sind. So viel wie möglich sollte intern passieren. Ich vertraue einem deutschen Beamten deutlich mehr als einem angeheuerten amerikanischen IT-Consultant. Ganz einfach.

Wir haben die Kompetenzen an unseren Unis. Warum sollen deutsche Behörden nicht auch in der Lage sein, ihre eigenen Softwarebedürfnisse sinnvoll zu erfüllen? Man kann aus den Fehlern der Vergangenheit, also den fehlgeschlagenen Projekten, da durchaus lernen, indem man halt lernt, dass man nicht nur Informatiker braucht, sondern auch Manager, die in der Lage sind, solche Softwareprojekte tatsächlich qualifiziert zu managen. Aber ich sehe da keine ernsthaften Hinderungsgründe, das zu tun.

Was jetzt die Frage des Henne-Ei-Dilemmas angeht: Kriegen wir denn überhaupt die Kompetenz hin kurzfristig? Können wir denn amerikanische Dienstleister rausschmeißen aus den deutschen Behördenausschreibungen? Weiß ich nicht. Das wird wahrscheinlich schwierig, das wird ein längerer Prozess. Ich sehe den gesamten Komplex eben tatsächlich eher mittelfristig so. Drei bis fünf Jahre werden wir wohl brauchen. Aber wenn man das Ziel hat, dann sollte man heute damit anfangen.

Zur Frage Ende-zu-Ende-Verschlüsselung, Usability: Ich bin in meiner professionellen Tätigkeit - der CCC ist ja nur mein Hobby sozusagen - seit vielen Jahren in diesem Markt tätig und weiß auch, was Nutzer da für Probleme aufwerfen. Aber wir sehen, dass Ende-zu-Ende-Verschlüsselung funktionieren kann. Also, Skype zum Beispiel wäre, wenn es nicht Hintertüren hätte, eine gute Ende-zu-Ende-verschlüsselte Software. Man könnte Skype mit minimalen Änderungen dazu bringen, dass es eine sichere Ende-zu-Ende-Kommunikation ermöglicht. Die ursprüngliche Skype-Software ganz am Anfang tat das tatsächlich auch mal; es wurde dann halt nur mit Hintertüren versehen.

Sie alle haben wahrscheinlich Skype schon mal benutzt. Ich würde nicht sagen, dass es schwierig zu benutzen ist. Daran kann man sehen, dass tatsächlich sichere Ende-zu-Ende-Verschlüsselung für Consumer, also für normale Nutzer, möglich ist, wenn man halt nur genügend Aufwand da reinsteckt. Da sehe ich eigentlich jetzt auch nicht so viele Probleme, dass wir das in Deutschland nicht können. Wir haben gute Leute an den Universitäten, wir haben gute Leute in Unternehmen. Es fehlt da tatsächlich nur an den Rahmenbedingungen, was Finanzierung angeht, was Wagniskapital angeht, was die Erleichterung von Bedingungen für solche Unternehmen angeht; aber machbar ist das allemal.

Die Kooperation der Firmen mit den Diensten, also sagen wir mal Facebook und ähnliche. Sie haben die Struktur - gezielte Anfragen, strukturelle Zusammenarbeit und am Ende Angriffe gegen diese Unternehmen - richtig zusammengefasst. Was ich weiß, ist, dass zumindest bei Google die Aufregung da groß war, als die verstanden haben, dass die NSA sie auch direkt angegriffen hat und nicht nur über Kooperation gearbeitet hat, sondern eben auch die Leitungen zwischen den Data Centers angegriffen hat und ähnliche Dinge. Das hat denen so gar nicht gefallen. Diese Unternehmen haben alle den Anspruch, Kontrolle über ihre Daten zu haben. Das Prinzip heißt: „no one but us“, also: niemand außer uns. Das verfolgt auch Facebook. Das heißt, die wollen die vollständige Kontrolle über diese Daten haben und versuchen da auch irgendwie, was zu tun. Die haben allerdings das strukturelle Problem, dass gerade in den Boards und den Managementetagen, insbesondere in amerikanischen Firmen, viele Ex-Mitarbeiter von Geheimdiensten sitzen, die noch für ihre alten Kumpels arbeiten.

Dieses Prinzip ist eben auch genau bei der Wirtschaftsspionage zu finden. Also, die Amerikaner - aus dem, was wir aus den Dokumenten wissen oder sonst beobachten können - versuchen, ihre Wirtschaftsspionage

immer rechtlich zu legitimieren, indem sie sagen: „Okay, wir machen keine Wirtschaftsspionage zum Vorteil von einzelnen Unternehmen, sondern wir sorgen für Ausschreibungsgerechtigkeit“, oder: „Wir verfolgen Steuerhinterziehung“, oder: „Wir suchen nach Firmen, die halt Embargobrüche begangen haben“, und erheben diese Daten über Unternehmen, zum Beispiel auch in Deutschland, unter diesem Vorwand.

Die Frage, wie die dann halt zu den Konkurrenzunternehmen, zum Beispiel in den USA oder gerade in Großbritannien oder Australien gelangen, klärt sich eben genau wiederum über dieses Drehtürprinzip, dass halt eine Menge Ex-Mitarbeiter von solchen Diensten in diesen Unternehmen sind, und auf dem kleinen Dienstweg passiert dann halt da die Übermittlung. Das funktioniert so ähnlich wie - - Wenn Sie sich heute die Sicherheitsbeauftragten der DAX-Unternehmen angucken, die haben alle mal beim BKA gearbeitet. Und genauso funktioniert da halt eben auch die Übermittlung von Erkenntnissen aus den Diensten in die Unternehmen.

Noch zu den kurzen Fragen von Frau Mittag. Risikobehaftete Infrastrukturen: Wir sehen immer mehr Angriffsversuche auf solche Infrastrukturen. Vorgestern hat F-Secure einen Trojaner gefunden, der gezielt versucht, in Industriesteueranlagen einzudringen und Erkenntnisse aus diesen Industriesteueranlagen nach außen zu übermitteln. Das heißt also, der enthält keine Sabotagekomponente, sondern nur ein Was-ist-denn-da-eigentlich-los. Die große Frage ist: Ist es Industriespionage, weil die wissen wollen, wie industrielle Prozesse funktionieren - gerade zum Beispiel im chemischen Bereich ist es ein Betriebsgeheimnis, wie die Detailsteuerung eines Prozesses funktioniert, was irgendwie auch viel Geld wert ist -, oder handelt es sich dabei um die Vorbereitung eines Sabotageangriffs oder eines großflächigen Sabotageangriffs? Das lässt sich aus dem Code des Trojaners nicht ohne Weiteres ersehen. Also man kann da nur spekulieren. Beides ist möglich.

Wir wissen, dass gerade im Bereich Sabotage und Vorbereitung von Sabotage - da gab es mal dieses schöne Stichwort Cyberwar - solche Systeme installiert werden. Stuxnet war ein Beispiel, Flame und andere, von denen Sie bestimmt gehört haben. Das heißt also, diese Vorbereitungen finden statt und vermutlich eben nicht nur durch die Amerikaner und nicht nur gezielt in Ländern, die sie gerade nicht mögen. Insofern würde ich da von einer relativ großen Wahrscheinlichkeit sprechen, dass solche Risiken da vorhanden sind und dass die Möglichkeit, solche Eingriffe vorzunehmen, möglicherweise vielleicht nicht durch die NSA, aber sicherlich durch andere Nationen, gegeben ist. Wir sollten da eine Menge tun.

Zum Beispiel eines der Dinge, die wir im Rahmen so einer europäischen Initiative zur Informationssouveränität tun sollten, wäre, einen sicheren Microcontroller zu entwickeln, also einen sicheren Prozessor zu entwickeln für Industriesteuerung. Das ist einfach, das können wir tun, dafür sind die Kapazitäten da. Wir haben die Möglichkeiten in Europa. Es ist nicht so teuer, wie einen Prozessor zu entwickeln für ein Telefon zum Beispiel, sondern viel einfacher. Man kann es relativ einfach sichern, und wir hätten damit einen großen strategischen Vorteil gegen solche Infrastrukturangriffe. Sollte man auf jeden Fall erwägen.

Zur abschließenden Frage: Was wären so die ersten Schritte in einem langfristigen Programm? Sicherlich gehört dazu, einen kritischen Blick auf die jetzigen Infrastrukturen zu werfen, auf die Dienstleister zu werfen, auf die Frage, welche Daten denn die Kronjuwelen sind, also wo man denn seine Schutzanstrengungen konzentrieren sollte, weil wir können nicht alles schützen; das ist schon ganz klar. Das ist auch das, was ich Unternehmen zum Beispiel rate, wenn die mich fragen: Was soll ich denn jetzt eigentlich tun? Dann sage ich: Gucken Sie, welche Daten sind die Daten, ohne die Sie wirklich nicht können, also die Daten, die wirklich kritisch sind. Dazu gehört sicherlich im öffentlichen Bereich die kritische Infrastruktur im Daseinsvorsorgebereich, nicht nur die Sicherheitsbehörden. Die Konzentration auf diese Bereiche plus die Entwicklung langfristiger Perspektiven muss beides passieren.

Das können Sie sich ungefähr so vorstellen: Wenn die IT-Security ein Druckwasserrohr wäre, dann spritzt es da gerade an allen Ecken und Enden raus, und wir werden zehn Jahre brauchen, ein neues Druckwasserrohr zu bauen. So lange

müssen wir da Heftpflaster draufkleben. Und worüber wir uns halt viel streiten, ist, welche Farbe gerade das Heftpflaster haben soll. Aber wir können nicht aufhören, die zu kleben - logischerweise nicht, weil sonst haben wir gar kein Wasserrohr -, bis wir halt ein neues Rohr gebaut haben. Und in der Situation sind wir da gerade.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich darf Ihnen, Herr Dr. Gaycken, als Nächstem das Wort geben.

Sachverständiger Dr. Sandro Gaycken: Vielen Dank. - Herr Flisek, zu Ihrer Frage: die rechtlichen Vorgaben für die Nachrichtendienste, ob das dann auch taktisch funktioniert. Diese Vorgabe mit dieser Kapazitätsbegrenzung hat mich, ehrlich gesagt, gewundert, weil das sagt ja überhaupt gar nichts über die Qualität, die Art der Daten aus und warum ausgerechnet 20 Prozent und nicht 50 oder 5. Also, ich fand, das war so ein bisschen ein Indikator für so eine typische desinteressierte Wischiwaschi-Regulierung, die dann halt eben natürlich auch von den Diensten schwierig zu handhaben ist. Die Dienste hätten natürlich gerne härtere, klare und eindeutige Vorgaben dafür, wie sie damit umgehen können; denn die sind natürlich auch nicht gerne im „limelight“ irgendwelcher Untersuchungsausschüsse, wo sie sich dann für irgendwelche Sachen rechtfertigen müssen, die sie eigentlich gar nicht falsch machen wollten.

Von daher kann ich hier nur wiederholen: Man muss sich da wirklich sehr intensiv mit dem Nachrichtendienstgeschäft neu befassen. Man muss genau ansehen, was diese neuen Möglichkeiten und Mittel sind. Viele von denen sind sicherlich auch für sehr viele Dinge sehr sinnvoll, aber man muss genau wissen, was man will und was das im Einzelnen bedeutet, was die Dienste tun und wo die Rahmenbedingungen sind, wie man die genau feststeckt. Und das muss eben gerade nicht so grob sein: „Ja, nimm mal hier 20 Prozent davon, und dann ist schon okay“, sondern es muss sehr feingranular sein, mit hoher Expertise beschlossen werden und auch mit hoher Agilität begleitet werden. Dadurch, dass sich das immer wieder ändert, dadurch, dass die IT sich viel ändert, neue Akteure dazukommen usw., muss da immer konstant draufgesehen und nachgebessert werden, und dann ist es, glaube ich, auch ein Werkzeug, das man ganz gut regulieren und gezielt einsetzen kann. Das wäre dem BND übrigens auch sehr recht, das so zu haben. Denn dann hätte man natürlich auch eine größere Handlungssicherheit in dem, was man da tut.

Dazu gehört dann übrigens auch die Frage des Ausbaus zur Aufklärung. Auch da müssen wir sagen - das kann man vielleicht auch mal in diesem Kontext sagen -: Wir reden ja eher über die Kontrolle und den Abbau der Nachrichtendienste, aber es ist natürlich auch gerade in diesem anderen Bereich, in dem ich noch tätig bin, Cyberspionage und Cyberwar, interessant, mehr über die Akteure zu erfahren, die da eine Rolle spielen, und was die da machen. Da sind wir immer noch sehr unterinformiert. Wir wissen nicht viel darüber. Da wäre dann natürlich auch eine Frage, ob wir da nicht ein paar gezielte Fähigkeiten zum Aufbau anstellen müssen, um dann beispielsweise mehr über Russland oder China aufzuklären, was da eigentlich läuft.

Dann die Frage mit dem Full Take. Ich glaube, die hat Frank schon ganz gut beantwortet. Darauf möchte ich jetzt nicht eingehen.

Die andere Frage mit Vergaberechten ist natürlich sehr interessant. In den USA gab es die Situation, da hatte das Pentagon auch mal überlegt, ob die von „commercial off-the-shelf IT“ zu „military off-the-shelf IT“ übergehen, dass die also sagen: Okay, wir kaufen jetzt hier nicht mehr diesen ganzen Windows/Intel-Kram, sondern wir lassen uns eigene Computer bauen usw. - Wenn sie es neu bauen wollten, wäre das relativ teuer gewesen, deswegen haben sie überlegt, ob sie einfach hohe Standards bei den normalen IT-Suppliern einziehen können, und da haben die dann gesagt: Hör mal, dass ihr hier von uns - Microsoft, Intel, Cisco usw. - sichere IT haben wollt, das ist uns zu blöd und zu teuer und zu umständlich, und ihr seid ein viel zu kleiner Markt, als dass wir das machen wollen. Von daher würden wir uns dann einfach zurückziehen. - Da hat das Pentagon dann entschieden, dass sie sich das dann nicht leisten können. Also genau diese Situation, wenn man die Standards sehr hoch setzt, dass sich dann die potenziellen Hersteller zurückziehen, hatten die.

Aber man kann es natürlich dann halt eben auch kombinieren, wenn man wie jetzt eine

Marktsituation hat, die sich grundlegend verändert hat, wo also durchaus ein nationaler und ein internationaler Bedarf ist und auch ein ziviler Bedarf besteht an Hochsicherheits-IT, dass man das so konzipiert, dass man die Produkte, die da entwickelt werden, beispielsweise für den Verteidiger, der das ganz, ganz dringend braucht, und dann die Basistechnologien so baut und gestaltet, dass die also auch einen Dual Use haben für zivile Kontexte, kritische Infrastrukturen zum Beispiel. Das wäre auch überhaupt nicht problematisch, die Kernkomponenten so zu bauen, und dann hat man automatisch eine sehr hohe Skalierung und hat also über das Vergaberecht dem Markt in die Schuhe geholfen.

Das wäre also auf jeden Fall sehr wünschenswert, denn die Bundeswehr zum Beispiel muss sowieso sichere IT haben. Zumindest überall da, wo eine Waffe dranhängt oder eine militärische Fähigkeit, möchte ich eine IT, die nicht nur gegen Skriptkiddies sicher ist, also gegen irgendwelche Teilzeitprogrammierer, sondern gegen NSA, FSB, PLA usw., sonst kann ich mir die Bundeswehr auch schenken. Dann brauche ich die gar nicht mehr. Von daher brauchen die das sowieso. Das dann mit diesem Gedanken des Dual Use aufzubauen, damit man dann gleich eine Industrie damit hochzieht, das wäre da, glaube ich, der richtige Weg, und dann kriegt man auch Hersteller mit ins Boot.

Zum Thema Usability: Das ist auch was, was mich immer ein bisschen nervt. Also, was wir sehr oft hören schon seit Jahren in dieser Diskussion über IT-Sicherheit, wenn wir mit Unternehmen diskutieren, deren IT grundlegend unsicher ist, dann sagen die immer gerne: Ja, der Nutzer ist ja schuld. Der hat das irgendwie falsch abgelegt, der hat dies nicht gemacht und das nicht gemacht. - Aber die Praxis zeigt einfach: Dass das in der Masse passiert, andauernd passiert, dass die Nutzer diese Passwortkultur nicht beherrschen - das Key-Management ist schlecht - und diese ganzen zusätzlichen Sicherheitsmaßnahmen nicht so richtig benutzen können, das ist ja eher ein Indikator dafür, dass das schlecht entwickelt ist und schlecht konzipiert ist und nicht, dass die Nutzer zu blöd sind.

