Privatdozent Dr. Carl-Friedrich Stuckenberg, LL.M. *(Harvard)* 13.3.2007

Strafrechtliches Institut der
Rechts- und Staatswissenschaftlichen Fakultät der
Rheinischen Friedrich-Wilhelms-Universität Bonn

Stellungnahme

zum Gesetzentwurf der Bundesregierung – Entwurf eines … Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (… StrÄndG), BT-Drs. 16/3656

für die öffentliche Anhörung am 21. März 2007

Der Gesetzentwurf dient der Umsetzung der Anforderungen des Rahmenbeschlusses des Rates der Europäischen Union (2005/222/JI) vom 24.2.2005 über Angriffe auf Informationssysteme (ABl.EU L 69/67 vom 16.3.2005) und des Übereinkommens des Europarats vom 23.11.2001 über Computerkriminalität (Cybercrime Convention, ETS No. 185), dessen Ratifikation geplant ist. Die kriminalpolitischen Weichenstellungen sind daher weitgehend durch supranationales bzw. Völkerrecht vorgeben. Spielraum sowie Anlaß zu Verbesserungen bleibt gleichwohl:

I. Zu §§ 202a, 202b E-StGB

1. Die Erstreckung des Tatbestands des Ausspähens von Daten (§ 202a StGB) auf den unbefugten Zugang *(Hacking)* zu fremden Daten schließt zu Recht eine Lücke, die der Gesetzgeber 1986 bewußt gelassen hatte, wenn sich der Täter keine Daten „verschafft" – obschon dies praktisch eher selten sein dürfte. Nötig bleibt die Überwindung einer besonderen Zugangssicherung, was unbedenklich erscheint.

   Die Auslegung der Entwurfsbegründung (S. 14, 31), daß die unbefugte Ingebrauchnahme gesicherter elektronischer Geräte nicht erfaßt wird, erscheint zutreffend. Gewiß kann es hier Bagatellfälle geben – wie bei zahlreichen anderen Straftatbeständen auch, die genauso nach §§ 153 ff. StPO zu behandeln wären.

2. § 202b E-StGB, der auch ungesicherte Daten schützt, setzt Art. 3 der Europarats-Konvention um. Die bisweilen zu findende Kritik am Begriff des „Abfangens“ sowie an der „nichtöffentlichen Datenübermittlung“ verkennt, daß dies die Vorgaben der Konvention sind, die von „interception of non-public transmissions“ spricht. Fehlinterpretationen liegen nicht nahe. Gegen eine Lokalisierung der Vorschrift als weiteren Absatz des § 202a spricht der unterschiedliche Schutzgegenstand (geschützte/ungeschützte Daten), der sich in unterschiedlichen Strafrahmen spiegelt.

3. **Versuchsstrafbarkeit**
   §§ 202a und 202b des Entwurfs verzichten auf eine Versuchsstrafbarkeit, was die Konvention freistellt. Grundsätzlich ist eine Begrenzung der Strafbarkeit stets zu begrüßen, doch führt dies hier zu einem unlogischen Systembruch, da in § 202c E-StGB Vorbereitungshandlungen zu diesen Delikten bzw. abstrakte Gefährdungen unter Strafe gestellt werden, obwohl nicht einmal deren Versuch strafbar ist. Bei §§ 303a und 303b, für die § 202c entsprechend geltend soll (§§ 303a Abs. 3, 303b Abs. 5 E-StGB), tritt das Problem nicht auf, da beide Vorschriften den Versuch unter Strafe stellen. Für eine Versuchsstrafbarkeit spricht auch der Vergleich mit dem strukturell gleichartigen § 149 StGB, der Vorbereitungshandlungen zu §§ 146, 148 StGB (Geld- und Wertzeichenfälschung) erfaßt, deren Versuch jeweils strafbar ist (ebenso bei § 263a Abs. 2 und 3 [Computerbetrug] und §§ 275, 273 StGB [Fälschen amtlicher Ausweise]).

