Abgeordnetenhaus BERLIN

17. Wahlperiode

Plenar- und Ausschussdienst

Wortprotokoll

Öffentliche Sitzung

Ausschuss für Digitale Verwaltung, Datenschutz und Informationsfreiheit

TOP 2 unter Zuladung des Ausschusses für Verfassungs- und Rechtsangelegenheiten, Verbraucherschutz, Geschäftsordnung und des Ausschuss für Inneres, Sicherheit und Ordnung

21. Sitzung
18. Februar 2013

Beginn: 16.05 Uhr
Schluss: 18.35 Uhr
Vorsitz: Alexander Morlang (PIRATEN)

Punkt 1 der Tagesordnung

Aktuelle Viertelstunde

Siehe Inhaltsprotokoll.

Punkt 2 der Tagesordnung

a) Antrag der Fraktion der SPD und der Fraktion der CDU — 0080
Drucksache 17/0729 — ITDat
Überwachung durch Quellen-TKÜ in Berlin rechtssicher und technisch sauber einsetzen — Recht(f) VerfSch

b) Antrag der Piratenfraktion — 0069
Drucksache 17/0568 — ITDat
Vertragsabschlüsse mit Privatfirmen zum Ankauf von Überwachungssoftware — Haupt

c) Antrag der Piratenfraktion — 0038
Drucksache 17/0197 — ITDat
Kein verfassungswidriger Staatstrojaner in Berlin — InnSichO(f)

Hierzu: Anhörung

Vorsitzender Alexander Morlang: Zum Antrag der Piratenfraktion – Drucksache 17/0568 – liegt ein Änderungsantrag der Fraktion Bündnis 90/Die Grünen vor – als Tischvorlage. – Es

soll eine Anhörung stattfinden. Möchten Sie, dass ein Wortprotokoll erstellt wird? – Ich höre keinen Widerspruch. Ich bitte um ein Wortprotokoll. – Dann kommen wir zur Begründung des Antrags zu 2 a durch die Fraktion der SPD oder der CDU. Wer von Ihnen möchte? – Herr Kohlmeier, Sie haben das Wort!

Sven Kohlmeier (SPD): Herzlichen Dank, Herr Ausschussvorsitzender! – Ich erlaube mir, es kurz zu machen, da die Beratung oder die Begründung jeweils zu sämtlichen Anträgen, die heute auf der Tagesordnung stehen, schon im Parlament und im Plenum erfolgt sind, sodass wir mehr Zeit dafür haben, uns die fachkundige Meinung der Experten anzuhören. In aller Kürze zu unserem Antrag selbst: Die Koalitionsfraktionen aus SPD und CDU haben sich verständigt, an der Quellen-TKÜ als Maßnahme der Strafverfolgung festzuhalten, sind aber der Auffassung, dass es erstens dazu eine Bundesratsinitiative geben soll, die eine neue Rechtsgrundlage in der StPO schafft.

Zweitens haben wir zur Vorgabe für den Einsatz im Land Berlin gemacht, dass zum einen die Vorgaben des Bundesverfassungsgerichts eingehalten werden und zum anderen der Datenschutzbeauftragte auch Prüfungsrechte und Prüfungsmöglichkeiten hat, damit genau das nicht passiert, was dem Bundesdatenschutzbeauftragten passiert ist, der eine entsprechende Software auf Bundesebene nicht prüfen konnte, weil die Firma hohe Tagessätze verlangt hat.

Drittens haben wir eine Regelung aufgenommen, die sicherstellen soll, dass das Parlament in adäquater Weise bei dem Einsatz der Software beim Berliner Verfassungsschutz eingebunden wird. Wir glauben, dass wir mit dem Antrag eine sehr ordentliche und sehr saubere Regelung gefunden haben, um das eine zu ermöglichen und gleichwohl den Grundrechtsschutz hier zu wahren. Wir sind gespannt auf die Anhörung durch die Experten.

Vorsitzender Alexander Morlang: Vielen Dank! – Als Nächstes kommen wir zur Begründung des Antrags 2 b und 2 c durch die Piratenfraktion. – Herr Weiß, Sie haben das Wort!

Dr. Simon Weiß (PIRATEN): Vielen Dank! – Ich halte mich aus dem gleichen Grund ebenfalls kurz. Bei den beiden Anträgen von uns, die auf der Tagesordnung stehen, geht es uns zum einen darum, dass beim Erwerb von Software, die der Überwachung dient, die Kontrollrechte des Datenschutzbeauftragten in vollem Umfang gewährleistet sind – wie schon angesprochen –, insbesondere durch die Möglichkeit, in den Quellcode einzusehen und zu prüfen, und auch sicherzustellen, dass der Datenschutzbeauftragte darüber informiert ist. Das ist ein Punkt, den Sie in Ihrem anderen Antrag aufgenommen haben, weshalb wir die jetzt auch zusammen beraten.

Zweitens: Der wichtigere der beiden Anträge ist der, in dem wir uns klar dagegen aussprechen, dass das Land Berlin die momentan geplante oder irgendeine Software verwendet, die einen Staatstrojaner darstellt und somit den Vorgaben des Bundesverfassungsgerichts nicht gerecht wird.

Vorsitzender Alexander Morlang: Dann haben wir den Änderungsantrag der Grünen. Wer möchte den begründen? – Herr Gelbhaar, Sie haben das Wort!

Stefan Gelbhaar (GRÜNE): In aller Kürze: Wir haben den Antrag gelesen, wir haben auch schon im Plenum darüber geredet und gesagt, dass wir ihn unterstützen und dass er gut ist.

Wir haben allerdings nicht verstanden, warum der Antrag der Piratenfraktion vorsieht, nur in Bezug auf Vertragsabschlüsse mit Privatfirmen tätig zu werden. Die Fragestellung kann sich genauso ergeben, wenn von staatlichen Behörden oder anderen Bundesländern entsprechende Software eingekauft wird. Deswegen haben wir da den Passus mit Privatfirmen entsprechend gekürzt.

Vorsitzender Alexander Morlang: Vielen Dank! – Ich möchte darauf hinweisen, dass zu diesem Antrag Materialien des Anzuhörenden Herrn Buermeyer vor liegen, die Sie am 11. Februar 2013 per Mail bekommen haben müssten. Außerdem ist eine Stellungnahme des Verfassungsschutzausschusses zum Antrag der Koalition nachrichtlich an den IT Dat eingegangen und ebenfalls per E-Mail weitergeleitet worden. Der Verfassungsschutzausschuss hat die Annahme des Antrags Drucksache 17/0729 empfohlen.

Wir kommen damit zur Anhörung. Wir haben Herrn Buermeyer, Herrn Rieger, Herrn Nöding und Herrn Schröder. – Ich schlage vor, wir beginnen mit Herrn Buermeyer.

Ulf Buermeyer (Richter am Landgericht): Herr Vorsitzender! Ganz herzlichen Dank! – Meine Damen und Herren! Vielen Dank für die Einladung! Ich möchte meine kurze Stellungnahme gliedern. Ich möchte ganz kurz etwas zum rechtlichen Hintergrund sagen. Was ist die verfassungsrechtliche Lage? – Das habe ich in ganz wenigen Sätzen zusammengefasst, um dann in einem zweiten Schritt sehr schnell dazu zu kommen, wie im Lichte dieser verfassungsrechtlichen Anforderung aus meiner Sicht der Koalitionsantrag zu bewerten ist und natürlich auch die Anträge der Piratenfraktion und der Grünen-Fraktion.

Stichwort „verfassungsrechtliche Lage“: Das Bundesverfassungsgericht hat 2008 den Einsatz von Trojanern zunächst einmal im präventiven Bereich ausführlich geregelt oder hat dazu ausführlich Stellung genommen. Es hat ein Grundrecht auf Integrität und Vertraulichkeit für informationstechnische Systeme geschaffen und zugleich festgelegt, welche Anforderung für Online-Durchsuchungen und Quellen-TKÜ gelten.

Zunächst: Was ist eigentlich die Unterscheidung? – Die Unterscheidung ist technisch zunächst einmal keine. In beiden Fällen muss das informationstechnische System mit einer Software infiziert werden, die staatlichen Stellen die Fernsteuerung dieses Rechners und die Erhebung von Daten aus diesem Rechner erlaubt. Zu den Details, denke ich, gibt es hier berufenere Stimmen auf diesem kleinen Podium. Aber das sollte man sich klar machen: In jedem Fall geht es darum, einen vollen Zugriff auf den Rechner zu bekommen. Der Unterschied ist eigentlich nur, dass man bei der Quellen-TKÜ diesen vollen Zugriff quasi auf die Erhebung bestimmter Daten beschränkt. Man könnte alles, man darf allerdings bei der Quellen-TKÜ nur die Gegenstände von laufender Kommunikation erheben. Das ist ein ganz wichtiger Unterschied, und das muss man sich klarmachen. Es handelt sich quasi um eine künstliche, rechtliche Beschränkung einer zunächst einmal viel weitergehenden Maßnahme.

An diese künstliche, rechtliche Beschränkung allerdings hat das Bundesverfassungsgericht quasi einen Bonus für hoheitliche Stellen geknüpft. Die Online-Durchsuchung generell ist an sehr hohe verfassungsrechtliche Hürden geknüpft. Die Quellen-TKÜ, also die Selbstbeschränkung von z. B. Ermittlungsbehörden führt auf der anderen Seite dazu, dass vergleichsweise leichtere Hürden zu nehmen sind. Allerdings hat das Bundesverfassungsgericht sehr deutlich gesagt: Zwei Hürden sind weiter erforderlich. Um von einer Quellen-TKÜ ausgehen

zu können, muss sowohl technisch als auch rechtlich sichergestellt werden, dass tatsächlich nur Daten laufender Kommunikation erhoben werden. Da ist auch gleich das Problem. Wie gesagt, technisch handelt es sich eigentlich auch bei der Quellen-TKÜ um eine Online-Durchsuchung, und das heißt, die Anforderungen des Bundesverfassungsgerichts sind an dieser Stelle zumindest nicht ganz leicht aufzulösen. Ich denke, Frank Rieger wird dazu gleich noch genauer etwas sagen können.

Ich möchte mich auf die rechtlichen Beschränkungen der Quellen-TKÜ konzentrieren. Da hat das Bundesverfassungsgericht sehr deutlich gesagt, dass die Begrenzung auf Gegenstände der Kommunikation tatsächlich auch rechtlich sichergestellt werden muss. Das bedeutet also, wir brauchen einen ganz klare Rechtsgrundlage dazu. Wenn man sich jetzt die Strafprozessordnung anschaut, dann haben wir selbstverständlich eine Rechtsgrundlage zur Telekommunikationsüberwachung, allerdings regelt diese Rechtsgrundlage zum Einsatz in § 100 b der StPO nur die klassische Überwachung unter Einschaltung eines Providers. Das heißt also, zur Frage der Quellen-TKÜ schweigt die Strafprozessordnung. Das kann auch nicht verwundern. Als sie zuletzt geändert wurde an dieser Stelle, im Jahr 2007, wurde zwar schon von Online-Durchsuchungen geredet, aber nach meinem Wissen nicht im parlamentarischen Raum.

Jetzt die Frage: Welche Konsequenzen sind daraus quasi für den Status quo und für die Zukunft zu ziehen? – Man muss ganz deutlich sagen: Es gibt zurzeit in der Strafprozessordnung keine Grundlage für die Quellen-TKÜ. Das ist in der Rechtswissenschaft eine nahezu unumstrittene Meinung. Es gibt inzwischen nur noch zwei Autoren, die etwas anderes vertreten. Wenn man dann mal genau hinguckt, findet man da teilweise nicht einmal Belege für diese Auffassung. Das ist erschütternd, aber das ist Teil des rechtswissenschaftlichen Diskurses, dass auch radikale Meinungen vertreten werden, während im vorliegenden Fall die breite Meinung – ich habe mal gezählt: von knapp 20 Autoren, u. a. Herr Prof. Hoffmann-Riem, der als Bundesverfassungsrichter für die Entscheidung zur Online-Durchsuchung zuständig war – glasklar sagt: Es geht nicht. – Man bräuchte also eine klare Rechtsgrundlage.

Der Bundesgesetzgeber hat sich interessanterweise dieser Position auch schon angeschlossen und hat das Bundeskriminalamtsgesetz um eine spezifische Rechtsgrundlage für die Quellen-TKÜ ergänzt. § 20 l des Bundeskriminalamtsgesetzes sieht in Absatz 2 inzwischen eine solche Rechtsgrundlage vor. Man kann also sagen, auch der Bundesgesetzgeber war sich darüber im Klaren, mit der bisherigen Rechtsgrundlage – natürlich gab es im BKA-Gesetz auch vorher schon eine normale TKÜ-Norm – darf man so etwas nicht durchführen.

In der StPO ist die Rechtslage exakt dieselbe. Ich will nur ganz kurz noch die Stichworte nennen, weswegen ein Ermittlungsrichter diese Lücke in der StPO nicht schließen darf. Das ist quasi die Hintertür, die einige, ganz wenige Autoren und, ich glaube, das Amtsgericht Bayreuth da mal gefunden haben. Das Landgericht Berlin hat das in einer Entscheidung, die dann Gott sei Dank nicht umgesetzt worden ist, auch mal so gesehen. Wie gesagt, die StPO sieht eben keine ausdrückliche Rechtsgrundlage vor, im Gegensatz zu den Anforderungen des Bundesverfassungsgerichts, dass es auch rechtliche Vorgaben geben muss.

Warum kann der Ermittlungsrichter diese Lücke nicht schließen? – Das ist letzten Endes eine ganz einfache verfassungsrechtliche Entscheidung. Das Rechtstaatsprinzip enthält unter anderem den sogenannten Wesentlichkeitsgrundsatz. Artikel 20 Absatz 3 des Grundgesetzes legt fest, dass alle für die Grundrechtsausübung wesentlichen Fragen vom Gesetzgeber selbst

durch formelles Gesetz zu regeln sind. Jedenfalls nach meiner rechtstaatlichen Auffassung ist die Frage, unter welchen Voraussetzungen der Staat in einen Computer seines Bürgers einen Trojaner einpflanzen kann und damit den vollen Zugriff, jedenfalls technisch, auf alle Daten bekommt, für die Grundrechtsausübung wesentlich, ebenso wesentlich z. B. wie die Frage, unter welchen Voraussetzungen man in eine Wohnung eindringen darf. Es handelt sich, wenn Sie so wollen, um eine virtuelle Hausdurchsuchung. Möglicherweise erfährt man sogar noch viel mehr in einem Computer als bei einer Wohnungsdurchsuchung heutzutage. Unter diesen Voraussetzungen kann es mich nur noch irritieren, wenn man sagt: Das muss nicht der Gesetzgeber klären, das soll doch der Ermittlungsrichter beschließen. – Das kann aus meiner Sicht rechtstaatlich schlicht und ergreifend nicht wahr sein.

Dann muss man fragen: Wie ist es mit der Annex-Kompetenz? – Das ist ein weiteres Stichwort, das in der Diskussion eine Rolle spielt. Auch da muss man sagen, dass die Annex-Kompetenz normalerweise für minimale Begleiteingriffe angenommen wird. Auch da gilt letztlich das, was ich gerade schon gesagt habe. Das Infizieren eines Rechners mit einem Trojaner ist kein Begleiteingriff. Das kann man nicht sagen, weil der gesamte Inhalt des Rechners damit preisgegeben wird.

Viertens ist es eine technisch relativ komplexe Frage, wie denn ein solcher Trojaner beschaffen sein muss. Auch da möchte ich wiederum an Frank Rieger und Thorsten Schröder verweisen, die das sicherlich viel genauer sagen können. Ich denke nicht, dass man es dem Ermittlungsrichter überlassen kann, darüber zu entscheiden, wie ein Trojaner beschaffen sein muss, damit die verfassungsrechtlichen Fragen geklärt werden können und damit die Grenzen des Verfassungsgerichts eingehalten werden. Ich denke, bei allem Respekt vor der Arbeit der Ermittlungsrichter muss man sagen: Das überschreitet ihre Kompetenz doch eindeutig. Hier braucht es aus meiner Sicht eine klare Rechtsgrundlage, wahrscheinlich sinnvollerweise mit einer Verordnungsermächtigung, um dann analog zu der Rechtslage bei klassischen Telefonüberwachungen über eine Verordnung – da ist es bislang die TKÜV – und eine darauf gestützte technische Richtlinie sicherzustellen, dass Trojaner nur in verfassungsmäßigerweise zum Einsatz kommen. Das kann nicht freischwebend im stillen Kämmerlein und am grünen Schreibtisch mal eben ein Ermittlungsrichter. Das sprengt, glaube ich, doch dessen Kompetenzen.

So viel zum rechtlichen Hintergrund. Quintessenz: Man braucht eine eigene Rechtsgrundlage. Insofern begrüße ich ausdrücklich die Initiative der Regierungskoalition. Es ist nämlich in der Tat eine sehr gute Idee, eine Norm analog zu § 20l des BKA-Gesetzes zu schaffen – das möchte ich an dieser Stelle sehr deutlich sagen –, weil sich die Berliner Regierung damit deutlich auf die Seite des rechtstaatlichen Vorgehens schlägt. Andere Landesregierungen, zum Beispiel in Bayern, haben das in einer aus meiner Sicht überaus heiklen Weise anders gehandhabt. Die Initiative der Regierungskoalition möchte ich also sehr deutlich begrüßen.

Die Regierungskoalition hat außerdem die im rechtspolitischen Raum gelegentlich schon geäußerte Kritik am § 20l BKA-Gesetz aufgegriffen, indem sie nämlich sagt: Wir wollen diese Norm nicht nur kopieren, sondern wir wollen sie auch um verfahrensrechtliche Regelungen ergänzen. – Auch das ist sehr zu begrüßen. Ich habe es gerade schon angedeutet. Aus meiner Sicht ist der § 20l ein wichtiger Schritt, aber er kopiert eins zu eins die Vorgaben des Bundesverfassungsgerichts, ohne verfahrensrechtlich sicherzustellen, dass sie auch eingehalten werden. Ich denke, bei diesen verfahrensrechtlichen Regelungen sollte man noch nachlegen.

Stichwort Verfahrensrecht: Damit komme ich zu den weiteren Punkten aus dem Koalitionsantrag. Aus meiner Sicht wäre eine Kontrolle durch einen Datenschutzbeauftragten in der Tat eine sehr sinnvolle Lösung, und zwar einfach deswegen, weil der Datenschutzbeauftragte – er ist hier und kann sich dazu aus seiner Sicht wiederum kompetenter äußern als ich – unabhängig ist. Es ist auch europarechtlich abgesichert, dass er gerade nicht der Einwirkung der Exekutive unterliegt, und er hat damit jedenfalls rechtlich einen Status, der es ihm ermöglichen müsste zu prüfen, ob tatsächlich die Vorgaben des Bundesverfassungsgerichts konkret umgesetzt werden.

Man sollte sich da natürlich nichts vormachen. Das ist auch technisch eine komplexe Frage, und man muss den Datenschutzbeauftragten dann auch mit den Möglichkeiten ausstatten, das wirklich zu tun. Außerdem stellen sich weitere komplexe technische Fragen. Wie ist sicherzustellen, dass die vom Datenschutzbeauftragten geprüfte Software letztlich tatsächlich zum Einsatz gekommen ist? Da würde ich zum Beispiel mal das Stichwort Softwaresignaturen in den Raum stellen. Also, man müsste dann schon sicherstellen, dass die geprüfte Software auch tatsächlich diejenige ist, die letztlich zum Einsatz kommt, denn was man prüft, ist der Quelltext. Der muss übersetzt werden in ein sogenanntes Binary, eine ausfüllbare Datei, und diese Übereinstimmungen sind theoretisch auch immer Fehlerquellen.