Eine Technologie muss so gebaut sein, dass der, der das Ding benutzen soll und sicherheitssensibel und richtig benutzen soll, das auch ohne Probleme so benutzen kann. Und in der Wirtschaft zum Beispiel genauso wie auch bei der Bundeswehr usw. sind das halt Leute, die haben andere Aufgaben, die sollen sich nicht die Hälfte ihrer Zeit mit IT-Sicherheit beschäftigen, die sind unter Umständen gelangweilt, desinteressiert und inkompetent, aber die müssen das immer noch fehlerfrei benutzen können. Das müssen wir als Entwicklungsaufgabe in diese Industrie reinbringen. Das muss auf diesem Level nutzbar sein.

Am liebsten wäre mir überhaupt, wenn der Nutzer, soweit wie möglich, von sicherheitskritischen Entscheidungen isoliert wird. Warum soll jemand, der ganz am Ende der Kette sozusagen ist, der am wenigsten Einfluss auf dieses gesamte System hat, warum soll der die zentrale Verantwortlichkeit und Schuldigkeit für die Sicherheit tragen? Das kann man architektonisch ganz anders machen, in der Entwicklung ganz anders machen. Das hat die Industrie nur nie gemacht. Deswegen redet die nicht gerne darüber und gibt lieber dem da hinten am anderen Ende die Schuld. Aber das ist keine gute Praxis.

Zur Zusammenarbeit der US-Firmen mit NSA, Pentagon usw.: Da gibt es eine Reihe von Problemen. Frank hat es schon genannt, die Revolving Door, also dass da viel Austausch ist zwischen Industrie und Sicherheitsbehörden an einigen Stellen. Das sehen wir also andauernd, dass da die Leiter der Abteilung mal hier sind zwei Jahre, dann sind sie mal in der Firma zwei Jahre, dann wieder bei der NSA zwei Jahre. Das gibt es relativ häufig, und da gibt es natürlich so einen relativ starken Fluss von Informationen, der da hin und her geht. Trotzdem müssen wir sagen, dass natürlich die großen IT-Firmen diese Kooperation nicht mögen. Also Microsoft ist absolut sonnenklar: Wenn da irgendwie rauskommt, dass die Hintertüren für die NSA einbauen, dann kollabiert für die der globale Markt. Das gilt für ganz viele IT-Unternehmen, und deswegen wollen die das natürlich auf Teufel komm raus nicht.

Das ist nicht so, dass das ein sehr freundliches und zuvorkommendes Verhältnis wäre. Das Verhältnis zwischen den Firmen und der Regierung, der Administration ist sehr gespannt. Wir merken das auch immer wieder, dass die sich da also

sehr vehement bekriegen und jetzt natürlich noch umso mehr sich beschweren, wo die Firmen sagen: Seht ihr, wir haben euch gesagt, es kommt raus. Jetzt stehen wir blöd da. Ihr verliert euer Geld usw. - Das ist also ein sehr angespanntes Verhältnis.

Da kann man auch ansetzen. Wir haben sozusagen viele der US-IT-Firmen auch als potenzielle Alliierte gegen diesen Überwachungswahn. Die möchten das auch nicht, aber möchten das natürlich nur aus kommerziellen Gründen nicht, und bei denen steht natürlich immer noch das Problem, dass die die Daten trotzdem überwachen und abgreifen und kommerziell verwenden. Das ist noch einmal eine andere Problematik. Aber die haben zumindest auch eine sehr kritische Haltung gegen die NSA.

Anders ist das aber bei IT-Sicherheitsfirmen und Sicherheitsfirmen. Die haben natürlich eine sehr enge Berührung zur Administration, arbeiten sehr viel und kriegen sehr viel Geld aus der Administration. Die Firma RSA zum Beispiel ist eine Firma, eine der großen IT-Sicherheitsfirmen in den USA, die auch übrigens den technischen Backbone großer deutscher IT-Sicherheitsproduktketten bildet, und die sind ein ganz bekannter Partner der NSA, die auch angeblich Geld genommen haben, um Crypto-Standards aufzuweichen in ihren eigenen Produkten, die sie dann exportieren. Da ist also die Kooperation sehr viel williger und sehr viel intensiver und auch der Kontakt sehr viel besser zu den Behörden. Von daher müssen wir also gerade gegenüber solchen Produkten und solchen Firmen doch noch mal sehr kritisch sein, wenn es darum geht, die hier zu implementieren.

Da würde ich auch raten, bei den deutschen IT-Sicherheitsanbietern, die dann hier so mit „Made in Germany“ rumspringen, aber in Wirklichkeit RSA-Produkte verkaufen, doch noch mal ein bisschen kritisch nachzufragen und den Hebel vorzuschieben, dass die also nicht solche Produkte von wissentlichen NSA-Kollaborateuren dann in kritische Infrastrukturen verbauen und so tun, als wäre das in Deutschland passiert.

Wirtschaftsspionage. Machen das die USA? Die USA machen das - - Also, das ist natürlich - - Da kann man nicht so viel drüber sagen.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Kennt man schon!)

- Ja, ich muss jetzt ein bisschen vorsichtig sein, was ich sagen kann und so. - Was wir hören, das sind halt auch nur Gerüchte. Was wir hören, ist halt natürlich, dass wir auch schon mal die Amerikaner erwischen, hier und da. Das sind dann aber auch vor allem solche Sachen wie Rüstungsprojekte, strategische Rüstungsprojekte, und da ist sozusagen ein automatischer Overlap aus diesem Bereich Industriespionage, aber auch strategische Spionage, die ja sozusagen legitim ist. Also, die wollen sozusagen - - Wenn wir einen Panzerdeal machen mit den Russen, dann rufen die uns zwar an und fragen: „Was macht ihr denn da mit den Russen?“, und dann sagen wir denen das, und dann ist das eigentlich auch okay. Aber man guckt dann doch trotzdem noch mal gerne nach bei dem Panzerhersteller, ob das auch stimmt mit den Stückzahlen und den Spezifikationen, einfach nur, um das strategisch bewerten zu können.

Es heißt dann immer von der CIA, dass diese Informationen nicht in die Wirtschaft gegeben werden. Die machen das, die gucken auch bei den Rüstern nach, die gucken auch bei wichtigen interessanten Projekten nach, sagen aber ganz klar und eindeutig, dass sie das nie weitergeben an ihre eigene Industrie. Das können wir aber nicht verifizieren, ob das so ist oder nicht. Andererseits ist das aber auch, glaube ich, gar nicht so wichtig. Denn wir haben natürlich eine ganze Bandbreite und Palette von Wirtschaftsspionen, Industriespionen, die an unsere Unternehmen rangehen, in unsere Produkte reingehen, auch in Europa und vor allem im Osten. Von daher ist das Problem sowieso virulent, und wir müssen uns um einen Schutz unserer Wirtschaft und des Know-how kümmern, egal ob die USA das jetzt machen oder nicht, weil genug andere machen das sowieso.

Dann noch zu den Fragen von Frau Mittag: Bei den kritischen Infrastrukturen gibt es im Moment noch nicht ein so hohes Interesse, die anzugreifen. Die Nachrichtendienste bauen Angriffe für die vor, implementieren die aber noch nicht, weil man diese Angriffe natürlich nicht entdeckt haben möchte frühzeitig. Von daher gibt es Angriffe im Schrank sozusagen, die

man auch relativ schnell ins Ziel bringen kann. Aber die da jetzt vorzuhalten und die warten zu müssen, obwohl man die gar nicht braucht, erhöht das Risiko der Detektion, und dadurch gehen die Kosten in die Höhe, wenn man es wieder neu entwickeln muss. Deswegen: Die gibt es, aber die gibt es noch nicht vor Ort, und für Kriminelle gibt es da natürlich keine richtigen Geschäftsmodelle. Da gab es zwar Erpressungsversuche, aber die waren nicht sehr erfolgreich. Von daher ist es nicht so richtig interessant für die.

Wir müssen trotzdem mit den Betreibern von kritischer Infrastruktur sprechen. Die sagen natürlich immer: Na ja, hier passiert doch kaum was. Ist doch schon immer gut gegangen. - Aber es gibt das Interesse, und es gibt die Möglichkeiten, und da müssen die sich natürlich auch drauf einrichten, dass das ein Risiko ist.

Sicherheitsbehörden werden sehr gerne angegriffen, und zwar vor allem von organisierter Kriminalität. Es gibt sehr, sehr viele Geschichten inzwischen, unschöne Geschichten, wo also zum Beispiel Zeugen verschwunden sind, und dann hat sich herausgestellt, der Server vom Zeugenschutzprogramm war gehackt - in einem anderen Land, nicht bei uns -, oder andere solcher Geschichten. Natürlich haben gerade die organisierten Kriminellen ein sehr hohes Interesse, bei den Polizeien einzubrechen - teilweise auch, bei den Diensten einzubrechen - und da nachzugucken, was über sie vorliegt, eventuell auch mal, rauszufinden, welche Namen da interessant sind, und solche Dinge. Da besteht auch hoher Bedarf, da nachzubessern; denn die sind natürlich auch mit ihrer IT-Sicherheit - - geben sich schon Mühe und die machen Entnetzung im Sinne von Air Gaps, dass die diese Sachen zumindest nicht am Internet haben; aber es gibt dann immer noch implizite Übergänge und solche Dinge. Da muss man also unter Umständen auch noch mal nachbessern und gucken, wie hoch da die Sicherheit ist und wie hoch sie sein muss.

Dann zum Schluss noch die mittelfristige Umsetzung von besserer IT-Sicherheit oder IT-Hochsicherheit. Da habe ich einen Plan. Also, da gibt es verschiedene Dinge, die man tun kann. Das erste wichtige wäre, dass man die aktuellen Fehlpfade ausbremst, also keine großen Investitionen in irgendwelche Flickschustertechnologien jetzt unternimmt, wo man hier was ausgibt, da was ausgibt, da was ausgibt. Das führt nur dazu, dass die Ressourcen verschwendet sind. Man weiß aber im Moment noch nichts Genaues über die Effizienz dieser Ansätze. Wir brauchen also erst systematische Kenntnis über die Effizienz dieser Ansätze, und zwar in Bezug auf die Effizienz der spezifischen Sicherheitsversprechen als auch in Bezug auf die Effizienz der Gesamtwirkung der Sicherheit auf das System. Das würde ich also da zurückstellen und da Geld sparen - ist ja auch schön.

Ein Punkt, wo man, glaube ich, am ehesten ansetzen kann im Moment, ist die aktuell anfangende Revolution der Industrie 4.0, dass man da also sagt: Wenn wir jetzt anfangen, die ganze Industrie und auch unsere ganzen Autos und Flugzeuge sehr viel stärker zu informatisieren als vorher, dann wäre das doch eigentlich, gerade weil es auch neu losgeht, eine gute Idee, da auch mit neuen Technologien ranzugehen. Da gibt es auch großes Interesse in der Großindustrie, bei den Maschinenbauern. Ich habe da schon relativ viele Gespräche - - Die sind auch schon ein bisschen weiter in Richtung Implementierung. Die möchten allerdings noch nicht mit dem Bundestag darüber reden. Da müssen wir vielleicht noch mal einen Weg finden, wie der Bundestag auch hilfreich sein kann und nicht als große Bedrohung wahrgenommen wird für so was: dass da irgendwelche komischen Regulierungen kommen, die sie dann ausbremsen im Vergleich zu den Chinesen usw.

Aber eine Idee, wie man das machen könnte, wäre vielleicht, in kleinen Stufen anzufangen, dass man also der Industrie jetzt nicht sagt: „Ihr müsst die gesamte Industrie 4.0 abbremsen und erst mal warten“, sondern denen sagt: Ihr könnt das ruhig machen, prescht voran; aber wir suchen uns so ein paar sehr kritische Teilkomponenten wie beispielsweise für Kernkraftwerke oder für Flugzeuge - wo hohe Safety-Anforderungen sind und die auch gut skalierbar sind in andere Technologien - und die nehmen wir uns mal raus und die machen wir jetzt mal hochsicher. - Da gibt es ein hohes Interesse auch in der Großindustrie, hatte ich gesagt. Wenn man denen dann ein bisschen Signale sendet, dass das auch gewollt ist und dass das auch standardisiert wird später, wenn

man sehr viel sicherere Technologie hat, dass das auch in den Markt gebracht wird, dann werden die das durchaus machen und werden auch hohe Millionenbeträge, mehrstellige Millionenbeträge, dafür investieren. Das wäre also so was, was man sozusagen nur abholen müsste in Gesprächen.

Man muss sich dann natürlich, hatte ich schon erwähnt, auch parallel darum kümmern, dass das relativ breit passiert; also eine maximale Skalierung - mindestens im europäischen Markt, aber auch in vielen anderen Exportmärkten - wäre sinnvoll. Von daher: Diese Standardisierungen sollten in den internationalen Standardisierungsgremien gleich mit angesprochen werden. Das ist auch sehr wichtig, nicht nur in Deutschland. Die sind im Moment auch sehr massiv belagert, auch von der US-IT-Industrie, die da versucht, die Standards so weit offen zu halten oder zu schwächen, dass sie da noch einen guten Stand drin haben. Da sollte man mal mit unseren großen Unternehmen sprechen, was wir in welchem Zeitrahmen erreichen können und wie wir das in diese Gremien einbringen können, damit wir uns da einen Incentive schaffen für diese großindustriellen Spieler, da Investitionen zu unternehmen.

Wir könnten auch solche Dinge überlegen: dass wir eine sofortige harte Übersetzung - das hatte ich in meinem Gutachten auch gesagt - der Safety-Anforderungen, die normalerweise sowieso für solche Technologien gelten, auf Security übernehmen, in der EU. Das heißt also: Alles, was an EU-Richtlinien für Maschinenbau, für solche Dinge existiert, definieren wir mal in der Härte, in der wir das für Safety haben, rüber auf Security. Das bremst dann automatisch alle Akteure aus, die in der EU solche Technologien verkaufen wollen, also auch die Amerikaner und die Chinesen, zwingt die zurück ans Zeichenbrett. Man kann dann von da aus auch mehrere Vektoren anbringen, bestimmte Industriehaftungen. Man kann auch Produkthaftung anbringen: dass man auch haftbar ist für Schäden, die durch ein fehlerhaft entwickeltes Produkt entstehen.

Ganz wichtig wäre in diesem Kontext auch, über eine Vorstandshaftung nachzudenken. Ein großes Problem ist, dass dieses Thema noch nicht so hoch priorisiert ist, dass der CEO sich darum kümmert. Das kriegen wir natürlich nur hin, wenn wir hier auch eine Vorstandshaftung herstellen, die ja in anderen Kontexten auch durchaus existiert. Da müssten wir eigentlich auch nur das parallelisieren, was wir schon haben.

Parallel dazu sollten wir uns natürlich auch darum bemühen, dass eine wesentlich höhere Transparenz zu Risiken und Gefahren hergestellt wird. Das geht einmal natürlich in Richtung der Meldepflicht, die ich für sehr sinnvoll halte, die aber natürlich für die Unternehmen teilweise schwierig ist, andererseits dann aber auch vielleicht in die Richtung, dass man ein bisschen mehr unabhängige Forschung macht in diesem Bereich - Risiken, Modellierung von Konsequenzen, Modellierung von Wahrscheinlichkeiten - und das vielleicht dann auch unterfüttert mit nachrichtendienstlich gewonnenen Informationen über Akteure in der Industriespionage. - Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wichtig ist bei diesen Themen natürlich immer, dass man das Signal auch sendet, dass das, was man dann beschließt, die Standards etc., auch langfristig Bestand haben, dass man nicht ständig von einem aufs andere springt. - Herr Professor Waidner.

Sachverständiger Prof. Dr. Michael Waidner: Ich habe, glaube ich, jetzt den Luxus, dass ich die Antworten meiner beiden Vorredner kommentieren darf und nicht alles neu in epischer Breite beantworten muss.