   Dafür spricht weiterhin, daß gemäß dem neuen **§ 205 E-StGB** die §§ 202a, 202b gemischte Antragsdelikte sind, während § 202c Offizialdelikt ist. Aus der fehlenden Versuchsstrafbarkeit in §§ 202a, 202b E-StGB ergibt sich die ungereimte Folge, daß eine Verletzung der Schutzgüter der §§ 202a, 202b regelmäßig nur auf Antrag, die konkrete Gefährdung (Versuch) überhaupt nicht und die abstrakte Gefährdung (§ 202c E-StGB) von Amts wegen verfolgt würde.

   Wenn der Vorbereitungstatbestand des § 202c nicht zur Disposition steht, verlangt das Gebot der Widerspruchsfreiheit eine Versuchsstrafbarkeit, da es widersprüchlich ist, die Vorbereitung einer Tat nach §§ 202a, 202b als strafwürdig anzusehen, deren Versuch aber nicht. Eine Überdehnung der Strafbarkeit ist nicht zu befürchten, da zum einen die Schwelle zur Vollendung gering ist. Zum anderen läßt sich auch bei isolierter Betrachtung in einem fehlgeschlagenen Versuch, sich unbefugt Zugang zu gesicherten Daten zu verschaffen oder ungesicherte Daten abzufangen, strafwürdiges Unrecht erblicken: Warum sollte derjenige, der versucht, in seines Nachbarn (un)gesichertes WLAN einzudringen, um zu sehen, welche Emails

dieser schreibt, weniger strafbar sein als derjenige, der versucht, seines Nachbarn Telefon abzuhören (§ 201 Abs. 4 StGB)?

II. Zu § 202c E-StGB

1. § 202c setzt Art. 6 der Europarats-Konvention um (Textvergleich im Anhang) und verlagert die Strafbarkeit der §§ 202a, 202b, 303a, 303b weit ins Vorfeld durch umfassende Kriminalisierung des Umgangs mit den typischen Tatmitteln. Auf die prinzipiellen Bedenken gegen solche Vorfeldtatbestände, die zu einer Hypertrophie des Strafrechts führen, kann hier nur hingewiesen werden,[1] ebenso auf die Frage, ob die Verbreitung der Tatmittel damit wirksam eingedämmt werden kann, selbst wenn noch mehr Staaten dem Europarats-Übereinkommen beitreten, oder ob lediglich ein neuer illegaler Markt geschaffen wird.

2. Die von der Konvention in Art. 6 Abs. 3 eröffnete Möglichkeit, auf die Poenalisierung von Computerprogrammen zu verzichten, wird nicht genutzt. Dies erscheint vertretbar, da es in der Tat Programme wie im Internet bisher frei kursierende Virenbausätze – das digitale Pendant zur Bombenbauanleitung – gibt, mit denen sich nur Schaden anrichten läßt und deren schiere Verfügbarkeit Straftaten erst ermöglicht und dazu anreizt.

   Der Entwurf verzichtet aber auf die Erfassung des bloßen Besitzes als inkriminierte Verhaltensform sowie von „Vorrichtungen“ („devices“) als Tatmittel. Der Verzicht auf einen Besitztatbestand erinnert daran, daß die 1933 eingeführte Bestrafung des Besitzes von Diebeswerkzeug in § 245a a.F. StGB 1969 als rechtsstaatlich bedenklich und praktisch wirkungslos aufgehoben wurde. Allerdings ist der Verzicht auf die Bestrafung des Besitzes praktisch ebenfalls bedeutungslos, denn wer solche Software besitzt, hat sie sich zuvor irgendwie „verschafft“.

3. **Umfang der Kriminalisierung von Computerprogrammen**
   Bei § 202c Abs. 1 Satz 2 E-StGB ergibt sich das Problem, den Kreis der Tatmittel, mit denen der Umgang verboten wird, sicher und deutlich abzugrenzen, um eine Überkriminalisierung zu verhindern. Denn auch harmlose Allerweltsprogramme lassen sich zu Straftaten nach §§ 202a ff. verwenden. Bloße *Eignung* zu kriminellem Gebrauch darf demnach nicht genügen. Die Europarats-Konvention verwendet einige Mühe auf die Begrenzung durch

---

[1] Vgl. zum strukturgleichen § 263a Abs. 3 StGB die harsche Kritik von *Duttge*, Festschrift für Weber, 2004, S. 284, 287 ff.

