Deutscher Bundestag

Protokoll Nr. 54

16. Wahlperiode
Rechtsausschuss
(6. Ausschuss)

P r o t o k o l l *)

der 54. Sitzung

am 21. März 2007, 12.00 Uhr
Berlin, Paul-Löbe-Haus, Raum 4.300

Beginn der Sitzung: 12.04 Uhr

Vorsitz: Vorsitzender Andreas Schmidt (Mülheim), MdB

Öffentliche Anhörung

*) redigiertes Wortprotokoll

Vorsitzender Andreas Schmidt (Mülheim): Meine sehr verehrten Damen und Herren, liebe Kolleginnen und Kollegen, liebe Gäste, liebe Sachverständige. Ich darf Sie sehr herzlich begrüßen zu unserer Sachverständigenanhörung zum Thema Computerkriminalität. Ich schlage vor, wie eben mit Ihnen besprochen, dass wir zunächst in alphabethischer Reihenfolge von jedem Sachverständigen ein Statement von ungefähr 5 Minuten hören und anschließend in die Fragerunde eintreten. Ich bitte Herrn Professor Dr. Borges, Lehrstuhl für bürgerliches Recht, deutsches und internationales Handels- und Wirtschaftsrecht, Ruhr-Universität Bochum, zu beginnen.

SV Prof. Dr. Georg Borges: Sehr geehrte Damen und Herren. Ich möchte meine Stellungnahme fokussieren auf zwei Aspekte, die aus Sicht der Arbeitsgruppe Identitätsschutz im Internet, kurz a-i3, von besonderer Bedeutung sind, die ich als Sprecher des Vorstands leite. Die a-i3 ist eine interdisziplinäre Organisation, die den Identitätsschutz im Internet erforscht und die Öffentlichkeit hierüber informiert. Der aktuelle Schwerpunkt unserer Tätigkeit liegt bei Phishing und ähnlichen Formen der Internetkriminalität. Daher werde ich unter diesem Gesichtspunkt den Gesetzentwurf beleuchten. Ein weiteres Problem ist das Risiko einer überschießenden Pönalisierung von Softwareentwicklung durch den Gesetzentwurf, insbesondere § 202c E-StGB, die unerwünscht ist. Eine Gefahr einer solchen überschießenden Strafbarkeit sollte aus meiner Sicht unbedingt vermieden werden. Zu den dogmatischen Fragen, insbesondere der Umsetzung der Cybercrime-Convention, verweise ich auf die Stellungnahme von Herrn Kollegen Stuckenberg, der ebenfalls a-i3-Mitglied ist und die strafrechtlichen Aktivitäten bei uns leitet. Phishing und verwandte Angriffe sind eine ernst zu nehmende Herausforderung für den elektronischen Geschäftsverkehr, da sie geeignet sind, das Vertrauen der Nutzer in die Internetsicherheit zu gefährden. Es ist auch nicht nur das Onlinebanking betroffen. Vielmehr erleben wir derzeit in allen Bereichen des elektronischen Geschäftsverkehrs Identitätsmissbräuche verschiedenster Art. Phishing ist bereits nach geltendem Recht strafbar. Es ist aber für eine effektive Bekämpfung von Phishing und ähnlichen Formen der Kriminalität wichtig, dass möglichst alle Angriffsformen dem Grunde nach in möglichst allen Stadien strafbar sind, damit die Instrumente der Strafverfolgung eingesetzt werden können. Vor allem durch die geplanten §§ 202b und 200c E-StGB werden die vorhandenen Strafbarkeitslücken

weitgehend geschlossen. Das beruht vor allem darauf, dass § 202c Abs. 1 Nr. 1 E-StGB das Sich-Verschaffen von Passwörtern unter Strafe stellt und damit den Kernunrechtsgehalt des Phishing in der ersten Stufe, bei denen sich Täter in den Besitz von Geheiminformationen wie Passwörtern bringen, umfänglich erfasst. Je nach Auslegung kann es aber noch Zweifelsfragen geben. Deswegen sollte § 202c E-StGB erweitert werden und insbesondere auch die Vorbereitung von Betrug und Computerbetrug ausdrücklich erfassen. Zu diesem Zweck müsste der Tatbestand des § 202c E-StGB im ersten Satz durch die besondere Bezeichnung der Straftatbestände §§ 263 und 263a StGB erweitert werden. § 202c Abs. 1 Nr. 2 E-StGB stellt die Entwicklung und Verbreitung von Programmen unter Strafe, die zum Abfangen oder Abhören von Daten bestimmt sind. Diese Strafbestimmung, die für die Bekämpfung der Computerkriminalität große Bedeutung hat, ist aber ihrerseits problematisch, da sie zu weit gefasst ist. Sie erfasst nämlich nach ihrer bisherigen Fassung auch legitime und erwünschte Tätigkeit im Bereich der Entwicklung von IT-Sicherheits-Software. Ein Beispiel: Passwortscanner sind Programme, mit denen Passwörter getestet werden können. Jeder Netzwerkadministrator verwendet zur Sicherheitsüberprüfung routinemäßig solche Programme. Die gleichen Programme können aber natürlich auch von Tätern verwendet werden, um Passwörter auszukundschaften und damit Zugang zu geschützten Informationen zu erhalten. Es gibt eine Reihe von weiteren Beispielen, ich weiß aus der schriftlichen Stellungnahme, dass Herrn Lindner dazu noch näher Stellung nehmen wird. Wegen dieser Problematik, die geeignet ist, die Entwicklung von Sicherheitssoftware entscheidend zu stören, muss § 202 c Abs. 1 Nr. 2 E-StGB enger gefasst werden. Es gibt zwei Ansatzpunkte hierfür. Der erste ist eine genauere Beschreibung des objektiven Tatbestandes. Hier sollte nur Software pönalisiert werden, die vor allem oder überwiegend der Verwirklichung der genannten Straftatbestände dient. Zum zweiten sollte auch in subjektiver Hinsicht eine besondere Engfassung gelten, denn nach der bisherigen Fassung „Vorsatz“ würde ein Inkaufnehmen ausreichen. Hier sollte positive Kenntnis oder Absicht, dolus directus, also Wissentlichkeit erfolgen. Mit diesen Vorschlägen würde der § 202c E-StGB so eng gefasst, dass eine überschießende Pönalisierung verhindert wird. Zugleich könnte er einen wesentlichen Beitrag leisten zur Erfassung der aktuellen Form von Internet-Kriminalität. Ich danke für Ihre Aufmerksamkeit.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Prof. Borges. Ich darf zunächst noch eine Begrüßung vornehmen. Es ist eine große Ehre und Freude für uns, dass wir als Gäste den Justizminister aus der Türkei, Herrn Cemil Cicek, begrüßen dürfen. Herzlich willkommen, Herr Justizminister. Ich begrüße auch den Botschafter der Türkei, Herrn Mehmet Ali Irtemcelik und heiße ihn herzlich willkommen.

Wir fahren fort mit der Anhörung. Das Wort hat jetzt Herr Bruns, Bundesanwalt beim Bundesgerichtshof Karlsruhe. Bitte schön.

SV Michael Bruns: Vielen Dank. Meine Damen und Herren. Wir begrüßen grundsätzlich den Gesetzentwurf, denn er trägt dem Bedürfnis der Praxis nach einem Instrument zur strafrechtlichen Bekämpfung des zunehmenden Missbrauchs informationstechnischer Netzwerke durchaus Rechnung. Dies geschieht in unserem Sinne auch hinreichend exakt und ohne dass hier überschießende Räume gegeben wären. Wir erwarten als Strafverfolger keinen großen Andrang von Verfahren, sollte dieses Gesetz in Kraft treten. Denn das muss man ja ehrlich sagen, die Sachverhalte sind zu komplex und die Ressourcen, gerade im technischen Bereich der Ermittlungsbehörden, sind zu beschränkt, als dass hier - abgesehen von Spitzenfällen - eine große Fallzahl zu erwarten ist.
Wozu der Entwurf dienen kann, das möchte ich hier nur hervorheben, ist so etwas wie eine Netiquette zu schaffen, also ein Bewusstsein in der Internet-Gemeinde, welches Verhalten angemessen und welches Verhalten unangemessen ist. Dass eben der Cyberspace nicht unendlich ist, sondern dass es hier durchaus Spielregeln gibt.
Zu dem Entwurf im Einzelnen habe ich Stellung genommen. Ich möchte hier vielleicht drei Punkte hervorheben. Das eine ist der Vorschlag für den neuen § 202a E-StGB, das Sich-Verschaffen von unerlaubtem Zugang zu fremden Daten und der Überwindung einer Zugangssicherung. Auch hier wurde im Vorfeld angemahnt, die Strafbarkeit reiche zu weit, das Instrument sei zu wenig exakt geschliffen. Ich denke das nicht. Ich denke, dass hier die Voraussetzungen „unbefugt“ und „Durchbrechung von Sicherheitsmaßnahmen“ genügend ausgeprägte Filter sind. Lassen Sie mich das hinsichtlich des Gesichtspunktes der Durchbrechung von Sicherungsmaßnahmen vielleicht ergänzen. Grundsätzlich greift der unbefugte Zugriff auf gesicherte Daten

deutlich in die Sphäre des Berechtigten ein. Der durch die Durchbrechung der Sicherungsmaßnahme erkennbar gewordene nachdrückliche Wille zur Rechtsmissachtung hebt den Eingriff durchaus aus dem Bagatellbereich hinaus. Will sagen, hier ist grundsätzlich schon mal von einem Vorfeld der Strafbarkeit auszugehen, wenn sich jemand bewusst über die von einem anderen vor seine Daten gesetzte Schranke hinweg setzt. Die weiteren Filter, um hier wirklich Bagatelldelikte auszuschalten, die sind in diesem Entwurf, wie ich meine, intelligent getroffen. Es gibt vergleichbare Strafbereiche beim Familiendiebstahl oder bei Vermögensdelikten innerhalb der Familie. Die Tat ist als Antragsdelikt ausgestattet. Der Rechtsverletzte kann und soll darüber entscheiden, in wieweit er seine Rechtsverletzung als ahndungswürdig ansieht.

Der nächste Punkt ist aus meiner Sicht § 202d E-StGB, hier die Problematik der Unterscheidung zwischen den berüchtigten Hacker-Tools und der Systemsoftware oder der seriösen Prüfsoftware. Ich meine, schon sprachlogisch lässt sich kein objektives Kriterium zur Unterscheidung finden, weil der objektive Zweck einer technischen Einrichtung, wie hier einer Software, einer technischen Funktion, eben diese Funktion ist. Ich möchte das an einem Beispiel verdeutlichen. Man kann mit einem Auto in Urlaub fahren, man kann mit dem Auto aber auch zum Bankraub fahren. Das ändert an der Zweckbestimmung des Fahrzeugs oder an der technischen Zweckbestimmung des Fahrzeugs nichts. Hinzutreten muss, und das hat der Entwurf hier berücksichtigt, eine subjektive Seite, nämlich die subjektive Zweckbestimmung, die der Hersteller oder Benutzer dieser Software anbringt. Das ist hier das Einleitungsmerkmal zur Begehung einer der Straftaten nach dem Gesetz. Ich meine, das reicht aus, zumal hier die Vorsatzstufe relativ hoch ist. Es wird schon recht schwierig werden, auch das kann ich eigentlich nur aus der Ermittlungspraxis sagen, jemandem nachzuweisen, dass er ein bestimmtes Programm zum Zwecke der Begehung von Straftaten produziert oder vertreibt.

Jetzt komme ich zum letzten Punkt, den ich hier vorab ansprechen muss und möchte. Das ist die Frage des Password-Phishings. Ich teile die Auffassung von Herrn Prof. Borges, dass das ein besonders kritischer und wichtiger Bereich ist. Ich teile auch die Auffassung, dass es hier insgesamt um den Phänomenbereich des Identitätsdiebstahls geht. Also um einen, über das Computerrecht weit hinaus greifenden, Phänomenbereich und möchte eigentlich nur davor warnen, dieses Gesetzgebungsvorhaben, das computerrechtlich zugeschnitten ist vor allem zur

Umsetzung der internationalen Vorgaben, dadurch zu überfrachten, dass wir hier einen Bereich einführen, wo es um ein ganz anderes Rechtsgut geht, wo es darum geht, dass hier die Identität abgesaugt und für fremde Zwecke missbraucht wird. Das geschieht sicherlich auch im Computerbereich, das geschieht mittels Computer und mittels Internettätigkeit. Das geschieht aber auch anders. Das kann telefonisch geschehen durch Anrufe unter Tarnidentitäten, das kann persönlich geschehen. Stellen Sie sich vor, der Täter taucht bei Ihnen auf und sagt, er wäre jetzt der neue Sachbearbeiter Ihrer Bank. Er bräuchte jetzt Ihre Bankunterlagen. Im Zweifel würden Sie ihm die geben. All das sind Aktionen, die unter den Bereich des Identitätsdiebstahls fallen, die aber hier das Computerrecht überfordern würden. Ich denke, auch wenn die Bundesregierung davon nicht begeistert sein wird, man könnte überlegen, ob in soweit der Bundesregierung ein Prüfungsauftrag zu erteilen ist, diesen Bereich des Identitätsdiebstahls einmal auf seine rechtspolitische Notwendigkeit bzw. auf Regelungsmöglichkeiten zu überprüfen. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Bruns. Das Wort hat jetzt Herr Dr. Gercke, Rechtsanwalt aus Köln. Bitte schön.

SV Dr. Marco Gercke: Meine Damen und Herren. Ich möchte im Rahmen meiner kurzen Stellungnahme auch nur einige wesentliche Punkte eher allgemeiner Natur aufgreifen. Sie haben die Stellungnahme ja vorliegen. Ich begrüße den Gesetzesentwurf grundsätzlich. Nun ist die Frist am Samstag ausgelaufen. Nichtsdestotrotz ist es ein wesentlicher Schritt, wenn das Gesetz, der Rahmenbeschluss umgesetzt wird. Es ist deutliche Kritik geäußert worden, insbesondere Grundsatzkritik, die allerdings, wenn man mal ganz formal davon ausgeht, ein wenig verspätet ist. Weil halt der Gesetzgeber doch an die Vorgaben gebunden ist, an die internationalen Vorgaben und im Endeffekt der Gesetzgebungsspielraum doch sehr klein ist. Nun ist das nicht wirklich befriedigend, wenn die Kritik allein aus formalen Gründen, nämlich "Ihr hättet bereits im Rahmen des EU-Verfahrens bzw. des Europarat-Verfahrens diese Kritik äußern müssen" erfolgt. Es ist nicht wirklich befriedigend, das so zurück zu weisen, denn da sind durchaus berechtigte Punkte dabei. Also, die Frage der Vorfeldkriminalisierung, § 202c E-StGB, das ist ein Punkt, über den man tatsächlich diskutieren kann. Brauchen wir wirklich singulär im Internet eine immer weitere Vorverlegung der

Strafbarkeit? Das wäre eine spannende Diskussion. Das sehen Sie im Bereich des § 263a StGB, da haben wir eine Vorfeldkriminalisierung, wir haben es im Bereich des Urheberstrafrechts. Wir haben es auch im Bereich des sexuellen Missbrauchs von Kindern. Ich mache mich also strafbar in dem Moment, wo ich einem Kind per E-Mail eine Aufforderung zuschicke, die darauf gerichtet ist, das Kind zur Vornahme sexueller Handlungen zu bewegen. Also, dass es sich mit dem Täter trifft. Wenn ich das gleiche per Telefon mache, mache ich mich nicht strafbar. Da gibt es also durchaus Wertungswidersprüche, über die man diskutieren könnte. Nun ist es halt aber tatsächlich jetzt zu spät. Der Rahmenbeschluss liegt vor und er muss umgesetzt werden. Das bedeutet jetzt hier grundsätzlich zu diskutieren, ist halt zu spät. Ich denke, da könnte man anregen, dass man diese Interessengruppen, vielleicht auch aus Sicht der Bundesregierung, frühzeitiger involviert, nämlich bereits auf der internationalen Ebene. Ich habe mir als Vorbereitung gestern noch mal die Ankündigung der Sitzung des Rechtsausschusses angesehen. Ich zitiere mal ganz kurz. Da steht drin, so soll zukünftig bereits der bloße unbefugte Zugang zu einem Computer- und Informationssystem strafbar sein. Da liegt der Hauptkritikpunkt von mir. Das wäre toll, wenn dem so wäre. Aber in dem Punkt, genau in diesem entscheidenden Punkt § 202a E-StGB weicht der Gesetzesentwurf doch deutlich von den Vorgaben ab, während die EU und der Europarat den Zugriff auf ein Computersystem unter Strafe stellen, greift der Gesetzesentwurf den Zugang zu Daten an. Jetzt könnte man sagen, ja gut, das ist doch das Gleiche. Das habe ich zunächst auch mal gedacht. Ich habe gedacht, da gibt es ja wirklich kaum Fälle, wo sich das unterscheidet, aber die Zahl der Fälle ist doch nicht ganz unerheblich. Es gibt durchaus Fälle, wo das divergiert, wo ich mich nach den Vorgaben der Rahmenbeschlüsse strafbar machen würde, nicht aber nach der deutschen Umsetzung. Vielleicht können wir darauf nachher noch mal im Einzelnen eingehen. Das Beispiel ist das Aufspielen von Daten auf einen FDP-Server, wo ich nicht lesen kann. Es gibt genügend Fälle, wo ich in ein Computer-System eindringe, aber keine Leserechte habe. Ich kann also nicht sehen, was da wirklich passiert. Ich kann aber Manipulationen vornehmen. Ich kann z.B. Daten überspielen. Ob das mit dem bestehenden Begriff des "Zugang verschaffen zu Daten", ob es davon umfasst werden kann, halte ich für fraglich. Die Frage, die sich mir dann gestellt hat, ist, warum wurde in dieser Frage dann davon abgewichen? Ich kann das im Moment nicht beantworten. Ich bin mal gespannt, ob ich da vielleicht heute mehr erfahre,

denn es ist ja im Endeffekt so, die Idee des Rahmenbeschlusses und auch der Cybercrime-Convention ist eine Harmonisierung. Das bedeutet, es geht darum, dass die einzelnen Länder nicht einzelne nationale Regelungen schaffen, sondern dass man die Strafverfolgung effektiviert, indem man einheitliche Regelungen schafft. Deutschland hat nun einen Sonderweg gewählt. Ich bin für den Europarat als Experte tätig und kann sagen, dass es relativ singulär ist in dem Bereich. An sich ist eine wortwörtliche Übernahme der Vorschriften vorgesehen und passiert auch so. Ich komme gerade aus Serbien, wo der Europarat eine regionale Konferenz mit südosteuropäischen Ländern abgehalten hat. Es waren zwölf Ländern anwesend, unter anderem auch Repräsentanten des Justizministeriums der Türkei. Neun der zwölf Länder haben die Cybercrime-Convention bereits ratifiziert. Und da würde ich sagen, liegt auch ein zweiter Schwerpunkt meiner Kritik. Also die Idee der Harmonisierung vor fast sechs Jahren, Unterschrift der Cybercrime-Convention durch Deutschland, nach sechs Jahren immer noch keine Ratifizierung, sondern kleine Schritte, da sehe ich also einen Hauptkritikpunkt. So lässt sich die Internet-Kriminalität nicht effektiv bekämpfen. In den sechs Jahren seit der Unterzeichnung der Cybercrime-Convention ist viel passiert. Phishing war damals ein eher theoretisches Phänomen. Heute ist es ein höchst praktisches Phänomen. Watchnetze, also massenhaft zusammen geschaltete Computer, die für Angriffe genutzt werden, war damals auch praktisch nicht relevant. Heute wohl. Und Internetseiten terroristischer Organisationen, das waren damals Einzelphänomene. Heute ist das fast flächendeckend. Was ich damit nur sagen will ist, die Geschwindigkeit der Entwicklung geht weiter. In den sechs Jahren und auch schon in der Beratungszeit davor ist viel passiert. Wir müssten eigentlich viel weiter sein. Wir müssten bereits über Zusatzprotokolle reden. Aber solange große Staaten wie Deutschland die Konvention nicht vollständig umgesetzt haben, fehlen die Möglichkeiten, da andere Länder dazu zu bringen, die Konvention zu erweitern. Und da sehe ich also einen der Hauptkritikpunkte, dass Deutschland da nicht als Vorbild voran gegangen ist.

Abschließend: Da die Notwendigkeit einer möglichst wortgetreuen Umsetzung besteht, hat der Gesetzgeber tatsächlich einen sehr geringen Spielraum. Ich würde halt an den Stellen, an denen abgewichen wurde, insbesondere § 202a E-StGB, versuchen, mich dem Rahmenbeschluss und der Konvention anzunähern.