Zu Ihrer ersten Frage, Herr Flisek - ob diese 20 Prozent ein sinnvolles Maß sind -, kann ich nichts ergänzen. Das ist natürlich ein relativ unsinniges Maß. Was ich aber betonen möchte: Wir reden sehr viel über die Fragen „Wie viel darf man ausleiten?“ oder „Kann man Glasfaserkabel abhören?“ oder irgendwas in dieser Art. Natürlich würde diese Frage komplett verschwinden, wenn man Ende-zu-Ende-Verschlüsselung hätte - also sozusagen noch mal das Plädoyer dafür. Es ist nicht so furchtbar wichtig, wie viel ausgeleitet wird. Es ist nicht so furchtbar wichtig, was man abhören kann und wie man es abhören kann. Es gibt die Gegenmaßnahme, und die Priorität sollte sein, einfach die Gegenmaßnahme umzusetzen; dann verschwindet das Problem komplett, und man

hat gleichzeitig die Motivation für das, was Sandro Gaycken gerade vorhin gesagt hatte: eine gewisse Motivation für die Nachrichtendienste, etwas kreativer und datenschutzfreundlicher vorzugehen. Mehr will ich dazu gar nicht sagen.

Zu Ihren Fragen „Ist ein Full Take realisierbar?“ und „Wie entstehen sozusagen Nadeln?“ oder „Wie findet man diese Nadeln?“ wurde auch schon fast alles gesagt. Was man, glaube ich, rein technisch einfach wissen muss: Die Frage ist[5]: Kann man das Internet auf Jahre hinaus speichern oder nicht? Das[5] ist technisch betrachtet wiederum keine sehr interessante Frage, sondern eine interessante Frage wäre gewesen: Wenn ich diese Daten habe: Kann ich sie jemals wieder verwenden? Man kann natürlich problemlos beliebig große Speicherzentren aufbauen. Facebook baut gerade ein riesengroßes Rechenzentrum mit einem Exabyte Speicherkapazität. Es gibt Gerüchte - die ich für etwas übertrieben halte -, dass die NSA ein Yottabyte speichern kann; das ist wirklich ziemlich viel. Das Problem ist: Die werden das Ding nie wieder einlesen können; das ist das Problem dabei. Man kann leicht speichern. Das große Problem in Big Data ist an und für sich, möglichst schnell alles loszuwerden, was man nicht speichern möchte und auch nie wieder angucken möchte, und darin, sozusagen in diesem Fluss von Daten, möglichst schnell das Richtige zu finden.

Ich habe keine Insiderinformationen zu XKeyscore. Wenn ich mir aber angucke, wie die Folien aussehen zu XKeyscore, und ich mir ansehe, wie normale, kommerzielle Produkte aussehen in diesem Bereich, dann gehe ich mal davon aus: Die werden ziemlich ähnlich sein; diese Interfaces sehen einfach extrem ähnlich aus. Und die sind alle darauf angelegt, dass man möglichst schnell alles loswird, was man nicht braucht, dass man in Realzeit nach diesen Nadeln sucht und nicht etwa in für irgendwelche Ewigkeiten gespeicherten Daten. In diesem Sinne ist es plausibel, dass XKeyscore auf ein paar wenige Tage von Full Take zurückgreift; das reicht aber dann vermutlich auch. Von daher: Man muss da sozusagen mehr auf die Verarbeitung achten, weniger auf die Speicherung.

In diesem Sinne ist auch wirklich wiederum sehr wichtig, sich klarzumachen, dass Metadaten eben auch in der Vorverarbeitung von anderen Daten entstehen; das hatte ich in meiner Einleitung schon gesagt. Aber Metadaten haben, wie Herr Rieger gesagt hat, den großen Vorteil, dass man effizient darin suchen kann, und man kann in dieser großen Flut von Nachrichten - so ähnlich wie man Spam als Spam entdeckt -, in diesen E-Mails auch nach anderen interessanten Dingen suchen. Man kann sie annotieren, man kann Videosequenzen annotieren, man kann sozusagen gucken, dass man diese Dinge beschreibt. Dann suche ich in der Beschreibung, nicht mehr in den sehr komplexen, sehr voluminösen Daten. So funktionieren diese Dinge dann typischerweise auch tatsächlich real: also eine lange Vorverarbeitung mit Annotationen, und dann suche ich nur noch in den Annotationen.

Dann hatten Sie gefragt zur Frage der öffentlichen Ausschreibung. Ist ja schön und gut; aber wenn wir so hohe Standards setzen, dass niemand mehr die Ausschreibung bedienen kann, dann ist auch nichts gewonnen.[6] Das ist natürlich eine absolut wahre Aussage. Man muss an dieser Stelle natürlich realistisch sein. Also, es ist sehr wichtig, eine vernünftige Strategie zu haben, wie man das Niveau langsam nach oben schraubt. Man darf nicht sofort das Maximum verlangen, sondern man muss mit dem Stand der Technik nach oben gehen.

Das geht auch ein bisschen in die Richtung der Frage von Frau Mittag, was vernünftige Zeithorizonte wären und wie man diese langen Fristen sinnvoll verwenden kann. Diese langen Fristen sind erstens, denke ich, keineswegs zehn bis fünfzehn Jahre. Ich höre das immer wieder. Ich weiß nicht, ob gerade jemand auswendig weiß, wann das iPhone eingeführt wurde oder so was; aber gefühlt - man redet immer von Jahrzehnten - - Aber Google gibt es vielleicht so etwas wie zehn Jahre, bisschen länger. Das iPhone gibt es so was wie fünf oder sechs Jahre. Die Innovationszyklen sind also extrem kurz. Wenn wir wollen, können wir innerhalb von fünf bis zehn Jahren sehr viel erreichen - eher in fünf als in zehn Jahren.

5) vgl. Anmerkung des Sachverständigen, siehe Anlage 1.

6) vgl. Anmerkung des Sachverständigen, siehe Anlage 1.

Bei diesem langsamen Nachobenschrauben gibt es sehr viel Dinge, die man tun kann. Sie hatten gefragt: Was muss man, was kann man Menschen sagen, die sofort was tun wollen? - Da sage ich originellerweise genau das Gleiche wie Herr Rieger, nämlich: bei der Schutzbedarfsanalyse anzufangen, damit man wenigstens weiß, was man schützen muss. Es gibt aber durchaus auch schon Technologien, die man schneller einführen kann, die mehr bewirken. Wir hatten alle schon Security and Privacy by Design erwähnt oder Softwareentwurfstechnologien, die Dinge verbessern. Ich habe schon gesehen, dass Firmen ohne Weiteres in zwei, drei Jahren von einem sehr lausigen Zustand im Bereich IT, der Softwareentwicklung zu einem durchaus vernünftig hohen Niveau kommen können. Also, das sind nicht Jahrzehnte oder auch nur fünf Jahre, sondern wenn wir sagen: „Wir wollen, dass die öffentliche Hand nur Software kauft, beispielsweise, die nach State-of-the-Art-Softwareentwicklungsprozessen entworfen worden ist, wo State-of-the-Art-Tests drauf gefahren worden sind, Audits beispielsweise“, dann geht es sehr schnell und es bewirkt auch sehr viel. Längerfristig kann man dann ohne Weiteres Dinge tun wie beispielsweise die schon erwähnte Plattform für Industrie 4.0 und ähnliche Dinge.

An der Stelle muss man aber, glaube ich, wiederum auch ziemlich vorsichtig sein, die Erwartungshaltung nicht zu hoch zu schrauben, darf nicht sozusagen aus Versehen, nur weil man glaubt, in der Zukunft tolle Dinge tun zu können, die kurzfristigen Dinge nicht tun. Ich stimme im Prinzip Sandro Gaycken voll zu: Man soll hier nicht blindlings beliebig viele Sicherheitsprodukte auf das Problem werfen; das hilft nicht so viel. Aber man sollte vernünftig analysieren: Was hilft, und was hilft nicht? - Das ist die berühmte Effizienz. Sehr viele Dinge helfen offensichtlich. Ich kann nur wiederholen: Firewalls sind eine schwache Sache, helfen aber viel gegen viele Angreifer. Und viele Firmen verwenden einfach keine. Das ist ein ganz triviales Beispiel. Diese Schutzbedarfsanalyse - letztes Jahr hatten, glaube ich, 60 Prozent aller Firmen keine -, so was ist kein Hightech oder so was. Das macht Berater sehr glücklich, wenn man das macht. Man muss es einfach tun. Also, da kann man sehr viele Dinge tun, wo man nicht einfach warten muss und große Analysen machen muss. Da kann man einfach mal vorangehen.

Umgekehrt: Ich bin auch sehr dafür, dass man sagt, man greift sich ein paar Dinge raus wie Industrie 4.0, wie Steuerungen von Maschinen, wo wir einen gewissen Vorteil haben, und sagt: Dort machen wir tolle neue Technologien. - Die Basis dafür ist ohne Weiteres in Deutschland vorhanden. In Deutschland, beispielsweise, wurde mal vor 20 Jahren, glaube ich, ein System entwickelt namens L4. Das ist eines der wenigen vernünftigen Basissysteme, auf deren Basis man so was hochziehen kann wie eine sichere Steuerung. Also: kleine, wohldefinierte Systeme. Man darf aber nicht glauben, dass man damit die Industrie 4.0 sicher gemacht hätte. Industrie 4.0 ist nicht einfach nur: eine unsichere Maschine durch eine sichere Maschine ersetzt, sondern der Witz an Industrie 4.0 ist ja gerade, dass man sagt: Unternehmen vernetzen sich über Unternehmensgrenzen, auch über Landesgrenzen hinweg, sie beziehen ihre Daten aus der Cloud, speichern ihre Daten in der Cloud, sie verwenden Data Mining, also Big-Data-Algorithmen, um so was wie vorsorgliche Wartung - Predictive Maintenance - zu machen und so was. Das sind all diese Techniken, die auch im kommerziellen Business-IT-Bereich verwendet werden, die wir dann auch absichern müssen. Wir haben also nichts gewonnen, überhaupt nichts gewonnen, wenn wir eine sichere Steuerung haben, die Daten, die die Steuerung dann ausführt, im Endeffekt aber aus irgendeiner Cloud kommen, die nach billigsten Kriterien, also nach Kostenkriterien, ausgewählt worden ist und dann jeder dort darauf zugreifen und sie manipulieren kann - also von da aus sozusagen ein Sowohl-als-auch-Plädoyer.

Dann ganz kurz zur Usability: Skype ist in der Tat ein wunderbares Beispiel, wie man eine sehr brauchbare Verschlüsselung hinbekommen kann. Es ist auch ein gutes Beispiel dafür, warum es oder unter welchen Bedingungen es gut funktionieren kann. Skype hat gut funktioniert, weil es gezielt auf Endbenutzer zu programmiert worden ist und weil die Infrastruktur von der Firma Skype - oder dann eben von Microsoft - mit entworfen worden ist. Es ist ganz wichtig, sich klarzumachen: Der Endbenutzerteil von all diesen Technologien ist typischerweise nicht der komplizierte, sondern der komplizierte Teil ist

immer die Infrastruktur, also wie man diese Schlüsselverteilung hinbekommt, beispielsweise wie man sichere Ende-zu-Ende-Verschlüsselung hinbekommt über die Server, die das Ganze dann steuern. Das ist einfach sehr aufwendig.

Jetzt habe ich leichtsinnigerweise gerade gesagt, dass Usability ein einfaches Problem wäre. Es könnte ein leichteres Problem sein, wenn man mehr Fokus darauf setzen würde. Usability, gerade im IT-Sicherheitsbereich, war über mindestens zehn, fünfzehn Jahre kein großes Thema in der IT-Sicherheitsindustrie. Deswegen kommen diese bekannten Abfragen, auf die Sandro Gaycken angespielt hat: dass arme Benutzer gefragt werden, irgendwelche Entscheidungen zu fällen, die sie nicht fällen können. Deswegen, beispielsweise, sind Systemadministratoren regelmäßig überfordert, mit ihrer Usability umzugehen. Die Interfaces, die wir als Endnutzer sehen, sind typischerweise schon sehr gut verständlich verglichen mit den Interfaces, die man dem normalen Systemadministrator vorsetzt. Da ist ein horrendes Potenzial, besser zu werden, auch weil es einen ziemlich einfachen Grund gibt, warum die Usability von Sicherheitssystemen relativ schlecht ist: Das liegt einfach daran, dass IT-Sicherheit lange Zeit pur auf Compliance abgehoben hat. Wenn Sie als IT-Sicherheitsfirma jemandem etwas verkaufen wollten, dann war es nicht wichtig, was die Benutzer davon halten, sondern ob Sie eine bestimmte gesetzliche Vorgabe eingehalten haben oder nicht. Dementsprechend hat man alles darauf hingetrimmt, dass sozusagen an den richtigen Stellen die richtige Warnung hochgepoppt ist und die richtige Frage gestellt worden ist. Aber man hat keine Hilfestellung zur Verfügung stellen müssen, weil das war nicht Teil der Compliance. Deswegen denke ich, wir haben es jetzt in der Hand, sinnvollere Regelungen zu machen, dass man mit diesem Ansatz nicht weiter durchkommt, sondern wirklich benutzbare Systeme entwerfen kann. Aber das halte ich wirklich für ein Problem, das man in den Griff kriegt, wenn man einfach mehr Fokus darauf hat.

Dann zu den Fragen „Einschätzung Industriespionage“ und „Was passiert real?“ und „Wie schätzt man das alles ein?“. Da kann ich, glaube ich, nicht sehr viel mehr dazu beitragen, als meine beiden Kollegen links und rechts schon gesagt haben. Was ich betonen möchte, ist aber: Wenn Sie mit Vertretern amerikanischer Firmen reden, dann ist es tatsächlich so: Diese Firmen sind entsetzt. Das ist, glaube ich, auch nicht gespielt. Sie fühlen sich tatsächlich auch betrogen. Das mag jetzt daran liegen, dass eine Firma eben keine holistische Sache ist: Es kann ohne Weiteres sein, dass ein Teil dieser Firmen durchaus wusste, was passiert; ein großer Teil wusste es vermutlich nicht. Was es aber für uns bedeutet, ist eben: Wenn wir so was machen, wie unsere Standards in Europa entwickeln, wenn wir Technologien entwerfen, um die Überprüfbarkeit von Systemen zu verbessern - - Wir können mit diesen Firmen zusammenarbeiten, wir müssen mit diesen Firmen zusammenarbeiten. Ich denke, digitale Souveränität wird nicht heißen, dass wir alles in Europa oder Deutschland machen, sondern das heißt, dass wir eben sinnvoll mit Firmen in den USA, in wo auch immer zusammenarbeiten, dass dort unsere Standards für die Überprüfbarkeit akzeptiert werden, dass die unterstützt werden und - - Einer von meinen beiden Kollegen hat das gesagt: Das sind zurzeit eigentlich unsere natürlichen Verbündeten. Ich denke, da rennen wir offene Türen ein.

Eine Grenze zwischen IT-Sicherheitsfirmen und IT-Firmen würde ich tatsächlich nicht ziehen. Man muss sich einfach mal im Klaren darüber sein: So eine Firma wie RSA wird gerade immer sehr hoch gehoben, weil sie ertappt worden ist. RSA ist eine kleine Division einer Firma namens EMC; das ist einer der größten Hersteller von IT überhaupt und einer der Marktführer im Bereich Speichertechnologien, also Platten und so Zeugs. Von daher: Man kann es nicht auseinanderhalten, es betrifft wirklich alle Firmen. Das unterstützt auch ein bisschen meine These, dass man sagen muss: Wenn man mit Firmen wie eben EMC oder Intel oder so was konkurrieren möchte, dann braucht man in Europa halt auch Firmen von diesem Kaliber. Deswegen noch mal vielleicht die Erklärung, warum ich nicht nur KMUs, sondern auch wenigstens ein oder zwei Firmen in Europa haben möchte, die eben mit solchen Riesen mithalten können und dann auch relativ schnell

so was wie Industrie-4.0-Plattformen gut[7] hochziehen können.

