MIR MEDIEN INTERNET und RECHT
Onlinepublikation zum Medien- und Internetrecht

Volltext zu MIR Dok.: 137-2009

Veröffentlicht in: MIR 06/2009

Gericht: BVerfG

Aktenzeichen: 2 BvR 2233/07; 2 BvR 1151/08; 2 BvR 1524/08

Entscheidungsdatum: 18.05.2009

Vorinstanz(en):

Permanenter Link zum Dokument: *http://www.medien-internet-und-recht.de/volltext.php?mir_dok_id=1978*

www.medien-internet-und-recht.de ISSN: 1861-9754

BUNDESVERFASSUNGSGERICHT
Im Namen des Volkes

**In den Verfahren
über
die Verfassungsbeschwerden**

1. des Herrn

gegen § 202c StGB

- 2 BvR 2233/07 -,

2. des

gegen § 202c Abs. 1 Nr. 2 StGB in Verbindung mit § 202a StGB, in der Fassung des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 7. August 2007 (BGBl I S. 1786), in Kraft seit dem 11. August 2007, soweit die Herstellung, das Verschaffen, das Überlassen, das Verbreiten und sonstige Zugänglichmachen von Computerprogrammen unter Strafe gestellt wird

- 2 BvR 1151/08 -,

3. des

gegen § 202c Abs. 1 Nr. 2 StGB

- 2 BvR 1524/08 -

hat die 2. Kammer des Zweiten Senats des Bundesverfassungsgerichts durch

die Richter Broß,
Di Fabio
und Landau

gemäß § 93b in Verbindung mit § 93a BVerfGG in der Fassung der Bekanntmachung vom 11. August 1993 (BGBl I S. 1473) am 18. Mai 2009 einstimmig beschlossen:

Die Verfahren werden zur gemeinsamen Entscheidung verbunden.

Die Verfassungsbeschwerden werden nicht zur Entscheidung angenommen.

Gründe

A.

[2] Die Verfahren betreffen die Frage, ob die Strafbarkeit des Vorbereitens des Ausspähens und Abfangens von Daten nach § 202c Abs. 1 StGB, insbesondere dessen Nr. 2, mit dem Grundgesetz vereinbar ist.

I.

[3] 1. § 202c wurde durch Art. 1 Nr. 3 des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 7. August 2007 (BGBl I S. 1786) zusammen mit § 202b in das Strafgesetzbuch eingefügt und trat am 11. August 2007 in Kraft. Gleichzeitig wurde § 202a StGB geändert. Die Vorschriften gelten seitdem unverändert mit folgendem Wortlaut:

[4] **§ 202c Vorbereiten des Ausspähens und Abfangens von Daten**

[5] (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

[6] 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

[7] 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

[8] herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

[9] (2) § 149 Abs. 2 und 3 gilt entsprechend.

[10] **§ 202a Ausspähen von Daten**

[11] (1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

[12] (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

[13] **§ 202b Abfangen von Daten**

[14] Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

[15] Durch entsprechende Verweise in § 303a Abs. 3 und § 303b Abs. 5 StGB gilt § 202c StGB ferner entsprechend für die Vorbereitung von Straftaten der Datenveränderung und der Computersabotage.

[16] 2. Das 41. Strafrechtsänderungsgesetz diente der Umsetzung von Rechtsinstrumenten des Europarats und der Europäischen Union (vgl. Gesetzesbegründung der Bundesregierung, BTDrucks 16/3656, S. 1, 7 f.), namentlich des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001 und des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (ABlEU Nr. L 69 vom 16. März 2005, S. 67).

[17] Das Übereinkommen über Computerkriminalität (engl.: Convention on Cybercrime) des Europarats wurde am 23. November 2001 in Budapest von Mitgliedstaaten des Europarats - darunter Deutschland - und einigen Nichtmitgliedstaaten - darunter den Vereinigten Staaten von Amerika, Kanada und Japan - unterzeichnet. Es trat am 1. Juli 2004 nach Erfüllung der vorgesehenen Bedingungen (Ratifikation durch mindestens fünf Staaten, darunter drei Mitgliedstaaten des Europarats) in Kraft. Mit dem „Gesetz zu dem Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität“ vom 5. November 2008 (BGBl II S. 1242) hat der Deutsche Bundestag dem Übereinkommen zugestimmt.

[18] Das Übereinkommen sieht vor, dass die Vertragsparteien den unbefugten Zugang zu Computersystemen (Art. 2), das unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen (Art. 3), das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten (Art. 4) und die unbefugte schwere Behinderung des Betriebs eines Computersystems (Art. 5) unter Strafe stellen. Art. 6 enthält in diesem Zusammenhang Bestimmungen über die Strafbarkeit wegen Missbrauchs von Vorrichtungen (zitiert nach der ÜbersetzungBGBl 2008 II S. 1243 ff.):

[19] (1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

[20] (a) das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen

[21] (i) einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen;

[22] (ii) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen,

[23] mit dem Vorsatz, sie zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden, und

[24] (b) den Besitz eines unter Buchstabe a Ziffer i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst mit Besitz einer bestimmten Anzahl dieser Mittel eintritt.

[25] (2) Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.

[26] (3) …

[27] Nach dem Erläuternden Bericht („Explanatory Report”) des Europarats bezieht sich die Erwähnung eines „Computerprogramms“ in Art. 6 auf Programme, die beispielsweise - wie Virenprogramme - dafür gestaltet worden sind, Daten zu verändern oder gar zu zerstören oder in Datenverarbeitungsvorgänge einzugreifen, oder die dazu gestaltet oder eingerichtet worden sind, Zugang zu Computersystemen zu erhalten („programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems“, Rn. 72 des im Internet unter http://conventions.coe.int/Treaty/en/Reports/Html/185.htm abrufbaren Berichts). Im Wege eines vernünftigen Kompromisses beschränke das Übereinkommen seine Anwendbarkeit auf Fälle, in denen Vorrichtungen objektiv in erster Linie dazu gestaltet oder eingerichtet worden sind, eine Straftat zu begehen. Dies allein werde „dual-use-Vorrichtungen” in der Regel ausschließen („As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices”, a.a.O. Rn. 73).

[28] 3. a) Die Bundesregierung führte in der Begründung ihres - letztlich unverändert vom Deutschen Bundestag verabschiedeten - Gesetzesentwurfs zu § 202c (BTDrucks 16/3656, S. 11 f.) aus, mit der Vorschrift sollten bestimmte besonders gefährliche Vorbereitungshandlungen selbstständig mit Strafe bedroht werden. Erfasst würden insbesondere die so genannten Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt seien, illegalen Zwecken zu dienen, und die aus dem Internet weitgehend anonym geladen werden könnten. Die durch das Internet mögliche Weiterverbreitung und leichte Verfügbarkeit der Hacker-Tools sowie ihre einfache Anwendung stellten eine erhebliche Gefahr dar, die nur dadurch effektiv bekämpft werden könne, dass bereits die Verbreitung solcher an sich gefährlicher Mittel unter Strafe gestellt würde.