Ansonsten halte ich es aber durchaus, von Kleinigkeiten abgesehen, für einen gelungenen Gesetzesentwurf. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Dr. Gercke. Das Wort hat jetzt Herr Dr. Graf, Richter am Bundesgerichtshof, Karlsruhe. Bitte schön.

SV Dr. Jürgen-Peter Graf: Herr Vorsitzender, meine Damen und Herren. Ich kann auf meine schriftliche Stellungnahme grundsätzlich verweisen. Vielleicht zwei kurze Vorbemerkungen, dann eine längere. § 202a StGB war längst schon, eigentlich von Anfang an, aber spätestens seit über 15 Jahren, renovierungsbedürftig. Also nicht nur die Beschaffung der Daten, sondern auch der Zugang, weil es nicht der Realität entsprach und insofern wird eigentlich mit dem Gesetzentwurf nur das umgesetzt, was im Prinzip die Kommentarliteratur und im Prinzip auch schon die Gerichte gemacht haben und damit auch Rechtsklarheit geschaffen. Was die Beispiele betrifft, die teilweise vom Bundesrat angeführt worden sind, denke ich, wie Herr Bruns schon sagte, kann man die auf der Ebene der Antragsdelikte erledigen. Im Übrigen ist diese Problematik wohl nicht zu beseitigen, auch wenn man auf Datenspeicher umgeht. Jeder MP 3-Player ist heutzutage ein Datenspeicher, dass Sie also auch hier nicht weg bekommen. Wir werden hier wohl letztlich im Rahmen der Ermittlungsverfahren, wenn es überhaupt welche gibt, opportune Lösungen finden müssen. Ich denke aber, eine andere Formulierung lässt sich hierfür nicht finden. Der § 202b E-StGB scheint mir ein Problem zu sein, was ich auch aus der Gesetzesbegründung nicht habe erkennen können, wie man es lösen könnte. Die Frage der Nichtöffentlichkeit von Daten. Hier scheint mir deswegen ein Problem zu sein, weil möglicherweise der W-LAN-Verkehr, also die Funknetze, darunter fallen und wir dann einen Bereich hätten, der u. U. plötzlich strafbar wäre, was im Augenblick wohl nicht strafbar ist. Wenn ich mich in ein nicht gesichertes W-LAN-Netz einlogge und dort keine Daten anderer abziehe, sondern eben nur praktisch einen reinen Internetzugang nutze. Das will ich aber hier zunächst nicht weiter vertiefen.
Und jetzt der dritte Punkt und etwas ausführlicher. Die Frage des Phishing. Die Frage des Phishing ist ja in der Literatur doch sehr stark umstritten und ich denke, hier muss man zwei Dinge ganz klar machen. Das eine: Phishing besteht nicht nur aus dem Phishing von Bankdaten. Das ist zwar im Augenblick der gängigste Bereich, aber nicht unbedingt der Bereich, der am meisten Schäden entstehen lassen kann.

Denn bei Bankkunden bin ich naturgemäß irgendwo beschränkt in der Verfügungsmöglichkeit. Da liegt dann irgendwo der Schaden pro Bankkonto bei 3.000 bis 5.000 Euro, je nachdem, wie die Angelegenheiten ausgedehnt sind. Wenn ich aber an die Möglichkeit denke, z. B. bei einer Versteigerungsbörse einen Account zu phishen, kann ich Schäden viel höherer Natur verursachen. Wenn ich den Account habe, kann ich z. B. innerhalb von 3 oder 4 Tagen, an denen ich 200 Digitalkameras, 200 Handys, vielleicht noch 150 Laptops und dann noch irgendwelche Elektronik-Artikel zum Verkauf anbiete und die dann nicht liefere, wahrscheinlich einen Betrag von mehreren 100 000 Euro als Schaden entstehen lassen und habe es dann vielleicht sogar einfacher, damit wegzukommen.

Ich gebe zu, dieser Bereich ist, wenn die Änderung kommt, durch § 202c E-StGB möglicherweise abgedeckt, aber ich habe ein subjektives Kriterium. Ich muss den Vorsatz nachweisen und ich kann mir gute Verteidiger vorstellen, die jede Menge Einlassungen bringen werden, die ich dann vor Gericht anbringen kann. Wir haben eben keinen Klausurfall, wo alles feststeht, sondern der Richter muss sich einfach Überzeugung verschaffen und wenn der Angeklagte eine bestimmte Einlassung bringt, warum er jetzt gerade da gephisht hat für wissenschaftliche Zwecke oder wofür auch immer, und ich ihm das nicht widerlegen kann, dann führt eben diese Regelung nicht weiter.

Aber der zweite Bereich scheint mir viel wichtiger zu sein. Nämlich die Frage, wann ich eine Straftat strafbar sein lassen kann und wann nicht. Ich erinnere mich noch gut an eine Anhörung im Unterausschuss Neue Medien vor mehr als zehn Jahren, als mir ein Vertreter des Chaos Computer Clubs entgegen hielt, Internet sei ein virtueller und deswegen rechtsfreier Raum. Das heißt also, alles, was im Internet passiert, sei nicht strafbar. Ich habe dem entgegen gehalten, aber wenn Sie Schaden erleiden durch Betrügereien, dann werden Sie auch auf eine Bestrafung hinaus wollen. Soweit sind wir inzwischen, wir sind nun im Augenblick im Bereich, wo, wenn ich den § 202c E-StGB sehe, ich plötzlich eine Strafbarkeit des virtuellen Raums, des Internets habe. Eine Strafbarkeit für eine E-Mail, während ein anderer Bereich - Herr Bruns hat es gesagt - zum Beispiel ein Telefonanruf nicht strafbar ist und das kann m. E. nicht richtig sein. Und wenn ich jetzt vergleiche, Online-Banking z. B. mit Telefon-Banking und es gibt immer noch viele Leute, die Telefon-Banking machen, dann wäre das Phishing eines Telefon-Accounts keine Strafbarkeit nach § 202c E-StGB und plötzlich straflos. Und das scheint mir nicht richtig zu sein und deswegen

denke ich, dass eine komplette Regelung gemacht werden muss, weil dann die so genannte „Real World“ genau so in eine Strafbarkeit einbezogen werden muss wie die virtuelle Welt. Und wenn Sie auf der anderen Seite noch sehen: Die Phishing-Mails sind zwar inzwischen erheblich besser geworden. Wenn ich aber eine gängige Phishing-Mail ausdrucken, in einen Umschlag stecken und Ihnen zusenden würde, dann würden Sie die im Regelfall in den Papierkorb werfen und nicht berücksichtigen. Wenn sie aber als E-Mail ankommt, soll sie plötzlich ganz ernsthaft und strafwürdiger sein als wenn sie eben ausgedruckt ist. Deswegen denke ich, wir müssten hier einen Gleichklang finden und ob wir das jetzt in diesem Gesetzentwurf machen können, wird man sehen. Aber ich denke, die Chance besteht, und deswegen auch keine Regelungen in einem § 202c E-StGB, sondern eine Gesamtregelung. Ich habe einen entsprechenden Vorschlag gemacht, der dies berücksichtigen könnte. Herzlichen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank Herr Dr. Graf. Das Wort hat jetzt Herr Hange, Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik, Bonn. Bitte schön, Herr Hange.

SV Michael Hange: Guten Tag meine Damen, meine Herren. Bereits im Vorfeld des Regierungsentwurfs wurden in der Öffentlichkeit wiederholt Befürchtungen laut, dass infolge der beabsichtigten Anpassungen des Strafrechts künftig auch der gutwillige Umgang mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen strafbar sein könnte. In meinem Statement möchte ich hierauf den Focus legen. Dazu möchte ich kurz auch die Aufgaben des BSI darstellen, die hierzu auch Berührungspunkte haben.
Nach dem BSI-Errichtungsgesetz haben wir die Aufgabe, Sicherheitsrisiken zu untersuchen, aber auch Sicherheitsvorkehrungen zu entwickeln, und zwar soweit das zur Erfüllung der Aufgaben des Bundes erforderlich ist. Ferner haben wir nach BSI-Errichtungsgesetz die Aufgabe, die zuständigen Stellen des Bundes bei der Wahrnehmung der Aufgaben IT-Sicherheit in der Informationstechnik zu unterstützen, wir unterstützen hierbei auch den Bundesbeauftragten für den Datenschutz. Hinzu kommt die Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen.

In konkreter Wahrnehmung heißt das, dass wir zur Erfüllung dieses gesetzlichen Auftrags die grundlegende Entwicklung von Sicherheitsanforderungen und Praxislösungen für Systeme und Komponenten, insbesondere Sicherheitsgateways (Firewalls), Netzinfrastrukturen und -applikationen vornehmen. Unsere Fachreferate analysieren darüber hinaus Protokolle, Internet-Anwendungen sowie Netze und Netzdienste auf ihre Sicherheitseigenschaften hin und bewerten diese. Einen Arbeitsschwerpunkt bildet zudem die Untersuchung der Computernetze von Behörden und sonstigen Institutionen von öffentlichem Interesse auf existierende Schwachstellen. Die Entwicklung von Maßnahmen zur Verbesserung des Schutzes der IT in kritischen Infrastrukturen sowie die Erarbeitung von Strategien und Lösungen zur Sensibilisierung der Verantwortlichen für IT-Sicherheit stellt ein weiteres Aufgabenfeld dar. Damit einher geht die Analyse von Programmen mit Schadensfunktion sowie die Untersuchung von Betriebssystemen und Anwendungsprogrammen hinsichtlich ihrer Auswirkungen auf die Sicherheit im Allgemeinen und die IT-Sicherheit im Besonderen. Im Rahmen dieser Aktivitäten arbeitet das BSI auch mit Unternehmen und Sicherheitsexperten im privaten Sektor zusammen, die z. T. ihrerseits vergleichbare Untersuchungen und Entwicklungen vornehmen. Das BSI informiert die Öffentlichkeit über Risiken und Gefahren beim Einsatz der Informationstechnik und stellt auf seiner Webseite Informationsmaterial sowie Sicherheitsprodukte zur Verfügung.

Im Vorfeld des Regierungsentwurfs eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität hatte das Bundesamt für Sicherheit in der Informationstechnik Gelegenheit zur Stellungnahme. Die eingangs angesprochenen Befürchtungen bei Teilen der Öffentlichkeit, dass die im Regierungsentwurf des Strafrechtsänderungsgesetzes vorgesehenen Anpassungen den gutwilligen Umgang mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen künftig unter Strafe stellen könnten, sind aus Sicht des Bundesamt für Sicherheit in der Informationstechnik nicht begründet. Insbesondere fallen die betreffenden Sachverhalte nicht unter die Vorschrift des § 202c E-StGB („Vorbereiten des Ausspähens der Abfangens von Daten"). Zum einen betrifft diese Vorschrift nach dem Willen der Bundesregierung bereits auf der Ebene des objektiven Tatbestands lediglich solche Programme, „denen die illegale Verwendung immanent ist, die also nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind." Programme, deren funktionaler Zweck nicht

eindeutig ein krimineller ist und die erst durch ihre Anwendung zu einem Tatwerkzeug eines Kriminellen oder zu einem legitimen Werkzeug (z.B. bei Sicherheitsüberprüfungen oder im Forschungsbereich) werden (sog. dual-use-tools), sind damit ausdrücklich ausgenommen. Zum anderen weist die Bundesregierung darauf hin, dass die Tathandlung zur Vorbereitung einer Computerstraftat erfolgen muss. In Übereinstimmung mit der Auslegungspraxis zu vergleichbar aufgebauten Tatbeständen setzt die Vorschrift also voraus, „dass der Täter eine eigene oder fremde Computerstraftat in Aussicht genommen hat." Dies ist - wie die Bundesregierung darlegt - nicht der Fall, wenn das Computerprogramm beispielsweise zum Zwecke der Sicherheitsüberprüfung, zur Entwicklung von Sicherheitssoftware oder zu Ausbildungszwecken in der IT-Sicherheitsbranche hergestellt, erworben oder einem anderen überlassen wurde, da die Sicherheitsüberprüfung, die Entwicklung von Sicherheitssoftware oder die Ausbildung im Bereich der IT-Sicherheit keine Computerstraftat darstellen.
Schließlich hat die Bundesregierung festgehalten, dass auch die Verschaffung von bestehenden Schadprogrammen zum Zwecke der Analyse im Rahmen der Entwicklung von Sicherheitssoftware nicht unter den Straftatbestand fällt. Denn auch in diesem Fall wird keine Computerstraftat in Aussicht genommen.
Zusammenfassend lässt sich also festhalten, dass die im Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (StrÄndG) vorgesehenen Anpassungen des Strafrechts die Untersuchung von Sicherheitsrisiken und die Entwicklung von Sicherheitsanforderungen, wie sie der Gesetzgeber dem Bundesamt für Sicherheit in der Informationstechnik aufgetragen hat, nicht beeinträchtigen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Hange. Jetzt hat das Wort Herr Prof. Dr. Hilgendorf, Julius-Maximilians-Universität, Würzburg. Bitte.

Prof. Dr. Dr. Erich Hilgendorf: Herr Vorsitzender, sehr geehrte Damen und Herren. Herzlichen Dank für die Einladung. Da ich einen sehr langen Text abgegeben habe, darf ich mich vielleicht jetzt sehr kurz fassen, damit wir uns auch nicht dauernd wiederholen. Ich halte den Entwurf in seinen Leitmotiven wie in den meisten Details trotz des großen Zeitdrucks, unter dem die Umsetzung offenbar stand, für überzeugend. Besonders positiv hervorzuheben ist, dass der Entwurf mehrfach die

Gefahr einer Überkriminalisierung deutlich macht und deshalb grundsätzlich einer engeren Fassung der Straftatbestände den Vorzug gibt. Den § 202a E-StGB halte ich - so wie er dasteht - für durchaus brauchbar. Zu § 202b E-StGB habe ich eine Anmerkung. Da scheint mir das Tatbestandsmerkmal *„unter Anwendung technischer Mittel“* weitgehend funktionslos zu sein. Denn Sie können etwa eine elektromagnetische Abstrahlung gar nicht anders als durch technische Mittel erfassen. Durch die Sinne sind die Abstrahlungen nicht erfassbar. Bei § 202c E-StGB möchte ich etwas Kritik anbringen. Die Norm scheint mir zu weit geraten zu sein. Dieser Tatbestand umschreibt keinen klaren Unrechtstypus. Er erfasst auch etwa die Tätigkeit von Systemadministratoren, die Passworte festlegen oder Sicherungscodes festlegen und droht, auch die Tätigkeit von Sicherheitsfirmen zu erfassen. Da auch in §§ 303a und 303b auf den § 202c E-StGB Bezug genommen wird, droht hier eine Ausweitung des Strafrechts, die durchaus problematisch ist. Wie könnte man dieser Ausweitung entgegen wirken? In der jetzigen Fassung ist es im Wesentlichen der subjektive Tatbestand. Dieses Korrektiv ist jedoch kaum ausreichend, denn nach der jetzigen Fassung reicht dolus eventualis, bedingter Vorsatz, aus. Also, das bloße Inkaufnehmen oder Sich-damit-Abfinden ist genügend. Hier sollte eine Änderung erfolgen und der subjektive Tatbestand enger gefasst werden. Etwa, indem man ein Absichtserfordernis hinein schreibt: Wer in der Absicht, eine Straftat nach §§ 202a oder § 202b E-StGB vorzubereiten…, der wird bestraft. Also, Absichtserfordernis, das ist ja im StGB schon häufig erwähnt worden. Man könnte auch ansetzen im objektiven Tatbestand. Das ist grundsätzlich noch besser und die Worte gebrauchen wir gezielt. „Eine Straftat nach §§ 202a oder 202b E-StGB vorbereiten.“ Also schon im objektiven Tatbestand eine Eingrenzung vornehmen. Der objektive Tatbestand ist deshalb für Eingrenzungen zweckmäßiger, da der subjektive Tatbestand ja notorisch schwer nachzuweisen ist.

Bei der Datenveränderung, § 303a E-StGB, habe ich wieder keine Bedenken. Der Vorschlag des Bundesrates, hier die Verfügungsbefugnis bei Daten zu präzisieren, kommt zu spät. Das ist ein großes Problem, das man jetzt unter dem Zeitdruck nicht umsetzen kann. Bei § 303b E-StGB habe ich auch keine grundsätzlichen Bedenken. Zur Strafbarkeit des Phishing möchte ich anmerken, dass der § 202c Abs. 1 Nr. 1 E-StGB, das *„Sich-Verschaffen von Passwörtern“*, die meisten Fälle schon erfassen dürfte. Das ist in der Begründung des Entwurfs merkwürdigerweise nicht näher ausgeführt. Man könnte noch nachbessern, um noch weitere Teilbereiche dieses

neuen Phänomens zu erfassen. Etwa indem man schreibt „wer in der Absicht, eine Straftat nach §§ 202a, 202b oder 263a StGB vorzubereiten". Denn viele Phishing-Aktivitäten dienen wohl der Vorbereitung einer Tat nach § 263a StGB, Computerbetrug. Eine Möglichkeit, wenn gewünscht wird, einen vollständigen Tatbestand neu zu fassen, in § 202d E-StGB könnte man - Vorschlag von mir - formulieren „wer es in der Absicht, einem anderen Nachteil zuzufügen, unternimmt, in den Kommunikationsdiensten des Internet den Empfänger durch unzutreffende Angaben zur Preisgabe von Passwörtern oder anderer Zugangsdaten zu bewegen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist". Also ein ganz weiter Tatbestand. Weite Tatbestände sind problematisch, aber wenn Sie der Ansicht sind, dass hier eine Strafdrohung erfolgen sollte, wäre das möglicherweise ein Wortlaut, mit dem man arbeiten könnte. Man könnte auch die Norm enger fassen. Als Vermögensdelikt ausgestalten und statt der Nachteilszufügungsabsicht formulieren, dass der Täter handeln muss, um sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen.
Also, wenn ich zusammenfassen darf. Erstens das Merkmal technische Mittel in § 202b E-StGB ist möglicherweise überflüssig. Zweitens § 202c E-StGB ist zu weit geraten. Der sollte entweder subjektiv oder objektiv - besser objektiv - eingeschränkt werden. Und um das Phishing besser zu erfassen, kann man im subjektiven Tatbestand des § 202e E-StGB, den § 202c E-StGB und den § 263a StGB aufnehmen oder die eben vorgetragene Norm ganz neu fassen. Vielen Dank.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Prof. Hilgendorf. Jetzt bitte Herr Prof. Dr. Kudlich, Lehrstuhl für Strafrecht, Strafprozessrecht und Rechtsphilosophie, Friedrich-Alexander-Universität, Erlangen-Nürnberg.

SV Prof. Dr. Hans Kudlich: Meine Damen und Herren. Auch ich kann mich relativ kurz fassen, da die meisten wichtigen Punkte hier schon angesprochen worden sind und doch zumindest in der groben Richtung weitgehend Konsens besteht und ich denke, dass wir dann eher die Zeit darauf verwenden können, sozusagen über Detailvorschläge noch einmal zu diskutieren. Der relativ geringe verbleibende Umsetzungsspielraum und die Vorentscheidung der grundsätzlichen rechtspolitischen Fragen hat Herr Gercke ja schon ganz zutreffend herausgearbeitet. Ich möchte vielleicht als allgemeinen Hintergrund doch noch betonen, dass aus

meiner Sicht auch jenseits der ohnehin bestehenden Umsetzungsverpflichtung es durchaus ein berechtigtes Anliegen ist, an eine Reform der einschlägigen Delikte heranzugehen. Als Delikte in dieser Form eingeführt worden sind, Mitte der 80er Jahre durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität, da sah eben das Leben mit Computern vollständig anders aus. Insbesondere hatten wir noch nicht die jetzt im Mittelpunkt stehende Vernetzung der unterschiedlichen Systeme und die Bedeutung der Computer, gerade auch nicht nur für den gewerblichen Bereich, sondern auch für den Einzelnen etwa als Kommunikationsmittel. E-Mail hat in weiten Bereichen den Brief vollständig abgelöst. Man speichert seine Daten dort, man hat vielleicht die Steuererklärung noch auf dem PC, schickt sie dann - per Elster auf elektronischem Weg - ans Finanzamt usw. Das führt eben dazu, dass hier wirklich ein herausgehobenes Schutzbedürfnis besteht und wir haben ja in den letzten Wochen eine ganz wichtige Diskussion, sozusagen auf der Kehrseite etwa im strafprozessualen Bereich. Dass wir sagen, wo müssen wir hier die Ermittlungsmaßnahmen ansetzen, welche Grenzen gibt es für die Ermittlungsmaßnahmen, wenn hier zugegriffen wird auf Computerdaten, beispielsweise Stichwort Online-Ermittlung. Sie kennen alle diese Entscheidung des Bundesgerichtshofs. Wenn wir nach den Grenzen für die Strafverfolger suchen, dann müssen wir natürlich sagen, diese Rechte, die müssen nicht nur gegenüber dem Staat, sondern die müssen auch gegenüber Kriminellen geschützt werden. Das ist ganz klar.

