Friedrich-Alexander-Universität Erlangen-Nürnberg

INSTITUT FÜR STRAFRECHT, STRAFPROZESSRECHT UND KRIMINOLOGIE

LEHRSTUHL FÜR STRAFRECHT, STRAFPROZESSRECHT UND RECHTSPHILOSOPHIE

PROF. DR. HANS KUDLICH

Prof. Dr. Hans Kudlich · Schillerstr. 1 · 91054 Erlangen

✉ Schillerstraße 1, 91054 Erlangen
☎ 09131/85-22248
🖷 09131/85-29232

Hans.Kudlich@jura.uni-erlangen.de
www.str2.jura.uni-erlangen.de

Erlangen, den 15.03.2007

Stellungnahme zum Gesetzesentwurf der Bundesregierung zu einem Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (BT-Drs. 16/3656) zur Vorbereitung der öffentlichen Anhörung im Rechtsausschuss am 21.3.2007

1. Teil: Allgemeine Überlegungen

I. Das Anliegen, den Stand der Strafgesetzgebung zur Bekämpfung der Computerkriminalität einer kritischen Revision zu unterziehen und dabei den strafrechtlichen Schutz zu erweitern, ist – nicht nur aufgrund des Umsetzungsbedarfes von europäischen Vorgaben (vgl. dazu *Gercke*, CR 2005, 468 ff.) – grundsätzlich zu begrüßen. Die Bedeutung der Informationstechnologie und des Einsatzes elektronischer Datenverarbeitungssysteme auch innerhalb von Netzwerken hat nicht nur für Wirtschaft und Verwaltung, sondern auch für den einzelnen Bürger als Privatperson in den letzten Jahren kontinuierlich zugenommen und ist mit dem Stand z.Z. der Einführung der einschlägigen Normen Mitte der 80er Jahre des 20. Jahrhunderts nicht mehr vergleichbar.

Wird in der strafprozessrechtlichen Diskussion gegenwärtig ganz zu Recht betont, dass der Schutz von Bürgerrechten etwa bei der Etablierung neuer Ermittlungsmaßnahmen in Informations- und Kommunikationssystemen nicht aus den Augen verloren werden darf, so muss dieser Schutz selbstverständlich auch und erst recht vor rechtswidrigen Eingriffen durch Private bestehen. Hinzukommen zwei weitere Gesichtspunkte: Zum einen hat die Verwendung von Computern insbesondere zu Zwecken der elektronischen Kommunikation der klassischen „Briefkommunikation“ in vielen Bereichen schon weitgehend den Rang abgelaufen, so dass ein vergleichbarer Schutz gewährleistet werden muss. Zum anderen ist – sei es zu Recht, sei es zu Unrecht – das subjektive Sicherheitsgefühl des Bürgers gerade bei der elektronischen Kommunikation vergleichsweise hoch, da entsprechende Nachrichten ihn sehr zielgenau und individualisiert erreichen;

dem strafrechtlichen Schutz vor Eingriffen gerade in diese Sphäre kommt daher erhebliche Bedeutung zu.

II. Der bestehende Umsetzungsbedarf mit Blick auf die europäischen Vorgaben wird im Entwurf im Wesentlichen zutreffend erkannt. In der Begründung sind diejenigen Ziele genannt, die im deutschen Recht bereits verwirklicht sind; diejenigen, bei denen dies noch offen steht, werden in enger Anlehnung an die europäischen Vorgaben behandelt. Dass im vorliegenden Kontext die Umsetzung der Europarats-Konvention hinsichtlich der Kinderpornographie nicht mit erfolgt, ist vertretbar, da es rechtstatsächlich und regelungstechnisch um ganz unterschiedliche Problemfelder geht; freilich wäre wünschenswert, dass auch diese Regelung bald nachgeholt wird, um nicht das unzutreffende Signal auszusenden, der Schutz von Kindern gegen sexuelle Ausbeutung bei der Verbreitung von Kinderpornographie wäre weniger wichtig als etwa der Schutz gegen Phishing-Angriffe oder gegen folgenloses Hacking.