[29] Eine Einschränkung der Strafbarkeit nach Abs. 1 Nr. 2 solle - in Anlehnung an § 263a Abs. 3 StGB - dadurch erreicht werden, dass bereits im objektiven Tatbestand auf die Bestimmung des Computerprogramms als Mittel zur Begehung einer Straftat nach den § 202a und § 202b StGB abgestellt werde, um eine „Überkriminalisierung“ zu verhindern. Es komme insoweit auf die (objektivierte) Zweckbestimmung des Programms an. Somit sei sichergestellt, dass nur Hacker-Tools erfasst würden und die allgemeinen Programmier-Tools, -sprachen oder sonstigen Anwendungsprogramme bereits nicht unter den objektiven Tatbestand der Strafvorschriften fielen. Das Programm müsse aber nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reiche, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat sei.

[30] b) Der Bundesrat äußerte in seiner Stellungnahme (BTDrucks 16/3656, S. 16 f.) Bedenken gegen den Gesetzentwurf. Der Tatbestand des § 202c StGB sei sehr weit geraten. Der Bundesrat bat insbesondere zu prüfen, ob die tatbestandliche Fassung des § 202c StGB den gutwilligen Umgang mit allgemeinen Programmier-Tools, -sprachen oder sonstigen Softwareprogrammen sowie „Hacker-Tools“ zur Sicherheitsüberprüfung von IT-Systemen - ausreichend vor Kriminalisierung schütze (a.a.O. S. 17).

[31] c) Die Bundesregierung hielt an dem vorgeschlagenen Wortlaut des § 202c StGB fest und vertrat in ihrer Gegenäußerung (BTDrucks 16/3656, S. 18 f.) die Auffassung, dass die Nichterfassung des gutwilligen Umgangs mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen über zwei Tatbestandsmerkmale sichergestellt sei.

[32] Bereits die objektive Beschränkung des Tatbestands auf Computerprogramme, deren Zweck die Begehung einer Computerstraftat sei, stelle sicher, dass keine Computerprogramme erfasst würden, die beispielsweise der Überprüfung der Sicherheit oder Forschung in diesem Bereich dienten. Unter Strafe gestellt würde lediglich das Herstellen usw. solcher Programme, die nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt seien. Bei Programmen, deren funktionaler Zweck nicht eindeutig kriminell sei und die erst durch ihre Anwendung zu einem Tatwerkzeug eines Kriminellen oder aber zu einem legitimen Werkzeug würden - so genannte dual use tools - sei bereits der objektive Tatbestand des § 202c StGB nicht erfüllt. Die bloße Eignung von Software zur Begehung von Computerstraftaten sei nicht ausreichend, so dass auch solche Programme aus dem Tatbestand herausfielen, die lediglich zur Begehung von Computerstraftaten missbraucht werden könnten.

[33] Eine weitere Einschränkung ergebe sich daraus, dass die Tathandlung zur Vorbereitung einer Computerstraftat erfolgen müsse. Entscheidend sei, dass der Täter eine eigene oder fremde Computerstraftat in Aussicht genommen habe. Das sei nicht der Fall, wenn das Programm beispielsweise zum Zwecke der Sicherheitsüberprüfung, zur Entwicklung von Sicherheitssoftware oder zu Ausbildungszwecken in der IT-Sicherheitsbranche hergestellt, erworben oder einem anderen überlassen werde. Das gelte auch für den Fall, in dem ein Computerprogramm, das ursprünglich nur zu kriminellen Zwecken hergestellt worden sei, verschafft, verkauft, überlassen, verbreitet oder sonst zugänglich gemacht werde, wenn dies ausschließlich zu nicht kriminellen Zwecken erfolge und keine Anhaltspunkte für eine eigene oder fremde Computerstraftaten bestünden. Wenn also beispielsweise in den Fällen des Entwickelns von Sicherheitssoftware auch Schadprogramme beschafft würden, dann erfolge dies nicht zur Vorbereitung einer Computerstraftat und sei daher auch nicht strafbar.

[34] d) Im Rahmen der Beratung der Gesetzesvorlage führte der Rechtsausschuss des Deutschen Bundestags am 21. März 2007 eine öffentliche Anhörung von Sachverständigen durch. Die Frage der Reichweite des § 202c StGB insbesondere im Hinblick auf so genannte dual use tools war Gegenstand sowohl der vorbereitenden schriftlichen Äußerungen der Sachverständigen als auch der mündlichen Diskussion (vgl. i. E. die Dokumentation unter http://www.bundestag.de/ausschuesse/a06/anhoerungen/Archiv/15_Computerkriminalitaet/index.html).

[35] e) Im Ergebnis empfahl der Rechtsausschuss dem Bundestag mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und Bündnis 90/Die Grünen gegen die Stimmen der Fraktion Die Linke die unverän-

derte Annahme des Gesetzentwurfs der Bundesregierung (BTDrucks 16/5449, S. 1, 3). In der Anhörung des Rechtsausschusses von Vertretern der IT-Branche vorgetragene Bedenken hinsichtlich des § 202c StGB seien sehr ernsthaft geprüft worden. Der Gesetzentwurf kriminalisiere nicht den branchenüblichen Einsatz von Hacker-Tools durch Netzwerkadministratoren, wenn diese nur die Sicherheit des eigenen Datennetzes prüfen wollten. Um Missverständnisse zu vermeiden, stelle der Rechtsausschuss klar, dass § 202c StGB hinsichtlich der Zweckbestimmung im Sinne des Art. 6 des Europarats-Übereinkommens auszulegen sei. Danach seien nur Computerprogramme betroffen, die in erster Linie dafür ausgelegt oder hergestellt würden, um damit Straftaten nach § 202a, § 202b StGB zu begehen. Die bloße Geeignetheit zur Begehung solcher Straftaten begründe keine Strafbarkeit. Die geforderte Zweckbestimmung müsse eine Eigenschaft des Computerprogramms in dem Sinne darstellen, dass es sich um so genannte Schadsoftware handle.

II.