Die verfahrensrechtlichen Vorgaben stellen einige Anforderungen an eine konkrete Lösung des Trojanerproblems. Ich denke, da wird man noch genau hinschauen müssen und darüber nachdenken müssen, aber der Grundansatz, eine wirklich unabhängige Stelle damit zu betrauen, scheint mir absolut überzeugend. Analog gilt das aus meiner Sicht für den Verfassungsschutz. Darauf möchte ich jetzt nicht ausführlicher eingehen.

Interessant finde ich noch die beiden Anträge der Piratenfraktion und die Ergänzung durch die Grünen. Ich denke aber, dass der Koalitionsantrag den Punkt der Kontrolle, der – wenn ich das richtig verstehe – der Piratenfraktion sehr wichtig war, aufgegriffen hat, nämlich durch die beabsichtigte Beauftragung des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Es kann in der Tat nicht sein, dass der Datenschutzbeauftragte vor einem Problem steht, wie zum Beispiel Dr. Petri, der bayerische Beauftragte, der schlicht nicht prüfen konnte, ob die Software den Anforderungen entsprach, und zwar wegen Tagessätzen, aber auch we-

gen einer Vertraulichkeitsvereinbarung. Das heißt, der Datenschutzbeauftragte hätte dort prüfen können, aber nur mit einem Schweigegelübde, und auch das ist in einem Rechtsstaat unannehmbar. Ich denke, das bedarf keiner genaueren Analyse, wieso der Datenschutzbeauftragte auch über das reden können muss, was er tatsächlich findet. – So viel zu den Anträgen. Nochmals herzlichen Dank für die Einladung! Ich freue mich auf die Diskussion.

Vorsitzender Alexander Morlang: Vielen Dank! – Herr Nöding!

Dr. Toralf Nöding (Vereinigung Berliner Strafverteidiger): Vielen Dank! Ich bin Rechtsanwalt Nöding von der Vereinigung Berliner Strafverteidiger. Was ich sagen möchte, schließt quasi, als wäre es abgesprochen, nahtlos an das an, was Herr Buermeyer gesagt hat.

Die Vereinigung Berliner Strafverteidiger unterstützt den Antrag insofern, als wir finden, dass daraus deutlich hervorgeht, wie Herr Buermeyer schon gesagt hat, dass es für die Quellen-TKÜ eine eigene Rechtsgrundlage braucht und dass es die bislang nicht gibt – Punkt 1 – und – Punkt 2 – dass es wohl derzeit auch nicht praktisch gemacht werden soll. So verstehen wir den Antrag.

Wozu ich gern etwas für die Vereinigung Berliner Strafverteidiger sagen wollte – insofern schließt sich das tatsächlich gut an –, ist, wie so eine Rechtsgrundlage, wenn sie denn kommen soll, und das scheint ja beabsichtigt zu sein, konkret aussehen oder – viel wichtiger noch – nicht aussehen sollte. Wir halten da fünf oder sechs Punkte für enorm wichtig.

Herr Buermeyer hat gerade schon gesagt, was die verfassungsrechtlichen Anforderungen sind. Wichtig ist, dass man bei der ganzen Diskussion im Kopf behält, dass die Quellen-TKÜ ein viel eingriffsintensiverer Eingriff ist als die normale TKÜ, die in § 100a und 100b StPO geregelt ist. Wir finden, dass sich das auch in der möglicherweise neu zu schaffenden Rechtsgrundlage spiegeln sollte.

Wir haben – das will ich ganz deutlich sagen – ein bisschen Angst, dass man quasi unter Übernahme dieser Voraussetzungen aus § 20l BKA-Gesetz jetzt eine zusätzliche Befugnis für die Quellen-TKÜ unter § 100a StPO runterschaltet, also im Wesentlichen unter denselben Voraussetzungen, ergänzt um die Anforderungen aus der Entscheidung des Bundesverfassungsgerichts, jetzt sagt, dass unter den Voraussetzungen auch eine Quellen-TKÜ möglich ist. Wir glauben, dass das der Eingriffsintensität nicht gerecht würde und dass insofern auch höhere Eingriffsvoraussetzungen, höhere tatbestandliche Voraussetzungen in dieser Norm verankert werden sollten. Wenn man mit so einer Initiative für eine Rechtsgrundlage in den Bundesrat geht, sollte man konkrete Vorstellungen zu den tatbestandlichen Voraussetzungen haben. Ich möchte jetzt ein paar Punkte auflisten, die uns da wichtig wären, und die, glauben wir, nicht bloß uns wichtig sind, sondern auch verfassungsrechtlich unabdingbar wären.

Zum einen: Die Regelung des § 100a StPO, die diese normale TKÜ regelt, sieht bestimmte Katalogstraftaten vor, bei deren Vorliegen so eine TKÜ angeordnet werden soll. Wir finden, dass aufgrund der höhen Eingriffsintensität dieser Katalog nicht einfach für die Quellen-TKÜ übernommen darf, sondern dass man da auf wirklich schwerste Straftaten beschränken muss. Da sind bislang Sachen drin wie Abgeordnetenbestechung, Bankrott, gewerbsmäßige Hehlerei, also Sachen, die aus unserer Sicht eher zur mittleren Kriminalität gehören als zur schwe-

ren oder Schwerstkriminalität. Wir finden, das muss sich aufgrund des intensiveren Eingriffs auf Voraussetzungsseite in so einer neuen Ermächtigungsgrundlage spiegeln. – Punkt 1.

Punkt 2: Wieder aufgrund der Tatsache, dass es ein intensiverer Eingriff ist, glauben wir, dass es eine klare Subsidiaritätsregelung braucht, das heißt, dass es eine Quellen-TKÜ nur geben darf, wenn die normale TKÜ nicht ausreicht. Das muss unter zwei Punkten jeweils geprüft werden, zum einen nämlich, ob es generell überhaupt notwendig ist, eine Quellen-TKÜ zu schalten, und zweitens, ob im konkreten Fall Hinweise darauf vorliegen, dass die Beschuldigten eine Art der Kommunikation nutzen, die eine Quellen-TKÜ notwendig machen. Wenn diese neue Ermächtigungsgrundlage kommt, sollte das da rein, damit es nicht zur reinen Makulatur verkommt.

Punkt 3: Wieder aufgrund des intensiveren Eingriffs muss der Kernbereichsschutz relativ hoch gehängt werden. Wir haben da derzeit sowohl im BKA-Gesetz als auch schon im § 100a StPO eine, wie wir finden, sehr schwache Regelung. Die sagt nämlich, überwacht werden darf nur dann nicht, wenn allein Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung zu erwarten sind. Das heißt, eine Überwachung wäre nur dann unzulässig, wenn man schon vorher weiß, die werden nie über irgendwas reden, was nicht dem Bereich, dem Kernbereich der privaten Lebensgestaltung zuzurechnen ist. Das wird nie der Fall sein. Insofern läuft diese Regelung in der Praxis leer. Da sollte man aufgrund des intensiveren Eingriffs überlegen, ob man da nicht im Bereich der Quellen-TKÜ nachbessert.

Vorletzter Punkt: Bei einer normalen TKÜ hat man immer im Wesentlichen die Anknüpfung an eine Telefonnummer. Das heißt, man weiß genau, was man konkret abhört. Wenn man jetzt am Endgerät ansetzt – das normale Beispiel: Es steht ein PC in der Wohnung, der über eine Quellen-TKÜ angeschlossen werden soll –, ist die Frage, wer es nutzt. Wenn man unbesehen am Endgerät ansetzt, erwischt man alle Leute mit, die diesen PC nutzen, ohne Subjekt eines Ermittlungsverfahrens zu sein. Da muss es einen Anknüpfungspunkt geben, der sicherstellt, dass das nicht der Fall ist. Ich bin kein Techniker, und wir haben uns in unserem laienhaften Verständnis vorgestellt, dass man vielleicht an einen Skype-Account anknüpft. Aber irgendwie muss man sicherstellen, dass nicht unbeteiligte Dritte erfasst werden.

Letzter Punkt von uns: Nach meinem Kenntnisstand erfasst Telekommunikation möglicherweise auch Videotelefonie. Das wird über Skype auch intensiv genutzt. Das darf aus unserer Sicht keinesfalls über eine Quellen-TKÜ sozusagen mit abgesaugt werden, und zwar, weil wir dann unmittelbar im Wohnungsgrundrecht sind. Wenn jemand einen PC in der Wohnung stehen hat und darüber Videotelefonie hat, haben wir ein weiteres wichtiges Grundrecht betroffen, und das muss man aus unserer Sicht aus verfassungsrechtlicher Sicht zumindest ausschließen. – Das waren die Punkte, die uns wichtig wären. Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Als Nächstes hat Herr Rieger das Wort.

Frank Rieger (Chaos Computer Club Berlin): Herr Vorsitzender! Meine Damen und Herren Abgeordnete! Vielen Dank für die Einladung! Ich kann mich in einem Punkt meinen Vorrednern anschließen. Ich finde es gut, dass Berlin zumindest erkannt hat, dass man mit diesem Trojanerunwesen zumindest nicht ohne Rechtsgrundlage weitermachen sollte, und zumindest versucht, im Prinzip das Richtige zu tun, nämlich Rechtssicherheit und Überprüfbarkeit sicherzustellen. Das Problem ist nur, dass die Überprüfbarkeit dessen, wie sich ein Quellen-

TKÜ-Trojaner von einem Online-Durchsuchungstrojaner abgrenzen soll, in der Praxis nur sehr schwer möglich ist und aus meiner Sicht eigentlich gar nicht möglich ist.

Wenn man sich den Kontext des Verfassungsgerichtsurteils anguckt, wo es um die Online-Durchsuchung ging und es diesen doch relativ plötzlich eingeschobenen Absatz zur Quellen-TKÜ gab, über den wir heute reden, merkt man, dass die Richter genau dieses Problem nicht lösen konnten und wollten.

Wenn wir uns jetzt die Technik angucken, wie so ein Trojaner aufgebaut ist: Ein Trojaner besteht heutzutage aus mehreren Komponenten. Die erste ist ein sogenannter Dropper, ein Programm, das den Trojaner, die eigentlichen Überwachungskomponenten, auf diesen Computer befördert. Das ist die eigentliche Infiltration des Computers. Ab diesem Zeitpunkt ist der Computer denjenigen, die diesen Trojaner darauf installiert haben, ausgeliefert. Aus Sicht des Benutzers ist es eine Schadsoftware. Ob es ein Trojaner ist, der vom LKA installiert wird, oder einer, der von der Russen-Mafia installiert wird, ist mir als Benutzer erst mal egal, und ich erwarte, dass meine Antivirussoftware, falls ich eine habe, oder meine sonstigen Gegenmaßnahmen was dagegen tun.

Was daraus folgt, ist, dass sich so ein Trojaner permanent verändern muss. Das heißt, Sie können nicht in jedem einzelnen Fall genau den gleichen Trojaner einsetzen. Sie brauchen quasi für jeden Einzelfall einen individuell angepassten Trojaner. Das sagt übrigens auch das BKA. Das Problem dabei ist nur, wie Sie den zertifizieren. Sie können nicht hingehen und sagen: Wir haben hier einen Trojaner. Den haben wir einmal zertifiziert, und dann schrauben wir nächste Woche dran herum und setzen ihn noch mal ein, und die Zertifizierung gilt weiter. – Das ist ungefähr so, als würden Sie bei Ihrem Auto, das gerade frisch TÜV bekommen hat, das Fahrgestell auswechseln und sagen: Das hat jetzt immer noch TÜV, weil es immer noch wie ein Auto aussieht –, steht immer noch „Trojaner“ drauf.

Das Problem, das sich da stellt, ist, dass die Abnahme, dass diese Software tatsächlich nur die verfassungsmäßig erlaubten Dinge tut, in jedem Einzelfall erfolgen muss. Sie können also nicht hingehen und sagen: Diese Firma hat uns mal einen Trojaner gebaut. Der sieht gut aus, den nehmen wir –, denn der sieht nächste Woche schon wieder ganz anders aus, denn sonst würde er nicht mehr funktionieren, sonst würde er zum Beispiel von den Abwehrmechanismen des Betriebssystems des Benutzers erkannt und rausgeschmissen werden.

Das nächste Problem dabei ist: Die Modulbauweise dieser modernen Trojaner, die Sie heute haben, funktioniert so, dass Sie zum einen dieses Lademodul haben, was zum Beispiel ein Modul zur Skype-Überwachung, zur MSN-Chat-Überwachung oder zur Webtelefonie-Überwachung nachlädt. Diese Module müssen auch in jedem Einzelfall einzeln zertifiziert und auch wiederum einzeln verändert werden, damit sie nicht zum Beispiel von einer Antivirussoftware erkannt werden. Also, jedes einzelne dieser Module muss einzeln zugelassen und einzeln zertifiziert werden. So eine Zertifizierung von Software dauert im Schnitt sechs Monate, wenn sie ernsthaft betrieben wird, und gilt dann für genau diese eine Version, wo nicht das Fahrgestell geändert wurde.

Wenn wir uns angucken, wie ein Überwachungsmodul funktioniert, z B. ein Skype-Überwachungsmodul oder andere Softwareüberwachungsmodule z. B. gegen verschlüsselte Kommunikationssoftware: Die Programmierer einer solchen Software sind ja nicht doof. Sie

versuchen, sich dagegen zu wehren, dass diese Software infiltriert wird. Das heißt, im Regelfall werden solche Module so gebaut, dass die Kamera oder das Mikrofon angemacht wird, während die Kommunikation läuft. Das bedeutet wiederum auch: Wenn Sie dieses Modul ändern, und zwar nur in einem einzigen Bit – es ist tatsächlich nur ein einziges Bit, was diese Überprüfung, ob da gerade eine Skype-Kommunikation läuft oder nicht, ausschaltet –, dann haben Sie schon eine Raumüberwachung. Das heißt also, eine Änderung in einem Überwachungsmodul, die so minimal ist, dass Sie einem Softwareprüfer möglicherweise nicht auffällt, macht den Unterschied zwischen einer Telekommunikationsüberwachung und einer Raumüberwachung, für die Sie den Großen Lauschangriff als Ermächtigung brauchen.

Das ist die technische Realität. Sie können nicht davon ausgehen, dass es so ist: Sie fahren das Auto zum TÜV, dann kommt ein Stempel drauf, und dann bleibt es so –, sondern Sie haben es mit einem sich ständig verändernden, dynamischen System zu tun – zwangsläufig, denn sonst würde es nicht funktionieren –, was Sie permanent nachzertifizieren müssen und wo extreme Aufmerksamkeit in der Überprüfung notwendig ist, um sicherzustellen, dass diese Software wirklich nur tut, was sie soll.

Das dritte Problem ist: Die Komplexität dieser Infiltration und dieser Maßnahmen, die da stattfindet, führt in der Regel dazu – das sehen wir in anderen Ländern, das haben wir auch in anderen Bundesländern gesehen –, dass die eigentliche Durchführung der Maßnahmen von den Sicherheitsbehörden nicht selbst durchgeführt wird, sondern dass sie sich in hohem Maße auf die technischen Dienstleister verlassen. So, wie es in anderen Überwachungstechnologien der Fall ist, wird häufiger mal – – Wir haben es zum Beispiel beim DigiTask-Trojaner gesehen. Da haben die entsprechenden LKA und das BKA quasi im Blindflug agiert. Die haben einen Computer von DigiTask bekommen, der ihnen die Ergebnisse des Trojaners angeliefert hat, und haben dem einfach vertraut. Die hatten keinerlei technische Kenntnis darüber, wie der eigentlich funktioniert und ob er noch mehr macht, als er sollte.

Was wir zum Beispiel bei DigiTask gesehen haben: Auch der DigiTask-Trojaner war in Modulbauweise gebaut. Die Module wurden nur alle an den Zielcomputer ausgeliefert, und sie waren nur ausgeschaltet, d. h. über einzelne Bits deaktiviert. Die tatsächliche Prüfung, was da eigentlich ausgeliefert wird – – Das BKA wusste nach eigener Aussage nicht davon, dass da noch diese anderen Module drin waren. Die haben sich darauf verlassen, dass DigiTask ihnen gesagt hat: Die sind da nicht drin –, denn die waren auch auf ihrer Benutzeroberfläche nicht zu sehen, die waren aus ihrer Sicht deaktiviert. Sie waren aber tatsächlich da und von einem Angreifer problemlos zu aktivieren.

Da sind wir schon beim vierten Problempunkt, nämlich diesen Firmen, die diese Trojaner herstellen. Mit Verlaub: Das sind so ungefähr die schattigsten Gewächse, die Sie im IT-Sumpf finden. Es handelt sich im Allgemeinen um Firmen, die eine relativ niedrige Reputation haben. Zur DigiTask-Software habe ich Kommentare von Informatik-Professoren gehört, die nicht zitierfähig waren. Andere Firmen aus Deutschland, nehmen wir zum Beispiel Gamma FinFisher aus München, sind dadurch bekannt geworden, dass sie Diktaturen im arabischen Raum beliefert haben. Dann haben wir Firmen wie die auch in Berlin verwendete Firma Syborg, die Telekommunikationsüberwachung liefert. Deren Mutterfirma ist in Holland in einen Skandal verwickelt, wo in der Überwachungsanlage der holländischen Polizei plötzlich Telefongespräche auftauchten, die nie stattgefunden haben. Da ging es nämlich um kurdische Drogendealer – Schrägstrich – Oppositionelle, die mit den Israelis, denen diese

Firma gehört, ein bisschen über kreuz sind, und dann gab es da plötzlich gefälschte Beweismittel. Das heißt, wir haben da mit Firmen zu tun, mit denen man als öffentliche Verwaltung eigentlich nichts zu tun haben will.

Deswegen als Fazit: Überlegen Sie sich bitte genau, ob Sie diese Büchse der Pandora aufmachen wollen! Jedes einzelne dieser Probleme, die ich aufgezählt habe, haben wir bei den Trojanern, die bisher verwendet wurden, schon gesehen, und es gibt keine wirklich guten Lösungsmöglichkeiten dafür. Wenn Sie sagen, Sie wollen es aber trotzdem, weil es die Sicherheitsbehörden unbedingt haben wollen, dann sorgen Sie bitte dafür, dass die Anforderungen so hoch gehängt sind, dass es nicht zum Alltagswerkzeug wird, denn mit der Menge der Einsätze multiplizieren sich die Probleme. Jeder einzelne Einsatz führt dazu, dass Sie neu zertifizieren müssen, dass Sie neu überprüfen müssen, dass die Wahrscheinlichkeit steigt, dass es entdeckt wird.

Das Problem ist: Wenn Sie einen Computer infiltrieren, wenn ein Computer einmal infiltriert ist, können Sie nicht davon ausgehen, dass die Beweismittel auf diesem Computer noch verwertbar sind. Wir hatten mehrere Fälle, wo uns dieser DigiTask-Trojaner tatsächlich zur Verfügung gestellt wurde. Das waren Fälle, wo hinterher die Festplatten noch beschlagnahmt wurden und dann durch die normale Auswertung der Polizei gingen, und wir konnten den Betroffenen nur sagen: Pass auf! Niemand kann dir garantieren, dass auf dieser Festplatte nur die Daten sind, die du da draufgetan hast. Jeder hätte dir Daten raufschieben können. – Wenn ein Quellen-TKÜ-Trojaner angewendet wird, muss genauso, als wenn es eine Online-Durchsuchung ist, hinterher ausgeschlossen werden, dass dieser Computer noch zur Beweismittelverwertung herangezogen wird, weil nicht mehr zu garantieren ist, dass die Daten, die auf diesem Computer sind, nur von dem Verdächtigen stammen. Das können Sie aus Sicht der Informatik nicht mehr sicherstellen.