Eine gesetzliche Regelung zur vorliegenden Materie mag sich immer dem Vorwurf ausgesetzt sehen, die zahlreichen technischen Details und die sich ständig wandelnden Modi operandi nicht immer vollständig treffgenau zu erfassen (vgl. Schultz, auf: http://www.medien-internet-und-recht.de/volltext.php?mir_doc_id=398, Rn. 2 f.). Indes ist dieses Unterfangen auch nicht ganz leicht zu bewerkstelligen, wenn andererseits keine völlig unübersehbare Kasuistik in dem Gesetzestext aufgenommen werden soll und wenn zugleich auch europäische Vorgaben erfüllt werden müssen. Insgesamt kann man dem Entwurf hier bescheinigen, subsumierbare und auch den strafrechtlichen Bestimmtheitsanforderungen genügende Regelungen gefunden zu haben, bei denen zumindest regelmäßig deutlich wird, welche Fälle der Gesetzgeber schwerpunktmäßig erfasst werden wollte und welche Konstellationen nach der ursprünglichen Konzeption nicht darunter fallen sollten.

III. Gleichwohl kann eine Kritik am handwerklichen Vorgehen hier nicht unterbleiben: Eine Reform des Computerstrafrechts, die auch an den durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität im Jahre 1986 eingefügten „Computerstraftatbeständen“ (insb. §§ 202a, 303a, 303b StGB) anknüpft, hätte zum Anlass genommen werden können, um zu diesen Vorschriften bestehende Auslegungszweifel bzw. geäußerte Kritik innerhalb der rechtswissenschaftlichen Literatur aufzugreifen oder zumindest einer Prüfung zu unterziehen. Das ist jedenfalls im gegenwärtigen Stadium der Gesetzgebung praktisch nicht mehr möglich, wenn die Verpflichtung zur Umsetzung bis spätestens 16. März 2007 aus Art. 12 des EU-Rahmenbeschlusses nicht nachhaltig verletzt werden soll. Insofern drängt sich die Frage auf, ob mit dem Beginn der Umsetzungsarbeiten des (vom 24.2.2005 datierenden) Rahmenbeschlusses zu lange hingewartet wurde oder aber ob sehenden Auges ein Rahmenbeschluss mitgetragen wurde, der eine nach den parlamentarischen Üblichkeiten kaum erfüllbare Umsetzungsfrist enthält.

2. Teil: Zu den Vorschlägen im Einzelnen

Es handelt sich um einen umfangreichen Entwurf mit vielen verschiedenen Punkten. Mangels einer konkreten Fragenliste können in der zur Verfügung stehenden Zeit in dieser schriftlichen Stellungnahme nur einige Punkte selektiv herausgegriffen werden. Dabei konzentriere ich mich insbesondere auf solche Aspekte, die für die Legitimation und Struktur der jeweiligen Änderung besonders bedeutsam sind, die in der Diskussion der vergangenen Monate bereits kontrovers behandelt worden sind oder aber die umgekehrt – soweit ersichtlich – noch gar nicht angesprochen worden sind, obwohl sie möglicherweise einer nochmaligen Überlegung bedürfen.

A. Änderungen des § 202a StGB

I. § 202a StGB soll in seiner neuen Fassung nicht mehr erst das Sichverschaffen von Daten, sondern bereits den Zugang zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, erfassen. Damit ist in Fällen des sog. *Hacking* nicht erst die Kenntnisnahme oder gar das Kopieren von Daten in dem gesicherten System erforderlich, sondern bereits die erfolgreiche Systempenetration als solche wird unter Strafe gestellt. Soweit sich hierdurch praktisch überhaupt eine Erweiterung der Strafbarkeit ergibt – bekanntlich sollte nach dem Willen des Gesetzgebers im 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität das „bloße“ Hacking nicht erfasst werden, was freilich technisch und praktisch nach der Gesetzesfassung nur schwer vorstellbar war, so dass insoweit teleologische Reduktionen erwogen wurden – ist diese Erweiterung nicht nur europarechtlich eindeutig gefordert, sondern auch in der Sache legitim.