[36] 1. a) Der Beschwerdeführer F... war Geschäftsführer der Firma V... Deutschland GmbH (im Folgenden: V...). Das Unternehmen bietet Dienstleistungen im Bereich der Sicherheit von Informations- und Kommunikationstechnologien an. Im Rahmen ihres Geschäftsbetriebes führt die Firma V... unter anderem so genannte Penetrationstests durch. Dabei handelt es sich um Sicherheitsüberprüfungen von EDV-Anlagen durch Simulation nicht autorisierter Zugriffsversuche: Die Mitarbeiter der V... versetzen sich in die Situation eines Angreifers und versuchen, Sicherheitslücken zu finden, um auf diese Weise in das zu überprüfende EDV-System - typischerweise ein Netzwerk eines Unternehmens - einzudringen. Gegenstand der unternehmerischen Tätigkeit der V... ist damit unter anderem die Feststellung, wie verletzlich das Zielsystem für „Hacker-Angriffe“ ist. Nach Abschluss der Überprüfung wird ein Bericht erstellt, der es dem Inhaber der geprüften EDV-Anlage ermöglicht, im Falle aufgedeckter Sicherheitslücken Gegenmaßnahmen zu ergreifen und so die Systemsicherheit zu verbessern. Die V... wird dabei ausschließlich im Auftrag und mit Einverständnis des Betreibers der EDV-Anlage tätig.

[37] Zur Realisierung der Penetrationstests setzt die Firma V... eine Vielzahl von EDV-Programmen ein, deren mögliche Einsatzbereiche nicht immer eindeutig definiert sind. Teilweise handelt es sich um Analysewerkzeuge, die sowohl vom berechtigten Nutzer / Administrator eines Computersystems zu dessen bestimmungsgemäßer Wartung und Pflege als auch ohne oder gegen den Willen des Berechtigten zum Zwecke des Ausspähens von Schwachstellen verwendet werden können (dual use tools). Teilweise entstammen die Programme auch anonymen „Hacker-Foren“ im Internet, die vermuten lassen, dass die Programme von ihren Urhebern zum Zwecke des illegalen Eindringens in EDV-Systeme konzipiert wurden (so genannte malware oder Schadsoftware).

[38] b) Mit der fristgerecht (§ 93 Abs. 3 BVerfGG) eingegangenen Verfassungsbeschwerde rügt der Beschwerdeführer F..., § 202c StGB verstoße gegen Art. 12 Abs. 1 GG.

[39] § 202c StGB greife in die Berufsfreiheit ein. Die Vorschrift habe eine objektive berufsregelnde Tendenz, indem sie die Beschaffung sowohl von eigentlicher Schadsoftware als auch von Programmen mit nicht eindeutiger Zweckbestimmung (dual use tools) verbiete. Auf die Beschaffung solcher Programme sei die Firma V... jedoch zwingend angewiesen. Das strafrechtliche Verbot des § 202c StGB mache der Firma V... also die Fortführung ihrer bisherigen Tätigkeit unmöglich, weswegen es sich hier um eine objektive Zulassungsbeschränkung handle. Sofern die Bundesregierung im Verlauf des Gesetzgebungsverfahrens erklärt habe, Programme, die zur Begehung von Computerstraftaten lediglich geeignet seien, fielen nicht unter die Vorschrift, habe diese Differenzierung im Gesetzestext keinen Niederschlag gefunden, was überdies gegen Art. 103 Abs. 2 GG verstoße.

[40] Der Eingriff in Art. 12 Abs. 1 GG sei nicht gerechtfertigt. Mit der Einführung des § 202c StGB hätten sowohl die private Wirtschaft wie auch die öffentliche Verwaltung und Privatpersonen einerseits vor wirtschaftlichen Schäden, andererseits vor Eingriffen in die Privatsphäre geschützt werden sollen. Das gleiche Ziel verfolge der Beschwerdeführer mit seinem Dienstleistungsangebot. Wenn genau diese Tätigkeit durch die Vorschrift verboten werde, sei letztere also zur Erreichung des mit ihr verfolgten Ziels nicht geeignet. Darüber hinaus handele es sich bei den von § 202c StGB geschützten Rechtsgütern nicht um überragend wichtige Gemeinschaftsgüter.

[41] 2. a) Der Beschwerdeführer Prof. Dr. W... ist Hochschullehrer an der technischen Fachhochschule Berlin im Fachbereich Informatik und Medien. Zu seinen Dienstverpflichtungen gehört es, Vorlesungen im Bereich der Informatik anzubieten. Im Rahmen der Vorlesungen geht es unter anderem um die Vermittlung der Kompetenz zur Nutzung so genannter Sicherheitsanalysewerkzeuge. Dies sind Softwareprogramme, die durch systematisches Testen mögliche Schwachstellen in informationstechnischen Systemen aufspüren und eine Sicherheitsbewertung dieser Lücken durchführen. Im Rahmen praktischer Übungen übergibt der Beschwer-

deführer den Studierenden entweder Datenträger mit entsprechenden Programmen oder gibt ihnen die Möglichkeit, diese von seiner Homepage herunterzuladen. Über die Homepage können sich auch Dritte die Programme verschaffen, ohne dass der Beschwerdeführer dies kontrollieren könnte. Bei der Software handelt es sich entweder um solche, die auch sonst frei im Internet erhältlich ist, oder um vom Beschwerdeführer selbst entwickelte oder modifizierte Programme.

[42] Sämtliche Software-Tools dieser Art können allerdings nicht nur zur Überprüfung von Sicherheitslücken in zu schützenden Systemen eingesetzt werden, sondern auch missbräuchlich für Zwecke des unerlaubten Zugangs zu fremden Rechnern und Netzwerken. Das gilt beispielsweise für das Tool „nmap“, welches häufig von Hackern vor einem Angriff auf einen fremden Rechnern benutzt wird, um möglichst viele Informationen über diesen Rechner zu erhalten. Der Beschwerdeführer weist in seinen Vorlesungen darauf hin, dass es unzulässig sei, Sicherheitsanalysewerkzeuge zum „Hacken“ fremder Rechner zu verwenden, also dazu, sich unter Überwindung von Sicherheitsmaßnahmen Zugang zu diesen zu verschaffen. Allerdings geht er davon aus, dass ein geringer Anteil seiner Studenten die im Rahmen der Vorlesung überlassenen Programme auch zu solchen verbotenen Zwecken nutzt. Hiervon ist ihm in der Vergangenheit auch bereits berichtet worden. Der Beschwerdeführer steht auf dem Standpunkt, dass solche Verhaltensweisen nicht von verfestigter krimineller Energie zeugen und reagiert darauf bislang nur insofern, als er auf das strafrechtliche Verbot nach § 202a StGB hinweist und von seinen Studenten verlangt, illegales Verhalten zukünftig zu unterlassen.

