Deutscher Bundestag
14. Wahlperiode

Protokoll 14/**13**

Ausschuss für Kultur und Medien
Unterausschuss „Neue Medien“

Wortprotokoll

13. Sitzung (öffentliche Anhörung)

Berlin, den 5. Juli 2001, 15.00 Uhr
(Plenarbereich Reichstagsgebäude, Sitzungssaal 3 N 001)

Vorsitz: Abg. Jörg Tauss, MdB (SPD)

Öffentliche Anhörung zum Thema: Cyber-Crime/TKÜV

Vorsitzender: Meine sehr verehrten Damen und Herren, ich darf Sie recht herzlich zur Sitzung des Unterausschusses „Neue Medien“ begrüßen. Wir haben die heutige Unterausschuss-Sitzung in einem etwas anderem Rahmen als gewöhnlich, nicht nur was die Räumlichkeiten angeht. Wir bedanken uns herzlich bei der CDU/CSU-Bundestagsfraktion für ihre Gastfreundschaft, in deren Räumen sind wir nämlich. Wir haben, glaube ich, die dicht besuchteste Unterausschuss-Sitzung seit Bestehen des Unterausschusses, der jetzt auch mehr als ein Jahr alt ist. Dies zeigt mir ganz deutlich, dass doch über das, was wir heute diskutieren, Cyber-Crime/TKÜV, Diskussionsbedarf vorhanden ist. Was ich mir abends alles anhören muss, wenn ich E-Mails bekomme, was ich an Überwachungsstaat hier als Parlamentarier alles einrichte und mich in der Regel gar nicht so richtig schuldig fühle, weil ich von vielem, was mir vorgeworfen wird, auch gar nichts weiß. Deshalb haben wir also gesagt, gut, dies ist der richtige Anlass, um hier auch einmal ein Expertengespräch stattfinden zu lassen. Ich glaube, wir haben schon zu konstatieren, dass es in diesem Bereich eine sehr harte Auseinandersetzung gibt. Wir haben es als Politikerinnen und Politiker mit wachsenden Befürchtungen zu tun, dass Datenschutz und informationelle Selbstbestimmung gerade im Internet durch das, was an Kriminalitätsbekämpfung vorgesehen ist, nun doch ein Stück weit sehr stark beeinträchtigt sind. Umgekehrt muss man sich natürlich um Fragen der inneren Sicherheit, um Entwicklung von Kriminalität Gedanken machen. Wir wollen selbstverständlich genauso wenig wie auf den Marktplätzen Kriminalität im Internet, aber ich sage immer, so wie es auf den Marktplätzen Kriminalität gibt, wird es sie möglicherweise auch im Internet geben.

Aber man muss sich mit der Frage beschäftigen: Was kann man tun? Emotionalisiert wird die Diskussion sicherlich. Ich zitiere jetzt aus HDI-Nachrichten der letzten drei Wochen, wo ein Vertreter des Bundeskriminalamtes gesagt hat: „Datenschutz ist Täterschutz“. Solche Äußerungen führen natürlich dann dazu, dass die Befürchtungen wiederum, die damit verbunden sind, auch sehr stark zunehmen. Was wir festgestellt haben ist allerdings, dass es sehr wenig Dialog gibt, hier in diesem Lande. Übrigens auch sehr wenig Dialog im europäischen Bereich. Es gibt ganz unterschiedliche Szenen. Es gibt auf der einen Seite die Szene, die sich berechtigt Sorgen um Entwicklungen im Internet – auch was die Kriminalität angeht – macht. Die zweite Seite, die Seite, die ich geschildert habe, die aus der bürgerrechtlichen Seite, aus der Verfassungsseite kommt, die sagt, hier müssen wir aufpassen, dass das Kind nicht mit dem Bade ausgeschüttet wird, sonst laufen wir Gefahr, dass wir von der Kriminalitätsbekämpfung bis hin zu unsichtbaren Netzen noch große Probleme bekommen werden. Beispielsweise durch Einbruchstellen, die wir für Polizeidienststellen schaffen, nach dem Motto, wo die Polizei von Castrop-Rauxel hineinkommt, kommen natürlich auch jederzeit der amerikanische NSA oder Wirtschaftskriminelle oder Hacker aller Schattierungen hinein. Also,

dies ist ein Stück weit das, was an Diskussion auch polarisierend geführt wird. Was wir festgestellt haben ist, dass man in diesen Szenen sehr viel über einander redet, aber leider sehr wenig miteinander redet. Ein kleines Aha-Erlebnis war für mich vor einigen Wochen in Bonn, als Frau Walter sich mit dem Wirtschaftsministerium zusammengesetzt hat, aus dem auch heute einige Vertreter zu begrüßen sind. Herr Wagner war dabei, als dann festgestellt wurde, ja lasst uns doch einmal zusammensitzen und die technischen Fragen miteinander diskutieren. Ich glaube, solche Zirkel sind sinnvoll und erfolgreich. Wenn wir einen solchen Dialog führen und dazu einen Beitrag leisten können, auch als Unterausschuss, dann freue ich mich sehr darüber, dann wäre dieses Ziel, das wir hier miteinander verfolgen, erreicht.

Was den Sitzplan angeht - ich habe es nicht genau im Blick, Herr Speer, Sie haben alles im Griff -, die Herren und Damen sitzen so, wie auch niedergeschrieben. Gut ! Sollte sich jetzt jemand illegal gesetzt haben, dann wird es problematisch. Ich beginne auf der linken Seite, dort haben wir heute das Bundeskriminalamt angesiedelt. Entschuldigung, das BKA ist heute verhindert und wird durch die übergeordnete Behörde vertreten, in diesem Fall durch Herrn Akmann und Herrn Reisen vom BMI, die dann aber auch sagen, zu welchen Teilen der Fragen sie Stellung nehmen wollen und können. Vielen Dank, dann direkt anschließend Frau Pernice vom Deutschen Industrie- und Handelstag. Sie hat sich immer auch um Fragen von ENFOPOL und diese Dinge aus wirtschaftlicher Sicht gekümmert, die Wirtschaft hat ja auch Sorgen, was die finanzielle Seite der Medaille angeht, die ich heute noch gar nicht angesprochen habe. Auch hier, Frau Pernice, gibt es eine Zweiteilung, zu einem anderen Themenkomplex wird dann Herr Dr. Dressel vom DIHT Stellung nehmen. Das ist Herr Speer vom Sekretariat, meine Name ist Tauss. Hier ist der Platz des Herrn Dr. Dix noch frei. Dr. Dix ist unter anderem Datenschutzbeauftragter in Brandenburg, er ist aber auch in der Art. 29 Gruppe auf europäischer Ebene tätig. Er stellt zur Stunde noch seinen Datenschutzbericht vor und wird unmittelbar nach der entsprechenden Vorstellung hierher eilen, so dass wir ihn dann auch haben werden. Ich begrüße dann des Weiteren aus meinen heimatlichen Regionen Herrn Dr. Graf von der Bundesanwaltschaft in Karlsruhe. Wie praktisch, nicht? Er wohnt in der schönsten Höhenlage, die wir zu bieten haben. Dann begrüße ich ganz herzlich Herrn Bogk vom Chaos Computer Club. Sie haben sich jetzt dazwischen gemogelt. Jetzt ist alles klar. Herr Bogk vom Chaos Computer Club, und dann gab es einen kleinen Tausch, nicht mehr rechts außen, sondern weiter innen sitzt Herr Prof. Pfitzmann von der Technischen Universität Dresden. Dann begrüße ich von UUNET, Herrn Gramm. Herr Gramm hat sich pointiert auch zu Kosten von Überwachungen geäußert, das ist auch der Grund, warum wir ihn eingeladen haben. Es gibt dann immer wieder Verbände, die fragen, warum denn eco und nicht andere. Wir diskriminieren hier niemanden, aber wir haben ihn als Person geladen, weil er sich hier sehr viel geäußert hat; ihm assistiert, wenn ich das richtig sehe, Herr

Prof.Rotert, ebenfalls von eco. Ich glaube, auch Sie werden ein wechselndes Spielchen machen, was die einzelnen Fragen angeht, die nun doch sehr komplex sind.

Wir machen es hier in unserem Unterausschuss in der Regel so, dass wir es nicht ganz so strenge halten. Es ist ja, wie gesagt, auch ein Gespräch und keine klassische Anhörung wie in anderen Ausschüssen. Wir wollen durchaus die Möglichkeit geben, dass der eine oder andere Sachverständige auch einmal auf eine andere Person eingeht. Unter dem Strich wollen wir das parlamentarische Verfahren aber wahren, d.h. dass Kolleginnen und Kollegen aus dem Deutschen Bundestag die Möglichkeit haben, hier entsprechend auch die Fragen zu stellen. Wir haben folgende Regel, man hat immer zwei Fragen, an zwei Personen je eine oder an eine Person zwei. Es erleichtert einfach den Geschäftsablauf, wenn nicht jemand zehn Fragen hintereinander stellt. Man kommt auch hier mehrmals zu Wort. Meine sehr verehrten Damen und Herren, wie gesagt, wir stehen vor der Notwendigkeit, Kompromisse zu machen zwischen technischen Möglichkeiten und Unmöglichkeiten, zwischen rechtsstaatlichen Erwägungen und dem Bedarf an Handlungen zur Bekämpfung der Kriminalität. Wir haben drei Fragenkomplexe, die tatsächlich sehr unterschiedlich sind. Ich schlage vor, dass wir allerdings zuvor die Möglichkeit eines Kurzstatements geben, damit man den Gesamtkomplex ganz kurz streift, damit wir einfach wissen, mit welcher Position wir es zu tun haben. Ich würde Sie bitten, diese Eingangsstatements auf ca. fünf Minuten zu begrenzen, bei so vielen Sachverständigen. Und dort, wo ein Verband zwei Sachverständige hat, würde ich auch darum bitten, dass man sich zunächst auf eine Person einigt, dann hätten wir die ersten 45 Minuten für diese Statements; ich bin sehr interessiert daran, diese zu bekommen. Die Vorstellung habe ich links begonnen, jetzt würde ich sagen, fangen wir rechts an. Wir haben zunächst einmal, wie gesagt, noch nicht den Einstieg in den unmittelbaren Fragenkatalog und in die entsprechenden Kapitel, sondern sozusagen Ihre Hauptbotschaft, und dies bitte in fünf Minuten. Es müssen nicht fünf Minuten sein, wenn Sie es in drei Minuten schaffen, werden Sie vom Vorsitzenden ausdrücklich gelobt. Herr Gramm, Sie haben das Wort.

Tobias Gramm (UUNET): Herr Tauss, ich werde mich bemühen, mich kurz zu halten. Das ist angesichts der komplizierten Materie allerdings etwas schwierig. Unsere grundsätzliche Einstellung zum Entwurf der TKÜV ist, dass sie unverhältnismäßig ist. Sie verfolgt auf der einen Seite das Ziel der umfassenden Überwachung. Es soll wirklich alles überwacht werden. Sie beachtet dabei nicht die technischen Gegebenheiten und auch nicht die dadurch entstehenden Kosten. Ich denke, Sie wollen insbesondere Aussagen zu den Kosten haben. Man muss dafür ein bisschen ausholen und die Funktionsweise des Internets erklären. In der klassischen Telefonie gibt es immer irgendwo eine Zentrale, wo Sie wissen, dass der Anruf, den Sie abhören wollen, da vorbeikommt und Sie ihn dann auch überwachen können. Das

ist im Internet nicht der Fall. Im Internet gibt es keinen zentralen Punkt. Das bedeutet, Sie können die Überwachung nur dort machen, wo der Anruf in das Netzwerk übergeleitet wird. Und da gibt es nicht nur einen Punkt, sondern mehrere Punkte. Da man nicht weiß, wo der Anruf hereinkommt - das ist ja der wesentliche Grund, warum wir uns an der Überwachung beteiligen sollen, weil man eben nicht weiß, von welcher A-Rufnummer der Anruf ausgeht -, muss man an jedem Access-Punkt, also jedem Eingangspunkt, einschalten. Das bedeutet, nur um einen einzigen Kunden zu überwachen, muss ich an jedem der Access-Punkte, unsere Firma hat davon 80, die Überwachungsmaßnahmen einschalten und ich muss natürlich auch, selbst wenn ich nicht überwache, diese Überwachungseinrichtungen kaufen und vorhalten. Dadurch entstehen diese exorbitanten Kosten. Wir haben uns die Verordnung durchgelesen. Ich habe mit den Technikern gesprochen, wir sind vom „worst case“-Szenario ausgegangen, wie man das als pflichtbewusster Rechtsanwalt für sein Untenehmen machen muss. Die Techniker sagen, wenn wir wirklich alle Anforderungen, so wie sie im Moment in der TKÜV niedergelegt sind, umsetzen sollen, dann müssen wir ein völlig neues Access Equipment anschaffen.

Wir hatten gestern eine Veranstaltung mit Herstellern von Überwachungseinrichtungen, also nach unserem Modell würden wir auf 60 Millionen DM kommen. 60 Millionen DM reine Anschaffungskosten nur für eine Firma. Ich spreche bei den Kosten nur für meine Firma. Die Hersteller haben zum Teil geringere Kosten angesetzt. Eigentlich hat nur einer konkrete Zahlen genannt, da kämen wir für unser Netzwerk auf 20 Millionen DM. Das Problem ist nur, dass die Lösungen, die sie vorgestellt haben, nicht funktionieren. Insbesondere ist die Überwachung unbeteiligter Dritter nicht auszuschließen. Zum Zweiten hatten die Hersteller meines Erachtens den Verordnungsentwurf noch nie gelesen, sie wussten insbesondere noch nicht einmal, zu welchem Zeitpunkt diese Verordnung umgesetzt werden soll. Ich denke, das ist noch das am einfachsten zu Verstehende in dieser Verordnung. Diesen erheblichen Kosten steht aus meiner Sicht kein wesentliches Mehr an Überwachung gegenüber. Ich möchte noch einmal kurz ausholen. Wir sollen überwachen, weil man auf der klassischen Carrier-Ebene, also Deutsche Telekom, sage ich mal einfach, nicht mehr jeden überwachen kann, da man die A-Rufnummer, also die Nummer, von der aus angerufen wird, nicht unbedingt kennt. Der klassische Internet-User kann sich ja von überall ins Netzwerk einwählen. Bei dem Provider muss er ein individuelles Login abgeben. Damit könnte ich ihn ja dann erwischen. Das wäre grundsätzlich richtig, wenn es nicht so etwas Schönes wie Internet-by-Call geben würde. Internet-by-Call-Kunden, die haben keine festen Verträge, die wählen sich alle im selben Login ein. Damit ist die Geschichte vorbei. Jemand, der kriminell ist und Straftaten begehen möchte, braucht nur Internet-by-Call zu nutzen, das ist nebenbei gesagt auch noch die günstigste Möglichkeit, das Internet zu nutzen. Wir erwischen diese Internet-by-Call-Nut-

zer nicht. Wir erwischen sie nur dann, wenn wir wissen, von wo sie sich einwählen; dann können Sie auch wieder auf die Carrier-Ebene gehen. Das ist meine Kernaussage.

Vorsitzender: Herzlichen Dank, nun bitte Herr Prof. Pfitzmann.

Prof. Andreas Pfitzmann (Technische Universität Dresden): Ich beschäftige mich in der Forschung und in den letzten Jahren auch ein bisschen in der Entwicklung mit Fragen anonymer Kommunikation, mit Kryptographie, mit - wenn Sie so wollen - Techniken für den persönlichen Datenschutz. Meine Hauptaussage ist, dass alle Überwachungsbefugnisse, die Sie zur Zeit diskutieren und alle technischen Maßnahmen, die vorgeschlagen werden, völlig ins Leere laufen gegenüber allen Leuten, die sich schützen wollen, so dass der Nettoeffekt dessen, was Sie mit viel Aufwand machen, ganz egal ob wir über die TKÜV, das TKG, wo aus meiner Sicht die eigentlichen Probleme liegen, oder die Cyber-Crime-Konvention reden, als einem Versuch, über Außenpolitik Innenpolitik zu machen, ist, dass alle diese Versuche nichts bringen werden, um Leute zu überwachen, die sich schützen wollen. Sie werden mit viel Aufwand dafür sorgen, dass Sie Leute überwachen können, die der Überzeugung sind, dass sie nichts zu verbergen haben und sich nicht schützen wollen. Von daher ist für mich eine Diskussion, wie viel irgendetwas kostet, völlig obsolet, weil die Maßnahme selbst aus meiner Sicht nicht zweckgeeignet und von daher schon einmal unverhältnismäßig ist. Ich habe seit vielen Jahren mit den einschlägigen Stellen darüber geredet. Es gibt gegen die Aussage, dass das gegen Leute, die sich schützen wollen, nichts bringt, keinen ernsthaften Widerspruch von Leuten, die sich mit den technischen Sachverhalten auskennen. Es gilt auf der Ebene doch bitte darzulegen, was das in einer Übergangsfrist bringt; also in einer Frist, wo, sagen wir einmal das technische Know-how der End-User noch nicht so hoch ist, dass die jetzt in größerem Stil diese Techniken umsetzen werden. Es gibt dort keine konkreten Zahlen, was mich sehr beunruhigt, es gibt sozusagen keine Leistungsbilanz, so dass aus meiner Sicht das Horrorszenario folgendes ist: Mittelfristig nur noch Leute zu überwachen, die völlig arglos sind, dafür viel Geld aufzuwenden und sich der eigentlichen Herausforderung, nämlich gegen die clevere organisierte Kriminalität vorzugehen, nicht zu stellen, indem man an der völlig falschen Stelle herummacht. Die Stelle, an der Sie etwas tun können, sind die Endpunkte der Kommunikation. Das sind die klassischen Dinge, wie Personen beschatten, Richtmikrofone, diese Dinge. Wenn Sie es im Netz machen wollen, ist es weitgehend wirkungslos und wird im Laufe der Zeit immer wirkungsloser. Wenn Sie mich also fragen, dann versucht eine Gruppe von Leuten, die in klimatisierten Büros sitzt, ihre Arbeitsplätze zu erhalten und nicht eine Gruppe im Staat, die Gesellschaft vor der organisierten Kriminalität zu retten. Dankeschön.

Vorsitzender: Vielen Dank, Herr Prof. Pfitzmann. Herr Bogk, bitte.

Andreas Bogk (Chaos Computer Club): Im Prinzip kann ich den Ausführungen von Prof. Pfitzmann nicht mehr viel hinzufügen. Auch ich beschäftige mich seit langem mit Sicherheitstechnologien im Internet und habe auch in meiner frühen Jugend Dinge getan, die wohl zumindest als minder illegal gelten, wie zum Beispiel Raubkopien durch die Gegend kopiert. Also, die cleveren Leute wird man nicht kriegen können, die Verschlüsselungen funktionieren ziemlich gut, die Netze, die dort aufgebaut werden, funktionieren ziemlich gut. Jeglicher Versuch, bestimmte Kommunikationsformen einzuschränken, führt nur dazu, dass die Kommunikation in andere Medien abgedrängt wird. Verhindern können wird man das nicht. Was mich aber bei der TKÜV und auch bei der Cyber-Crime-Konvention viel mehr beschäftigt, ist, dass da ein Instrumentarium geschaffen wird zur Überwachung, wo die Stasi feuchte Finger gekriegt hätte, wenn sie das gehabt hätte. Ich gehe davon aus, dass ich nach wie vor in einem Rechtsstaat lebe; ich finde es allerdings sehr bedenklich, wenn Instrumentarien geschaffen werden, die mit relativ geringem Aufwand dazu benutzt werden können, ein totalitäres Regime aufzubauen. Es wird hier einfach ein Gefahrenpotenzial geschaffen, ohne dass auch nur der geringste Nutzen für die Bevölkerung existiert.

Vorsitzender: Ich habe etwas vergessen, wir reden hier sehr viel über Datenschutz. Sinn dieser Anhörung ist es natürlich auch, der Nachwelt erhalten zu bleiben, d.h., wir werden hier aufzeichnen. Wenn irgendjemand wünscht, dass seine Beiträge nicht aufgezeichnet werden, das ist bei einer Anhörung noch nie passiert, bitte ich um einen entsprechenden Hinweis, aber ansonsten wird aufgezeichnet, wir wollen die Veranstaltung natürlich entsprechend auswerten. Herr Dr. Graf.

Dr. Jürgen-Peter Graf (Bundesanwaltschaft): Vielen Dank, Herr Vorsitzender. Es war mir klar, als ich eingeladen wurde, dass ich hier eine Position haben werde, die vielleicht von der Mehrheitsposition abweicht, aber ich möchte diese einleitenden Worte, vielleicht auch etwas provozierend, dazu benutzen, einmal zu sagen, die TKÜV und auch die Cyber-Crime-Konvention, die ja auch erst umgesetzt werden muss, werden hier als totalitäres Regime beschrieben - wenn ich das gerade so nehmen kann, was der Vorredner gesagt hat -, als würde hier ein Bereich geschaffen, wo Milch und Honig für Verfolger, für Ermittler, für Schlapphüte fließen, ein Schlaraffenland. Das ist ja gerade nicht der Fall. Man muss sehen, dass die TKÜV, wenn ich mich jetzt einmal beschränke, keine tiefergehenden Eingriffsbefugnisse für Ermittlungsbehörden, auch nicht für den Geheimdienst, bringt. Sie regelt nur das Prozedere. Die Eingriffsermächtigungen kommen aus anderen Bereichen, nämlich aus den Gesetzen, die dann auch dazu gedacht sind, überprüft zu werden, nämlich im Wesentlichen,

was die Strafsachen betrifft, aus der StPO, dem § 100a und den Folgevorschriften, dem § 139 AWG. Das sind die wesentlichen Eingriffsermächtigungen und diesen ist allen gemein, dass sie richterlich überprüft werden oder dass die Anordnungen im Regelfall durch den Richter erlassen werden. Wir haben hier also eine sehr starke Eingriffsschranke und da ist die TKÜV zunächst einmal gar nicht gefragt. Die TKÜV bringt da nur nachher das Werkzeug, wie eine solche Überwachungsmaßnahme umgesetzt werden kann und muss. Ich würde da vielleicht auch noch etwas verschärft sagen, sie bringt eigentlich, wenn sie dann so kommt, Rechtssicherheit auch für die Provider, denn die Provider wissen genau, was auf sie zukommt. Es ist nicht so, dass irgendwann ein Staatsanwalt vor ihrer Tür steht mit einer Anordnung, die sie vielleicht auf ihre Weise gar nicht erfüllen können und sich dann für viel Geld Technik beschaffen müssen, viel Manpower, wie man so schön sagt, anlegen müssen. Wenn sie bereits technisch vorgerüstet sind, dann wissen sie genau, das muss ich bieten und wenn ich das bieten kann, dann kann ich die Anordnung erfüllen und wenn die Anordnung anders ist, geht die Anordnung ins Leere.