Zu Einzelfragen möchte ich nur ganz wenig sagen. Zum einen vielleicht, was ich jetzt erst im Rahmen der Vorbereitung aufgrund der Stellungnahmen gesehen habe. Deswegen taucht es bei mir nicht auf, aber ich finde das einen guten Hinweis, den sowohl Herr Borges als auch Herr Hilgendorf gegeben haben. Nämlich bei § 200c E-StGB als eine Tat, die vorbereitet werden kann, auch den § 263 StGB aufzunehmen, um eben dann wirklich Fälle zu erfassen, in denen dann die spätere Strafbarkeit nach § 202a E-StGB zweifelhaft sein könnte.

Zum zweiten ganz kurz zu der Frage § 202c, Nr. 2 E-StGB. Die Frage, objektive oder subjektive Begrenzung im Zusammenhang mit den "Hacker-Tools". Ich möchte da den Vorrednern zustimmen, die betont haben, dass es wohl schwierig ist, eine objektive Begrenzung letztes Endes zu finden und mit Verlaub, ich darf das sagen, weil wir uns gut kennen, jetzt bei dem Vorschlag von Herrn Hilgendorf: Objektiver Tatbestand. Der gezielte Einsatz scheint mir nicht leichter nachzuweisen zu sein als

entsprechender Vorsatz. Da sehe ich jetzt auch von der Nachweisproblematik her keinen Unterschied. Vielleicht, weil es auch vorhin in einer Stellungnahme in etwa so anklang. Da wurde mal gesagt, es steht im Entwurf ja drin, „wer zum Zwecke der Vorbereitung einer solchen Straftat". Das steht so eben nicht drin, sondern es ist objektiv formuliert „wer eine Straftat vorbereitet, indem". Wenn wir schreiben würden „wer zur Vorbereitung", dann wäre im Prinzip schon die von Herrn Borges und von Herrn Hilgendorf überzeugend geforderte Beschränkung im subjektiven Tatbestand drin. Das wäre also gar kein großer Eingriff, der erforderlich wäre.
Ein letzter Punkt, bisher noch nicht angesprochen. Ich bin nicht sicher, ob in der Neufassung des § 303b E-StGB, soweit es hier um die Beeinträchtigung fremder Computersysteme geht, wo jetzt auch nicht nur behördliche und gewerbliche Systeme, sondern auch Systeme von Privatpersonen geschützt sind, ob wir hier dieses Merkmal der Systeme von wesentlicher Bedeutung, dieses einschränkende Merkmal tatsächlich in jedem Fall brauchen. Die europäischen Vorgaben sehen das m. E. nicht vor. Es heißt dann zwar "in leichten oder in nicht schweren Fällen", aber das bezieht sich eigentlich eher auf den Grad der Beeinträchtigung und nicht auf die Bedeutung dieses Systems für das Opfer. Und nun mag diese Unterscheidung zwischen größerer oder kleinerer Bedeutung für Behörden, für Betriebe vielleicht noch irgendwie mehr oder weniger objektiv zu fassen sein. Für Privatpersonen stelle ich mir diese Unterscheidung sehr sehr schwierig vor. Im Entwurf ist die Rede davon, wenn jemand das eben braucht, um nebenberuflich zu arbeiten oder um zu schriftstellern, dann mag das sein. Nun haben wir ja eine wesentliche Bedeutung, wenn ich es dagegen nur nutze, um zu kommunizieren, ist es keine wesentliche Bedeutung, also private E-Mails. Wir sind in einer Vorschrift, die im systematischen Kontext der Sachbeschädigungsdelikte steht. Wenn ich ein privates Telefon zerstöre, das nur zu Privatgesprächen genutzt wird, habe ich natürlich auch eine Strafbarkeit. Deswegen sehe ich nicht eigentlich, weswegen die rein private Kommunikation aus dem Bereich herausfallen sollte. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Prof. Kudlich. Jetzt bitte Herr Lindner, Geschäftsführer der SABRE Labs GmbH., Berlin.

SV Felix Lindner: Meine Damen und Herren. Ich möchte, wie schon in meiner schriftlichen Stellungnahme auf die Auswirkungen des § 202c Nr. 2 E-StGB

ausschließlich eingehen, denn das ist, was uns in der Sicherheitsindustrie betrifft. Ich bin seit zehn Jahren Security-Consulter und bin in dieser Eigenschaft für Microsoft, SAP und u.a. auch die Toll Collect zur Sicherung des deutschen Maut-Systems tätig geworden. Für Microsoft habe ich mehrmals Sicherheitsüberprüfungsteams geleitet, die u. a. die spätere Firewall von Windows Vista, das Mobilbetriebssytem Windows Mobile auf Sicherheitssysteme überprüft haben. Weiterhin bin ich Mitglied in freien Teams, die zur Aufklärung von Computerkriminalität im internationalen Bereich tätig werden.

Alle ernst zu nehmenden Unternehmen wählen die Dienstleister für solche Aufgaben nach genau zwei Kriterien aus: Vertrauen und technische Fähigkeit. Der Anspruch an die technische Fähigkeit ist enorm, da nur die besten der legalen Sicherheitsteams mit den Ressourcen und dem Können der kriminellen Organisationen mithalten können. Für Windows Vista z. B. wurden diejenigen Teams gewählt, welche die besten Angriffs- und Überprüfungsprogramme entworfen hatten und entwerfen. Microsofts eigenes Sicherheitsteam ist weltweit Spitze. Der Entwurf des § 202c Nr. 2 StGB gefährdet genau diese Eigenschaften. Das Vertrauen und die technischen Fähigkeiten. Der Entwurf bietet keinerlei Rechtssicherheit für Unternehmen, welche sich auf die Überprüfung von Sicherheitsmechanismen spezialisiert haben. Im Falle einer Anzeige beispielsweise durch ein konkurrierendes Unternehmen würde eine Ermittlung eingeleitet, sämtliche Rechentechnik des betroffenen Unternehmens beschlagnahmt, um die Beweismittel für das Vorbereiten des Ausspähens und Abfangens von Daten zu sichern. Und das betroffene Unternehmen wäre auch im Falle eines Freispruchs seiner existenziellen Grundlagen beraubt und müsste den Betrieb einstellen. Bevor es überhaupt zu einer Verhandlung kommt.

Dienstleistungen im Bereich Computersicherheit, gleich welcher Art, sind Vertrauenssache. Kein Unternehmen würde Mitarbeiter einstellen oder Dienstleistungsunternehmen beauftragen, welche schon einmal aufgrund einer Computerstraftat aktenkundig geworden sind. Hierfür spielt es eine untergeordnete Rolle, ob es in dem betreffenden Fall zu einer rechtskräftigen Verurteilung kam. Zum momentanen Zeitpunkt gehört Deutschland im Hochtechnologiebereich der Computersicherheit noch zu den führenden Nationen weltweit. Ein Inkrafttreten des vorliegenden § 202c E-StGB würde mit großer Sicherheit die Abwanderung der führenden Unternehmen zur Folge haben. Des Weiteren können Kunden in Deutschland, z. B. Deutsche Bank oder SAP, die notwendigen

Überprüfungsdienstleistungen nicht mehr einkaufen, da die Durchführungen in vielen Fällen die örtliche Präsenz voraussetzt, welche der Anbieter aufgrund der fehlenden Rechtssicherheit mit großer Wahrscheinlichkeit ablehnen müsste. Dies schließt auch Anbieter aus dem Ausland ein. Es kann auch nicht davon ausgegangen werden, dass die innerdeutsche Nachfrage etwas an dieser Entwicklung ändern würde. Da die globale Nachfrage nach den entsprechenden Dienstleistungen im hoch qualifizierten Bereich deutlich größer ist als das Angebot und somit die wirtschaftlichen Auswirkungen für die abgewanderten Unternehmen minimal bleiben. Computersicherheit lebt zum größten Teil von Forschung und Publikation. Hier sind vor allem akademische und private Interessensvereinigungen, aber auch die Beratungsunternehmen tätig, welche mit Hilfe von neuesten Angriffen die Sicherheit von Computersystemen kontinuierlich auf die Probe stellen, Lösungen für die identifizierten Probleme erarbeiten und beides kostenfrei publizieren. Eine Abgrenzung, ob dadurch eine fremde Straftat in Aussicht genommen worden ist, ist unmöglich, wenn ein Sicherheitsproblem gemeinsam mit dem Beweis einer Ausnutzbarkeit oder eines neuen Tools auf einer internationalen E-Mail-Liste publiziert wird. Das BSI ist wohl die einzige Organisation, die keine Anklage zu befürchten hätte. Kriminelle Organisationen auf der anderen Seite arbeiten seit mehr als zehn Jahren darauf hin, dass diese Praxis, welche gemeinhin als full disclosure bekannt ist, unterbunden wird. Sie publizieren Falschmeldungen, bieten Geld für Nichtstattfinden von Publikationen und versuchen auch sonst ziemlich alles Erdenkliche, um exklusive Besitzer dieser, für sie wertvollen, Informationen zu sein. Die öffentliche Darstellung eines Sicherheitsproblems macht alle Anwender, Administratoren und den Hersteller auf das Problem aufmerksam und damit werden die betroffenen Systeme innerhalb kürzester Zeit entsprechend geschützt. Ist die Information über das Sicherheitsproblem einmal öffentlich, ist sie für die kriminellen Organisationen wertlos. Solange allerdings das Problem nicht öffentlich ist, existiert kein Schutz und die kriminellen Organisationen haben leichtes Spiel.

Die momentane Fassung des § 202c Nr. 2 E-StGB setzt genau das um, was sich jede kriminelle Organisation und so mancher Geheimdienst schon immer gewünscht haben. Den Mitwirkenden der EU-Cybercrime-Convention sind diese Probleme offensichtlich bekannt gewesen. Warum sonst hätte man Art. 6 Abs. 3 eingefügt, in dem es heißt "each party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or

otherwise making available of the items referred to in paragraph 1 a.ii". Was die ganze Geschichte mit dem Password-Phishing meint.
Ich empfehle dringend, von dieser Option Gebrauch zu machen und Nr. 2 des § 202c E-StGB ersatzlos zu streichen, da alle erdenklichen Straftaten heute und in Zukunft durch die restlichen Gesetze und das restliche Werk vollständig abgedeckt sind. Ich danke Ihnen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Lindner. Jetzt bitte abschließend Herr Dr. Stuckenberg. Privatdozent am Strafrechtsinstitut der Rechts- und Staatswissenschaftlichen Fakultät der Rheinischen Friedrich-Wilhelms-Universität, Bonn. Sie haben das Wort zum Schluss.

SV Dr. Carl-Friedrich Stuckenberg, LL.M.: Vielen Dank, Herr Vorsitzender, meine Damen und Herren. Ich werde mich auch auf drei Punkte beschränken. Vieles ist schon gesagt worden. Ich werde mich auch auf § 202c E-StGB beschränken. Ich sehe da die Gefahren bei weitem nicht so dramatisch wie Herr Lindner, denke aber, dass die Vorschrift in der jetzigen Fassung die Regelungsabsicht des Gesetzgebers nicht eindeutig zum Ausdruck bringt. Erstens, wir wissen, dass Art. 103 Abs. 2 Grundgesetz den Gesetzgeber verpflichtet, die Voraussetzungen der Strafbarkeit so genau zu umschreiben, dass Tragweite und Anwendungsbereich des Straftatbestands schon aus dem Gesetz selbst zu erkennen sind. Das erscheint mir bei dem § 202c Abs. 1 Nr. 2 E-StGB so nicht gelungen. Bestraft werden soll das Herstellen, Verschaffen, Vertreiben usw. von Programmen, deren Zweck die Begehung einer Tat nach § 202a folgende E-StGB sein soll. Dieser Zweck soll lt. Entwurfsbegründung objektiv bestimmt werden, wobei gleich gesagt wird, es reicht, wenn der Zweck auch die Begehung einer solchen Tat ist. Wir haben jetzt mehrfach gehört, viele Programme lassen sich sowohl legal wie illegal verwenden, insbesondere die im Bereich der IT-Sicherheit eingesetzten Analysetools und sonstigen Instrumente. Daher eben auch die verständliche, denke ich, Aufregung in den Fachkreisen, ob jetzt ihr Handwerkszeug kriminalisiert werden soll. Lt. Begründung sollen solche dual use tools nicht erfasst werden. Das ist aber dem Gesetzeswortlaut nicht anzusehen und die Cybercrime-Convention, deren Art. 6 hier umgesetzt werden soll und § 202c sind da klarer, weil sie eben sagen, die Programme müssen vorwiegend, überwiegend „primarely" zu einem kriminellen

Zweck geschaffen worden sein. Auch wenn dann vielleicht nicht viele übrig bleiben, was absehbar ist. Und wie gesagt, die Konvention ordnet in Abs. 2 des Art. 6 ausdrücklich an, dass die Vorschrift nicht so auszulegen ist, dass der Einsatz von Programmen zu Test und Schutz der Computersysteme bestraft wird. In diesem Sinne, denke ich, sollte es eine Präzisierung geben, und zwar nicht nur in der Gesetzesbegründung, sondern, wenn es geht, schon im Text.

Zweitens, wir haben gesehen, auch der Umgang mit dann noch verbotener Software gehört zum Alltagsgeschäft in der IT-Sicherheit. Man muss sich ja auch solche Schadprogramme ansehen können, um zu wissen, was man dagegen tun kann. Um sie in Fachkreisen diskutieren zu können, müssen sie versandt, verbreitet, zugänglich gemacht werden. Natürlich ist es nur strafbar, wenn es mit dem Vorsatz geschieht, dadurch Computerstraftaten vorzubereiten und die IT-Sicherheit will genau das Gegenteil. Da aber nach der jetzigen Formulierung schon bedingter Vorsatz, dolus eventualis, genügt, das billigende Inkaufnehmen der Möglichkeit, dass jemand damit die genannten Straftaten begeht und jeder Techniker weiß, dass er das wahrscheinlich nie ausschließen können wird. Dass irgend jemand aus einer offenen, halboffenen Gemeinde trotz allen Vertrauens vielleicht doch sich als schwarzes Schaf erweist, dann hinge seine Strafbarkeit davon ab, ob die nicht ganz leicht zu bestimmende Schwelle zum dolus eventualis schon überschritten ist oder nicht. Das ist nicht im Sinne der Europarats-Konvention, die eben Verfahren zum Schutz von Computersystemen eindeutig aus der Strafbarkeit ausschließen will. Dieses ungewollte Strafbarkeitsrisiko wäre ausgeschaltet, wie auch zuvor schon angesprochen wurde, wenn man die subjektive Tatseite, ich würde sagen, wenigstens auf direkten Vorsatz, Wissentlichkeit und Absicht im engen Sinne beschränkt, wie es die Cybercrime-Convention selbst auch tut.

Drittens. Der § 202c E-StGB, und das ist vielleicht mehr ein rechtsförmlicher Kritikpunkt, beginnt mit den Worten "wer eine Straftat vorbereitet, indem er…". Diese Formulierung findet sich schon mehrfach im StGB bei der Vorbereitung der Geldfälschung, § 149 StGB, aber auch in §§ 263a Abs. 3 und 275. Die Formulierung ist auch elegant, eleganter als die Konvention, aber sie ist m. E. unklar und sachlich falsch. Sie ist unklar, weil bei den drei anderen genannten Straftatbeständen seit langem Streit besteht, ob das Vorbereiten einer konkreten Tat oder die abstrakte Gefahr, dass eine solche Tat begangen wird, gemeint ist. Folglich auch, ob der Vorsatz sich auf eine nach Tat und Täter jedenfalls konkretisierte Tat beziehen muss

oder nicht. Ich denke, die Formulierung ist auch sachlich falsch, weil die Entwurfsbegründung von einem abstrakten Gefährdungsdelikt spricht. Das ist auch durchaus berechtigt. Denn wer etwa einen Virenbausatz ins Internet stellt, schafft damit bewusst Tatanreize und Tatmöglichkeiten, kann aber in den meisten Fällen gar nicht wissen, wer wann welchen Schaden genau damit anrichtet. Handelt es sich aber um ein abstraktes Gefährdungsdelikt, dann sollte das doch eindeutig so formuliert werden und nicht eine Formulierung benutzt werden, deren Unklarheit eigentlich bekannt ist. Im Übrigen spricht die Konvention selber nicht von Vorbereiten, sondern schlicht davon, dass jemand Passworte oder Computerprogramme erstellt mit dem Vorsatz, sie zu Computerstraftaten zu verwenden.
Vielleicht noch einen ganz kurzen, letzten Satz zu einem eigenen Phishing-Tatbestand oder Identitätsdiebstahl. Identitätsdiebstahl, nicht begrenzt auf elektronisches Vorgehen, halte ich durchaus für erwägenswert, glaube aber nicht, dass man das jetzt noch so en passant mitregeln kann. Denn dann würde man ein Vorbereitungsdelikt zum Betrug oder noch viel weiter schaffen und ganz großräumig Strafbarkeitslücken schließen. Ich denke, es sollte sehr genau überlegt werden, was man überhaupt erfassen will und wie weit man das erfassen will. Denn da geht man noch weiter in den Vorbereitungsbereich. Ich danke Ihnen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Dr. Stuckenberg. Damit sind wir am Ende der Statement-Runde und treten ein in die erste Fragerunde. Wir haben ein bestimmtes Verfahren hier im Rechtsausschuss. Ich will es noch mal kurz erläutern. Jede Kollegin, jeder Kollege hat jetzt die Möglichkeit, in einer ersten Runde maximal zwei Fragen zu stellen. Eine Frage an maximal zwei Sachverständige oder zwei Fragen an einen Sachverständigen. Der angesprochene Sachverständige wird zu Beginn genannt, damit er sich auf die Antwort vorbereiten kann. Wir sammeln diese Fragen und beginnen nach der ersten Fragerunde mit der Beantwortung.
Es liegen einige Wortmeldungen vor. Der Kollege Manzewski beginnt. Bitte schön.

Dirk Manzewski (SPD): Ich fange mal an mit dem § 202a E-StGB und habe zwei Fragen dazu. Die erste richte ich an Herrn Bruns und an Herrn Prof. Kudlich. Meine Herren Sachverständigen, würden Sie meine Auffassung teilen, dass wir den Versuch von § 202a und 202b E-StGB, wie er angedacht ist, unter Strafe stellen

sollten und wenn ja bzw. nein, warum bzw. warum nicht? Die zweite Frage richtet sich wiederum an Herrn Bruns und an Herrn Dr. Gercke. Meinen Sie, dass beim § 202a E-StGB auf das Merkmal einer besonderen Zugangssicherung verzichtet werden könnte?

Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN): Die erste Frage habe ich an Herrn Borges und an Herrn Prof. Hilgendorf. Ich bin ja jemand, der sehr wohl für enge, klare Straftatbestände streitet. Nun, weil Sie beide den § 202c Abs. 1 Nr. 2 E-StGB als objektiv zu weitgehend beschrieben haben, wollte ich Sie bitten, dass Sie das uns oder mir noch einmal ganz klar darstellen. Das Beispiel, das Herr Lindner genannt hat, war ja die Angst vor Ermittlungsverfahren. Er selber sprach dann davon, dass man hinterher freigesprochen wird. Ist das das Thema? Also, dass die Vorschrift zu Ermittlungsverfahren anreizt, die später im Sande verlaufen? Oder ist es tatsächlich materiell eine zu weite Fassung? Ich lese bisher jedenfalls die Vorschrift so, dass sich nur derjenige strafbar macht, der eine Straftat vorbereitet. Der eine Straftat vorbereitet und nicht der, der irgendetwas anderes macht. Er muss schon eine Straftat vorbereiten, und zwar wie? Wie muss er sie vorbereiten? Indem er ein Computerprogramm herstellt? Aber der Zweck dieses Programms muss die Begehung genau dieser Straftat sein. Jetzt könnte man sich natürlich überlegen, haben Programme überhaupt Zwecke? Wenn Programme keine Zwecke haben, dann führt diese Vorschrift zu überhaupt keiner Strafbarkeit. Aber wenn Programme Zwecke haben, dann ist man nur strafbar, wenn man ein Programm herstellt, das den Zweck hat, eine Straftat zu begehen. Und nicht irgendeinen anderen Zweck. Deswegen würde ich gerne Ihre Einwände begreifen, wieso diese Vorschrift Ihrer Meinung nach materiellrechtlich zu weit geht.
Meine zweite Frage richtet sich an Herrn Bruns und Herrn Stuckenberg. Dazu nur ein kurzes Vorwort, Herr Gercke. Wir sehen das überhaupt nicht so, dass wir Rahmenbeschlüsse wortwörtlich umsetzen wollen, wir sehen das inzwischen so, dass wir Rahmenbeschlüsse vielleicht sogar überhaupt nicht umsetzen. Das Bundesverfassungsgericht hat uns das in dem Verfahren Europäischer Haftbefehl mit richtig derben Worten um die Ohren gehauen. Also, jedenfalls im Bereich der Rahmenbeschlüsse fühlen wir uns als nationales Parlament immer noch frei, nachzudenken und zu entscheiden. Meine konkrete Frage an Sie beide, Herr Borges und Herr Stuckenberg, läuft darauf hinaus, ob es eine Begründung gibt, die trägt?