[43] b) Der Beschwerdeführer wendet sich mit seiner Verfassungsbeschwerde gegen § 202c Abs. 1 Nr. 2 StGB in Verbindung mit § 202a StGB und macht eine Verletzung von Art. 12 Abs. 1, Art. 5 Abs. 3 und Art. 2 Abs. 1 GG geltend.

[44] Er geht davon aus, dass er sich durch die weitere Fortführung seiner Forschungs- und Lehrtätigkeit nach § 202c Abs. 1 Nr. 2 StGB in Verbindung mit § 202a StGB strafbar macht. Die von ihm beschafften, teilweise auch selbst hergestellten und verbreiteten Programme stellten dual-use-Software dar, deren Zweckbestimmung jedenfalls auch die Begehung von Computerstraftaten nach § 202a StGB sei. Nach den tatsächlichen Umständen der Verwendung dieser Software durch einzelne Studenten und der Erkenntnisse des Beschwerdeführers hiervon erfülle der Beschwerdeführer auch den subjektiven Tatbestand der Norm. Er stehe praktisch vor der Wahl, entweder die bezeichneten Lehrinhalte nicht mehr zu unterrichten - womit er seine Dienstpflichten verletzen würde - oder das latente Risiko einer Strafverfolgung einzugehen.

[45] Der Beschwerdeführer hält die angegriffene Regelung für einen Eingriff in die Freiheit der Berufsausübung und die Freiheit der Lehre. Das Gesetz verfolge mit dem Bestreben, die Integrität und Vertraulichkeit informationstechnischer Systeme zu sichern, legitime Zwecke von Verfassungsrang, sei jedoch mit dem Verhältnismäßigkeitsgrundsatz nicht vereinbar. Zur Erreichung des Zwecks, bestimmte besonders gefährliche Vorbereitungshandlungen zu Computerstraftaten selbständig unter Strafe zu stellen, sei die angegriffene Norm nicht erforderlich; zu beanstanden sei insbesondere, dass sie die Strafbarkeit nicht vom Vorliegen direkten Vorsatzes bezüglich einer zukünftigen Computerstraftat abhängig mache. Angesichts des Interesses der Allgemeinheit, dass Sicherheitslücken in Computersystemen durch die Simulation von Hacker-Angriffen geschlossen und die entsprechenden Kenntnisse von Studenten erworben würden, sei es kontraindiziert, die Vermittlung eben solcher Fähigkeiten durch Strafnormen zu verbieten. Im Hinblick auf den Eingriff in Art. 12 Abs. 1 GG sei zudem das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG nicht beachtet worden.

[46] 3. Der Beschwerdeführer K... nutzt das Computerbetriebssystem Linux. Dabei setzt er auch Programmkomponenten ein, die im Internet frei erhältlich sind, so genannte Linux-Distributionen. Diese werden weltweit von Linux-Nutzern entwickelt und zur Verfügung gestellt, um das Betriebssystem zu verbessern. Zu den vom Beschwerdeführer genutzten Anwendungen gehört das (auch vom Beschwerdeführer Prof. Dr. W... angesprochene) Tool „nmap“. Der Beschwerdeführer geht davon aus, dass dieses sowie andere von ihm genutzte Programme auch dafür genutzt werden könnten, unter Verstoß gegen § 202a StGB in fremde Computersysteme einzudringen. Er rügt mit der Verfassungsbeschwerde eine Verletzung seiner allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) und des strafrechtlichen Bestimmtheitsgebots (Art. 103 Abs. 2 GG). Er befürchtet, sich bereits durch das Installieren von Linux-Distributionen wie „nmap“ nach § 202c Abs. 1 Nr. 2 StGB strafbar zu machen.

III.

[47] Zu der Verfassungsbeschwerde des Beschwerdeführers F... haben sich das Bundesministerium der Justiz, der Generalbundesanwalt, der Chaos Computer Club und die Gesellschaft für Informatik e. V. geäußert.

[48] 1. Nach Auffassung des Bundesministeriums der Justiz ist die Verfassungsbeschwerde überwiegend unzulässig und im Übrigen unbegründet. Soweit der Beschwerdeführer eine Verletzung des Art. 12 Abs. 1 GG durch die Vorschrift des § 202c Abs. 1 Nr. 2 StGB geltend mache, fehle es in weiten Teilen an einer Betroffenheit des Beschwerdeführers, da die Norm einen Großteil seines unternehmerischen Betätigungsfeldes nicht erfasse. Im Übrigen sei in der Vorschrift allenfalls eine Regelung der Berufsausübung zu sehen, die - falls man sie an Art. 12 Abs. 1 GG überhaupt messen wolle - durch vernünftige Gründe des Allgemeinwohls gerechtfertigt sei und den Anforderungen des Grundsatzes der Verhältnismäßigkeit genüge.

[49] 2. Der Generalbundesanwalt hält - mit ähnlichen Erwägungen - die Verfassungsbeschwerde für insgesamt unzulässig und zudem unbegründet.

[50] 3. Der Chaos Computer Club betont in seiner Stellungnahme, dass § 202c StGB bei Unternehmen, Forschern und Arbeitnehmern in der IT-Branche zu großer Unsicherheit hinsichtlich der danach bestehenden Grenzen legalen Verhaltens geführt habe. Es sei nicht möglich, Computerprogrammen - wie es das Gesetz vorsehe - einem eindeutigen Zweck zuzuordnen. Der Zweck eines Computerprogramms leite sich in der Praxis vielmehr stets aus dem situativen Kontext ab, in welchem es verwendet werde. Gerade Programme, die typischerweise bei der Vorbereitung eines rechtswidrigen Angriffs auf einen Computer zum Einsatz kämen, verfügten oft auch über legitime Anwendungsfelder. Für die Verbesserung der Sicherheit heutiger und zukünftiger Computer und Software sei es zudem unerlässlich, Schadsoftware und Angriffsprogramme zu besitzen und detailliert zu analysieren. Der Chaos Computer Club hält § 202c StGB für ungeeignet, das Ziel einer Verbesserung der IT-Sicherheit zu erreichen. Die Verfügbarkeit potentieller Schadsoftware über das Internet und ausländische Quellen für Kriminelle werde durch die Vorschrift in keiner signifikanten Weise eingeschränkt. Umgekehrt werde die Arbeit an der Verbesserung von Sicherheitsstrukturen durch die Vorschrift erschwert.