(i) eine objektive Beschränkung auf *vorwiegend* zu kriminellen Zwecken hergestellte oder angepaßte Programme ("a computer program, designed or adapted *primarily* for the purpose of committing any of the offences"), womit *dual use tools* in aller Regel[2] ausgeschlossen sein sollen,

(ii) eine subjektive Beschränkung, daß der Umgang mit dem direkten Vorsatz geschehen muß, daß mit dem Programm eine der genannten Straftaten begangen wird ("with intent that it be used for the purpose of committing any of the offences"),

(iii) das (unklare) Merkmal „rechtswidrig"/„unbefugt" ("without right") und

(iv) durch die Auslegungsanweisung in Art. 6 Abs. 2, daß die Vorschrift nicht so zu interpretieren ist, daß sie den Umgang mit solchen Programmen zu anderen Zwecken, namentlich zu Prüfung und Schutz von Computersystemen, bestraft.

a) Der Gesetzentwurf verwendet eine knappere und leichtfüßigere Formulierung als der schwerfällige Konventionstext, ist dadurch aber auch weniger klar:

ad (i) Der Gesetzentwurf übernimmt die objektive Zweckbestimmung („deren Zweck die Begehung einer solchen Tat ist", insoweit wortgleich mit § 263a Abs. 3 StGB) ohne das qualifizierende „vorwiegend"/"primarily" – man könnte sogar meinen, der Entwurfstext sei strenger und verlange einen alleinigen kriminellen Zweck. Hingegen lockert die Begründung die Zweckbestimmung wieder auf, wenn es heißt, das Programm müsse „aber nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reicht, wenn die objektive Zweckbestimmung des Tools *auch* die Begehung einer solchen Straftat ist." (S. 20). Fast dieselbe Gesetzesbegründung findet sich zu § 263a Abs. 3 StGB[3] und ist dort mit Fug als unklar moniert worden.[4] Dieser Fehler sollte hier nicht wiederholt, vielmehr im Sinne des Konventionstextes klargestellt werden, daß der *primäre, vorwiegende* Zweck die Begehung der genannten Straftaten sein muß und bloße Eignung nicht reicht. Da Zwecke immer subjektiv vom Verwender be-

---

2 Die Formulierung ist ein Kompromiß zwischen ausschließlicher objektiver krimineller Zweckbestimmung und bloß subjektiver Umgrenzung, siehe Convention on Cybercrime, Explanatory Report, 8 November 2001, No. 73.

3 BT-Drs. 15/1720, S. 10 f.; dazu *Husemann*, NJW 2004, 104, 108.

4 Z.B. Tröndle/*Fischer*[53], § 263a Rn. 30 f. („damit sind alle Fragen offen …").

stimmt werden, kann sich die „objektive“ Zweckbestimmung letztlich nur darauf beziehen, daß das Programm *so gestaltet* („designed“) ist, daß es hauptsächlich nur zu kriminellen Zwecken verwendet werden *kann*. § 126c öStGB („das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung … geschaffen oder adaptiert worden ist“), aber auch der insoweit parallele § 149 Abs. 1 Nr. 1 StGB („ … die ihrer Art nach zur Begehung einer solchen Tat bestimmt sind“) formulieren dies genauer. Programme mit unspezifischem Anwendungsprofil wären damit ausgeschlossen. Ob Programme, die sowohl berechtigt als auch unberechtigt verwendet werden können (*dual use tools*), aber ein hohes Mißbrauchspotential aufweisen,[5] erfaßt sind, ist nach Text und Begründung unklar und wird erst in der Gegenäußerung der Bundesregierung verneint (S. 33). Solche Zweifelsfragen sollten durch eine eindeutige Gesetzesformulierung von vornherein vermieden werden.