Warum in dem Rahmenbeschluss immer von Computerdaten gesprochen wird und in dem Gesetzentwurf immer nur von Daten? Ist das eine sprachliche Gleichheit oder gehen wir über das, was der Rahmenbeschluss will, mit dieser Begrifflichkeit hinaus? Ich habe das Gefühl, dass dahinter mehr steckt als nur Wortklauberei und wenn Sie uns das erklären könnten, wäre das das ganz schön.

Dr. Jürgen Gehb (CDU/CSU): Ich habe auch zwei Fragen. Die erste richtet sich an Herrn Graf und Herrn Hilgendorf. Sie sind ja alle dauernd beim § 202c E-StGB. Ich möchte Sie fragen, ob es aus rechtspolitischen Gründen notwendig ist, die Strafbarkeit so weit, wie im Entwurf vorgesehen, vorzuverlegen und ob das europarechtlich wirklich zwingend vorgeschrieben ist. Und die zweite Frage, auch wieder an Herrn Graf, aber dann vielleicht an Herrn Hange, weil er ja auch im Bundesamt für Sicherheit einen großen Überblick hat: Sind mit diesem Gesetzesentwurf, ich überlege ja nur, ob es vielleicht zu viel ist, alle Facetten der Computerkriminalität erfasst oder bleiben noch offene Flanken aus Ihrer Sicht, um das alles zu arrondieren? Das würde mich mal interessieren, Sie werden sicherlich nicht alle Fälle antezipieren können, die es noch geben kann, aber wenn ein signifikanter Mangel da wäre und offene Flanken, dann könnte man das vielleicht mit dieser Frage beantworten.

Jan Korte (DIE LINKE.): Ich habe auch zwei Fragen. Zum einen noch mal eine Nachfrage mit der Bitte um Präzisierung an Herrn Borges und Herrn Stuckenberg zum § 202c E-StGB. Ich möchte gerne wissen, ob Sie bezüglich der Bestimmtheit des § 202c E-StGB vor allem darin eine Eignung sehen, wirklich zu unterscheiden zwischen strafwürdigem und nicht strafwürdigem Verhalten, ob das ansatzweise dort mit geregelt ist. Zum zweiten würde ich dann gern Herrn Lindner noch mal fragen, Bezug nehmend auf sein Statement und die schriftliche Stellungnahme. Es gilt ja für alle Fraktionen, dass wir uns natürlich insbesondere um die kleinen und um die mittelständischen Unternehmen sorgen. Gerade in dieser Frage gibt es eine große Einmütigkeit bei Organisationen und auch Unternehmen, die ansonsten relativ wenig miteinander zu tun haben. Da würde mich interessieren, Herr Lindner, wie die Debatten in diesen Kreisen insgesamt wahrgenommen werden. Denn das halte ich ja dann doch für recht maßgeblich, was die konkreten Folgerungen daraus sein könnten.

Jörg Tauss (SPD): Ich hätte zwei Fragen. Eine an Herrn Hilgendorf und eine an Herrn Lindner. Wobei ich übrigens vorausschicken will, ich bin hier nicht Lobbyist, aber ein interessanter Fall für den Immunitätsausschuss, weil ich mich mit Fragen der IT-Sicherheit beschäftige und mich in der Tat auch schon ohne Einwilligung von Berechtigten darum gekümmert habe, ob IT-Systeme sicher sind oder nicht sicher sind. Und ich auch künftig vorhabe, dies zu tun. Ich sage dies in aller Deutlichkeit. Insofern würde ich mir eigentlich wünschen, nicht ein solcher Fall zu werden, sondern dass wir uns über § 202c E-StGB nochmals unterhalten.

Herr Vorsitzender, mit Ihrem Einverständnis hat freundlicherweise das Sekretariat draußen das Protokoll einer Expertengesprächsrunde ausgelegt, die wir im Unterausschuss Neue Medien gemacht haben. Wo, ich sage mal, in fast vernichtender Form niemand zu der Erkenntnis gekommen ist, wie sie Herr Hange hier vorgetragen hat. Niemand. Das blanke Gegenteil war der Fall. Vielleicht auch diese interessante Information, vielleicht auch für die Sachverständigen dieses Protokoll nachher zur Verwendung.

Meine Frage an Herrn Hilgendorf wäre: Also, wenn der Tauss jetzt als Hacker ein Betriebssystem auf Lücken überprüft, nehmen wir mal an von einer bestimmten Firma X. Von wem muss ich die Einwilligung eigentlich einholen? Von demjenigen, der der Autor ist? Oder andersrum beispielsweise, ich verwende ein Produkt dieser Firma, prüfe es auf Sicherheit, es ist mein Eigentum, ich habe die Lizenzgebühr dafür bezahlt oder ich habe sie übernommen oder wie auch immer. Wessen Einverständnis brauche ich hier eigentlich? Also, das Einverständnis dessen, der möglicherweise unsichere Software produziert oder das Einverständnis dessen, der diese unsichere Software in seinem Computer, im Zweifel auch im Deutschen Bundestag verwendet? Das wäre die eine Frage.

Die zweite Frage nochmals an Herrn Lindner. Sie haben ja, glaube ich, in beeindruckender Form, die Folgen geschildert. Ich bin auch Vorsitzender eines Kuratoriums einer Deutschen Universität im Bereich IT-Sicherheit. Die Verunsicherung ist groß und die Befürchtung, dass unsere besten jungen Leute ins Ausland gehen, wie wir es in anderen Stellen immer wieder beklagen, ist noch größer. Herr Lindner, ich möchte Sie einfach noch mal bitten, dass Sie die fatalen Folgen dessen, was die Gefährdung der deutschen IT-Sicherheitswirtschaft im

Zusammenhang mit § 202c E-StGB angeht, noch mal über Ihre Aussagen hinaus ein bisschen präzisieren.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Ich habe jetzt keine weiteren Fragen vorliegen. Dann können wir in die Antwortrunde gehen. Wir beginnen jetzt in umgekehrter Reihenfolge und ich bitte Herrn Dr. Stuckenberg auf die Fragen der Kollegen Montag und Korte zu antworten. Bitte schön.

SV Dr. Carl-Friedrich Stuckenberg: Zu der Frage von Herrn Montag nach der unterschiedlichen Bezeichnung, einmal Computerdaten, von denen die Konvention redet und Daten, von denen der deutsche Gesetzentwurf redet. Wie sich diese Unterscheidung erklärt, ist eine gute Frage und eine einfache Antwort darauf, glaube ich, gibt es nicht, außer dass etwa die Rahmenbeschlussvorgabe, aber auch die Cybercrime-Convention spezialisiert auf Computerdaten als Sachbereich sind, während die ganzen Vorschriften wie §§ 202a, 303a StGB ja älteren Datums sind und viel weiter gefasst sind. Die Definition von Daten in § 202a E-StGB will offenbar alles was etwa datenschutzrechtlich auch interessant sein könnte, aber auch optisch und sonst irgendwie gespeichert ist, erfassen. Das Problem mit diesen Vorschriften, bei § 303a und § 303b StGB findet man es auch in der Literatur, ist, dass man gar nicht genau weiß, was eigentlich geschützt sein soll. Ich kann es Ihnen, muss ich gestehen, auch nicht recht sagen. Es wird ja diskutiert, ob schon das unbefugte Verschicken einer Diskette Datenverarbeitung in dem Sinne ist, die eventuell darunter fällt und dieser weite Begriff ist sicherlich problematisch. Das führt dann eben auch zu den Beispielen, die in der Bundesrat-Stellungnahme waren. Dann hätte man Computerdaten, hätte man mit dem MP-3-Player oder mit dem Fernseher, der da kindergesichert ist, kein Problem. Es wäre ohne weiteres möglich, diese Einschränkung vorzunehmen, aber ich sehe auch ein, dass man das offenbar in der nicht besonders, sagen wir mal, erfreulichen Tradition dieser Unklarheit jetzt eingefügt hat. Es wäre eigentlich, das ist ja auch mehrfach gesagt worden, schon lange fällig, auch bei § 303a, § 303b StGB sich zu überlegen, was will man eigentlich genau schützen. Und das heißt dann auch welche Art von Daten, denn inzwischen sind wir von Daten überall umgeben und eine Einschränkung wäre sicherlich nahe liegend. Zur Frage von Herrn Korte: Strafwürdiges und nicht strafwürdiges Verhalten gemäß § 202c E-StGB. Soweit ich das verstanden habe mit dem Anliegen der

Europaratskonvention will man versuchen, so eine Art Gefahrengutregime für bestimmte Art von Software zu errichten. Also ähnlich, wie man Waffen oder Drogen oder Sprengkörper unter Kuratel stellt, nur dass wir hier kein verwaltungsrechtliches Regime mit Erlaubnis und so fort haben, was nun wahrscheinlich erst recht nicht durchführbar ist, was eben voraussetzt, dass man eindeutig gefährliche Dinge auch benennen kann. Bei einer Handgranate ist es einfach, beim Auto ist es, haben wir gesehen schwierig, auch wenn das auch gefährlich sein kann. Es mag sicherlich Crime-Ware geben, die man eigentlich zu nichts anderem als zum Schadenanrichten verwenden kann, ich denke jetzt an irgendwelche Virenbausätze im Internet. Da ist es vielleicht auch nicht recht einzusehen, warum so etwas als Beilage zu Computerzeitschriften oder sonst frei verfügbar im Netz herumstehen sollte, denn das bringt Leute nur auf dumme Gedanken, das halte ich für nachvollziehbar. Insofern halte ich es auch für nachvollziehbar, dass man nicht von der Option Gebrauch gemacht hatte, die die Europaratskonvention eröffnet, auf diesen Teil, die Nummer 2 der Föderalisierung, zu verzichten, sondern nur den Missbrauch von Passwörtern unter Strafe zu stellen. Andererseits greift es eben weit, weil das mit der eindeutigen Zweckbestimmung so eine Sache ist. Ich denke, dass die Vorschrift auch in dem Sinne, wie der Entwurf sie angewendet sehen will, keinen großen - insofern teile ich auch die Einschätzung von Herrn Bruns - gar keinen großen Anwendungsbereich haben wird, wenn man die Einschränkungen, die hier ja ziemlich einheitlich vorgeschlagen sind, vornehmen wird. Da geht es ja nur darum, Fälle so deutlich auszuscheiden, die ja von vornherein gar nicht darunter fallen sollen. Zu dem wirklichen Bereich von der Frage, ob das dann überhaupt einen präventiven Effekt haben kann, muss ich sagen, ich verspreche mir da nicht allzu viel, aber es ist sicherlich einen Versuch wert, wenn der Versuch nicht noch Dinge en passant mitbestraft, die gar nicht gemeint sein sollen. Was übrigens die Frage anbelangt, ob das nur die deutsche IT-Wirtschaft betrifft, muss man sehen, dass auch die USA diese Europaratskonvention ratifiziert haben und sie umsetzen werden. Österreich hat es ja auch getan, aber allerdings so, dass ich glaube, dass diese Befürchtungen gar nicht aufgetaucht sind, sondern hat klarer formuliert.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Lindner auf die Fragen der Kollegen Korte und Tauss.

SV Felix Lindner: Zuerst zu der Frage von Herrn Korte. Die Debatte in der Security-Szene zum Thema § 202c bezog sich natürlich ausschließlich auf Nummer 2. Der ganze restliche Gesetzentwurf, das muss man auch mal klar sagen, war überhaupt kein Problem, denn natürlich haben wir auch ein Interesse, Computerstraftaten besser verfolgen zu könne, damit wir ein bisschen weniger Probleme haben. Wir haben schon genügend Probleme in der Computer-Security und es ist schön, wenn man dann Leute auch tatsächlich mal hinter Gitter bringen kann, dann machen die keinen Mist weiter. Das Problem dabei ist, wenn man mit irgendjemanden, der sich damit beschäftigt - egal aus welchem Land - spricht, dann kommt erstmal das pure Entsetzen und die Frage: Was soll denn das? Und die nächste Frage ist dann immer automatisch: Und wie soll ich jetzt meine Arbeit machen? Das Problem ist tatsächlich, dass niemand auch nur wirklich ein einziges Stück Software eindeutig identifizieren kann. Niemand von den Fachleuten in der ganzen Welt kann eindeutig sagen, das ist etwas, dass wirklich strafbar sein muss, wenn man sich das beschafft. Der Dr. Stuckenberg hat gerade gesagt, Crimeware sollte nicht im Internet verfügbar sein. Das wäre zum Beispiel in den Zirkeln, wo wir Crimeware auf internationaler Ebene auseinander nehmen, was eine signifikante Menge Arbeit ist, die alle Beteiligten freiwillig und ehrenamtlich machen, ein Riesenproblem, weil ich den Kollegen sagen müsste, okay, ihr habt mich in den Zirkel mit reingenommen, weil ich relativ gut Software auseinander nehmen kann, aber ihr dürft sie mir nicht mehr schicken. Es ist illegal für mich, die zu bekommen. Das Risiko ist da, Sie schütteln mit dem Kopf, aber ich habe einfach keine Lust für jedes einzelne Stück Software, was ich auf meiner Festplatte habe, dann Rede und Antwort stehen zu müssen und vielleicht am Ende keine Argumentation mehr zu haben. Das sind tatsächlich die Auswirkungen, die es in der internationalen Security-Szene gab. Zu der Frage von Herrn Tauss, zu den Auswirkungen, es gibt da fünf Punkte, die generell anzuführen sind. Der erste Punkt ist, wer macht denn eigentlich dann die Arbeit? Also wenn Sie sich mal vorstellen, eine normale Windowsinstallation, das ganz normale Stück Software Windows, was Sie sich installieren, damit Ihr Computer überhaupt funktioniert, hat eine dreistellige tausender Anzahl ausführbarer Programme. Kein Unternehmen, nicht einmal Microsoft kann es sich leisten, wirklich jedes einzelne bis ins Detail, zu überprüfen. D. h. diese ganze Sicherheitsindustrie und vor allem, das möchte ich hier auch noch mal betonen, das BSI leben davon, dass Leute freiwillig das in ihrer Freizeit machen und das Ergebnis publizieren, sonst könnten sie ihre

Sicherheits-CD nämlich gar nicht rausgeben. Security-Experten-Konferenzen bestehen ausschließlich aus Vorträgen nach dem folgenden Muster: Dies ist ein Stück Software, das wird überall eingesetzt, das ist sehr sehr kritisch, hier ist ein Sicherheitsproblem, das ist inhärent von diesem Stück Software und dies ist der Angriff. Eine solche Konferenz könnten Sie in Deutschland nicht mehr durchführen, es würde kein Mensch freiwillig eine Konferenz ausrichten und es würde kein internationaler Speaker nach Deutschland kommen, wenn er wüsste, dass nur die Möglichkeit, dass er in Kauf genommen hat, dass jemand eine Straftat mit dieser Information begeht, ihn hinter Gitter bringt. Auf gar keinen Fall. Die Unternehmen, die in Deutschland Software-Produkte herstellen, haben natürlich dann das umgedrehte Problem, dass niemand mehr herfliegen möchte, um ihre Software-Produkte zu testen. Aber auch noch eine ganz andere interessante Auswirkung: Was ist denn mit, zum Beispiel auch in Deutschland hergestellter Linux-Distribution. SUSE wäre jetzt ein schönes Beispiel, kommt aus 6, 7 CD's, eine CD ist voll mit Angriffsprogrammen, man könnte sagen, diese Programme sind ausschließlich dafür da, in Computer einzubrechen. Da sind Sniffer dabei, die ihnen die Passwörter ausgeben, die sie über das Netzwerk laufen lassen, Scanner dabei, die ihnen sagen, welche Dienste auf anderen Rechnern offen sind. Das war auch eine große Verunsicherung in den Securitykreisen, weil man einfach gesagt hat, okay, also wir wissen, was diese Tools machen und wir können auch legitim sagen, wir setzen die nicht für kriminelle Aktivitäten ein, aber was ist denn mit den tausenden Linux-Usern da draußen, die einfach einen Haken bei Security-Tools gemacht haben und sich das mitinstalliert haben. Das ist ein Produkt, was sie mitgekauft haben und das ist ein Feature, wo sollen die den Unterschied sehen. Das sind eigentlich die Hauptgefährdungen. Abschließend vielleicht noch zu dem universitären Bereich. Es ist schon ganz schön schwierig, überhaupt anständige Leute zu finden, die ein bisschen eine Hintergrundausbildung haben. Wir haben eine einzige wirklich gute universitäre Ausbildung in Deutschland, das ist an der Ruhr-Uni Bochum, die sich mit Computer-Securitiy beschäftigt. Man würde diesen jungen Leuten tatsächlich das Mittel nehmen. Wenn sie so eine Ausbildung anfangen und noch gar keine Ahnung von dem Thema haben, haben sie keine Chance, das innerhalb ihres Studiums bis zum Diplom so weit voranzutreiben, dass sie dann wirklich eine Vorstellung davon haben. Und wenn sie alleine zu Hause sitzen und ganz ohne Kontakt zur Außenwelt sich ihren Computer vornehmen, sich angucken, wie funktioniert das Ding, sich

angucken, was hat das denn für potenzielle Sicherheitsprobleme und dann anfangen, zum Beispiel einen neuen Angriff zu entwickeln und dann einer ihrer Freunde sagt: hm, das sieht aber ganz schön kriminell aus, was du da tust, könntest du damit denn nicht in folgendes Unternehmen einbrechen? Wenn Sie wahrheitsgemäß antworten: Vielleicht, keine Ahnung, könnte sein, finde ich, nach der momentanen Gesetzeslage wäre dieser junge Mann straffällig.

Vorsitzender Andreas Schmidt (Mülheim): Jetzt Herr Prof. Kudlich auf die Frage des Kollegen Manzewski.

SV Prof. Dr. Hans Kudlich: Herr Manzewski, meine Damen und Herren, die Frage war, ob Versuchstrafbarkeit auch bei § 202a E-StGB möglich, vielleicht geboten ist und wenn ja bzw. wenn nein, warum oder warum nicht. Die europäischen Vorgaben sind insoweit offener als die Cybercrime-Konvention in Artikel 11 Abs. 2, wo die Versuchstrafbarkeit grundsätzlich gefordert wird, hier den Artikel 2 aber gerade ausnimmt. Im Rahmenbeschluss ist es so, dass für den unbefugten Zugang zu den Daten zwar die Versuchstrafbarkeit genannt ist, aber auch eine Ausnahmemöglichkeit davon zugelassen wird. Das zeigt schon, dass wir im Grunde genommen in einem Bereich sind, wo wir sagen, dass ist letztlich eine rechtspolitische Entscheidung, wollen wir das machen, wollen wir es nicht. Es ist ein Grenzbereich, das zeigt auch ein Blick in die verwandten oder in die systematisch daneben stehenden Vorschriften, dass wir zum Beispiel im § 201 Abs. 4 StGB eine Versuchstrafbarkeit haben, im § 202 StGB dagegen nicht. Meines Erachtens sprechen bessere Gründe für eine Versuchstrafbarkeit. Zum einen, wenn wir den Gesamtentwurf anschauen von der Systematik her, haben wir sonst - darauf hat unter anderem Herr Stuckenberg in seiner Stellungnahme ja auch hingewiesen - im § 200c E-StGB im Grunde genommen eine Vorbereitungshandlung zu § 202a StGB, die unter Strafe gestellt wird und die Versuchstrafbarkeit ist nicht unter Strafe gestellt. Man könnte das zwar begründen, indem man sagt, § 202c E-StGB hat ein noch größeres unspezifiziertes Gefährdungspotenzial, das erklärt ja auch die unterschiedlichen Strafantragserfordernisse, aber es ist trotzdem ungewöhnlich zum einen. Das zweite ist, dass wir bisher im § 202a StGB keine Versuchstrafbarkeit haben; das mag in der alten Fassung vielleicht auch darin begründet liegen, dass ja der ursprüngliche Wille des Gesetzgebers in den 80iger Jahren war, dass bloße

Hacken, den bloßen Zugang zu diesen Systemen nicht unter Strafe zu stellen, wo man dann eben die Befürchtung hatte, dass vielleicht hier eine Versuchstrafbarkeit zum späteren Zugriff auf die Daten das Straflosstellen des bloßen Zugangs konterkarieren könnte. Wenn wir aber den bloßen Zugang auch unter Strafe stellen, dann scheint es durchaus auch konsequent, einen entsprechenden erfolglosen Angriff strafrechtlich zu erfassen. Das ist sicherlich nicht das dringendste Bedürfnis oder das dringendste Anliegen im Rahmen dieser Umsetzung, aber es erschiene mir systematisch durchaus stimmig und ich denke, es spricht mehr dafür als dagegen.
Zum § 202b E-StGB, ich habe jetzt gerade die europäischen Vorgaben dazu nicht angeschaut, gehe aber davon aus, dass die das auch nicht zwingend fordern, sonst wäre es sicherlich hier umgesetzt worden. Wenn wir uns den § 201 StGB betrachten, der ja das Abhören und die Aufzeichnung des nichtöffentlich gesprochenen Wortes regelt und der im Grunde genommen die Parallelvorschrift hier zu dem § 202b E-StGB wäre und der in seinem Absatz 4 eine Versuchstrafbarkeit kennt, dann würde es mir hier auch sogar noch konsequenter erscheinen, auch hier eine Versuchstrafbarkeit anzuraten, weil wir hier wirklich in der entsprechenden Parallelvorschrift eine Versuchstrafbarkeit haben. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Prof. Dr. Hilgendorf auf die Fragen der Kollegen Montag, Dr. Gehb und Herrn Tauss. Bitte schön.