Der letzte Punkt ist: Wenn Sie tatsächlich einen Trojaner einsetzen und genehmigen wollen, ist es aus unserer Sicht zwingend notwendig, dass der Betroffene hinterher Einsichtsrecht in die technischen Umstände seiner Überwachung bekommt, d. h., dass er anhand des Binary und der Source-Code-Protokolle überprüfen kann, ob tatsächlich nur die verfassungsgemäßen und rechtlich gesicherten Dinge bei ihm getan wurden oder darüber hinaus andere stattgefunden haben. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Herr Schröder!

Thorsten Schröder (modzero AG): Mein Name ist Thorsten Schröder. Ich möchte mich recht herzlich für die Einladung bedanken. Ich würde gern auf zwei konkrete Punkte eingehen und versuchen, möglichst verständlich die komplexen technischen Sachverhalte zu erläutern.

Es heißt, es dürfe keinesfalls die Grenze zu einer Online-Durchsuchung überschritten werden, und es sei sicherzustellen, dass die Software keine Daten über den aktuellen Kommunikationsprozess hinaus ausspäht und übermittelt. Herr Buermeyer hat es schon gesagt. Es gibt hier bei der Quellen-TKÜ einfach nur noch eine weitere Beschränkung – im Gegensatz zu anderen Maßnahmen, die sehr viel tiefer in die Persönlichkeitsrechte und in die Rechte des jeweiligen Menschen eingreifen. Und es heißt, es soll von Unabhängigen überprüft und zertifiziert werden, dass die Software das tut, was sie eigentlich tun soll. Hier muss man ganz klar auch die Ziele erläutern. Was ist das Ziel einer solchen Überprüfung und Zertifizierung? Man kann

nicht ohne Weiteres zertifizieren, dass eine Software keine schadhaften Funktionen beinhaltet. Aber dazu komme ich später noch.

Die nächste Aussage ist: Es soll eine unabhängige Stelle geben, die die Überwachungssoftware signiert, um zu gewährleisten, dass diese selbst gesetzten Grenzen eingehalten werden. Dazu möchte ich ein paar Fakten loswerden. Eine Behörde, die solch eine Software im Source Code oder auch in Binärform vorliegen hat, um sie einzusetzen, ist technisch grundsätzlich in der Lage, diese Software zu modifizieren, dass diese mehr tut, als sie eigentlich darf und als vorausgesetzt war. Die Hemmschwelle hierfür ist recht hoch, weil ein sehr spezielles technisches Wissen dafür notwendig ist, und sollte zum Ende einer solchen Maßnahme aufgedeckt werden, dass es entsprechende Modifikationen gab, wäre halt klar, dass hier sehr bewusst gegen Gesetze verstoßen wurde.

Darüber hinaus kann es durchaus möglich sein, dass die Software bei solcherlei Modifikation anschließend nicht mehr 100-prozentig korrekt funktioniert. Das heißt, die Gefahr eines Fehlverhaltens ist recht groß. Gut, die Gefahr eines Fehlverhaltens ist auch bei regulär programmierter Software recht groß. Es kann durchaus passieren, dass die Programmierer eines solchen Trojaners Fehler gemacht haben, die es wiederum anderen, Dritten, erlauben, den Rechner auf eine illegale Art und Weise auszuspionieren – so, wie wir schon bei diesem „O'zapft is!"-Trojaner gesehen habe, dass es grundsätzlich diverse Ansätze gibt, diesen auch zu missbrauchen.

Als Nächstes heißt es, es gebe Nachlademodule. Da sprechen wir grundsätzlich über explizite Schnittschnellen an diese Überwachungssoftware, die es dann erlauben, wieder anderen Programmcode über ein definiertes Format über diese Schnittstelle anzubinden. Das bedeutet, dass die Hürden, die ich eben angesprochen habe, die Software zu modifizieren, wiederum sehr viel niedriger sind, denn eine definierte Schnittstelle erlaubt es sehr leicht, eigenen Code dort anzubinden, der über die gesetzlich geregelten Funktionen hinausgeht. Das heißt, ein Erweiterungsmodul, welches über Einschränkungen verfügt, die es sich selbst setzt, könnte durch diverse Tests durchlaufen und zertifiziert werden, und am Ende kann es einfach gegen andere Module ausgetauscht werden – das ist der Sinn modularer Programmierung –, die dann nicht mehr über diese Selbsteinschränkungsmechanismen verfügen.

Eine definierte Programmierschnittstelle erlaubt grundsätzlich die schnelle, einfache und zuverlässige Erweiterung der Überwachungssoftware zu jeder Zeit. Diese Module können leichter versteckt, verschleiert und später auch zerstört werden, sodass möglicherweise am Ende nicht mehr wirklich nachweisbar oder beweisbar ist, dass es ein solches Modul mit diesen erweiterten Funktionalitäten überhaupt gegeben hat. In jedem Fall könnte ein zugelassener Trojaner temporär in einen illegalen Trojaner verwandelt werden, ohne am Ende Spuren zu hinterlassen.

Zu der Aussage, dass keinesfalls die Grenze zur Online-Durchsuchung überschritten werden dürfe, würde ich gern anführen, dass man auf einem Rechner – – Herr Rieger hat es schon angedeutet. Es ist klar: Sobald dieser Code, der aus Sicht eines Rechners oder eines Benutzers ein schadhafter Code, eine Schadsoftware ist, ausgeführt wird, kann man sich nicht auf ein ganz bestimmtes Blickfeld einschränken. Also das Ignorieren von anderen Datenverarbeitungen, für die es meinetwegen keine rechtliche Grundlage gibt – wie zum Beispiel das Mitschneiden von Videos, also von einer Webcam usw. –, ist nicht möglich. Es gibt keine digita-

len Scheuklappen für Trojaner. Beamte, die eine Hausdurchsuchung durchführen, schauen auch nach links und rechts. Denen kann man ebenso wenig verbieten, auch den Rest der Wohnung anzusehen.

Es ist grundsätzlich technisch nicht möglich, eine generische Überwachungssoftware herzustellen, die von technisch nicht versiertem Personal konfiguriert und eingesetzt werden kann und gleichzeitig die ihr gebotenen Einschränkungen enthält. Die Behörden können nicht sicherstellen, dass es in ihren Reihen niemanden gibt, der nicht über das notwendige Wissen verfügt, die gegebenen Schnittstellen zu missbrauchen. Es gibt also nicht so etwas wie einen negativen Einstellungstest, der sicherstellt, dass eine Person nicht über das Wissen verfügt, etwas zu tun. Genauso wenig kann ein unabhängiger und externer Dienstleister sicherstellen – also beweisen –, dass eine Schadsoftware wie ein Staatstrojaner zu einem bestimmten Zeitpunkt keine illegale Hintertür besitzt. So ein Prüfer kann die Anwesenheit einer schadhaften oder illegalen Funktion beweisen, aber nicht die Abwesenheit, genauso wenig, wie eine Überwachungsbehörde sicherstellen kann, dass die Mitarbeiter nicht über das notwendige Wissen verfügen, technisch diese Software zu manipulieren.

Zur Signierung der Überwachungssoftware, um sicherzustellen, dass die Grenzen eingehalten werden, möchte ich zumindest vermuten, dass die Autoren des Antrags keine praktischen Erfahrungen hinsichtlich der Softwaresicherheit und Kryptografie haben, denn das Sicherstellen der Authentizität einer staatlichen Schadsoftware mittels digitaler Signatur ist grundsätzlich ziemlich ausgeschlossen. Vergleichen Sie diesen Vorschlag mit einem Vorgehen bei der Authentifizierung: Wenn ich Sie beispielsweise anrufe, dann bitten Sie mich, mich zu authentifizieren, und ich sage: Alles klar. Ich stelle mich vor einen Spiegel, gucke mich an, und sage: Ich bin es –, und Sie sind mit dieser Form der Authentifizierung einverstanden. So ungefähr kann man sich das vorstellen, wenn wir über die digitale Signatur von Schadsoftware sprechen.

Sie sehen, das Verfahren ist für das Ausschließen eines schadhaften Verhaltens ziemlich ungeeignet und unpraktikabel. Wenn wir tatsächlich von einer digitalen Signatur sprechen, bedeutet das auch, dass wir im Hintergrund eine Public-Key-Infrastruktur haben. Es ist auch überhaupt nicht beschrieben, wie die praktisch aussehen soll. Das heißt, wenn ich eine digitale Signatur überprüfen möchte, muss ich zumindest auch im Besitz der entsprechenden Zertifikate der signierenden Stelle sein, d. h. des öffentlichen Schlüssels. Wo liegt dieser öffentliche Schlüssel? Ist der irgendwo hinterlegt? Ist der vielleicht Bestandteil dieser Schadsoftware? Das heißt, soll die Schadsoftware tatsächlich hergehen und sagen: Ja, ich bin es – oder: Nein, ich wurde modifiziert? – Wird am Ende der betroffenen Person noch das Binary ausgehändigt, damit man vielleicht später noch nachvollziehen kann, was genau für eine Schadsoftware installiert war?

Ich bin davon überzeugt, dass es kein Framework oder keinen Modulbaukasten geben kann, der generisch für Computerüberwachungen in diesem Sinne geeignet ist, da man diese Software, die dort eingesetzt wird, nicht kontrollieren kann. Es ist technisch nicht möglich zu beweisen, dass diese Software nicht manipuliert ist oder nicht manipulierbar ist.

Oft wird der Vergleich herangezogen, dass Polizisten grundsätzlich als vertauenswürdig angesehen werden. Die laufen schließlich auch mit einer scharfen Waffe herum, und die würden nicht jemanden einfach so erschießen, nur, weil sie es können. Aber der Vergleich hinkt ein Stück weit, denn wir reden hier von digitalen Waffen, die eingesetzt werden, und im Gegensatz zu einer Waffe, die ein Polizist am Gürtel trägt, werden hier keine Bytes verschossen und sind dann anschließend weg, und man muss sich anschließend auch nicht dafür rechtfertigen, warum irgendwelche Bytes weg sind, denn sie sind nicht weg.

Die Befürworter der Theorie, dass diese Technik 100-prozentig kontrollierbar sei und dass man sehr wohl diese Funktionalität im Rahmen einer Quellen-TKÜ beschränken könne, sollten möglicherweise mal darüber nachdenken, erst mal einen konkreten Beweis auf den Tisch zu legen, dass das grundsätzlich möglich ist, denn es ist nach heutigem Stand der Wissenschaft nicht möglich.

Die einzige Möglichkeit, eine rechtlich unbedenkliche TKÜ durchzuführen, ist, diese TKÜ individuell und unter permanenter Beobachtung durch Dritte durchzuführen. Möglicherweise ist eine solche TKÜ eben nur dann rechtlich zulässig, wenn ohnehin eine umfangreiche Online-Durchsuchung angeordnet wurde. Deshalb bin ich der Auffassung, dass das programmatische Ausspionieren eines Computers unter der rechtlichen Maßgabe einer Quellen-TKÜ praktisch nicht umsetzbar ist. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Als Nächstes hören wir die Stellungnahme des Senats. – Herr Statzkowski!

Staatssekretär Andreas Statzkowski (SenInnSport): Herr Vorsitzender! Meine sehr geehrten Damen und Herren! Für den Berliner Senat haben wir zwei Fachleute eingeladen, die Stellungnahmen für den Berliner Senat abgeben. Das sind Herr Kriminaldirektor Andreas Reinhard, Dezernatsleiter für die qualifizierte technische Ermittlungsunterstützung, und Herr Fischer, Diplom-Ingenieur für Informatik von der Abteilung 72 des Landeskriminalamtes. Beide sind anwesend, und beide erhalten von mir die Genehmigung zur Stellungnahme.

Vorsitzender Alexander Morlang: Gehen Sie bitte zu einem der Mikrofone, damit wir das auch im Stream haben, und sagen Sie bitte vorher noch mal Ihren Namen!

Andreas Reinhard (Berliner Polizei): Mein Name ist Andreas Reinhard. Wie schon vorgestellt, bin ich Dezernatsleiter im Landeskriminalamt Berlin für den Bereich qualifizierte technische Ermittlungsunterstützung und zuständig für die Kommunikationsüberwachung innerhalb der Polizei des Landes Berlin. Ich habe den Diplom-Informatiker Manuel Fischer, der Mitarbeiter in meinem Dezernat ist, mitgebracht, weil ich mit den technischen Dingen nicht so vertraut bin wie andere hier. Er ist für die Erstellung von Sicherheitskonzepten für unsere Tätigkeiten im Landeskriminalamt zuständig.

Ich möchte mich vorab für die Einladung bedanken und auch für das Vertrauen, dass ich als Polizist hier sprechen darf. Ich kann nachvollziehen, dass das eine oder andere kritisch gesehen wird, und möchte die Sicht der Polizei aus der Sicht der Strafverfolgung kurz darstellen, mit etwas allgemein einführenden Worten, und bin auch bereit, dann Fragen zu beantworten.

Wir haben den gesetzlichen Auftrag der Strafverfolgung. Es ist heute schon thematisiert worden, dass im Rahmen der Kommunikationsüberwachung jetzt, wo schon seit einiger Zeit verschlüsselt kommuniziert wird, dieser Bereich nicht deshalb ausgeblendet werden kann, weil er eben verschlüsselt erfolgt, sondern wir sind grundsätzlich im Rahmen der Verfassung und der anderen gesetzlichen Vorgaben gefordert, uns damit auseinanderzusetzen.

Das haben wir begonnen, indem wir 2011 – ich greife jetzt zeitlich mal vor – eine Quellen-TKÜ-Software beschafft haben, die bisher nicht eingesetzt worden ist, um das hier gleich darzustellen. Das hatte zum einen den Grund, weil wir innerhalb der Behörde zum einen durch die Datenschutzbeauftragte der Berliner Polizei, dann durch die innere Revision – ein Instrument, das besonders darauf zu achten hat, dass wir auch im IT-Bereich ganz korrekt vorgehen – überprüft worden sind bzw. diese Software dort vorgestellt und im Rahmen eines Sicherheitskonzeptes weiterentwickelt worden ist. Wir haben auch eine Risikoanalyse begonnen, die noch nicht ganz fertiggestellt ist. Wenn Sie den Zeitpunkt der Beschaffung mit dem heutigen Tag vergleichen, sehen Sie schon, dass wir uns über ein Jahr ganz intensiv diesen Fragen gewidmet haben und noch widmen, ohne die Software bisher einzusetzen.

Zwischenzeitlich – die Probleme mit anderen Herstellern und auch anderen Bundes- und Landesbehörden sind schon angesprochen worden – ist unter Federführung des Bundeskriminalamtes ein Qualitätssicherungsprozess angestoßen worden. Bei uns heißt das intern „standardisierte Leistungsbeschreibung“, mit der insbesondere aufgrund der bundesweiten, auch notwendigen rechtssicheren und möglichst einheitlichen Verfahrensweise eine solche Leistungsbeschreibung erstellt werden sollte, um Mindeststandards zu schaffen, die dann für alle Strafverfolgungsbehörden gleichermaßen gelten soll. Diese ist in einem Entwurf dem AK II, dem Ausschuss für innere Sicherheit der Innenministerkonferenz, vorgelegt worden und so weit als sinnvoll erachtet worden, daran weiterzuarbeiten.

Insofern haben wir uns dem Votum aller anderen Länder und der Bundesbehörden angeschlossen, dass wir unsere Quellen-TKÜ-Software erst dann einsetzen, wenn diese Leistungsbeschreibung abgeschlossen ist und wenn entsprechend auch der Quellcode auditiert worden ist, was – durch das Bundesamt für Sicherheit in der Informationstechnik und auch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angestoßen – durch das BSI an eine Fremdfirma vergeben worden ist. Solange diese Ergebnisse nicht vorliegen, wird es keinen Einsatz einer Quellen-TKÜ in Berlin geben.

Als Strafverfolger müssen wir, wie gesagt, daran interessiert sein, alle Ermittlungslücken zu schließen, auch die technischen, und da sind wir auf einem guten Weg. Wenn dieses Sicherheitskonzept, was die Berliner Lösung betrifft, fertiggestellt ist, wird diese – ebenso deutlich gesagt – vor dem Einsatz in Berlin dem Berliner Beauftragten für Datenschutz und Informationsfreiheit im Rahmen eines Ortstermins zur Einsichtnahme zur Verfügung gestellt werden. Es ist auch vorgesehen, dass dann, wenn wir möglicherweise, weil uns ein Gerichtsbeschluss zumindest die Möglichkeit gibt, das zu tun – das vor dieser bundesweiten Lösung erfolgen soll –, der Berliner Datenschutzbeauftragte die Möglichkeit haben wird, den Quellcode in den Räumlichkeiten des Herstellers einzusehen, ohne dass dafür weitere Kosten entstehen.

Zusammenfassend ist zu sagen: Wir warten noch, weil die Diskussion, die hier dargestellt wurde, uns genauso betrifft. Wir sind zwar weder Politiker noch Techniker im engeren Sinn, aber wir beobachten sehr gut und wollen uns der rechtsstaatlichen Lösung anschließen, wie

wir das im Übrigen auch bisher in allen anderen strafprozessualen Maßnahmen tun. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Herr Dix, Sie haben das Wort.

Dr. Alexander Dix (Beauftragter für Datenschutz und Informationsfreiheit): Vielen Dank! – Ich würde angesichts der Anträge, die hier zur Beratung vorliegen, gern auf einen wesentlichen Unterschied hinweisen wollen. Zum einen muss man die Frage der rechtlichen Zulässigkeit der Quellen-TKÜ von der Frage ihrer Kontrollierbarkeit unterscheiden. Der Koalitionsantrag – und auch das begrüße ich ausdrücklich – befürwortet die Schaffung einer Rechtsgrundlage im Bereich der Strafverfolgung über eine Bundesratsinitiative, die es bisher nicht gibt. Das sehe ich ganz genauso, allerdings wird unter Ziffer 3 – möglicherweise verstehe ich den Koalitionsantrag da falsch – der Eindruck erweckt, als ob es für den Berliner Verfassungsschutz schon jetzt eine Rechtsgrundlage für den Einsatz dieser Software gebe.

Das wird auf eine Vorschrift im Landesverfassungsschutzgesetz gestützt, die älter und unbestimmter ist als die Vorschrift des nordrhein-westfälischen Verfassungsschutzgesetzes, die vom Bundesverfassungsgericht 2008 kassiert wurde, und sie entspricht auch nicht den Vorgaben des § 20l des BKA-Gesetzes, die gegenwärtig noch dem Bundesverfassungsgerichtshof zur Prüfung vorliegen. Ich lege Wert auf die Feststellung, dass nach meiner Auffassung gegenwärtig von keiner Berliner Behörde die Quellen-TKÜ durchgeführt werden kann, weil es dafür keine Rechtsgrundlage gibt. Die müsste erst geschaffen werden.

Zu Ziffer 2: Jetzt komme ich zum Problem der Kontrollierbarkeit. Ich begrüße es sehr, dass dem Berliner Beauftragten für Datenschutz und Informationsfreiheit weitgehende Kontrollrechte eingeräumt werden sollen. Die sind auch dringend erforderlich, aber es gibt unter Ziffer 2 die Formulierung:

> Bis dahin darf im Land Berlin Software für die Quellen-TKÜ nur unter der Bedingung eingesetzt werden, dass dem Berliner Beauftragten für Datenschutz eine uneingeschränkte Kontrolle ermöglicht wird.

Solange eine Rechtsgrundlage nicht vorliegt, darf sie auch unter dieser Kontrollmaßgabe nicht eingesetzt werden. Das würde ich gern unterstreichen wollen. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Wir kommen damit zur ersten Fraktionsrunde. Das Wort hat Kollege Kohlmeier.