Letzter Punkt: Ich unterstütze völlig, was Sandro Gaycken angesprochen hatte: dass man die hohen Safety-Standards, die man im Bereich von Flugzeugen und Ähnlichem kennt, auch auf IT-Sicherheit überträgt. Das ist zurzeit auch ein großes Thema in allen Standardisierungsdiskussionen zu Industrie 4.0, ist ein europäisches Thema. Das ist alles nicht so furchtbar einfach; aber ich kann auch da wiederum nur sagen: Industrie 4.0 ist sehr viel größer. Wenn ich Safety-Standards übertragen kann für eine Fabrik, habe ich noch nicht Safety für die Industrie 4.0 - Industrie 4.0 ist übergreifend.

Jetzt habe ich, glaube ich, alles beantwortet, was ich beantworten wollte. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für Ihre Ausführungen.

Ich darf nun zur Fraktion Bündnis 90/Die Linken kommen.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): So weit ist es noch nicht! - Heiterkeit - Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Da würde vor allen Dingen Bündnis 90 einige Einwände dagegen haben; aber sei es drum!)

- Bündnis 90/Die Grünen. Das ist, wenn zwei Gehirnhälften versuchen, gleichzeitig unterschiedliche Dinge zu denken, nämlich auf die Minuten zu gucken und gleichzeitig zu schauen, welche Fraktion dran ist. Lieber Konstantin von Notz, das sollte keine Verwirrung hervorrufen. Bündnis 90/Die Grünen haben jetzt für acht Minuten die Möglichkeit, Fragen zu stellen. Wir freuen uns dann auf die intensiven Antworten. Ich gebe dem Obmann von Bündnis 90/Die Grünen das Wort: Konstantin von Notz. Bitte schön.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. - Ich versuche, diese acht Minuten schnell zu nutzen. Erst mal ganz herzlichen Dank für die Expertise am heutigen Tag und vor allen Dingen an Sie, Herr Rieger, dass das so kurzfristig möglich war; das ist wirklich ausgesprochen freundlich und entgegenkommend.

Ich will mal anfangen mit einer Metaebene-Frage. Ich glaube, wir sind uns einig, dass das Vertrauen in diese Infrastruktur massiv erschüttert wurde; manche sagen ja, dass diese Snowden-Veröffentlichungen der Super-GAU für diese globale Kommunikationsinfrastruktur sind. Da will ich Sie gerade vor Ihrem technischen Sachverstand fragen, ob Sie das Gefühl haben, dass die Politik bisher ausreichend etwas dafür tut, dass dieses Vertrauen wiederhergestellt wird. Also im Hinblick auf all die klugen Dinge, die Sie jetzt angesprochen haben, was man machen kann - von der Ausbildung von Informatikern bis hin zu Konsortien usw. -: Passiert im Augenblick politisch genug, oder ist alles, was passiert, eigentlich, dass wir hier im Untersuchungsausschuss darüber reden? - Da würde mich Ihre Einschätzung interessieren.

Den zweiten Punkt fand ich interessant, Herr Professor Waidner: was Sie gesagt haben im Hinblick darauf, dass man diese Überwachung, die im Internet zum Großteil passiert, eigentlich nicht spürt, nicht wahrnehmen kann, nicht sehen kann. Als technischer Laie sage ich mal: Man findet nicht die Wanze im Telefon oder so. Vor dem Hintergrund auch die Frage: Hätte es technische Möglichkeiten gegeben - auch für die Spionageabwehr, wenn sie denn guten Willens gewesen wäre, was ich nicht genau weiß -, diese Spionage und Grundrechtsverletzungen aufzudecken, ohne dass jemand in einem Akt zivilen Ungehorsams diese Sachen einfach öffentlich macht? Das würde mich interessieren, vielleicht vor allen Dingen von Ihnen, Herr Professor Waidner; aber gerne können alle auch was dazu sagen.

Dann noch mal konkret - weil ich das sehr interessant fand eben noch mal mit XKeyscore - zu den Programmen an sich: Da geistern ja viele Namen durch die Gegend. Wir haben uns hier alle mit den einzelnen Sachen auch ein bisschen beschäftigt; aber ich wäre Ihnen dankbar, wenn vielleicht jeder von Ihnen noch mal ein, zwei Programme ansprechen könnte und in zwei, drei Sätzen erklären könnte, was da eigentlich

7) Protokoll korrigiert, siehe Anlage 1.

passiert - XKeyscore haben wir jetzt; aber Prism, Mystic, Tempora und die vielen anderen Sachen -, was technisch eigentlich das Interessante daran ist, was da passiert. Also was sind diese anlasslosen, massenhaft gefahrenen Instrumente? Vielleicht kann einer oder alle drei von Ihnen etwas zu RAMPART-A sagen. Das haben Sie ja bestimmt verfolgt im Zusammenhang mit „Warp Drive“. Haben Sie da schon einen Kenntnisstand, wie Sie das einschätzen? Ich finde, das ist ein sehr spannendes Thema.

Dann die Ende-zu-Ende-Verschlüsselung, die ja angesprochen wurde: Das war ja eine große Diskussion, auch hier im Deutschen Bundestag, im Zusammenhang mit der Einführung von De-Mail. Viele Sachverständige haben uns damals geraten, Ende-zu-Ende-Verschlüsselung bei De-Mail vorzuschreiben. Es ist nicht gemacht worden. Jetzt hat man den Salat. Aber die interessante Frage, die sich daraus ableitet, ist: Kann es sein - aus Ihrer Wahrnehmung heraus -, dass der Staat, bisher zumindest, an der Verletzlichkeit der Infrastruktur durchaus auch ein Eigeninteresse haben könnte, weil, wenn man die Infrastruktur unverletzlich zu machen versucht, eben auch Überwachung und auch polizeiliche Maßnahmen zugegebenermaßen deutlich schwieriger werden? Also, ist das nicht eigentlich ein Interessenkonflikt eines Staates, der sagt - keine Ahnung -: „Wir wollen IMSI-Catcher einsetzen; aber wir wollen auch die Datensicherheit bei Mobiltelefonie erhöhen“? Ist das nicht was Widersprüchliches, und könnte es nicht sein, dass die letzten zwanzig Jahre im Bereich Sicherheit/Infrastruktur eigentlich ganz bewusst nicht viel gemacht worden ist?

Dann die Frage zu diesem Schengen-Routing: Da frage ich mich im Zusammenhang mit Safe Harbor: Solange man so eine Regelung wie Safe Harbor hat, macht da Schengen-Routing eigentlich irgendwie Sinn? Oder würden Sie nicht auch sagen: „Wenn man hier die Datenschutzinteressen Deutschlands und Europas durchsetzen können will, dann müsste man ein solches Abkommen sofort stoppen, damit sozusagen die Probleme, die damit einhergehen, und das, was wir von unserer Seite tun könnten, eben auch sofort gestoppt werden“?

Das waren meine Fragen. - Jetzt hätte der Kollege Ströbele noch eine Frage.

Vorsitzender Dr. Patrick Sensburg: In fast bewährter Praxis kriegt Herr Kollege das wohl hin in zwei Minuten.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Es sind zwei Fragen geworden; aber die gehen ganz schnell. Beide schließen an das an, was der Kollege von Notz schon gesagt hat.

Das eine ist: Gibt es nicht in den USA die Erfahrung, dass die Regierung sogar strafrechtlich gegen Firmen vorgeht, die Verschlüsselungsprogramme anbieten, sodass die diese ihre Handelsware - Verschlüsselungsprogramme - in den USA gar nicht mehr vertreiben können und dürfen? Welche Erfahrungen sind damit gemacht worden?

Die zweite Frage ist: Der Gesetzgeber hat sich ja viel dabei gedacht, als er die Tätigkeit des Bundesnachrichtendienstes bei der Erfassung von Auslandsdaten eingeschränkt hat. Zu diesen 20 Prozent haben Sie schon einiges gesagt. Das Zweite ist, dass die deutsche Kommunikation da ausgeschlossen werden soll, also von deutschen Staatsbürgern bzw. mit Deutschland. Beide diese Bedingungen oder Einschränkungen sind ja gut gemeint gewesen; aber wenn ich Sie richtig verstanden habe, funktionieren beide, jedenfalls heute, nicht mehr.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Herr Kollege Ströbele. - Ich darf nun um die Beantwortung der Fragen bitten und würde mit Ihnen, Herr Professor Waidner, anfangen.

Sachverständiger Prof. Dr. Michael Waidner: Vielen Dank. - Kleinere Parteien scheinen immer schwierigere Fragen zu stellen.

Die erste Frage von Herrn von Notz war, ob die Politik ausreichend gehandelt hat. Das ist natürlich eine zweischneidige Frage. Es gibt sehr viele Dinge, wo ich mir wünschen würde, dass die Politik sie schon in Angriff genommen hätte, die aber noch nicht passiert sind. Vieles von dem - oder eigentlich alles, was wir hier diskutiert haben - sind jetzt, glaube ich, keine revolutionären Ideen genau genommen, sondern Dinge, die eigentlich schon länger auf dem Tisch liegen. Ich denke, das hätte man natürlich auch schon früher machen können. Umgekehrt denke ich, in diesem Ausschuss sind wahrscheinlich

sehr viele Ideen schon diskutiert worden, und meine persönliche Erwartungshaltung ist eigentlich, dass Ihr Ausschuss gerade bei der Umsetzung dieser Ideen einen großen Beitrag leisten wird. Also, ich bin sehr optimistisch - einfach: Wenn nicht jetzt, wann dann?

Hätte man die Überwachung finden können? Dazu können meine beiden Kosachverständigen bestimmt auch viel sagen. Generell ist es mal so: Bei der Massenüberwachung hat ein großer Teil dieser Überwachung nicht in Deutschland stattgefunden. Von daher muss man überlegen: Was bedeutet es eigentlich, dass man etwas hätte finden können? Hätte das BSI einen Supersuchtrupp losschicken und irgendwas finden können in dieser Art? Da würde ich sagen: Es ist sehr unwahrscheinlich, dass man alles hätte finden können.

In der Massenüberwachung - - Das Abhören an Knoten ist eben spurlos machbar. Ich denke realistischerweise: Viele der Überwachungsmaßnahmen, die geschildert worden sind, sind sicherlich nicht spurenlos gewesen, sondern waren eben mit Kooperation von Telekommunikationsunternehmen oder, im Bereich Prism, mit Kooperation von irgendwelchen Anbietern von Dienstleistungen. Das könnte man im Prinzip sehen. Die Mitarbeiter der Telekommunikationsunternehmen können so etwas sehen. In diesem Sinne hatte ich auch meine Glasfaserantwort vorhin gemeint. Auch die Mitarbeiter von großen Dienstleistern können sehen, wenn da Daten ausgeleitet werden. Das ist sozusagen eine zweischneidige Sache. Also es gibt keine eindeutige Antwort. Sagen wir es eher so: Manches hätte man finden können. Abstrakt gesehen kann man Massenüberwachung nicht feststellen in dieser Art.

Einzelüberwachung ist ganz anders: Wenn jetzt so was wie ein Router im Nachhinein manipuliert wird, wenn die Software ausgetauscht wird beispielsweise, wenn irgendwo ein Chip ausgetauscht wird - was ja durchaus passiert ist, alles beides -, dann kann man das natürlich sehr wohl feststellen. Man kann beispielsweise, indem man Code Signing verwendet, im Nachhinein feststellen, wenn Software ausgetauscht worden ist. Es gibt Technologien wie Trusted Computing. Das hat teilweise einen sehr schlechten Ruf, hat aber den Vorteil: Man könnte tatsächlich feststellen, ob bestimmte Hardwarekomponenten ausgetauscht worden sind. Auch da gilt wieder: Wenn ein Angreifer beliebig viel Aufwand reinsteckt, kann er auch solche Mechanismen irgendwie aushebeln. Aber man kann sehr viel tun, um Einzelüberwachungsmaßnahmen, also Einzelangriffe, tatsächlich feststellen zu können; aber generell: Die meisten dieser Sachen sind sehr schwer festzustellen.

Dann hatten Sie gefragt: Was sind unsere drei beliebtesten Spionageprogramme sozusagen?

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

An der Stelle würde ich immer das Tripel sagen, was Sie auch schon genannt hatten, nämlich Tempora, Prism und XKeyscore, einfach weil die wirklich illustrieren, wie das halt immer funktioniert.

Tempora ist das Programm, mit dem sozusagen Daten vom Internet abgesaugt werden in großen Massen, undiskriminierend, einfach zwischengespeichert, irgendwo hineingepumpt. Diese Daten sind sozusagen die Daten, die ich persönlich mit Ende-zu-Ende-Verschlüsselung komplett loswerden würde. Das Problem könnte ich lösen damit.

Prism ist in gewisser Weise dann der nächste und gefährlichere Gegner, weil dort geht es eben darum, dass Daten von Diensteanbietern direkt abgesaugt werden, also von den Endpunkten, die ich durch Ende-zu-Ende-Verschlüsselung eben nicht schützen kann. Dort brauche ich ganz andere Maßnahmen, um diese Daten zu schützen. Aber wenn ich sozusagen die Rohdaten der Kommunikation habe - alle möglichen Verbindungsdaten, Soziale-Netze-Daten, direkten Zugriff auf vorsortierte E-Mails und ähnliche Dinge -, dann ist sozusagen das nächste Instrument eben dieses XKeyscore, was ja vorhin eigentlich schon ausführlich erläutert worden ist, mit dem man dann auf das Vorverarbeitete aus Tempora und auf die Daten, die man von Prism abzweigen kann - - gezielt suchen kann.

Als Nächstes hatten Sie gefragt nach der Ende-zu-Ende-Verschlüsselung, die ja in De-Mail in der Tat bedauerlicherweise nicht vorgeschrieben worden ist, und Sie fragen, ob es einen

Interessenkonflikt gibt zwischen Überwachung durch die eigenen Sicherheitsbehörden und dem Schutz der Bürger. Da ist natürlich ganz klar ein Interessenkonflikt. Dieser Interessenkonflikt wurde ja in Deutschland und auch im Ausland öfters mal diskutiert. Ich denke, so 1985 herum, schätze ich mal, hat die erste große Diskussion angefangen, ob man Kryptografie zulassen soll in Deutschland, ob man Kryptografie mit Hintertüren haben möchte, ob es so was wie Key Escrow geben soll. Also sozusagen: Will man die Menschheit oder will man die Bürger schützen, bedingungslos? Oder will man sozusagen den Schutz so gering halten, dass man im Endeffekt doch darauf zugreifen kann? Die Diskussion damals, die irgendwann in den 80er-Jahren angefangen hat und bis, glaube ich, fast Ende der 90er-Jahre ging, hat recht eindeutig den Schluss gehabt, dass man den Bürger schützen muss. Der Schutz des Bürgers, auch gegenüber den Bedürfnissen der Sicherheitsbehörden, muss Priorität haben gegenüber der Möglichkeit, Abhörmaßnahmen zu machen.
Dafür gibt es sicherlich einerseits eine rein ethische Argumentation. Es gibt aber auch einfach die technische Argumentation, dass jede Form von Hintertür missbraucht werden kann. Als Techniker kann ich nur sagen: Jeder, der auf die Idee kommt, in irgendein System eine Hintertür einzubauen oder eine Schwachstelle einzubauen, muss damit rechnen, dass diese Hintertür auch von Leuten gefunden wird, die weniger gutmeinend sind als diejenigen, für die man sie mal vorgesehen hat. - Sie wollten etwas fragen.

Vorsitzender Dr. Patrick Sensburg: Eine Zwischenfrage? Gerne.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wenn ich da ganz kurz einen Gedanken nachfragen kann - weil Sie das vorhin auch ansprachen -, bezüglich der Exploits: Wenn dieser Gedanke stimmt - was ich unterstreichen würde; ich finde, es leuchtet ein, dass das sozusagen zugunsten der Sicherheit der Bürgerinnen und Bürger entschieden werden muss -, wie kann es dann sein, dass wir über Exploits, Zero-Day-Exploits, in Händen von Geheimdiensten reden, wo es eben genau darum geht, dass diese Sicherheitslücken künstlich offengehalten werden, obwohl staatliche Behörden von ihnen wissen, und man die nicht öffentlich macht, um sie sozusagen zu Sicherheitszwecken zu nutzen, und dabei dann häufig, millionenfach, Betroffene dann auch diesen kriminellen Aktivitäten und anderen Problemen aussetzt?