SV Prof. Dr. Dr. Erich Hilgendorf: Die Fragen beziehen sich alle auf den § 202c E-StGB, so dass ich mich auf diese Norm beschränken kann. Es geht bei Ihnen um die Frage, warum ist diese Norm zu weit?
Also ich halte sie in der Tat für zu weit, für ganz gefährlich weit, man sollte sie einschränken. Ich habe drei Gründe für die Einschränkung. Einmal die Strafbarkeitsrisiken, das hatten Sie auch schon angesprochen, es bestehen in der Tat nicht klar überschaubare Strafbarkeitsrisiken für deutsche Unternehmen. Das hat Herr Lindner ja ausgeführt. Es bestehen aber auch, das ist mein zweiter Punkt, Strafbarkeitsrisiken für ausländische Firmen, die hier in diesem Bereich arbeiten. Wir müssen immer daran denken, dass wir nicht mehr im nationalen Raum allein tätig sind, sondern wir leben in einer globalisierten Welt und der § 202c E-StGB würde seinem Wortlaut nach wohl auch den Fall erfassen, dass im Ausland ein solches

Überprüfungsprogramm hergestellt wird, dessen Auswirkungen auf deutschen Territorium genutzt werden, zugänglich machen heißt ja der Wortlaut. Oder wenn Sie sagen, es ist ein abstraktes Gefährdungsdelikt, dann verweise ich auf die Töben-Entscheidung, wo der BGH gesagt hat: Weltweite Anwendbarkeit des deutschen Strafrechts, wenn nur irgendwelche Auswirkungen in Deutschland stattfinden. Ich habe das Urteil kritisiert, aber das ist BGH-Rechtsprechung. Also, es ist tatsächlich ein Problem. Wenn auf deutschem Territorium ein tatbestandsmäßiger Erfolg eintritt, ist deutsches Strafrecht anwendbar, selbst wenn die entsprechende Programmierungshandlung in den USA stattgefunden hat. Also, ich sehe hier die Gefahr, dass wir auch für ausländische Firmen Strafbarkeitsrisiken schaffen und das sollten wir uns wohl nicht aufladen. Und der dritte Punkt, das ist jetzt mehr ein akademischer, für die Einschränkung: Diese Norm § 202c E-StGB umschreibt nach meiner Einschätzung keinen klaren Unrechtstyp. Es ist nicht so wie bei § 212 StGB, Totschlag, oder § 242 StGB, Diebstahl, dass hier ein klarer Fall von Unrecht umschrieben wird, sondern das sind so Handlungen im Graubereich. Handlungen auch von Systemadministratoren, von Firmen, die teilweise positiv arbeiten - möglicherweise ist deren Arbeit aber auch negativ zu bewerten, aber es fehlt an der Typisierung eines klaren Unrechts. Deswegen kann die Norm auch die Wirkung, die man mit Strafrecht normalerweise verbindet, Prävention, Abschreckung, nicht wirklich gut erfüllen. Sie schreckt zu viel ab, schreckt zu viele und dass heißt, die Abschreckung wird dann abgeschwächt, es werden nicht nur die Bösen betroffen, es werden sehr viele betroffen, dass heißt die Wirkung nach außen wird diffus. Es ist also ein großes Problem für das Strafrecht, es ist letztlich ein weiteres Beispiel für diese Inflationierung von Strafrecht, die wir in den letzten 20 Jahren haben. Jetzt allgemein diese drei Punkte.

Sie hatten darauf hingewiesen, dass doch der § 202c E-StGB durchaus Ansatzpunkte hat für eine Einschränkung, im Hinblick auf Nr. 2, diese Zweckformulierung. Die Frage ist nur, haben Programme eigentlich Zwecke? Eigentlich haben Menschen Zwecke, die verfolgen sie mit den Programmen, die Programme verfolgen selber keine Zwecke, Zwecke sind etwas, was man mit subjektiven Zwecksetzungen verbinden muss. Das Programm ist also beliebig einsetzbar, je nach der Zweckrichtung dessen, der das Programm einsetzt. Deswegen ist schon der Wortlaut hier unklar und die Rechtsanwender werden große Probleme damit haben. Also ich sehe hier keine klare Einschränkung in dieser

Formulierung in § 202c Abs. 1 Nr. 2 E-StGB. Und auch das Wort „vorbereiten“ im ersten Satz. „Vorbereiten“ meint jede Forderung, jede Beihilfe im Vorfeld der Tat, das ist denkbar weit, ja, jeder kausale Beitrag, der die Tat irgendwie erleichtert, das ist vorbereiten. So würde es auch die Rechtsprechung interpretieren. Also auch hier haben wir eine sehr weite Tatbestandsfassung, so dass man wirklich unbedingt über eine Einschränkung nachdenken müsste und die könnte geschehen dadurch, dass man z. B. den Absichtsbegriff hinein nimmt, das ist eine Möglichkeit, oder man versucht objektiv nachzubessern, indem das Wort „gezielt“ eingebaut wird oder auch ein anderes Wort. Die Bedenken des Kollegen Kudlich nehme ich immer ganz ernst, vielleicht fällt ihm ja noch was Besseres ein, wie man den Tatbestand objektiv präzisieren kann. Aber so, wie er da steht, typisiert er kein Unrecht, er ist durch und durch problematisch und ein typisches Beispiel für modernes Strafrecht.
Ist das rechtspolitisch zwingend? Ich meine nicht, Sie hatten das ja selbst angedeutet, wir haben hier einen gewissen Freiraum, es ist nicht zwingend. Und Herr Tauss hatte ein weiteres Problem, das ich noch gar nicht gesehen hatte, zusätzlich noch in den Raum gestellt. Bei der Lückenüberprüfung, wer muss da eigentlich zustimmen? Der Autor, der Urheber des Programms, oder der jeweilige Nutzer, also vielleicht der jeweilige Datenberechtigte? Ich würde jetzt mal, ohne das geprüft zu haben, sagen, primär der Nutzer, der Datenberechtigte, weil der die Vollrechte vom Autor übernommen hat. Aber was ist etwa, wenn der Autor bestimmte Rechte zurückbehält und das Programm verkauft mit der Maßgabe, dass ein weiter Teil genutzt werden darf oder bestimmte Anteile des Programms nicht offen liegen sollen auch für den Käufer, dann müssen wohl beide zustimmen und dann wird es ganz problematisch. Das dazu in aller Kürze.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt bitte Herr Hange auf die Frage des Kollegen Dr. Gehb.

SV Michael Hange: Es geht darum, kann man antezipieren, ob noch gesetzlicher Handlungsbedarf gegeben ist für die Zukunft oder ob das, was an Gesetzen da ist, ausreicht. Wenn man die drei Grundprinzipien der IT-Sicherheit, also Schutz der Vertraulichkeit, Schutz der Integrität und Schutz der Verfügbarkeit sieht, ist alles abgedeckt. Aber die Entwicklung der IT-Sicherheit hängt natürlich davon ab, wie die technische Entwicklung ist. Die DSL-Anschlüsse schaffen heute ganz andere

Möglichkeiten, so genannte Denial-of-Service-Angriffe zu starten, die die Verfügbarkeit von Systemen beeinträchtigen können. Genauso ist es natürlich mit Online-Banking, da hat das Phishing-Problem eine ganz andere Dimension angenommen, so dass man, zumindest auf der technischen Seite ständig gefordert ist, neue Gefährdungen zu antezipieren, Sicherheitsvorkehrungen nicht nur technisch, sondern auch im organisatorischen Bereich zu sensibilisieren. Ob daraus sich dann gesetzlicher Handlungsbedarf ergibt, das muss man sehen. Das ist also teilweise auch ultima ratio, da muss man auch die Verhältnismäßigkeit dann sehen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Dr. Graf auf die Fragen auch des Kollegen Dr. Gehb.

SV Dr. Jürgen-Peter Graf: Zunächst auch noch mal zum § 202c E-StGB, Vorverlagerung der Strafbarkeit. Das ist sicherlich ein Problem, was man lösen muss, ich denke aber, grundsätzlich sind die Formulierungen in Absatz 1 und auch in Nummer 2 schon in der Lage, diese Bedenken auszuräumen. Also Vorbereitung einer Straftat, es ist ja schon mal ein relativ klarer Begriff, der auch in dem § 202a und § 202b E-StGB deutlich wird und dann müssen eben die Computerprogramme zum Zwecke der Begehung der Straftat hergestellt werden. Das ist ja auch ein Bereich, der im subjektiven Tatbestand mit verortet ist und der bei allem Respekt vor den theoretischen Möglichkeiten, die man sich vorstellen kann, in der praktischen Wirklichkeit einem Täter nachgewiesen werden muss, bevor man ihn dazu verurteilen kann. Natürlich besteht die Möglichkeit von Ermittlungsverfahren, die man einleiten kann, aber da muss dann auch der Staatsanwalt das erstmal bejahen. In der Praxis habe ich eigentlich keine Sorgen, dass hier zumindest für die Industrie, die diese Programme herstellt, gutwillig herstellt, eine Verurteilungswahrscheinlichkeit entsteht. Ich brauche Anhaltspunkte, die kann ich vielleicht durchaus da finden, und das wird dann vielleicht der Computerpresse wehtun, wo auf solche Programme hingewiesen wird und dann auch gleich noch Ratschläge gegeben werden, wie diese Programme angewendet werden können. Ich muss zugeben, ich bin manchmal auch versucht, solche Programme, wenn man sie mit einem Heft erworben hat, auszuprobieren. Ich kann sie allerdings im eigenen Netz ausprobieren und habe dann keine Probleme damit, aber ich denke, es gibt sehr viele Nutzer, die so etwas lesen und denken, das probiere ich jetzt mal aus. Also insofern ist die Verlockung

schon groß, wenn solche Programme angekündigt werden, auch Sniffer, und dann noch dabei steht, wie man es macht, das dann auch im Computerbereich auszuprobieren, auch im Internet auszuprobieren und dann in die Strafbarkeit zu kommen, so dass also hier vielleicht schon der Verbreitung entgegen gewirkt werden sollte. Ich halte die Vorschrift als solche nicht für falsch und bei richtiger Auslegung auch dann nicht unbedingt für zu weitgehend. Und das zweite, ob alle Facetten der Kriminalität jetzt hier erfasst sind, das weiß ich selbst nicht. Alle Fälle kennen wir nicht, ich würde mich auch hier nicht festlegen wollen, ich bin nur überrascht, was die Lebenswirklichkeit an Fällen produziert. Das hängt natürlich vom technischen Fortschritt in diesem Bereich ab und den Möglichkeiten, wieweit man ihn umsetzen kann. Aus jetziger Sicht, denke ich, sind die gängigen Probleme mit diesem Gesetzentwurf eigentlich alle erfasst.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Dr. Gercke auf die Frage des Kollegen Manzewski.

SV Dr. Marco Gercke: Die Frage war, ob man auf das Merkmal „besondere Zugangssicherung“ verzichten kann. Der erste Entwurf des EU-Rahmenbeschlusses sah überhaupt eine Einschränkungsmöglichkeit gar nicht vor. Unabhängig davon, ob die Systeme geschützt waren oder nicht, sollte das Eindringen unter Strafe gestellt werden. Da gab es Proteste. Die bezogen sich nicht nur darauf, dass man mit der Möglichkeit der Bagatellklausel ohnehin einschränken konnte, sondern es wurde eine substanzielle Einschränkungsmöglichkeit gefordert. Die wurde dann auch umgesetzt, also der Rahmenbeschluss sieht jetzt vor, ich kann als nationaler Gesetzgeber eine Einschränkung vorsehen und zwar in Form einer Schutzmaßnahme. Von einer besonderen Schutzmaßnahme spricht weder der Rahmenbeschluss noch die Konvention. Die Frage ist, wie man das auslegt, was für Anforderungen man an die Schutzmaßnahme stellt und ob es dann einen Unterschied zwischen einer besonderen und einer einfachen Schutzmaßnahme gibt. Wir haben die Problematik der Schutzmaßnahmen an unterschiedlichen Stellen, wir haben das einmal beim § 95a Urhebergesetz, wo den Gerichten völlig unklar ist, was denn jetzt die besondere Schutzmaßnahme ist. Am Anfang hieß es, das sollte schon ein effektiver Schutz sein; da den die Industrie bis jetzt nicht geleistet hat, hat man es dahin ausgelegt, „na wenn es nicht völlig unwirksam ist, dann ist es eine Schutzmaßnahme“. Es ist also

völlig ungeklärt. Im Bereich Pornografie haben wir die gleiche Diskussion. Wie können wir sicherstellen, dass Jugendliche nicht auf pornografische Inhalte zugreifen, also auch da wieder das Problem der Zugangssicherung. Es ist auch hier weitgehend offen, wie das technisch realisiert werden kann. Es gibt klare Vorgaben eines Zwei-Schichten-Modells, aber auch da ist noch vieles in Bewegung. Wir haben an mehreren Stellen diese Problematik, welche Anforderungen an die Zugangssicherung zu stellen sind. Ich würde sagen, eine normale Zugangssicherung würde ausreichen, wobei sich dann die Frage stellen würde, wenn ich in den Gesetzestext reinschreibe „... sofern keine Zugangssicherung überwunden wird“: Was ist der Unterschied zu § 202a E-StGB? Sind die Anforderungen geringer als nach bestehendem Recht oder sind sie die gleichen? Insofern bin ich der Auffassung, es macht keinen wirklichen Unterschied. Das geltende Gesetz geht von einer besonderen Schutzmaßnahme aus. Also, wenn man den Zustand beibehalten will, spricht vieles dafür, dass man die Formulierung so beibehält. Wirklich notwendig ist es nicht.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Bruns auf die Fragen der Kollegen Manzewski und Montag.

SV Michael Bruns: Die erste Frage war Versuchstrafbarkeit bei §§ 202a, 202b E-StGB, ich denke, Herr Kudlich hat systematisch dazu alles gesagt, was dazu zu sagen ist. Es ist in Tat so, es gibt auch intern im Entwurf ein gewisses Spannungsverhältnis, wenn ich unter § 202c E-StGB Vorbereitungshandlungen unter Strafe stelle, aber den eigentlichen Versuch ausnehme. Andererseits, jetzt erwarten Sie von mir bitte keine rechtspolitische Ausführung, ich bin Praktiker. Als Praktiker muss ich sagen, ich bin ganz froh, wenn da nicht der Versuch drin ist, weil die Vorschriften ohnehin schon sehr schwer nachzuweisen sind, sie sind sehr knapp an der Realität, um das mal so zu sagen, wenn ich jetzt auch noch den Versuch ausermitteln soll. Ich kann mir keinen Fall vorstellen, wo ich ernsthaft in die Situation käme, festzustellen, dass jemand versucht, sich unbefugt Zugang zu Daten usw. zu verschaffen. Also, als Praktiker würde ich emotional sagen: Bitte verschonen Sie uns damit, als Systematiker würde ich sagen: Natürlich ist es nicht sauber.
Die weitere Frage betrifft die besondere Zugangssicherung. Hier ist eine ähnliche Situation. Natürlich ist der Rechtseingriff bei dem unbefugten Zugriff auf fremde

Daten gegeben, den könnte man auch als strafwürdig ansehen. Andererseits ist es eine auch, wiederum hier für den Praktiker, eine ungeheuere Erleichterung, wenn man die Willensmanifestation des Täters noch mal zusätzlich hat, zu sehen, er hat sich tatsächlich darum bemüht, das war jetzt kein Zufall, das war nicht irgendwie en passant, dass er sich diesen Zugriff da verschafft hat, sondern er hat sich bemüht, eine Zugangssicherung zu knacken und Herr Gercke hatte das Problem mit der besonderen Zugangssicherung angesprochen. Ich verstehe das dahingehend, dass diese Frage technisch nicht zu lösen ist. Ich glaube, es ist auch nicht Aufgabe des Gesetzgebers, hier technische Standards festzuschreiben, sondern ich verstehe das hier in dem Sinne, dass es eine Zugangssicherung sein muss, die zum Schutz eben dieser Daten geschaffen wurde.

Vorsitzender Andreas Schmidt (Mülheim): Danke. Jetzt hat das Wort Herr Borges auf die Fragen der Kollegen Montag und Korte. Bitte schön.

SV Prof. Dr. Georg Borges: Es waren insgesamt drei Fragen. Ich möchte zunächst anfangen mit der Frage von Herrn Montag nach Computerdaten und Daten. Es dürfte so sein, dass der § 202a StGB, der den Begriff „Daten“ zum Beispiel verwendet, hier auf die deutsche Tradition verweist, wo wir den Begriff „Daten“ schon in vielfachem Zusammenhang verwenden, während es in anderen Staaten, insbesondere im angloamerikanischen Rechtskreis, üblich ist, von „Computerdaten“ zu sprechen, also eine engere Fassung, so dass ich vermute, dass die unterschiedliche Diktion einfach auf unterschiedlichen Traditionen in der sprachlichen Fassung beruht. Richtig ist, dass der Begriff der Daten im deutschen Recht ja viel weiter ist und auch nicht elektronische Speicherungen von Daten einschließt.
Vielleicht darf ich an dieser Stelle eine Bemerkung einfließen lassen zu den verschiedenen Stellungnahmen im Zusammenhang mit Phishing. Gibt es einen Grund für spezielles Strafrecht, Online-Strafrecht, oder sollte man alle Straftatbestände allgemein fassen? Hierbei ist zu berücksichtigen, dass das Internet bestimmte Delikte in besonderer Weise fördert. Natürlich gab es immer schon die Möglichkeit der Passwort-Erschleichung, aber nur im Internet ist es interessant. Betrügereien im Bankbereich gab es immer schon, aber erst das Internet und das Online-Banking machen Delikte wie Phising zu einer Milliarden-Industrie und zu einem Gegenstand weltweit organisierter Kriminalität. Deswegen gibt es gute

Gründe, meine ich, nicht dogmatischer Art, aber strafrechtspolitischer Art, Computersachverhalte, Online-Delikte anders zu behandeln und vielleicht hier schon eine weitergehende Pönalisierung einzuführen als man es bei parallelen Sachverhalten machen müsste, die außerhalb des Internets stattfinden.