Wir haben Ähnliches auch bereits jetzt schon im Bereich der Mobilfunküberwachung, wo die Richter sich gar nicht danach richten, was irgendwo in einer Verordnung steht, sondern sie erlassen eine Anordnung nach § 100a StPO und der Provider muss dann diese Anordnung erfüllen, ob er will oder nicht. Wir erleben das, wie gesagt, im Mobilfunkbereich, wo die Provider sagen, das wollen wir nicht oder können wir nicht - aber sie haben dann gar keine Wahl, sie müssen sich dann die Technik beschaffen. Insofern bringt letztlich die TKÜV auch eine gewisse Form von Rechtssicherheit. Das ist eigentlich der Punkt, den man sehen muss, der ganz wichtig ist. Vielleicht eines noch zu dem, was auch von meinen beiden Vorrednern gesagt worden ist: Es werden nur die Dummen abgehört, es werden nur die Dummen erwischt - das ist eine Argumentation, die sicherlich schon seit 30 Jahren bezüglich der Telefonüberwachung immer wieder genannt wird, will sagen, es werden nur die abgehört, die sich dagegen schützen. Wenn es so wäre, dann würden überhaupt keine Fahndungserfolge durchs Abhören mehr gemacht, das Gegenteil ist der Fall. Wenn Sie sich zum Beispiel im Aufsichtsbereich die Gerichtsverfahren anschauen, dann entsteht ein großer Prozentsatz dieser Fahndungserfolge aufgrund von Telefonüberwachungsmaßnahmen - und es sind alles Leute, die wissen, dass sie möglicherweise überwacht werden. Wenn ich das aus der Praxis erwähnen darf, wir haben oft genug Telefonate, in denen die Leute am Anfang sagen, lass uns das nicht besprechen, wir werden vielleicht abgehört und nach einer Viertelstunde sagen sie genau das, worauf man wartet und dann ist es passiert. Das wiederholt sich permanent und genau dasselbe gibt es auch in anderen Bereichen. Wenn Sie hier fragen - an dem Tisch sitzen lauter Leute, die sich sehr gut mit den Gefahren auskennen - wer seine E-Mail verschlüsselt hierher geschickt hat, damit sie nicht verfälscht wird, dann bin ich ziemlich

sicher, dass wahrscheinlich keine einzige hier verschlüsselt angekommen ist. Man hätte es sicherlich mit einem bestimmten Prozedere machen können. Von daher, auch die Leute, die sich auskennen, nutzen die Technik im Regelfall nicht; ob es die organisierte Kriminalität wirklich macht, da habe ich meine großen Zweifel.

Vorsitzender: Vielen Dank. Wobei wir hier ja nicht konspirativ zusammen gekommen sind. Das halten wir einmal fest. Frau Dr. Pernice.

Dr. Ina Pernice (Deutscher Industrie- und Handelskammertag): Danke schön. Auch der DIHK sieht den Schwerpunkt heute in der Diskussion der TKÜV und zwar deswegen, weil sie nicht nur schwerwiegende Auswirkungen auf die betroffene Wirtschaft hat, sondern weil sie sich noch in einer Phase befindet, wo etwas zu retten ist, d.h., die TKÜV ist ja noch nicht erlassen, man kann jetzt noch einwirken, dass folgenschwere Fehlentscheidungen vermieden werden. Die Telekommunikationsüberwachung ist sicherlich unerlässlich für die Strafverfolgung. Ich glaube, darüber besteht kein Streit. Das wollen wir auch gar nicht in Frage stellen. Sie muss allerdings nach rechtsstaatlichen Gesichtspunkten ablaufen. Ich glaube, dass das in der gesamten Diskussion einfach stärker beachtet werden muss. Der Sache nach, das wurde auch schon gesagt, ist Kritik an der TKÜV hauptsächlich eine Kritik an den zugrunde liegenden Rechtsgrundlagen, nämlich am § 88 TKG und an den materiellen Eingriffsnormen, § 100a StPO und dem Außenwirtschaftsgesetz und dem G 10-Gesetz, in diesen Normen sind die eigentlichen Eingriffe schon enthalten. Dort steht, dass man überhaupt überwachen darf und dass die Telekommunikationsbetreiber dazu die Telekommunikation aufzeichnen und abgeben müssen; in § 88 TKG ist weiterhin die ganze Kostenfrage geregelt. Also, die grundsätzlichen Eingriffe sind schon auf Gesetzesebene gemacht worden. Aber - verzeihen Sie mir, wenn ich das so salopp sage - der Gesetzgeber hat dabei einen Fehler gemacht, als er das erlassen hat. Er ist nämlich bei der Verabschiedung dieser Gesetze seiner verfassungsrechtlichen Pflicht zur Ermittlung der relevanten Tatsachen gar nicht nachgekommen. Der Gesetzgeber ist ja verpflichtet, Gesetze zu machen, die verhältnismäßig sind. Ob diese Gesetze verhältnismäßig sind, kann er nur beurteilen, wenn er die Tatsachen zur Verfügung hat, die er miteinander abwägen muss; Schaden und Nutzen müssen miteinander abgewogen werden. Was man in diesem Bereich wissen muss, ist erstens, welche Effizienz Telekommunikationsüberwachungsmaßnahmen überhaupt haben, zweitens, welchen zusätzlichen Erkenntnisgewinn man dadurch hat, dass die Telekommunikation jetzt auf das Internet ausgeweitet wird, und zum Schluss, wie oft und in welcher Intensität überhaupt durch die Überwachung in Grundrechte eingegriffen wird - und dazu fehlen einfach die Untersuchungen. Es gibt keine Tatsachenerkenntnisse, es fehlen auch Untersuchungen oder Erkenntnisse darüber, wie das technisch überhaupt machbar wäre. D.h., der Gesetzgeber

hat hier Regelungen geschaffen, deren Verhältnismäßigkeit er selber gar nicht einschätzen konnte und die deswegen verfassungswidrig sind. Daraus folgt natürlich, dass er das nachholen muss, d.h., Aufgabe des Gesetzgebers wäre es, diese Sachen zu ermitteln und dann das Gesetz neu zu überdenken und ggf. zu novellieren. Ich gehe davon aus, dass das erforderlich sein wird.

Grundlage hierfür könnte zum Beispiel die vom Justizministerium in Auftrag gegebene Studie „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation“ sein, die Sie vielleicht kennen. Falls das nicht ausreichen sollte, muss auch weiterhin ermittelt werden. Bis dahin muss der Entwurf der TKÜV nach unserer Ansicht zurückgezogen werden, denn auch dieser Entwurf ist unverhältnismäßig. Es werden den Unternehmen unverhältnismäßig hohe Kosten aufgebürdet, ohne dass da ein zusätzlicher Erkenntnisgewinn der Strafverfolgungsbehörden nachweisbar ist. Es wurde ja hier auch schon oft gesagt, ob durch solche Verschlüsselungstechniken oder allerhand andere Finessen, man kann sich eben der Verfolgung im Netz entziehen. Hinzu kommt, dass durch die Struktur der datenvermittelten Kommunikation sehr große Gefahr besteht, dass in Rechte unbeteiligter Dritter eingegriffen wird. Durch die Schnittstelle werden auch Sicherheitsrisiken für die Unternehmen geschaffen. Das sind alles Dinge, die bei der Verhältnismäßigkeit berücksichtigt werden müssen. Auch dem Wirtschaftsstandort Deutschland wird durch die TKÜV ein schwerer Schaden zugefügt, weil die Umsetzung der TKÜV zu enormen Kosten führt - Herr Gramm hat das ja schon gesagt -, die in anderen Staaten so nicht anfallen und natürlich ein sehr starker Wettbewerbsnachteil sind. Zum Schluss möchte ich noch etwas zu der Kostentragungspflicht sagen, die ja in § 88 TKG verankert ist. Unseres Erachtens ist sie verfassungswidrig, denn Überwachungsmaßnahmen erfolgen ja zum Zweck der Strafverfolgung, was ein im Allgemeininteresse liegender Zweck ist - das kann nicht den Unternehmen aufgebürdet werden. Finanziert werden müssen diese Maßnahmen durch den Staat. Vielleicht ist in diesem Zusammenhang auch von Interesse, dass das entsprechende französische Gesetz für verfassungswidrig erklärt worden ist; dort sind auch den Netzbetreibern die Investitions- und Betriebskosten aufgebürdet worden und das ist eben aus dem Grunde für verfassungswidrig erklärt worden, weil das eine Sache ist, die der Allgemeinheit auferlegt werden muss. Also, unsere Forderungen: Zurücknahme der TKÜV, Erkenntnisse sammeln, zumindest die Studie des Max-Planck-Institutes abwarten und danach das TKG novellieren. Danke schön.

Vorsitzender: Herzlichen Dank, Frau Pernice. Ich wollte an der Stelle übrigens noch einmal darauf aufmerksam machen, dass es eine ganze Reihe von Wirtschaftsverbänden gab, die großen Wert darauf gelegt haben, ebenfalls zu dieser Anhörung geladen zu werden. Wir haben einfach wegen des Ablaufs hier gesagt, wir nehmen einen der großen, in diesem Falle

den DIHK, machen aber ausdrücklich darauf aufmerksam, dass es ja auch weitere Anhörungen, beispielsweise im BMWi gegeben hat. Insbesondere zu der Kostenfrage. Wir machen die Anhörung selbstverständlich zum Bestandteil der Auswertung dieser Anhörung. Wir wollten aber heute das Gewicht nicht ausschließlich auf die Wirtschaft legen und deshalb bitte ich auch an dieser Stelle um Verständnis, dass der Unterausschuss so entschieden hat. Gibt es eine zusammenfassende Stellungnahme vom BMI für die Eingangsrunde? Dann Sie, Herr Reisen, bitte.

Andreas Reisen (Bundesministerium des Innern): Vielen Dank, Herr Tauss. Da mein Kollege, Herr Akmann, und ich, die Fragenkomplexe 1 bzw. 2 bis 3, ich sage einmal, betreuen, würden wir gerne zu den Punkten jeweils einzeln ein kurzes Statement machen. Während meine Vorrednerinnen und Vorredner im Wesentlichen das Thema TKÜV angesprochen haben, möchte ich Ihre Aufmerksamkeit auf einen anderen Aspekt lenken, der insbesondere durch den Katalog 1 hier angesprochen ist: Die Bedrohung durch Cyber-Crime und insbesondere durch Cyber-War. Ich vertrete bei uns im Haus die Task Force „Sicheres Internet“ und von daher liegen uns natürlich auch in wesentlicher Hinsicht die Aspekte der Prävention am Herzen, d.h. Bedrohungen, die uns durch andere Staaten letztendlich zur Kenntnis gelangen, sofern sie denn relevant sind, oder durch konkrete Aktivitäten Einzelner im Bereich Cyber-Crime; denen muss die Bundesregierung natürlich durch entsprechende Maßnahmen vorbeugen. Einer unserer wesentlichen Ansätze ist, Verbrechen oder Angriffe auf Informationstechnik von vornherein zu verhindern. Es gibt einige sehr vielversprechende Ansätze: Ich möchte dazu zunächst einmal darauf verweisen, dass die Bundesregierung im Juni 1999 die Krypto-Eckpunkte im Kabinett verabschiedet hat, die dafür Sorge tragen und die Grundlage schaffen, Krytopgraphie am Markt frei verfügbar zu machen und auch die Verfügbarkeit dieser Produkte zu fördern. Das ist auch ein Aspekt, auf den der nichtständige Ausschuss beim Europäischen Parlament zum Thema Echelon ganz entschieden hingewiesen hat, dass nämlich, um sich vor solchen eventuellen Bedrohungslagen zu schützen, hier einfach mehr Selbstschutz der Nutzer stattfinden muss. In Deutschland haben die Krypto-Eckpunkte zumindest eine ganz wesentliche Grundlage geschaffen. Andere Aspekte, die hier von Bedeutung sind, sind der so genannte Aufbau von Sicherheitsinfrastrukturen in Deutschland - erinnert sei nur an das im Mai dieses Jahres in Kraft getretene Signaturgesetz, mit dem eine Sicherheitsinfrastruktur für Verfahren zur Verschlüsselung der Signatur und ähnliche Dinge dann letztendlich vorbereitet werden - und auch der Aufbau von so genannten Computer-Notfallteams im Rahmen einer flächendeckenden Infrastruktur für die ganze Bundesrepublik, die jedermann zur Verfügung stehen soll. Wer sich hinsichtlich der Computertechnologie mit Problemen und Angriffen konfrontiert sieht, soll hier letztendlich einen Ansprechpartner für Beratung und Unterstützung finden. Es sollen Computer-Notfall-

teams entstehen für die Bundesverwaltung, für die Wissenschaft und die Forschung, für die Wirtschaft, für die kleinen und mittelständischen Unternehmen und für die Bürger. Ich möchte es mit einzelnen Projekten hinsichtlich des präventiven Aspekts im Gegensatz zu den Aspekten der Strafverfolgung, die ja jetzt angesprochen sind, erst einmal bewenden lassen. Für mich ist wichtig, dass man die Bedrohungslage, ob sie an Cyber-War oder Cyber-Crime orientiert ist, differenziert und realistisch betrachtet. Unnötige Panik ist hier fehl am Platze, andererseits ist auch Sorglosigkeit fehl am Platze. Angemessene Sicherkonzepte sind notwendig, um Bedrohung der einen oder anderen Art zu begegnen. Vielen Dank.

Vorsitzender: Ganz herzlichen Dank, damit haben Sie die Konflikte, auf die auch sicherlich eingegangen wird, angesprochen: Führt das, worüber wir eben diskutieren, zu solchen unsicheren Infrastrukturen, die wir auf der anderen Seite gefördert wissen wollen. Herr Akmann.

Torsten Akmann (Bundesministerium des Innern): Zunächst zur Cyber-Crime-Konvention: Der Entwurf des Europarates wird vom BMI begrüßt, die Konvention wäre die erste internationale Kodifizierung im Bereich der Verfolgung grenzüberschreitender Datennetzkriminalität überhaupt. D.h., die Vorschriften könnten sich damit zu einem wichtigen Instrument bei der Bekämpfung der Kriminalität in Datennetzen entwickeln und so auch internationale Bekämpfungsstandards setzen, auf die wir damit eigentlich auch hoffen. Da auch vier wichtige außereuropäische Staaten, nämlich die USA, Südafrika, Kanada und Japan dabei sind, ist dem Übereinkommen auch im Hinblick auf die Globalisierung des Internets aus unserer Sicht große Bedeutung beizumessen. Der Entwurf trägt insgesamt der Internet-Kriminalität Rechnung und beinhaltet für eine effektive Bekämpfung der Datennetzkriminalität unerlässliche Instrumente. Vielleicht noch kurz zum TKÜV-Entwurf: Aus unserer Sicht sieht dieser Entwurf einen vernünftigen Ausgleich zwischen ökonomischen und sicherheitspolitischen Interessen vor, der TKÜV-Entwurf gewährleistet, dass die technische Durchführung der Telekommunikationsüberwachung sichergestellt ist. Wir denken, die gesetzlich geregelten Telekommunikationsüberwachungsmaßnahmen sind zur Verbrechensbekämpfung notwendig und stellen ein unverzichtbares Hilfsmittel für die Sicherheitsbehörden dar. Aus unserer Sicht kann das „Ob“ dieser Verordnung nicht in Frage gestellt werden. Wir treten daher dafür ein, dass die TKÜV so schnell wie möglich in Kraft tritt.

Vorsitzender: Ganz herzlichen Dank, Herr Akmann. Damit haben Sie wunderbar noch einmal den Konflikt, den wir ja auch an verschiedenen Stellen austragen, auf den Punkt gebracht. Ich habe vorher vergessen zu erwähnen, wir wollten sehr gerne noch die europäische Komponente hier auf dem Podium vertreten haben. Leider gab es hier eine kurzfristige Absage von der EU-Kommission aus dem Kabinett der Frau Reding; Herr Laitenberger war

angekündigt, er wird allerdings eine Stellungnahme für die Auswertung zur Verfügung stellen, so dass wir also auch diesen Teil berücksichtigen können. Ja, meine Damen und Herren, liebe Kolleginnen und Kollegen, ich glaube, wir liegen sehr gut in der Zeit und haben jetzt doch für die Diskussion, für die Fragen einiges an Stichworten bekommen. Wir wollen es so machen, dass wir den Teil Cyber-War, der noch eine ganz spezielle Komponente hat, aber der jetzt auch angesprochen ist, etwas kürzer abhandeln unter dem Gesichtspunkt kritischer Infrastrukturen und dass wir uns dann mit den beiden Teilen B und C Zeit lassen und die Fragen auch entsprechend sortieren. Darf ich einfach darum bitten, dass wir jetzt mit den Fragen beginnen und, wie gesagt, wenn die Kolleginnen und Kollegen jeweils hinzufügen, an welchen der Sachverständigen die Fragen dann auch gestellt sind. Frau Kollegin Dr. Krogmann hat sich als Erste zu Wort gemeldet.

Abg. Dr. Martina Krogmann (CDU/CSU): Ich möchte zunächst einmal festhalten, dass ich, vielleicht von den letzten beiden Rednern abgesehen, erst einmal überrascht bin, wie breit und deutlich hier auf dem Podium doch die Ablehnung des jetzigen Entwurfs der TKÜV noch einmal vorgetragen worden ist.

Vorsitzender: Vielleicht können wir die TKÜV noch einmal ein bisschen zurückstellen und zunächst mit den kritischen Infrastrukturen beginnen.

Abg. Dr. Martina Krogmann (CDU/CSU): Ach so, aber wir hatten doch eben über die TKÜV gesprochen.

Vorsitzender: Entschuldigung, da habe ich mich falsch ausgedrückt. Wir haben ja eine Dreiteilung: A. Bedrohung durch Cyber-Crime, B. Internationale Ansätze durch das Abkommen und C. Nationale Ansätze wie die Telekommunikations-Überwachungs-Verordnung. Ich würde einfach sagen, dass wir diese Frage noch einmal zurückstellen. Wir sind jetzt in dem Teil der kritischen Infrastruktur.

Abg. Dr. Martina Krogmann (CDU/CSU): Dann stelle ich meine Frage erst einmal zurück.

Vorsitzender: Herr Kollege Kelber, Sie zum ersten Teil.

Abg. Ulrich Kelber (SPD): Ich wollte die Gelegenheit natürlich noch wahrnehmen, dem Vorsitzenden auch öffentlich zum Geburtstag zu gratulieren; eine öffentliche Anhörung am Geburtstag ist natürlich ein besonderer Spaß. Meine Frage geht an Herrn Reisen und vielleicht in Ergänzung dann auch an Herrn Dr. Pfitzmann. Wenn Politik und Administration Selbst-

schutz und Integrität der Netze und sichere Infrastrukturen fördern wollen, sehen Sie darin nicht zumindest einen gewissen Widerspruch, ein trade-off zu der Idee, Sollbruchstellen in diesen Netzen und Möglichkeiten der Aufhebung des Selbstschutzes bei der Entschlüsselung zu schaffen?

Vorsitzender: Frau Bonitz, bitte.