Sachverständiger Prof. Dr. Michael Waidner: Die NSA hat ja zugegeben, indirekt, dass sie tatsächlich Exploits verwendet von Schwachstellen, die nicht absichtlich eingebaut sein müssen, sondern zufällig entstanden sein können. Das heißt einfach: An dieser Stelle ist die Güterabwägung offensichtlich anders ausgefallen.

Ich kann nur sagen: Als Bürger ist meine Meinung: Das darf nicht passieren. Als Techniker kann ich Ihnen sagen: Es ist einfach eine ganz, ganz schlechte Idee. Diese Exploits, also nicht die Exploits, sondern die Schwachstellen: Manche davon werden absichtlich eingebaut, teilweise. Die meisten Schwachstellen entstehen vermutlich dadurch, dass Fehler gemacht worden sind in der Programmierung. Wie gesagt, Statistiken zeigen: Große Pakete haben so was wie 1 000 Schwachstellen. Einfach jeder Geheimdienst dieser Welt müsste im Klaren darüber sein: Wenn ein Geheimdienst Schwachstellen auf dem offenen Markt kauft - was man durchaus kann -, dann müssen sie damit rechnen, dass sie nicht der einzige Käufer dieser Schwachstelle sind. Und wenn man diese Schwachstellen selbst gefunden hat, dann muss man sich auch im Klaren darüber sein: Die gleichen Mechanismen, die man selbst verwendet hat, um diese Schwachstellen zu finden, die verwenden auch Forschungsinstitute und andere Organisationen, die Schwachstellen suchen. Also, wenn ich etwas gefunden habe, ist die Wahrscheinlichkeit, dass jemand anders es findet - oder kauft -, nicht so gering. Aus diesem Grunde ist es, wie gesagt, eine richtig schlechte Idee, so etwas zu machen.

Ihre letzte Frage war, ob Schengen-Routing sozusagen einen Sinn hat, wenn man daran denkt, es gibt so was wie Safe Harbor. Zum einen: Schengen-Routing hat, wie gesagt, im Prinzip seinen Sinn, wenn man Daten innerhalb von Europa hält. Es ist ein kleines Pflaster. Ich persönlich würde das größere Pflaster Ende-zu-Ende-Verschlüsselung, wie ich jetzt schon öfter

gesagt habe, bevorzugen. Natürlich haben Sie recht: Safe Harbor - also die Regelung, dass man persönliche Daten in die Mitgliedstaaten von Safe Harbor transferieren kann unter der Annahme, dass dort das gleiche Datenschutzniveau gilt - ist natürlich fragwürdig, wenn dort das Datenschutzniveau relativ offensichtlich an vielen Stellen nicht ganz so gleichwertig ist. Der Gedanke von Safe Harbor ist vielleicht gar nicht mal so dumm - an dieser Stelle stimmt er halt einfach nicht.

Das waren, glaube ich, Ihre Fragen und die beiden Fragen von Herrn Ströbele. Ihre eine Frage bezog sich darauf, was wir davon halten, dass in den USA auch schon strafrechtlich vorgegangen worden ist gegen Firmen, die ihren Kunden dort starke Verschlüsselung angeboten haben. Das ist tatsächlich passiert - nicht so sehr wegen der starken Verschlüsselung,

(Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): Wegen der Schlüssel!)

sondern eher wegen der Weigerung, die Schlüssel nicht [sic!] herauszugeben. Natürlich: Wenn die Schlüssel draußen sind, hilft die ganze starke Verschlüsselung nichts mehr. Auch da kann ich nur sagen: Ich kann mir nicht vorstellen, dass das in Deutschland passieren würde, und es ist eine absolut schlechte Idee. Für einen Staat sollte der Schutz der Bürger immer Priorität haben gegenüber allen anderen Dingen.

Ihre zweite Frage war, ob die 20 Prozent oder das Filtern irgendeinen Sinn hat. Also, die 20 Prozent haben wir, glaube ich, schon ausführlich diskutiert: dass das ein völlig ungeeignetes Maß ist, weil die 20 Prozent wahrscheinlich schon deutlich mehr sind als das, was einen wirklich interessiert.

Zum Herausfiltern von deutscher Kommunikation hatten wir schon etliche Beispiele. Jetzt kann ich auch meine persönlichen Beispiele beisteuern: Meine E-Mail ist in der Schweiz und meine andere E-Mail ist in den USA; ich wäre also wahrscheinlich sofort in jedem Überwachungsprogramm drin, was man sich so denken kann. Man kann in einer globalen Welt nicht sagen, welche Daten zu einem Deutschen gehören oder zu einem Amerikaner oder wem auch immer. Wenn man das wollte, müsste man, offen gesagt, einen massiven Überwachungsapparat aufbauen, der kein anderes Ziel hätte als herauszufinden, welche Daten man überwachen darf, was offensichtlich eine völlig absurde Vorstellung ist. Von daher ergibt das keinerlei Sinn. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Dr. Gaycken, ich darf Ihnen das Wort geben.

Sachverständiger Dr. Sandro Gaycken: Danke. - Zu Ihrer ersten Frage, ob die Politik genug tut, um das Vertrauen wiederherzustellen: Nein. Sie müssen wissen, wir haben dieses Thema ewig, Dekaden, vernachlässigt. Entsprechend sind auch die Strukturen einmal klein und nicht so sehr professionell in vielerlei - - haben viel Erfahrung und sind sehr gut auch, viele Leute - - aber einmal klein. Und dann hat man denen den Mut abgewöhnt, auch mal härtere, etwas disruptivere Lösungen vorzuschlagen. Dadurch, dass sie jahrzehntelang immer nur abgebogen wurden mit allem, was die wollten - - Teilweise wurden die auch strafversetzt, wenn sie mal gesagt hatten: So, wir wollen jetzt hier mal eine harte Sicherheit. - Das können die nicht machen; dann ab irgendwo anders hin! Dadurch ist insgesamt die Haltung nicht so, dass man in der Lage wäre, wirklich gute Strategien zu entwickeln.

Wenn ich eine gute Strategie entwickle, dann sehe ich mir ja an: Was habe ich an Problemen, was habe ich aus diesen Problemen heraus für Bedürfnisse, und wie kann ich das lösen? Das ist eigentlich der Gang von einer Strategie. Wir machen aber Strategie immer: Was kann ich, und wie kann ich jetzt irgendwas formulieren, was vielleicht zu dem Problem passt, das mich gut aussehen lässt mit dem, was ich kann? Also, so eine fähigkeitsorientierte Strategieformulierung von unten nach oben haben wir immer ganz stark in diesem Feld. Wir müssen aber andersrum kommen. Dann sagen ganz viele: Na ja, dabei kommen so viele unrealistische Sachen heraus. - Aber ich finde es nicht unrealistisch, Sicherheit einzufordern in kritischen Strukturen. Von daher: Auch wenn da die Hürden für die Kompetenzen, für die Fähigkeiten, für die Ressourcen vielleicht erst mal höher sind, muss

man das trotzdem von da definieren und dann sehen, wie man mit seinen Fähigkeiten dahin kommt - vielleicht nicht nächste Woche, aber nächstes Jahr -, um das dann zu bedienen. Das ist ein wichtiger Punkt für diese ganze Formulierung von IT-Strategie, Cyberstrategie.

Auch Datenschutz: Wir müssen da wegkommen davon, dass wir das von unseren Fähigkeiten aus definieren, und dahin kommen, dass wir das wirklich von unseren Bedürfnissen nach unten definieren.

Andererseits muss man auch mal überfragen, ob denn überhaupt schon genug Misstrauen erhöht wurde. In einigen Bereichen würde ich mir deutlich mehr Misstrauen wünschen; da ist die Unterbrechung und Zerstörung des Vertrauens ja durchaus berechtigt. Wir sollten jetzt nicht daran arbeiten, dieses Vertrauen wieder irgendwie so hinzubiegen, dass die Menschen damit weitermachen, unsichere oder schlechte Dinge zu benutzen.

Wir brauchen noch deutlich mehr Misstrauen gegenüber den Basisunsicherheiten in der IT. Da wird viel zu wenig nachgefragt, warum wir eigentlich so furchtbar angreifbar sind und warum diese Basis, Commercial IT, so furchtbar schlecht ist.

Dann brauchen wir deutlich mehr Unsicherheit auch gegenüber solchen Phänomenen wie Information Operations. Das steht uns im Westen automatisch im Weg, weil wir unsere Pressefreiheit, unsere Meinungsfreiheit da angegriffen sehen. Aber das ist ein großes Problem, dass uns im Internet quasi PR-Institute und fremde Nachrichtendienste Tag für Tag irgendwelche Geschichten vorgaukeln, die wir gar nicht mehr verifizieren können.

Wir müssen auch das Misstrauen im Bereich Industriespionage noch deutlich erhöhen.

Die zweite Frage, ob die Spionageabwehr das technisch hätte abwehren können: Nein. Gerade bei den gezielten Aktivitäten - - und überall, wo eine Spionageabwehr gewesen wäre, wären gezielte Aktivitäten zum Tragen gekommen; denn das sind Hochsicherheitsstrukturen, die sich nur mit gezielten Angriffen angreifen lassen, und die sind im Moment in der Struktur und in der Modularität, wie sie gebaut werden, so gebaut, dass sie jede Detektion hundertprozentig vermeiden können. Die greifen also diesen ganzen Safety- und Security-Apparat mit an, das sind mehrstufige Angriffe aus verschiedenen Modulen, die dann verschiedene Dinge gleichzeitig bedienen. Die können auch, wie gesagt, sehr lange da drinbleiben und sehr viele verschiedene Updates auch mitmachen und solche Dinge. Da sind wir einfach technisch noch lange nicht, um das irgendwie zu erkennen.

Es ist natürlich schwierig, zu sagen, wie groß das Dunkelfeld ist. Aber um nur mal eine Zahl dazu in den Raum zu werfen: Wir haben ja auch in den Snowden-Leaks diese Zahl der Operationen des US-Cybercommand im Jahr 2011 - da hat man mal einen guten Maßstab -: Wir haben im Jahr 2011 Operationen des US-Cybercommand offiziell gefunden und beobachtet: eine einzige. Es haben aber stattgefunden: 231. Das ist so ungefähr das Verhältnis von Hellfeld zu Dunkelfeld bei diesen gezielten Operationen. Und der eine, den wir gefunden haben, war auch - wie immer in diesem Feld - ein dummer Zufall. Das ist immer so: Wenn wir die finden, diese gezielten Angriffe - - Wir hatten auch mal was im Schweizer Außenministerium, wo auch jahrelang einer saß, sich ein Darknet gebaut hatte usw. Der ist nur durch einen dummen Zufall rausgeflogen und nie durch diese tollen IT-Sicherheitsprodukte, die wir da haben.

Meine Top-Programme: Ich würde dann auch unterscheiden zwischen Massenüberwachung und gezielten Sachen. Bei der Massenüberwachung wäre ich mit Michael Waidner auch bei Prism und Tempora. Ansonsten sind für mich natürlich die Tailored-Access-Geschichten interessanter, also alles, was gezielte Aktivitäten angeht; denn da haben wir teilweise richtige Kataloge geliefert bekommen von Sachen, die die tun. Diese Kataloge sind natürlich für uns der Benchmark, an dem wir uns orientieren müssen, wenn wir jetzt IT-Sicherheit weitermachen wollen. Wir können jetzt nicht so tun, als hätte es das nicht gegeben, als hätten wir nicht gesehen, zu was die in der Lage sind, auf was für einem Niveau die angreifen. In diesem Endkatalog 2008, der ja nun auch schon veraltet ist, wo wir davon ausgehen müssen, dass es viel mehr gibt - - Was da schon alles drin war an Hacks auf Hardwareebene, BIOS-Ebene, wo die kleine Chips in Kabel installiert haben, Kabel zu einem Monitor und lauter so Geschichten: Das müssen wir doch mal zur Kenntnis nehmen und

uns da mal daran orientieren, was für eine Problemlandschaft sich da eigentlich abbildet. Das ist von daher für mich immer sehr wichtig.

Könnte der Staat Interesse an der Verletzlichkeit der Infrastrukturen haben? Ja, klar. Ich meine, natürlich klagen die Dienste und die Strafverfolger immer, wenn da irgendwie eine tolle neue Krypto eingeführt wird. Das macht deren Arbeit halt schwer. Aber das heißt noch nicht, dass die das auch systematisch verhindern.

Es gab einmal in den USA im State Department eine Diskussion, wo Hillary Clinton im Rahmen des arabischen Frühlings den Oppositionellen Mittel zur sicheren anonymen Kommunikation zur Verfügung stellen wollte. Da kam dann auch das FBI rein und hat gesagt: Nein, könnt ihr nicht machen; wenn ihr das auf dem Niveau, das die Nachrichtendienste nicht knacken können, macht, dann benutzen das auch unsere Kriminellen usw. - Das ging dann hoch bis in den Senat. Der Senat hat entschieden: „Freedom of speech“ ist wichtiger und dass wir diese Region befreien; also entwickelt ihr die Dinger und liefert die dahin, und ihr, FBI, müsst euch hinten anstellen. - Das ist eben eine Frage, wo dann Politik reinkommt. Das ist dann Ihre Angelegenheit, zu entscheiden, was Ihnen wann wichtiger ist. Auch da kann man sagen: Es ist eben wichtig, dann auch differenziert zu betrachten: welche Fälle in welchen Kontexten?

Es gibt ja auch viele - um das mal als Gegenargument einzuwerfen -, die sagen, dass der Schutz des Bürgers vor Atomwaffen auch wichtig ist und dass von daher die Sabotage des iranischen Atomprogramms, das ja eventuell doch eine gewisse Instabilität in diese Region bringen könnte, auch eine gute Seite hatte. Das muss man jetzt politisch nicht teilen; aber es ist auf jeden Fall auch ein valides Argument, dass man damit dann auch solche Dinge infiltrieren kann und da andere Dinge tun kann. Da ist auch ein bisschen Raum für Fall-zu-Fall-Abwägung.

Aber prinzipiell müssen wir natürlich sagen: Wenn es jetzt darum geht, ob wir in der Fläche mehr Sicherheit einziehen sollen oder nicht, dann ganz klar: definitiv Ja, und auch eine sehr hohe Sicherheit. Denn erstens sind die Verbrecher, mit denen wir zu tun haben - - und die hochqualifizierten Dienste und Terroristen, die sind sowieso so gut, dass die mindestens auf dem Niveau operieren; von daher ist es für die sowieso nicht relevant, wenn wir den Rest unsicher lassen.

Zweitens haben wir durch Unsicherheit in der Summe deutlich mehr zu verlieren als zu gewinnen. Gerade die hochindustrialisierten Nationen, wir haben so viele Assets auf IT rumliegen, die uns unglaublich kritisch beeinflussen könnten, dass wir da eine ganz klare Priorität haben.

Bei Safe Harbor mit Schengen-Routing sehe ich, ehrlich gesagt, keinen Konflikt. Bei Safe Harbor gehen natürlich immer noch Daten dahin; aber das sind doch wesentlich weniger und sehr spezifische Daten und nicht diese unglaublichen Massen.

Bei den Überwachungsprogrammen geht es ja vor allen Dingen um diese massenhafte Auswertung, das Finden von Querverbindungen usw. Von daher nimmt man da doch einen erheblichen Prozentsatz raus. Ich weiß nicht, wie weitreichend da noch irgendwelche Zusatzabkommen vielleicht gehen oder so was.

Auch bei Strafkooperationen muss man natürlich sehr genau hingucken, dass es irgendwie nicht zu voluminös wird; aber auch da ist es natürlich dann eine anlassbezogene und gezielte Aktivität und nicht dieses massenhafte, anlasslose Abgreifen. Also, da würde ich möglicherweise schon ein bisschen differenzieren.

Wurden die US-Unternehmen zur Kooperation geklagt? Ich habe gehört, ja. Das war aber so gerüchtehalber, wo sich von den großen IT-Firmen nach drei Bieren dann mal einer geäußert hat: Ja, die sind dann schon bei uns richtig zum Vorstand, nach ganz oben, gegangen und haben gesagt: Entweder ihr macht das, oder ihr kommt vor den Geheimdienst-Court, dass ihr hier nicht mit der und der Regulierung kooperiert und so. - Das ist aber natürlich die tiefste und dunkelste Gerüchteküche. Da haben wir auch keine - - Da wird uns auch keiner was sagen wollen, ob das so war und wie das war.