Sven Kohlmeier (SPD): Herzlichen Dank, Herr Ausschussvorsitzender! – Einen großen Dank an die Anzuhörenden, weil das in dieser Diskussion um unterschiedliche Anträge und unterschiedliche Begrifflichkeiten, die genannt wurden, zu sehr viel Aufklärung beiträgt, und es war eine der besten oder kenntnisweitergebensten Anhörungen, die ich in diesem Haus in dieser Legislaturperiode erlebt habe.

Ich habe einige Fragen an die Anzuhörenden. Ich versuche, es nach meinem Zettel zu machen, der ein bisschen ungeordnet geworden ist. Ich muss es einfach so machen, dass ich sage, wem ich die Frage stelle, und dann müssen die Betreffenden mitschreiben.

An die Verwaltung: Herr Buermeyer bzw. mehrere Anzuhörende haben gesagt, dass technisch nicht sicherzustellen ist, dass diese Software nur für Quellen-TKÜ verwendet wird und nicht für einen Staatstrojaner oder eine Online-Durchsuchung. In der politischen Diskussion wird böswillig oder mutwillig oder aus Unkenntnis gern das eine mit dem anderen verwechselt. Können Sie mir erläutern, wie die Behörden sicherstellen, dass sie nur das eine machen, und zwar eine Quellen-TKÜ, wenn sie dazu ermächtigt sind, und keine Online-Durchsuchung? Vielleicht kann man das so darstellen, dass man das versteht, dass technisch auch nur das eine möglich ist.

Zweitens: Herr Buermeyer sagte, dass Sie aus rechtlichen Gründen der Auffassung sind, dass es derzeit keine Rechtsgrundlage für eine Quellen-TKÜ gibt. Nun gab es in der Vergangenheit, vielleicht nicht im Land Berlin – das haben wir gerade gehört; so soll es wohl nicht gewesen sein –, aber in anderen Bundesländern Maßnahmen der Quellen-TKÜ. Glauben Sie, dass wir mit dem Antrag, den wir hier vorlegen, und zwar einer Bundesratsinitiative, eine entsprechende Rechtsgrundlage für die Quellen-TKÜ schaffen würden?

Herr Dr. Nöding sagte, er würde das nicht so sehen, da müssten viel mehr Tatbestandsvoraussetzungen eingebracht werden. Deshalb die Frage an die Anzuhörenden, vielleicht auch an Herrn Dr. Nöding: Wie sollte denn eine Rechtsgrundlage aussehen? – Vielleicht zur Erklärung an beide Anzuhörenden: Es ist im parlamentarischen Brauch nicht so, dass man dann, wenn man eine Bundesratsinitiative macht, den beabsichtigten Gesetzestext schon im Wortlaut vorgibt, weil man – wenn das Land Berlin als einzelnes Land so eine Bundesratsinitiative startet – darauf angewiesen ist, dass sich weitere Bundesländer anschließen. Deshalb gibt es selten einen vorgefertigten Text, sondern in der Regel nur diese Absichtserklärung, dass man eine entsprechende Änderung – wir haben geschrieben: „entsprechend dem BKA-Gesetz“ – haben möchte. Deshalb die Frage an beide Anzuhörenden, wie eine entsprechende Rechtsgrundlage aussehen müsste.

Herr Dr. Nöding! Sie haben gesagt, dass Sie sich eine Subsidiaritätsregelung gegenüber einer normalen TKÜ vorstellen können. Ich frage mich, wie die praktisch funktionieren soll. Vielleicht habe ich das Verfahren in der Innenbehörde oder beim Einsatz von Quellen-TKÜ falsch verstanden. Da wird wohl in der Regel wenig Zeit sein, erst eine normale TKÜ zu machen, die auszuwerten und dann festzustellen, dass die Auswertung nicht den gewünschten Erfolg hat, um dann eine Quellen-TKÜ zu machen, wo möglicherweise in der Vergangenheit irgendwelche Gespräche über Quellen-TKÜ gelaufen sind. Deshalb die Frage, vielleicht an alle Anzuhörenden, ob es tatsächlich möglich ist, im Ermittlungsverfahren erst mal eine normale Telefonüberwachung zu machen und dann festzustellen: Er telefoniert gar nicht über das Telefon, sondern der macht eine Quellen-TK, und dann springen wir mal auf eine Quellen-TKÜ um. – Ich kann es mir aus ermittlungstechnischen Gründen nicht vorstellen.

Herr Dr. Nöding! Sie haben gesagt, dass als Anknüpfungspunkt für eine Quellen-TKÜ der Eingriff erheblicher wäre. Ich lasse mal die rechtlichen Voraussetzungen, dass man auf einen PC zugreift usw., außen vor. Sie sagten, dass es anders wäre als bei einer normalen Telefonüberwachung, weil am PC Personen betroffen sind, die vielleicht nicht betroffen sein sollen. Wenn ich mir das überlege, kann ich keinen qualitativen Unterschied zwischen der normalen Telefonüberwachung feststellen, wo auf einmal die Tochter Lisa telefoniert, und der Staat und die Ermittlungsbehörde hören mit – die soll möglicherweise nicht davon betroffen sein, sondern der böse Vater Mafioso –, und dem PC des Mafioso, wo eine Quellen-TKÜ gemacht

wird und wo sich auch Lisa dransetzt und ein Spiel machen möchte. Deshalb die Frage: Wo sehen Sie da den qualitativen Unterschied zwischen einer normalen Telefonüberwachung und einer Quellen-TKÜ?

Herr Rieger! Sie haben ausgeführt, wie so eine Modulbauweise oder so eine Schadsoftware aussehen soll, und darauf geschlossen, weil die Firmen eine niedrige Reputation haben, dass man damit unterstellen würde, sie würden nicht ordnungsgemäß oder nicht rechtmäßig arbeiten – oder so. Mich würde interessieren, ob es einen weiteren Beleg für die These gibt, dass das Land Berlin ebenfalls nicht rechtmäßig arbeiten würde. Dass es einen Fall gegeben hat, der nicht in Ordnung war, ist uns allen hier in diesem Raum bekannt. Ich weiß bloß nicht, ob man aufgrund dieses Falls – vielleicht gibt es noch fünf andere Fälle, von denen wir alle nichts wissen – darauf schließen kann und daraufhin den Berliner Behörden unterstellt, dass sie nicht rechtmäßig oder nicht den Vorgaben des Bundesverfassungsgerichts entsprechend arbeiten würden. Also, die reine Tatsache, dass eine Firma Software oder andere Dienstleistungen in Drittstaaten liefert, die uns nicht besonders genehm sind! Das könnte möglicherweise dazu führen, dass große deutsche Firmen zukünftig nicht mehr für den Staat arbeiten dürften, weil auch einige große Firmen Anlagen usw. an Drittstaaten liefern, die uns nicht besonders genehm sind.

Sowohl Herr Schröder als auch Herr Rieger haben über die Signierung gesprochen. Wir haben in dem Fall keine Signierung. Es gab schon Überlegungen, ob man so eine Software signieren lässt, bevor sie eingesetzt wird. Das Verfahren ist wohl dann so, dass die Signierung zu lange dauert. Herr Rieger! Das haben Sie entsprechend dargestellt. Deshalb war unser Vorschlag, die Möglichkeit der Einsichtnahme durch den Datenschutzbeauftragten des Landes Berlin, weil er die unabhängige Stelle bei uns ist. Können Sie sich vorstellen, wenn so, wie Herr Reinhard es vorgestellt hat, eine Software zur Quellen-TKÜ nur dann eingesetzt wird, wenn sie entsprechend vom BSI oder durch unabhängige Drittüberwacher oder wie auch immer auditiert oder signiert wird, dass dann ein Einsatz möglich wäre?

Mir ist bekannt, dass Sie den Einsatz nicht wollen. Den wollen wir möglicherweise alle nicht, aber die Ermittlungsbehörden sagen, sie wollen diese Möglichkeit nutzen. Ich finde, das ist überzeugend dargestellt worden. Ich kann mir nicht vorstellen, dass die Ermittlungsbehörden nur noch mit Papier arbeiten und alle andern am PC. Herr Rieger! Gehen wir mal davon aus, die Ermittlungsbehörde soll eine Quellen-TKÜ-Software haben oder nutzen können, könnten Sie damit leben, wenn die vom BSI in Verbindung mit einem unabhängigen Dritten signiert wird?

Vorsitzender Alexander Morlang: Vielen Dank! – Als Nächstes ist Herr Behrendt dran.

Dirk Behrendt (GRÜNE): Danke schön, Herr Vorsitzender! – Ich möchte eine Bemerkung von Herrn Dix aufgreifen, die mich auch umtreibt, nämlich die durch die Antragsteller verursachte Wirrnis, was sie eigentlich wollen. Man muss noch mal klarkriegen, welche verschiedenen Bereich es präventiv und repressiv gibt, wo die Quellen-TKÜ zum Einsatz kommen könnte. Sie müssen Farbe bekennen, wo Sie das eigentlich wollen und wo nicht. Ihre Bundesratsinitiative richtet sich klar in Richtung StPO-Regelung, also repressiv. Im präventiven Bereich sind Sie viel undeutlicher. Wir müssten diskutieren, ob Sie diese Möglichkeit im Berliner Polizeirecht schaffen wollen. Das scheint nicht der Fall zu sein, das begrüßen wir.

Die Ziffer 3, auf die Herr Dix abgehoben hat, beschäftigt sich mit dem Verfassungsschutz. Uns würde schon interessieren, ob Sie diese Regelung für den Berliner Verfassungsschutz schaffen wollen. Darauf deutet zumindest der Inhalt von Ziffer 3 hin. Ich hatte schon in der Plenarrede darauf hingewiesen, dass es schlechterdings keinen Sinn macht, eine Bundesratsinitiative mit diesem Inhalt zu starten, weil das unsere Gesetzgebungskompetenz als Landesgesetzgeber ist. Deswegen fällt dieser Punkt 3 ein bisschen komisch raus. Da würden wir um Aufklärung bitten.

Was die Frage angeht, wie der Bund das handhabt: Der hat ja im BKA-Gesetz im präventiven Bereich schon eine entsprechende Regelung getroffen. Nur damit es klar ist: Diese fünf Bereiche gibt es, und, wie gesagt, wir müssten klarhaben, wo Sie es eigentlich wollen.

Dann würde mich interessieren: Sie schreiben im ersten Satz, das sei ermittlungsnotwendig und das würden die Ermittlungsbehörden einfordern. Es ist das Wesen von Ermittlungsbehörden, dass sie am liebsten jede Ermittlungsmöglichkeit hätten. Aber es ist genauso das Wesen unseres Rechtstaats, dass sie nicht jede Ermittlungsmethode kriegen. Für unsere Meinungsbildung wäre es hilfreich – aber wahrscheinlich müsste man mal mit der Staatsanwaltschaft ins Gespräch kommen –, in Erfahrung zu bringen, an welchen Stellen es krankte, wo sie konkrete, spezifische Hinweise hatten, dass womöglich über Skype oder andere Formen E-Mail-Austausche stattfanden, die man nicht ermitteln konnte, und wo schwere Straftaten begangen wurden, wo bestimmte Ermittlungen länger dauerten, und wo Leute sich womöglich absetzen konnten und man sie gehabt hätte, wenn man schneller zugegriffen hätte.

Diese Frage ist offen. Es wird nicht dadurch richtig, dass man es als Behauptung in den ersten Satz reinschreibt. Das ist eben so. Da sind Sie alle vier nicht diejenigen, die das beantworten können. Aber wichtig für die Beurteilung, ob wir eine Quellen-TKÜ brauchen, wäre es uns, denn wir diskutieren das Gleiche bei der Vorratsdatenspeicherung, und auch da behaupten alle, das sei ganz dringend nötig, und auch da sind wir sehr skeptisch und noch nicht davon überzeugt, dass man das wirklich braucht. Da sind wir mit Herrn Nöding auf einer Linie, dass wir uns das eingeschränkt vorstellen können, wenn der Beweis geführt ist oder so konkrete Anhaltspunkte mitgeteilt werden, dass sich die Notwendigkeit dann daraus ergibt.

Ich schließe mich sehr gern dem Dank an alle vier Anzuhörenden an. Das war ein gutes Beispiel – weil wir zwei Juristen und zwei Techniker haben –, wo sich verschiedene Disziplinen treffen. Ich stelle fest, dass wir schon ein bisschen weiter sind, was die Verständigung von Juristen mit Technikern angeht, was das Internet angeht. Ich erinnere mich noch – das ist zugegebenermaßen schon einige Jahre her –, wo Staatsanwaltschaften Durchsuchungs- und Beschlagnahmebeschlüsse erwirkten, um einen konkreten Computer aus irgendeiner Wohnung rauszuholen, weil derjenige irgendwelche Sachen ins Internet eingestellt hatte, und sie waren der Meinung, dass dann, wenn man den Computer von ihm zu Hause mitnimmt – das ist tatsächlich von der Polizei vollstreckt worden, das kann man sich heute nicht mehr vorstellen –, das automatisch aus dem Internet verschwindet. So was gab es. Da sind wir heute weiter.

Aber die Notwendigkeit, dass wir als Juristen die technischen Voraussetzungen im Blick behalten, besteht weiterhin. Wenn ich richtig verstanden habe, was die beiden Techniker hier gesagt habe, ist diese Differenzierung – Quellen-TKÜ auf der einen Seite und Online-Durchsuchung auf der anderen Seite – technisch gar nicht machbar. Deswegen trifft die Debatte, ob man unter besonderen Voraussetzungen Quellen-TKÜ macht, also unter weiteren

Voraussetzungen als bei der Online-Durchsuchung, auf eine technische Grenze, wo es keinen Sinn mehr macht. Das ist auch etwas, das sich das Bundesverfassungsgericht deutlich vor Augen führen muss. Wenn diese Differenzierung, die man hier einzieht, im Technischen keine Entsprechung hat, ist sie nicht nur willkürlich, sondern sinnlos. Sie nicken mit dem Kopf, Herr Buermeyer. So habe ich Sie auch verstanden.

Solange dieses Problem, wenn es überhaupt ein Problem ist, nicht ausgeräumt ist, macht es keinen Sinn, über irgendwelche Gesetzgebungsinitiativen zu sprechen, auch wenn wir uns Juristen ja wünschen würden, dass die Welt so wäre, wie wir sie gern hätten. Aber die Welt ist nicht immer so, wie wir sie gern hätten, und wir müssen uns als Juristen an die Welt und nicht die Welt an die juristische Vorstellung anpassen. Das gilt auch hier.

Wenn ich Sie richtig verstanden habe – das wäre eine wichtige Frage –, dann ist diese technische Seite nicht möglich, sondern das wäre eigentlich nur möglich, wenn man in die Siebzigerjahre zurückgeht, wie man damals die Telefonüberwachung gemacht hat: Man schraubte das Telefon auf, machte eine Wanze rein, und schraubte das Telefon wieder zu. – Wenn man das an das Mikrofon des Computers von außen dranmacht – wir wissen alle, man würde es sehen, aber wir denken uns jetzt mal, das wäre unsichtbar –, dann würde man auf der Strecke vom Mund zum Mikrofon den Ton abpassen und nicht in den Computer reingehen, denn sobald man in den Computer reingeht, ist das alles nicht mehr auseinanderzuhalten, und es lässt sich dann nicht differenzieren, was man an Kommunikationsvorgängen überwacht und was man an weiteren Inhalten überwacht.

Ich bin Herrn Nöding dankbar, dass er das deutlich gemacht hat, was die Frage der Verhältnismäßigkeit angeht und die Frage, wie schwerwiegend der Eingriff ist. Das Bundesverfassungsgericht hat das erfreulicherweise sehr deutlich in seinen Beschluss geschrieben, bei anderen juristischen Erörterungen kommt das meiner Einschätzung nach zu kurz, nämlich die Bewertung und Einschätzung, welche Rolle der Computer heute für die private Lebensführung hat – Stichwort: Tagebuchfunktion und Ähnliches. Das ist deutlich etwas anderes als das Telefon. Diese Sensibilität gibt es in der Bevölkerung. Bei der Vorstellung, dass jemand von außen in den Computer eindringt und alles überwacht, gibt eine hohe Sensibilität. Dafür bin ich dankbar, weil das auch ein Problembewusstsein zeigt. Aber wenn man Strafermittler oder andere Ermittlungsbehörden hört, so sagen die: Wir brauchen das einfach, und das ist unerlässlich für die Ermittlungen, und deswegen muss man das einfach hinnehmen.

Es bleiben die Fragen: Was will die Koalition eigentlich hinsichtlich des Verfassungsschutzes? Das ist völlig unklar. Und habe ich das mit der technischen Unmöglichkeit dessen, was das Bundesverfassungsgericht uns aufgegeben hat, und den daraus folgenden Konsequenzen so richtig verstanden? – Danke!

Vorsitzender Alexander Morlang: Vielen Dank! – Als Nächstes hat Herr Dregger das Wort.

Burkard Dregger (CDU): Vielen Dank, Herr Vorsitzender! – Ich möchte mich zunächst bei den Anzuhörenden für die Ernsthaftigkeit und die Sachlichkeit dieser Ausführungen bedanken. Wir wissen alle, dass das auch im politischen Raum ein sehr emotionales Thema ist. Es hat der Debatte sehr gut getan, dass hier auf der Grundlage von Fakten und Argumenten diskutiert wird.

Wenn es um TKÜ geht, geht es darum, dass es sich um einen erheblichen Grundrechtseingriff handelt. Ich glaube, das ist allen klar. Wir haben immer abzuwägen: auf der einen Seite das Strafverfolgungsinteresse des Staates, das Gewaltmonopol des Staates, das durchzusetzen ist – letztlich damit auch den Schutz nicht nur des Staates, sondern auch seiner Bürger vor Schwerverbrechen –, und auf der anderen Seite die Grundrechtssphäre des Betroffenen, gegen den solche Maßnahmen angeordnet werden. Wir haben auf jeden Fall einen Schutzmechanismus darin, dass derartige Maßnahmen nur durch einen Richter verhängt werden können, also nicht durch einen Polizeibeamten, einen Staatsanwalt oder womöglich einen Abgeordneten. Aber Sie haben in Ihren Ausführungen zu Recht darauf hingewiesen, dass es möglicherweise einen Ermittlungsrichter überfordert, zusätzlich zu den konkreten Tatbestandsvoraussetzungen auch noch zu prüfen, ob die anzuordnende TKÜ überhaupt technisch im rechtlichen Rahmen zulässig ist. Deswegen freue ich mich, dass wir hier über die spezifischen Fragen der Quellen-TKÜ sprechen.

Ich hätte eine Frage an Herrn Buermeyer, der am Anfang meines Erachtens sehr eindrucksvoll die rechtlichen Fragen zur Zulässigkeit einer Quellen-TKÜ dargelegt hat. Sie haben genauso wie wir alle die technischen Ausführungen der anderen Anzuhörenden vernommen, also das Thema der Modulbauweise und der Nachladbarkeit von Modulen. Ich wollte Sie fragen, ob Sie angesichts dieser Ausführungen der Auffassung sind, dass das, was die Koalition mit ihrem Antrag beantragt, nach wie vor den Voraussetzungen des Bundesverfassungsgerichts entspricht. Das würde mich interessieren.

Dann hätte ich eine weitere Frage. Herr Nöding hat zu Recht darauf hingewiesen, dass es sich um einen sehr intensiven Grundrechtseingriff handelt. Sie sagten sogar, dass eine Quellen-TKÜ ein intensiverer Grundrechtseingriff ist als eine normale Telefonüberwachung. Auf der anderen Seite sind die Grundrechte, die durch solche Maßnahmen geschützt werden sollen, wahrscheinlich die gleichen, d. h. das Strafverfolgungsinteresse, aber auch der Schutz Einzelner. Auch dort sind erhebliche Rechtsgüter vorhanden.