Es mag in den 80er Jahren Vorstellungen gegeben haben, weshalb auch der unberechtigte Zugang auf besonders gesicherte Daten aus der Strafbarkeit ausgenommen werden sollte – zwingend ist eine solche Beschränkung aber keineswegs. Vielmehr besteht ganz im Gegenteil kein wirklich rechtfertigendes Bedürfnis dafür, derartige Handlungen als legitim zu erachten, obwohl sie nicht nur häufig Vorbereitungshandlungen für andere illegale Verhaltensweisen bilden, sondern auch in die formale Geheimsphäre des Opfers eindringen. Auch bei Straftaten wie etwa dem Hausfriedensbruch (§ 123 StGB) kommt es nicht entscheidend darauf an, was der Täter dann in der Wohnung, in der er eingedrungen ist, sonst noch macht. Kommen noch weitere Straftaten hinzu, so werden diese u.U. durch andere Delikte spezieller erfasst (so dass man an die Einfügung einer Subsidiaritätsklausel denken könnte, die freilich wegen der möglicherweise ganz unterschiedlichen betroffenen Rechtsgüter auch nicht völlig problemlos wäre); dies ändert aber nichts daran, dass auch allein das Eindringen in die „Daten-Privatsphäre“ strafwürdiges Unrecht darstellt. Ein etwaiges Hacken im Auftrag des Dateninhabers, z.B. zum Zweck der Überprüfung der Systemsicherheit, würde von der neuen Strafvorschrift nicht erfasst, da hier der Zugang nicht „unbefugt“ verschafft wird, so dass insoweit keine Probleme zu befürchten ist.

II. Erwägenswert wäre allenfalls eine Einschränkung auf „Computerdaten“, da die Erfassung von Daten jeder von § 202a II StGB erfassten Art über die zwingenden

europäischen Vorgaben noch hinausgeht. Damit wäre wohl auch den vom Bundesrat geäußerten Bedenken einer unverhältnismäßigen Ausdehnung der Strafbarkeit hinreichend Rechnung getragen. Freilich ist zu beachten, dass der vom Bundesrat im Ergebnis kritisierte weite Begriff der Daten sich auch schon in der gegenwärtigen Gesetzesfassung findet und dass die in der Stellungnahme genannten Beispiele – wenn sie so verstanden bzw. modifiziert werden, dass sie den Tatbestand der Neufassung tatsächlich erfüllen – unschwer so fortentwickelt werden könnten, dass sie auch den Tatbestand der bisherigen Gesetzesfassung erfüllen.

Darüber hinaus besteht aber auch ein unabweisliches Interesse daran, zumindest teilweise über den Bereich von Computerdaten im engeren Sinne gespeicherte Daten (etwa auf Zahlungskarten) strafrechtlich gegen unbefugten Zugang zu schützen. Angesichts der Stellung des § 202a StGB im Gesetz erwägenswert wäre allerdings eine Beschränkung auf „persönliche“ Daten o.ä. (was nicht mit „personenbezogenen Daten“ im Sinne des Datenschutzrechtes zu verwechseln ist). Hierdurch würde der Zugang zu solchen Daten zumindest *sub specie* § 202a StGB straflos gestellt, die grundsätzlich auch für beliebige Dritte verfügbar sein können und zu denen der Inhaber den Zugriff aus Gründen verwehrt, die nicht in den Schutzbereich des 15. Abschnitt des Besonderen Teils fallen.

III. Die geplante Einfügung des Merkmals „unter Überwindung der Zugangssicherung“ entspricht der schon bisher h.M. und ist inhaltlich vollständig gerechtfertigt und daher zur Klarstellung zu begrüßen.

IV. Die Erweiterung der Tathandlung sollte nicht dazu führen, im Gegenzug die Anforderungen an die „besondere Zugangssicherung“ bei der Rechtsanwendung zu stark herabzusetzen. Gerade mit Blick auf Angriffe auf Privatrechner ist daran festzuhalten, dass auch der technische Laie die Möglichkeit haben sollte, seine Daten dem Schutz des § 202a StGB zu unterstellen. Ein entsprechender Sicherungswille ist daher etwa bereits dadurch hinreichend ausgedrückt, dass eine Privatperson „am Internetverkehr teilnimmt, ohne einen freizugänglichen Server/ Dienst zu betreiben“ (zutreffend Schultz, a.a.O, Rn. 16).