Vielleicht kann man da das vertrauliche Gespräch mit einigen der US-Unternehmen suchen, die davon betroffen sind. Die sind, wie gesagt, gewissermaßen natürliche Alliierte; das ist extrem schlecht für deren Geschäft. Wenn man mit denen mal das vertrauliche Gespräch sucht, dann können die da vielleicht eher Auskunft geben oder Indikatoren.

Die letzte Frage, ob die Einschränkungen des BND funktionieren: Wie gesagt, mir sind die zu unscharf. Da ist auch überhaupt gar nicht definiert, was wir überhaupt wollen, was der BND tut und was er nicht tut. Da ist dringender Nachholbedarf sowohl in den Formulierungen als auch in der Aufstellung der Kontrollgremien. - Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank, Herr Dr. Gaycken. - Ich glaube, wir haben auch eine sehr hohe Erwartungshaltung an diese Unternehmen in Sachen Kooperation mit diesem Untersuchungsausschuss, auch was die Präsenz gegebenenfalls von Zeugen und Sachverständigen betrifft. Ich sehe es auch im ureigensten Interesse dieser Unternehmen, mit diesem Untersuchungsausschuss zusammenzuarbeiten.

Herr Rieger, ich darf Ihnen das Wort zur Beantwortung der Fragen geben.

Sachverständiger Frank Rieger: Zur Frage „Tut die Politik genug, um Vertrauen wiederherzustellen?“: Ich würde die mal zusammenziehen mit der Frage nach De-Mail und der Frage „Hat der Staat denn nicht ein Interesse daran, auf Kommunikation im Zweifel zugreifen zu können?“. Das ist tatsächlich eines der inhärenten Probleme dieser momentanen Diskussion: dass der Staat - und zwar egal ob jetzt die USA oder Großbritannien oder Deutschland - aufgrund der vergangenen Geschehnisse kein Vertrauen mehr genießt. Es gibt irgendwie zwei Wege, Vertrauen herzustellen: Entweder man tut lange Zeit das Richtige; dann glaubt man einem, dass man auch in der Zukunft das Richtige tun wird. Oder es gibt tatsächlich Motivationen, die mit denen der Bürger und der Nutzer übereinstimmen. Beides ist, insbesondere was staatliche Stellen angeht, eigentlich nicht mehr der Fall, was irgendwie das Vertrauen angeht.

Ich präferiere da tatsächlich eine andere Lösung als zu sagen: Der Staat muss sich jetzt wieder Vertrauen erarbeiten. - Wir haben in der deutschen Geschichte eine Lösung für dieses Problem, nämlich öffentlich-rechtliche Institutionen. Die sind momentan etwas, sagen wir mal, verharzt und ein bisschen schwierig zu managen, aus der Geschichte. Aber die grundsätzliche Idee einer öffentlich-rechtlichen Institution, also einer Institution, die weder Unternehmen noch Staat ist - - wäre zum Beispiel für so was wie ein „clean slate“-Programm, wo man hingeht und sagt: „Okay, wir müssen mal größere Teile der IT-Infrastruktur neu bauen“, und: „Wir müssen mal Software bauen, die vertrauenswürdig ist“, und: „Wir müssen staatlich geförderte Open-Source-Programme haben“. Ich denke, dass so was wie ein Neuerfinden des Begriffs öffentlich-rechtlich, also eine neue Institution zu schaffen, die in ihrer demokratisch kontrollierten - und zwar direkt kontrollierten - Struktur nicht der Staat an sich ist mit seinen Sicherheitsbehördeninteressen, der zu präferierende Ansatz ist. Ob das durchsetzbar ist, weiß ich nicht; ich fände es nur sinnvoll, irgendwie darüber nachzudenken, insbesondere vor dem Hintergrund genau dieser Vertrauenskrise sowohl in die Technologie als auch in die Institutionen, die - wenn wir sie nicht beheben und dann nicht Lösungen finden, die zu umgehen - tatsächlich das Problem noch immer schlimmer machen wird.

Die Sicherheitsbehörden sind in den Diskussionen zu diesen Themen immer präsent; sie bringen immer ihre Interessen vor, bis hin zu Vertretern der Polizeigewerkschaft, die öffentlich daherfaseln, dass sie sich ja auch solche Überwachungsmethoden wie die NSA wünschen. Wenn wir Beamte haben - das ist dokumentiert in der Presse; das können Sie lesen -, die solche Dinge fordern, dann ist mein Vertrauen null. Da kann ich dann leider irgendwie kein Vertrauen entwickeln dahin, dass die Abwägung der legitimen Strafverfolgungsinteressen versus der Interessen der Bürger immer zur richtigen Seite ausschlägt.

Wir haben ein Urteil des Verfassungsgerichts zum Thema Vertrauenswürdigkeit/Integrität informationstechnischer Systeme. In dem wird ausdrücklich das digitale Selbstverteidigungsrecht des Bürgers etabliert; das heißt, wir dürfen verschlüsseln. Ich sehe es durchaus als Aufgabe des Staates, den Bürger in genau diesem Recht, was ja ein etabliertes Grundrecht ist - das muss man mal klar sagen: Im Gegensatz zum dahergefaselten Supergrundrecht auf Sicherheit handelt es sich beim Grundrecht

auf Vertraulichkeit und Integrität informationstechnischer Systeme um ein etabliertes Grundrecht -, zu unterstützen. Insofern ist die Frage, wo der Staat da seine Priorität setzen sollte, aus meiner Sicht klar. In der Praxis ist es so, dass Strafverfolgungsbehörden ein großes Arsenal an Möglichkeiten zur Verfügung steht. Ich persönlich weiß von Fällen, wo, insbesondere wenn Kriminelle Verschlüsselungsprodukte eingesetzt haben - - die wiederum dazu führten, dass die Strafverfolger damit zu den Staatsanwälten und zu den Richtern gegangen sind und Genehmigungen für eskalierende Ermittlungsmaßnahmen, sprich: irgendwie Einbringen von Raumüberwachung und ähnlichen Dingen, bekommen haben. Das heißt also, es gibt da durchaus Wege und Mittel, zum Beispiel auch Verschlüsselung zu umgehen im Einzelfall, wenn es denn sein muss, und das ist auch okay.

Genauso stellt sich die Frage „Wissen über Exploits, die nicht geschlossen werden“ dar. Wir haben in Deutschland zum Glück die Situation, dass das BSI mittlerweile eine relativ gute Trennung von den Diensten hat. Ob sie jetzt schon hundertprozentig abgeschlossen ist, kann ich nicht beurteilen. Es bleibt aber das Problem, dass es als nachgeordnete Behörde des Innenministeriums nie ein hundertprozentiges Vertrauen haben kann. Wenn man da anfängt, an der Architektur zu bauen, würde ich dringend empfehlen, das BSI aus dem Verantwortungsbereich des Ministeriums, das für die Sicherheitsbehörden zuständig ist, zu lösen, um dafür zu sorgen, dass es da keinen, nicht einmal den Anschein eines Interessenkonfliktes gibt, was das Wissen um Angreifbarkeiten angeht.

Die NSA ist in einer anderen Position: Da sind Angriff und Verteidigung in derselben Behörde versammelt. Dementsprechend gibt es da auch diese Konfusion; dementsprechend gibt es auch die Beeinflussung von Kryptostandards, um die Angreifer zu bevorzugen.

Zur Frage „Hätte es technische Möglichkeiten zur Aufdeckung gegeben?“: Also, wenn Sie auf Ihrem zweiten Arbeitsplatz, dem Reichstag, mal nach oben in die Kuppel laufen und rüber zum Adlon gucken, da sehen Sie seit 2003 den Radom auf der britischen Botschaft. Das ist eine Antennenkuppel, die steht in der britischen Botschaft. Das heißt, Sie hätten von Ihrem Arbeitsplatz direkt schräg rüber guckend genau sehen können, dass da abgehört wird, und zwar offensichtlich: Das sieht aus wie ein Mini-Teufelsberg da hinten in dem Botschaftsgelände. Die Fotos können Sie auf Google Maps sehen, die können Sie überall - - Sie brauchen einfach nur ins Adlon gehen; dann sehen Sie die auch. Das heißt, natürlich wussten die deutschen Behörden davon, was die Amerikaner und was die Briten treiben. Die haben ja mit denen kooperiert. Selbstverständlich weiß das BSI auch darüber, dass vonseiten der Verbündeten Spionage stattgefunden hat.

Dass eine flächendeckende Überwachung aller Glasfaserverbindungen stattgefunden hat, konnten sie möglicherweise ahnen. Wenn der Verfassungsschutz XKeyscore einsetzt und der BND in diesen Kooperationsprogrammen tätig ist, dann kann ich mir nicht vorstellen, dass die nicht in der Lage gewesen wären, zu extrapolieren, was im Rest der Welt stattfindet; das ist völlig unplausibel. Ich halte die dort arbeitenden Menschen nicht für doof. Insofern glaube ich schon, dass sie sich Gedanken darüber machen, was die Verbündeten tun. Insofern gehe ich schon davon aus, dass es technische Möglichkeiten zur Aufdeckung gegeben hätte.

Wir haben ja auch in Einzelfällen durchaus davon erfahren. Ich erinnere zum Beispiel nur an die Aufdeckungen, die vor 2000 passiert sind, zum Echelon-Programm, wo wir den Bericht ans Europaparlament hatten, in dem eigentlich das, was im Vor-Internet-Zeitalter passiert ist, in genau derselben Flächendeckung, in genau derselben Intensität und mit genau demselben Wir-wollen-alles-sehen-Ansatz schon dokumentiert wurde. Das heißt also: Das hätte man sehen können.

Zur Frage „Was passiert in diesen ganzen Programmen?“: Ich will noch mal deutlich darauf hinweisen: Diese Codewords sind irreführend. Es ist sehr empfehlenswert, wenn man sich damit beschäftigt, sich auf die sogenannten SIGADs zu konzentrieren; das sind diese Nummern, also zum Beispiel - - Mein Kollege Andy Müller-Maguhn betreibt auf buggedplanet.info eine Übersicht über die bekannten SIGADs. Da kann man sich viel besser ein örtlich verortetes Bild machen, was wo angezapft wird, an welchen Örtlichkeiten welche Zugänge in welchen Ländern gelegt werden, weil alles, was da drüber

passiert in diesen ganzen Programmen, sind nur Zusammenfassungen.

Nehmen wir zum Beispiel Mystic - wenn Sie nach meinem Lieblingsprogramm fragen -: Mystic ist ein Programm, was diesen sogenannten Full Take aller Telefondaten in mehreren Ländern durchführt, also eben alle Telefondaten wegspeichert und analysiert, für 30 Tage oder mehr, also auch die Inhalte, nicht nur die Metadaten, besteht aber aus mehreren Örtlichkeiten. Das Programm alleine sagt Ihnen wenig; aber wenn Sie wissen, dass es in diesem, diesem und diesem Land passiert, dann können Sie daraus politische Schlussfolgerungen ableiten. Deswegen noch mal der Hinweis: Konzentrieren Sie sich auf die SIGADs, nicht so sehr auf die einzelnen Programmnamen.

Die Frage „Schengen-Routing versus Safe Harbor“: Das sind in gewisser Art und Weise natürlich zwei Ausdrücke desselben Problems. Wir haben ein globales Netz, wir haben globale Dienste, und wir müssen uns überlegen: Welche Schutzmechanismen können wir etablieren? Safe Harbor sollte aus meiner Sicht so bald wie möglich beendet werden, aus dem einfachen Grund, weil es offensichtlich schon in der kommerziellen Praxis nicht funktioniert. Wenn wir den Zugriff der Geheimdienste auf die Daten bei den Unternehmen und Behörden in den USA ansehen, ist auch vollkommen klar, dass es dann nicht mit den deutschen/europäischen Datenschutznormen vereinbar ist, dieses Programm weiter zu fliegen.

Es gibt noch einen weiteren Hintergrund: Wenn wir uns angucken, wie politische, innenpolitische Gestaltung in den USA funktioniert, dann sehen wir, dass gerade die Technologiekonzerne über eine immer größere Macht über die Innenpolitik dort verfügen. Wenn wir wollen, dass sich da was ändert, also dass sich in der amerikanischen Überwachungspraxis was ändert und an der Auswertungspraxis, dann müssen wir die durchaus in die Zange nehmen. Dazu gehört unter anderem, Safe Harbor zu beenden, einfach aus dem Grund, weil die dann nervös werden und anfangen, in Washington Druck zu machen. Das haben wir zum Beispiel gesehen - - Die Änderung, wo die Amerikaner jetzt ein bisschen was gedreht haben, dass sie gesagt haben: „Okay, wir werten Metadaten nicht mehr drei Schritte tief aus, sondern nur noch zwei Schritte tief aus“, ist unter anderem auf Druck von Google und Co. passiert. Insofern bin ich sehr dafür.

Die Fragen von Herrn Ströbele, Vorgehen gegen Verschlüsselungsprodukte: Wir haben dokumentierte Fälle, wo offensichtlich insbesondere Kommunikationsinfrastruktur, die von Herrn Snowden benutzt wurde, nämlich Lavabit zum Beispiel, also verschlüsselte Infrastruktur, mit rechtlichen Mitteln in den USA plattgemacht wurde, wo auf rechtlichem Wege erzwungen wurde, dass Zugang zu Schlüsseln gegeben werden sollte, und zwar pauschal und nicht im Einzelfall. Die Frage, ob man ein solches Rechtssystem, in dem der Staat sich den Zugang zu Verschlüsselung erzwingen kann, als äquivalent zu unserem rechtsstaatlichen System betrachten kann, stellt sich sehr deutlich.

In Großbritannien gibt es ein ähnliches System, was mit dem hier bekannten Verbot der Selbstbelastung völlig inkompatibel ist: Da gibt es den sogenannten RIP Act, nach dem einzelne Personen sogar dazu gezwungen werden können - mit Androhung von Gefängnisstrafen -, ihre Schlüssel rauszurücken, und auch Unternehmen dazu gezwungen werden können, Verschlüsselungsprodukte im Zweifel so anzupassen, dass dies möglich ist.

Dass wir in Deutschland diese Situation nicht haben, sondern dass wir hier eine Industrie haben, die Verschlüsselungsprodukte frei offerieren kann, die auch sicher sind und die hintertürenfrei sind, weil es eben genau diesen Druck von gesetzlicher Seite nicht gibt, ist ein dramatischer Standortvorteil, den wir auf jeden Fall erhalten sollten.

Was die Funktionsfähigkeit der BND-Regulierung angeht, hatte ich schon mal die wesentlichen Punkte genannt, denke ich. Aus meiner Sicht ist der Kernpunkt dabei die Wiederherstellung des Primats der Politik. Wir haben eine Situation, wo der Auslandsgeheimdienst quasi im luftleeren Raum arbeitet, wo die Kontrollsysteme offensichtlich versagt haben, wo der Austausch der Daten mit den Partnerdiensten im Wesentlichen zwischen den Diensten ausgehandelt wird. Sie erinnern sich an den denkwürdigen Satz von Herrn Pofalla, als er den NSA-Skandal für beendet erklärte, wo er sagte, dass die Dienste sich an alle Regeln gehalten haben, die sie untereinander

ausgehandelt haben, wo man sich dann schon fragt: Wo blieb denn da eigentlich die Politik? - Genau diese Frage gilt es zu beantworten, denke ich.

Was die Änderung oder die Zukunft der BND-Regulierung angeht, muss ganz klar das Primat der politischen Kontrolle und ein effektiver Einblick der Kontrollorgane in den Dienst erfolgen, auch auf technischer Ebene. Es gibt in europäischen Nachbarländern durchaus solche Konstrukte, wo es zum Beispiel Befugnisse von Kontrollbehörden gibt, die in alle Daten bei den Geheimdiensten Einblick nehmen können, um zu gucken, ob dort eben - - und zwar von sich aus; die können da einfach hingehen und sagen: Ich hätte gerne mal diese Akte da gesehen - - und nicht, was der Dienst anliefert. Ich denke, so eine ähnliche Konstruktion werden wir hier auch brauchen, um eben das Primat der Politik über die Geheimdienste wiederherzustellen. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für Ihre Ausführungen.