Abg. Sylvia Bonitz (CDU/CSU): Ja, Herr Vorsitzender, meine lieben Kolleginnen und Kollegen, meine sehr verehrten Damen und Herren. Gestatten Sie mir zunächst zwei kleine Vorbemerkungen. Wir sprechen ja jetzt im Moment über den Bereich Cyber-War und Cyber-Crime in der speziellen Ausgestaltung. Ich bedauere das so ein kleines bisschen, dass in den vorausgegangenen Stellungnahmen dieser Bereich sehr kurz ausgefallen ist, dass eigentlich nur der Vertreter des BMI darauf eingegangen ist. Ich habe den Eindruck, dass man in der Politik zu wenig auf diesen Bereich eingeht, der im Grunde genommen von dem, was an Schadensdimension angerichtet werden kann, einer intensiveren Betrachtung würdig ist. Insbesondere, wenn man die Angriffe oder potenziellen Angriffe auf zivile Infrastrukturen, aber auch auf militärische Einrichtungen sieht, ist es eine ganz neue Dimension von Angriffen, die wir hier zu beklagen haben, die uns möglicherweise noch ins Haus stehen, die teilweise von heimischen Computern ausgeführt werden können und mit denen wir uns im Bereich TKÜV zum Beispiel, auf den wir nachher kommen, einfach nicht mehr eingehend beschäftigen können. Ich bedauere in diesem Zusammenhang sehr, dass heute kein Vertreter des BKA da ist und dass auch eine Stellungnahme des BKA, die zunächst vorgelegen hat und die hierzu sicherlich einige aufschlussreiche Ausführungen hätte machen können, wieder zurückgezogen worden ist, was mir völlig unverständlich ist. Ich habe insofern konkrete Fragen, insbesondere an die Vertreter des BMI. Es gibt ja eine Arbeitsgruppe unter dem Namen „Kritis“, die im Grunde fast im Geheimen tagt und bislang auch noch nie offiziell ihre Ergebnisse der Öffentlichkeit präsentiert hat, obwohl sie seit Frühjahr 1998 vorliegen. Diese Arbeitsgruppe „Kritis“ setzt sich im Wesentlichen aus Behördenvertretern zusammen und erörtert die Schadensdimensionen und wie diese im Bereich der Angriffe auf Infrastruktureinrichtungen vielleicht vermieden werden können. Informations- und Kommunikationstechniken, Bankfinanzwesen, Wasserversorgung, Energieversorgung und Verkehrsystem, all das könnte ja lahm gelegt werden, weil heute eben alles auf diesem technischen Wege miteinander verknüpft ist. Auch das Gesundheitswesen, alles könnte lahm gelegt werden. Eine Dimension, die im Grunde für uns unvorstellbar ist. Ich frage Sie ganz konkret, warum die Ergebnisse dieser Arbeitsgruppe bislang noch nicht vorgelegt worden sind, obwohl sie inzwischen seit über zwei Jahren bekannt sind. Warum es dort keinen Abschlussbericht gibt, der auch uns in der Politik zur Kenntnis gegeben wird, damit wir eine vernünftige Diskussions-

grundlage haben. Ich frage auch weiterhin das BMI, warum das BMI sich eigentlich bislang mit dieser Task Force „Sicheres Internet“ bescheidet. Das ist ja im Grunde mehr eine Kommunikationsplattform, aber ich kann daraus nicht erkennen, dass wir wirklich vernünftige Strukturen schaffen, die uns auch als Deutsche in die Lage versetzen, hier einen möglichen Schutzmechanismus aufzubauen, soweit er überhaupt aufgebaut werden kann. Es gibt zwar unter dem Begriff „CERT“ inzwischen erste Ansätze, die mir aber doch ein zartes Pflänzchen zu sein scheinen. Vielleicht können Sie darauf noch einmal eingehen, wie weit Sie hier wirkungsvolle Strukturen aufzubauen gedenken, die z.B. analog den amerikanischen Vorstellungen zumindest versuchen, hier ein wirkungsvolles Frühwarnsystem zu installieren und weitestgehend, soweit das überhaupt möglich ist, und versuchen, hier Schutzmechanismen zu installieren.

Vorsitzender: Soweit ich das verstanden habe, waren das Fragen an beide Vertreter des BMI, Herrn Reisen und Herrn Akmann. Was übrigens die Teilnahme des BKA anlangt, das ursprünglich von uns auch eingeladen war, hat uns das BMI mitgeteilt, dass es als übergeordnete Behörde hier an der Anhörung teilnehmen wolle, dass nicht die untergeordnete Behörde dies tun sollte. Ich habe es auch bedauert, aber so war die Mitteilung. Kollegin Griefahn noch, und dann gehen wir in die erste Antwortrunde. Kollege Otto, Sie sind jetzt zuerst dran.

Abg. Hans-Joachim Otto (F.D.P.): Den letzten Punkt, Herr Vorsitzender, den möchte ich noch einmal aufgreifen. Ich finde es einen ungewöhnlichen Vorgang, dass die Bundesregierung bei einer Anhörung über eine geplante Rechtsverordnung der Bundesregierung selber hier oben sitzt als Expertin und sagt, wir können das besser als die nachgeordnete Behörde. Der Vorgang ist ungewöhnlich. Wir hatten schon öfter Anhörungen in diesem Saal und in anderen, aber dass die Bundesregierung selber als Expertin zu ihrer eigenen Rechtsverordnung gehört wird, das ist jedenfalls diskussions- und gewöhnungsbedürftig. Von der Vertreterin des DIHK ist doch in aller Deutlichkeit gesagt worden, wir haben nicht ausreichend rechtstatsächliche Ergebnisse, die einen so weitgehenden Eingriff ermöglichen und erlauben würden. Meine Frage an die beiden Vertreter des BMI, vielleicht auch als die vorgesetzte übergeordnete Behörde zum BKA: Welche rechtstatsächlichen Erkenntnisse gibt es denn tatsächlich bzw. inwieweit sind die überhaupt für Abgeordnete offen und zugänglich? Vielleicht auch die Frage an den Vertreter der Bundesanwaltschaft, Herrn Graf, dass Sie uns das vielleicht auch aus Ihrer Sicht sagen können, denn bei dieser Frage der Rechtstatsachen sind Sie alle, vielleicht auch wegen der Kürze der Zeit, erstaunlich pauschal und ungenau geblieben. Die Kollegin Bonitz hat auch darauf hingewiesen. Ich denke, dass man die doch recht schwerwiegenden Eingriffe zunächst einmal durch saubere Entscheidungsgrundlagen

vorbereiten muss. Die habe ich bis jetzt als Abgeordneter noch nicht erhalten, da würde ich gerne zusätzliche Informationen haben.

Vorsitzender: Das habe ich notiert, die Frage ging an Herrn Akmann und Dr. Graf. Frau Kollegin Griefahn, die ich übrigens als Vorsitzende unseres Hauptausschusses herzlich begrüßen darf.

Abg. Monika Griefahn (SPD): Herrn Tauss darf ich an dieser Stelle auch ganz herzlich zum Geburtstag gratulieren. Ein tolles Geburtstagsgeschenk, sich mit Cyber-Crime zu beschäftigen. Wir geben ihm ein Stück Kuchen aus, denke ich. Herr Gramm, Herr Pfitzmann und Herr Bogk, Sie haben alle Kommentare über die Dramatik der vorliegenden Verordnung abgegeben. Ich habe da noch nicht so richtig die Lösungsmöglichkeiten gesehen, außer dem Appell, gar nichts zu machen. Mich würde deshalb einfach interessieren: Kennen Sie andere Regelungen oder andere Länder, wo es andere Regelungen gibt, die Sie für wirkungsvoller halten und sehen Sie da Erfahrungen oder konkrete Vorgaben, die vielleicht dann für uns eher greifbar wären und, falls diese Regelung hier eingeführt würde, würden Sie dann tatsächlich einen Standortnachteil gegenüber anderen Ländern sehen, oder gibt es nicht in anderen Ländern auch so eine Regelung? Weil ich ja immer nur zwei Personen benennen darf, möchte ich dazu Herrn Gramm und Herrn Bogk fragen.

Vorsitzender: Herzlichen Dank. Die meisten Fragen gingen jetzt an die Vertreter des BMI, an Herrn Akmann jeweils von Frau Bonitz und Herrn Otto. Ich würde Sie, Herr Akmann, einfach bitten zu beginnen und anschließend Herr Reisen.

Torsten Akmann (Bundesministerium des Innern): Also, ich bin eigentlich für Herrn Otto zuständig. Herr Reisen übernimmt dann das aAdere noch, wenn Sie erlauben. Ich kann die Verbindung, die Sie zwischen den Rechtstatsachen und der TKÜV herstellen, nicht ganz nachvollziehen. Richtig ist, dass die Telekommunikationsüberwachung an sich natürlich für die Strafverfolgungsbehörden zur Aufklärung von schweren Straftaten sehr wichtig ist. § 100a StPO sei hier nur als ein Beispiel genannt. Hierzu gibt es natürlich auch eine Rechtstatsachensammlung des BKA, hierzu werden auch Fallzahlen veröffentlicht, die auch den Abgeordneten zugänglich gemacht werden. Vor kurzem gab es im Übrigen auch eine Kleine Anfrage, auf die Staatssekretär Geiger meines Wissens nach im Bundestag geantwortet hat. Also, die Zahlen der TKÜV liegen vor. Die sind auch im Bericht des Bundesdatenschutzbeauftragten nachzulesen. Die TKÜV führt ja eigentlich die Technik herbei, dass diese TKÜ-Maßnahmen letztendlich geschaltet werden können; diese Verbindung kann ich nicht nachvollziehen.

Andreas Reisen (Bundesministerium des Innern): Die erste Frage kam von hier vorne hinsichtlich Überwachungsmaßnahmen, dass diese eventuelle Sollbruchstellen schaffen würden, die unter Präventionsgesichtspunkten natürlich bedenklich sein könnten. Wir sehen diese Problematik eigentlich nicht, weil hier keine Sollbruchstellen geschaffen werden sollen, sondern Maßnahmen angesetzt werden, die das Sicherheitsniveau für alle Seiten entsprechend durchsetzen wollen. Die Sicherheitsmaßnahmen, die hier zu ergreifen sind, müssen in der Art und Weise konzipiert werden, dass Unberechtigte, sei es nun ein unberechtigter Einzeltäter oder unberechtigte Staaten, die versuchen, diese Sollbruchstellen zu nutzen, definitiv keinen Zugriff auf diese Systeme bekommen. Sicherheitsmaßnahmen und Sicherheitskonzepte müssen greifen, die das ermöglichen. Dazu dient beispielsweise auch der Entwurf der TKÜV, eine technische Richtlinie, die von den Fachbehörden des Bundes auch entsprechend untermauert werden muss, indem Sicherheitskonzepte dargestellt werden, die eben nicht dazu führen, dass Sollbruchstellen entstehen, sondern nur Stellen, an denen ein ordnungsgemäßer Zugriff im Rahmen der bestehenden Gesetzeslage möglich ist. Das zur Frage eins. Dann zur Frage von Frau Bonitz. Zunächst möchte ich klarstellen, dass das von Ihnen erwähnte amerikanische Verteidigungsschild, das auch in der Presse genannt worden ist, von US-amerikanischer Seite eingestellt worden ist, weil sich dieses System als nicht realisierbar und nicht tragbar gezeigt hat. Die Bundesregierung hat hier selbst ähnliche Vorschläge im Rahmen eines Frühwarnsystems, ich hatte das in meinem Eingangsstatement erläutert, was aber nicht in technischer Hinsicht funktionieren soll. In Deutschland soll eine Infrastruktur dieser Computer-Notfallteams geschaffen werden - und zwar für die Wirtschaft, die Kreditwirtschaft und die anderen Sektoren -, die in ihrem einzelnen Bereich dem Vertraulichkeitsaspekt Genüge tun, aber andererseits auch einen formalisierten Informationsaustausch sicherstellen sollen, so dass, wenn ein einzelnes Wirtschaftsunternehmen attackiert wird, auch alle anderen Sektoren zeitnah informiert werden können.

Zur Arbeit der Task Force und der Arbeitsgruppe „Kritis“ lässt sich festhalten, dass beide Arbeitsgruppen durch konkrete Maßnahmen entscheidende Beiträge für mehr Sicherheit im Internet und zur Prävention auch vor Angriffen von außen leisten. Diese Aktivitäten sind mittlerweile in einigen Punkten zusammengeführt worden. Ich möchte nur auf einen Punkt hinweisen, die Task Force „Sicheres Internet“ hat mit den Vertretern der AG „Kritis“ festgehalten, dass wir uns mit einer Internet-Strukturanalyse beschäftigen müssen und dass wir das Internet in gewisser Weise auch als kritische Infrastruktur verstanden haben wollen. Hier ist es aus unserer Sicht notwendig - und das wird kurzfristig aufgesetzt -, dass wir die neuralgischen Punkte im Internet identifizieren und, soweit noch nicht geschehen, entsprechend schützen. In dem Zusammenhang hatten Sie auch nach dem Sensibilisierungsbericht der Bundesregierung gefragt. Hier gibt es zwei Gründe, warum dieser im jetzigen Status noch

nicht veröffentlicht worden ist. Der eine ist, dass man sich in den Beratungen über alle Ressorts hinweg hier mit einer sensitiven Materie auseinandersetzt, die zunächst in einzelnen Punkten dort festgehalten ist und für eine öffentliche Diskussion zum jetzigen Zeitpunkt nicht vorgesehen ist. Zum anderen ist es notwendig, die Ergebnisse, die bisher erarbeitet worden sind, mit den Ergebnissen der Wirtschaft zu konsolidieren, denn auch die entsprechenden Infrastrukturträger, wie Verkehrswesen und Telekommunikation, arbeiten an diesen Gesichtspunkten, haben ähnliche Sensibilisierungsberichte, die zusammengeführt werden müssen, so dass wir eine Gesamtlagedarstellung haben, die die Analysen der Bundesregierung einerseits und die Analysen Wirtschaft andererseits zusammenführt.

Vorsitzender: Ich würde an der Stelle gerne eine Nachfrage zulassen, das würde zur Belebung beitragen.

Abg. Sylvia Bonitz (CDU/CSU): Ich würde da ganz gerne einmal nachfragen, wenn Sie es eben so darstellen, dass manche Informationen zum jetzigen Zeitpunkt noch nicht für die Öffentlichkeit gedacht sind. Also, ich habe zum Beispiel von der Arbeitsgruppe „Kritis“ zum ersten Mal durch einen Bericht des „Spiegel“ erfahren und dann eben in einer Stellungnahme des BKA, die ja offensichtlich für uns nicht mehr existent ist. Insofern muss ich sagen, ich finde das schon sehr bedauerlich, wenn man selbst als Parlamentarier über diese Dinge, die von gravierendem Ausmaß sind, die auch Aufschluss über die Dimension des Schadens geben könnten, im Grunde von Seiten der Regierung absolut nichts erfährt und damit auch in keiner Weise als Parlamentarier über die offiziellen Stellen darüber sensibilisiert werden könnte. Ich muss Ihnen sagen, ich kann nicht ganz nachvollziehen, warum Sie im Grunde seit zwei Jahren solche Dinge im Hause haben und das Ganze anscheinend immer noch eher verwaltungsbürokratisch behandeln, atatt daraus konkret Handlungsoptionen abzuleiten. Denn ich habe den Eindruck, dass wir in Deutschland immer erst warten, bis der nächste größere Schadensfall eingetreten ist. Gott sei Dank haben wir mit Ausnahme der Viren, die ja schon einen erheblichen Milliardenschaden angerichtet haben, bislang noch keine gravierenden Angriffe auf zivile oder nationale Infrastruktureinrichtungen erlebt. Aber wir müssten hier einen wesentlich höheren Sensibilisierungsgrad erreichen, sowohl der Öffentlichkeit als auch des Parlaments. Das kann ja auch meinetwegen erst vertraulich geschehen, wenn man panikartige Zustände befürchten würde. Aber ganz konkret die Nachfrage: Sie haben Fitnet erwähnt, das eingestellt worden ist. Es gibt aber sehr wohl, und das meinte ich, auf US-amerikanischer Seite auf wesentlich höherer Regierungsebene eingerichtete Kreise, die sich mit diesem Thema intensiver beschäftigen. Ich habe den Eindruck, dass wir mit der Task Force „Sicheres Internet“, die ja nach ganz gezielten Virenattacken geschaffen worden ist, ein Diskussionsforum eingerichtet haben, das im Grunde genommen

ein bisschen mehr Kommunikationsplattform ist, aber nicht so sehr operative Aufgaben hat. Das BSI, ich will da keinem in der Kompetenz zu nahe treten, ist vielleicht bislang noch die einzige Stelle, die sich überhaupt mit diesem Thema, mit fachlichen Anleitungen, beschäftigt, aber ansonsten beschäftigt sich mit dem operativen Geschäft organisatorisch eigentlich keiner so richtig. Wo ist die Einheit, die sich auf Regierungsebene ganz dezidiert mit operativen Anleitungen für den Fall eines Angriffs auf nationale Infrastruktureinrichtungen oder eben eines Großangriffs auch auf die Infrastruktureinrichtungen der freien Wirtschaft beschäftigt? Wo ist diese Einrichtung?

Vorsitzender: Herzlichen Dank, das war jetzt eine sehr lange Zwischenfrage, aber ich habe sie jetzt zugelassen. Herr Akmann, ich weiß nicht, sind Sie dafür zuständig? Wer möchte darauf eingehen?

Torsten Akmann (Bundesministerium des Innern): Ich möchte mit drei kurzen Punkten auf die Frage antworten. Zum einen sind wesentliche Elemente des Sensibilisierungsberichtes bereits von uns in die Öffentlichkeit getragen worden; zwar nicht als Zitat des Sensibilisierungsberichtes, aber die Leitung des BMI hat sich in vielerlei Hinsicht in der Öffentlichkeit hierzu positioniert und auch Handlungsoptionen aufgezeigt. Zweiter Punkt ist, dass konkrete Handlungsoptionen, die sich aus den internen Diskussionen ergeben, bereits in der Umsetzung sind, dazu gehört dieses Frühwarnsystem; dazu gehört der zur Zeit stattfindende Aufbau eines Melde- und Informationssystems, an das auch die Wirtschaft angeschlossen ist, so dass hier Vorfälle gemeldet und auch kommuniziert werden können; dazu gehört, dass im BSI ein Verbund mit mittelfristig 30 Personen eingerichtet wird, mit Lagezentrum, das 24 Stunden besetzt ist, das heute ad hoc in Stundenfrist auch außerhalb der Dienstzeiten aktiviert werden kann. Also, die Maßnahmen hier sind vielfältig. Drittens muss man sehen, dass dem BSI hier in dieser Hinsicht kein operativer, sondern ein präventiver Gesichtspunkt zufällt. In dem Zusammenhang möchte ich darauf hinweisen, dass die Bundesregierung zusammen mit der Wirtschaft ein Planspiel plant, um genau eine solche Gefährdungslage einmal durchzuspielen, dass ein informationstechnischer Angriff stattgefunden hat, welche Konsequenzen der hat, welche Krisen sich daraus entwickeln können und wie die Bundesregierung im Rahmen eines Notfall- und Krisenmanagements darauf reagiert. All das ist in der Planung. Die Simulationen sind so gut wie abgeschlossen, so dass wir gegen Ende des Jahres ein solches Spiel dann tatsächlich auch durchführen können. Vielen Dank.

Vorsitzender: Vielen Dank, dann die nächste Frage, die der Kollege Kelber an Prof. Pfitzmann gerichtet hat; dies verbindet sich auch noch einmal damit, dass das BMI gesagt hat, es sollen keine Einbruchstellen geschaffen werden. Ich glaube, das setzen wir alle voraus, dass

sie nicht geschaffen werden sollen. Die spannendere Frage ist ja, werden welche geschaffen? Aber das war die Frage des Kollegen Kelber.

Prof. Andreas Pfitzmann (Technische Universität Dresden): Ich kann nur dringend raten, dass Sie darauf bestehen, dass Sie vom BKA und auch vom BSI direkt informiert werden. Und zwar nicht nur von der Leitungsebene, sondern von den Leuten, die den Tagesbetrieb machen, weil Sie nicht davon ausgehen können, dass das, was Ihnen gesagt wird, das ist, was die Leute einem unter vier Augen sagen - wo sie über gewisse Überwachungsverordnungen und die Krypto-Regulierung vor vier, fünf Jahren lachen, weil sie sie für völlig wirkungslos halten. Die Sache wird über viele Ebenen gefiltert, bis Sie nur die offizielle Meinung des Ministeriums erfahren. Zum Inhalt: Ich kann nur sagen, wer die Meinung äußert, man könnte komplizierte informationstechnische Systeme, egal wieviel Mühe man sich gibt, auf Anhieb sicher bauen und sicher betreiben, hat keine Sachahnung. Und er hat auch nicht auf die Leute unter sich gehört, die hoffentlich Sachahnung haben. Das geht nicht. Soweit ist der Stand der Wissenschaft nicht, soweit ist die Entwicklung der Systeme nicht. Es geht schlicht nicht. D.h., wenn Sie im bestem Wollen Abhörschnittstellen schaffen, beispielsweise für die deutschen Bedarfsträger, dann biete ich Ihnen jede Wette an, dass unsere amerikanischen und auch sonstigen Freunde innerhalb von wenigen Monaten auch mithören und dass es höchstens noch ein paar weitere Monate dauert, bis auch die organisierte Kriminalität mithört. Die Schwierigkeit wird nur sein, wenn wir diese Wette haben, dass wir uns nie werden einigen können, wer gewonnen hat. Weil natürlich die amerikanischen Freunde nicht kommen und sagen : „Ätsch, wir hören mit.“ Auch die organisierte Kriminalität wird nicht kommen und sagen: „Ätsch, wir hören mit.“ An der Stelle ist aus meiner Sicht die wesentliche Konfliktlinie, die wir hier oben auf dem Podium haben, nicht die zwischen Verbrechensbekämpfern einerseits und Datenschützern andererseits - das ist die Linie, über die immer in der Öffentlichkeit geredet wird. Wir haben den eigentlichen Konflikt zwischen Leuten, die Prävention, die sichere IT wollen und solchen Leuten, die unsichere IT wollen, weil sie sich zunächst einmal kurzfristig davon Vorteile für die Ermittlung versprechen. Das ist die eigentliche Konfliktlinie, d.h. also, wenn Herr Reisen sagt, dass die Task Force Angriffe im Internet verhindern wird, dann will diese Task Force etwas ganz anderes als das, was sich Herr Graf wünscht.