V. Der Verzicht auf eine Versuchsstrafbarkeit ist zwar europarechtlich mit Blick auf Art. 5 III des EU-Rahmenbeschlusses möglich. Man sollte jedoch berücksichtigen, dass der Verzicht auf eine Versuchsstrafbarkeit in § 202 a StGB der bisherigen Fassung nicht zuletzt auch deswegen sinnvoll war, weil ansonsten die vom Gesetzgeber ursprünglich gewünschte Nichteinbeziehung des Hacking möglicherweise unterlaufen worden wäre; nachdem nunmehr aber auch das bloße Hacking erfasst sein soll, wäre eine Versuchsstrafbarkeit jedenfalls nicht mehr systemwidrig. Auch die Vorverlagerung des strafrechtlichen Schutzes steht einem entsprechenden Strafbedürfnis nicht notwendig entgegen, da ja durchaus nicht gesagt ist, dass es dem Täter auf jeden Fall gelingen wird, sich tatsächlich Zugang zu den Daten zu verschaffen. Soweit entsprechende Versuche, in das System einzudringen, zwar erfolgreich abgewehrt werden können, aber gleichwohl bemerkt und identifiziert werden können, bestünde durchaus ein sinnvoller und wohl auch legitimer Anwendungsbereich für eine Versuchsstrafbarkeit.

VI. Auch wenn es „eigentlich“ kein schutzwürdiges Interesse daran gibt, eigenmächtig und ohne Auftrag die Sicherheit fremder Systeme „auszutesten“, ist der Fall denkbar, in dem so etwas passiert und in dem dann nach gegenwärtiger Rechtslage u.U. auf Grund der (freilich nicht eindeutigen, vgl. o.!) Straflosigkeit des „bloßen Hacking“ eine Motivation bestehen kann, dem Betroffenen diese Sicherheitslücke zu melden. Hier besteht – nicht zuletzt auch durch die Relativierung des Strafantragserfordernisses, vgl. unten D – die Gefahr, dass solche Fälle aus Angst vor Strafbarkeit noch seltener auftreten. Sollte man Chancen und Nutzen solcher Meldungen für sehr wichtig halten, ist an die Einführung einer Vorschrift zur tätigen Reue zu denken (die dann konsequenterweise zur bisherigen Rechtslage freilich nur anwendbar sein dürfte, solange die Daten noch nicht „verschafft“ worden sind).

B. Geplante Einführung eines § 202b StGB

I. Hauptstoßrichtung der neuen Vorschrift zum „Abfangen von Daten“ ist das unbefugte Mitschneiden von elektronischer Kommunikation und damit eine Angleichung des Schutzes dieser Kommunikation an denjenigen etwa der Sprachtelephonie in § 201 StGB. Aufgrund der eingangs bereits genannten großen Bedeutung der elektronischen Kommunikation ist diese Angleichung jedenfalls gerechtfertigt. Deshalb bestehen auch (entgegen anders lautender Äußerungen aus der IT-Szene, vgl. nur die Stellungnahme des Chaos Computer Club unter http://www.ccc.de:80/press/releases/2006/20060925/forderungen.xml) keine Bedenken, bei dieser Vorschrift auf das Merkmal einer besonderen Sicherung zu verzichten, da eine solche auch bei der Sprachtelephonie keine Voraussetzung für einen strafrechtlichen Schutz ist. Zwar ist nichts dagegen einzuwenden, wenn auch eine gewisse Eigenverantwortlichkeit der User vorausgesetzt und damit gestärkt wird. Noch ist aber der Einsatz von Verschlüsselungstechniken bei Privatpersonen keinesfalls so weit verbreitet, dass man in ihrem Unterlassen ein Einverständnis in eine allgemeine Kenntnisnahme sehen könnte.