[51] 4. Auch die Gesellschaft für Informatik e. V. hält § 202c StGB für eine zu weit geratene Strafvorschrift. Computerprogramme hätten typischerweise keinen eindeutigen „Zweck“; jedenfalls könne man einen solchen Zweck aus informationstechnischer Sicht nicht definieren. Selbst wenn der Entwickler (Programmierer) einen bestimmten - positiven - Zweck intendiere, könnten sie immer missbraucht werden. Umgekehrt könnten Angriffsprogramme (malware) auch für „gute“ Zwecke (Informationssicherheits-Prüfprogramme) genutzt werden und seien insofern sogar unverzichtbar. Gleiches gelte für den Einsatz von malware im Rahmen qualifizierter Lehre im Bereich der Informationssicherheit an Hochschulen; insofern könne regelmäßig davon ausgegangen werden, dass weder die Informatik-Professoren noch die Studierenden konkrete Taten planten oder auch nur vor Augen hätten.

IV.

[52] Der Beschwerdeführer F... hat zwischenzeitlich mitgeteilt, nicht mehr bei der Firma V... tätig zu sein, sondern in der deutschen Niederlassung des Schweizer Unternehmens C... AG. Er hat dargelegt, dass die Betätigungsfelder dieses Unternehmens, soweit hier von Interesse, denen der V... vergleichbar seien.

[53]

B.

[54] Die Verfassungsbeschwerden werden nicht zur Entscheidung angenommen.

[55] Die Annahmevoraussetzungen des § 93a Abs. 2 BVerfGG sind nicht erfüllt. Den Verfassungsbeschwerden kommt weder grundsätzliche verfassungsrechtliche Bedeutung zu noch ist ihre Annahme zur Durchsetzung der in § 90 Abs. 1 BVerfGG genannten Rechte angezeigt (vgl.BVerfGE 90, 22 <24 ff.>; 96, 245 <248 ff.>). Die Verfassungsbeschwerden sind mangels unmittelbarer Betroffenheit der Beschwerdeführer von der angegriffenen Norm unzulässig.

I.

[56] Die Zulässigkeit einer Verfassungsbeschwerde gegen ein Gesetz setzt nach der ständigen Rechtsprechung des Bundesverfassungsgerichts voraus, dass der Beschwerdeführer selbst, gegenwärtig und unmittelbar durch die angegriffenen Rechtsnormen in seinen Grundrechten betroffen ist (vgl. nurBVerfGE 1, 97 <101 ff.>). Eine unmittelbar aus dem Gesetz folgende Beschwer hat das Bundesverfassungsgericht unter anderem anerkannt, wenn das Gesetz den Betroffenen schon vor Erlass eines Vollzugsaktes zu entscheidenden Dispositionen veranlasst, die er nach dem späteren Gesetzesvollzug nicht mehr nachholen oder korrigieren könnte (vgl.BVerfGE 90, 128 <136>; 97, 157 <164>), und wenn er erst das Risiko eines

Bußgeld- oder Strafverfahrens eingehen müsste, um Rechtsschutz vor den Fachgerichten erwirken zu können (vgl.BVerfGE 20, 283 <290>; 46, 246 <256>; 81, 70 <82 f.>; 97, 157 <165>).

[57] Das Risiko einer Bestrafung besteht bereits dann, wenn ein grundrechtlich geschütztes Verhalten vom Wortlaut einer Strafnorm noch erfasst sein kann (vgl.BVerfGE 75, 329 <341>), also unter Zugrundelegung einer möglichen, nicht ganz fernliegenden Auslegung des Tatbestands unter diesen fällt. An einer unmittelbaren Beschwer durch eine Strafnorm fehlt es dagegen, wenn ein verfassungsrechtlich geschütztes Betätigungsfeld von der angegriffenen Norm nach deren Wortlaut, Entstehungsgeschichte und Systematik eindeutig nicht betroffen ist (BVerfGK 8, 75 <76>); denn eine im Wege der Auslegung vorgenommene Anwendung von Strafbestimmungen über deren Wortlaut hinaus wäre wegen Art. 103 Abs. 2 GG verfassungswidrig und braucht deshalb nicht in die Zumutbarkeitserwägungen einbezogen zu werden (BVerfGE 97, 157 <168>).

[58] In jedem Falle ist es Sache des Beschwerdeführers, die Einzelheiten der von ihm erstrebten Handlungen, deren Verbot er bekämpfen möchte, hinreichend substantiiert darzulegen, so dass das Bundesverfassungsgericht in die Lage versetzt wird, die Frage der unmittelbaren Betroffenheit zu beurteilen (§ 23 Abs. 1 Satz 2 i. V. m. § 92 BVerfGG).

II.

[59] Nach diesem Maßstab sind die Beschwerdeführer durch die angegriffene Strafvorschrift nicht beschwert.

[60] Soweit der Beschwerdeführer F... seine Verfassungsbeschwerde formell auch auf § 202c Abs. 1 Nr. 1 StGB erstreckt hat, geht er selbst auf diese Tatbestandsvariante nicht weiter ein; eine Betroffenheit des Beschwerdeführers von dem Verbot bestimmter auf Passwörter oder sonstige Sicherungscodes bezogener Vorbereitungshandlungen ist daher nicht erkennbar.

[61] Auf der Grundlage des Vorbringens der Beschwerdeführer lässt sich aber auch nicht feststellen, dass die von ihnen beschriebenen Tätigkeitsfelder von dem strafbewehrten Verbot des § 202c Abs. 1 Nr. 2 StGB erfasst würden; ein Risiko strafrechtlicher Verfolgung ist mithin nicht gegeben. Überwiegend sind die von den Beschwerdeführern eingesetzten Programme schon keine tauglichen Tatobjekte der Strafvorschrift in den Grenzen ihrer verfassungsrechtlich zulässigen Auslegung (dazu 1.). Soweit - im Falle des Beschwerdeführers F... - taugliche Tatobjekte vorliegen können, fehlt dem Beschwerdeführer jedenfalls der nach § 202c Abs. 1 Nr. 2 StGB erforderliche Vorbereitungsvorsatz (dazu 2.).

[62] 1. a) Tatobjekt des § 202c Abs. 1 Nr. 2 StGB kann nur ein Programm sein, dessen Zweck die Begehung einer Straftat nach § 202a StGB (Ausspähen von Daten) oder § 202b StGB (Abfangen von Daten) ist. Danach muss das Programm mit der Absicht entwickelt oder modifiziert worden sein, es zur Begehung der genannten Straftaten einzusetzen. Diese Absicht muss sich ferner objektiv manifestiert haben.