ad (ii), (iii): Die Merkmale „without right“ („unbefugt“) und das Vorsatzerfordernis („with intent that it be used for the purpose of committing …“) der Konvention werden durch die Formulierung „Wer eine Straftat nach … vorbereitet“ ersetzt – eine elegante Lösung, da das Merkmal „unbefugt“ in §§ 202a, 202b ohnehin enthalten ist (ein zusätzliches Merkmal „unbefugt“ verwiese entweder überflüssigerweise auf die allgemeinen Rechtfertigungsgründe oder erforderte ein verwaltungsrechtliches Regime für Software wie im Waffenrecht) und der Vorsatz sich schon nach allgemeinen Regeln (§ 15 StGB) auf die Vorbereitung beziehen muß. Dadurch wird freilich über die Anforderungen der Konvention hinaus auch *dolus eventualis* erfaßt: Die von der Konvention verwendeten Ausdrücke “intent”/“intention“ umfassen nur die beiden Formen des *dolus directus*, Wissentlichkeit und Absicht im engen Sinne.[6] Der Terminus „Vorbereiten“ wirft außerdem vermeidbare Probleme auf (dazu 4.).

Zu erwägen ist, ob der subjektive Tatbestand des § 202c Abs. 1 Nr. 2 E-StGB nicht auch enger gefaßt werden muß. Zwar ist stets der Vorsatz vonnöten, daß mit der Software Taten nach §§ 202a, 202b E-StGB begangen werden – folglich wird die Verwendung von Testprogrammen zu Zwecken der Forschung und Entwicklung nicht erfaßt. Doch genügt, wie bei §§ 149 Abs. 1, 263a Abs. 3, 275 Abs. 1 StGB, bereits *dolus eventualis* hinsichtlich einer illegalen Verwendung, also die Vorstellung von deren Möglichkeit. Diese Möglichkeit einer illegalen Ver-

---

5 Vgl. für § 263a Abs. 3 StGB Tröndle/*Fischer*[53], § 263a Rn. 32.

6 Convention on Cybercrime, Explanatory Report, 8 November 2001, No. 76.

wendung dazu geeigneter Software ist jedoch auch bei ansonsten legaler Nutzung (Beispiel unten b) oftmals nicht auszuschließen. Vorzuziehen wäre deshalb eine Begrenzung der subjektiven Tatseite auf Wissentlichkeit und Absicht (*dolus directus* 1. und 2. Grades), was der Konvention genau entspräche.

ad (iv): Auf die Klarstellung in Art. 6 Abs. 2 der Konvention, daß die Vorschrift nicht so auszulegen ist, daß Test und Schutz von Computersystemen beeinträchtigt würden, verzichtet der Entwurf. Auch dies ist elegant, denn wer nur die Sicherheit seines Netzwerks testen will, dem fehlt eben der Vorsatz, eine der genannten Straftaten vorzubereiten (er handelte ja „befugt" und erfüllt daher §§ 202a, 202b nicht). Art. 6 Abs. 2 der Konvention ist folglich normativ überflüssig. Damit soviel Eleganz nicht zu Lasten der Normenklarheit geht, sollte der deklaratorische Inhalt des Art. 6 Abs. 2 der Konvention dennoch wenigstens in die Gesetzesbegründung aufgenommen werden.

b) **Anwendungsbeispiele:**
Seit Bekanntwerden des Gesetzentwurfs ist vielfach befürchtet worden, die vorgelegte Fassung des § 202c Abs. 1 Nr. 2 E-StGB könne bei weiter Auslegung auch Arten des Umgangs mit Software erfassen, die im Bereich der IT-Sicherheit etabliert und unverzichtbar sind. Beispiele:

(1) Die Analyse der ordnungsgemäßen Funktion und Entdeckung von Schwachstellen von IT-Systemen verlangt, daß Administratoren die Systeme mit geeigneten Software-Tools abfragen und so über den Systemzustand Auskunft erhalten können. Dieselben Analysetools können aber auch von potentiellen Angreifern genutzt werden, um Taten nach §§ 202a, 202b StGB zu begehen. Eine eindeutige objektive Zweckbestimmung solcher Programme läßt sich somit nicht angeben *(dual use tools). Das* „Hacker-Tool" gibt es so nicht. So überprüft ein Administrator in regelmäßigen Abständen die Sicherheit der Paßworte seiner Anwender durch ein Programm, das alle möglichen Paßworte durchprobiert und dann auf das Paßwort des Nutzers stößt. Das Ziel ist, Nutzer mit unsicheren Paßworten zu informieren, zur Änderung des Paßwortes aufzufordern und so die Sicherheit des IT-Systems zu erhöhen. Ein Angreifer kann dasselbe Programm nutzen, um Paßworte zu brechen und sich damit unberechtigten Zugang zu IT-Systemen zu verschaffen.

Die in der Gegenäußerung der Bundesregierung vertretene Auffassung, daß *dual use tools* nicht unter den objektiven Tatbestand fallen

(S. 33), sollte deshalb im Gesetzeswortlaut einen klaren Ausdruck finden durch Präzisierung des Tatbestandsmerkmals der objektiven Zweckbestimmung. Denn bislang geht die gewollte Begrenzung aus dem Gesetzestext nicht hervor.

(2) Es gibt zweifellos Programme, denen die illegale Verwendung immanent ist, wie Viren, Würmer etc. und entsprechende „Bausätze", die folglich unter den objektiven Tatbestand des § 202c Abs. 1 Nr. 2 E-StGB fallen. Der Schutz von Computersystemen gegen solche Schadsoftware erfordert deren Untersuchung, um Abwehrstrategien entwikkeln zu können. Dies geschieht häufig durch Diskussion im Internet, die regelmäßig auch die Versendung der zu bekämpfenden Schadsoftware in offenen oder halb-offenen Foren erfordert, weil sonst über deren Funktionsweise und Abwehrmöglichkeiten nicht gesprochen werden kann. Diese in der Praxis der IT-Sicherheit etablierten Methoden gelten als unabdingbar. Damit wäre der objektive Tatbestand des § 202c Abs. 1 Nr. 2 E-StGB durch Sich-Verschaffen, Verbreiten, Überlassen und Zugänglichmachen erfüllt und die Strafbarkeit hängt nur noch vom Vorliegen des Vorsatzes ab. Natürlich ist das Ziel hierbei nicht die Vorbereitung von Straftaten nach §§ 202a, 202b, sondern deren Verhinderung. Gleichwohl ist den Beteiligten stets bewußt, daß sie nicht ausschließen können, daß jemand ein im Internet zugänglich gemachtes Schadprogramm zu illegalen Zwecken einsetzt – *dolus eventualis* liegt somit vor. Ohne die Inkaufnahme dieses Risikos, das wohl nicht völlig beseitigt werden kann, würden aber die derzeitigen Mechanismen der IT-Sicherheit nicht funktionieren.

   Darauf zu vertrauen, daß die Rechtsprechung hier Wege findet, einen bedingten Vorsatz dennoch zu abzulehnen (etwa durch Verneinen des voluntativen Vorsatzelements mangels „billigenden" Inkaufnehmens), erscheint zu unsicher, um die explizite Vorgabe der Konvention, daß Handlungen zum Test und Schutz von IT-Systemen straflos bleiben sollen, zu erfüllen.

Nach der Intention der Entwurfsverfasser sind beide Fälle straflos. Diese Auslegung ist auch möglich, aber schon im zweiten Beispielsfall schwierig. Hinzu kommt, daß die geplante Gesetzesfassung einen *chilling effect* auf die Entwicklung von Analyse-Tools usw. haben könnte, da die Entwickler als juristische Laien dem Risiko, sich strafbar zu machen, großräumig ausweichen werden.

Besser wäre, die Gefahr einer ungewollten Ausdehnung durch einen eindeutigen Gesetzestext sicher zu vermeiden und deshalb den objektiven

und subjektiven Tatbestand des § 202c Abs. 1 Nr. 2 E-StGB klarer und enger zu fassen Die betroffenen Fachkreise könnten dann schon mit Hilfe des Gesetzestextes und nicht erst durch juristische Beratung den strafbaren Bereich klar erkennen – wie es das Bestimmtheitsgebot des Art. 103 Abs. 2 GG fordert[7].