Was ich jetzt gerne auf der technischen Ebene diskutieren würde: Wie soll das gehen ? Es geht nicht und deswegen muss man sich an der Stelle entweder entscheiden, dass wir sagen, wir möchten eine unsichere IT, da treiben dann alle möglichen Instanzen und Institutionen ihr Wesen und Unwesen zu guten wie zu schlechten Zwecken, oder aber dass wir sagen, wir machen das über einen langen Prozess - das dauert Jahrzehnte, da ist nichts mit

wenigen Monaten oder Jahren -, wir wollen eine möglichst sichere IT, die auch leicht zu benutzen ist, die dann auch von Firmen, von Bürgerinnen und Bürgern benutzt wird. Um ein Beispiel zu nennen: Ihre Telefonüberwachung, seit 30 Jahren wird darüber geredet. Der Unterschied wird einfach folgender sein: In diesen kleinen Handys, die ersten sind bereits lieferbar, werden Sie in den nächsten Monaten und Jahren erleben, dass die programmierbar werden. Da können Sie also genauso wie Sie heute Software auf Ihren PC laden können, Programme herunterladen, die Kryptographie machen werden. Das hat einige Nebeneffekte, Ihr Handy wird auch öfter abstürzen, denn wenn Sie Programme installieren können und die Betriebssysteme schlecht sind, passiert Ihnen auf Ihrem Handy genau das gleiche wie auf Ihrem PC. Das ist die eine Seite, aber die andere Seite ist: Sie werden auch Kryptographie benutzen können und zwar so, dass es automatisch passiert. Natürlich war mein Statement nicht, dass wir sagen: Menschenskind, also Kriminelle sind außerordentlich diszipliniert und die reden nie am Telefon über irgendwas, was sie geheim halten wollen, so naiv bin ich doch nicht. Aber die Kriminellen werden irgendwann, wie die braven Bürger, auf ihren mobilen Endgeräten Ende-zu-Ende-Verschlüsselung haben; oder aber wir sagen, wir wollen die absolute Unsicherheit und wir versuchen, diese Ende-zu-Ende-Verschlüsselung zu verbieten. Also, ich würde heute gerne nicht in erster Linie oder ausschließlich über den Gegensatz zwischen Datenschutz und Verbrechensaufklärung reden, sondern den zwischen den Wünschen der Task Force „Sicheres Internet“ und der Strafverfolgung.

Vorsitzender: Herzlichen Dank, ich darf jetzt Herrn Dr. Dix noch sehr herzlich begrüßen, aber bevor er zu Wort kommt - sein Eingangsstatement werden wir nachher mit den internationalen Ansätzen gleich verbinden - wäre jetzt Herr Dr. Graf an der Reihe, ihm folgt Herr Gramm und dann Herr Bogk.

Dr. Jürgen-Peter Graf (Bundesanwaltschaft): Ja, zur Frage Entscheidungsgrundlage, das trifft ja auch ein kleines bisschen das, was Herr Pfitzmann gesagt hat. Entscheidungsgrundlagen, was Internet-Ermittlungen betrifft, gibt es derzeit in der Tat noch sehr wenige, weil eben die Ermittlungen da ganz am Anfang stehen, das muss man ganz klar sagen. Deswegen braucht man ja auch die TKÜV, um hier technisch einen gewissen Standard zu setzen. Ich kann nur sagen, wenn man jetzt noch einmal auf die Telefonüberwachung zurückgeht, dann wird es, was das Internet betrifft, ja ähnlich ablaufen. Sie müssen sehen, zum einen brauchen Sie als Ermittler zuerst einmal einen Beschluss, der von einem Richter erlassen wird, der die Sache prüft. Das Zweite ist vielleicht sogar im Ergebnis das Schwierigere, nämlich die Frage, wer bezahlt das Ganze. Es ist ja nicht so, dass Telefonüberwachung und Internet-Überwachung kostenlos ist, dass die Provider die Überwachung bezahlen, sondern dass das ganz enorme Kosten an Leitungsgebühren, an Infrastruktur auch bei den Ermitt-

lungsbehörden umfasst. Das kostet viel Geld und führt letztlich dazu, dass jeder Staatsanwalt eine Auge darauf hat, ob eine Überwachung überhaupt sinnvoll ist, ob sie zum Erfolg führen kann. Sie werden wahrscheinlich, wenn dann diese Überprüfung, dieses Gutachten vorliegt, sehen, dass - so kenne ich jedenfalls die Fälle - sehr oft eine Überwachung nach wenigen Tagen abgeschaltet wird, weil man sagt, diese Überwachung bringt uns nicht weiter. Man überwacht hier nicht einfach zum Spaß und weil das BKA oder das LKA seine Maschinen auslasten muss. D.h., man schaltet dann ab und dies wird in ähnlicher Weise in Zukunft auch passieren. Die Überwachungen, die über die volle Zeit, z. B. drei Monate oder mit Verlängerung, gefahren werden, sind in aller Regel auch erfolgreich oder bringen jedenfalls weitere Ermittlungsansätze. Ich habe es vorhin erwähnt, in vielen Bereichen, z.B. in der Rauschgiftkriminalität, wäre ohne Telefonüberwachung praktisch kein Fahndungserfolg zu machen. Wenn man die Akten dann liest, dann stellt man eben fest, dass durch sehr viele Überwachung dann weitere Ermittlungen ermöglicht werden und weitere Täter gefasst werden. Das ist letztlich der Punkt, auf den man es im Augenblick zurückführen kann und zurückführen muss, weil bezüglich des Internets im Augenblick keine Erfahrungen vorliegen.

Vorsitzender: Vielen Dank, Herr Dr. Graf. Es bleiben jetzt noch die beiden Fragen von Frau Kollegin Griefahn an Herrn Gramm und dann Herrn Bogk übrig.

Tobias Gramm (UUNET): Frau Griefahn, Sie hatten nach Lösungsmöglichkeiten in anderen Ländern gefragt. Es gibt Gesetze in UK, den Niederlanden; in Frankreich, haben wir gerade schon gehört, ist es für verfassungswidrig erklärt worden. In UK sind mir jetzt keine Erkenntnisse bekannt, dass die Umsetzung dieses Gesetzes schon begonnen hat. In den Niederlanden wird gerade - zumindest ist es das, was ich von unseren Unternehmen höre - eine Lösung implementiert und zwar eine solche, wie sie uns auch gestern vorgestellt worden ist. Diese Lösung halte ich in Deutschland für verfassungswidrig. Sie würde auf jeden Fall nicht den Vorgaben des vorliegenden TKÜV-Entwurfs entsprechen, da zum einen nicht sichergestellt werden kann, dass man die Kommunikation des zu Überwachenden von Anfang an überwachen kann, und zum anderen nicht sichergestellt ist, dass keine unbeteiligten Dritten überwacht werden können. Ich könnte Ihnen das jetzt technisch erklären, aber ich befürchte, dass ich Sie da sehr langweilen werde. Lösungsmöglichkeiten aus unserer Sicht: Wir hätten uns gewünscht, dass man . . .

Vorsitzende: Entschuldigung. Es wäre aber sicher interessant, jetzt nicht in längeren Ausführungen, aber wenn Sie uns das in Ihrem Statement für die Auswertung zur Verfügung stellen könnten, weil wir dann ja auch irgendwann zu einer technischen Diskussion kommen

müssen. Ich wollte nur ausdrücklich bitten, dies eventuell nachzuliefern und nicht unter den Tisch fallen zu lassen. Darum ging es mir.

Tobias Gramm (UUNET): Ja, gut. Ich kann es erklären. Jemand, der sich ins Internet einwählt, muss sich natürlich authentifizieren, d.h., wir müssen ja wissen, dass er das Recht hat, das Internet zu benutzen, damit wir ihn anschließend abrechnen können. Die Idee der vorgestellten Überwachung ist jetzt folgende: Der Call kommt auf einem Access-Device an, da wird zunächst einmal abgefragt - „Hallo, wer bist Du, darfst Du hier rein?“ -, dann gibt er sein Login, sein Passwort ein, dies wird weitergeleitet an den sogenannten Radioserver, der die Authentifizierung vornimmt. Die Überwachung nach den vorgestellten Lösungen soll jetzt hinter dem Access-Device stattfinden. Das Problem ist, die TKÜV knüpft an eine Kennung an, wir würden also eine Anordnung bekommen, die da sagt, überwacht die folgende Kennung. Im Internet-Verkehr würde das, ich sage einmal zum großen Teil, ein Login sein, eben das Login, mit dem sich der User authentifiziert. Der User gibt jetzt dieses Login ein, das Login taucht aber nachher bei der gesamten Kommunikation nie mehr auf. Nachdem der User sich eingeloggt hat, bekommt er eine IP-Adresse und anhand der IP-Adresse müssten wir dann überwachen. Das bedeutet, wir müssen herauskriegen, welche IP-Adresse diesem Login zugewiesen ist. Das vorgestellte Verfahren sagt jetzt, gut, wir hängen uns hinter das Access-Device, dann kommt irgendwann das Login vorbei und irgendwann wird der Radioserver ja antworten, in der Antwort steht dann die IP-Adresse. Das ist falsch, zumindest ist das nicht in allen Netzwerken so. Insbesondere in unserem Netzwerk nicht. Bei uns antwortet der Radioserver nur: „Ja, der darf hinein; bitte, Access-Device, weise ihm eine IP-Adresse zu.“ Das würde also vor dem Abhörgerät stattfinden. Irgendwann wird das Access-Device dann ein IP-Paket schicken und sagen: „Wir haben folgendem Login folgende IP-Adresse zugewiesen.“ Das Problem ist nur, das passiert nicht unbedingt zeitgleich und das Abhörgerät muss warten bis dieses Paket vorbeigekommen ist, sonst kennt es die IP-Adresse nicht und dann kann es keine Überwachung durchführen. Das bedeutet also schon einmal, die ersten Minuten der Kommunikation können wir nicht überwachen, weil wir die IP-Adresse nicht kennen und daher dann keine Überwachung möglich ist. Was die Sache noch viel schlimmer macht: Die Überwachung soll beendet werden, sobald das Abhörgerät mitbekommt, dass die IP-Adresse nun einem anderen Nutzer zugewiesen worden ist - Sie müssen sich vorstellen, die IP-Adresse wird immer individuell zugewiesen, es gibt keine fixe IP-Adresse. Da haben wir dann aber genau dasselbe Problem. Wenn der neue Nutzer ins Netz kommt - der alte beendet irgendwann die Session, das kriegt man mit und irgendwann wird diese IP-Adresse wieder frei, die wird einem Neuen zugewiesen - dann haben wir genau dasselbe Problem: Das Paket, das sagt, jetzt ist diese IP-Adresse dem User zugewiesen worden, sagt das unter Umständen auch erst ein paar Minuten später. Das würde also be-

deuten, da die Überwachungsmaßnahme noch aktiv ist, würden wir die ersten Minuten des neuen Users mit überwachen und damit in sein Fernmeldegeheimnis eingreifen. Ja, wir bekommen das natürlich nicht mit, wir überwachen einfach. Wir überwachen alles, was von und zu dieser IP-Adresse geschickt wird, weil wir ja nicht wissen, dass diese nun einen anderen User hat. Damit ist diese Lösung für mich nicht akzeptabel.

Ich möchte trotzdem zu unserem Lösungsansatz zurückkommen. Jetzt wird das BMI wahrscheinlich die Hände wieder über dem Kopf zusammenschlagen. Wir hätten uns gewünscht, dass man einen Ansatz fährt, der da sagt: Wir setzen zunächst einmal auf der Carrier-Ebene an, im Endeffekt müssen die Daten ja irgendwie übertragen werden, wir haben zum einen die Festnetz-Carrier, wir haben die Mobilfunkbetreiber, wir haben die Satellitenbetreiber. Die sind auf jeden Fall verpflichtet und die kommen ja auch nicht da heraus, ich möchte jetzt auch nicht den § 88 TKG diskutieren. Es wäre aber verhältnismäßig zu prüfen, was wir auf dieser Ebene alles nicht erwischen können, und dann für diese Fälle Sonderregelungen zu machen. Das ist aber nicht gemacht worden. Man hat einfach gesagt, wir machen eine sehr weite Verordnung - die trifft auf alle Verpflichteten zu und die müssen das alles erfüllen, d.h., wir haben im Grunde genommen eine Mehrfachstufung. Das, was wir überwachen können, können im Grunde schon die Carrier überwachen. Wenn Sie jetzt einen Mail-Server darüber haben, dann wird der auch noch einmal mit überwacht, was soll das? Was soll dieser breite Ansatz? Warum geht man nicht hin und sagt: Schauen wir doch erst einmal ganz unten im Netzwerk, was wir da erwischen können, dann prüfen wir, was wir da nicht erwischen können, dann prüfen wir, ob wir das mit verhältnismäßigem Aufwand vielleicht auf einer anderen Ebene erwischen können und dann haben wir eine angemessene und verhältnismäßige Lösung. Das ist nicht gemacht worden und das finde ich sehr bedauerlich.

Standortnachteil war die zweite Frage. Aus unserer Sicht entsteht ein Standortnachteil zum einen durch die erheblichen Kosten, zum Zweiten wird durch den vorliegenden TKÜV-Entwurf auf jeden Fall keine Rechtssicherheit geschaffen. Ich stimme Ihnen zu, Herr Graf, dass durch eine Verordnung Rechtssicherheit geschaffen werden könnte, allerdings müsste man dann aus der Verordnung auch konkret herauslesen können, was man denn eigentlich machen soll. Ich erzähle in dem Zusammenhang immer gerne die Anekdote: Als ich den Entwurf zum ersten Mal gelesen habe, habe ich mir gedacht, ja, das ist ja sehr technisch, aber unsere Ingenieure werden das schon verstehen. Dann habe ich einen Termin mit unserem leitenden Netzwerkingenieur gemacht, um die Verordnung zu besprechen. Er kam herein und sagte zur mir: „Tobias, Du bist der Jurist, ich hoffe, Du hast das verstanden.“ Gestern bei der Vorstellung der Hersteller hieß es in jedem dritten Satz, ja, wir wissen nicht so genau, was wir eigentlich machen müssen. Eine solche Verordnung schafft einfach keine Rechtssi-

cherheit und fehlende Rechtssicherheit ist ein Standortnachteil. Zum Dritten werden durch die im Moment in den verschiedenen Staaten versuchten Lösungsansätze nationale Insellösungen gefunden. Für uns als international tätiges Unternehmen, das sich bemüht, ein global einheitliches Netzwerk aufzubauen, schon allein aus Kostengründen, aber auch aus „quality of service“-Gründen, ist das natürlich nicht besonders erfreulich. Wir müssten jetzt anfangen, in jedem Staat anderes Equipment zu kaufen, was natürlich die Kosten ernorm in die Höhe treiben wird. Wir wollen noch irgendwann einmal Gewinne machen, die Kosten müssen wir weitergeben, die wären dann vom Endverbraucher zu tragen; was natürlich allen Bestrebungen, das Internet günstiger zu machen, zuwiderläuft. In dem Zusammenhang möchte ich auch noch auf einen Punkt hinweisen. Im Moment wird im Bereich des Interconnection diskutiert, die Telekom-Preise auf Grundlage des Modells „element based charging“ zu erheben. Wir sind ja auf die Telekom angewiesen, die uns die Calls zuführt. Günstigste Preise von der Telekom bekommt man, wenn man möglichst viele Punkte hat, an denen man die Daten von der Telekom abnehmen kann. Wenn man möglichst viele Punkte im Internet-Netzwerk hat, hat man leider aber auch viele Punkte, an denen man überwachen muss. Sprich, ich bekomme von der Telekom günstigere Preise, das wird aber leider dadurch aufgehoben, dass ich dann überall Überwachungsgeräte hinstellen muss, die die Preise wieder in die Höhe treiben. Danke.

Vorsitzender: Herzlichen Dank, und zum Schluss in dieser ersten Runde zum ersten Themenkomplex Herr Bogk.

Andreas Bogk (Chaos Computer Club): Ich finde es bemerkenswert, dass wir schon wieder bei der TKÜV sind, wo wir eigentlich die Runde zu Cyber-Crime eingeleitet hatten. Ich finde auch diese Vermischung der Ebenen ein bisschen bedenklich, weil auf der einen Seite Bedrohungsszenarien mit ausländischen Geheimdiensten konstruiert werden und auf der anderen Seite dann Gesetze geschaffen werden, die dazu führen, dass neugierige Schüler kriminalisiert werden - das muss man alles noch einmal auseinander diskutieren. Ich möchte aber jetzt dann trotzdem noch auf die TKÜV eingehen. Also, mein Vorschlag wäre, dass wir zu Cyber-Crime dann noch eine Runde machen. Ich bleibe also erst einmal bei der TKÜV. Ein Argument von Herrn Graf möchte ich gleich einmal aufgreifen. Da ging es um die Aussage: Ja, wir hören auch jetzt schon Telefone ab und das wird weiterhin auf rechtlicher Grundlage passieren. Das, was mit dieser TKÜV aber geplant wird, ist vergleichbar mit der Festinstallation von Abhöreinrichtungen in allen Wohnungen für den Bedarfsfall. Dass man einmal eine Wohnung abhören kann, das macht man ja auch gelegentlich und das läuft ja auch alles rechtsstaatlich mit richterlichem Beschluss und das führt ja auch dazu, dass wir immer ganz viele Kriminelle fangen - aber der Machtmissbrauch, das Potenzial, das da ge-

schaffen wird, ist einfach unglaublich. Die Chance, hinterher tatsächlich jemanden damit zu kriegen, der sich wirklich auskennt, ist relativ gering. Die Frage ist, was kann man sonst tun? Die TKÜV richtet sich natürlich in erster Linie als Instrument der Strafverfolgung aus, da muss man sagen, dass die klassische Strafverfolgung nach wie vor relativ gut funktioniert. Indem man Leitungen abhört, bekommt man zwar vielleicht Informationen heraus, im Wesentlichen geht es aber immer noch darum, Netzwerke zwischen Leuten kennen zu lernen, herauszufinden, wer macht was, wo fließen Gelder lang, was sind die Waren, wo werden sie hergestellt, wo werden sie gehandelt und wo werden sie verbraucht. Das ist einfach klassische Ermittlungsarbeit, diese Arbeit ist meiner Meinung nach durchaus ausreichend für die meisten Kriminalitätsprobleme, die auch im Internet auftreten. Wobei wir aber schon wieder fast bei der Cyber-Crime-Diskussion sind, weil auch da eine Vermischung auftritt zu Verbrechen, bei denen Computer bzw. Computernetzwerke lediglich als Werkzeug verwendet werden, und solchen, die den Computernetzwerken eigen sind.

Wenn man z.B. das beliebte Beispiel Kinderpornographie auspackt, dann hat sich ja eigentlich nichts geändert. Das gab es früher auch schon, da wurden Bildchen getauscht, heute werden Bildchen über Internet getauscht. Beides ist genauso verabscheuungswürdig und beides kann mit denselben Strafverfolgungsmitteln aufgeklärt und verfolgt werden, dafür brauchen wir keine neuen Gesetze und keine neuen Richtlinien. Ein bisschen anders ist es bei den Problemen, die spezifisch für Computernetze sind, ich denke da z.B. an „distributed denial of service“-Angriffe, wo ja auch die Internet Task Force des BMI meiner Meinung nach hervorragende Arbeit geleistet hat mit ihrem Maßnahmenkatalog. Schade, dass das nur Empfehlungen sind. Da ist es schon ein Stück weit sinnvoll, auch technische Richtlinien zu schaffen, um solchen Missbrauch von Computernetzwerken verhindern zu können bzw. das Fortbestehen der kritischen Infrastruktur Internet garantieren zu können. Es gibt nach wie vor Provider, die bei ihren Border Routern sparen und die nicht über ausreichende Leistungen verfügen, z.B. um zu filtern, d.h., man sieht dann nicht mehr, wo ein Angriff herkommt, und es ist schwierig, ihn nachzuverfolgen und abzustellen. Also, das sind durchaus Bereiche, wo es sinnvoll ist, Regelungen zu schaffen. Was das Abhören von Telekommunikationsverbindungen über das Internet angeht, bin ich nicht der Meinung, dass man unbedingt ein so mächtiges Instrumentarium, das unheimlich viel Geld kostet, braucht, sondern dass es auch ausreicht, sich den Einzelfall anzuschauen und zu überlegen, welche Variante des Abhörens die geeignete ist. Auch wenn man den Telefonanschluss abhört, kann man ja die Datenverbindung, die darauf stattfindet, analysieren, da muss man nicht den Provider abhören, da reicht es auch, den Telefonanschluss abzuhören. Oder man hört vielleicht den Server desjenigen ab, da reicht dann ein 2000 DM-PC, den man sich einfach hinstellt und mit einer zusätzlichen Leitung einstöpselt, auch völlig aus, oder ähnliche Maßnahmen. Wo es meiner

Meinung nach bei der TKÜV ganz besonders bedenklich wird, ist, wenn wir den Zwischenbereich der Strafverfolgung verlassen und uns den Tätigkeiten des Verfassungsschutzes und des Bundesnachrichtendienstes und ähnlicher Institutionen widmen. Nachdem ich hier gerade mitbekommen habe, dass die Damen und Herren Parlamentarier nicht einmal über die Analyse der kritischen Infrastruktur in der Bundesrepublik hinreichend informiert werden, frage ich mich, wie weit die parlamentarische Kontrolle über die Gemeindienste geht und inwieweit da sichergestellt werden kann, dass, wenn ein solcher Machtapparat explizit für solche Leute geschaffen wird, dann auch eine demokratische Kontrolle stattfindet und diese nicht einfach ausgeblendet wird.

Vorsitzender: Ganz herzlichen Dank, das war eine Frage an die Parlamentarier, aber die werden wir heute Mittag nicht mehr umfassend beantworten können. Aber vielen Dank jetzt für die erste Runde. Ich habe in der Tat nicht eingegriffen bei Frau Dr. Krogmann, die ich um Veständnis bitte. Aber ich hätte die Bitte, bei der zweiten Runde, wo es tatsächlich im Cyber-Crime geht, sich darauf zu konzentrieren. Sobald das Stichwort TKÜV kommt, werde ich auch ein bisschen dazwischen gehen, sonst wird es sehr schwierig. Frau Dr. Krogmann, Sie werden immer ungeduldiger. Also, dann kommen Sie jetzt auf Ihre Frage zurück und dann gehen wir in das andere Kapitel.