Herr Rieger! Sie sagten, dass die Hersteller, die Sie genannt haben, offenbar auch Produkte anbieten – das haben Sie zumindest angedeutet –, die nicht den Voraussetzungen des Bundesverfassungsgerichts entsprechen, weil sie auch für andere Rechtsordnungen hergestellt werden, nicht nur für die Rechtsordnung der Bundesrepublik Deutschland. Ist das tatsächlich ein Argument, um eine solche Maßnahme bzw. technische Einrichtung per se abzulehnen, oder kommt es nicht darauf an, wie sie im Einzelfall ausgestaltet ist? Wir wissen alle, es gibt auch Waffenexporte in alle möglichen Länder. – [Sven Kohlmeier (SPD): Sie schockieren mich, Herr Kollege!] – Es gibt jedenfalls weltweit einen großen Markt, und die Frage ist immer, unter welchen Voraussetzungen etwas eingesetzt wird. Da hätte ich gern nachgefragt.

Herr Schröder hatte einen Punkt genannt – Sie hatten das zitiert –: Auch ein Polizeibeamter kann eine Dienstwaffe missbrauchen. Ich habe aber Ihre Erklärung nicht verstanden, warum Sie das hier offenbar anders sehen. Natürlich ist jede Kompetenz, die man einem Kompetenzträger angedeihen lässt, in jederlei Hinsicht missbrauchbar, nicht nur im Rahmen der Strafverfolgung. Warum also soll das ein Argument sein, es per se abzulehnen, oder habe ich Sie vielleicht missverstanden? – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Für die Linksfraktion nun Frau Möller!

Katrin Möller (LINKE): Vielen Dank! – Vielen Dank auch an die Anzuhörenden! Sie konnten leider unsere Bedenken bezüglich der rechtlichen und verfassungsrechtlichen Probleme, die das alles mit sich bringt, nicht zerstreuen und haben für sehr viel Aufklärung gesorgt, was den technischen Hintergrund betrifft. In dem Zusammenhang freue ich mich, von Ihnen zu hören, Herr Reinhard, dass Sie erst noch das Ergebnis der Risikoanalyse abwarten wollen, um weitere Schritte einzuleiten. Ich habe in diesem Zusammenhang noch eine Frage, die noch nicht zur Sprache gekommen ist. Was darf man sich unter einer verdeckten Installation vorstellen, einem heimlichen technischen Eingriff, sollte die Software doch zum Einsatz kommen und möglicherweise sich der Stand der technischen Entwicklung weiterentwickeln? Wie darf ich das verstehen? – Das ist das eine.

Eine andere Frage ist – darüber werden Sie sich auch schon Gedanken gemacht haben –: Wie sieht es mit der Deinstallation nach einer solchen Überwachung aus, von der wir eigentlich gelernt haben, dass sie aktuell technisch noch nicht kontrollierbar ist und dass die Funktionalität auch nicht auf eine Quellen-TKÜ allein beschränkbar ist? Wie haben Sie sich das vorgestellt?

In dem Zusammenhang auch die Frage: Gibt es da nicht mit anderen Ländern Vergleiche? Wie wird das anderswo gehandhabt? Wir werden in Berlin ja nicht die einzigen sein, die damit konfrontiert sind. Gibt es da schon Erfahrungen?

Eine weitere Frage wäre: Die Koalition hat begründet, dass entwicklungsnotwendige Maßnahmen zur Strafverfolgung Anlass geben, diesen Antrag zu schreiben bzw. diese Rechtsgrundlagen zu schaffen. Mich würde interessieren, auf welche Straftatbestände wir da blicken dürfen. Ich kann es mir im Moment nicht vorstellen, auch das muss ja recht scharf eingegrenzt werden. Da werden Sie sich ja zum jetzigen Zeitpunkt auch schon Gedanken gemacht haben. Dazu hätte ich gerne noch eine Aussage.

Zum anderen möchte ich Ihnen, Herr Nöding, danken. Sie haben auf einen Aspekt aufmerksam gemacht, der mir noch gar nicht so deutlich geworden ist, nämlich dass auch massive Eingriffe in die Persönlichkeitsrechte Dritter passieren, speziell in Anbetracht der Tatsache, dass immer mehr Menschen Home-Office betreiben, also vom gleichen Rechnersystem arbeiten und auch ihr Privatleben bestreiten. Das ist, selbst wenn es möglich wäre, dass die Funktionalität – – Also selbst dann, wenn nur die laufende Kommunikation überwacht würde, ist dieses Problem überhaupt nicht in den Griff zu bekommen. – Vielen Dank! So weit erst einmal.

Vorsitzender Alexander Morlang: Vielen Dank! – Herr Weiß!

Dr. Simon Weiß (PIRATEN): Danke! – Vielen Dank auch von unserer Seite an die Anzuhörenden! Ich versuche, meine Fragen auch analog zu trennen – technisch, organisatorisch, rechtlich. Zunächst einmal danke ich Ihnen noch mal für die technische Klarstellung, was das ist, womit wir es überhaupt zu tun haben, weil das auch im Vorfeld schon zu Diskussionen geführt hat: zum einen die rechtliche Trennung zwischen Online-Durchsuchung und Quellen-TKÜ, wie sie das Bundesverfassungsgericht vorgegeben hat, und dann der Trojaner als technischer Oberbegriff, weil wir es hier immer mit einem Trojaner zu tun haben werden.

Ich muss noch mal kurz von den Anzuhörenden weg und auch noch mal bei Herrn Kohlmeier nachfragen. Sie haben in der Plenardebatte noch gesagt, dass man bei einer Quellen-TKÜ sicherstellen muss, dass kein Staatstrojaner eingeschleust wird. Mich würde interessieren, ob Sie daraus jetzt irgendwelche Folgerungen für Ihren Antrag ziehen.

Technisch – zunächst einmal die Frage von den Erfahrungswerten her: Nehmen wir mal an, es gibt eine solche Software und sie wird regelmäßig eingesetzt. Von welchen Zeiträumen reden wir denn, wie schnell die geknackt ist? Von welchem Zeitraum reden wir, bevor der Quelltext irgendjemandem vorliegt wie z. B. dem CCC, wie im Fall des Trojaners von DigiTask, und von welchen Zeiträumen reden wir, bis der von herkömmlichen Antivirenscannern erkannt wird und man dann wiederum nachrüsten muss? – Herr Rieger, Sie haben eben angedeutet, dass man quasi bei jedem Einsatz noch mal neu nachmodifizieren müsste. Das ist auch insofern relevant, wenn man dann eine Form von Zertifizierung oder Prüfung für jedes einzelne Update durchführen will, folgt daraus auch ein entsprechender Personalbedarf bzw. ein nötiger Aufwand.

Die Frage ist auch, was hier auch schon ausgeführt wurde: Wenn man einmal einen solchen Trojaner installiert hat und das System damit aufgeknackt ist, insbesondere, wenn man noch nachladen kann: Wie einfach ist es dann für Dritte, diese Schnittstelle zu benutzen bzw. diese Sicherheitslücke zu benutzen?

Wenn ich mir jetzt vorstelle, dass man da z. B. ein Modul hat, wo man beliebig nachlädt – auch wenn es da eine Authentifizierung gibt, die wird ja systemseitig, also auf der Seite des Trojaners stattfinden –, wenn man den einmal aufgeknackt hat: Wie einfach ist es dann, da auch selber etwas nachzuladen und dann möglicherweise die Sicherheitslücke für noch ganz andere Sachen zu benutzen?

Die Frage nach der Abgrenzung steht im Raum. Um jetzt noch mal konkret nachzufragen: Ist denn das leistbar, oder mit welchem Aufwand ist das leistbar, sicherzustellen, dass jetzt nicht die juristischen Maßnahmen, sondern die technischen Maßnahmen, die vom Bundesverfassungsgericht vorgeschrieben sind, gewährleistet sind? Mit anderen Worten: Wie aufwendig ist es, grob geschätzt, eine solche Software daraufhin zu prüfen, ob sie wirklich nur das macht, was oben drüber steht? – Sagen wir mal so: Wie aufwendig ist es, das mit ziemlicher Sicherheit zu prüfen? Wie aufwendig ist es, das mit absoluter Sicherheit zu prüfen?

Zum Organisatorischen – was ich eben schon angesprochen habe: Wenn man jetzt, wie es sowohl unser Antrag als auch der Koalitionsantrag fordert, dem Datenschutzbeauftragten entsprechende Prüfrechte gibt, mit welchem Aufwand ist das eigentlich verbunden, und welche zusätzlichen Mittel müsste man dafür bereitstellen, je nachdem wie oft man da nachbessern muss oder wie oft man dann auch prüfen muss?

Die rechtliche Seite: Zunächst einmal ist natürlich die Diskussion: Will man dafür eine Rechtsgrundlage – eine politische? Ich wäre nicht geneigt, die Schaffung einer solchen Rechtsgrundlage als Fortschritt per se zu sehen. Ich meine, es gibt auch keine Rechtsgrundlage dafür, dass Ermittlungsbehörden foltern können. Ich glaube, wir sind uns alle einig, dass es eine gute Sache ist, dass es diese Rechtsgrundlage nicht gibt. Gleichwohl, wenn man sie will, muss man natürlich die Vorgaben des Bundesverfassungsgerichts beachten.

Noch mal die Frage zurück, weil Sie sich, Herr Buermeyer und Herr Dr. Nöding, nicht vollständig gegen eine solche Rechtsgrundlage, sondern eher noch als Schritt in die richtige Richtung ausgesprochen haben: Wenn es denn jetzt tatsächlich so ist, dass das, was das Bundesverfassungsgericht vorgeschrieben hat, technisch nicht machbar ist oder zumindest nicht so machbar ist, dass man kontrollieren kann, dass es auch wirklich gemacht wurde, folgt daraus nicht eigentlich, dass es eben keine gute Idee wäre, eine Rechtsgrundlage zu schaffen, denn eine Rechtsgrundlage für etwas zu schaffen, von dem man eigentlich weiß, dass es gar nicht geht, lädt ja eigentlich nur zu missbräuchlichem Verhalten ein, weil missbräuchliches Verhalten dann das einzig mögliche Verhalten ist, außer halt die Rechtsgrundlage gar nicht anzuwenden, was auch wiederum, wenn sie einmal da ist, nicht so einfach ist bzw. wiederum eine entsprechende Festlegung erfordern würde?

Zwei Punkte noch – beide wurden auch schon angesprochen: Das eine ist gewissermaßen die Verwertbarkeit von dem, was bei einem solchen Trojanereinsatz herauskommt. Es wurde von Herrn Rieger ganz konkret angesprochen, dass eben, wenn ein System einmal so kompromittiert ist, die Möglichkeit besteht, dass dann auch Manipulationen stattfinden, die der Benutzer nicht – – Die halt unter den Augen des Benutzers stattfinden. Wenn ein Staatstrojaner auf dem System installiert ist – und wir gehen einmal davon aus, dass er dort nicht per Hand, sondern irgendwie aus der Ferne installiert worden ist –, dann ist damit quasi nachgewiesen, dass das System unsicher ist. Das heißt, da ist quasi schon einmal ein Tor auf. Wenn man dann gleichzeitig noch den Trojaner kompromittiert hat, hat man noch mal ein weiteres potenzielles Einfallstor dadurch geschaffen. Wie verwertbar macht das eigentlich so zustande gekommene Ermittlungsergebnisse? Was ist denn dann – jetzt mal ganz konkret gefragt wird –, wenn jetzt jemand sagt: Na ja, da wurde jetzt dieses Telefongespräch aufgezeichnet, aber bei dem Anbieter – – Es gibt dokumentierte Fälle, in denen anscheinend solche Dinge untergeschoben wurden. – Er sagt also: Ich habe dieses Telefongespräch nicht geführt, und mein Rechner war offensichtlich kompromittiert.

Die zweite rechtliche Frage: Sie haben schon die Möglichkeit angesprochen, dass man nicht eindeutig bestimmen kann, wer jetzt eigentlich am Rechner aktiv ist, wer gerade den Rechner benutzt, den man kompromittiert hat. Hat man bei der Kommunikationsüberwachung auch – – Wobei man da natürlich noch sagen könnte, gut, da hört man sofort an der Stimme, dass das jemand anderes ist. Das ist jetzt bei der elektronischen Kommunikation, wenn es keine Stimmenkommunikation, sondern verschlüsselte E-Mails oder was auch immer sind, natürlich nicht so einfach der Fall – oder gar, wenn man den Eingriff noch weiter führt. Jetzt gibt es bei der angedachten Quellen-Telekommunikationsüberwachung noch einen zusätzlichen Punkt, und zwar im Gegensatz zur Hausdurchsuchung, wo man weiß, wessen Wohnung man untersucht und wo die ist, und im Gegensatz zur TKÜ, wo man immer noch weiß, wo sich dieser Anschluss befindet, ist bei der Quellen-Telekommunikationsüberwachung, wenn man das aus der Ferne macht, gar nicht klar, wo sich der Rechner befindet. Der könnte sich theoretisch auch irgendwo im Ausland befinden. Theoretisch könnte der auch von jemandem genutzt werden, der nicht nur nicht Zielperson ist, sondern auch gar nicht deutscher Staatsbürger. Ergeben sich daraus nicht auch noch mal zusätzliche rechtliche Komplikationen, wenn man gar nicht feststellen kann, ob das, was man gerade macht, wirklich ein Einsatz im Inland ist, oder ob man da nicht gerade etwas macht, was eigentlich geheimdienstliche Tätigkeit im Ausland ist?

Noch eine Frage an Sie, weil Sie gerade da sind und weil wir dazu in der Vergangenheit auch schon widersprüchliche Informationen gehört haben. Mich würde noch mal ganz konkret interessieren, wer genau – Sie haben ja Software zur Quellen-Telekommunikationsüberwachung – da jetzt der Hersteller ist, was genau das für ein Produkt ist und was genau das eigentlich leistet.

Vorsitzender Alexander Morlang: Herr Lauer!

Christopher Lauer (PIRATEN): Ich hatte noch ein paar ergänzende Fragen. Herr Rieger! Herr Schröder! Können Sie in einfachen Worten das Halteproblem in der Informatik erläutern und noch mal in einfachen Worten erklären, welche Bedeutung das für diesen Trojaner hätte? An die beiden Herren von der Technik: Habe ich Sie dahin gehend richtig verstanden – jetzt mal an einem plastischen Beispiel: Wir finden auf dem Computer von Herrn Dregger – –

Vorsitzender Alexander Morlang: Entschuldigen Sie, Herr Lauer! Fassen Sie sich sehr kurz. Wir haben eigentlich Fraktionsrunden, und das ist nicht zulässig. Beenden Sie bitte schnell!

Christopher Lauer (PIRATEN): Ich habe aber leider noch Fragen, die beantwortet werden müssen. Wir finden irgendwelches Material z. B. auf dem Rechner von Herrn Dregger, und dann war es im Zweifelsfall gar nicht Herr Dregger, aber er wird angezeigt. So etwas wäre dann mit einer solchen Software auch möglich.

Herr Buermeyer! Habe ich Sie richtig verstanden, dass Sie das gut finden mit einer Rechtsgrundlage? Aber – Sie sind ja, glaube ich, auch Richter – vor dem Hintergrund, was hier gesagt worden ist, was die Technik angeht: Würden Sie denn dann die Benutzung eines solchen Trojaners anordnen, wenn es jetzt eine Rechtsgrundlage gibt – angesichts der technischen Bedenken?

Herr Rieger oder Herr Schröder! Vielleicht könnten Sie noch mal erklären, was bei der Bundespolizei mit diesem Petra-System (phonet.) passiert ist und welche Rolle dort ein Trojaner gespielt hat.

Dann habe ich an Herrn Reinhard eine Frage: Habe ich das jetzt richtig verstanden, dass Sie selbst eine Software entwickeln bzw. ist das gang und gäbe im Senat, dass man ohne eine Rechtsgrundlage für eine bestimmte Maßnahme auch bei der Berliner Polizei sich schon mal Dinge anschafft und prüft, so nach dem Motto: Wir wissen ja nicht, ob bestimmte Waffen im Einsatz bei der Polizei demnächst legal werden, aber wir kaufen sie uns einfach schon mal an und prüfen schon mal auf dem Schießstand, ob das gut funktioniert. – Auch von der Systematik her verstehe ich das nicht ganz. Vielleicht können Sie als jemand, der sich mit diesen technischen Sachverhalten beschäftigt, noch einmal erklären, wie das Wettrüsten zwischen Strafverfolgungsbehörden und organisierter Kriminalität funktioniert. Was denken Sie, wer wird denn da getroffen? Einfaches Beispiel: Telefoniert die Russenmafia in Berlin mit Telefonen, die sie so im T-Punkt kaufen können, über einen Vertrag der Deutschen Telekom, oder wie muss ich mir das vorstellen? Wer wird da überhaupt gefunden?

Herr Dregger! Sie hatten noch das interessante Beispiel gebracht, dass auch die Dienstwaffe missbraucht werden kann, um in Ihrem Bild zu bleiben. Der Staatstrojaner ist so etwas wie

eine Dienstwaffe, die ständig feuert, und Sie können am Ende noch nicht einmal nachvollziehen, wer den Schuss abgegeben hat. Das ist durchaus problematisch, und natürlich müssen wir auch darüber sprechen, wenn Sie hier die Frage stellen: Diskreditiert das ein Unternehmen, wenn es auch für Diktaturen Überwachungssoftware liefert? – Natürlich müssen wir auch mal die Frage stellen, inwieweit das deutschen Unternehmen gut zu Gesichte steht, also Siemens und anderen, wenn die an solche Staaten Sachen liefern. Das ist doch ganz klar. Darüber diskutiere ich auch gerne mit Ihnen. Ich finde es auch schwierig, hier anzubringen, ob es irgendwelche Beispiele gibt, in denen das irgendwie mal etwas gebracht hat oder so, denn das haben wir als Piratenfraktion auch klargemacht: Wir halten es für nicht möglich und auch nicht erstrebenswert.

Vorsitzender Alexander Morlang: Das war nicht kurz. – Das heißt, ich müsste jetzt noch Herrn Taş und Herrn Behrendt dranlassen. Kriegen Sie das in zwei Minuten hin? Ich hätte gern auch noch Antworten. Fragen haben wir jetzt. – [Zuruf von Sven Kohlmeier (SPD)] – Okay! Wir machen jetzt eine Antwortrunde, wenn das in Ordnung ist, Herr Behrendt, sonst ufert es hier aus, und dann gucken wir, ob wir noch eine kurze Fragerunde hinbekommen. Ich finde den Vorschlag von Herrn Kohlmeier sehr gut. – Ich höre keinen Widerspruch. Dann kommen wir zur ersten Antwortrunde. – Herr Buermeyer!

Ulf Buermeyer (Richter am Landgericht): Vielen Dank! – Buermeyer ist mein Name. Das ist ein westfälisches Dehnungs-E, das ist kein Ü. Das kann man aber nicht wissen. – Zum Stichwort „Regelung“: Um gleich einmal diese leicht angedeutete Kritik aus der Piratenfraktion vorwegzunehmen, ich möchte nicht sagen, dass wir eine solche Regelung brauchen. Ich sage nur, wenn wir so etwas durchführen wollen, was eine rechtspolitische Frage ist, dann brauchen wir jedenfalls eine Regelung. Wir sind in dieser konkreten Situation in der etwas misslichen Lage, also wir quasi als Rechtsstaat, dass es natürlich den einen oder anderen richterlichen Kollegen gegeben hat, der ohne Rechtsgrundlage so etwas angeordnet hat, was nach meinem richterlichen Ethos ein ziemliches Unding ist – offen gesagt. Es ist aber passiert, und insofern brauchen wir ein solches Gesetz auch deswegen, damit wir den Kolleginnen und Kollegen einen noch etwas klareren Rechtsrahmen an die Hand geben, damit da niemand auf Abwege kommt.