[63] aa) Schon nach dem Wortlaut nicht ausreichend wäre, dass ein Programm - wie das für so genannte dual use tools gilt - für die Begehung der genannten Computerstraftaten lediglich geeignet oder auch besonders geeignet ist. Der allgemeine Sprachgebrauch versteht unter „Zweck“ „etwas, was jemand mit einer Handlung beabsichtigt, zu bewirken, zu erreichen sucht; Beweggrund und Ziel einer Handlung“ (Duden, Das Große Wörterbuch der deutschen Sprache, 3. Aufl. 1999, S. 4706), also das Ziel, das willentlich durch den Einsatz bestimmter Mittel in Handlungen geplant und verfolgt wird (Brockhaus, Enzyklopädie, Bd. 30, 21. Aufl. 2006, S. 747), oder das, „was man mit einer Handlung will, die Aufgabe um deren Willen sie geschieht, das Ergebnis, das irgendwie hinter der Handlung als Endpunkt steht. Das Wort wird so von der Vernunft aus gesehen; man setzt voraus, dass, was man tut, eine Absicht zum Grunde hat, die man erkennt, die man andern mitteilen kann“ (Deutsches Wörterbuch von Jacob und Wilhelm Grimm, Bd. 32, 1954/1984, Sp. 959). Mit dieser finalen Dimension unterscheidet sich der Begriff des Zwecks deutlich von dem der Eignung; systematische und entstehungsgeschichtliche Erwägungen bestätigen diesen Befund.

[64] In systematischer Hinsicht ist darauf zu verweisen, dass das Gesetz an anderer Stelle ausdrücklich auf die Eignung von Gegenständen für die Begehung bestimmter Straftaten abstellt, insbesondere in § 149 StGB und § 275 StGB. § 149 StGB wird anknüpfend an die Gesetzesbegründung im Allgemeinen so ausgelegt, dass den dort benannten Fälschungsmitteln eine spezifische Verwendbarkeit zur Ausführung von Fälschungen innewohnen muss (Ruß, in: Leipziger Kommentar zum Strafgesetzbuch, Bd. 5, 11. Aufl. 2005, § 149 Rn. 3; Hoyer, in: Systematischer Kommentar zum Strafgesetzbuch, § 275 Rn. 2 <März 2007>); damit sei gemeint, dass diese Mittel nur zur Herstellung von Falsifikaten tauglich sein dürfen. Bereits deswegen sollen etwa solche Gegenstände aus dem Anwendungsbereich des § 149 StGB ausscheiden, die (lediglich) auch zur Geldfälschung verwendet werden können, etwa leistungsfähige Farbkopierer (vgl. Fischer, StGB, 55.

Aufl. 2008, § 149 Rn. 3; Erb, in: Münchener Kommentar zum StGB, 2005, § 149 Rn. 3). Zu den in § 149 StGB genannten Computerprogrammen wird vertreten, es müsse wenigstens ein abgrenzbares Programmmodul enthalten sein, dass ausschließlich zur Fälschung einsetzbar sei (Rudolphi/Stein, in: Systematischer Kommentar zum Strafgesetzbuch, § 149 Rn. 2 <März 2007>). All dies spricht dafür, den Begriff des Zwecks in § 202c Abs. 1 Nr. 2 in einem engeren Sinne als dem der Eignung oder auch der spezifischen Eignung zu verstehen.

[65] Die Entstehungsgeschichte des § 202c Abs. 1 Nr. 2 StGB schließlich belegt eindeutig, dass an die Eignung oder auch nur an die besondere Eignung von Programmen nicht angeknüpft werden sollte; durch den Rekurs auf den „Zweck" der Software sollten engere Voraussetzungen im Vergleich zur bloßen „Geeignetheit" aufgestellt werden (vgl. Popp, GA 2008, S. 375 <388>). In ihrer Gegenäußerung zu den Bedenken des Bundesrats erklärte die Bundesregierung, bei Programmen, deren funktionaler Zweck nicht eindeutig kriminell sei und die erst durch ihre Anwendung zu einem Tatwerkzeug eines Kriminellen oder aber zu einem legitimen Werkzeug würden - so genannten dual use tools - sei bereits der objektive Tatbestand des § 202c StGB nicht erfüllt (vgl. BTDrucks 16/3656, S. 18 f.). Die bloße Eignung von Software zur Begehung von Computerstraftaten sei nicht ausreichend, so dass auch solche Programme aus dem Tatbestand herausfielen, die lediglich zur Begehung von Computerstraftaten missbraucht werden könnten. Der Rechtsausschuss stellte zur Vermeidung von Missverständnissen in seinem Bericht an den Deutschen Bundestag klar, dass die bloße Geeignetheit eines Programms zur Begehung der betreffenden Straftaten keine Strafbarkeit nach § 202c StGB begründe. Die geforderte Zweckbestimmung müsse eine Eigenschaft des Computerprogramms in dem Sinne darstellen, dass es sich um so genannte Schadsoftware handle (vgl. BTDrucks 16/5449, S. 4).

[66] Nach alledem ließe es sich nicht vertreten, im Rahmen des § 202c Abs. 1 Nr. 2 StGB für die Bestimmung des Zwecks eines Computerprogramms auf dessen Eignung oder auch spezifische Eignung abzustellen. Eine solche Auslegung würde dem Wortlaut der Norm und dem Willen des Gesetzgebers widersprechen und stellte damit gleichzeitig einen Verstoß gegen Art. 103 Abs. 2 GG dar. Die in der Sachverständigenanhörung durch den Rechtsausschuss des Deutschen Bundestags (vgl. schriftliche Stellungnahmen des Sachverständigen Prof. Dr. Borges vom 19. März 2007, S. 6 ff.) und im Schrifttum (vgl. Gröseling/Höfinger, MMR 2007, S. 626 <629>; Schreibauer/Hessel, K&R 2007, S. 616 <618>; Cornelius, CR 2007, S. 682 f.) teilweise vertretene Auffassung, der objektive Tatbestand des § 202c Abs. 1 Nr. 2 StGB erfasse allgemein auch so genannte dual use tools, lässt sich nicht halten.

[67] bb) Schon die Entstehungsgeschichte der Vorschrift spricht hingegen deutlich dafür, die Absichten des Entwicklers des jeweiligen Programms als maßgeblich für dessen Zweckbestimmung zu erachten (so auch Popp, GA 2008, S. 375 <384>). Art. 6 Abs. 1 Buchstabe a Nr. i des Übereinkommens des Europarats, auf den § 202c Abs. 1 Nr. 2 zurückgeht, bezieht sich ausdrücklich auf eine „Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen" (im englischen Originaltext: „designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5"). Hier wird der Entstehungsvorgang des Programms in seiner konkreten Gestalt in den Blick genommen. Entsprechend sind nach der Beschlussempfehlung des Rechtsausschusses nur Computerprogramme gemeint, „die in erster Linie dafür ausgelegt oder hergestellt wurden, um damit Straftaten nach den § 202a, § 202b StGB zu begehen".