4. **Deliktstyp: Vorbereitungshandlung oder abstraktes Gefährdungsdelikt?**

Die Übernahme der Formulierung aus §§ 149 Abs. 1, 263a Abs. 3, 275 Abs. 1 StGB („wer eine Straftat nach … vorbereitet, indem er") führt dazu, die dortigen Auslegungsprobleme[8] gleich mit zu übernehmen. Der Wortlaut macht nicht deutlich, ob es sich wirklich um eine Vorbereitungshandlung zu einer konkreten Tat nach §§ 202a, 202b handeln muß oder um die abstrakte Gefahr, daß irgendwer irgendwann Taten nach §§ 202a, 202b StGB begeht – mithin, ob eine Vorverlagerung der Strafbarkeit in das Vorbereitungsstadium einer konkreten geplanten Tat nach §§ 202a, 202b (sowie §§ 303a, 303b) vorliegt oder ein typisiertes, verselbständigtes Vorbereitungsdelikt im Sinne eines abstrakten Gefährdungsdelikts. Damit entscheidet sich auch, ob sich der Vorsatz im Sinne einer überschießenden Innentendenz auf eine konkretisierte Tat beziehen muß oder nicht.[9] Der Wortlaut des Art. 6 der Europarats-Konvention ist gleichermaßen undeutlich („with intent that it *be* used for the purpose of committing *any* of the offences"). Die Weitergabe etc. von Paßwörtern und ähnlichen Zugangsdaten in § 202c Abs. 1 Nr. 1 legt einerseits den Bezug auf konkrete Taten nahe mit einer konkreten Gefahr nach §§ 202a, 202b. Da andererseits offensichtlich mit § 202c Abs. 1 Nr. 2 die generelle Kriminalisierung von „Hacker-Tools" etc. angestrebt wird, ist zumindest hiermit ein abstraktes Gefährdungsdelikt gemeint – denn es sollte nicht darauf ankommen, ob derjenige, der solche Programme vertreibt, eine konkrete Anwendung vor Augen hat.

---

7 Art. 103 Abs. 2 GG „verpflichtet den Gesetzgeber, die Voraussetzungen der Strafbarkeit so genau zu umschreiben, daß Tragweite und Anwendungsbereich der Straftatbestände schon aus dem Gesetz selbst zu erkennen sind und sich durch Auslegung ermitteln und konkretisieren lassen", st. Rspr., BVerfGE 73, 206, 234; 75, 329, 340; 78, 374, 381 f.; 2 BvR 930/04 vom 9.12.2004, Rn. 21 = NJW 2005, 2140, 2141.

8 Siehe nur Tröndle/*Fischer*[53], § 149 Rn. 1, 5; § 263a Rn. 34; § 275 Rn. 3a.

9 Vgl. den Meinungsstand zu § 149 StGB: (1) für Konkretisierung: LK[11]-*Ruß*, § 149 Rn. 7; SK-StGB-*Rudolphi*, § 149 Rn. 2; Schönke/Schröder[27]/*Stree/Sternberg-Lieben*, § 149 Rn. 7; ähnl. Tröndle/*Fischer*[53], § 149 Rn. 5; (2) gegen Konkretisierung: Lackner/*Kühl*[25], § 149 Rn. 5; § 263a Rn. 26c; NK-StGB[2]-*Puppe*, § 149 Rn. 3, 13; § 275 Rn. 11; *Herzberg*, NJW 1977, 469, 470; auch MüKo-*Erb*, § 149 Rn. 6.