Weiter zum Stichwort „Regelung“: Ich würde gerne noch zwei Sätze zu der Frage sagen: Wie ist das eigentlich ermittlungstaktisch? Was bringt denn das eigentlich? – Meine persönliche Auffassung ist, dass die ermittlungstaktischen Chancen, die in der Quellen-TKÜ gesehen werden, bei weitem überschätzt werden. Die Begründung dafür ist ganz einfach. Wenn man eine solche Software erfolgversprechend einsetzen will, dann muss man die auf jedes zu überwachende System gezielt abstimmen. Natürlich – das haben wir gehört – ist es rechtsstaatlich außerdem erforderlich, jede einzelne abgestimmte Software auch wieder im Einzelnen darauf zu prüfen, dass sie die rechtlichen Spielregeln einhält.

Computer heißt heutzutage nicht mehr nur das, was ich hier stehen habe oder was andere auf dem Tisch stehen haben, Windows-Rechner und Mac-Rechner. Computer sind auch die kleinen Geräte, die wir hier in der Hand haben. Auf diesen Smartphones kann man nämlich auch z. B. Skype oder Mumble, was die Piraten gerne einsetzen, was so eine Art Skype ist, nur Open Source, laufen lassen. Das heißt also, wenn man von Quellen-TKÜ redet, reden wir nicht von Windows und Mac, sondern wir reden praktisch vor allem davon, Trojaner auf dem I-Phone einzuspielen. Da muss man natürlich ganz klar sagen: Das ist nicht unmöglich. Es

gibt einen Schwarzmarkt für Sicherheitslücken in I-Phones. Da werden Hunderttausende von Dollar gezahlt – für Geheimdienste. Ich halte es aber für eine ziemlich naive Vorstellung, davon auszugehen, dass das LKA Berlin 100 000 Euro für eine Sicherheitslücke im I-Phone auf den Tisch legt, nur um irgendwelche Leute von der Russenmafia abhören zu können. Das halte ich für vollkommen illusorisch. Und diese Sicherheitslücken verbrennen natürlich auch. Sobald die bekannt geworden sind, schließt Apple die. Apple hat ein großes Interesse daran, dass das System dicht ist, weil sie ihre Software verkaufen wollen, und wenn die I-Phones anloggt, kann man die Software kopieren. Das will Apple nicht. Kurz und gut, das war nur ein Beispiel.

Das ist eine Plattform. Wir haben aber auch noch Blackberry. Wir haben Android. Es gibt neuerdings Windows-Phone. Quellen-TKÜ ist nicht *eine* Maßnahme. Das ist nicht der eine Schuss, der das Problem löst. Quellen-TKÜ wäre, wenn man das wirklich will, ein dauernder Prozess, ein ständiges Hase-und-Igel-Laufen zwischen Sicherheitsbehörden und Kriminellen. Da muss man ganz ehrlich sagen: Diesen Wettlauf werden wir verlieren. So einfach ist das. Diese Mittel haben wir nicht, das wirtschaftlich überhaupt zu bestreiten. Insofern glaube ich, dass wir – das hatte ich eben noch nicht so deutlich gemacht – hier in weiten Teilen über theoretische Fragen reden. Wir werden es ohnehin nicht zielführend einsetzen können, jedenfalls nicht gegen halbwegs professionelle Kriminelle. Wir werden vielleicht den Ebay-Betrüger kriegen, aber wir werden sicherlich nicht die Russenmafia damit kriegen. Das ist meine feste Überzeugung. Die Techniker können sicherlich noch etwas mehr dazu sagen, aber ich glaube, wir machen uns hier auch ein Stück weit etwas vor.

Weil das so ist und weil das so komplex ist, glaube ich, dass der Koalitionsantrag zwar funktionieren kann, zum Stichwort „Quellen-TKÜ“, aber vor allem deswegen, weil er zu dieser Frage der verfahrensmäßigen Vorgaben nicht furchtbar präzise ist. Es steht, wenn man ehrlich ist, vor allem eine Zielvorgabe drin, quasi ein Verfahren zu etablieren, das sicherstellt, dass die Vorgaben aus Karlsruhe eingehalten werden. Das kann natürlich funktionieren, aber das ist komplex, und ich glaube, wir bräuchten da eine Kaskade aus gesetzlicher Regelung, Verordnungsermächtigung und darauf gestützt noch technischer Richtlinie, die diese Dinge dann quasi für die Praxis durchdekliniert. Das wird extrem komplex, und, wie gesagt, wenn man ehrlich ist, wird die Quellen-TKÜ ohnehin zu teuer für den Standardeinsatz, jedenfalls, wenn man das rechtsstaatlich sauber regeln will.

Deswegen wäre meine rechtspolitische Forderung – das ist Rechtspolitik, also eigentlich nicht mein Feld, aber ich wurde danach gefragt, was ich für Regelungen befürworten würde –, dass man nur die Online-Durchsuchung regelt. Dann hat man nämlich zum einen nur das Kriminalitätsfeld im Blick, das es quasi verdient, also echte Schwerkriminalität. Man hat zum Zweiten das Problem Quellen-TKÜ/Online-Durchsuchung nicht mehr, und man kann sich zum Dritten, weil es dann vergleichsweise wenige Anwendungsfälle sind, darauf konzentrieren, dass die auch wirklich rechtsstaatlich sauber durchgeführt werden. Wenn es jetzt wirklich z. B. um Terrorismus geht oder um Fälle von Leben und Tod, dann stellen sich die rechtspolitischen Fragen auch nicht mehr so gravierend, wie sie das bei der Quellen-TKÜ tun. Das ist meine persönliche Auffassung.

Um auf Ihre Frage zu antworten: Würde ich das anordnen? – Ich würde das als Richter natürlich nur dann anordnen, wenn es zum einen eine Rechtsgrundlage gibt. Gegenwärtig würde ich auf jeden Fall nein sagen, und ich denke, dass das auch die Mehrheit der Kolleginnen und

Kollegen so sieht. Ich habe jetzt noch keine Fortbildung am Landgericht gemacht, aber vielleicht sollte man das mal machen. Das ist das eine.

Gegenwärtig würde ich es nicht tun, und wenn es eine Regelung gäbe, dann würde ich natürlich diese Regelung anwenden. Das versteht sich völlig von selber. Der Gesetzgeber entscheidet, was passiert. Nur würde ich mir diese Regel natürlich sehr genau angucken und auf die einzelne Maßnahme schauen und mir dann schon ein eigenes Urteil bilden, ob in den Spielregeln dieser Maßnahme auch die Vorgaben aus Karlsruhe wirklich eingehalten worden sind. Ich teile da letztlich die Auffassung der Kollegen von der Technik, wie es eben so schön hieß. Ich glaube nicht, dass es gegenwärtig eine Möglichkeit gibt, eine Quellen-TKÜ-Software zu programmieren, die diesen Anforderungen entspricht.

Ganz banal: Ich muss schon wissen, welche Software auf dem System eigentlich läuft. Damit muss ich Daten aus dem System erheben, die nicht laufende Kommunikation sind. Quasi allein, um das Ziel ins Visier nehmen zu können, um zu wissen: Läuft Skype in der Version 4. irgendwas? –, muss ich schon Dinge erheben, die mir überhaupt nur eine Online-Durchsuchung sagt. Das heißt, ich habe im Grunde so eine Art Deadlock-Situation, wie man als Programmierer sagt. Es beißt sich quasi die Katze in den Schwanz. Ich kann zurzeit legal, nach meiner Wertung jedenfalls, keine Quellen-TKÜ durchführen.

Was ich da gesagt habe, ist also aus zwei Gründen abstrakt. Zum einen können wir es technisch nicht – ich weiß nicht, ob es jemals gehen wird –, und zum anderen haben wir technisch ein großes Problem, was die Durchführung angeht. Wir können also technisch nicht die Regeln einhalten, und wir haben technisch auch schon ein Problem, überhaupt in die Systeme reinzukommen.

Stichwort „Verwertbarkeit“: Da, muss ich offen sagen, würde ich etwas von der Sicht der Techniker abweichen wollen. Ich sehe natürlich die leichte Manipulierbarkeit von Beweismitteln in diesem Kontext. Das muss man so deutlich sagen. Auf der anderen Seite, wenn ich mir das mal aus der Perspektive der Relevanz angucke, bin ich als Richter ohnehin darauf angewiesen, der Polizei zu vertrauen. Das muss man so deutlich sagen. Ich kann die Arbeit der Polizei nur zu einem ganz geringen Teil wirklich überprüfen. Ich bin darauf angewiesen, dass mir ein Polizeibeamter als Zeuge die Wahrheit sagt. Und wenn er das nicht macht, habe ich ein Problem. Dann werde ich möglicherweise auch ein Fehlurteil sprechen, aber meine persönliche Erfahrung ist, dass die Polizei in aller, aller Regel ihre Arbeit ordentlich macht, auch die Berliner Polizei, insofern habe ich auch keinen Anlass zu Misstrauen.

Vor diesem Hintergrund möchte ich sagen: Dieses Missbrauchsargument sehe nicht. Es zieht aus der technischen Perspektive, aber aus der Richterperspektive zieht es deswegen nicht, weil es quasi für jede Ermittlung gleich gilt. Ich muss auch bei einer Hausdurchsuchung dem Beamten glauben, dass das stimmt, dass er dieses Päckchen mit dem weißen Pulver da gefunden hat und dass das nicht aus der Asservatenkammer stammt. Wenn ich dem nicht glauben kann, dann habe ich ohnehin als Richter ein großes Problem. – Das vielleicht von meiner Seite. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Herr Dr. Nöding!

Dr. Toralf Nöding (Vereinigung Berliner Strafverteidiger): Ich versuche es, ganz kurz zu mache, obwohl ich glaube, dass ich hier das größte Package abbekommen habe. Zunächst, ich glaube, ich bin missverstanden worden. Die Strafverteidigervereinigung findet neue Ermittlungsbefugnisse eigentlich nie gut, vor allen Dingen dann nicht, wenn sie eingriffsintensiv sind. Ich wollte nur sagen, wir finden das gut, dass hier klar gesagt wird: Es braucht eine Rechtsgrundlage, es gibt keine, und im Moment machen wir das nicht. – Das ist viel mehr, als in vielen anderen Bundesländern gesagt wird, und das finden wir sehr rechtsstaatlich. Das wollte ich einfach unterstreichen.

Auf die Frage von den Piraten: Das hätte jetzt ein bisschen den Spaß genommen. Natürlich, wenn es technisch nicht geht, kann man es nicht machen. Das ist eine ganz klare Antwort. Das Bundesverfassungsgericht hat gesagt, dass das nur unter den Voraussetzungen zu machen ist, und wenn das technisch nicht durchzusetzen ist, dann darf es das nicht geben. Das ist ganz klar unsere Position.

Ich möchte noch etwas zur praktischen Notwendigkeit sagen. Ich habe den Eindruck, die Ermittlungsbehörden kommen ganz gut auch ohne die Quellen-TKÜ zurecht. Auch im Bereich der organisierten Kriminalität wird dann schnell mal eine PKW-Innenraumüberwachung geschaltet, um zumindest eine Gesprächsseite mitzubekommen, oder man reitet halt alle zwei Wochen in die Wohnung ein, nimmt jedes Mal den PC mit und guckt, was da für eine Kommunikation lief. Da gibt es schon Möglichkeiten.

Zur Regelungstechnik – das war der Kollege von der SPD, glaube ich: Da finde ich den Anfang so ein bisschen blutleer. Der sagt ja nur, was im Prinzip gehen soll und wie das technisch ausgestaltet werden soll. Und wenn man sagt, dass soll sich an § 20l BKA-Gesetz orientieren, dann sagt das nichts für den repressiven, also den Strafverfolgungsbereich. Denn dann haben wir immer noch keine tatbestandlichen Voraussetzungen. Wann soll das gemacht werden dürfen? Die StPO verwendet eine Katalogtatentechnik. Das heißt, sie listet Straftaten auf, bei deren Verdacht das gemacht werden darf. Da muss man sich dann sozusagen überlegen: Wie schwer müssen diese Straftaten sein? – Und da sage ich, da sagen wir: Das muss Schwerstkriminalität sein, weil der Eingriff viel gewichtiger ist als bei einer normalen TKÜ.

Die Subsidiarität nach der praktischen Handhabung: Da muss ich einfach sagen, eine Subsidiaritätsklausel haben wir in fast jeder strafprozessualen Eingriffsermächtigung und übrigens auch im BKA-Gesetz. Da heißt es ja auch – ich darf das kurz vorlesen; sozusagen bei der Vorbildregelung ist die auch drin –, dass es nur dann geht, wenn es notwendig ist,

> um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

Das ist genau die Subsidiaritätsklausel. Das heißt einfach, auch das BKA-Gesetz, die Vorbildregelung sieht vor, man soll erst gucken: Geht es weniger eingriffsintensiv? – Und warum wir darauf hinweisen, dass wir das wichtig finden, ist – jetzt wird es leider wieder juristisch: In § 100a StPO, also in der Regelung für die derzeit mögliche Telekommunikationsüberwachung, ist auch so eine Subsidiaritätsklausel drin. Da steht drin, dass es dann zulässig ist,

> wenn die Erforschung des Sachverhalts ... auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Das heißt, der Gesetzgeber wollte, dass man sich überlegt, bevor man eine normale TKÜ anordnet, ob es eingriffschwächere Maßnahmen gibt. Da ist einfach die Erfahrung aus der Praxis – da wird mir Herr Buermeyer recht geben –: Der Ermittlungsrichter schreibt in jeden TKÜ-Beschluss einen Satz hinein. Da steht immer drin:

> Die Erforschung des Sachverhalts auf andere Weise wäre wesentlich erschwert oder aussichtslos.

Er schreibt das, ohne da irgendetwas zu prüfen. Das ist dann einfach eine leere Regelung. Wir sollten bei so einer eingriffsintensiven Maßnahme keine leeren Regelungen schaffen. Deshalb muss man, finden wir, die Richter zwingen, das konkret zu begründen.

Jetzt hatten wir noch die Frage, wie das mit Dritten ist. – Ich kann nur das unterstreichen, was hier gesagt wurde. Es ist schon ein Unterschied, ob ich ein Handy habe, denn das wird im Regelfall immer nur von einem genutzt – bei einer normalen TKÜ. Wenn wir aber einen PC haben, der in einer Wohnung steht, dann ist das Potenzial für den Zugriff Dritter, also Nichtbetroffener, von Nichtzielpersonen, viel größer. Deshalb finden wir, dass wir da eine zusätzliche Prüfung, eine zusätzliche Voraussetzung brauchen. – Wenn ich nicht vergessen habe, etwas aufzuschreiben, dann bin ich mit meinen Fragen durch. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank, Herr Nöding! – Als Nächster Herr Rieger! Sie haben das Wort!

Frank Rieger (Chaos Computer Club Berlin): Ich fange gleich mit der Frage von Herrn Kohlmeier an: Ist es möglich, technisch erst eine normale TKÜ und dann eine Quellen-TKÜ durchzuführen? – Ich habe nur indirekt damit zu tun, nämlich wenn uns Anwälte fragen, insbesondere wenn es komische Anomalitäten in TKÜ-Maßnahmen gibt, die sie in der Akteneinsicht sehen. Da ist es in der Regel so, dass typischerweise da schon immer eine Eskalation drin ist, also wenn aus einer TKÜ z. B. bestimmte Erkenntnisse nicht gewonnen werden, erst dann wird z. B. eine PKW-Innenraumüberwachung beantragt oder andere Observationsmaßnahmen oder sonstige Mittel. Das heißt, wir haben ohnehin schon diese Steigerungen drin, dass immer erst versucht wird, einen vermeintlich minderschweren Eingriff, nämlich eine TKÜ zu wählen, und dann erst den nächst schwereren Eingriff.

Bei einer Quellen-TKÜ ist es so: Sie müssen zwingend überhaupt erst einmal Erkenntnisse darüber gewinnen: Was nimmt er denn eigentlich für Kommunikationsmittel? Benutzt er Skype? Welche Chatformen benutzt er? Welche Telefonieformen benutzt er? Ohne die Erkenntnisse aus der TKÜ haben Sie die überhaupt nicht. Sie haben nicht einmal eine Chance, da reinzukommen. Subsidiarität ist zumindest aus meiner Sicht, wenn Sie da überhaupt eine solche Quellen-TKÜ zulassen wollen, nahezu selbstverständlich, schon aus technischer Sicht.

Zu der Frage, die von verschiedenen Seiten kam, was die Belege für das nichtrechtmäßige Arbeiten der Zuliefererfirmen und der Behörden betrifft. – Was die Berliner Behörden angeht, habe ich keine Erkenntnisse. Das ist nicht so mein Hobby. Was diese Firmen angeht, gibt es einige davon. Alle diese Firmen, die in diesem Markt aktiv sind, sind bereits in Skandale verwickelt gewesen – z. B. die Firma DigiTask. Der Gründer dieser Firma ist jemand gewesen, der wegen Bestechung von Zollbehörden verurteilt wurde, damit sein Telekommunikationsüberwachungsequipment angekauft wird. Das fällt ganz deutlich unter sowohl Versagen der

Behörden als auch der Firma. Wenn Sie da ein bisschen in der Presse lesen, einfach nur die Namen dieser Firmen, dann finden Sie eigentlich zu allen diesen Firmen Dinge, die Sie lieber nicht lesen wollen, übrigens auch zur Mutterfirma der Firma Syborg, die in Berlin das TKÜ-Equipment liefert, die eine israelische Firma ist und in Holland Merkwürdigkeiten hatte.

Was das Thema „Lieferung an Diktaturen“ angeht, das ist eine moralische Frage. Ich weiß nicht, ob die in der Politik etwas zu suchen hat. Ich persönlich arbeite nicht mit Firmen zusammen, die so etwas tun, also Überwachungsmittel an Unrechtsregime ausliefern. Wir machen als Chaos Computer Club Schulungen für Oppositionelle aus diesen Ländern. Wir haben mit den Leuten zu tun, die Opfer von Folterungen geworden sind – durch Telekommunikationsüberwachungsmaßnahmen, die mit solcher Software passiert ist. Ob man dieses Blut an den Händen und in unserem Haushalt haben will, muss man selber entscheiden. Ich als Bürger würde das nicht so schön finden.

Kann man eine Prüfung durch externe Auditoren als Einsatzgrundlage heranziehen? – Diese Frage wurde auch schon in der Stellungnahme vom LKA ganz klar benannt. Es gibt einen mittlerweile viele Monate währenden Prozess, überhaupt erst einmal zu definieren, was denn diese Software können und dürfen soll und wie man denn überprüfen soll, dass dem so ist. Wir haben die bizarre Situation, dass das Bundesamt für Sicherheit in der Informationstechnik eigentlich zuständig ist für die Sicherheit in der Informationstechnik, also nicht für die Unsicherheit in der Informationstechnik, wie es eine Malware – so ein Trojaner – sein würde. Die haben gesagt: Na ja, wir delegieren das Problem mal an externe Dienstleister –, und haben ein paar Firmen zertifiziert, die diese Prüfungen durchführen sollen, weil das BSI selbst eigentlich auch nichts damit zu tun haben will, da sie ganz genau wissen, dass man sich da nur die Finger verbrennen kann. Denn es ist ganz klar: Das erste Mal, wenn eine solche Software zum Beispiel in unsere Hände fällt und analysiert wird, wird sich irgendetwas darin finden. Das ist quasi ein Naturgesetz, weil solche Leute natürlich auch schlampig programmieren.