Abg. Dr. Martina Krogmann (CDU/CSU): Ich habe gelernt, dass ich der Weisheit der Obleute nicht mehr so schnell bereit bin zu folgen, Herr Tauss. Ich bedanke mich ausdrücklich, dass Sie mir jetzt noch einmal das Wort geben. Zur TKÜV, weil ich schon denke, dass deutlich geworden ist, auch in der Breite des Podiums, dass sich aus Vertretern verschiedener Bereiche zusammensetzt: Das Grundproblem der TKÜV ist, dass man die Wirtschaft über Gebühr belastet ohne dadurch zu einem Mehr an Sicherheit zu kommen, eben durch moderne Verschlüsselungstechniken, Herr Pfitzmann, Sie haben es gesagt, Kryptoprogramme, die sich heute jeder ja schon kostenlos aus dem Netz herunterladen kann. Herr Gramm, Sie haben es eben noch einmal gesagt, jeder ist heute überall auf der Welt in der Lage, einen Account aufzumachen, auch temporär, und von daher sind schon die Zugriffsmöglichkeiten auf bestimmte Adressen gar nicht gegeben. Jetzt stellt sich natürlich die Frage, wie geht man weiter vor. Der Entwurf der Bundesregierung, des Wirtschaftsministeriums, wird wohl so aussehen, dass man weiter gewisse Ausnahmen zulässt, den Kreis der Verpflichteten eventuell eingrenzt und bestimmte Schwellenwerte anhebt, um eben da bestimmte Verbesserungen zu erreichen. Frau Pernice, Sie haben vorhin deutlich gemacht, dass der größte Schwachpunkt der TKÜV eigentlich schon in der Struktur angelegt ist, nämlich dass man versucht, die Gesetzmäßigkeiten der normalen Telefonie gewissermaßen auf das Netz zu übertragen und dass man deshalb viel weiter gehen müsste, nämlich das TKG zu novellie-

ren, um wirklich zu einer sachgerechten Lösung zu kommen, die ja alle haben wollen. Da hätte ich gerne noch mal Ihre Stellungnahme zu dem Punkt. Der zweite Bereich geht an die Vertreter des Innenministeriums. Die Frage der Sicherheit im Internet ist aus meiner Sicht wirklich auch noch eine große Hürde, wenn es um die Akzeptanz des Internets in der Gesellschaft geht. Sicherheit hat auch sehr viel mit Vertrauen zu tun. Da stellt sich dann natürlich schon die Frage, wie weit ein Mehr an Überwachung überhaupt ein Mehr an Sicherheit bedeuten kann, oder ob es nicht sogar dazu anregt, das Vertrauen in das Netz eher zu zerstören, weil man gewissermaßen immer den gläsernen Surfer befürchten muss, der sich durch ein Mehr an Überwachungsmaßnahmen, vor allem wie sie jetzt vorgesehen sind, dann eben ergibt. Deshalb meine konkrete Frage an Sie: Die Zahl der Telefonüberwachungen hat in den letzten Jahren ja bereits enorm zugenommen. Es ist eine Studie des Justizministeriums in Auftrag gegeben worden, um einfach einmal zu prüfen, ob dadurch denn tatsächlich auch ein Mehr an Sicherheit eingetreten ist oder welche Erkenntnisse man überhaupt aus dieser gesteigerten Zahl an Überwachung gewonnen hat. Warum wartet man die Ergebnisse dieser Studie der Telefonie nicht ab, bevor man die TKÜV jetzt einfach erlassen will ?

Dr. Ina Pernice (Deutscher Industrie- und Handelskammertag): Zur Novellierung des TKG: Es ist genau so, wie Sie es sagten, Frau Krogmann. Die Crux liegt schon im TKG, denn das ist so weit gefasst, dass all das, was in der TKÜV steht, theoretisch mit umfasst ist. Also, es ist keine Einschränkung vom Wortlaut her, der Begriff der Telekommunikation ist ja sehr weit und da fällt auch das Internet mit drunter. Das Ganze bezieht sich nicht auf das TKG, sondern auch auf die Begleitgesetze, also die eigentlichen Eingriffsnormen in der StPO, im Außenwirtschaftsgesetz und im G 10. Der eine Punkt ist der, dass der Begriff der Telekommunikation sehr weit ist, und dann diejenigen, die betroffen sind, die geschäftsmäßigen Betreiber - das ist auch schon in den Begleitgesetzen enthalten. Das sind die Punkte, die es eigentlich schon im Wortlaut möglich machen, dass das, was in der TKÜV drin steht, so drin steht. Wobei man natürlich dazu sagen muss, dass der Verordnungsgeber nicht frei ist, alles hineinzuschreiben, was er möchte, denn er ist ja immer auch als Verordnungsgeber an den Grundsatz der Verhältnismäßigkeit gebunden und zwar nicht nur, wenn es ausdrücklich in der Verordnungsermächtigung enthalten ist, sondern grundsätzlich, auch, wenn es nicht enthalten ist. Es scheint mir so, als dass der Verordnungsgeber das auch nicht in dem Maße anerkennt, wie es sein müsste. Deswegen ist eigentlich die einzige Lösung, auch um Rechtssicherheit zu schaffen, das TKG zu novellieren.

Andreas Reisen (Bundesminsterium des Innern): Wir möchten gerne noch, weil Frau Dr. Krogmann eigentlich zwei Fragen gestellt hat, jeder einen Teil beantworten.

Vorsitzender: Das kann ich nicht zulassen, machen Sie eine Antwort daraus.

Andreas Reisen (Bundesminsterium des Innern): Es geht um den Aspekt Vertrauen, man muss hier sicherlich in gewisser Weise einen Spagat zwischen den Interessen der Strafverfolgungs- und Sicherheitsbehörden einerseits und dem Schutz der Nutzer des Internets andererseits machen. Es ist offensichtlich, dass wir Bemühungen unternehmen, um die Partizipation aller am Internet sicherzustellen und da auch ein entsprechendes Vertrauen zu schaffen. Im Rahmen der D21-Initiative ist im Frühjahr dieses Jahres die AG 6 gegründet worden, die sich mit Sicherheit und Vertrauen im Internet beschäftigt. Auf dem nächsten D21-Kongress werden Themen wie Bildung und Partizipation aller an der Informationsgesellschaft behandelt und da sind Sicherheitsfragen elementar. D.h., das Vertrauen in die Nutzung des Internets wird durch bestimmte Maßnahmen sicherzustellen sein und da muss ich wieder auf den Aufbau von Sicherheitsinfrastrukturen zurückkommen. Ich bin heute einige Male darauf eingegangen, welche Sicherheitsinfrastrukturen Vertrauen schaffen, das sind insbesondere Anwendungen - Signaturgesetz und Verschlüsselung - auf Basis sogenannter vertrauenswürdiger Dritter - Trust-Center-Zertifizierungsstellen, die heißen nicht umsonst Trust-Center. Hier wird Vertrauen bereitgestellt und das soll transparent werden. Die D21-Initiative beschäftigt sich außerdem mit dem Aspekt von Qualitätskriterien und Gütesiegeln. Die sollen ermöglichen, dass Internet-Dienstleister die von ihnen ergriffenen Sicherheitsmaßnahmen transparent machen können, so dass der Nutznießer solcher Dienstleistungen von vornherein weiß, er hat es hier mit einer Anwendung im Internet zu tun, die entsprechend sicher ist. Herr Tauss, wenn Sie erlauben, kann dann mein Kollege noch einmal kurz auf die Studie eingehen.

Vorsitzender: Das ist noch nicht die Antwort auf die Frage von Frau Krogmann.

Torsten Akmann (Bundesministerium des Innern): Die BMJ-Studie, die ja vom Bundesjustizminister in Auftrag gegeben worden ist, soll nach meinen Informationen - ich bin kein Angehöriger des BMJ und ich kann hier eigentlich nur für das BMI sprechen - ungefähr im Herbst vorliegen, vielleicht auch ein wenig später. Es ist nicht so, dass die Bundesregierung, das darf ich vielleicht sagen, keine Rücksicht auf diese Studie nimmt. Soweit es bereits Forderungen im Deutschen Bundestag und auch im Bundesrat gab, etwa die Forderung, im § 100a StPO den Straftatenkatalog zu erweitern, hat man darauf verwiesen, wir haben eine Studie beim Max-Planck-Institut in Auftrag gegeben und die warten wir erst einmal ab. Und dann schauen wir einmal, ob wir eventuell den Straftatenkatalog des § 100a StPO erweitern. Also, auf die Studie wird Rücksicht genommen, das kann ich ihnen nur sagen. Im Übrigen, einen direkten Bezug zur TKÜV kann ich nicht feststellen.

Vorsitzender: Danke. Wir kommen jetzt zum zweiten Teil. Hier bitte ich einfach, noch stärker die Telefonüberwachung, Cyber-Crime – das jetzt noch wenig behandelt worden ist - zu trennen. Wir kommen nachher, Frau Kollegin Bonitz, ausdrücklich noch einmal darauf zurück. Ich begrüße Herrn Dr. Dix, der zwischenzeitlich eingetroffen ist. Herr Dr. Dix, Sie haben sich mit Cyber-Crime auf europäischer Ebene sehr beschäftigt. Die EU-Kommission ist heute leider nicht vertreten. Dann würde ich Ihnen jetzt die Gelegenheit geben, in wenigen Minuten zum Thema Cyber-Crime aus europäischer Sicht und aus Ihrer Sicht Stellung zu nehmen.

Dr. Alexander Dix (Landesbeauftragter für Datenschutz, Brandenburg): Vielen Dank Herr Tauss. Ich muss zunächst um Nachsicht bitten, dass ich wahrscheinlich den Ablauf der Sitzung durch mein Zuspätkommen doch etwas durcheinander gebracht habe.

Vorsitzender: Wir haben die Reihenfolge umgestellt.

Dr. Alexander Dix (Landesbeauftragter für Datenschutz, Brandenburg): Gut, eine Umstellung, dann umso besser. Ich war leider eine Stunde an Potsdam gebunden. Ich habe mich in der Tat schwerpunktmäßig mit dem Entwurf der Cyber-Crime-Konvention beschäftigt, aber auch etwas zur Telekommunikations-Überwachungs-Verordnung gesagt. Dazu sage ich jetzt nichts mehr, um mir Ihren Zorn nicht jetzt zusätzlich zuzuziehen. Die Bekämpfung von Cyber-Kriminalität ist, denke ich, ein gemeinsames Ziel, auch der Datenschutz hält das natürlich für notwendig. Wir sehen aber in dem Entwurf, der jetzt vorliegt, in der Tat einen falschen Weg, eine grundsätzlich falsche Richtung, weil hier ein Abkommen für Zwecke der internationalen Rechtshilfe in diesem wichtigen Bereich geschlossen wird. Verbesserung der Kooperation ist unstreitig notwendig. Dieses Abkommen stellt aber einseitig auf die Interessen der Strafverfolgungsbehörde ab und lässt genau das vermissen, was notwendig ist, sowohl aus verfassungsrechtlicher Sicht wie auch aus europarechtlicher Sicht, nämlich eine sorgfältige Abwägung zwischen den Interessen der Strafverfolger einerseits und den Interessen des Grundrechtsschutzes auf internationaler Ebene. Ein positives Beispiel in dieser Hinsicht ist die Mitteilung der Europäischen Kommission für eine sichere Informationsgesellschaft, die Ende vergangenen Jahres veröffentlicht worden ist. In diesem Papier findet man eine sehr umfassende und auch abgewogene Gegenüberstellung der beiderseitigen Interessen, dort werden auch Lösungen aufgezeigt. Der Entwurf der Cyber-Crime-Konvention erwähnt demgegenüber im Text mit keinem Wort den Datenschutz und das hat nicht nur äußerliche oder symbolische Bedeutung. Ich will das gerne noch erläutern. Der Entwurf ist praktisch ausschließlich von Vertretern der Strafverfolgungsbehörden erstellt worden. Die internationalen Experten zum Datenschutz, die erst sehr spät überhaupt Gelegenheit bekommen haben, dazu Stellung zu nehmen, insbesondere die Internationale Arbeitsgruppe

zum Datenschutz in der Telekommunikation und die Europäische Datenschutzgruppe nach Art. 29, haben detaillierte Kritik geübt - in mehreren Phasen, aber sie haben es allenfalls erreicht, dass Spurenelemente des Datenschutzes sozusagen indirekt in den Konventionsentwurf eingebaut worden sind. Ich würde sagen, der Datenschutz, der vorher überhaupt nur in Fußnoten erwähnt wurde, findet jetzt immerhin in Erwägungsgründen Erwähnung. Das ist reichlich wenig, aus meiner Sicht zu wenig, um in einem so grundrechtsintensiven und relevanten Bereich eine so weit reichende internationale Konvention abzuschließen. Ich würde gerne in einer späteren Runde noch auf Details eingehen.

Vorsitzender: Ganz herzlichen Dank, auch für diese Kürze. Ich glaube, wir werden darauf noch zu sprechen kommen. Ich würde die Fragerunde unter den Kollegen und Kolleginnen zum Thema Cyber-Crime eröffnen. Frau Kollegin Bonitz.

Abg. Sylvia Bonitz (CDU/CSU): Ich habe eine Frage zu der rein praktischen Ausübung der Rechtshilfen. Vielleicht kann Herr Dr. Graf am ehesten dazu Stellung nehmen. Diese Cyber-Crime-Konvention sieht ja vor, dass ausländische Staaten uns im Grunde genommen im Rahmen der Rechtshilfe in Anspruch nehmen könnten, auch um Straftaten weiterzuverfolgen, die bei uns nach deutschem Recht keine Straftaten wären. Die bislang an dieser Cyber-Crime-Konvention beteiligten Staaten haben vielleicht nicht alle ein solches Rechtsgefüge und mitunter könnte man auch sagen, dass einige vielleicht nicht so demokratisch sind wie wir. Ich sage das jetzt, ohne bestimmte Staaten hier auch zu nennen. Gibt es dann eigentlich irgendeine Prüfung, wenn ein solches Rechtshilfeersuchen an deutsche Behörden herangetragen wird, ob wir in irgendeiner Weise hier möglicherweise Bedenken hätten, uns dem Begehren anzuschließen und quasi einfach in einem Automatismus solche Weiterleitungen zu ermöglichen? Gibt es Prüfungen, ob bestimmte Straftatbestände, weil sie bei uns nicht strafbewehrt sind, vielleicht nicht dazu führen, dass Daten weiter herausgegeben werden dürfen? Oder gibt es Prüfungen, ob es bedenklich sein könnte, an bestimmte Staaten aufgrund ihrer Regierung, aufgrund vielleicht nicht demokratischer Elemente diese Dinge herauszugeben? Ich sage es jetzt ganz gezielt vor dem Hintergrund, dass Wirtschaftsspionage damit auch erleichtert werden könnte, dass damit teilweise auch Regimegegner auf diese Art und Weise Opfer von Ausspähungen werden könnten. Wir wollen das alle nicht hoffen, aber vom Grundsatz wäre das ja dadurch möglich, weil es sich eben nicht nach unserem weiteren Rechtsfüge richten würde. Insofern die Frage an Herrn Dr. Graf: Wie wurde das konkret gehandhabt? Vielleicht kann auch der Datenschutzbeauftragte noch einmal darauf eingehen. Denn wir haben im Grunde genommen eine offene Flanke im Bereich des Datenschutzes, so dass auch deutsche Staatsangehörige natürlich Opfer von Strafverfolgungsmaßnahmen oder, sagen wir, Ausspähungsmaßnahmen anderer Staaten werden könnten und dass wir im

Grunde genommen hier unsere eigenen Staatsbürger in Zukunft einem doch relativ geringen Schutz ausgesetzt sehen würden.

Vorsitzender: Herzlichen Dank. Ich habe an dieser Stelle selbst eine Frage an Herrn Akmann, der sich auch als Fan des Cyber-Crime-Abkommens geoutet hat. Gibt es im BMI auf Beamtenebene oder auf der politischen Ebene des Hauses Debatten darüber, ob es nicht doch als problematisch angesehen werden kann, dass dem Cyber-Crime-Abkommen Staaten beitreten - das schließt dann an die Frage von Frau Bonitz an -, die die Menschenrechtskonvention, aber auch andere grundsätzliche Konventionen des Europarates nicht unterzeichnet haben? Meine Frage wäre - und das schließt dann auch unmittelbar daran an - inwieweit das BMI bzw. die entsprechend zuständigen Abteilungen für diese Problematik bei den bisher vorliegenden Entwürfen sensibilisiert waren. Das wäre meine Frage an Herrn Akmann. Gibt es weitere Fragen im Moment? Dann hätte ich die Bitte, dass Herr Dr. Graf beginnt.

Dr. Jürgen-Peter Graf (Bundesanwaltschaft): Bislang haben wir das Problem, dass Rechtshilfe bekanntermaßen sehr aufwändig und sehr langwierig ist. Das ist ein Problem, das heutzutage schon Ermittlungen sehr stark hemmt. Das ist auch teilweise abhängig vom Fall, teilweise abhängig vom Staat, wie lange ein Rechtshilfeersuchen dauert, bis es erledigt ist. Das ist völlig klar, dass im Internet-Zeitalter solche Rechtshilfe keine Hilfe mehr ist, weil, wenn dann nach Monaten oder unter Umständen Jahren Rechtshilfe geleistet wird, die Daten nicht mehr vorhanden und Ermittlungen dann nicht mehr möglich sind. Insofern bedarf es sicherlich einer erheblichen Beschleunigung des Rechtshilfeverkehrs, sei es dass er unter Umständen etwas formalisierter wird, d.h., dass das Ganze auf anderen Stufen abläuft. Da muss man sehen, was es für internationale Vereinbarungen dazu geben kann, aber eine Beschleunigung ist dringend notwendig. Ich glaube, das ist auch unstreitig, dazu gibt es keinerlei Gegenmeinungen. Das andere, was da geliefert werden kann, hängt davon ab, wie diese Bestimmungen umzusetzen sind. Das Erste ist, dass unter Umständen vorgesehen ist, Daten auf Anforderung anderer Staaten einzufrieren, wobei man sagen muss: Einfrieren von Daten heißt noch lange nicht, dass diese Daten herausgegeben werden, sie werden quasi nur konserviert, bis dann das Rechtshilfeersuchen bearbeitet und darüber entschieden ist, wie diese Daten und ob diese Daten herausgegeben werden. Ich denke, dass auch nach jetzigem Standpunkt sicherlich in aller Regel nur Rechtshilfe geleistet wird – aber das hängt eben von der Umsetzung ab -, wenn die Straftat dann auch in beiden Staaten strafbar ist. Das kann dann überprüft werden, wenn die Daten eingefroren sind, dann kann man in aller Ruhe überprüfen, ob hier eine Strafbarkeit nach beiderseitigem Recht vorliegt und ob dann die Daten herausgegeben werden. Solange sie eingefroren sind, liegen sie noch beim Provi-

der, sind dort gesichert, dann besteht keine Gefahr; das Telekommunikationsgeheimnis ist noch nicht entscheidend tangiert.

Vorsitzender: Vielen Dank. Herr Dr. Dix, bitte.

Dr. Alexander Dix (Landesbeauftragter für den Datenschutz, Brandenburg): Auch zu Ihrer Frage der sozusagen grenzüberschreitenden Abhörmaßnahmen und ergänzend zu dem, was Herr Graf gesagt hat. Ich denke schon, dass es ein Problem auch in der umgekehrten Richtung ist. Durch die Beitrittsmöglichkeit für Länder, die dem deutschen Grundrechts- oder Datenschutzstandard nicht genügen, kommen wir in eine Situation - die Konvention ist ja ausdrücklich geöffnet für den Beitritt solcher Länder -, dass es keinen zwingenden Mechanismus gibt, der dazu führt, dass die rechtsstaatlichen Sicherungsmaßnahmen auch in diesen Ländern adäquat angehoben werden, bevor ein solcher Beitritt zugelassen wird. Das Schengener Abkommen sieht ein solches Verfahren vor, dem Schengener Abkommen über die polizeiliche Zusammenarbeit im Schengener Raum können nur solche Länder beitreten, die dementsprechend auch die Europäische Datenschutzkonvention vorher ratifizieren. Das wäre das Mindeste, was man auch in diesem Bereich beim Cyber-Crime-Abkommen verlangen müsste, ansonsten sehe ich die akute Gefahr, dass wir sozusagen nach und nach zu einem Herunterbrechen kommen - sozusagen zu einem „race to the bottom“ -, was die Schutzstandards im internationalen Bereich angeht, und das kann aus deutscher Sicht nicht wünschenswert sein.

Vorsitzender: Herzlichen Dank. Herr Akmann.

Torsten Akmann (Bundesministerium des Innern): Das BMI hat keine Bedenken, und zwar insbesondere nicht in verfassungsrechtlicher Hinsicht, aber auch eben nicht in datenschutzrechtlicher Hinsicht. Ich darf vielleicht darauf hinweisen, dass im Vertragstext jetzt jüngst ausdrücklich Verweise auf den Schutz der Menschenrechte und das Verhältnismäßigkeitsprinzip aufgenommen worden sind. Im Übrigen, im erläuternden Bericht ist auch ein Hinweis zur Vermeidung übermäßiger Belastung der Wirtschaft. Was jetzt speziell die Datenschutzerfordernisse angeht, denen wird bei der Umsetzung der Konvention ins nationale Recht eigentlich Rechnung getragen durch eine Formulierung in Art. 15 Abs. 2. Dort wird ausdrücklich auf die Menschenrechte verwiesen, das hatte ich eben bereits angesprochen, und auch auf Bedingungen und Garantien des nationalen Rechts. Das ist im Übrigen auch ein Novum in einer solchen Konvention. Ich denke schon, dass hier Regelungen geschaffen worden sind, die dem Grundrechtsschutz Rechnung tragen.

Vorsitzender: Vielen Dank. Ich habe mir auch nochmals erlaubt, eine Frage zu stellen. Ein Argument für das Cyber-Crime-Abkommen war unter anderem die Bekämpfung von Nazi-Propadanda. Hier haben wir das große Problem, dass insbesondere ein großer Teil dieser Dinge aus den USA herkommt. Nun hört man, Herr Dr. Dix, dass die Amerikaner exakt aus diesen Gründen diesem Zusatzprotokoll, das diese Frage regelt, nicht beitreten wollen. Wäre da nicht ein Teil der Argumentation, die wir hier haben, dass wir sagen, wir müssen etwas gegen die Bekämpfung der Nazi-Kriminalität tun, möglicherweise durch den Nichtbeitritt der Amerikaner der Boden entzogen.