Die zweite Frage betrifft § 202c E-StGB, die Bestimmtheit und die Unterscheidung zwischen strafwürdigem und nicht strafwürdigem Verhalten, auf die Herr Stuckenberg ja schon geantwortet hat. Hier ist es so, dass die Einschätzung von Herrn Stuckenberg, glaube ich, ganz richtig ist, dass die Konvention so eine Art Gefahrgutbereich für Software schaffen will, bei dem besondere Anforderungen gelten. Die Umsetzung des § 202c E-StGB würde genau dieses Ziel wohl auch erreichen, sie würde im objektiven Tatbestand dazu sogleich einen großen Teil der Dual-Use-Software schon ausschließen, so dass für einen bestimmten Bereich besonders kritischer Software nur noch der Vorsatz maßgeblich wäre. Ein Beispiel dafür sind Trojaner. Wenn Sie einen Trojaner entwickeln, dann ist das keine Dual-Use-Software, das ist Software, die vorrangig bestimmt ist um Straftaten zu begehen. Solche Software sollte in der Tat nur mit besonderen Vorsichtsmaßnahmen kursieren können. Hier sollte in der Tat auf der subjektiven Ebene durch den subjektiven Tatbestand klargestellt sein, dass es sich hier um legale Verwendung handelt. Deswegen finde ich es besonders richtig, Trojaner und ähnliche rein kriminelle Software von Dual-Use-Software objektiv zu unterscheiden. Dual-Use-Software, Herr Lindner hat es gesagt, Herr Kudlich hat es wiederholt, wir haben beispielsweise Passwort-Scanner und Sniffer, die von Netzwerkadministratoren routinemäßig verwendet werden. Und das führt zur nächsten Frage von Herrn Montag, seine Bitte um Präzisierung einer objektiven Einschränkung des Tatbestandes. Hier liege ich im Grunde ganz auf der Linie vieler Vorredner, insbesondere von Herrn Stuckenberg und Herrn Hilgendorf, die ganz ähnliche Dinge vorgeschlagen haben in ihren schriftlichen Stellungnahmen. Und zwar meine ich, sollte man in Übereinstimmung mit Herrn Stuckenberg ansetzen an dem Wortlaut der Konvention. Die Cybercrime-Konvention spricht hier von ‚primarely designed', das könnte man durch die schlichte Einführung von ‚vorrangig bestimmt für" übernehmen. Vorrangig bestimmt für die Begehung von Straftaten sind nicht Passwort-Scanner, sind nicht Sniffer und andere Programme, die in der schriftlichen Stellungnahme von Herrn Lindner ganz sorgfältig aufbereitet worden sind. Trojaner, die speziell gestaltet sind, um Passwörter von Banken auszuspionieren und damit vollautomatisch Überweisungen zu fälschen, die

würde ich allerdings sehr objektiv natürlich da einordnen, völlig unzweifelhaft. Wir haben ja jetzt zu tun mit solchen Trojanern, die analysiert werden von Leuten wie Herrn Lindner oder unseren Technikern an der ai3, an der Ruhr-Uni Bochum ist das der Lehrstuhl des Kollegen Schwenk, Netzwerk Datensicherheit, was die dort machen ist legales Hacken. Es gibt ein Labor, weil man es eben außerhalb nicht tun darf, in dem solche Programme getestet werden und alle Software-Techniker, die sich da mit den Dingen befassen tun, ähnliche Dinge. Man analysiert solche Trojaner, versucht sie vielleicht, und kommt mit ihnen in Berührung und diese Trojaner sind Crime-Ware, sind keine Dual-Use, Herr Lindner. Sie werden mir zustimmen, das ist keine Dual-Use-Software und die sollte man sicherlich nicht auf eine offene Web-Site stellen und zum Download für jedermann bereitstellen, weil damit Anreize für kriminelle Handlungen geschaffen werden. Durch diese objektive Einschränkung wird eine bestimmte Art von Software in einen potenziell kriminellen Bereich gestellt. Um hier die Entwicklung der Software nicht zu beeinträchtigen, müsste man auf einer zweiten Stufe den Vorsatz, den subjektiven Tatbestand klar fassen. Hier hat der Kollege Hilgendorf die Beschränkung auf Absicht vorgeschlagen, ich würde in Übereinstimmung mit Herrn Stuckenberg ‚Absicht' oder dolus directus ersten Grades vorschlagen. In der Sache sind wir uns da, glaube ich, einig, das ist eine rein dogmatische Frage. Also ein Formulierungsvorschlag, wie er, glaube ich, in den schriftlichen Unterlagen von Herrn Stuckenberg vorkommt: „Wer wissentlich oder in der Absicht" eine Straftat vorbereitet, das wäre die erforderliche Verengung des subjektiven Straftatbestandes.

Mit diesem Verbleiben, mit diesen Einschränkungen, würde der § 202c E-StGB die Befürchtungen, die wir sehr ernst nehmen aus der Industrie, glaube ich, im Großen entkräften. Hierzu ist zu sagen, dass diese Befürchtungen durchaus ernst zu nehmen sind. Wir haben im Mitgliederbereich und auf der Web-Site der Arbeitsgruppe Identitätsschutz im Internet eine ganze Reihe von Stellungnahmen aus der Praxis zusammengefasst, die genau das widerspiegeln, was Herr Lindner gesagt hat. Es gibt ein erhebliches Maß an Unsicherheit bei Software-Entwicklern und Sie wissen sicherlich, dass Sicherheitssoftware von vielen Menschen neben ihrer normalen Tätigkeit entwickelt wird und dass gerade Open-Source-Software darauf angewiesen ist, dass es auch weiterhin so bleibt. Deswegen meine ich, sollte man nicht darauf vertrauen, dass die Rechtsprechung es schon richten wird. Wenn der BGH in einem Jahr darüber zu befinden hat, wird er, darauf vertraue ich ganz fest, den § 202c E-

StGB schon sachgerecht auslegen, aber wenn man die Chance hat, rechtspolitisch schon im Vorfeld mit einer klaren Fassung eines Gesetzes, eines Straftatbestandes, diese Arbeit zu leisten, dann sollte man diese Chance nicht vorübergehen lassen. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Wir treten dann in die zweite Fragerunde ein. Zu Wort gemeldet hat sich zunächst der Kollege Manzewski.

Dirk Manzewski (SPD): Ich meine, Herr Prof. Borges, was Sie jetzt angesprochen haben, beleuchtet ja wohl das größte Problem im Zusammenhang mit diesem Gesetzesentwurf und deswegen möchte ich auch da noch mal nachfragen, weil man natürlich nicht von der Hand weisen kann, dass Herr Lindner da wirklich ein Problem angesprochen hat. Dazu würde ich würde gerne noch Herrn Bruns und Herrn Dr. Stuckenberg hören, ob die das genauso sehen. Ob Sie auch der Auffassung sind, dass bei der jetzigen Form des § 202c E-StGB zum Beispiel die IT-Sicherheitsbranche ihren Aufgaben nicht mehr nachkommen könnte. Bitte auch die Vorbereitungshandlung einbeziehen. Die kennen wir ja auch aus anderen Gesetzen, unter anderem gibt es einen Passus in einem ganz anderen Gesetz, im § 22b StVG, da geht es um den Missbrauch von Wegstreckenzählern und Geschwindigkeitsbegrenzern. Das klingt erstmal uninteressant, wird jetzt aber interessant, weil das Bundesverfassungsgericht eine Entscheidung getroffen hat im letzten Jahr, dass die Tachomanipulation eben nicht das Bereitstellen der entsprechenden Software umfasst, was ich hochinteressant finde. Wenn ich dies wiederum berücksichtige bei dieser Problematik, müsste ich doch eigentlich erst recht bei IT-Sicherheitssoftware zu dem Ergebnis kommen, dass hier doch die Bedenken von Herrn Lindner möglicherweise gar nicht bestehen können, weil das Bundesverfassungsgericht sich in einem anderen Zusammenhang schon relativ weit herausgetraut hat. Hierzu würde ich gerne Ihre Einschätzung hören. Die zweite Frage richtet sich an Herrn Kudlich und an Herrn Gercke und betrifft den § 202b E-StGB, da würde ich gerne von Ihnen wissen, ob Ihrer Auffassung nach der Tatbestand des Abfangens von Daten auf solche Tathandlungen beschränkt werden sollte, die eben in der Absicht vorgenommen werden, sich unbefugt Daten aus einer nichtöffentlichen Übermittlung zu verschaffen und ob Sie in dem Zusammenhang der

Auffassung sind, dass in der jetzigen Form dieser Tatbestand zu weit gefasst ist und im Grunde genommen zu einer Überkriminalisierung führen würde.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Herr Tauss.

Jörg Tauss (SPD): Ich will Sie noch mal, einfach damit ich es verstehe, mit einem praktischen Problem aus dem Leben des Abgeordneten Tauss behelligen. Die Frage geht an Herrn Bruns und an Herrn Hange. Praktisches Beispiel jetzt einfach, weil die Staatsanwaltschaft Karlsruhe immer besonders eifrig ist, wenn es um Ermittlungen gegen mich geht. Die Staatsanwaltschaft Karlsruhe wird mit folgendem Problem konfrontiert. Ich war Weihnachten und Neujahr in einem Workshop, in dem eine Videoanlage eines Privatmannes geknackt worden ist. Man ist eingedrungen in das System und zur großen Überraschung aller standen wir plötzlich im Wohnzimmer des Betroffenen, wo er gerade mit seiner Familie zu Abendessen aß. Wir haben ihn natürlich höflicherweise darauf aufmerksam gemacht, dass er vielleicht sinnvollerweise die Kamera dann doch eher nach außen richtet, weil ich vermute, wenn er mehr Sicherheit will, will er eher sein Gelände überwachen als seine eigene Familie beim Abendessen. Was habe ich getan oder was haben andere getan? Ich will mich ja nicht in Schwierigkeiten bringen. Also, andere haben es getan und mich interessiert, wie würde es ganz praktisch jetzt aussehen, wenn Sie mit diesem Fall des Abgeordneten Tauss konfrontiert wären. Ich mache ohne Einwilligung des Videogeräteherstellers, der mit Sicherheit seine Einwilligung nicht gegeben hätte, diesen kleinen Check. Ich habe auch nicht die Einwilligung der Familie, ich wusste gar nicht, dass es die überhaupt gibt und ich stand bei denen im Wohnzimmer. Kann ich damit rechnen, dass sie mich nur löblicher Absichten bezichtigen und mich ungeschoren davonkommen lassen, denn die Videofirma war im nachhinein zumindest ganz dankbar, dass man sie auf diese Lücken hingewiesen hat. Ich habe es ja vorsichtig formuliert, es könnte ja sein, dass ich dabei war. Der zweite Punkt, Herr Hange, es wurde darauf hingewiesen, dass vieles, was in Ihrem Haus dann auch zu einer Empfehlung führt, nicht von Ihnen selbst entwickelt worden ist, sondern von außen, aus der „Szene“, an Sie herangetragen wurde. Wie viel zusätzliches Personal bräuchten Sie eigentlich, um das, was hier durch andere bis hin zum Chaos-Computer-Club und wie gesagt von Menschen, die da in Workshops zwischen Weihnachten und Neujahr sich mal Videodinge angucken, gemacht wird,

wenn Sie alles selbst machen müssten? Im Gesetz steht ja, es würde keine Kosten verursachen. Würden Sie in der Lage sein, dies zu bewerten und wie bewerten Sie darüber hinaus die Aussage von Herrn Paulis von der SAP, der sagte: Ich würde nie im Leben auf die Idee kommen, den Chaos-Computer-Club - bleiben wir mal beim praktischen Beispiel, weil ich es ja verstehen will - zu bitten, unsere Sicherheit zu überprüfen. Aber wenn wir Hinweise kriegen vom Chaos-Computer-Club, das wäre ja schon fast ein Problem für SAP, wenn sie sagen, wir gehen da nach draußen und bitten den Chaos-Computer-Club, das werden sie nicht tun, aber nehmen wir mal an, sie sind dankbar für einen Hinweis, den sie bekommen haben. Sie haben nie ihre Einwilligung gegeben, wie würden Sie denn diesen Sachverhalt dann beurteilen, auch was künftige Fälle angeht.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Tauss, wobei ich darauf hinweisen will, dass eine Rechtsberatung für Herrn Tauss heute nicht stattfindet. Herr Kollege Montag.

Jerzy Montag (BÜNDNIS 90/DIE GRÜNEN): Das wäre auch nach dem neuen Entwurf eines Rechtsdienstleistungsgesetzes honorarpflichtig. Meine erste Frage an Herr Kudlich und an Herrn Hilgendorf. In dem Rahmenbeschluss steht an mehreren Stellen, so zum Beispiel in Artikel 2, dass von den einzelnen Staaten eine Strafbarkeit gefordert wird für bestimmte Vorgänge oder Sachverhalte und dann kommt immer die Einschränkung: Wenn kein leichter Fall vorliegt. Von dieser Einschränkungsmöglichkeit macht der Entwurf, so weit ich das verstanden habe, an keiner Stelle Gebrauch. Würden Sie uns empfehlen davon Gebrauch zu machen, indem wir leichte Fälle schon tatbestandlich ausschließen oder die Möglichkeit vorsehen, in leichten Fällen von Strafe abzusehen oder in irgendeiner anderen Formulierung auf diese Möglichkeit einzugehen? Und die zweite Frage ist, wir haben im § 202a E-StGB, wenn ich das jetzt richtig verstanden habe, eine Verdreifachung des Strafrahmens von einem Jahr auf drei Jahre und beim § 303b Abs. 4 E-StGB einen Strafrahmen von sechs Monaten bis zehn Jahren. Diese Strafrahmen sind durch den Rahmenbeschluss nicht gefordert. Meine Frage ist, sehen Sie eine praktische Notwendigkeit so drastisch in den Strafrahmen hochzugehen. Hat es in der Praxis Probleme gegeben mit dem bisherigen Strafrahmen des § 202a StGB? Meine zweite Frage geht an Sie, Herr Stuckenberg, und zwar geht es um das

Problem der so genannten elektronischen Massenproteste. Eine Organisation, wie Greenpeace oder irgendeine andere, fordert die Bürgerinnen und Bürger auf, sich bei einem Ministerium oder bei irgendeiner anderen Institution mit E-Mails zu beschweren. Sehen Sie in dem Entwurf eine Kriminalisierungsgefahr für solche politischen Aktionen oder halten Sie das für ausgeschlossen?

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Abschließend Herr Korte.

Jan Korte (DIE LINKE.): Ich habe zwei Fragen, die erste an Herrn Hilgendorf und an Herrn Stuckenberg. Anschließend an Herrn Montag zu § 303 b E-StGB und zwar inwieweit Sie das für vereinbar mit dem Bestimmtheitsgrundsatz halten. Herr Montag ist darauf eingegangen, sowohl was das Strafmaß angeht, aber auch die recht weite Fassung, da heißt es „... nach dem beispielsweise demjenigen bis zu zehn Jahren Freiheitsstrafe drohen“ und dann „... der eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich stört, wenn diese für das Unternehmen von wesentlicher Bedeutung ist und er einen Vermögensverlust großen Ausmaßes herbeiführt.“ Dazu würde mich Ihre Einschätzung interessieren, ob das eigentlich mit dem Bestimmtheitsgrundsatz vereinbar ist. Eine zweite Frage habe ich an Herrn Lindner, ableitend aus dem, was Herr Hilgendorf eben zu den möglicherweise internationalen Auswirkungen gesagt hat. Ich hätte gerne noch mal von Ihnen als Praktiker eine Einschätzung, inwieweit jetzt schon dieser vorliegende Gesetzentwurf in Debatten, die natürlich auch in der Szene und publizistisch stattfinden, wie Sie dargestellt haben, wirklich konkrete Auswirkungen hat oder eben auch nicht.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Ich habe jetzt keine weiteren Fragen vorliegen, dann gehen wir jetzt in die zweite Antwortrunde und es beginnt Herr Bruns auf die Fragen der Kollegen Manzewski und Tauss.

SV Michael Bruns: Vielen Dank. Die Frage von Herrn Manzewski war, ob die Besorgnis der IT-Sicherheitsindustrie hier als berechtigt anzusehen ist oder nicht. Ich muss sagen, Sie sprechen da ein ganz wesentliches Problem an, nämlich das Problem, dass sich unsere Rechtssprache zunehmend vom Alltag entfernt. Dass diese Vorschrift natürlich von juristischen Laien ganz anders verstanden wird und

hier ein scheinbares Gefahrenpotenzial aufbaut, was aus meiner Sicht juristisch nicht zu sehen ist, das, denke ich, muss man sehr ernst nehmen, weil das auch durchaus Folgen haben kann, wie Herr Lindner ja eindrucksvoll geschildert hat. Ich denke, dass diese Besorgnisse nicht angebracht sind. Der § 202c E-StGB hat zwei Filter, der erste Filter ist die „Vorbereitung einer Straftat“. Der Täter muss ja vorsätzlich handeln, eventualdolus reicht, aber das heißt, dass er billigend in Kauf nehmen muss, eine Straftat vorzubereiten. Das ist keine Fahrlässigkeit, das heißt, es muss eben nicht sozusagen en passant passieren, dass er da etwas auf den Markt wirft, was möglicherweise auch zu Straftaten verwendet wird, sondern er muss das in sein Bewusstsein aufgenommen haben und er muss das billigen. Er muss nur nicht konkret wollen, dass es jetzt zu einer Straftat kommt, aber ich denke, die Stufe ist relativ hoch. Und der zweite Filter, das sind Computerprogramme, deren Zweck die Begehung einer solchen Tat ist. Natürlich, ich habe es ja vorhin gesagt, der objektive Zweck eines Computerprogramms ist, das zu erledigen, wofür es geschrieben wurde. Also, von daher ist es sprachlich etwas schwierig, aber wenn man es in die Rechtsprache übersetzt, dann kommt auch hier das subjektive Element rein, dass nämlich derjenige, der so etwas herstellt, nachweislich in der Absicht handeln muss, dieses Computerprogramm zum Zwecke der Begehung von Straftaten herzustellen. Ich denke, diese beiden Filter reichen, mir jedenfalls als Praktiker. Herr Tauss hat natürlich gleich in die Tiefen der Probleme reingegriffen, indem er hier nicht einfach Computerdaten genommen hat, sondern Videodaten. Ich sehe hier eigentlich schon mal den § 202a StGB gegeben, er hat sich Zugang zu Daten, die nicht für Ihn bestimmt sind und gegen unberechtigten Zugang besonders gesichert sind, verschafft. Und das, denke ich, ist auch richtig so. Jetzt ist die rechtliche Lage so, dass das dann verfolgt wird, wenn der Herr oder die Familie, die Sie da im Wohnzimmer beobachtet haben, der Auffassung sind, dass die Staatsanwaltschaft sich darum kümmern sollte und einen entsprechenden Strafantrag stellt. Und das halte ich für richtig. Sie haben hier tief in die Rechtsphäre eingegriffen und ich denke, dann sollte der Berechtigte die Möglichkeit haben, darüber zu entscheiden. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Ich würde sagen, wir machen jetzt mit der Anhörung weiter. Das Wort hat der Herr Dr. Gercke auf die Frage des Kollegen Manzewski.

SV Dr. Marco Gercke: Herr Manzewski, bitte erlauben Sie eine Rückfrage. Hatten Sie an eine bestimmte Absicht gedacht oder bezog sich Ihre Frage allgemein darauf? Also, zunächst einmal sieht die Konvention die Möglichkeit vor, eine entsprechende Einschränkung vorzunehmen, also eine unredliche Absicht kann ich als zusätzliches einschränkendes Merkmal fordern. Die Frage ist, ob das Sinn macht? Ich würde sagen, es macht dann Sinn, wenn das Risiko besteht, dass ich in einem Graubereich solche Daten empfange oder mir solche Daten verschaffe, ohne dass ich das eigentlich möchte oder ohne dass man diesen Bereich wirklich kriminalisieren möchte. Wir haben die erste Einschränkung dadurch, dass es eine nicht öffentliche Übertragung sein muss, das bedeutet, wenn Leute ihre Daten im Umkreis von 300 m mit ihrer W-LAN-Station verteilen, muss man also überlegen, wenn die ungeschützt sind, ob man dann wirklich noch von einer nichtöffentlichen Datenübertragung spricht. Das bedeutet, dieser Bereich, der mir spontan eingefallen ist, um den auszuschließen, reicht meines Erachtens das Merkmal der nichtöffentlichen Übertragung. Meine Phantasie, muss ich gestehen, reicht jetzt nicht aus, um mir andere Fälle vorzustellen, wo ich sagen würde, also da besteht wirklich ein Risiko, dass bei einer legitimen Nutzung gleichwohl die Möglichkeit besteht, dass ich den § 202a E-StGB verwirkliche, wenn ich einen dolus eventualis ausreichen lasse.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Hange auf die Frage des Kollegen Tauss.