Die Software in diesen Trojanern ist zwangsweise von schlechterer Qualität als die industrieübliche Software, weil sie sich in einem Umfeld bewegen muss, das ihr feindlich gegenübergestellt ist. Wir haben Antivirensoftware auf solchen PC. Der Nutzer möchte nicht, dass diese Software darauf läuft. Demzufolge müssen sie dort Programmiertechniken anwenden, die ein bisschen „fishy“ sind. Demzufolge ist vollkommen klar: Wer auch immer eine solche Software freistempelt, wird hinterher der Sündenbock sein, weil klar ist, dass er nicht alles darin finden kann. Selbst die vollständige Analyse einer solchen Software, die Monate dauert, wird niemals alle Möglichkeiten des Missbrauchs dieser Software aufdecken können – auch nicht durch Dritte.

Damit kommen wir zu dem Problempunkt der Verwertbarkeit: Was wir bei dem DigiTask-Trojaner gesehen haben, das ist eine massive Schlamperei, ein Nichtnachdenken und schlechtes Design. Es ist gut, dass das BKA jetzt offensichtlich etwas mehr Zeit dafür verwendet, aber klar ist auch: Wenn ein solcher Computer erst einmal infiltriert ist, dann sind da offensichtlich Sicherheitslücken vorhanden. Das heißt: Wenn ich der Betroffene einer solchen Maßnahme wäre, würde ich mich immer auf den Standpunkt stellen und sagen: Also, die Daten, die Sie auf meiner Festplatte gefunden haben, sind nicht von mir. Beweisen Sie mir mal, dass die von mir sind! Mein Computer ist offensichtlich nachweisbar von staatlichen Stellen infiltriert worden – sogar der Staat, der für seine IT-Kompetenz nicht besonders berühmt ist, hat es geschafft, meinen Computer zu infiltrieren –, dann kann ich mich als Betroffener wohl auf den Standpunkt stellen und sagen, dann hat es offenbar auch jemand anderes geschafft. – Das heißt, über die Verwertbarkeit von Daten von solchen Festplatten von solchen Maßnahmen Betroffener kann man sich wahrscheinlich vor Gericht trefflich streiten.

Was die Unterscheidung zwischen Quellen-TKÜ und Online-Durchsuchung angeht, das haben wir schon ausgeführt. De facto ist eine wirkliche Unterscheidung nicht möglich. Deswegen ist der Hinweis von Herrn Buermeyer sehr sinnvoll, nämlich zu sagen: Okay! Wenn, dann regelt doch bitte einfach die Online-Durchsuchung ordentlich, sodass dann, wenn es wirklich notwendig ist, wie zum Beispiel beim großen Lauschangriff, solche Maßnahmen einzusetzen, dafür eine vernünftige Regelung da ist, die dann auch als Quellen-TKÜ-Regelung benutzt werden kann! – Das halte ich für sehr sinnvoll.

Was die Versionen und Zeiträume angeht – DigiTask ist ein Beispiel dafür –, können wir folgern: Die haben im Abstand von einigen Wochen jeweils neue Versionen releast, die niemand

zertifiziert hat. Also, die wurden nur angeguckt, dass das Nutzer- und E-Face (phonet.) genauso aussieht. Wenn wir uns angucken, wie die Software-Updatefolgen bei den Betriebssystemen für Mobiltelefone und Computer sind, haben wir ebenfalls einen Abstand von zwischen vier und sechs Wochen, in denen es neue Versionen gibt, die dann im Zweifel dafür sorgen, dass der jeweilige Trojaner nicht mehr funktioniert.

Wenn Sie die Statistiken angucken, die von den Landeskriminalämtern über den Einsatz von Online-Durchsuchungsmaßnahmen und Quellen-TKÜ-Trojanern veröffentlicht wurden, bevor es diese Diskussion gab, dann stellt sich heraus, dass in ungefähr der Hälfte der Fälle überhaupt gar keine erfolgreiche Installation stattfand oder dass diese Installation nach kürzester Zeit nicht mehr funktioniert hat, weil IT-Sicherheitsmaßnahmen seitens der Betroffenen getroffen wurden, die eine solche Installation invalidiert haben. Daraus sieht man schon: Der Aufwand ist im Einzelfall erheblich. Das heißt, die Idee, man könne eine Quellen-TKÜ, wenn man sie denn zulassen will, genauso verwenden wie eine normale TKÜ, ist technisch tatsächlich nicht realistisch, sondern es handelt sich dabei um etwas, das einen relativ hohen Aufwand und insbesondere, wenn man es rechtsstaatlich durchführen will, einen hohen Zertifizierungsaufwand hat.

Die Frage nach der Prüfbarkeit, wie ich also sicherstellen kann, dass eine solche Software nur das tut, was versprochen wurde, und nicht noch irgendwelche anderen Dinge tut, ist eines der grundlegenden Probleme in der Informatik. – Herr Schröder kann gleich noch ein bisschen mehr dazu sagen. – Sie können immer gut nachweisen, dass eine Software bestimmte Funktionen hat, aber Sie können quasi nicht nachweisen, dass eine Software bestimmte Funktionen nicht hat. Es gibt – genauer gesagt – auch Wettbewerbe in der Informatik, Underhanded Contests, in denen ausprobiert wird: Wie kann man Funktionen in Programmen so verstecken, dass sie niemand findet, und zwar auch nicht die anderen Informatiker, die dafür ausgebildet und darin Spezialisten sind? Es gewinnt dann derjenige, der den besten Weg findet, eine Funktion darin zu verstecken, und genau solche Techniken kann man natürlich da auch verwenden.

Übrigens werden genau solche Techniken von Trojaner-Programmierfirmen verwendet, um zum Beispiel Antivirussoftware auszutricksen. Das heißt, die sind Experten darin, Sachen in Trojaner-Software zu verstecken, die nicht gefunden werden wollen. Es handelt sich also nicht um eine normale Software wie Word oder so, sondern das ist de facto genau dasselbe Zeug, das die Russenmafia verwendet, um Computer zu infiltrieren. Da sind Leute am Werk, die sehr tricky programmieren und die Experten darin sind, Sachen in Software zu verstecken, die nicht gefunden werden sollen.

Die Frage nach dem Problem, das die Bundespolizei hatte, stellt sich natürlich auch. – Die Bundespolizei hatte ein Problem mit einem zentralen System, auf dem GPS-Logger-Daten für eine Lokationsüberwachung gespeichert wurden. Dieses System wurde ihnen von ein paar Kiddies aufgemacht, die dort nicht einmal besonders viel Aufwand reinstecken mussten. – [Zuruf von Christopher Lauer (PIRATEN)] – Entschuldigung! Die wurden ihnen von technisch interessierten Jugendlichen aufgemacht, die dort keinen besonders hohen technischen Aufwand reinstecken mussten. Es gab dann einen Zugang zu den Lokationsdaten von mehreren Hundert Ermittlungsverfahren, und aus diesem Grund mussten diese GPS-Logger abgeschaltet werden. Wie ich hörte, waren einige dieser Fälle für einige LKA tatsächlich ziemlich dramatisch. Das weist deutlich darauf hin, dass es ein realistisches und nachgewiesenes Miss-

brauchspotenzial durch Dritte für die Infrastruktur solcher Ermittlungssysteme gibt. Da muss man noch nicht einmal einen bösen Willen unterstellen. Wie gesagt: Ich unterstelle unserer Polizei in der Regel auch keinen bösen Willen, aber klar ist: Technische Systeme sind komplex. Da werden Fehler gemacht, wovon man einfach mal ausgehen muss. – Damit bin ich durch. – Danke!

Vorsitzender Alexander Morlang: Vielen Dank! – Ich möchte darauf hinweisen, dass Herr Statzkowski um Viertel nach gehen muss. Das heißt, wenn wir noch die Stellungnahme des Senats hören wollen, dann müssten Sie sich kurzfassen – es liegt an Ihnen. – Bitte, Herr Schröder!

Thorsten Schröder (modzero AG): Ich versuche es. – Auch wenn die Zeit knapp ist, möchte ich kurz noch Herrn Buermeyer ergänzen, der nämlich etwas ganz Wichtiges sagte, gerade, wenn es um Skype als Beispiel geht: Diese Skype-Kommunikation läuft verschlüsselt ab. Es ist nicht unbedingt wirklich klar, auf welchem Endgerät der Skype-Client einer beschuldigten Person letztlich läuft. Das kann ein PC sein, ein Mac, ein I-Phone oder auch ein Skype-fähiges DECT-Gerät. Ich vermute, dass es zumindest für Letzteres keinen Trojaner geben wird, der dann eine Überwachung zulässt. Von daher ist sowieso anzuzweifeln, ob die Ergebnisse, die aus einer solchen Quellen-TKÜ gewonnen werden können, überhaupt sinnvoll sind.

Zu der Frage, ob es sich möglicherweise um ein Missverständnis handelte, als ich den Vergleich mit der Dienstwaffe einbrachte: Ich habe diesen Vergleich eingebracht, weil ich ganz klar sehe, dass diese digitale Waffe sehr viel leichter verschleiert werden kann. Das heißt, die Hemmschwelle ist möglicherweise sehr viel niedriger – ähnlich wie bei den Online-Kriminalitätsdelikten. Für einen Jugendlichen, der irgendwie versuchen möchte, schnell an ein bisschen Geld zu kommen, ist es einfacher, irgendeine Straftat über das Internet zu begehen, weil er da auch seine Spuren verschleiern kann. Der wird vermutlich nicht so ohne Weiteres auf die Straße gehen und einer Person die Handtasche klauen. Es geht mir vor allen Dingen darum, dass die Spuren bei dieser digitalen Geschichte einfach sehr viel besser verwischt werden können.

Zu der Frage, wie schwierig es ist, ein Modul nachzuladen, oder ob Dritte in der Lage sind, bei einem Staatstrojaner ein Modul nachzuladen: Wenn es die Möglichkeit gibt, Module nachzuladen, dann ist die Frage nicht, ob es möglich ist, sondern wann jemand, der diese Software analysiert, herausfindet, wie das geht. Im Falle des veröffentlichten Trojaners von DigiTask war im Grunde genommen nach ungefähr ein oder zwei Abenden im Hotel klar, dass es grundsätzlich die Möglichkeit gibt. Die übrige Zeit wurde damit verwendet, dass auch mal zu implementieren. Das kann man natürlich erst dann sagen, wenn man eine solche Software sieht. Man kann die entsprechenden Funktionalitäten verschleiern, was allerdings nichts hilft, wenn da jemand mit genügend Zeit dran sitzt und sich im Detail anguckt, wie diese Schnittstelle gestaltet ist und wie man sie missbrauchen kann.

Bei der Frage nach dem Aufwand einer Prüfung, ob eine Software jetzt einwandfrei ist und genau das tut, was sie tun soll, sollte man sich zunächst einmal über das Ziel klar sein. Das heißt: Suchen wir nach Hintertüren, oder suchen wir nach Fehlern in der Programmierung? Das eine ist mutwillig und das andere ist vielleicht versehentlich geschehen. Wie Herr Rieger schon ausführte, gibt es regelrechte Contests, Wettbewerbe, bei denen versucht werden soll, eine Hintertür einzubauen. Die Implementierung dieser Hintertür sollte einem Source-Code-

Review standhalten. Das heißt, jemand, der einen Source-Code-Review durchführt und nach Hintertüren sucht, soll diese Hintertür übersehen. Wenn er sie dann doch entdeckt, dann sollte das Ganze wie ein dummer Programmierfehler aussehen, der aus reiner Ahnungslosigkeit geschehen ist, und genauso sehe ich das auch. Man kann den Aufwand einer Prüfung nicht klar benennen, weil das auch davon abhängt, wie komplex die Software ist, ob sie im Source-Code vorliegt oder nur als Binary und ob da eine Fiscation, also eine Verschleierung mit drin ist oder nicht.

Die Frage, was das Halteproblem ist, lässt sich im Grunde sehr gut mit einem einfachen Beispiel erklären: Wer eine wissenschaftlich korrekte Definition des Halteproblems haben möchte, kann das gern auf Wikipedia nachschauen, das wird schon korrekt sein. Wenn wir die Möglichkeit eines Nachlademoduls haben und eigentlich nur sicherstellen wollen, ob diese Software terminiert – also bezugnehmend auf das Halteproblem –: Sobald wir die Möglichkeit haben, ein Softwaremodul nachzuladen – während der Laufzeit –, kann ich zum jetzigen Zeitpunkt noch gar keine Aussage darüber treffen, ob dieses Modul, das nachgeladen wird, überhaupt auch terminiert. Ich nenne ein harmloses Beispiel: Ich bin meinetwegen in der Lage, ein Modul nachzuladen, das in einer Endlosschleife hängen bleibt, dann kann man nicht davon sprechen, ob bewiesen werden kann, dass der Gesamttrojaner tatsächlich irgendwann einmal anhält. – Ich glaube, dass ich die an mich gerichteten Fragen insoweit beantwortet habe.

Vorsitzender Alexander Morlang: Vielen Dank! – Das Wort hat Herr Statzkowski.

Staatssekretär Andreas Statzkowski (SenInnSport): Ich gebe das Wort an Herrn Fischer bzw. an Herrn Reinhard weiter.

Manuel Fischer (Berliner Polizei): Mein Name ist Fischer. Ich bin Mitarbeiter im Dezernat von Herrn Reinhard und zuständig für die kommissariatsübergreifende Administration und für das Sicherheitskonzept im Rahmen von Quellen-TKÜ etc. Viele Fragen kann ich leider nicht beantworten, weil tatsächlich etliche Informationen Verschlusssache sind. – [Christopher Lauer (PIRATEN): Super!] –

Zur Abgrenzung zwischen Online-Durchsuchung und Quellen-TKÜ gibt es durchaus funktionierende Mechanismen, sowohl technischer als auch organisatorischer Art, die tatsächlich verhindern, dass aus einer Quellen-TKÜ plötzlich eine Online-Durchsuchung wird. Dazu gehören – wie gesagt – technische und organisatorische Mittel, dazu gehört allerdings auch, dass sich die Firma verpflichtet – das wird auch durch entsprechende Auditierungen festgestellt werden –, dass die Software der SLB, der Standardisierten Leistungsbeschreibung, entspricht und demzufolge entsprechende Module schlicht nicht vorhanden sind. Entsprechende richterliche Beschlüsse definieren – wenn es sie dann geben wird oder wenn es sie schon gegeben hat – sehr genau, was die Ermittlungsbehörden dürfen und was nicht, und daran halten sich die Ermittlungsbehörden in diesem Fall selbstverständlich. – Viele andere Fragen kann ich tatsächlich nicht beantworten, weil das zu sehr ins Detail gehen würde und die ganzen Sachen als Verschlusssache eingestuft sind.

Vorsitzender Alexander Morlang: Vielen Dank! – Das war alles? – Bitte, Herr Reinhard!

Andreas Reinhard (Berliner Polizei): Nein, ich möchte noch zu ein paar grundsätzlichen Dingen oder Fragen, die hier aufgeworfen worden sind, kurz Stellung nehmen. Da war zum einen die Frage: Wie kommt es überhaupt zur Quellen-TKÜ? – Wie schon mehrfach erwähnt wurde – Herr Kohlmeier, das soll jetzt auch keine Belehrung sein: Erst dann, wenn andere strafprozessualen Maßnahmen entweder nicht erfolgreich waren oder darauf hindeuten, dass im Rahmen einer möglichen Quellen-TKÜ weiteren Erkenntnisse, Beweise oder Beweismittel erhoben werden können, wird diese beim Richter beantragt. Das heißt, wir rennen nicht alle zwei Wochen in irgendeine Wohnung und holen dort irgendwelche PC heraus. Das dürfen wir gar nicht ohne richterlichen Beschluss. Wir werden einen Richter, insbesondere den gleichen, auch nicht davon überzeugen, alle zwei Wochen bei dem Gleichen einzufallen.

Zur kriminalistischen Notwendigkeit und der Frage, ob es dafür einen Beleg gibt, dass wir das überhaupt brauchen: Wenn wir grundsätzlich feststellen, dass sich in unserer Zeit, in unserer Gesellschaft und in unserem Umfeld technische Veränderungen ergeben, dann werden diese irgendwann Ausmaße annehmen, wo wir sagen, dass wir bestimmte Lücken nicht zulassen können. Wir werden auch neue Fahrzeuge kaufen, wenn diese jetzt bestimmte Dinge können, die sie vorher nicht konnten, weil wir dem Straftäter genauso schnell hinterherfahren wollen wie vielleicht früher mit dem Pferdewagen. Die Idee, sich dem anzupassen, was grundsätzlich in der Gesellschaft passiert, selbstverständlich im Rahmen der gesetzlichen und verfassungsmäßigen Vorgaben, ist etwas, was einer modernen Polizei normalerweise innewohnt.

Zur Frage, ob wir uns nur um russische OK-Täter kümmern und ein Wettrüsten anfangen oder fortsetzen: Wir sind insofern immer die Verlierer in einem langen Rennen, weil wir uns – abgesehen von der finanziellen Ausstattung – als rechtsstaatliche Institution an rechtsstaatliche Regeln halten und der Straftäter eben nicht. Das sage ich so pauschal, wie es ist. Wir werden nie auf der Höhe der Zeit sein, das ist auch nicht unser Anspruch, aber wir wollen wenigstens den Abstand so kurz und knapp wie möglich halten. Wir entwickeln keine eigene Software – das zu dieser Frage –, sondern haben die, die wir erworben haben, dieser Überprüfung unterzogen, die ich beschrieben habe, sowohl rechtlich als auch technisch, und deshalb setzen wir sie auch nicht ein.

Zu der Frage, ob wir den Hersteller preisgeben, bleibt es bei dem, was wir bisher immer auf alle parlamentarischen Anfragen geantwortet haben: Die unterliegen der Vertraulichkeit. Solange das so ist, werden Sie auch hier nicht erfahren, von wem wir beschafft haben und welche technischen Spezifika – – [Dr. Simon Weiß (PIRATEN): Das ist neu!] – Nein! Wir haben bisher immer gesagt, dass wir nicht sagen, von wem wir die Software haben. – [Christopher Lauer (PIRATEN): Herr Henkel hält sich an die Empfehlung nicht!] – Dann wissen Sie ja, von wem wir es haben. Ich habe damit kein Problem. Ich sage nur: Als Polizei haben wir bisher diese Linie durchgehalten. – Wie wir verdeckt einbringen, ist unterschiedlich. Den Medien können Sie entnehmen, dass vor E-Mails gewarnt wird, die man nicht öffnen soll. Also, die Polizei nutzt alle Möglichkeiten, aber diese werde ich jetzt nicht im Einzelnen aufführen. – Okay, das wäre es von mir.

Vorsitzender Alexander Morlang: Vielen Dank! – Wir haben uns auf eine weitere, sehr kurze Fraktionsrunde geeinigt – zumindest war das der Vorschlag von Herrn Kohlmeier. – Ich höre keinen Widerspruch, dann ist als Nächster Herr Behrendt dran. – Können wir uns auf eine Redezeit von drei bis fünf Minuten einigen – besser weniger –, denn dann haben wir

mehr Zeit für die Antworten. Ich glaube, die sind heute besonders gehaltvoll. Deshalb würde es mich freuen, wenn wir dafür mehr Zeit hätten. – Bitte, Herr Behrendt, Sie haben das Wort!