Die Entwurfsbegründung geht später (S. 19) von einem „abstrakten Gefährdungsdelikt“ aus. Das sollte wenigstens in der Begründung zu § 202c (und nicht erst zu § 205) genügend klargestellt werden, um den bei §§ 149, 263a, 275 StGB existierenden Streit gar nicht erst aufkommen zu lassen. Vorzuziehen wäre, auf den Ausdruck „Vorbereiten“ – dann auch in §§ 303a Abs. 3, 303b Abs. 5 E-StGB – ganz zu verzichten, weil es weniger um Vorbereiten konkreter Taten als um abstraktes Ermöglichen, Fördern geht. Der Begriff wird zudem in Art. 6 der Konvention nicht benutzt (die Überschrift lautet, allerdings ebenfalls wenig treffend, “Misuse of devices”; wörtlich genauso die österreichische Norm „Missbrauch von Computerprogrammen oder Zugangsdaten“) und führt nur auf die falsche Fährte wie bei §§ 149, 263a Abs. 3, 275 StGB. Als Vorbild mag die österreichische Umsetzungsvorschrift dienen (z.B. „Wer … herstellt, … oder sonst zugänglich macht, mit dem Wissen oder in der Absicht, daß sie zur Begehung einer in Nr. … genannten Tat verwendet werden …“ o.ä.).

5. **Praktische Bedeutung**

Daß § 202c besonders häufig zur Anwendung kommen wird, ist trotz seiner Weite kaum zu erwarten, von den allgemeinen Schwierigkeiten der Strafverfolgung von Internetkriminalität ganz abgesehen. Wenn alle Programme, die nicht eindeutig vorwiegend nur zu illegalen Zwecken nutzbar sind, vom objektiven Tatbestand nicht erfaßt werden, bleiben womöglich nicht mehr viele übrig. Nachgewiesen werden muß zudem in jedem Einzelfall der Vorsatz, damit eine Straftat „vorzubereiten“. Dieser Nachweis wird sich regelmäßig auf objektive Indizien stützen. Aussagekräftig dürften wiederum allein der Umgang mit solcher Software sein, die praktisch keinen legalen Zielen dienen kann. Die vorgeschlagenen Beschränkungen des Tatbestands ändern daran nichts, sondern schließen nur Fälle, die ohnehin nicht erfaßt sein sollen, sicherer aus.

III. Phishing und § 202c E-StGB

Es ist vielfach gefordert worden, einen besonderen Straftatbestand für „Phishing“ zu schaffen. Die Bundesregierung und die Mehrzahl der von ihr befragten Landesjustizverwaltungen vertreten indes zu Recht den Standpunkt, daß Phishing bereits vom geltenden Strafrecht erfaßt wird.[10]

---

[10] Vgl. nur *Stuckenberg*, ZStW 118 (2006), 878 ff. Jüngst teilweise anderer Ansicht *Graf*, NStZ 2007, 129 ff.

In der Tat erfüllt § 202c E-StGB diese Forderung weitgehend, was die Entwurfsbegründung zu erwähnen versäumt:

— Das „klassische" Phishing dürfte unter § 202c Abs. 1 Nr. 1 E-StGB fallen, sofern ein Sich-Verschaffen von Sicherungscodes wie PIN und TAN auch durch Täuschung erfolgen kann – der Wortlaut steht nicht entgegen. Jedenfalls aber das Entgegennehmen von PIN und TAN auf einer gefälschten Website benötigt ein entsprechendes Programm, das zu nichts anderem als der Begehung einer Straftat nach § 202a StGB (Zugang zu den gesicherten Kontodaten) dient, mithin von § 202c Abs. 1 Nr. 2 E-StGB eindeutig erfaßt wird. Nur das folgenlose Versenden einer Phishing-Email wird nicht erfaßt, weil § 202c – angesichts der weiten Vorverlagerung der Strafbarkeit zu Recht – keinen Versuch der Vorbereitungshandlung vorsieht. Hier sind aber m.E. bereits §§ 263, 22; 269 StGB erfüllt.

— Die Varianten des Phishing, bei denen der Täter sich Paßworte oder Sicherungscodes mit technischen Mitteln verschafft, wären nach § 202c Abs. 1 Nr. 1 E-StGB strafbar. Gleiches gilt für *Man-in-the-middle*-Angriffe, bei denen das Paßwort vom Täter sogleich etwa an die Website einer Bank weitergeleitet wird.