SV Michael Hange: Es sind zwei Fragen gewesen. Die erste Frage, die Herr Bruns schon beantwortet hat, wo es darum ging, wenn man aus sportlichem Ehrgeiz getrieben, einen Penetrationstest, hier mit einer Videoanlage, durchführt. Das kennzeichnet etwas die Entwicklung. Früher hatten wir den Typus des 16jährigen Freaks, der versucht hat, in Systeme einzudringen und dann die Visitenkarte hinterlassen hat und damit gesagt hat, ich war hier, und weiter nichts ‚verbrochen' hat. Aber auch das ist durchaus, ich sage mal, auch strafwürdig gewesen. Heute haben wir ja eindeutig eine Entwicklung, dass, sagen wir mal, die kriminelle Energie, die hinter solchen Attacken steht - zum Beispiel Phishing ist eindeutig kriminell -, dass die wesentlich stärker in den Vordergrund steht. So dass dort leichter auch zu erkennen ist, ob ein Straftatbestand vorliegt. Das vielleicht zur ersten Frage,

ansonsten gilt, wo kein Kläger, da kein Richter. Also, wenn die Familie sich gestört fühlt, dann wird sie sicherlich rechtliche Schritte einleiten, ansonsten wird sie es vielleicht als Hinweis verstehen. Aber ich sage noch mal, Penetrationsversuche dieser Art gehören durchaus auch zum Geschäft von Consultingfirmen, aber das findet immer im Einverständnis mit dem Betreiber der Informationstechnik statt. Dann hat das eine andere Qualität.
Die zweite Frage war die nach der Arbeitsteilung zwischen BSI und der IT-Sicherheitsindustrie. Also die IT-Sicherheitsindustrie ist für uns zentral, es gibt entsprechend dem gesetzlichen Auftrag - grob gesprochen - die Aufteilung: Wir sind der Dienstleister für die Bundesverwaltung, für die Verwaltung. Nach dem Subsidaritätsprinzip ist die Industrie mit konkreten Dienstleistungen für sich selbst zuständig. Gleichwohl bedeutet das, dass wir uns zusammensetzen, wir haben zum Beispiel das Standardwerk, das Grundschutzhandbuch zusammen mit der Industrie entwickelt und es finden laufend auch Treffen statt. Zum Beispiel der Sicherheitskongress, wo man sich austauscht, wo man sich auch als Bundesamt kritisch hinterfragen lassen muss, ob diese oder jene Maßnahme auf technischer Ebene jetzt korrekt ist, aber das gehört zum Geschäft. Also Sicherheit in dem Sinne, auf technischer Ebene, kann nicht nur von einer Bundesbehörde vorgeschrieben sein. Sie haben Recht, es ist, wie Herr Lindner schon sagte: Kompetenz und Vertrauenswürdigkeit spielen eine zentrale Rolle, wobei man schon den Fall hatte, dass sich ein Saulus zum Paulus gewandelt hat, dass es Personen gibt, die sich mal irgendwo als Hacker hervorgetan haben und durchaus später auch als Sicherheitsexperten eingesetzt wurden. Aber das hängt vom konkreten Fall ab, das waren mehr die sportlich getriebenen Hacker aus den 80ger Jahren. Also heute würde ich das auch mehr oder weniger ausschließen.

Vorsitzender Andreas Schmidt (Mülheim): Jetzt bitte Herr Prof. Hilgendorf auf die Fragen der Kollegen Montag und Korte.

SV Prof. Dr. Dr. Erich Hilgendorf: Zunächst zu dem Problem Erfassbarkeit von leichten Fällen. Ich sehe hier an sich keine Möglichkeit, leichte Fälle separat zu erfassen. Unserer Tradition im Strafrecht entspricht es, besonders schwere Fälle in Regelbeispielen zu erfassen, für die Erfassung von leichten Fällen gibt es das Bagatellprinzip, das man gelegentlich anwenden kann. Ich sehe große

Schwierigkeiten darin, tatbestandlich einen leichten Fall adäquat zu erfassen. Schon der Ausdruck „wesentliche Bedeutung“, der hier schon mehrfach angesprochen wurde, zeigt da, wie schwer das ist auch mit Blick auf den Bestimmtheitsgrundsatz, obwohl ich grundsätzlich der Ansicht bin, leichte Fälle sollten nicht erfasst werden, aber die rechttechnische Umsetzbarkeit ist sehr problematisch. Bei den Strafrahmen § 202a, § 303b Abs. 4 E-StGB; also in der Tat, gerade bei § 303b Abs. 4 E-StGB ist der Strafrahmen, ich würde nicht sagen bedenklich, aber eine Freiheitsstrafe bis zu zehn Jahren, das ist doch eine ziemlich beachtliche Strafe, rechtfertigbar ist das mit Blick auf die Nummer 3, Beeinträchtigung „der Versorgung der Bevölkerung mit lebenswichtigen Gütern“. Hier ist offenbar an so etwas wie Cyber-Terrorismus gedacht, was ja zum Glück noch nicht stattgefunden hat. Insofern kann man diesen Strafrahmen rechtfertigen, aber er ist doch etwas baufällig.

Zum Bestimmtheitsgrundsatz, Herr Korte, Sie sprachen, wenn ich es nicht falsch verstanden habe, von § 303 StGB, aber Sie meinen sicher §§ 303a und 303b StGB. Bei § 303a StGB sind ja in der Tat von hochrangigen Kommentatoren im Leipziger Kommentar Bedenken geäußert worden, hier steht nur drin „Wer rechtswidrig Daten löscht ...“, da sind beliebige Daten gemeint. Was ist nun, wenn man „eigene“ Daten löscht? Das Problem, was dahinter steht, ist das Problem der Verfügungsberechtigung über Daten. Das ist immer noch nicht gelöst. Das ist nicht ganz klar, wonach sich das richtet. Das ist kein Sachenrecht im klassischen Sinn, manche Kollegen stellen auf einen Skripturakt ab, also das erste Abspeichern dieser Daten, aber auch das hat sich noch nicht durchgesetzt. Immerhin ist zu konstatieren, dass in den letzten 20 Jahren es hier offenbar keine großen Probleme in der Praxis gegeben hat und insofern denke ich, kann man das Problem bei § 303a StGB jetzt erstmal offen lassen und auf die Weisheit des BGH und der Oberlandesgerichte vertrauen, die hier bisher ordentlich judiziert haben. Zu § 303b, gerade die „wesentliche Bedeutung“, das ist natürlich ein relativ unpräziser Ausdruck, was heißt wesentlich? Gerade Studienanfänger tun sich damit schwer. Ältere Juristen, Strafverfolger können auf die Tradition zurückgreifen, die sich in der Rechtsprechung in den letzten 20 Jahren seit 1986 entwickelt hat. Insofern ist zu konstatieren: Tatsächlich, wir haben ein Problem mit dem Bestimmtheitsgrundsatz, aber die Praxis hat sich bisher vernünftig gezeigt und darauf können wir weiterhin bauen. Wenn die Möglichkeit bestünde, hier präzisere Begriffe zu verwenden, wäre das sicher erfreulich. Das ganze, um mal an Herrn Bruns anzuknüpfen, ist ein Zeichen dafür,

dass die Rechtsprache sich in der Tat vom Alltagssprachgebrauch entfernt. Das ist tatsächlich so. Das ist aber durchaus problematisch, denn Strafrecht soll ja für den Normalbürger verständlich sein, er soll ja erkennen können, was ihm erlaubt ist und was ihm bei Strafe verboten ist. Deswegen sollte der Gesetzgeber, wenn irgend möglich, die Tatbestände so fassen, dass sie auch für den Normalbürger, für den Nichtprofessor, verständlich bleiben.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Prof. Kudlich auf die Fragen der Kollegen Manzewski und Montag.

SV Prof. Dr. Hans Kudlich: Ich möchte mit der Frage von Herrn Manzewski anfangen. Ich kann mich im Grundsatz eigentlich dem anschließen, was Herr Gercke ausgeführt hat. Vielleicht noch ergänzend dazu, wenn wir jetzt insbesondere abstellen auf die Möglichkeit des Abfangens in unredlichen, bösartigen usw. Absichten oder wie sie eben in Artikel 3 der Cybercrime-Convention formuliert ist, haben wir auch in den, wenn ich es mal so nennen darf, Paralleltatbeständen - also § 201 StGB, Abhören des nichtöffentlich gesprochenen Wortes und § 202 StGB, Verletzung des Briefgeheimnisses - keine entsprechenden Einschränkungen. Ich persönlich sehe eigentlich als Strafrechtler kein Erfordernis einer Differenzierung, ich meine, das geht wahrscheinlich jedem anders, aber für mich ist es so, dass in meiner Lebenswirklichkeit - und das wird vielen Leuten so gehen - eigentlich gerade diese Kommunikation über elektronische Medien, über E-Mails eine besonders herausgehobene Rolle spielt und man hier eigentlich sogar im Grunde genommen ein besonders herausgehobenes Vertrauen in die Unversehrtheit dieser Kommunikation hat. Also, wenn ich jetzt - es ist egal, ob es eine Universität oder ein Unternehmen ist - an eingehende Post denke: Dort ordnet und vorsortiert nicht selten eine Sekretärin die Post, während es bei den E-Mails das zwar auch gibt, aber es häufig so ist, dass doch jeder zumindest auch seinen eigenen persönlichen E-Mail-Account hat, den dann nur er öffnet. Hier wird gelacht, Sie meinen, das ist naiv? Möglicherweise, aber wenn man darüber nachdenkt, muss einem klar sein, dass es irgendwelche Leute gibt in den Rechenzentren, die theoretisch alle diese E-Mails lesen könnten. Aber ich sehe keine niedrigere Schutzwürdigkeit dieser Kommunikation, deswegen auch kein zusätzliches Einschränkungserfordernis.

Die Fragen von Herrn Montag bezogen sich zum einen auf den leichten Fall, zum anderen auf den Strafrahmen. Bei dem leichten Fall sehe ich das im Grunde genommen ähnlich wie Herr Hilgendorf, nur würde ich vielleicht ergänzen, dass wir in den Straftatbeständen teilweise Formulierungen haben, wie eben das Erfordernis der besonderen Sicherung, des Einsatzes technischer Mittel in § 202b E-StGB usw., in denen also zusätzliche, die Strafbarkeit schärfer konturierende Tatbestandsmerkmale enthalten sind, die dann vielleicht schon zum Teil die leichten Fälle ausschließen. Ich könnte mir vorstellen, dass das im Grunde genommen auch der Sinn dieser Klauseln ist. Dass sie dem nationalen Gesetzgebern eben ermöglichen sollen, bestimmte Kriterien zu finden oder dass es auch etwa im praktischen Umgang mit den Straftaten – vorhin sind ja mehrfach die 153 ff. StPO angesprochen worden – für den nationalen Gesetzgeber eine Möglichkeit gibt, für die nationalen Strafverfolgungsbehörden die Dinge irgendwie so zu regeln, wie das bei uns üblich ist, ohne dass wir deswegen jedes Mal einen Verstoß gegen die europäischen Vorgaben hätten. Aber einen speziellen Umsetzungsbedarf – hier müsste ein tatbestandlicher, ohnehin schwer zu formulierender Ausnahmetatbestand oder eine Ausnahmeklausel geschaffen werden – würde ich nicht sehen.

Hinsichtlich des Strafrahmens des § 202 a E-StGB muss ich gestehen, bin ich mir nicht sicher, ob ich das mit der Verdreifachung möglicherweise missverstanden habe, denn wir haben doch schon in der gegenwärtigen Fassung eine Strafandrohung von bis zu drei Jahren und in der neuen Fassung ist sie auch bis zu drei Jahre. Also beim § 202a E-StGB sehe ich jetzt den Unterschied nicht, man könnte natürlich sagen, selbst wenn es gleich bleibt, wir haben im Grunde genommen eine Vorverlagerung der Strafbarkeit ins Vorfeld, dem bloßen Zugang, nicht mehr nur das Sich-Verschaffen, und haben dann trotzdem hier den gleichen Strafrahmen. Damit sind dann die Sich-Verschaffungsfälle nach wie vor erfasst. Ganz generell ist es ja so, das wissen Sie alle, dass die Strafrahmen regelmäßig nicht ausgeschöpft werden. Sie sind auch nicht dazu da, dass sie in den meisten Fällen ausgeschöpft werden, sondern dass man eben einen Spielraum hat für besonders gravierende Fälle und da würde ich hier meinen, dass das jetzt beim § 202a E-StGB an sich noch unproblematisch ist. Beim § 303b Abs. 4 E-StGB hätte ich persönlich allenfalls etwas Bauchschmerzen bei dem Regelbeispiel mit den relativ hohen Strafrahmen der banden- und gewerbsmäßigen Begehung. Woran liegt das?

Im Grunde genommen ist § 303b E-StGB seiner systematischen Stellung nach eine besondere Form der Sachbeschädigung bezogen auf Computerdelikte. Und dass wir einen besonders schweren Fall einer Sachbeschädigung mit diesem enormen Strafrahmen belegen, das ist doch etwas Außergewöhnliches. Wenn wir in die anderen beiden Regelbeispiele hineinschauen: zu Nummer 3 hat Herr Hilgendorf schon gesagt, wenn die Versorgung der Bevölkerung gefährdet ist, ist der Strafrahmen nachvollziehbar; der Vermögensverlust großen Ausmaßes (Nummer 2), das kennen wir zumindest auch aus anderen Straftatbeständen, etwa Betrug. Aber wenn es jetzt „nur“ um die banden- und gewerbsmäßige Begehung geht, dann kommt kein zusätzliches unrechtskonstituierendes Merkmal dazu, sondern es bleibt im Prinzip dieses Sachbeschädigungsunrecht. Beim bloßen Sachbeschädigungsunrecht diesen hohen Strafrahmen zu eröffnen, das halte ich zumindest für überdenkenswert. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Herr Lindner auf die Frage von Herrn Korte.

SV Felix Lindner: Die Frage bezog sich auf die internationalen Auswirkungen. Also als ersten Punkt sehe ich ganz klar – das hat Herr Hange ja schon richtig gesagt –, dass immer mehr kriminelle Energie hinter den tatsächlichen Einbrüchen in Computersysteme steht, als es zum Beispiel in den 80er oder 90er Jahren der Fall war. Wenn Sie in Statistiken schauen, woher die Angriffe kommen – es gibt so Threat-Readers und so etwas, das kennen Sie alles – sehen wir, dass heutzutage aus Deutschland relativ wenige Angriffe kommen, d. h. das Verhältnis von fähigen Leuten in Deutschland zu Leuten, die dieses für kriminelle Machenschaften verwenden, ist vergleichsweise sehr gering. Schauen Sie nach Osteuropa, da sieht das völlig anders aus. Ich sehe als Auswirkung, wenn Sie weniger legale Betätigungsfelder in Deutschland haben - und das hängt nicht davon ab, ob das juristisch gebildete Menschen so sehen, sondern das sehen junge Menschen, die sich einen Ausbildungsberuf suchen, die sich das einfach ansehen, ob sie ihren Lebensunterhalt mit Computersicherheit bestreiten können und die dann feststellen, ich finde das mit der Computersicherheit total toll, aber ich sehe nicht, dass ich das in Deutschland machen kann, ohne dafür ständig mit einem Bein im Gefängnis zu stehen -, dann ist natürlich auch der Anreiz für illegales Verhalten sehr viel höher.

Wir sehen das schon seit mehreren Jahren in Großbritannien, wo solche Sachen einfach ein bisschen härter geahndet wurden, schon immer, und wo die Polizei, also Scotland Yard, auch sehr viel mehr hinterher war, Computerkriminalität auch im kleineren Rahmen sehr stark zu verfolgen. Da ist es tatsächlich so, dass sehr viele junge Leute, bevor sie überhaupt aus der Schule rauskommen, schon von den kriminellen Gruppen angeworben werden und dann Scotland Yard eigentlich das Riesenproblem hat, dass sie die gar nicht ins Gefängnis stecken wollten, sondern sie eigentlich nur befragen wollten, um an die tatsächlichen Drahtzieher ranzukommen, aber in dem Moment, wo sie die jungen Menschen finden, diese dann meistens nicht mehr am Leben sind.

Zur zweiten Auswirkung: Da gehe ich noch mal auf das Thema Konferenzen und Teilnahme an Mailinglisten ein. Ich danke Herrn Bruns für die Klärung, was „Billigung“ heißt, aber genau in diesem Kontext ist es ja mit „Crimeware“ interessant. Wenn ich in einer geschlossenen Mailingliste Teilnehmer bin und dort wirklich explizit sehr anspruchsvolle Crimeware verteilt wird und ich jetzt der Meinung bin, es gibt hier einen weiteren Kollegen aus Deutschland, den ich mit in diese Mailingliste aufnehmen möchte, weil ich bis jetzt durchaus der Meinung war, dass der keine Verbindungen zu irgendwelchen kriminellen Vereinigungen hat, der aber in dem Moment, wo er in diese Mailingliste aufgenommen wird, sofort sieht, das ist ja richtig coole Software, also da würde ich zwei Jahre dran sitzen, um mir selber so einen Trojaner zu schreiben und dann auf die Idee kommt, das umzusetzen. Nach Ihrer Klarstellung der Billigung hätte ich mich dann tatsächlich strafbar gemacht. Auf der anderen Seite das Konferenzthema. Ich sehe das immer noch als eine der Hauptthematiken. Ganz praktisch, wenn auf einer Konferenz in Deutschland sich jemand hinstellt und sagt, hier gibt es einen neuen Angriff, der funktioniert genau so und der demonstriert ihn in vollem Detail und dann ein Teilnehmer rausgeht, sich umdreht und damit den Online-Auftritt des Bundestages übernimmt und dort lustige schwarz-weiß Grafiken drauflegt, ist das natürlich ein Problem. Deswegen, wenn es nicht eine klare Ausschlussregelung dafür gibt, wird kein Mensch irgendwelche Konferenzen hier machen.

Mir ist in der Diskussion noch eine weitere Auswirkung im internationalen Kontext aufgefallen. Der § 202b E-StGB sieht ja tatsächlich nur die technischen Mittel als

Einschränkung und nicht den Zweck, also die Bösartigkeit, vor. Das betrifft zum Beispiel die Blue-Tooth-Technologie: Da hängt man ein kabellose Handy ans Auto, mit kabellosem Headset usw.. Das wurde mal designt, damit man das nicht abhören kann. Also die Idee dabei war, dass man die Dinger nicht ohne weiteres über die Luftschnittstelle abhören kann. Wie sich so etwas generell immer entwickelt, zwei, drei Jahre später gibt es fertige Produkte auf dem Markt, die kosten dann irgendwas um die 60.000 Euro, dann ein Jahr später hat es irgendjemand für 100 Euro hingebaut. Die Frage ist natürlich, wie ist das, wenn ich jetzt die Verbindung zwischen meinem Mobiltelefon und meinem Auto versuche zu debaggen - also mittels eines Sniffers versuche herauszufinden, warum sie nicht funktioniert -, und Sie an meinem Auto vorbeigehen und ich dann Ihr Telefongespräch aufzeichne. Ich hatte das technische Mittel, aber es gibt ja nicht die Einschränkung, dass ich das böswillig wollte. Ich habe ja sozusagen den § 202b E-StGB vollständig erfüllt. Ich hatte das technische Mittel und ich habe Ihre private Datenübertragung abgehört, sogar basierend auf Ihrer Abstrahlung, die von dem Handy und dem Headset gekommen ist. Im Umkehrschluss würde das heißen, dass sämtliche Produkte, die sich in diesem Bereich bewegen, eigentlich auf dem deutschen Markt nicht angeboten werden dürften oder zumindest nicht verwendet werden dürften.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt abschließend Herr Dr. Stuckenberg auf die Fragen der Kollegen Manzewski, Montag und Korte.