Dirk Behrendt (GRÜNE): Danke schön! – Ich habe eine Frage an Herrn Dix: Ihnen sollen nach den Vorstellungen der Koalition zukünftig Überwachungsaufgaben, Überprüfungsaufgaben zuwachsen. Sind Sie aus heutiger Sicht, was das Know-how, die Technik und das Personal angeht, eigentlich dazu in der Lage, oder was bräuchten Sie an Zuwachs in diesen Bereichen, um die skizzierten Aufgaben – sprich Überprüfung der Programme – adäquat erfüllen zu können? Denn das muss man mitbedenken, wenn man hier über die Vorstellungen der Koalition redet, damit das nicht nur eine reine Absichtserklärung ist, sondern dass man das dann auch mit Leben erfüllt. Wir gehen davon aus, dass uns die Koalition nicht nur Sand in die Augen streuen möchte, sondern dass sie das tatsächlich mit Leben füllen will.

Die zweite Anmerkung – zu Ihnen, Herr Dregger: Sie haben gesagt, Sie möchten mit der Quellen-TKÜ schwere Verbrechen aufklären. Davon sind wir gar nicht so weit entfernt. Nur, warum schreiben Sie das da nicht hinein? Der Katalog wurde von Dr. Nöding angesprochen. Wenn es um den Katalog geht und Sie reinschreiben würden, dass Sie die Quellen-TKÜ nur zur Aufklärung von schweren Verbrechen wollen – das ist der oberste Bereich der Kriminalität, wenn man sich das auf einer Skala vorstellt –, dann ist das etwas völlig anderes, als heute in § 100a StPO drinsteht. Das fängt schon bei der unteren und mittleren Kriminalität an und geht bis nach oben. Ich würde mir wünschen, dass Sie das tatsächlich so wollen.

Ansonsten ziehe ich den Schluss aus diesem etwas Vagehalten im Antrag der Koalition und der Nichtbeantwortung meiner Frage, was Sie eigentlich mit der Ziffer 3 bezwecken – Stichwort Verfassungsschutz; ob Sie nun das Verfassungsschutzgesetz ändern wollen oder nicht –, dass es dazu noch keine festgelegte, einheitliche Überzeugung in der Koalition gibt. Deswegen deutet die Bitte von Herrn Kohlmeier an die Sachverständigen, heute hier konkretere Angaben darüber zu machen, was Sie denn in die Bundesratsinitiative reinschreiben sollen, darauf hin, dass Sie da noch in einem Arbeitsprozess sind. Ich kann das nur so deuten, dass Sie da noch „Work in progress“ machen.

Ich hoffe, dass Sie das, was die Sachverständigen gesagt haben, auch wirklich als Anregung aufgreifen, und zwar sowohl, was die technische Realisierung angeht, als auch, was die rechtliche Umsetzung angeht, und dass Sie noch einmal darüber nachdenken, dass man das zum einen enger fassen muss, also wirklich nur die schweren Verbrechen, Straftaten gegen Leib und Leben, und nicht die mittlere Kriminalität. Und ich hoffe, dass man zum anderen immer mitbedenkt – da finde ich das, was Herr Buermeyer gesagt hat, sehr bemerkenswert: Lasst uns doch lieber nur die Online-Durchsuchung regeln, das andere ergibt sich als Minus dazu, bevor wir uns bei der Quellen-TKÜ die Finger verbrennen, weil das technisch gar nicht machbar ist! – Das ist ein Gedanke, mit dem ich heute nach Hause gehe und über den ich noch länger nachdenken werde. In der Auswertung der Anhörung werde ich noch einmal darauf zurückkommen.

Vorsitzender Alexander Morlang: Vielen Dank! – Das Wort hat Herr Taş!

Hakan Taş (LINKE): Danke, Herr Vorsitzender! – Auch ich werde heute mit einigen guten Gedanken nach Hause gehen. Die Koalition scheint ihre eigenen Anträge nicht zu kennen. Wir haben heute einige wichtige Sachen dazu gehört. Technisch kann nichts eingehalten wer-

den. Wir werden nicht zielführend Staatstrojaner einsetzen können. Bislang gibt es, was allgemein bekannt ist, auch keine Software, die die Vorgaben des Bundesverfassungsgerichts tatsächlich einhält. Ob diese Software entwickelt werden kann, dazu haben wir – zumindest heute – nichts gehört, sodass diese Frage nach wie vor offen bleibt. Wir können in Sachen Software nichts nachweisen. Es ist heute mehrfach gesagt worden, dass sie bestimmte Funktionen nicht hat.

Herr Dix hat auf etwas Wichtiges hingewiesen, nämlich darauf, dass es keine Grundlage für den Einsatz beim Verfassungsschutz gibt. Der Verfassungsschutz hat zwar noch nicht erklärt, ob er tatsächlich Staatstrojaner einsetzen will. Der Herr Staatssekretär ist gerade weg, und insofern weiß ich nicht, ob Herr Palenda heute noch etwas dazu sagen darf. Mich interessiert, wie Sie den Einsatz von Staatstrojanern beim Verfassungsschutz sehen. Es ist fraglich, ob Staatstrojaner als V-Leute im Internet eingesetzt werden können, aber vielleicht können Sie noch kurz auf meine Frage eingehen, wie Sie den Einsatz von Staatstrojanern beim Verfassungsschutz sehen würden. – Danke!

Vorsitzender Alexander Morlang: Ich möchte darauf hinweisen, dass der Staatssekretär schon gegangen ist und damit auch alle seine Mitarbeiter keine Aussagen mehr treffen können und dürfen. – Das Wort hat Herr Kohlmeier.

Sven Kohlmeier (SPD): Es wird Sie nicht überraschen, Herr Rieger, dass ich nicht mit allem, was Sie gesagt habe, übereinstimme. Von der Polizei wurde angedeutet, dass möglicherweise die entsprechende Software nicht nur draufgespielt wird, indem man erst einmal auf den PC schaut, welche Software und Skype-Version dort verwendet wird, sondern dass es womöglich andere Wege gibt.

Ich finde es bedauerlich, dass wir vermutlich nicht dazu kommen, noch einige tiefschürfende Ausführungen zu hören, wenn es sich um eine geheimhaltungsbedürftige oder VS-Sache handelt. Ich wäre gern bereit, mir die Dinge anzuhören, die Öffentlichkeit insofern auszuschließen und die VS-Vertraulichkeit herzustellen, damit die entsprechenden Auskünfte gegeben werden können, sodass nicht der Eindruck erweckt wird, als wenn hier irgendwelche Sachen nicht erzählt werden können. Ich kann aber durchaus nachvollziehen, dass es da Sachen gibt, die Sie im öffentlichen Raum ungern mitteilen wollen. Deshalb mein Angebot an die Kollegen, das entweder im Verfassungsschutzausschuss, der geheim tagt und VS-Möglichkeiten hat, oder in diesem Ausschuss heute zu machen oder zu einem späteren Zeitpunkt nachzuholen.

In der Sache selbst: Wenn man es mit Herrn Buermeyer nimmt, dann wird die Quellen-TKÜ wohl nie eine Standardmaßnahme sein. Möglicherweise lohnt sich der Aufwand, den die Koalition betreibt, um eine rechtmäßige Quellen-TKÜ zu machen, nicht in Anbetracht der tatsächlichen Verhältnissen und auch nicht mit Blick darauf, wie die Polizei bzw. die Ermittlungsbehörden sie dann einsetzen werden.

Gleichwohl glaube ich, dass die Diskussion gezeigt hat, dass es in einem ersten Schritt richtig ist, hier zu einer vernünftigen und ordentlichen Rechtsgrundlage zu kommen. Man muss die Maßnahme Quellen-TKÜ an sich nicht toll finden, aber wenn man sie dann einsetzen möchte, dann muss es eine ordentliche Rechtsgrundlage dafür geben. Da gibt es – anders als es Herr Behrendt zu tun versucht – meines Erachtens kein Vertun, was wir gewollt und wie wir es

beantragt haben. Das ist für Sie, Herr Kollege Behrendt, immer ein bisschen einfacher. Sie legen gar keinen Antrag vor. Das heißt, ich kann davon ausgehen, dass Sie andauernd im „Work in progress“ sind – wenn ich das zitieren darf –, sodass es für Sie immer relativ einfach ist, zu irgendwelchen Sachen eine Nichtmeinung zu haben.

Wenn Sie dann den Antrag zu einer neuen Regelung der Online-Durchsuchung vorlegen wollen, die die Quellen-TKÜ beinhaltet, dann freue ich mich schon auf dessen Einreichung. Ich gehe davon aus, dass die Koalition ihn wohlwollend prüfen wird. Bisher haben Sie sich weder darüber ausgelassen, ob Sie Online-Durchsuchungen wollen, noch darüber, auf welche Weise Sie die Quellen-TKÜ wollen. So gesehen freue ich mich auf diesen Antrag.

Die Anregungen der Anzuhörenden würden wir dann nach dem Vorliegen des Wortprotokolls innerhalb der Koalition auswerten wollen. Ich kann mir durchaus vorstellen, dass sich daraus noch der eine oder andere Besprechungspunkt ergeben wird und möglicherweise auch der eine oder andere Ergänzungsbedarf zur Konkretisierung dessen, was uns die Anzuhörenden hier mit auf den Weg gegeben haben, sodass es heute – zumindest nach unserer Auffassung – nicht zu einer Abstimmung über die Anträge kommen wird, sondern wir zunächst das Protokoll abwarten. In einer der nächsten Sitzungen werden wir die Anträge abschließend beraten und dann darüber beschließen.

Vorsitzender Alexander Morlang: Vielen Dank, Herr Kohlmeier! – Bitte, Herr Kollege Lauer, Sie haben das Wort!

Christopher Lauer (PIRATEN): Ich habe nur eine kurze und etwas theoretische Frage an Herrn Dr. Nöding als Strafverteidiger: Sehen Sie in dem Moment, in dem es diese – Herr Buermeyer hat es gesagt – Rechtsgrundlage gibt und dann eine solche Software eingesetzt wird, für sich als Strafverteidiger angesichts der technischen Bedenken die Möglichkeit, immer zu sagen: Sorry, aber das war nicht mein Mandant, sondern das wurde da draufgespielt! – Der Staat setzt es ja ein, auch bei Fällen, wo es nicht nachweislich eine Quellen-TKÜ oder so gab, sondern nur die Tatsache, dass es das gibt und dass es eingesetzt werden kann. Sehen sie da für sich eine Möglichkeit?

Vorsitzender Alexander Morlang: Bitte, Herr Dr. Nöding!

Dr. Toralf Nöding (Vereinigung Berliner Strafverteidiger): Das ist in gewisser Weise natürlich Neuland, aber es liegt nahe, dass dann, wenn ein PC infiltriert wird, ein Strafverteidiger prüfen muss, ob das, was letztlich darauf ausgewertet wird, wirklich von seinem Mandanten stammt. – Dieser Einwand ist natürlich naheliegend, ja.

Vorsitzender Alexander Morlang: Bitte, Herr Dregger, Sie haben das Wort!

Burkard Dregger (CDU): Herzlichen Dank! – Ich mache es kurz: Herzlichen Dank noch einmal für die aufschlussreichen Ausführungen! Wenn man das mal auf die Grundfragen reduziert, dann muss man sich als Erstes die Frage stellen: Brauchen wir überhaupt eine Quellen-TKÜ? Jedenfalls ist die Koalition der Auffassung, dass das eine Ermittlungsmaßnahme ist, auf die wir beim Kampf gegen Verbrechen nicht verzichten können. – Wenn Sie das anders sehen, bin ich total offen, Argumente entgegenzunehmen, wie das sonst sicherzustellen

ist. Wir haben keine Lust daran, irgendwelche Überwachungsmedien zu erfinden, sondern es geht darum, unseren Rechtsstaat zu verteidigen.

Wenn wir dieser Auffassung sind – Herr Kollege Behrendt, wenn ich Sie richtig verstanden habe, haben Sie die Quellen-TKÜ nicht per se ausgeschlossen, denn Sie sagten gerade, man könne sie im Bereich der Schwerstkriminalität auch aus Ihrer Sicht anwenden –, dann stellt sich die Frage: Wie macht man sie? Erfüllt sie die Voraussetzungen des Bundesverfassungsgerichts? – Ich glaube, das Hauptanliegen des Koalitionsantrags ist es, dass wir sicherstellen, dass eine zukünftige Quellen-TKÜ diesen strengen Voraussetzungen entspricht, und zwar sowohl in rechtlicher als auch in technischer Hinsicht.

Ich habe heute sehr viele Fragen und Bedenken gehört und muss diese auch abschließend noch einmal anhand der schriftlichen Protokolle für mich selbst auswerten, aber ich habe auch vernommen – jedenfalls, was die rechtlichen Regelungen betrifft –, dass wir da auf dem richtigen Weg sind. Aber ich bin völlig frei, weitere Hinweise und Erkenntnisse entgegenzunehmen, und möchte mich deswegen abschließend für diese Anhörung bedanken.

Vorsitzender Alexander Morlang: Vielen Dank! – Wir kommen jetzt zur letzten Antwortrunde und beginnen mit Herrn Buermeyer. – Bitte sehr, sie haben das Wort!

Ulf Buermeyer (Richter am Landgericht): Vielen Dank! – Ich mag es überhört haben, aber ich muss gestehen, dass ich keine weitere an mich konkret gerichtete Frage auf meiner inneren Liste habe. – [Hakan Taş (LINKE): Zum Verfassungsschutz!] –

Ich teile da die Einschätzung des Berliner Beauftragten für Datenschutz und Informationsfreiheit. Also, das ist einfach glasklar so, dass das Bundesverfassungsgericht natürlich auch den Grundsatz der Normenklarheit in seiner Entscheidung zur Online-Durchsuchung betont hat, und man wird kaum umhinkommen zu sagen, dass eine Norm, die älter ist als überhaupt diese Entscheidung, und damit eine Norm, die kaum diese Differenzierungen aus Karlsruhe quasi antizipieren konnte, dass eine solche Norm wohl auch nicht als Rechtsgrundlage geeignet sein dürfte.

Und letztendlich stellen sich dann bei der Frage, ob die parlamentarischen Gremien diese Rechtssicherung herstellen können, dieselben Probleme wie bei der Frage nach dem Ermittlungsrichter. Ich denke, ich habe eben deutlich gemacht, warum aus meiner Sicht der Ermittlungsrichter diese Lücken in der StPO nicht schließen kann. Ich halte es für ähnlich problematisch, ohne jetzt einem der Abgeordneten zu nahe treten zu wollen, diese insbesondere technische Verantwortung auf den parlamentarischen Kontrollgremien quasi abzuladen. Auf der anderen Seite, wenn ich das richtig sehe, ist es ja schon so, dass das Verfassungsschutzgesetz in Berlin da etwas entwicklungsoffener formuliert ist – für Ermittlungsmaßnahmen, die eben nicht in einem Katalog aufgezählt worden sind.

Nehmen Sie es mir nicht übel, aber ich will es nicht an dieser Stelle definitiv in die eine oder andere Richtung beurteilen, denn dazu kenne ich auch wiederum die Sitzungen dieser parlamentarischen Gremien zu wenig, wie genau da diskutiert wird. Natürlich macht zum Beispiel der Geheimschutz es schwieriger, dort echten technischen Sachverstand von außen einzuholen. Auf der anderen Seite hat man da möglicherweise mehr Gelegenheit zur Beratung, als ein Ermittlungsrichter das hat. Denn Ermittlungsrichtertätigkeit ist einfach Massengeschäft, während ich jedenfalls davon ausgehe, dass Überwachungsmaßnahmen in den parlamentarischen Gremien nicht quasi durchgewinkt werden. Aber, wie gesagt, nehmen Sie mir es nicht übel, wenn ich da keine definitive Position vertreten möchte. Nur der Hinweis darauf, dass es eben da um sehr komplexe technische Fragen geht, und da sollte man, denke ich, sehr genau hinschauen. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Dr. Nöding!

Dr. Toralf Nöding (Vereinigung Berliner Strafverteidiger): Ich habe die eine konkret an mich gerichtete Frage schon beantwortet. Vielleicht noch dazu, wozu auch Herr Buermeyer gerade Stellung genommen hat: Ich würde mich da auch ein bisschen zurückhalten wollen, einfach, weil das die präventive Ermächtigungsseite ist, und wir da als Strafverteidiger – – Das ist nicht unser Metier.

Worauf ich hinweisen würde – das ist ja auch schon angeklungen –: Es gibt auch eine Verfassungsbeschwerde gegen § 20l BKA-Gesetz, und im November, gerade erst frisch, hat der Thüringer Verfassungsgerichtshof eine ähnliche Regelung aus dem Thüringer Polizeigesetz gekippt – wegen verfassungsrechtlicher Bedenken. Also auch da, glaube ich, muss man durchaus vorsichtig sein, an was für eine Regelung man sich da anlehnt. – Vielen Dank!

Vorsitzender Alexander Morlang: Vielen Dank! – Herr Rieger!

Frank Rieger (Chaos Computer Club Berlin): Zu dieser Frage zum Verfassungsschutz würde ich nur noch mal eine politische Einschätzung geben. Nach den NSU-Skandalen – stellen Sie

sich bitte mal vor, Sie würden verteidigen müssen, dass ausgerechnet diese Behörde nun auch die Computer ihrer Bürger legal infiltrieren darf! Ich kann mir nicht vorstellen, dass Sie dies im politischen Raum verteidigen wollen.

Vorsitzender Alexander Morlang: Herr Schröder!

Thorsten Schröder (modzero AG): Ich denke, es gab jetzt auch keine direkt an mich gerichtete Frage. Aber ich würde mich auf jeden Fall Herrn Rieger anschließen. – [Zuruf von Sven Kohlmeier (SPD)] –

Vorsitzender Alexander Morlang: Herr Kohlmeier, das finden Sie dann im Wortprotokoll. – [Sven Kohlmeier (SPD): Ich will nicht so lange warten. Ich bin schon ganz aufgeregt!] – Herr Dix! Bitte, Sie haben das Wort!

Dr. Alexander Dix (Beauftragter für Datenschutz und Informationsfreiheit): Ich möchte noch die Frage von Herrn Behrendt zur personellen Ausstattung beantworten. Ich kann nur eine Erwartung äußern, oder ich vermute, dass unsere personelle Ausstattung nicht in vollem Umfang ausreichend sein wird, um solche Prüfungen auf Dauer durchzuführen. Wir werden uns dem natürlich stellen, aber ich kann im Moment auch noch keine Aussage darüber treffen, welcher personelle Mehrbedarf entstehen wird. Wir werden aber auch natürlich mit Mitteln, die uns jetzt schon zur Verfügung stehen, unter Umständen externen Sachverstand hinzuziehen. Wie gesagt, das ist eine vorläufige Aussage, aber ich kann Ihnen jetzt nicht sozusagen eine Hausnummer nennen, was wir tatsächlich mehr an Personal brauchen.

Vorsitzender Alexander Morlang: Vielen Dank! – Damit sind wir zum Ende des Tagesordnungspunktes 2 gekommen. Ich gehe davon aus, dass hier ein Einvernehmen darüber herrscht, dass wir den Tagesordnungspunkt vertagen, damit Sie alle noch mal über dem Wortprotokoll brüten können. Herr Kohlmeier hat ja auch schon angeregt, dass wir möglicherweise noch einmal einen geschlossenen Sitzungsteil machen, wo die Kollegen der Exekutive Tacheles reden können. – Ich höre keinen Widerspruch. Damit sind die Tagesordnungspunkte 2 a, 2 b, 2 c und der Änderungsantrag der Grünen zu dem Tagesordnungspunkt 2 b vertagt. – Ich danke an dieser Stelle ganz besonders den Angehörten und auch den Kollegen von der Kripo, die uns hier viele großartige Einsichten gegeben haben. – Vielen Dank!

Punkt 3 der Tagesordnung

Verschiedenes

Siehe Beschlussprotokoll.