Jetzt haben wir die erste Fragerunde beendet. Wir hätten jetzt die Möglichkeit für eine zweite, weitere Fragerunde. Jetzt frage ich die Fraktionen, angefangen bei der CDU/CSU-Fraktion: Gibt es Bedarf an weiteren Fragen? - Kollege Kiesewetter.

Roderich Kiesewetter (CDU/CSU): Ich möchte an dieser Stelle den drei Experten ausdrücklich danken nicht nur für die hervorragenden Statements, sondern auch die entsprechenden Antworten. Wir haben von unserer Seite keine Nachfragen mehr.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Als Zweite frage ich die Fraktion Die Linke: Haben Sie weiteren Fragebedarf?

Martina Renner (DIE LINKE): Dem Dank schließe ich mich natürlich an. Wir haben auch keinen weiteren Fragebedarf mehr für heute.

Vorsitzender Dr. Patrick Sensburg: Die gleiche Frage würde ich an die Fraktion der SPD richten.

Christian Flisek (SPD): Ich schließe mich auch dem Dank an und verbinde das vor allen Dingen mit einem Lob für die Verständlichkeit der Ausführungen. Herzlichen Dank.

Vorsitzender Dr. Patrick Sensburg: Die Frage geht jetzt an die vierte Fraktion: Bündnis 90/Die Grünen.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich habe hier noch ein paar hundert Fragen aufgeschrieben - - Nein, also für heute - - Ich meine, das ist ein unendlich tiefes Thema, und es war sehr spannend, mit Ihnen heute zu sprechen. Natürlich gibt es noch ganz viele Fragen auch von unserer Seite. Aber ich würde sagen: Nichts hält uns davon ab, im Rahmen der nächsten zwei Jahre - so lange werden wir ja wahrscheinlich unterwegs sein - auch noch mal miteinander hier zusammenzukommen. Für heute ganz herzlichen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Damit, weil keine Fragen mehr aus den Reihen der Mitglieder des Untersuchungsausschusses bestehen, sind wir am Ende der Sachverständigenanhörung.

Nach seiner Fertigstellung wird Ihnen vom Sekretariat das Stenografische Protokoll übersandt. Sie haben dann zwei Wochen Zeit, Korrekturen an der Überarbeitung vorzunehmen oder Richtigstellungen oder Ergänzungen Ihrer Aussagen mitzuteilen; ich hatte Ihnen das ja am Anfang der Sitzung schon gesagt.

Auch ich darf mich ganz herzlich bei Ihnen bedanken. Ich hatte es schon nach den Eingangsstatements gesagt: Ich fand diese Sitzung wirklich beeindruckend, nicht nur, weil sie uns viele Erkenntnisse gebracht haben aus Ihrem Arbeitsbereich, aus Ihrem Kenntnisbereich, die gerade bei technischen Fragen nicht für jeden immer so offensichtlich gegeben waren, sondern weil Sie uns intensiv auch Vorschläge, Ideen und Richtungsweisungen gegeben haben, wie man der aktuellen Probleme und Themen auch Herr werden kann.

Wir alle können unzufrieden sein, dass das passiert, was wir jetzt peu à peu in diesem Untersuchungsausschuss aufdecken. Da können wir aber nicht stehen bleiben. Es ist soeben teilweise vielleicht zu Recht gesagt worden: Es ist nicht ge-

nug getan worden. - Dieser Untersuchungsausschuss muss nach meiner Meinung die Weichen stellen, dass jetzt etwas getan wird, einmal im Schnellen, aber auch langfristig, grundsätzlicher Art. Das Beispiel mit dem Schlauch mit den Löchern, wo das Wasser herausdringt, fand ich sehr anschaulich. Schnelle Pflaster sind eines und auch notwendig, aber eine Grundkonzeption eines stabilen Schlauchs, glaube ich, auch. Von daher ganz herzlichen Dank, dass Sie auch diese Richtungsweise gemacht haben und uns damit helfen, auch in einem dritten Themenkomplex sicherlich Vorschläge zu machen, wie wir zu mehr Datensicherheit für Bürgerinnen und Bürger, aber auch für unsere Unternehmen kommen können, damit diese Dinge abgestellt werden. Also ganz herzlichen Dank an Sie alle dafür, dass Sie uns unterstützt haben.

Die nächste Ausschusssitzung - ich komme jetzt noch nicht auf die unterbrochene Beratungssitzung - findet dann am 3. Juli statt. Zum öffentlichen Teil ist bisher der Sachstand - wenn sich daran nichts ändert -: ab 12 Uhr, mit Vernehmung der Zeugen Drake und Binney.

Damit ist diese Sitzung geschlossen.

Ich würde jetzt eine kurze Unterbrechung von 15 bis 20 Minuten machen, weil auch Kommunikationsbedarf besteht, und würde im Anschluss daran die unterbrochene nichtöffentliche Beratungssitzung wiedereinberufen.

Danke ganz herzlich für Ihre Teilnahme.

(Schluss: 15.05 Uhr)

ANLAGE 1

dargestellt werden, wohl aber davon, in welchem Umfang sie angewandt wurden.

Nun zu Ihrer Frage, wie abgehört werden kann: Das Internet, auf welches ich mich hier konzentriere, ist mit Abstand das wichtigste Kommunikationsnetz - sowohl für die individuelle Kommunikation wie auch als Backbone für praktisch jede Form der Weitverkehrskommunikation, etwa den internationalen Telefonverkehr.

Zu Beginn des Internets in den 1960er-/1970er-Jahren spielte Sicherheit auf Netzwerkebene keine Rolle. Als Folge ist das Internet bis heute ein ungesichertes Netz. Wer Zugriff auf eine Leitung oder einen Netzknoten hat oder sich verschaffen kann, kann dort auch abhören, und zwar ohne jedes Risiko, dass jemand dies bemerken könnte. Besonders kritisch sind die Stellen und Organisationen, über die ohnehin ein großer Teil des Internetverkehrs läuft, also zum Beispiel die internationalen Telekommunikationsanbieter und die Internet Exchange Points.

Das Internet erlaubt einem Angreifer sogar, gezielt interessante Nachrichten über eigene Systeme umzuleiten. Der Angreifer schaltet sich hierbei zwischen Sender und Empfänger und kann so die Kommunikation als Man in the Middle mitlesen. Beispielsweise wurde so 2013 der Internetverkehr innerhalb der amerikanischen Stadt Denver im Bundesstaat Colorado komplett über einen ISP in Island gelenkt und dort vermutlich auch ausgeleitet. Das Internet hat also, bildlich gesprochen, zahlreiche offene Türen, durch die Kommunikation ausgespäht werden kann. Grundsätzlich effektiver, als Spähangriffe lediglich zu verbieten, ist es, sie technisch auch zu verhindern.

Erfreulicherweise kennt die IT-Sicherheit für das beschriebene Abhörproblem auch schon seit langem die Lösung. In der Fachwelt herrscht Einigkeit darüber, dass Ende-zu-Ende-Verschlüsselung das geeignete Instrument ist, das Internet gegen Abhören zu schützen. Ende-zu-Ende-Verschlüsselung bedeutet, dass Nachrichten vom Sender verschlüsselt werden, dann verschlüsselt durch das Netz laufen und erst beim endgültigen Empfänger wieder entschlüsselt werden. Die Ende-zu-Ende-Verschlüsselung ist allen anderen bekannten Ansätzen deutlich überlegen, selbstverständlich auch dem sogenannten Schengen-Routing oder einer Verschlüsselung nur auf den Verbindungen zwischen Servern.

Die flächendeckende Einführung von Ende-zu-Ende-Verschlüsselung setzt aber eine Investition in Vertrauensinfrastrukturen, sogenannte Public-Key-Infrastrukturen, voraus. Solche PKIs sind erforderlich, um die korrekte Zuordnung eines Schlüssels zu einer Person oder Organisation oder auch zu einem Objekt zu gewährleisten. Dadurch kann man zum Beispiel Man-in-the-Middle-Angriffe durch betrügerisch untergeschobene Schlüssel verhindern. Die flächendeckende Einführung von Ende-zu-Ende-Verschlüsselung halte ich für einen ebenso wichtigen Aspekt der Grundversorgung einer digitalen Gesellschaft wie etwa den Breitbandausbau.

Nun zum zweiten Fragenkomplex: Wie lassen sich aus abgehörten Daten relevante Informationen gewinnen? Zunächst möchte ich kurz erläutern, was man unter Inhalts- und Metadaten versteht. Inhaltsdaten sind all die Daten, um die es in einer Kommunikation eigentlich geht, also etwa Bild- und Tonaufnahmen, E-Mails, Webseiten, Anfragen an Suchmaschinen oder auch die vielen Sensordaten aus der Smart Factory oder dem Smart Home. Alle anderen Daten sind Metadaten, also beispielsweise Adressen, Zeitpunkt, Umfang einer Kommunikation, Standorte, aber auch Hilfsdaten zum schnelleren Suchen wie Datenbankindizes und automatisch erstellte Annotationen.

In der Praxis verschwimmen die Grenzen zwischen Inhalts- und Metadaten, und spätestens in der Verarbeitung wird diese Unterscheidung bedeutungslos. Mit zwei Beispielen möchte ich dies illustrieren. Beispiel 1: Medien kann man automatisiert annotieren und dann mit einer effizienten Suche erschließen. Aus Tonaufnahmen kann man automatisiert den gesprochenen Text extrahieren. Aus Bildaufnahmen kann man entsprechend Personen, Orte, teilweise sogar Szenen extrahieren und erkennen. Aus Texten, E-Mails, Webkommentaren kann man die Sprache und diverse Attribute des Sprechenden extrahieren. Aus Inhaltsdaten werden damit Metadaten.

Umgekehrt Beispiel 2: Aus den Verbindungsdaten in sozialen Netzen wie Facebook oder LinkedIn, also aus der Wer-kennt-wen-Beziehung, kann man zu einzelnen Personen Kompetenzen, Vorlieben und Neigungen ableiten und in Profilen speichern. Aus Metadaten werden damit also Inhaltsdaten.

Diese Beispiele zeigen, dass Inhalts- und Metadaten gleichermaßen schützenswert sind. Eine unkontrollierte Auswertung führt zu einem Verlust an Privatsphäre und Vertraulichkeit. Schon das Wissen, dass eine solche Auswertung möglich ist, schränkt die Freiheit und Selbstbestimmung ein. Vorverarbeitungen und Auswertungen, wie ich sie

Ihre nächste Frage ist richtig schwierig, muss ich sagen. Sie haben gefragt - sinngemäß -: Was muss geschehen, damit in Deutschland und Europa ein Markt entsteht? Ich halte das eigentlich wirklich für die wichtigste Frage sogar, weil ich denke, da ist eine Gelegenheit. So ein Markt entsteht typischerweise ja nicht, sondern da ist ein Markt. Und die Frage ist: Wie kann man diesen Markt bedienen, wie kann man ihn gestalten, sodass er für uns eine Möglichkeit ist?

Ich möchte ganz kurz einschieben: Frank Rieger hat, glaube ich, mich in die Ecke geschoben, ich würde nur Großforschung und die Großindustrie fördern. Dem ist natürlich nicht so. Natürlich braucht man sehr viele innovative KMUs, um neue Technologien zu erzeugen. Von daher: Alles, was ich sage, gilt auch für die KMUs.

Ich denke, uns fehlt allerdings tatsächlich auch ein großer Hersteller; darauf komme ich aber gleich zurück. Danach hat auch jemand von Ihnen gefragt.

Wie würde man so einen Markt generieren? Wie gesagt: Zum einen: Das Grundbedürfnis nach IT-Sicherheit existiert. Die Frage ist: Wie kann man es so gestalten, dass man es erstens bedienen kann - und dass wir es bedienen können, also „wir": Europa, Deutschland? Was dafür, glaube ich, ganz essenziell ist, ist, dass man an der Stelle vernünftige Standards schafft, die zu mehr Sicherheit führen. Deswegen habe ich so viel Wert darauf gelegt, dass man europäische Standards schafft, die über alle Zweifel erhaben sind.

Wichtig ist: Wer Standards schafft, hat typischerweise einen Technologievorteil - typischerweise. Wenn Sie sich angucken, wie Standards gemacht werden: Heutzutage werden Standards selten in den großen ISOs gemacht, von den nationalstaatlichen Organisationen, sondern Standards werden von Firmen getrieben, die sich davon Vorteile versprechen, und die haben die auch.

Damit man diese Vorteile umsetzen kann, ist es wiederum wichtig, denke ich, dass man erstens die Technologien schafft - deswegen ist Forschung so wichtig, deswegen ist Entwicklung so wichtig -, aber auch, dass man in der Vergabe von Aufträgen der öffentlichen Hand beispielsweise oder durch Haftungsfragen sicherstellt, dass wirklich auch diese Dinge eingesetzt werden müssen.

Ich hatte ja erwähnt, dass tatsächlich erstaunlich wenig passiert, wenn man alleine dem Markt die IT-Sicherheit überlässt. Ich habe jetzt die Zahlen nicht hier, aber sinngemäß: Selbst bei solchen elementaren Dingen wie Firewalls, wo man jetzt wirklich sagen würde: „Sie helfen vielleicht nicht furchtbar viel, aber sie helfen ein bisschen was", gibt es das. Ich glaube, so was wie 15 Prozent aller Unternehmen sind ohne Firewalls, also ohne Netzwerk-Firewall. Das zeigt sozusagen: Da werden Innovationen nicht so schnell angenommen wie üblicherweise.

Die Innovationsgeschwindigkeit kann man, wie gesagt, erhöhen durch Vergaberichtlinien, also dass einfach Standards, die gesetzt werden, von der öffentlichen Hand auch umgesetzt werden müssen, und durch Dinge wie Gefährdungshaftung, was jetzt nicht mein Thema ist; ich bin ja Techniker, kein Jurist. Aber ich denke auch, da könnte man einiges tun, um die Sachen voranzubringen.

Der zweite Teil, den ich erwähnen wollte, ist: Wir müssen auch schauen - und da ist ein Riesenmarkt für Europa -, dass wir die Produkte, die nicht in Europa hergestellt werden, trotzdem verwenden können. Ich bin ein großer Verfechter davon, dass es einen Riesenmarkt geben kann für uns. Aber wir werden nie unabhängig werden von Technologie aus anderen Ländern. Das Problem ist einfach zu groß, und ich denke, wir müssen daran denken: Wir sind eine exportorientierte Nation. Wenn wir uns von dem Rest der Welt abkoppeln, ist das, glaube ich, nicht sehr vorteilhaft für unsere Wirtschaft. Also wir wollen international Dinge integrieren können.

An der Stelle muss man investieren in die Fähigkeit, zu überprüfen, und auch das ist wiederum ein großer Markt. Also wenn Sie beispielsweise mit potenziellen Anwendern im Nahen Osten reden oder sonst wo - also in manchen Gegenden dieser Welt -, die die gleichen Probleme haben wie wir: Ich glaube, die würden voller Freude Produkte aus Deutschland, aus Europa nehmen und Testmethoden, wenn wir sagen: Nach diesen Methoden können wir darauf vertrauen, dass, wenn wir Produkte integrieren, die sozusagen hinreichend okay sind. - Gut, also soweit vielleicht mal zu diesem Punkt.

Die nächste Frage war von Herrn Kiesewetter, wie Ende-zu-Ende-Verschlüsselung einzuschätzen ist - gegeben, dass es ja auch noch Metadaten gibt und andere Dinge. Da muss man ganz klar sagen: Ende-zu-Ende-Verschlüsselung ist das Mittel der Wahl gegen Massenüberwachung durch Abhören auf Leitungen in Netzknoten - also alles, was zwischen den Enden passiert.

Es gibt darüber hinaus natürlich Metadaten, die fallen trotzdem an. Also einfach: Wer redet mit wem? Da sieht man trotzdem die klassischen Verbindungsdaten. Auch dagegen kann man sich

Vorschriften, dass man da was kaufen kann, sondern es muss ja auch jemanden geben, der das Zeug wirklich produzieren kann.