[68] Wenn andererseits neben dem Wortlaut der Vorschrift sowohl der Erläuternde Bericht zum Übereinkommen (siehe oben A. I. 2.) als auch zahlreiche Äußerungen im Gesetzgebungsverfahren (oben A. I. 3.) sowie teleologische und pragmatische Überlegungen (vgl. Popp, GA 2008, S. 375 <384>; Böhlke/Yilmaz, CR 2008, S. 261 <262>) den objektiven Charakter der mit der Vorschrift gemeinten Zweckbestimmung betonen, lässt sich dem Rechnung tragen durch eine Auslegung, die zwar von den Absichten des Programmentwicklers ausgeht, aber zusätzlich eine äußerlich feststellbare Manifestation dieser Absichten fordert. Eine solche Manifestation mag in der Gestalt des Programms selbst liegen - im Sinne einer Verwendungsabsicht, die sich nunmehr der Sache selbst interpretativ ablesen lässt (Popp, GA 2008, S. 375 <382>) - oder auch in einer eindeutig auf illegale Verwendungen abzielenden Vertriebspolitik und Werbung des Herstellers (vgl. Cornelius, CR 2007, S. 682 <688> unter Hinweis auf Parallelen im Urheberrecht und in der US-amerikanischen Rechtsprechung); dies im Einzelnen zu klären ist Aufgabe der hierfür zuständigen Fachgerichte.

[69] Eine sich an den objektiv manifestierten Absichten des Programmentwicklers orientierende Auslegung des § 202c Abs. 1 Nr. 2 StGB dürfte in der Sache mit Ansätzen im Schrifttum übereinstimmen, nach denen Programme den Tatbestand erfüllen sollen, wenn sie gerade im Hinblick auf eine spezielle Tatvariante einer Tat nach § 202a, § 202b geschrieben sind (Fischer, StGB, 55. Aufl. 2008, § 202c Rn. 5), wenn ihnen die Möglichkeit der Begehung entsprechender Straftaten als Kernbestandteil innewohnt (Böhlke/Yilmaz, CR 2008, S. 261 <263>) oder wenn sie bereits nach Art und Weise ihres Aufbaus darauf angelegt sind, illegalen

Zwecken zu dienen (Ernst, NJW 2007, S. 2661 <2663>). Ferner entspricht sie den Maßstäben, die das Bundesverfassungsgericht bereits für die Auslegung des § 22b Abs. 1 Nr. 3 StVG aufgestellt hat (BVerfGK 8, 75 <77>).

[70] b) Für die Situation der Beschwerdeführer ergibt sich Folgendes:

[71] Der Beschwerdeführer Prof. Dr. W... hat hinsichtlich der Programme, die er seinen Studenten zur Verfügung stellt, lediglich dargelegt, dass diese zur Begehung von Computerstraftaten geeignet sind, zu solchen Zwecken also verwendet werden können; konkret hat er das am Beispiel des Tools „nmap“ erläutert. Diese Eignung genügt zur Erfüllung des objektiven Tatbestands des § 202c Abs. 1 Nr. 2 StGB jedoch nicht. Der Beschwerdeführer hat keinerlei Angaben gemacht, die - wenn auch nur indiziell - auf eine deliktische Zweckbestimmung der betreffenden Software schließen ließen. Die Bezeichnung dieser Programme als „Sicherheitsanalysewerkzeuge“ deutet ganz im Gegenteil darauf hin, dass der - legitime - Zweck der Sicherheitsanalyse bei diesen Instrumenten im Vordergrund steht. Zu deliktischen Absichten der Entwickler der betreffenden Programme hat sich der Beschwerdeführer weder geäußert, noch hat er auf eine Manifestation solcher Absichten hingewiesen. Auch der Beschwerdeführer K... hat die Erfüllung des objektiven Tatbestands des § 202c Abs. 1 Nr. 2 StGB durch die von ihm verwendeten Linux-Distributionen nicht dargelegt. Er geht - wie der Beschwerdeführer Prof. Dr. W... - nur auf die Eignung der von ihm verwendeten Programme für die Begehung von Computerstraftaten ein.

[72] Der Beschwerdeführer F... hat hingegen vorgetragen, dass er im Rahmen seiner beruflichen Tätigkeit nicht nur objektiv (auch) zur Begehung von Computerstraftaten geeignete Software, also dual-use-Software, verwendet, sondern darüber hinaus „Schadsoftware“ aus zweifelhaften Quellen im Internet beschafft oder beschaffen lässt, um sie bei Penetrationstests einzusetzen. Während nach dem Gesagten die verwendete (bloße) dual-use-Software nicht unter den objektiven Tatbestand des § 202c Abs. 1 Nr. 2 StGB fällt, kann hinsichtlich der vom Beschwerdeführer so bezeichneten Schadsoftware angesichts deren Herkunft und Vertriebsweise durchaus angenommen werden, dass sie gerade zum Zweck der Begehung rechtswidriger Taten entwickelt wurde und über Eigenschaften verfügt, in denen sich diese Zweckbestimmung manifestiert.

[73] 2. Insoweit scheitert eine mögliche Strafbarkeit des Beschwerdeführers nach § 202c Abs. 1 Nr. 2 StGB (gegebenenfalls in Verbindung mit § 25 Abs. 1 Var. 2, § 25 Abs. 2, § 26 oder § 27 StGB) jedoch jedenfalls an dem subjektiven Merkmal der Vorbereitung einer Computerstraftat.

[74] a) Hinsichtlich der vom Gesetz insofern umfassten Vorsatzformen herrscht im Schrifttum zu § 202c StGB weitestgehend Einigkeit, dass Eventualvorsatz ausreichen soll (vgl. Fischer, StGB, 55. Aufl. 2008, § 202c Rn. 7; Schumann, NStZ 2007, S. 675 <678 f.>; Popp, GA 2008, S. 375 <391>). In systematischer Hinsicht spricht hierfür das entsprechende einhellige Meinungsbild zu den im Hinblick auf das Vorbereitungsmerkmal gleich formulierten Vorschriften von § 149, § 275 und § 263a Abs. 3 StGB (vgl. Ruß, in: Leipziger Kommentar zum Strafgesetzbuch, Bd. 5, 11. Aufl. 2005, § 149 Rn. 6; Sternberg-Lieben, in: Schönke/Schröder, StGB, 27. Aufl. 2006, § 149 Rn. 8; Fischer, a.a.O., § 263a Rn. 34; Hoyer, in: Systematischer Kommentar zum Strafgesetzbuch, § 263a Rn. 61 <März 2007>; Kindhäuser, in: Nomos Kommentar zum Strafgesetzbuch, Bd. 2, 2. Aufl. 2005, § 263a Rn. 44; Gribbohm, in: Leipziger Kommentar zum Strafgesetzbuch, Bd. 7, 11. Aufl. 2005, § 275 Rn. 11; Hoyer, in: Systematischer Kommentar zum Strafgesetzbuch, § 275 Rn. 4 <März 2007>; Puppe, in: Nomos Kommentar zum Strafgesetzbuch, Bd. 2, 2. Aufl. 2005, § 275 Rn. 11).