— Alle Formen des Phishing, die mit Hilfe von Schadprogrammen wie Trojanern durchgeführt werden oder innerhalb einer bestehenden Verbindung des Kunden zum Bankserver Daten wie Betrag und Zielkonto verfälschen, erfüllen (zugleich) § 202c Abs. 1 Nr. 2 E-StGB, da der Täter diese Programme entweder herstellen oder beschaffen muß.

Nicht-elektronische Formen des Phishing, etwa per Telefon oder Brief, fallen naturgemäß nicht unter § 202c E-StGB, aber m.E. bereits unter § 263, ggf. § 267 StGB

IV. § 303a StGB

Die seit längerem vorgebrachten Bedenken, daß § 303a in seiner geltenden Fassung keinen Unrechtstyp beschreibe, sind berechtigt. Der Gesetzentwurf fügt den Monita nichts hinzu, sondern behebt sie lediglich nicht. Um dem abzuhelfen, müßte der Gesetzgeber zuvor eine klare Vorstellung entwickeln, welche Rechtspositionen die Vorschrift eigentlich schützen soll. Das europäische Recht läßt für solche Konkretisierungen Raum.

V. § 303b E-StGB

Unbedenklich erscheint die Erweiterung des Tatbestands der Computersabotage (§ 303b StGB), der nun zusätzlich private Datenverarbeitung „von wesentlicher Bedeutung“ schützt und die weiteren Störungshandlungen des „Eingebens“ und „Übermittelns“ von Daten kennt, um *Denial-of-Service*-Angriffe zu erfassen.

Das Stören von elektronischen Haushaltsgeräten (S. 29) dürfte schon tatbestandlich nicht darunter fallen. Solche Geräte verarbeiten bei ihrer Funktion zwar Daten, dienen aber nicht primär dazu, so daß sie schon deshalb keine „Datenverarbeitung von wesentlicher Bedeutung“ darstellen. Der Begriff der „Datenverarbeitung“ ist freilich alles andere als ein Muster an Bestimmtheit.[11] Art. 5 der Europarats-Konvention bezieht sich lediglich auf “computer systems”, was jedenfalls sonstige Haushaltsgeräte ausschließt.

VI. Fazit

1. Der Versuch von §§ 202a und 202b E-StGB sollte unter Strafe gestellt werden.

2. Der irreführende Begriff des „Vorbereitens“ in § 202c E-StGB sollte ersetzt werden (auch in §§ 303a Abs. 3, 303b Abs. 5 E-StGB).

3. Die objektive Zweckbestimmung in § 202c Abs. 1 Nr. 2 E-StGB ist dahin zu präzisieren, daß die Programme *vorwiegend* zur Begehung von Straftaten nach §§ 202a, 202b E-StGB gestaltet sein müssen. Wenigstens in die Gesetzesbegründung sollte die Klarstellung aus Art. 6 Abs. 2 der Europarats-Konvention aufgenommen werden, daß Test und Schutz von Computersystemen nicht unter Strafe stehen.

4. Die subjektive Tatseite des § 202c E-StGB sollte auf Wissentlichkeit und Absicht begrenzt werden.

5. Die Tatbestände der §§ 303a, 303b StGB sind nach wie vor zu unbestimmt.

---

[11] Für Verfassungswidrigkeit daher NK-StGB[2]-*Zaczyk*, § 303b Rn. 2; krit. auch Tröndle/*Fischer*[53], § 303b Rn. 2.

Cybercrime Convention
Art. 6 — Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally** and **without right**:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, **designed or adapted primarily for the purpose of committing any** of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability **where** the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article **is not for the purpose of committing an offence** established in accordance with Articles 2 through 5 of this Convention, **such as for the authorised testing or protection of a computer system.**

3 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 of this article.

§ 202c E-StGB
Vorbereiten des Ausspähens und Abfangens von Daten

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

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

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

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.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 126c österreichisches StGB
Missbrauch von Computerprogrammen oder Zugangsdaten

(1) Wer

1. ein Computerprogramm, **das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung** eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines mißbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) **geschaffen oder adaptiert worden ist**, oder eine vergleichbare solche Vorrichtung oder
2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, **dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden**, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) …