SV Dr. Carl-Friedrich Stuckenberg: Zunächst zu der Frage von Herrn Manzewski, ob die IT-Sicherheit ihre Aufgaben nach der Neufassung vom § 202c E-StGB nicht mehr wahrnehmen können wird. Hier ist die Antwort ein klares „Nein, diese Gefahr besteht in meiner Sicht nicht.“, weil die Praxis es richten wird. Ich habe überhaupt keinen Zweifel daran. Ich weiß nicht, ob § 202c StGB auch in der gegenwärtigen Form überhaupt so oft praktisch angewendet wird, dass wir in den nächsten fünf Jahren dazu höchstrichterliche Rechtsprechung sehen. Ich habe gewisse Zweifel, dass das passieren wird. Aber würden wir irgendwann Oberlandesgerichte oder vielleicht den BGH dazu judizieren sehen, dann glaube ich, dass all diese Probleme und all diese Befürchtungen, die Herr Lindner hier geäußert hat, sich als unbegründet erweisen würden, denn es liegt natürlich nicht in der Intention der Entwurfverfasser, das schreiben Sie ja in der Begründung auch hinlänglich, dass all diese Dinge nun unter

Strafe stehen. Das wäre absurd. Andererseits, es gibt, das ist mir ja nun wie jedem deutschen Juristen hinlänglich bekannt, diese deutsche Gesetzestechnik, möglichst knapp zu formulieren und alles, was nicht unbedingt in den Text hinein muss, in die Begründung zu verfrachten, das gibt schöne schlanke übersichtliche Gesetze. Strafgesetze, denke ich, sind manchmal aber dann vielleicht doch etwas zu schlank. Ich bin auch kein Freund von Paragraphen, die über zwei Seiten gehen, aber das eine oder andere Wort wäre doch manchmal, glaube ich, ganz angebracht, damit es nicht nur – und so ist es ja eigentlich auch von Verfassung wegen gedacht - die Rechtsprechung und vorher die Strafverfolgungsbehörden mit ihrer Auslegung richten. Man kann es - und das kostet ja nun auch kein Geld - einfach durch ein paar Worte der Einschränkung hier klar machen. Was Herr Bruns angesprochen hat: Ich befürchte, dass es in der Tat eine Zeitlang – und das hat ja die bisherige Flut von gleichgerichteten Stellungnahmen ganz im Sinne der, die Herr Lindner hier abgegeben hat, gezeigt – trotz juristischer Beratung ein Chilling-Effekt eintreten wird, den man erstmal wieder aus der Welt schaffen muss. Das ist jetzt, wenn man diese Gesetzesfassung unverändert übernimmt, wahrscheinlich schon schwer genug, man müsste also erstmal Aufklärung leisten, so ist es überhaupt nicht gemeint, so wird es wohl nicht angewendet werden. Das ist eigentlich nicht schön, wenn man ein Gesetz so lange erklären muss. Man könnte es, wie gesagt, ohne weiteres einfacher machen, die Europaratskonvention hat das ja sehr deutlich, vielleicht überdeutlich für unseren Geschmack, versucht. Den Österreichern, denke ich, ist es besser gelungen in ihrer Umsetzungsvorschrift und so weit ich weiß, ich bin da nicht völlig im Bilde, ob da die IT-Wirtschaft entsprechend reagiert hat, aber es ist einfach klarer. Wenn man das Gesetz klarer machen kann, um den Regelungszweck, denn der Regelungszweck gefährdet die IT-Sicherheit ja nun wirklich nicht, auszuloten, dann sollte man es tun, denke ich, und nicht erst darauf warten, dass es dann tatsächlich so passiert, wie es gemeint ist. Was den Vergleich übrigens mit dem § 22b StVG und den Wegstreckenzähler anbelangt, glaube ich, ist das hier weniger der Fall, denn die Vorbereitungshandlung ist typisiert. Deshalb haben wir ja ein abstraktes Gefährdungsdelikt, da steht ja drin „Wer sich Passworte verschafft, erstellt, verwendet, zugänglich macht usw.“. Das steht ja unter Strafe. Ob damit eine Straftat vorbereitet wird, ist nicht wesentlich. Man muss nur wissen, dass irgendeiner damit vielleicht eine begeht, das reicht ja aus, die Handlungen selber sind ja eindeutig benannt. Und das, denke ich, ist der Grund auch für die Kritik an der Fassung, es ist

Aufgabe des Gesetzgebers, das klar zustellen, was für ihn ja ein leichtes ist, er braucht es nur reinzuschreiben. Das sollte dann eben auch gemacht werden.

Zu der Frage von Herrn Montag mit den elektronischen Massenprotesten. Wenn jetzt also so viele E-Mails in einer bestimmten Sache an ein Ministerium meinetwegen gesendet werden, dass dort der E-Mail-Server zusammenbricht, dann hätten wir vielleicht einen Effekt, den § 303b E-StGB beschreibt. Das, denke ich, ist das, worauf Sie hinauswollen. Da § 303b E-StGB zugleich eine Nachteilsabsicht voraussetzt, denke ich, in diesem Fall dürfte die Absicht verneint werden: Wenn die Leute das in der Tat nur tun, um ihre Meinung auszudrücken, eine Anfrage zu richten, mögen sie es, wenn sie wissen, da ist jetzt eine halbe Million Leute, die gleichzeitig mit mir so etwas tun, vielleicht billigend in Kauf nehmen, ob es ihnen darum geht, denke ich, die Absicht ließe sich verneinen. Und selbst dann, wenn es ein Fall von Artikel 5 GG ist, wo man seine Meinung kundgeben will, dann müsste man § 303b E-StGB eben entsprechend verfassungskonform auslegen, dass ein, unter anderem auch Wissen oder vielleicht Sich-Darüber-Freuen, wenn der Server zusammenbricht, dann eben nicht reicht.

Die dritte Frage von Herrn Korte, was die Bestimmtheit von § 303a und b E-StGB und den Strafrahmen anbelangt. Ich denke, das ist bereits auch schon mehrfach hier gesagt worden, natürlich sind solche Ausdrücke wie Vermögensverlust großen Ausmaßes oder von wesentlicher Bedeutung nicht das Muster an Bestimmtheit, andererseits muss der Gesetzgeber ja immer den Grat gehen zwischen Bestimmtheit und Rigidität und einer gewissen Flexibilität, da kann ich jedes Jahr eine neue inflationsbereinigte Summe in all die Gesetze bei finanziellem Schaden hineinschreiben und in der Tat findet sich, Herr Kudlich hatte es gesagt, der finanzielle Schaden großen Ausmaßes bereits im Betrugstatbestand. Die wesentliche Bedeutung können wir so ähnlich haben bei § 305a StGB - Zerstörung wichtiger Arbeitsmittel - oder in ähnlicher Weise beim § 316b StGB, das ist die Störung öffentlicher Betriebe. Das sind alles quantitative Größen und das, denke ich, ist etwas, was man getrost der Rechtsprechung überlassen kann, die ja ohnehin gewohnt ist, Strafrahmen dann auch auszufüllen. Was eine wesentliche Bedeutung ist und was ein großes Ausmaß ist, kann man, zumal es ja andere Tatbestände gibt, getrost so stehen lassen ohne Bedenken mit Art. 103 Abs. 2 GG zu haben. Ich sehe

auch keinen Weg, wie man das handhabbar präziser formulieren sollte. Ich glaube, das hat Ihre Frage beantwortet.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank, Herr Dr. Stuckenberg, wir sind damit am Schluss der zweiten Runde. Eigentlich waren wir uns einig, dass wir jetzt insgesamt schließen. Wir haben aber noch zwei Fragen, die lassen wir noch zu, Herr Kollege Tauss, Herr Kollege Manzewski und dann schließen wir aber auch mit den Antworten auf die Fragen.

Jörg Tauss (SPD): Ganz herzlichen Dank, Herr Vorsitzender, wie gesagt, ich hatte mich auf einen ganz anderen, weitergehenden Zeitrahmen eingestellt. Trotz vieler Fragen, ich konzentriere mich jetzt auf zwei. Einmal noch mal an Herrn Lindner und eine zweite noch mal an Herrn Prof. Hilgendorf. Herr Lindner, ich wollte Ihnen einfach noch mal die Gelegenheit geben, zu Saulus und Paulus Stellung zu nehmen, zu den Anmerkungen von Herrn Hange, Gut und Böse. Ich werde Sie jetzt hier nicht fragen, wer Sie jetzt sind und wohin Sie sich gewandelt haben, sondern einfach, um es vielleicht auch noch mal zu erläutern, bei Computerprogrammen, die für kriminelle Vorgänge natürlich geeignet wären, also Stichwort hier noch mal Dual-Use. Vieles von dem, was vielleicht auch ursprünglich sogar so gedacht war, ist hinterher einsetzbar für den gegenteiligen Zweck, ziemlich exakt vor Vorgängen bzw. Angriffen schützen zu können, also fast so ähnlich wie Schlangengift: man setzt es medizinisch ein. Die Frage wäre einfach, diese Trennung zwischen Gut und Böse, die Herr Hange ja beschrieben hat, da wäre auch eine gewisse Sachaufklärung aus der Praxis ganz hilfreich. Und meine Frage an Herrn Hilgendorf, weil wir uns ja an anderer Stelle mit Folgen von Gesetzgebung im Bereich der Strafbarkeit beschäftigen, Stichwort Stammzellengesetz. Da werden wir uns also demnächst in einer separaten Anhörung wieder begegnen. Da, wo die Wirkungen natürlich auf die deutsche Forschungsszene, auf die Wissenschaftsszene, nun so sind, wie sie vom Gesetzgeber nicht beabsichtigt waren und auch nicht im Gesetz stehen, aber die Folgen haben wir. Deswegen meine Frage, Sie haben mir dankenswerter Weise einige Hinweise gegeben, wie § 202c E-StGB gefasst werden soll. Und meine Frage wäre, sollen wir versuchen, § 202c E-StGB zu reparieren, wie von Ihnen vorgeschlagen, oder wäre es im Sinne der Vermeidung des „Stammzelleffekts“ vielleicht auch ganz sinnvoll, darauf zu verzichten?

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Herr Kollege Manzewski.

Dirk Manzewski (SPD): Auf den Beitrag von Herrn Dr. Stuckenberg zurückkommend möchte ich Fragen stellen an Herrn Dr. Stuckenberg und an Herrn Bruns. Dr. Stuckenberg, Sie haben ja dargelegt, dass vielleicht eine Klarstellung wünschenswert wäre. Gut, dann würde ich ganz gerne von Ihnen und von Herrn Bruns mal hören, wie denn so eine Klarstellung aussehen könnte. Ich plädiere eigentlich, das sage ich so deutlich, immer kurze und knappe Gesetzestexte, weil die einfach verständlicher sind. Je mehr man reinschreibt, desto komplizierter wird das, und ich habe auch früher gelernt, dass man sich daran zu orientieren hat, was der Gesetzgeber eigentlich im Sinn hat, wenn es denn Zweifelsfragen gibt. Und da hilft natürlich die Begründung eines Gesetzes meiner Auffassung nach vortrefflich. Meine Frage daher, ob Sie nicht doch der Auffassung sind, dass es ausreichen könnte, wenn man in der Begründung dort noch mal eine Klarstellung fasst. Und würden Sie nicht auch meine Auffassung teilen, dass die Probleme nicht im rechtlichen, sondern eher im psychologischen Bereich bestehen und dass es relativ wenige Felix Lindners in Deutschland gibt? Ich behaupte einfach mal forsch, dass gerade dieser Personenkreis, weil er sich ja auch des Internets bedient wie sonst niemand, sehr schnell korrespondiert, was erlaubt ist und was eben nicht. Also, ich halte das offen gestanden für ein bisschen naiv zu glauben, dass das, was wir hier bereden und das, was nachher in die Gesetzgebung Eingang findet, an diesem Personenkreis nun völlig vorbei geht. Ich behaupte sogar mal eher das Gegenteil, dass die innerhalb kürzester Zeit ganz genau wissen, was sie dürfen und was nicht. Und deswegen sind die Befürchtungen von Herrn Lindner, glaube ich, ein bisschen überzogen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt antwortet Herr Dr. Stuckenberg zunächst auf Herrn Manzewski.

Dr. Carl-Friedrich Stuckenberg: Ich gebe Ihnen Recht, dass knapp immer gut ist, aber knapp ist nicht immer verständlich und dann ist knapp nicht gut, wenn es eben zu knapp ist. Und das scheint mir in diesem Fall passiert zu sein. Es ist sicherlich auch ein psychologischer Effekt, aber das kann man eben mit Gesetzen auch erreichen. Man kann, wie Sie das eben angedeutet haben, Herr Tauss, ungewollte

Effekte erreichen, weil eben ein Gesetz - auch Strafgesetz, wenn man so will – nicht nur vollzogen wird von den Strafverfolgungsbehörden und Gerichten, sondern eben auch sonstige Auswirkungen auf das Verhalten der Bevölkerung haben kann. Ich gebe zu, anfangs habe ich auch die ganzen Bedenken mit den ersten Stellungnahmen von BitCom usw. nicht recht nachvollziehen können, weil mir klar war, das ist doch alles gar nicht erfasst. Wenn man das Gesetz liest, kann man das theoretisch drunter fassen; dass das alles nicht gewollt ist, stand so klar in der Gesetzesbegründung der ersten Entwurfsfassung aber nicht drin. Die Gegenäußerung der Bundesregierung hat das klarer gemacht, das sollte wenigstens drin stehen. Aber ich denke auch, die wesentlichen Sachen, und sei es nur das eine Wort „*überwiegend* zum Zweck der Begehung von Straftaten“ und so fort oder „mit dem Wissen oder in der Absicht, dass damit Straftaten begangen werden“, das sollte auch schon im Gesetz drinstehen. Man kann nicht alles auf die Begründung verschieben, dann könnte man ja hineinschreiben, wer sich ungebührlich verhält wird angemessen bestraft und die Einzelheiten kann man in der Begründung nachlesen. Das ist ja nicht der Sinne des Art. 103 Abs. 2 GG. Ich denke, diese kleine Reparatur, ich habe Ihnen ja wie Herr Hilgendorf einen Formulierungsvorschlag in der schriftlichen Stellungnahme angeboten und ich denke, dass dies durchaus nötig ist. Natürlich haben Sie Recht, dass sich irgendwann herumsprechen wird, was nicht strafbar ist, das spricht sich immer herum, aber es ist die Frage, ob man darauf wirklich vertrauen soll, dass dann irgendwie mit Hilfe von Rechtsberatung oder sonstigem irgendwann ein jeder einigermaßen Bescheid weiß. Das kann man nicht kontrollieren, ob jeder alles weiß - und anders als in anderen Rechtsgebieten ist die klare Abgrenzung des strafbaren vom nichtstrafbaren Bereich nun mal Aufgabe des Gesetzgebers und von niemandem sonst. Ich denke, das ist hier relativ leicht zu machen mit dem „primarily“ in Art. 6 der Europaratskonvention, mit der Einschränkung auch des subjektiven Tatbestandes. Wenn man den dolus eventualis herausnimmt, dann hat man die exakte Fassung auch der Konvention, also gibt es völkerrechtlich überhaupt keine Probleme. In der Konvention steht „with intent that it be used“ in der englischen und auch in der französischen Version „l’intention“ - das ist einfach Wissentlichkeit und Absicht. Also, dass jemand bloß möglicherweise ahnt, das könnte jemand missbrauchen, ich denke, das ist nichts, was man erfassen will und das kann man auch getrost rauslassen, da passiert nichts Schlimmes. Und wenn man in die Gesetzesbegründung dann noch hereinschreibt, was in Artikel 6 Abs. 2

der Konvention steht, dass eben die Vorschrift nicht so auszulegen ist, dass all das, was die IT-Sicherheit notwendigerweise braucht, darunterfällt, dann müsste das ausreichen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Lindner auf Herrn Tauss.

SV Felix Lindner: Um die Frage nach dem Gut / Böse zu beantworten, möchte ich zunächst kurz auf das eingehen, was in den 80iger Jahren in zwei, drei Büchern und vielleicht in ein paar Kinofilmen mal verarbeitet wurde: Dass die bösen Hacker dann zu den guten worden sind, das ist ziemlich aus der Mode gekommen, weil man dann nämlich kein Vertrauensverhältnis mehr zu diesen Leuten hat und schlicht und ergreifend auch die Ausbildung eine andere ist. Es gibt heute kein wirklich ernstzunehmendes Beispiel mehr aus diesem Bereich. Aber zu der Frage Gut / Böse von Tools und Angriffen. Es ist natürlich wichtig zu sehen, woher die Dinge kommen. Die entstehen ja nicht irgendwo, sondern zuerst setzt sich jemand hin und forscht tatsächlich danach, erkennt Angriffsmöglichkeiten. Ich meine, die Hersteller von Software und die Hersteller von Computersystemen denken ja schon daran, den Zugriff zu limitieren, man baut ja Passwortanfragen und so etwas nicht aus Spaß ein, Entwicklungszeit kostet ja auch Geld. Es setzen sich eine oder mehrere Personen hin und denken offensiv darüber nach, was gibt es für Schwächen in dieser Absicherung. Über das Ziel kann man sich streiten, weil das Ziel tatsächlich erst im dritten Schritt kommt, im zweiten Schritt findet man nämlich – und das ist bei allen gleich, bei den Guten und den Bösen und denen dazwischen – erstmal raus, kann ich diesen Angriff überhaupt umsetzen, ist der denn überhaupt realistisch. Es gibt natürlich einen ganzen Haufen Angriffe, die überhaupt nicht realistisch sind. Und erst danach, erst in der dritten Ausprägung, gibt es den großen Unterschied. Die einen veröffentlichen es und zwar nach einem Prozess „full disclosure – responsible disclosure“, d. h. man geht erstmal zum Hersteller, erzählt dem das, wartet bis die fertig sind, das zu fixen und dann erzählt man es allen anderen. Oder man macht es eben nicht, sondern wendet es an. Und da hat man dann auch den großen zeitlichen Unterschied. Denn wenn man es im Internet anwendet, um irgendwo in einen Rechner einzubrechen - egal, ob man damit noch weitere kriminelle Ziele verfolgt oder ob man es einfach so macht -, der Unterschied ist, dass es zwei bis drei Jahre

dauert, bis die Sicherheitslücke erkannt wird, weil es zuvor nicht publiziert wurde. Solange dauert es, bis dann tatsächlich mal jemand bei einer „foransic“ - das ist der Vorgang nachzugucken, wie ist denn jemand in einen Rechner eingebrochen -, herausfindet, oh, das war ja was Neues, das haben wir ja vorher noch nicht gesehen und erst dann, im Vergleich zu der sofortigen Veröffentlichung, kann ein Schutz überhaupt angeboten werden. Erst dann können die diversen Hersteller von Sicherheitssoftware oder der Betriebssystemhersteller selbst oder der Softwarehersteller selbst – wir reden ja nicht nur über Personalcomputer, wir reden ja über eingebettete Systeme, wir reden ja mittlerweile sogar über Autos – einen Schutz einbauen. Beantwortet das Ihre Frage?

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Jetzt Herr Prof. Hilgendorf auf die Frage von Herrn Tauss.

SV Prof. Dr. Dr. Hilgendorf: Ich kann an sich nahtlos an das anschließen, was der Kollege Stuckenberg ausgeführt hat. Der § 202c E-StGB lässt sich relativ leicht reparieren, in dem man entweder im objektiven Tatbestand das Wort „gezielt“ einfügt oder im subjektiven Tatbestand ein Absichterfordernis einbaut. Wenn man das tut, ist die Norm meines Erachtens praktikabel, gerade mit Blick auch darauf, dass die Praxis bisher sehr vernünftig mit Computerstrafrecht umgegangen ist. Wenn solche Änderungen nicht erfolgen, dann würde ich, wenn ich die Macht dazu hätte, dafür plädieren, auf den § 202c E-StGB lieber ganz zu verzichten. Also so, wie er jetzt hier steht, sollte er nicht beschlossen werden, weil er zu weit und ein Beispiel für schlechtes, nicht praktikables Strafrecht ist. Sie tun dem deutschen Strafrecht nichts Gutes, wenn Sie eine Norm dieser Art in die Wirklichkeit entlassen.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Abschließend hat das Wort Herr Bruns, um die Frage von Herrn Manzewski zu beantworten.

SV Michael Bruns: Vielen Dank. Das hat mich jetzt etwas erschreckt, was Sie sagen, Herr Hilgendorf. Wie sollte eine Klarstellung aussehen? Vielleicht darf ich zum einleitenden Verständnis sagen, ich habe Rechtsförmlichkeit im BMJ gelernt und da ist Rechtsprache technische Sprache und unterliegt ganz bestimmten Gesetzmäßigkeiten. Vor dem Hintergrund dessen, was ich da gelernt habe, das wird

sich inzwischen nicht so sehr geändert haben, trifft nach wie vor das zu, was ich vorhin gesagt habe. Wir haben zwei Filter in dieser Vorschrift, die sind auch für jedermann, Entschuldigung, eben nicht jedermann, sondern für den juristisch, gesetzestechnisch insofern Informierten ohne weiteres verständlich. Das ist auch keine schlechte Gesetzgebung, da habe ich den Eindruck, schießen Sie so ein bisschen über das Ziel hinaus. Ich muss umgekehrt sagen, natürlich könnte man aus psychologischen Gründen da jetzt noch hier und da ein Wort anfügen, vielleicht noch einen zweiten Absatz, in dem man die Sicherungsunternehmen möglicherweise noch mit Bezeichnung der Firmennamen von der Strafbarkeit ausnimmt, das wäre Feuilleton, das wäre gesetzgeberisches Feuilleton. Wir machen das heute häufiger, leider Gottes, aber ich denke sozusagen, als Vertreter der klassischen Linie ist dieser Tatbestand so in Ordnung. Es ist eine Frage, wie Sie richtig sagen Herr Manzewski, der Vermittlung, wie man jetzt dem rechtsunkundigen Publikum mitteilt, was steht in diesem Gesetz eigentlich drin. Aber das gehört in die Begründung, jedenfalls bisher. Danke schön.

Vorsitzender Andreas Schmidt (Mülheim): Vielen Dank. Wir sind damit am Schluss der Sachverständigenanhörung angekommen. Ich darf mich sehr herzlich bedanken, dass Sie hier waren und dass Sie uns Rede und Antwort gestanden haben. Die Sitzung ist geschlossen. Vielen Dank.

Ende der Sitzung: 14.38 Uhr

Andreas Schmidt (Mülheim), MdB
Vorsitzender