[75] Legt man diese Auffassung (zur Kritik im Hinblick auf die Entstehungsgeschichte vgl. Popp, GA 2008, S. 375 <391 f.>) zugrunde, so muss der Täter lediglich damit rechnen, dass das tatgegenständliche Programm zukünftig zur Begehung von Straftaten gebraucht wird (kognitives Element), und diese Benutzung des Programms billigend in Kauf nehmen (voluntatives Element). Nach der Rechtsprechung des Bundesgerichtshofs billigt der Täter auch einen an sich unerwünschten, aber notwendigen Erfolg, wenn er sich mit ihm um eines erstrebten Zieles willen abfindet (vgl. nur Fischer, a.a.O., § 15 Rn. 9a mit umfassenden Nachweisen). Andererseits setzt die Feststellung gerade des voluntativen Elements des Eventualvorsatzes in Abgrenzung zur bewussten Fahrlässigkeit im Einzelfall konkrete tatsächliche Anhaltspunkte voraus (vgl. BGH, Beschluss vom 5. März 2008 - 2 StR 50/08 -, juris Rn. 4; Beschluss vom 26. August 2003 - 5 StR 145/03 -, juris Rn. 46, 49 m.w.N.; vgl. auch Beschluss vom 16. April 2008 - 5 StR 615/07 -, juris Rn. 5).

[76] b) Hinsichtlich des Beschwerdeführers F... oder seiner Mitarbeiter ist nach diesen Maßstäben auf der Grundlage des Beschwerdevorbringens nicht zu sehen, dass diese das subjektive Merkmal der Vorbereitung einer Straftat nach § 202a oder § 202b StGB erfüllen, soweit sie objektiv unter den Tatbestand des § 202c Abs. 1 Nr. 2 StGB fallende Programme beschaffen oder diese innerhalb des Unternehmens weitergeben. Denn die bei diesen Tätigkeiten in Aussicht genommene Verwendung der Programme im Rahmen von Penetrationstests erfüllt den Tatbestand des § 202a oder § 202b StGB zweifellos nicht: Da die Unternehmen, für die der Beschwerdeführer tätig wird oder tätig geworden ist, im Auftrag und somit im Einverständnis mit

den über die überprüften Computersysteme Verfügungsberechtigten handeln, fehlt es am Tatbestandsmerkmal des „unbefugten“ Handelns, wie auch der Generalbundesanwalt betont hat. Zu einem solchen legalen Zweck dürfen nach dem insofern eindeutigen und durch die Äußerungen im Zuge der Entstehungsgeschichte sowie Art. 6 Abs. 2 des Übereinkommens des Europarats bekräftigten Wortlaut des § 202c Abs. 1 Nr. 2 StGB jedoch grundsätzlich auch Schadprogramme, deren objektiver Zweck in der Begehung von Computerstraftaten liegt, beschafft oder weitergegeben werden - und zwar auch dann, wenn aufgrund der Herkunft der Programme, etwa aus zweifelhaften Internetforen, der Verdacht nahe liegt, dass andere Nutzer der gleichen Quelle keine lauteren Absichten verfolgen (vgl. auch Böhlke/Yilmaz, CR 2008, S. 261 <264>; Popp, GA 2008, S. 375 <392 f.>). Sieht der Beschwerdeführer hier Risiken einer strafrechtlichen Verfolgung, kann er diese unter anderem durch eine umfassende Dokumentation der Verfahrensabläufe und der erteilten Bewilligung des Auftraggebers für sein Tätigwerden weiter verringern (vgl. Böhlke/Yilmaz, a.a.O., S. 261 <266>).

[77] Zwar kann sich im Rahmen eines solchen Einsatzes objektiv unter § 202c Abs. 1 Nr. 2 StGB fallender Programme zu erlaubten Zwecken ein Strafbarkeitsrisiko ergeben, sobald die betreffenden Programme durch Verkauf, Überlassung, Verbreitung oder anderweitig auch Personen zugänglich gemacht werden, von deren Vertrauenswürdigkeit nicht ausgegangen werden kann. Hier macht sich auch ein Akteur, dessen eigentliche Absicht in einer legalen Verwendung des Programms liegt, dann strafbar, wenn er gleichwohl damit rechnet und es auch billigend in Kauf nimmt, dass die Person oder die Personen, die durch seine Handlung Zugang zu dem Programm erhalten, dieses zumindest unter anderem zu rechtswidrigen Zwecken einsetzen. Wie das Bundesministerium der Justiz in seiner Stellungnahme zur Verfassungsbeschwerde hervorgehoben hat, liegt die Annahme eines solchen Vorsatzes beispielsweise auch dann nahe, wenn die handelnde Person das Programm einem von ihr nicht mehr überschaubaren Personenkreis zugänglich macht, etwa durch freies Einstellen ins Internet oder durch Zurverfügungstellen innerhalb von Foren mit entsprechendem Mitgliederkreis. Dass aber die Firma V... Schadprogramme außerhalb des Unternehmens verbreiten würde und darauf zur Ausübung ihrer gewerblichen Tätigkeit auch angewiesen wäre, ist weder vorgetragen noch ersichtlich; nichts anderes gilt für den neuen Arbeitgeber des Beschwerdeführers, die Firma C... AG. Insbesondere hat der Beschwerdeführer nicht dargelegt, dass er oder seine Mitarbeiter darauf angewiesen wären, die von ihnen rechtmäßig verwendete Software über offene oder halboffene Foren nicht nur zu beziehen, sondern dort Software auch selbst einzustellen und so zu verbreiten.

[78] Ob im Falle des Beschwerdeführers Prof. Dr. W... davon ausgegangen werden kann, dass dieser sich in einer dem voluntativen Element des Eventualvorsatzes genügenden Weise mit einem rechtswidrigen Einsatz der von ihm verbreiteten Programme abfindet, kann offen bleiben, weil es im Falle dieses Beschwerdeführers wie in dem des Beschwerdeführers K... schon nach dem Beschwerdevorbringen an tauglichen Tatobjekten fehlt (oben 1. b).

[79] Diese Entscheidung ist unanfechtbar.