Dr. Alexander Dix (Landesbeauftragter für den Datenschutz, Brandenburg): Dieses Zusatzprotokoll geht unter anderem auch auf eine Anregung der Parlamentarischen Versammlung des Europarates zurück und auf Absprachen zwischen europäischen Regierungen, etwa der französischen und der deutschen. Man hat wohl bewußt gesagt, weil man sah, dass ein Konsens mit den Amerikanern in dieser Frage wegen der verfassungsrechtlichen Situation in den USA nicht realistisch ist, wir trennen das ab und machen ein Zusatzprotokoll, speziell dazu, wie man diese Probleme effektiv in den Griff bekommen kann. Ich würde nicht sagen, dass die Hauptkonvention schon gefährdet ist, wenn die USA diesem Zusatzprotokoll nicht beitreten, aber die USA haben auch gegen die eigentliche Konvention noch erhebliche Vorbehalte, und zwar besteht noch Streit - auch in der letzten Fassung im Strafrechtsausschuss bestand Streit - über die sogenannte Bundesstaatsklausel. Da geht es auch um ein internes verfassungsrechtliches Problem in den USA. Die amerikanische Regierung hat erklärt, wenn eine solche Bundesstaatsklausel nicht in die Konvention aufgenommen wird, würden sie auch der Hauptkonvention nicht beitreten. Ich würde mir wünschen, dass die Bundesregierung einen ähnlichen Vorbehalt im Ministerkomitee macht, dass in die Konvention auch materiell datenschutzrechtliche Bestimmungen aufgenommen werden, damit den verfassungsrechtlichen Vorgaben, wie sie das Fernmeldegeheimnis hier etwa vorsieht, auch im Text der Konvention Rechnung getragen wird.

Vorsitzender: Ganz herzlichen Dank. Es haben sich jetzt Herr Bogk und Herr Prof. Pfitzmann gemeldet. Wir haben gesagt, die Sachverständigen dürfen auch kommentieren. Weitere Fragen liegen im Moment von Ihrer Seite nicht vor, so dass ich sage, wir beenden dann auch diese Runde, falls sich aus diesen beiden Darstellungen nicht Nachfragen ergeben sollten, und gehen dann wieder zurück zu unserer Telekommunikationsüberwachung.

Andreas Bogk (Chaos Computer Club): Also, wenn ich meinen Vorrednern so zuhöre, „rollen sich mir eigentlich die Fußnägel hoch“. Insbesondere der Aussage, dass die Cyber-Crime-Konvention so schon okay und verfassungskonform ist, kann ich in keinster Weise

zustimmen. Da tauchen Bestimmungen auf wie die Unterstrafestellung einer Absicht, eine Tat zu begehen, was wirklich krass gegen jegliche rechtsstaatliche Norm verstößt. Die Anordnung zur Datenspeicherung findet unter richterlichem Beschluss statt, d.h. da kann jemand einfach so entscheiden: Speichere doch einmal 90 Tage die Daten. Was dann mit den Daten passiert, ist völlig unklar. Klar ist, wo Daten anfallen, da schaut auch einmal jemand hinein. Und das geht auch so weiter. Da werden Dritte gezwungen, Passwörter herauzugeben, das verstößt nicht nur gegen das Prinzip, dass man sich nicht selber belasten muss, sondern ist auch ein eklatantes Sicherheitsproblem, weil man in dem Moment, wo man Passwörter hinterlegen muss, keine sichere Verschlüsselung mit den üblichen Problemen für die kritische Infrastruktur usw. hat. Die Cyber-Crime-Konvention in der derzeitigen Form halte ich für grob verfassungswidrig. Der nächste Punkt, den man auch einmal diskutieren muss, ist das aufgebrachte Argument, wir müssen etwas gegen die Neonazi-Propaganda im Netz tun. Ich halte das für ausgesprochenen Blödsinn, Meinungsäußerungen zu verbieten. In dem Moment drängt man die Meinungsäußerung in den Untergrund, verhindert dadurch eine vernünftige Auseinandersetzung damit, schafft einen Mythos, den man möglicherweise gar nicht haben will. Wenn man sich anschaut, was derzeit gängige Praxis ist - da werden Leute verklagt, weil sie auf die Homepage von jüdischen Holocaust-Betroffenen linken, weil die wiederum auf Naziorganisationen linken, nur um die Diskussion voranzutreiben. Also, hier wird versucht, ein Problem zu erschlagen, das sich gar nicht erschlagen lässt, und so geht das weiter mit der Cyber-Crime-Konvention. Da geht es dann in der Cyber-Crime-Konvention um Urheberrechtsgesetze, was hat das denn damit zu tun? Also, jetzt einfach zu sagen, das ist okay und das werden wir demnächst ratifizieren, halte ich in keinster Weise für angebracht.

Vorsitzende: Prof. Pfitzmann, bitte.

Prof. Andreas Pfitzmann (Technische Universität Dresden): Frau Bonitz, man muss das noch zuspitzen, was Sie gefragt haben. Die Frage ist nicht, wer darf beitreten, sondern wenn man wirklich überwachen will, dann lautet die Frage: Wie bekommen wir alle Staaten, auch alle Schurkenstaaten dazu, dass sie beitreten? Sie können, wenn Sie über Kommunikation reden, ganz grob zwei Klassen von Daten unterscheiden: Die Inhalte und, sozusagen, die Verbindungsdaten. Die Inhalte der Kommunikation schützen Sie durch Ende-zu-Ende-Verschlüsselung. Das kommt, wie schnell es kommt, darüber kann man streiten, aber es kommt und die Verschlüsselung ist gut. Da ist an der Stelle der Verschlüsselung nichts zu drehen. Sie können versuchen, die Endgeräte anzugreifen, Zeiten usw., aber im Netz selbst ist da nichts zu machen. Abgehakt. Was kann man also noch herauskriegen? Man kann versuchen, herauszukriegen, wer kommuniziert wann mit wem. Jetzt gibt es eine ganze

Reihe von Techniken - die gehen zurück auf Arbeiten von David Chaum aus dem Jahre 1981 und Folgearbeiten von ihm und anderen -, wie man kryptographisch hart verbirgt, wer mit wem kommuniziert. Diese Techniken können Sie praktizieren, solange es noch einen einzigen Staat auf der Welt gibt, mit dem Sie kommunizieren können und wo Sie ein Relais haben, das für sie arbeitet. Und das bedeutet ganz hart, wenn Sie Telekommunikationsüberwachung machen wollen - und Sie wollen es wirklich -, müssen Sie mit jedem Schurkenstaat zusammenarbeiten, ob Sie es wollen oder nicht. Und wenn Sie nicht mit Schurkenstaaten zusammenarbeiten wollen, dann sparen Sie sich bitte die ganzen Rechtseinschränkungen, die ganze Pseudo-Lyrik von wegen, wir könnten auf diese Art irgendwas für Verbrechensbekämpfung tun. Das war jetzt mittel- und langfristig argumentiert. Ich sage nichts über die nächsten zwei Jahre, aber wir reden an der Stelle über Investitionen und Infrastrukturen, die typischerweise über 30, 35 und 40 Jahre wirken. Während unsere Endgeräte - das ist das, wo dann Ende-zu-Ende verschlüsselt wird, mit denen man die Anonymisierungstechniken aufzieht - einen Markt haben, wo man typischerweise innerhalb von drei, vier Jahren alle Endgeräte ersetzt. So, da muss man sich entscheiden, was man will. Ich muss ganz offen sagen, dass ich inzwischen die Position des Innenministeriums bereits in sich selbst für widersprüchlich halte. Also, am Anfang hatte ich nur das Gefühl, dass es zwischen Herrn Graf und der Position des Innenministeriums nicht überbrückbare Widersprüche gibt, inzwischen habe ich das Gefühl, die Position des Innenministeriums ist in sich selbst so widersprüchlich, dass man kein technisches System bauen kann, was dem genügt. Dankeschön.

Vorsitzender: Jetzt wäre es natürlich fair, wenn die Angesprochenen auch etwas sagen könnten.

Torsten Akmann (Bundesministerium des Innern): Darum würde ich gerne zu Herrn Bogk noch etwas sagen. Herr Bogk hatte das Ermittlungsinstrumentarium kritisiert, das sind die Artikel 14 ff. des Entwurfs der Konvention. Er hat insbesondere kritisiert, diese Maßnahmen würden dann ohne richterlichen Beschluss durchgeführt - das ist nicht der Fall. Ich habe eben in meinem Statement ausgeführt, dass Art. 14 und 15 von Bedingungen und Garantien des nationalen Rechts sprechen. Das bedeutet für Deutschland natürlich ganz eindeutig, dass eine Ermittlungsmaßnahme, ich sage einmal eine Telekommunikationsüberwachung, die hier in Art. 20, 21 festgelegt wird, natürlich nur mit einem richterlichen Beschluss durchgeführt werden kann, bei Gefahr im Verzug durch den Staatsanwalt, das haben wir jetzt auch schon. Ich bitte, den Entwurf da auch wirklich richtig zu lesen. Danke.

Vorsitzender: Ich möchte jetzt keine unmittelbare Podiumsdiskussion machen. Herr Bogk, aber einen Satz bitte.

Andreas Bogk (Chaos Computer Club): Ich redete von Art. 16.

Vorsitzender: Kann der Jurist Dr. Dix uns in dem Streit jetzt noch eine kurze Sachaufklärung gewähren?

Dr. Alexander Dix (Landesbeauftragter für den Datenschutz, Brandenburg): Es muss klargestellt werden, Herr Akmann hat den Art. 15 Abs. 2 richtig wiedergegeben. Nur, das Interessante ist, die Konvention gibt dem ersuchten Staat, bei dem Daten oder Rechtshilfe angefordert werden, als Konvention selbst kein Recht, ein solches Ersuchen mit dem Argument abzulehnen, dass entsprechende Garantien im ersuchenden Staat fehlen. Das ist ihnen nach der Konvention freigestellt. Deutschland wäre mit Sicherheit, das muss man betonen, verfassungsrechtlich verpflichtet, ein solches Ersuchen abzulehnen. Das würde ich auch sagen, aber man muss den internationalen Prozess beobachten, der durch diese Konvention ausgelöst wird. Es wird ein Rechtshilfeabkommen geschlossen mit relativ niedrigen Schwellen für die Sicherung der Rechte der Einzelnen und die anderen Staaten, die nicht so hohe Sicherungen haben wie Deutschland; dies wird den Druck auf Deutschland erhöhen, das deutsche Rechtssystem auch entsprechend anzupassen, um mehr internationale Kooperation zuzulassen. Das ist ein rechtspolitischer Prozess, dem können und müssen wir unsere Garantien entgegenhalten, aber man würde naiv sein, wenn man glauben würde, dass Deutschland, wenn es nicht von Anfang an hier eindeutige Vorbehalte erklärt, sich dem auf Dauer entziehen könnte.

Vorsitzender: Vielen Dank. Ich glaube, das war auch noch einmal ein interessanter Abschluss dieses Teils „Cyber-Crime“. Zum Stand des Cyber-Crime-Abkommens muss gesagt werden, es ist bisher in verschiedenen Variationen vorgelegt worden. Man hat ein bisschen Probleme, den Variationen zu folgen, zumal als Parlamentarier, da wir diese Unterlagen nicht bekommen. Im europäischen Bereich war es so, dass die Anhörungsunterlagen den Mitgliedern der Parlamentarischen Versammlung des Europarates nicht vorgelegt worden sind. Dies ist ein befremdlicher Vorgang. Er wurde damit begründet, dass es ohnehin nur darum ginge, Kinderpornographie und Nazis zu bekämpfen; dies sei doch ein hinreichendes Argument, hier endlich etwas zu tun und diese Wildwestzeit im Internet zu beenden. Ich füge dieses als Information aus der Parlamentarischen Versammlung des Europarates nur noch zur Information und für das Protokoll an. Wir kommen noch einmal zur Telekommunikationsüberwachung, nachdem diese schon umfassend diskutiert worden ist. Ich würde hier auch

noch einmal um eine Fragerunde bitten. Frau Dr. Krogmann, jetzt haben Sie wirklich die Chance.

Abg. Dr. Martina Krogmann (CDU/CSU): Ich möchte gerne noch einmal nachfragen, bei Ihnen, Herr Graf und den beiden Herren vom BMI, Herrn Reisen und Herrn Akmann, und zwar, wo denn nun wirklich aus Ihrer Sicht der staatliche Erkenntnisgewinn bei der TKÜV liegt. Also, wir haben zum einen keine Identifizierung des Absenders. Darauf sind wir vorhin hier eingegangen. Wir haben zum Zweiten keinen Zugriff auf die Inhalte, unter anderem wegen der Kryptoprogramme, und wir haben zum Dritten wegen der Dezentralität der Rechner keine Fixierung auf bestimmte Orte. Wir wissen also nicht, wer, was und wo. Wo liegt dann der Erkenntnisgewinn?

Vorsitzender: Herr Kelber, bitte.

Abg. Ulrich Kelber (SPD): Im Prinzip die gleiche Fragestellung, damit Ihnen das wirklich klar wird, dass das der entscheidende Punkt auch für die Politik ist - neben den Fragen, die wir über Verhältnismäßigkeit, Kosten und Ähnliches gestellt haben. Wir haben eine klare Diskussion über die Frage der Kryptographie mit überhaupt nicht überzeugenden Antworten von Seiten der Bundesanwaltschaft und des BMI gehabt. Wir haben die Diskussion, dass Sie überall dort, wo sich die entsprechenden Infrastruktureinrichtungen, die ich nutze, im Ausland befinden, keine Zugriffsmöglichkeiten haben. Wir haben das, was der Kollege Tauss immer als Ziehen eines der Giftzähne der alten TKÜV bezeichnet hat, ein Herausnehmen bestimmter sehr kleiner Anbieter und geschlossener Netze, auch darüber fallen wieder bestimmte Adressen, bestimmte Personen heraus. Von daher ist meine entscheidende Frage, die vor allem an Herrn Graf geht, aber auch an das BMI, wen wollen Sie eigentlich noch wirklich überwachen? Sie dürften es eigentlich nicht schaffen, einen hier im Raum Anwesenden zu überwachen, wenn er nicht möchte.

Vorsitzender: Herr Dr. Graf.

Dr. Jürgen-Peter Graf (Bundesanwaltschaft): Diese Frage ist jetzt schwierig; es ist schwierig, auf diese Argumente einzugehen, weil diese Argumente alle auf Unterstellungen aufbauen. Auf Unterstellungen dahingehend, dass jeder, der es kann, Kryptographie benutzt. Dass jeder, der es kann, Endgeräte zum Verschlüsseln benutzt. Dass jeder, der es kann, einen ausländischen Provider benutzt und solche Dinge. Die Realität ist bislang eine andere. Im Rahmen der Kryptodebatte vor drei, vier Jahren hieß es damals, wir können alle Kryptoprogramme nehmen, als free-ware als, share-ware sind sie vorhanden. Die Realität ist die,

dass Kryptoprogramme bis zuletzt und bis in neuere Zeit praktisch keine Verwendung finden. Sie finden, jedenfalls auch nach den Erfahrungen, keine Verwendung, jedenfalls keine umfassende und ausschließliche Verwendung im Rahmen organisierter Kriminalität, wenn wir darunter die Bereiche verstehen, wo das Geld vorhanden ist, wo man sagt, die können sich das leisten. Wenn Sie zum Beispiel sehen, dass es auch jetzt schon im Rahmen von ISDN-Telefonleitungen die Möglichkeit gibt, Ende-zu-Ende-Verschlüsselung mit Hilfsmitteln zu machen - große Unternehmen bieten so etwas an und das kostet nicht die Welt. Das findet keine Verwendung. Für die Seite der Ermittlung ist es natürlich insofern angenehm. Aber auch, wenn Sie das BMI fragen, wieviele Fälle kryptographierter Daten es hat, dann werden Sie sehen, dass diese Zahl relativ gering ist im Vergleich zu den Ermittlungszahlen, die durchgeführt werden. Das ist das Eine. Das Zweite, Sie sagen, Kryptoprogramme, jeder im Raum kann das machen. Natürlich ist die Frage, wer macht es? Wann wird es gemacht? Ich bezweifle, dass es durchgängig gemacht wird. Mag sein, dass ich nachmittags um 3 Uhr meine Daten verschlüssele, abends um 11 Uhr aber nicht mehr, weil ich vielleicht müde bin, das passiert oft genug. Ich kann sie ja morgen früh noch verschlüsseln, aber dann ist es zu spät. Denn, wenn Sie sagen, es gibt Programme, die machen das automatisiert, dann sind das die Programme, die eben nicht hundertprozentig funktionieren. Natürlich kann ich PGP in E-Mail-Programme einbinden, das geht. Die Frage ist nur, wer das macht und, wie gesagt, ob es denn tatsächlich Straftäter durchgängig machen. Das sind Unterstellungen, die im Rahmen der Kryptodebatte liefen und wo wir inzwischen wissen, tatsächlich finden diese Dinge keine sehr umfassende Anwendung. Und genauso das andere Argument, ich kann überall über Telefonleitungen einen Provider im Ausland anrufen, kann mich ins Netz einwählen, das passiert eben auch nicht sehr oft. Das ist eben der nächste Punkt. Das Dritte, dass ich mich anonym einwählen kann. Ich kann mich sicherlich anonym einwählen, aber gerade dann, wenn es um E-Mail-Verkehr geht, da muss ich selbst, um die E-Mail empfangen zu können, die Anonymität in einem gewissen Maße aufheben. Das ist auch schon wieder ein Punkt, wenn ich eine E-Mail-Adresse verwende, dann muss ich sie ja bekannt geben. Wenn ich die E-Mail-Adresse kenne, dann habe ich auch die Möglichkeit, auf diese E-Mail-Adresse spätestens im Rahmen von Rechtshilfeersuchen Eingriff zu nehmen. Ich brauche das technisch nicht auszudiskutieren.

Vorsitzender: Wir kommen gleich noch einmal zu einer technischen Diskussion. Frau Krogmann.

Abg. Dr. Martina Krogmann (CDU/CSU): Ich möchte da gerne nachfragen, Herr Graf, weil ich zunehmend den Eindruck gewinne, dass die Bundesanwaltschaft nur die Dummen und Müden überwachen will.

Vorsitzender: Herr Dr. Graf, wie halten Sie das mit den Dummen?

Dr. Jürgen-Peter Graf (Bundesanwaltschaft): Die Erfahrung zeigt schlichtweg, dass es eben nicht unbedingt die Dummen und Müden sind. Ich kann im Augenblick nur auf die Maßnahmen im Telefonüberwachungsbereich zurückgreifen, weil für das Internet verlässliche Grundlagen fehlen. Das ist eben so, da kommen wir nicht darum herum. Letztlich ist es auch nicht die Bundesanwaltschaft, sondern die Justiz als solche. Die Landesjustiz hat ähnliche Erfahrungen, dass eben eine durchgängige Sicherung - Sicherung in Anführungszeichen - bei Betroffenen nicht stattfindet. Ob sich das im Internet irgendwann anders darstellt, vermag ich jetzt nicht zu sagen. Aus meiner Sicht sind das eben ähnliche Unterstellungen wie auch bisher bei der Telefonüberwachungsdebatte, wo man auch gesagt hat, wer will, kann sich sichern. Natürlich kann ich meine Telefonate von jeder XY-Telefonzelle führen, wechselnd, und dann auch noch nach Hamburg fahren und dort telefonieren. Das geht alles. Die Frage ist, ob es gemacht wird und ob dann tatsächlich jeder Straftäter, um die Internetverbindung aufzubauen, seine E-Mail abzurufen, jedes Mal in ein Internet-Café fährt, jedes Mal sich vielleicht im Ausland einwählt, jedes Mal unter Umständen mehrere hundert Kilometer fährt, um dort eine unüberwachte Internet-Verbindung durchzuführen. Das ist eben die Frage, ob es tatsächlich so ist. Das sind Spekulationen, an denen kann ich mich nicht beteiligen, weil es bislang keine Erfahrungswerte gibt. Da wird uns aber letztlich der Erfahrungswert bei der Telefonüberwachung nicht weiterhelfen. Das sehe ich auch so, aber wir haben keine endgültige Aussage.

Vorsitzender: Dankeschön. Herr Akmann, bitte.

Andreas Reisen (Bundesministerium des Innern): Herr Tauss, wenn Sie erlauben, würde ich gerne auf diese Frage eingehen.

Vorsitzender: Herr Reisen, wenn Sie sich so geeinigt haben, dann ja.

Andreas Reisen (Bundesministerium des Innnern): Also, zunächst einmal möchte ich mich der Stellungnahme von Herrn Dr. Graf im Wesentlichen anschließen. Ich muß dazu aber noch einmal auf die Krypto-Eckpunkte vom Juni 1999 zurückkommen, da ist nämlich genau dieser Aspekt bereits berücksichtigt und im Krypto-Eckpunkt 4 auch behandelt worden. Dass nämlich hier aufgrund der Aufgaben der Strafverfolgungs- und Sicherheitsbehörden der Entwicklung Rechnung getragen werden muß. Die Bundesregierung hat festgehalten, dass sie die Entwicklung aufmerksam beobachtet und dann einen Erfahrungsbericht

über die Entwicklung der mißbräuchlichen Verwendung von Kryptographie vorlegt. Die bisher vorliegenden Erkenntnisse - auch wenn Herr Prof. Pfitzmann darauf hingewiesen hat, dass in einigen Jahren die Situation sicherlich eine andere ist - geben für uns zum jetzigen Zeitpunkt keinen Anlass, die Krypto-Eckpunkte von 1999 in diesem Gesichtspunkt zu ändern. Die vorliegenden Fallzahlen, dass Kryptographie verwendet worden ist, sprechen nicht dafür, an den Maßnahmen, die jetzt auch im Rahmen der Telekommunikations-Überwachungs-Verordnung vorgeschlagen werden, vor dem Hintergrund, dass es so gut wie keine oder ich sage einmal, wenig mißbräuchlich verwendete Kryptographie gibt, an diesen Maßnahmen zu zweifeln und daran, dass sich ein tatsächlicher Benefit für die Strafverfolgungsbehörden noch einstellt.