Es gibt sehr viele Diskussionen dazu, dass man solche Dinge machen möchte wie vertrauenswürdige Plattformen, also eine vertrauenswürdige Plattform für Industrie 4.0 beispielsweise, was Herr Gaycken vorhin angesprochen hatte. Das kann man sehr schnell tun, wenn man die Ressourcen da reinsteckt. Also, die Innovationszyklen in der IT unterschätzt man oft. Das sind so was wie vier, fünf Jahre; dann hat man so was. Das ist nicht lange; aber es ist eine horrende Investition, die über die Kraft von einzelnen KMUs hinausgeht. Deswegen denke ich, man braucht einen Zusammenschluss von mehreren. Ob das jetzt, wie Airbus, der Zusammenschluss der ganzen europäischen Industrie ist, weiß ich nicht - eher unwahrscheinlich -, ob es eine Föderation ist, also eine Stiftung oder eine Genossenschaft oder so was, dazu kann ich nicht viel sagen. Aber es gibt Mechanismen, die kritischen Maße zusammenzuziehen, die man braucht, um wirklich sichere Systeme zu bauen.

Abschließend möchte ich nur ganz kurz zur Ehrenrettung der SAPs und aller anderen Firmen, die Sandro die ganze Zeit als schlechtes Beispiel genommen hat, sagen: Also, natürlich ist es nicht so, dass jeder Entwickler in einer Firma, der eine Tastatur hat, jeden beliebigen Code ändern kann. Es ist in der Tat so, dass es so was wie 300 Millionen Zahlen gibt und mehrere 10 Millionen Zahlen Codes in allen großen Programmen. Dementsprechend kann man hochrechnen: mehrere Tausend Schwachstellen, die man ausnutzen kann. Aber es hat sehr, sehr viel schon stattgefunden.

Ich möchte auch mal positiv erwähnen: Also, seitdem wir uns mit diesem Thema beschäftigen - Security and Privacy by Design - und seit den NSA-Enthüllungen ist die Bereitschaft gerade bei großen Firmen wie SAP, Prozesse einzuführen, um die Qualität nach oben zu treiben, Kontrollen einzuführen, gerade auch mit Open Source Code besser umzugehen und so, dramatisch nach oben gegangen. Also, es gibt furchtbar viel zu tun; aber man darf nie in Pessimismus verfallen. Das hilft niemandem. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ich glaube, jetzt sind alle Fragen beantwortet, und auch alle Kollegen nicken. Es wäre schon fast bizarr, wenn die NSA dazu beigetragen hätte, dass sich hier ein dementsprechend großer Markt entwickelt, dass sich „Security like in Germany" oder europäische Standards entwickeln. Allein wenn man mal sich vorstellt, welches volkswirtschaftliche Volumen die Vorschläge, die gerade diskutiert werden, haben, dann kann man, glaube ich, erkennen, wie groß dieses Thema ist. Also, ich finde das unheimlich beeindruckend.

Ich möchte jetzt zur nächsten Fraktion kommen und Ihnen, liebe Kolleginnen und Kollegen von der Fraktion Die Linke, Gelegenheit geben, Fragen zu stellen. Frau Obfrau Renner.

Martina Renner (DIE LINKE): Danke, Herr Vorsitzender. - Mein Dank natürlich zuerst auch mal an Sie, meine Herren Sachverständige, auch für Ihre schriftliche Zuleitung der Gutachten.

Ich will am Anfang eine allgemeine Frage stellen und dann zu vier technischen Details einzelne Fragen noch mal an Sie richten.

Die allgemeine Frage schließt sich an eine Eingangsbemerkung von Professor Waidner an. Er sagte, er will referieren zum Stand der Schwarzen Kunst bei der Überwachung des Internets. Was mich so umtreibt, ist eigentlich: Wie halte ich denn die Hexenmeister der Schwarzen Kunst von dem fern, was Sie dann jetzt alle an möglichen technischen, politischen und rechtlichen Schlussfolgerungen formuliert haben, Ende-zu-Ende-Verschlüsselung und all dem, was wir hier diskutieren? Ich frage das vor dem Hintergrund vieler Einzelbefunde, die wir ja auch in den letzten Wochen und Monaten in der Presse gesehen haben, die wir in den Akten sehen, die wir diskutieren.

Eine Behörde, die zum Beispiel mit diesen Fragen befasst ist - das BSI, das Bundesamt für die Sicherheit in der IT-Technik -, kooperiert mit der NSA. Wir hatten die letzten Tage - ich würde es fast so sagen - den Skandal, dass eines der Unternehmen, die schon sehr lange im Verdacht stehen, ich sage mal, Schnittstellen für Geheimdienste zur Verfügung zu stellen - Verizon -, nicht nur den Bundestag zum Teil bedient, sondern auch Landtage und Bundesbehörden. Sie sprachen davon, Herr Rieger, Experten wechselten die Seiten. Oder: Herr Gaycken sagte, der Dienst sei auch in der Lage, zum Beispiel in Firmen Leute einzuschleusen, und dann nannten Sie SAP. Das Beispiel war ja beliebig. Es ging ja nicht um SAP, sondern insgesamt um die Problematik.

Das heißt, wie halte ich die Hexenmeister der Schwarzen Kunst von alledem fern, was wir hier diskutieren, was unser aller IT-Sicherheit - der Bürger und Bürgerinnen, der Unternehmen, der Exekutive, der Parlamente - erhöhen würde? Da sehe

darf und nicht alles neu in epischer Breite beantworten muss.

Zu Ihrer ersten Frage, Herr Flisek - ob diese 20 Prozent ein sinnvolles Maß sind -, kann ich nichts ergänzen. Das ist natürlich ein relativ unsinniges Maß. Was ich aber betonen möchte: Wir reden sehr viel über die Fragen „Wie viel darf man ausleiten?“ oder „Kann man Glasfaserkabel abhören?“ oder irgendwas in dieser Art. Natürlich würde diese Frage komplett verschwinden, wenn man Ende-zu-Ende-Verschlüsselung hätte - also sozusagen noch mal das Plädoyer dafür. Es ist nicht so furchtbar wichtig, wie viel ausgeleitet wird. Es ist nicht so furchtbar wichtig, was man abhören kann und wie man es abhören kann. Es gibt die Gegenmaßnahme, und die Priorität sollte sein, einfach die Gegenmaßnahme umzusetzen; dann verschwindet das Problem komplett, und man hat gleichzeitig die Motivation für das, was Sandro Gaycken gerade vorhin gesagt hatte: eine gewisse Motivation für die Nachrichtendienste, etwas kreativer und datenschutzfreundlicher vorzugehen. Mehr will ich dazu gar nicht sagen.

Zu Ihren Fragen „Ist ein Full Take realisierbar?“ und „Wie entstehen sozusagen Nadeln?“ oder „Wie findet man diese Nadeln?“ wurde auch schon fast alles gesagt. Was man, glaube ich, rein technisch einfach wissen muss: Die Frage ist: Kann man das Internet auf Jahre hinaus speichern oder nicht? Das ist technisch betrachtet wiederum keine sehr interessante Frage, sondern eine interessante Frage wäre gewesen: Wenn ich diese Daten habe: Kann ich sie jemals wieder verwenden? Man kann natürlich problemlos beliebig große Speicherzentren aufbauen. Facebook baut gerade ein riesengroßes Rechenzentrum mit einem Exabyte Speicherkapazität. Es gibt Gerüchte - die ich für etwas übertrieben halte -, dass die NSA ein Yottabyte speichern kann; das ist wirklich ziemlich viel. Das Problem ist: Die werden das Ding nie wieder einlesen können; das ist das Problem dabei. Man kann leicht speichern. Das große Problem in Big Data ist an und für sich, möglichst schnell alles loszuwerden, was man nicht speichern möchte und auch nie wieder angucken möchte, und darin, sozusagen in diesem Fluss von Daten, möglichst schnell das Richtige zu finden.

Ich habe keine Insiderinformationen zu XKeyscore. Wenn ich mir aber angucke, wie die Folien aussehen zu XKeyscore, und ich mir ansehe, wie normale, kommerzielle Produkte aussehen in diesem Bereich, dann gehe ich mal davon aus: Die werden ziemlich ähnlich sein; diese Interfaces sehen einfach extrem ähnlich aus. Und die sind alle darauf angelegt, dass man möglichst schnell alles loswird, was man nicht braucht, dass man in Realzeit nach diesen Nadeln sucht und nicht etwa in für irgendwelche Ewigkeiten gespeicherten Daten. In diesem Sinne ist es plausibel, dass XKeyscore auf ein paar wenige Tage von Full Take zurückgreift; das reicht aber dann vermutlich auch. Von daher: Man muss da sozusagen mehr auf die Verarbeitung achten, weniger auf die Speicherung.

In diesem Sinne ist auch wirklich wiederum sehr wichtig, sich klarzumachen, dass Metadaten eben auch in der Vorverarbeitung von anderen Daten entstehen; das hatte ich in meiner Einleitung schon gesagt. Aber Metadaten haben, wie Herr Rieger gesagt hat, den großen Vorteil, dass man effizient darin suchen kann, und man kann in dieser großen Flut von Nachrichten - so ähnlich wie man Spam als Spam entdeckt -, in diesen E-Mails auch nach anderen interessanten Dingen suchen. Man kann sie annotieren, man kann Videosequenzen annotieren, man kann sozusagen gucken, dass man diese Dinge beschreibt. Dann suche ich in der Beschreibung, nicht mehr in den sehr komplexen, sehr voluminösen Daten. So funktionieren diese Dinge dann typischerweise auch tatsächlich real: also eine lange Vorverarbeitung mit Annotationen, und dann suche ich nur noch in den Annotationen.

Dann hatten Sie gefragt zur Frage der öffentlichen Ausschreibung. Ist ja schön und gut; aber wenn wir so hohe Standards setzen, dass niemand mehr die Ausschreibung bedienen kann, dann ist auch nichts gewonnen. Das ist natürlich eine absolut wahre Aussage. Man muss an dieser Stelle natürlich realistisch sein. Also, es ist sehr wichtig, eine vernünftige Strategie zu haben, wie man das Niveau langsam nach oben schraubt. Man darf nicht sofort das Maximum verlangen, sondern man muss mit dem Stand der Technik nach oben gehen.

Das geht auch ein bisschen in die Richtung der Frage von Frau Mittag, was vernünftige Zeithorizonte wären und wie man diese langen Fristen sinnvoll verwenden kann. Diese langen Fristen sind erstens, denke ich, keineswegs zehn bis fünfzehn Jahre. Ich höre das immer wieder. Ich weiß nicht, ob gerade jemand auswendig weiß, wann das iPhone eingeführt wurde oder so was; aber gefühlt - man redet immer von Jahrzehnten - - Aber Google gibt es vielleicht so etwas wie zehn Jahre, bisschen länger. Das iPhone gibt es so was wie fünf oder sechs Jahre. Die Innovationszyklen sind

Es könnte ein leichteres Problem sein, wenn man mehr Fokus darauf setzen würde. Usability, gerade im IT-Sicherheitsbereich, war über mindestens zehn, fünfzehn Jahre kein großes Thema in der IT-Sicherheitsindustrie. Deswegen kommen diese bekannten Abfragen, auf die Sandro Gaycken angespielt hat: dass arme Benutzer gefragt werden, irgendwelche Entscheidungen zu fällen, die sie nicht fällen können. Deswegen, beispielsweise, sind Systemadministratoren regelmäßig überfordert, mit ihrer Usability umzugehen. Die Interfaces, die wir als Endnutzer sehen, sind typischerweise schon sehr gut verständlich verglichen mit den Interfaces, die man dem normalen Systemadministrator vorsetzt. Da ist ein horrendes Potenzial, besser zu werden, auch weil es einen ziemlich einfachen Grund gibt, warum die Usability von Sicherheitssystemen relativ schlecht ist: Das liegt einfach daran, dass IT-Sicherheit lange Zeit pur auf Compliance abgehoben hat. Wenn Sie als IT-Sicherheitsfirma jemandem etwas verkaufen wollten, dann war es nicht wichtig, was die Benutzer davon halten, sondern ob Sie eine bestimmte gesetzliche Vorgabe eingehalten haben oder nicht. Dementsprechend hat man alles darauf hingetrimmt, dass sozusagen an den richtigen Stellen die richtige Warnung hochgepoppt ist und die richtige Frage gestellt worden ist. Aber man hat keine Hilfestellung zur Verfügung stellen müssen, weil das war nicht Teil der Compliance. Deswegen denke ich, wir haben es jetzt in der Hand, sinnvollere Regelungen zu machen, dass man mit diesem Ansatz nicht weiter durchkommt, sondern wirklich benutzbare Systeme entwerfen kann. Aber das halte ich wirklich für ein Problem, das man in den Griff kriegt, wenn man einfach mehr Fokus darauf hat.

Dann zu den Fragen „Einschätzung Industriespionage“ und „Was passiert real?“ und „Wie schätzt man das alles ein?“. Da kann ich, glaube ich, nicht sehr viel mehr dazu beitragen, als meine beiden Kollegen links und rechts schon gesagt haben. Was ich betonen möchte, ist aber: Wenn Sie mit Vertretern amerikanischer Firmen reden, dann ist es tatsächlich so: Diese Firmen sind entsetzt. Das ist, glaube ich, auch nicht gespielt. Sie fühlen sich tatsächlich auch betrogen. Das mag jetzt daran liegen, dass eine Firma eben keine holistische Sache ist: Es kann ohne Weiteres sein, dass ein Teil dieser Firmen durchaus wusste, was passiert; ein großer Teil wusste es vermutlich nicht. Was es aber für uns bedeutet, ist eben: Wenn wir so was machen, wie unsere Standards in Europa entwickeln, wenn wir Technologien entwerfen, um die Überprüfbarkeit von Systemen zu verbessern - - Wir können mit diesen Firmen zusammenarbeiten, wir müssen mit diesen Firmen zusammenarbeiten. Ich denke, digitale Souveränität wird nicht heißen, dass wir alles in Europa oder Deutschland machen, sondern das heißt, dass wir eben sinnvoll mit Firmen in den USA, in wo auch immer zusammenarbeiten, dass dort unsere Standards für die Überprüfbarkeit akzeptiert werden, dass die unterstützt werden und - - Einer von meinen beiden Kollegen hat das gesagt: Das sind zurzeit eigentlich unsere natürlichen Verbündeten. Ich denke, da rennen wir offene Türen ein.

Eine Grenze zwischen IT-Sicherheitsfirmen und IT-Firmen würde ich tatsächlich nicht ziehen. Man muss sich einfach mal im Klaren darüber sein: So eine Firma wie RSA wird gerade immer sehr hoch gehoben, weil sie ertappt worden ist. RSA ist eine kleine Division einer Firma namens EMC; das ist einer der größten Hersteller von IT überhaupt und einer der Marktführer im Bereich Speichertechnologien, also Platten und so Zeugs. Von daher: Man kann es nicht auseinanderhalten, es betrifft wirklich alle Firmen. Das unterstützt auch ein bisschen meine These, dass man sagen muss: Wenn man mit Firmen wie eben EMC oder Intel oder so was konkurrieren möchte, dann braucht man in Europa halt auch Firmen von diesem Kaliber. Deswegen noch mal vielleicht die Erklärung, warum ich nicht nur KMUs, sondern auch wenigstens ein oder zwei Firmen in Europa haben möchte, die eben mit solchen Riesen mithalten können und dann auch relativ schnell so was wie Industrie-4.0-Plattformen (akustisch unverständlich) hochziehen können.

Letzter Punkt: Ich unterstütze völlig, was Sandro Gaycken angesprochen hatte: dass man die hohen Safety-Standards, die man im Bereich von Flugzeugen und Ähnlichem kennt, auch auf IT-Sicherheit überträgt. Das ist zurzeit auch ein großes Thema in allen Standardisierungsdiskussionen zu Industrie 4.0, ist ein europäisches Thema. Das ist alles nicht so furchtbar einfach; aber ich kann auch da wiederum nur sagen: Industrie 4.0 ist sehr viel größer. Wenn ich Safety-Standards übertragen kann für eine Fabrik, habe ich noch nicht Safety für die Industrie 4.0 - Industrie 4.0 ist übergreifend.

Jetzt habe ich, glaube ich, alles beantwortet, was ich beantworten wollte. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank für Ihre Ausführungen.