Vorsitzender: Vielen Dank. Es haben sich Herr Prof. Pfitzmann und Herr Gramm noch einmal gemeldet. Herr Prof. Pfitzmann, ich hätte nochmals, weil auch Herr Graf es angesprochen hat, den Bereich der Sprachtelefonie von Ihnen in für einen Laien verständlichen Worten behandelt, die Frage, ob tatsächlich die Überwachung der Sprachtelefonie im analogen Bereich, die an verschiedenen Stellen angesprochen worden ist, auf Datennetze so ohne weiteres möglich ist und wo daraus Probleme resultieren. Dieses bitte ich jetzt, mit Ihrer Anmerkung zu verbinden.

Prof. Andreas Pfitzmann (Technische Universität Dresden): Herr Tauss, es ist klar, dass man aus der Vergangenheit lernen muss und dass man die Zukunft nie genau kennt. Man muß sich auch Mühe geben zu erkennen, wo man extrapolieren kann und wo es einen Trend geben wird. Wir haben beim Internet - überhaupt bei IT - öfter erlebt, dass etwas ganz lange erst einmal noch nicht passiert, obwohl alle davon reden, und dann passiert es ganz schnell und ist ein Massenphänomen. Kryptographie wird so ein Bereich sein. Krypto können sie in der Kommunikation dann sinnvoll anwenden, wenn ihre normalen Kommunikationspartner alle auch bereit sind, Krypto anzuwenden, dann machen sie nämlich Folgendes: Sie ändern in Ihrem E-Mail-Programm die Grundeinstellung, ob im Zweifelsfall verschlüsselt wird oder nicht. Die meisten Leute arbeiten momentan mit einer Grundeinstellung, wo sie einen Extraknopf drücken müssen, wenn sie verschlüsseln wollen, weil es ist bisher noch kein Massenphänomen ist. Meine Vorhersage ist, dass zu erwarten ist, dass irgendwann - ich kann Ihnen auch nicht sagen, ob in einem halben oder in drei Jahren - die Mehrheit der Leute bereit ist, an der Verschlüsselung teilzunehmen und dass innerhalb von wenigen Monaten alle Leute diese Einstellung ändern. Auf einmal hat sich grundlegend etwas geändert, denn jetzt verschlüsselt man auch abends um 11.00 Uhr, wenn man nahezu vollständig betrunken ist. Das ist absehbar, da braucht man kein Prophet zu sein, das ist nichts Mystisches, das passiert dann einfach. Für diese Sache, denke ich, muss man vorbereitet sein. Wenn die Bundesre-

gierung jetzt sagt, sie fördert sichere Infrastrukturen, insondere sichere digitale Signaturen, dann fördert sie damit auch genau die Infrastruktur, die ich brauche, um dieses Verschlüsselungsphänomen, was ich gerade beschreibe, in Gang zu setzen. Also, bitte, da müssen sich die Bundesregierung und auch das Innenministerium einmal überlegen, wollen sie jetzt das oder das - und bitte klar sagen, was sie wollen. Das ist der erste Punkt.

Der zweite Punkt ist, wenn man nichts sieht, dann gibt es dafür zwei Erklärungen, da ist nichts oder man sieht schlecht hin. Wenn ich momentan Krimineller wäre, dann würde ich mir sehr gut überlegen, ob ich jetzt mit Kryptographie, die noch kein Massenphänomen geworden ist, arbeite, wenn ich Alternativen habe. Die Alternative ist Steganographie, d.h., ich verstecke die Daten, die ich geheimhalten will, in Daten, die völlig harmlos aussehen. Dass Sie momentan bei den Kriminellen und den Leuten, die sie zu überwachen versuchen, wenig Krypto finden, das bedeutet nur, dass Krypto noch kein Massenphänomen geworden ist und dass die Leute, die Sie überwachen, nicht blöd sind. Wenn sie etwas tun, dann machen sie momentan Steganographie. Wenn die Steganographie gut ist, dann finden Sie das nicht. Also, soweit die technischen Sachverhalte. Zu einer Anmerkung von Ihnen, wenn man per E-Mail erreichbar ist, müsste man die Anonymität aufheben, also das müssten wir sozusagen technisch genau diskutieren. Natürlich, wenn Sie einen Kontaktpunkt haben, müssen sie den Kontaktpunkt angeben, das ist klar - aber Sie würden das auch etwa im Agentenmilieu tun. Ich beschreibe das jetzt einmal gegenständlich: Wenn Sie einen toten Briefkasten benutzen - das können sich jetzt alle vorstellen, weil die E-Mail-Adresse etwas mystisch ist -, dann müssen Sie auch die Anonymität aufheben und ihren vollen Klarnamen an den Briefkasten tun. So ähnliche Dinge gibt es auch im Internet. Man kann das entsprechend implementieren. Also, glauben Sie es mir, darüber mache ich seit 18 Jahren Forschung.

Zu der Frage: Kann man sich im Ausland einwählen, und wer macht das? Wir haben als Ziel, dass internationale Telekommunikation preiswert wird. Ich bekenne mich, ich bin ein ganz naiver Telekom-Kunde. Da kenne ich jetzt die Tarife. Wenn ich ins Ausland telefoniere, dann zahle ich momentan – ich habe einen Sondertarif abgeschlossen, das kostet mich 10,00 DM/Monat - neun Pfennig und mein günstiger Preis, um in Deutschland ein Ortsgespräch zu führen, um mich in der Uni einzuwählen, ist drei Pfennig. D.h., mich über das Ausland einzuwählen, kostet mich sage und schreibe dreimal so viel; im Extremfall, wenn ich das Ganze werktags mache, ist das noch anders, dann kostet es mich sechs Pfennig. Eine Alternative wären neun Pfennig, dann reden wir jetzt also über 50 Prozent. Das heißt also, wenn Sie hier in der Bundesrepublik versuchen etwas durchzusetzen, so unwirksam es auch immer sein mag, und die Leute haben das Gefühl - also jetzt eine Faktenvermutung - sie bekommen im Ausland besseren Service, ich habe Ihnen gerade die Zahlen für die Telekommuni-

kation gesagt, was glauben Sie, was das hier für die Internet-Wirtschaft bedeutet. Dankeschön.

Vorsitzender: Vielen Dank. Herr Gramm, bitte.

Tobias Gramm (UUNET): Dankeschön. Ich möchte die Diskussion noch einmal auf das Internet-by-Call bringen. Das klingt alles so furchtbar kompliziert, Kryptographie, Verschlüsselung, um Gottes willen, damit wollen wir alle nichts zu tun haben, das ist furchtbar, das Verstehen sowieso nur „Treckies“, usw. Internet-by-Call, es geht darum, dass das Argument der Cyber-Force-Behörden, warum sie abhören sollen, Folgendes ist: Der Kriminelle wird so schlau sein, häufiger seinen Anschluss zu wechseln, deswegen scheitert das Abhören auf der Carrier-Ebene. Er ist zwar so schlau, zur Oma zu gehen und seine kriminelle E-Mail zu versenden, aber nicht schlau genug, um das, nebenbei gesagt, kostengünstige Verfahren Internet-by-Call zu verwenden, wobei wir davon ausgehen, dass er keine Kryptoprodukte einsetzen wird. Das halte ich für unglaubwürdig. Herr Dr. Graf, Sie sagen Ihre Erfahrungen zeigen das Gegenteil. In dem Zusammenhang möchte ich auf die Aussage der Vertreter des BMI hinweisen. Sie sagen, die Studie, die Sie gerade über den Erfolg von Überwachungsmaßnahmen gemacht haben, hätte einen Einfluss auf die TKÜV. Ich frage mich, wie wir die Verhältnismäßigkeit von Kosten wirklich prüfen wollen, wenn Sie sagen, der Erfolg von Überwachungsmaßnahmen spielt bei der Prüfung der Verhältnismäßigkeit überhaupt keine Rolle. Gleichzeitig berufen Sie sich aber bei der Diskussion um die TKÜV auf Ihre Erfahrungen bei der Strafverfolgung, im Grunde genommen also doch wieder auf den Erfolg. Da müssten Sie mir einmal klar sagen, wie Sie die Verhältnismäßigkeit der Kosten prüfen, mit denen Sie uns belasten wollen. Hier ging es auch noch einmal um Kosten der Verschlüsselung: PGP ist umsonst, das können Sie sich umsonst im Internet herunterladen. Ich kann die Argumente, die hier zum Teil ausgetauscht werden, kaum noch nachvollziehen.

Vorsitzender: Herr Dr. Graf ist angesprochen worden, er wird auch noch Gelegenheit zur Antwort bekommen, aber zunächst einmal Frau Bonitz mit einer Frage und dann Herr Bogk.

Abg. Sylvia Bonitz (CDU/CSU): Ich habe noch ein gewisses Verständnis dafür, wenn wir bei der Strafverfolgung auf Grundlage des Status quo diskutieren und sagen, dass Kryptographie, zur Zeit jedenfalls, noch nicht als Massenphänomen eingesetzt wird, aber ich halte es doch für wichtig - Sie haben das auch gesagt, Herr Prof. Pfitzmann -, dass wir auch ein bisschen den Trend berücksichtigen müssen. Insofern möchte ich schon die Frage an den Vertreter des BMI stellen - man müsste sie auch an die Vertreter des BMJ stellen, wenn wir sie hier hätten: Wie kann denn eigentlich in Zukunft eine effektive Strafverfolgung im Bereich

der Cyber-Kriminalität aussehen, wenn wir im Grunde genommen davon ausgehen, dass irgendwann die Inhalte wesentlich stärker verschlüsselt werden, was auch von der Bundesregierung gewünscht wird? Diesen Trend wollen wir auch unterstützen, d.h., dass wir im Grunde genommen eigentlich damit gleichzeitig unser Interesse als Staat an der Strafverfolgung von vornherein auch wieder erschweren. Ich frage in diesem Zusammenhang nochmals anhand der Stellungnahme des BKA, von der ich jetzt immer noch nicht weiß, warum sie zurückgezogen wurde, deren Inhalt ich somit eigentlich nicht kenne, ob denn das BKA vielleicht der Meinung gewesen sein könnte, dass zwar auf der einen Seite nach dem Entwurf der TKÜV jetzt vorgesehen ist, natürlich die Provider im Grunde genommen zu verpflichten, wenn es Verschlüsselungen geben sollte von Daten, hier Dinge offen zu legen, aber das dann, wenn private Verschlüsselungsprogramme im Rahmen der Kryptographie zum Beispiel bei PGP eingesetzt werden,dass dann eben auch keine Verpflichtung erfolgen kann. Also, dass diese Einschränkung auch ganz klar gesehen wird, dass die Inhalte damit eben nicht lesbar würden. Die Frage ist: Was wollen wir denn feststellen? Wollen wir im Grunde genommen bei einer Strafverfolgung auch die Inhalte kontrollieren, wie es zum Beispiel bei telefonischen Abhörmaßnahmen erfolgt? Das ist ja gerade der knifflige Punkt. Wie wollen Sie hier eigentlich eine effektive Strafverfolgung in der Zukunft gewährleisten - jetzt unabhängig vom intellektuellen Level der Kriminellen, bei denen eben jetzt schon die Pfiffigen in der Lage sein würden, auch bei der neuen TKÜV, sich diesen Dingen zu entziehen, und wir dann vielleicht nur die Dümmeren bekämen. Wie wollen Sie das in Zukunft gewährleisten, wenn wir gleichzeitig einen Trend befördern, der immer intelligentere Verschlüsselung ermöglicht, so dass Strafverfolgung danach dann eigentlich, auch nach Ihrem Entwurf der TKÜV, im Grunde genommen nicht mehr stattfinden könnte.

Vorsitzender: Herr Kelber.

Abg. Ulrich Kelber (SPD): Ein Aspekt, der mir noch wichtig ist, ist die Frage, inwieweit die Gefahr besteht, das Fernmeldegeheimnis unbeteiligter Dritter zu verletzten. Die Frage 14. Wir haben da sehr unterschiedliche Antworten. Wenn ich mit Erlaubnis des Vorsitzenden ganz kurz zitieren darf, zum Beispiel von Herrn Dr. Graf: „Der Verpflichter hat sicherzustellen, dass nur der in der Anordnung bezeichnete Anschluss überwacht wird.“ Antwort zum Beispiel vom DIHK - bei meinem technischen Verständnis und auch als Informatiker in meinem Privatberuf, habe ich, glaube ich, ein bisschen davon zu verstehen -. steht: „Bei paketvermittelter Datenkommunikation besteht grundsätzlich die Gefahr, das ins Fernmeldegeheimnis Dritter eingegriffen wird. Grund dafür ist, dass bei paketvermittelter Datenübertragung die Nachrichtenkette nicht immer vom Nachrichteninhalt separiert werden kann, ohne den Nachrichteninhalt selbst aufzuschließen. Außerdem werden IP-Adressen dem Nutzer

dynamisch zugeteilt, so dass es sein kann, dass die IP-Adresse zum Zeitpunkt der Überwachung von einem anderen Teilnehmer genutzt wird, auf den sich die Überwachungsanordnung nicht bezog.“ Wenn die Antworten vom BMI und von der Bundesanwaltschaft weiter stimmig sein sollen, dann müssen Sie mir bitte erklären, was an dieser Antwort falsch ist.

Vorsitzender: Die Frage war an Herr Dr. Graf und Herr Akmann gerichtet.

Andreas Bogk (Chaos Computer Club): Ich wollte zum Einsatz von Kryptographie noch etwas sagen, weil ich doch den Verdacht hatte, dass Herr Dr. Graf davon ausgeht, dass in der Praxis so etwas nicht eingesetzt wird. Nun habe ich dieses Notebook hier vor mir stehen, da ist nicht die Festplatte mit meinen Mails verschlüsselt, sondern sämtliche Verbindungen, die nach draußen gehen, finden verschlüsselt statt. Das heißt also, da steht irgendwo ein Mailserver, der nimmt meine Mail entgegen, der steht derzeit in Deutschland, der könnte ganz genauso gut in Afrika oder sonst wo stehen. Nach der derzeitigen Telekommunikations-Überwachungs-Verordnung ist alles, was man von meiner Internet-Kommunikation sehen würde, eine verschlüsselte Verbindung mit diesem Rechner - und entgegen der landläufigen Meinung ist das auch nicht besonders schwierig. In der Firma, in der ich arbeite, in der ich Teilhaber bin, arbeiten mittlerweile 50 Leute und sogar die Geschäftsführer und Vorstände sind in der Lage, verschlüsselt zu arbeiten, da muss man nur im Netscape Navigator sein X-509-Client-Zertifikat eintragen, das ist einfach, dass bekommt man einfach geschickt. Da drückt man auf den Knopf. Dann sagt man: „gesicherte Verbindung an“ und der Netscape verschickt und holt die Mail über eine verschlüsselte Leitung. Da muss man sich kein aufwendiges PGP installieren. Das hat den zusätzlichen Vorteil, dass man auch den Sender und Empfänger der Mail nicht sieht, d.h., man kann auch keine Traffic-Analyse daraus machen. Das ist einfach, das ist „deployed“ und im Grunde genommen findet hier etwas statt, dass wir nämlich eine unglaublich große Menge Geld - die gibt nicht einmal der Staat aus, sondern die wird dem Betreiber aufgedrückt, der das dann wahrscheinlich auf die Kunden umlegen wird - dafür ausgeben, dass wir nichts gewinnen, außer ein Instrumentarium, in dem der unbescholtene Bürger überwacht werden kann, um zu sehen, wie oft er denn auf den „Spiegel“ oder auf die „Bild“ geklickt hat! Für die Strafverfolgung fallen eigentlich keinerlei sinnvolle Informationen mehr ab, sondern die Art der Information, die dann anfällt, ist nur noch geeignet, Profile von Leuten zu schaffen, deren Verwendung im besten Fall zweifelhaft ist.

Vorsitzender: Herzlichen Dank, Herr Bogk. Damit verwenden Sie ganz offensichtlich die selbe intelligente Technik wie der Bundesinnenminister. Ich hoffe, Sie sind gleich gut geschützt. Wir haben jetzt einige Fragen an Herrn Dr. Graf. Herr Dr. Graf, ich würde Sie ganz

einfach bitten, ganz kurz auf die beiden Punkte einzugehen. Dann Herr Akmann auf die Fragen der Kollegin Bonitz und des Kollegen Kelber.

Dr. Jürgen-Peter Graf (Bundesanwaltschaft): Ganz kurz direkt zum Nächsten. Ich habe natürlich nicht bezweifelt, dass es solche Programme gibt. Das ist gar keine Frage, dass es die gibt. Ich habe nur bezweifelt, dass sie allgemeine Anwendung finden. Dass es Leute gibt, die solche Programme anwenden, bezweifle ich ebenfalls nicht. Die Frage ist nur, wie stark sie Anwendung finden. Genauso die Frage, wie stark Kryptographie-Programme Anwendung finden. Ich meine, es ist natürlich auch bekannt, dass Steganographie inzwischen ein sehr einfaches und auch einfach anzuwendendes Hilfsmittel ist. Wenn Sie Steganographie verwenden, brauchen Sie dafür ebenfalls ein Programm. Wenn wir dann den Rechner eines Betroffenen haben und dann kein entsprechendes Programm darauf finden, kann mit relativ großer Sicherheit davon ausgehen, dass er Steganographie nicht verwendet. Es sei denn, er hat mehrere Rechner, dann muss man dieses anders betrachten. Was die Frage „Kosten und Verhältnismäßigkeit“ betrifft, das ist in der Tat zu bedenken. Ich sage, dazu muss man auch wissen, welche Kosten entstehen. Ich habe heute zum ersten Mal von Herrn Gramm gehört, dass es eine solche Schätzung gibt. Bislang - selbst kürzlich bei der Veranstaltung der eco auf dem Petersberg - hat sich keiner der Provider auf einen Kostenpunkt festlegen können. Wie gesagt, Sie sind heute der Erste, der eine Summe auf den Tisch legt, wobei die Summen bislang zwischen 100.000 DM, mehreren Hunderttausend und mehreren Millionen liegen, je nach Providergröße und sicherlich auch je nach Technik, die dem zugrunde liegt. Wenn da auch von anderen Providern Summen genannt werden, dann kann man in der Tat auch über eine Modifizierung der zugrunde liegenden Technik reden; vielleicht auch mobile Anlagen einsetzen, wenn das organisatorisch geklärt werden kann. Das wären sicherlich Dinge, über die man reden kann und über die in den betroffenen Gruppierungen, Gremien - Herr Tauss hat das ja vorhin genannt - vielleicht zu reden ist.

Der andere Punkt: Eingriff ins Fernmeldegeheimnis unbeteiligter Dritter. Hier muss man sagen, das ist kein spezifisches Problem einer Internet-Überwachung. Bei jeder Fernmeldeüberwachung wird auch in das Fernmeldegeheimnis Dritter eingegriffen. Wenn Sie - ich muss jetzt wieder auf die Telefonüberwachung zurückgreifen, es ist ganz einfach darzustellen - eine Telefonleitung eines Betroffenen überwachen, dann werden Sie auch immer in das Fernmeldegeheimnis Dritter eingreifen, sei es der Friseur, der vom Betroffenen angerufen wird, sei es auch vielleicht sein Arzt oder sei es etwas anderes. Sie werden immer Eingriffe haben und es gilt dann, das war schon bislang die Thematik der Ermittlungsbehörden, diese Dinge herauszufiltern, diese Dinge dann sofort von der Überwachung auszuschließen oder die Protokolle zu sperren. Das geschieht inzwischen auch immer, wenn abgehört wird. Die Ermittlungsrichter wissen das inzwischen auch, die haben sich auch technisch fortgebildet.

Das steht auch meist in den Überwachungsanordnungen, dass diese Protokolle eben, sobald Unbeteiligte überwacht werden und es mit dem Ermittlungsgegenstand nichts zu tun hat, sofort gelöscht oder gesperrt werden. Das ist auch jetzt schon ein Thema und da muss man in der Tat auch dafür sorgen, dass dann das Instrumentarium, was die Ermittlungsbehörden, die Polizei, die Bedarfsträger haben, darauf eingestellt wird. Schließlich noch der letzte Punkt: Überwachungsanordnung von IP-Adressen. Ich kenne bislang keine Überwachungsanordnung, die auf eine IP-Adresse gerichtet ist, wahrscheinlich deshalb - das haben Sie selbst gesagt -, weil die IP-Adressen dynamisch erteilt werden. Insofern kann man IP-Adressen, es sei denn, es ist eine feste IP-Adresse, nach meinem Kenntnisstand derzeit auch so nicht überwachen. D.h., es wird immer darum gehen, dass man schon einen Bezugspunkt hat, eine Kennnung, die wie auch immer geartet ist; Überwachung von IP-Adressen ist mir bislang nicht bekannt.

Vorsitzender: Auch Herr Gramm hat sich gemeldet. Sie haben gleich die Gelegenheit, aber wir haben jetzt noch einige Wortmeldungen. Ich glaube, das ist auch ein ganz interessanter Teil der Diskussion, wobei wir 17.30 Uhr haben und uns dann langsam dem Ende nähern.

Torsten Akmann (Bundesministerium des Innern): Frau Bonitz, Sie hatten nachgefragt, wie wir uns in Zukunft eine effektive Strafverfolgung im Bereich Cyber-Crime vorstellen. Das ist natürlich auch schwierig zu beantworten. Ich möchte auch keine Prognose abgeben. Aber ich bin ihnen trotzdem dankbar für diese Frage, denn das ist ja genau der Grund, warum sich 43 Europaratstaaten in Straßburg zusammengesetzt und die Cyber-Crime-Konvention erarbeitet haben. Im Übrigen ist das auch der Grund dafür, dass die G 8-Staaten im Rahmen einer High-Tech Sub-Group zusammenarbeiten, die sich regelmäßig trifft. Die EU-Kommission ist jetzt auf dem Feld aktiv geworden. Auch die EU bzw. die Kommission plant im Übrigen, hier ein EU-Forum einzusetzen. Das wird im September dieses Jahres das erste Mal tagen. Da wird auch die Bundesregierung vertreten sein, mit den verschiedenen Ressorts. Im Übrigen werden wir natürlich auch im nationalen Rahmen Überlegungen anstellen, wir prüfen dort, ob nicht im Bereich des Strafrechts oder auch des Strafverfahrensrechts Novellierungen angebracht sind. Ich kann auch auf die Große Anfrage der CDU/CSU-Fraktion verweisen, die wir beantwortet haben. Was Ihre andere Frage in Sachen Kryptographie anging: Auch das BKA ist sich dieses Problems bewusst und hat nicht zuletzt vor diesem Hintergrund jetzt geplant, bis zum Ende des Jahres ein IUK-Kompetenzzentrum einzurichten, das sich auch mit diesen Fragen beschäftigen wird. Soweit zu den Fragen von Frau Bonitz.

Vorsitzender: Können wir dann mit den ganzen Entwürfen nicht warten, bis dieses Kompetenzzentrum eingerichtet ist und wir von dort vielleicht noch Antworten bekommen

Torsten Akmann (Bundesministerium des Innern): Dazu möchte ich jetzt nichts sagen.
Der Vorsitzende: Okay.

Torsten Akmann (Bundesministerium des Innern): Das zu den Fragen von Frau Bonitz; bei Ihnen, Herr Kelber, da kann ich mich eigentlich nur Herrn Dr. Graf anschließen. Danke.

Vorsitzender: Vielen Dank. Ich habe jetzt in der Reihenfolge Herrn Prof. Pfitzmann, Herrn Dr. Dix und Herrn Gramm.

Prof. Andreas Pfitzmann (Technische Universität Dresden): Eine Anmerkung zu dem, was Herr Dr. Graf sagte, dass man Steganographie immer im nachhinein entdecken könnte, wenn man Geräte beschlagnahmt. Es gibt in der steganographischen Forschung seit etwa vier Jahren Arbeiten darüber, dass man Dateisysteme auf einem Rechner so gestalten sollte, dass man bereits die Existenz von Dateien verbirgt, in verschiedenen Leveln, je nachdem, wie Sie sich einloggen usw. Da ist an der Stelle der Trend absehbar, dass das, was Sie momentan beschreiben und was momentan zutrifft, größtenteils auch unwirksam werden wird. Jetzt wurde die Frage gestellt: Wie effektiv ist Strafverfolgung langfristig? Ich will versuchen, Ihnen diese Frage so gut zu beantworten, wie ich es aus meiner technischen Kenntnis heraus kann. Wenn man über Cyber-Kriminalität spricht, muss man zwei Dinge strikt auseinanderhalten. Nämlich Kriminalität, klassische Kriminalität, die es eigentlich immer schon gab, die im Wesentlichen außerhalb des Netzes wirkt und die sich des Netzes nur bedient. An der Stelle gilt, diese Kriminalität bekämpfen Sie außerhalb des Netzes. Sie haben langfristig wirklich keine Chance, sie im Netz zu bekämpfen. Bekämpfen Sie sie außerhalb, fokussieren Sie Ihre Ressourcen! Es ist Verschwendung von Steuergeldern zu versuchen, diese Kriminalität im Netz zu bekämpfen.

Die zweite Art von Kriminalität richtet sich auf Dinge, die es nur im Netz gibt. Sie hat also Serverinformationen, das, was im Netz ist, als Ziel. Da ist die Antwort schwieriger. Langfristig ist die wirksamste Bekämpfung dieser Kriminalität ein sicheres Netz, also ein sicheres IT-System, zu bauen. Bauen Sie eine sichere Infrastruktur. Das löst Ihre Probleme wie Hacking, das löst eine ganze Menge Probleme - manche Probleme natürlich nicht, also etwa die Frage missliebiger Inhalte im Internet, dass da Dinge zugreifbar sind, wo manche Staaten und Normgemeinschaften sagen, das wollen wir nicht - dieses Problem lösen Sie nicht. Aber es gibt vielleicht auch Probleme auf der Welt, die unlösbar sind. Es ist besser, das zu akzeptieren als im Versuch, sie lösen zu wollen, größeren Schaden herbeizuführen. Also, die wesentliche Sache, um Kriminalität im Netz zu verhindern, ist: Bauen Sie ein sicheres Netz und

versuchen Sie nicht etwa, das Netz unsicherer zu bauen, um noch in alles Mögliche hineinzukommen. Für eine gewisse Übergangsfrist - ich hatte vorhin angedeutet, das Bauen einer sicheren Infrastruktur sei Aufgabe für einige Jahrzehnte - statten Sie die Polizei, auch die Geheimdienste, gut mit IT-Know-how aus, so dass sie die bestehenden Unsicherheiten - nicht etwa Unsicherheiten, die Sie vorschreiben, die Sie hineinkonstruieren, sondern die bestehenden Unsicherheiten, die unter den entsprechenden Regularien da sind, je nachdem, um welche Straftaten es geht - dann nutzen dürfen. Das heißt, da hätte ich eine ganz klare Strategie. Kriminalität außerhalb des Netzes wird außerhalb bekämpft, Kriminalität innerhalb des Netzes wird dort zu verhindern versucht. Für eine gewisse Übergangszeit, solange die Systeme noch unsicher sind, rüsten Sie die Leute gut aus und dann dürfen sie diese vorhandenen Unsicherheiten nützen. Alles andere ist eine Ressourcenverschwendung. Wir fokussieren da eine Diskussion, so wie momentan die Fronten aufgebaut werden, auf eine Art, dass das nicht zielführend ist. Dankeschön.

Der Vorsitzende: Herr Dr. Dix

Dr. Alexander Dix (Landesbeauftragter für den Datenschutz, Brandenburg): Vielen Dank. Ich wollte noch einmal an einem Detailbeispiel erläutern, wieso aus meiner Sicht der TKÜV-Entwurf auch innovationshemmende Wirkung haben könnte, und zwar geht es um die Überwachung des Standorts bei Mobilfunkteilnehmern in Mobilfunknetzen. Die gegenwärtigen Mobilfunknetze sind standardisiert so gebaut, dass die Standortkennung erforderlich ist, um überhaupt Verbindungen herzustellen. Das gilt für das GSM-Netz wie auch für den kommenden UMTS-Standard. Darauf setzt die TKÜV, übrigens wie auch schon ihre Vorläuferverordnung, indem sie die Anbieter, die Netzbetreiber verpflichtet, den Standort oder die Funkzelle des jeweiligen Mobilfunkteilnehmers im Überwachungsfall auch bereit zu halten. Diese Fähigkeit wird auch zur Voraussetzung für die Zulassung solcher Netze gemacht, dafür, dass solche Betreiber überhaupt ein Netz betreiben können. Ich behaupte, diese Voraussetzung hat gleichzeitig innovationshemmende Wirkung, denn es gibt Forschung - ziemlich weit gediehen, Herr Prof. Pfitzmann ist einer der Vertreter dieser Forschungsrichtung -, die Mobilfunknetze und Kommunikationsnetze entwickelt, die nicht davon abhängig sind, dass der jeweilige Standort des Teilnehmers überhaupt bekannt wird. Infolgedessen würden solche Netzbetreiber von der Zulassung ausgeschlossen, wenn mit dieser Verordnung das Bereithalten des Standorts des jeweiligen Teilnehmers zwingend zur Voraussetzung gemacht wird. Das ist etwas technisch formuliert, aber ich hoffe, es ist deutlich geworden, was ich meine. Ich meine, ein Verordnungsgeber muss auch darauf achten, dass er sozusagen nicht so technikfixiert auf eine bestimmte Technik, die noch dazu höchst datenschutzunfreundlich ist, setzt, dass er diese Technik quasi einfriert.

Der Vorsitzende: Dankeschön. Herr Gramm, bitte.

Tobias Gramm (UUNET): Ich wollte nur auf die Frage von Herr Dr. Graf eingehen. Auf die Frage der IP-Adresse, weil ich den Eindruck habe, dass durch Ihr Statement meine vorherigen Ausführungen zur Überwachung Dritter ein bisschen in Zweifel gezogen werden. Das ist natürlich wichtig, sie können die Anordnung im Dial-Verkehr nicht auf die IP-Adressse abstellen lassen, weil die IP-Adresse im Vorhinein nicht bekannt ist, sondern dynamisch zugewiesen wird. Sie werden die Anordnung deswegen auch auf Login ausstellen, das Problem ist nur, das Login tritt, nachdem der Kunde sich zum ersten Mal damit authentifiziert hat, niemals wieder auf. Wir müssen dafür sorgen, dass wir das Login dann auf die zugewiesene IP-Adresse matchen und dann die IP-Adresse überwachen. Anders geht es technisch schlicht und ergreifend nicht. Deswegen überwachen wir im Endeffekt natürlich doch die IP-Adresse mit genau den Problemen, die ich gerade geschildert habe. Danke.

Vorsitzender: Frau Bonitz, ich hätte noch eine kurze Frage an Herrn Bogk. Wir waren bei dem ganzen Themenbereich „Hacking“. Wir haben über den Bereich Werkzeuge und diese Dinge noch nicht geredet. Mich würde einfach interessieren, an irgendeiner Stelle, quasi als Ihr Schlusswort, ob der Chaos Computer Club demnächst dann eine illegale Vereinigung ist oder ein e.V. bleiben kann. Jetzt hat Frau Kollegin Bonitz das Wort.

Abg. Sylvia Bonitz (CDU/CSU): Ich bin Herrn Prof. Pfitzmann dankbar, dass er noch einmal zum Schluß sehr klar zwischen den unterschiedlichen Formen von Cyber-Kriminalität, über die wir hier reden, differenziert hat und das im Grunde genommen auch mit einem Plädoyer verbunden hat. Deswegen daraus resultierend eine Frage an die Vertreter des BMI. Es passt sicherlich sehr gut, dass Sie heute hier sind und das BKA vielleicht doch kompetent ergänzen können. Ich kann mich daran erinnern, dass der Präsident des BKA mir einmal gesagt hat, dass es ungemein schwierig ist, im BKA entsprechende Fachleute für diesen EDV-Breich einstellen zu können, die dann natürlich auch ein entsprechendes Gehalt bekommen, weil wir bei uns bestimmte Grenzen kennen, weil dort auch kein Ausgleich zwischen Sachkosten und Personalkosten stattfinden kann. Ist dieses Problem inzwischen gelöst, so dass hier inzwischen kompetente Leute, denn wir brauchen auch dafür Spitzenkräfte, für die Strafverfolgung im BKA eingestellt werden können? Weil in der Öffentlichkeit immer wieder unterschiedliche Zahlen kursieren und da der Eindruck entsteht, dass im BKA ein Riesentrupp von Beamten in der Lage ist, eine effektive Strafverfolgung wahrzunehmen, würde mich interessieren, dass Sie vielleicht einmal die Größenordnung darstellen könnten, wie viele Mitarbeiter im BKA für diesen Bereich zuständig sind.

Vorsitzender: Vielen Dank. Ironisch wollte ich es anmerken, am 24. September machen wir eine Anhörung zum Thema Besoldungsrecht, aber das betrifft einen anderen Teil. Als Nächster Herr Akmann, bitte.

Torsten Akmann (Bundesministerium des Innern): Die Frage ist für mich schwer zu beantworten - aus zwei Gründen. Zum einen ist die Frage, die Sie gestellt haben, eine beamtenrechtliche Frage, die ich eigentlich, da ich aus der Polizeiabteilung komme, nicht beantworten kann, zum anderen gibt es auch die Personalhoheit des BKA. Was mir aber bekannt ist, ist, dass im Rahmen dieses von mir eben erwähnten Kompetenzzentrums schon darüber nachgedacht wird, hier auch neue Wege zu suchen. Ich hoffe, dass ich Ihnen ausreichend geantwortet habe.

Vorsitzender: Sie kennen unsere Rechnungshöfe und all das. Bei den Forschungseinrichtungen probieren wir es gerade, aber das ist ein Thema für sich. Die Rechnungshöfe sind noch vor. Aber das ist selbstverständlich ein wichtiger Hinweis, wenn wir die Kompetenz haben wollen, dann müssen solche Dinge auch möglich sein.

Torsten Akmann (Bundesministerium des Innern): Sie sprachen diese Anzahl von Personen an, die dort arbeiten. Was ich Ihnen sagen kann, ist, dass in dem gegenwärtigen Referat OA 34 oder insbesondere dieser Zentralstelle für die Recherche beim BKA 20 Personen arbeiten.

Andreas Bogk (Chaos Computer Club): Ich bin ganz froh, dass Sie den Punkt angesprochen haben. Das ist ja auch einer der Paragraphen der Cyber-Crime-Konvention, dass Werkzeuge zum Hacking, was auch immer Sie dann darunter verstehen, unter Strafe fallen sollen. Ich sehe schon ein bisschen das Problem, dass die Forschung darunter leiden wird, dass Leute, die sich mit diesem Problembereich beschäftigen, sei es, weil sie selber Systeme haben, die sie schützen müssen, sei es aus Neugierde, kriminalisiert werden. Letzten Endes fragen sich alle: Wo soll denn das Personal herkommen? Wo kommt der Nachwuchs her? Und bei uns sitzen Leute, die um die 15, 16, 17 zu uns kommen, sich für Computer und Computersicherheit interessieren, etwas lernen wollen, denen wir sagen müssen, wir können euch nichts sagen und wir dürfen euch nichts geben, denn dann machen wir uns strafbar und ihr euch auch. Dann wird dieses Land irgendwann ohne Sicherheitsexperten dastehen, darin sehe ich eine ganz große Gefahr. Auch die Überlegung, die dahinter steht, ist eigentlich ziemlich unsinnig. Was hilft es denn der Bundesrepublik Deutschland, wenn ihre Verwaltung zwei Tage lang lahmgelegt wird, und dann dafür irgendein 16-jähriger amerikanischer Teenager zwei Jahre ins Gefängnis geht. Dadurch sind die Kosten auch nicht wieder

da und der Schaden ist trotzdem entstanden. Werkzeuge zu verbieten, ist der völlig falsche Ansatz. Im Gegenteil, es muss eine Öffentlichkeit für solche Werkzeuge geschaffen werden, damit auch den letzten Systemadministratoren klar ist, wo die Gefahren liegen und damit auch dem letzten Anwender klar wird, was er eigentlich tut. Die Einladung zu der Veranstaltung heute habe ich per E-Mail erhalten, mit einem Word-Dokument - das ist der übliche Verbreitungsweg von Viren. Wenn ich jetzt böse wäre, dann könnte ich, nachdem ich weiß, dass da Word-Dokumente verschickt werden und die Leute auch darauf klicken, die Word-Dokumente mit einem Virus zurückschicken. Wenn ich mich geschickt anstellen würde, dann wäre das nicht ein Virus wie „Melissa“, der einfach alles lahmlegt, sondern der würde sich ganz bescheiden im Hintergrund installieren und mir einmal am Tag sämliche neuen Dokumente von der Festplatte zuschicken und dann würde ich wissen, was die Bundesregierung, was die Parlamentarier so tun. Nichtsdestotrotz, wenn man über solche Probleme nicht diskutieren kann, wenn man solche Viren nicht analysieren kann und nicht sehen kann, was man hier für Technologien einsetzt, dann ist man da anfällig, dann landet man letztendlich bei großen anfälligen Systemen und das ist genau das, was wir nicht wollen. Insofern bin ich für die Ausführungen von Herrn Pfitzmann sehr dankbar, weil das genau meine Meinung widerspiegelt. Es geht hier um Prävention und nicht darum, irgendjemanden für etwas zu bestrafen, für das er eigentlich keine Schuld hat. Das liegt daran, dass wir unsichere IT-Infrastrukturen haben.

Vorsitzender: Ganz herzlichen Dank, Herr Bogk. Sie können immer sicher sein, dass Sie aus dem Deutschen Bundestag keine Viren bekommen, darauf können Sie vertrauen; aber ansonsten sind auch wir hier damit beschäftigt, uns zu überlegen, ob wir mit etwas sicherer Software noch etwas mehr für unsere eigene Sicherheit tun können. Da gibt es übrigens im Bereich „Open Source“ zur Zeit ein paar Diskussionen, auch im Ältestenrat, der dafür zuständig ist. Das wollen wir jetzt nicht vertiefen. Herr Akmann hat sich noch einmal gemeldet und dann würde ich für eine ganz kurze Schlussrunde plädieren, falls irgendjemand das Gefühl hat, mit einer Meinungsäußerung nicht zu Wort gekommen zu sein. Ansonsten würde ich dann die Veranstaltung schließen, weitere Wortmeldungen sehe ich nicht. Herr Akmann, bitte schön.

Torsten Akmann (Bundesministerium des Innern): Vielen Dank. Ich möchte gerade noch einmal auf den Vorredner Bezug nehmen. Sie haben konkret den Art. 6 der Cyber-Crime-Konvention angesprochen, wenn ich das richtig sehe. Art. 6 handelt von Mißbrauch von Vorrichtungen, d.h., es soll unter Strafe gestellt werden, dass Werkzeuge vertrieben, verkauft, in Besitz genommen werden. Man war sich schon dessen bewußt, dass man hier Ausnahmeregelungen schaffen muss, das sieht auch Abs. 3 vor. Hier werden etwa für die Hersteller

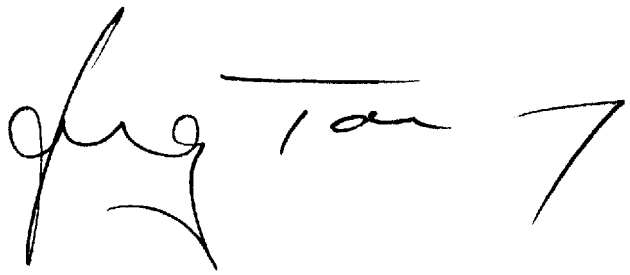
von Antiviren-Programmen Ausnahmen geschaffen. Wie man das im deutschen Recht letztendlich umsetzt, das wissen wir nicht, das kann man eventuell über einen Rechtfertigungsgrund im Strafgesetzbuch oder auch in einem anderen Gesetz machen. Ich kann Ihnen versichern, dass hier Ausnahmen geschaffen werden sollen.

Vorsitzender: Besagter Hersteller wird aber nicht der 16-Jährige sein, der hier angesprochen worden ist. Insofern ist es auch noch einmal ein Punkt, auf den wir noch einmal das Augenmerk richten.

Prof. Andreas Pfitzmann (Technische Universität Dresden): Ich möchte noch einmal betonen, bauen Sie keine neuen Unsicherheitsschnittstellen in irgendwelche Systeme ein. Die Systeme sind unsicher genug, es ist schwierig genug, sie nach und nach sicher zu machen - das ist das mein Statement. Wenn Sie das Gefühl haben, es gibt ein Defizit an Aufklärung im Internet, dann kann ich nur nachhaltig empfehlen, in gut ausgebildete Menschen und deren lokales Equipment zu investieren, aber nicht in neue Unsicherheitsschnittstellen. Ob es dort ein Bedürfnis gibt, wohin Sie die Ressourcen schieben, das ist dann letztlich eine originäre Frage des Parlamentes. Da müssen Sie sich eine Meinung bilden, diese Entscheidung kann ich Ihnen nicht abnehmen, da kann ich Ihnen nicht einmal einen guten Rat geben. Dass man aber nicht neue Unsicherheiten schaffen sollte, da bin mir meines Rates sehr sicher. Dankeschön.

Vorsitzender: Herzlichen Dank. Ich glaube, es war eine hochinteressante Anhörung. Das zeigt sich auch darin, dass wir kaum eine Abbröckelung bis zu dieser sehr vorgerückten Zeit hatten. Über Verschiedenes, was wir heute diskutiert haben, haben sich Parlamentarier auch das erste Mal den Kopf zerbrochen, sich das erste Mal damit beschäftigt. Wir reden hier nicht über Ausschussvorlagen oder Ähnliches, sondern zum Teil über Verordnungen und Entwürfe, die den parlamentarischen Raum noch gar nicht erreicht haben. Insofern glaube ich, haben wir diese Anhörung rechtzeitig durchgeführt. Ich kann auch sagen, es gibt eine Reihe von Parlamentariern, die darum gebeten haben, die Justizministerin solle explizit von einer Unterzeichnung des Cyber-Crime-Abkommens absehen bis die verschiedenen Fragen, die angesprochen worden sind, abgeklärt sind. Insofern, glaube ich, werden wir auch diese Ergebnisse dem BMJ zur Verfügung stellen; selbstverständlich auch dem BMI und unseren Kollegen und Kolleginnen nach entsprechenden Auswertungen auch in den Arbeitsgruppen. Ich möchte übrigens darauf aufmerksam machen, dass Kollegen und Kolleginnen aus diesen Arbeitsgruppen der unterschiedlichen Fraktionen auch eingeladen waren, heute Nachmittag teilzunehmen. Ich darf mich ganz herzlich bedanken und wünsche den Sachverständigen eine gute Heimreise. Ich danke insbesondere den Sachverständigen, dass Sie sich in sehr

umfassender Form zu den Fragen, die wir gestellt haben, aber auch denen, die untereinander aufgeworfen worden sind, geäußert haben. Ich darf mich recht herzlich dafür bedanken.



Jörg Tauss
(Vorsitzender)