II. Ob – wie in der Entwurfsbegründung auf S. 18 unter 3. vorausgesetzt – als „technische Mittel“ im Sinne der Vorschrift auch bloße Passwörter in Betracht kommen, erscheint freilich mit Blick auf Art. 103 II GG zweifelhaft. Möglicherweise ist die Einschränkung „durch technische Mittel“ zur Verhinderung einer Überkriminalisierung aber überhaupt nicht erforderlich, da in § 200b ausdrücklich auch auf § 202a II StGB verwiesen werden soll. Das Abfangen solcher „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeicherter bzw. übermittelter“ Daten ist jedoch praktisch nur mit Methoden bzw. Hilfsmitteln möglich, die jenseits der Bagatellgrenze liegen.

III. Der in der Folge der Entwurfsveröffentlichung erhobene Vorwurf, § 202b müsse dahingehend konkretisiert werden, dass „nur ‚ungewollte Abstrahlungen von fremden Datenverarbeitungsanlagen’ von dem Schutzbereich des Verbotes umfasst sind“, da sonst „jede Nutzung (bzw. bereits das Einbuchen) eines WLAN-Accesspoints einer Strafbarkeit unterworfen“ wäre und es auch „selbstverständlich möglich sein, die Abstrahlung eigener Geräte zu messen und auszuwerten“ (vgl. nochmals unter http://www.ccc.de:80/press/releases/2006/20060925/

forderungen.xml), trifft nicht zu: Beide „Gefahren“ werden durch das Merkmal „unbefugt“ problemlos gebannt.

IV. Ohne dass dieses Ziel im Entwurf explizit genannt wurde, ist in der daran anschließenden Diskussion die Frage aufgeworfen worden, ob § 202b StGB auch eine Strafvorschrift gegen das sog. Phishing sein könnte (vgl. Schultz, a.a.O., Rn. 22 f.). Dabei spricht wohl mehr dafür, zumindest in der Vielzahl der Fälle, in denen die Dateneingabe aufgrund einer erfolgreichen Täuschung des Opfers auf der Phishing-Site selbst erfolgt, § 202b StGB nicht als einschlägig zu erachten, da zum einen Begrifflichkeit „Abfangen“ vorliegt und zum anderen zwischen dem Opfer und der Phishing-Zeit ja gerade die Kommunikation stattfindet, d.h. nicht von außen auf eine nichtöffentliche Kommunikation zugegriffen wird.

Ergänzend ist in diesem Zusammenhang freilich darauf hinzuweisen, dass jedenfalls die verbreitete Variante des Phishing, mit der Passwörter, PINs oder TANs zu einer späteren Verfügung über Konten o.ä. erlangt werden sollen, bereits nach dem geltenden Recht hinreichend unter Strafen stehen (vgl. auch Weber, HRRS 2004, 406, 410). Insbesondere kann man in der Preisgabe der Daten jedenfalls auf der Grundlage der Rechtssprechung des BGH (NStZ-RR 2004, 333, zum gewaltsamen Abpressen einer Geldautomaten-PIN) bereits eine Verfügung und eine hinreichend unmittelbare Vermögensgefährdung für einen Betrug nach § 263 StGB sehen (vgl. auch Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Rn. 765). Hinzu käme nach dem Entwurf ferner ein Schutz über § 202c StGB (vgl. sogleich im Anschluss C).

C. Geplante Einfügung eines § 202c StGB

Durch § 202c StGB soll die Vorbereitung von Straftaten nach §§ 202a oder 202b StGB durch das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonstige Zugänglichmachen von Passwörtern oder sonstigen Sicherungscodes bzw. von Computerprogrammen, deren Zweck die Begehung einer Tat nach §§ 202a, 202b StGB ist, unter Strafe gestellt werden.

I. Abs. 1 Nr. 1: Passworte

Die Strafvorschrift setzt Art. 6 Ia (ii) der Europarats-Konvention um und ist inhaltlich damit zwingend vorgegeben. Ein Strafbarkeitskorrektiv zur Ausscheidung sozialadäquater Verhaltensweisen erfolgt hier nicht über das Merkmal der (Un-)Befugtheit o.ä., sondern subjektiv durch das Erfordernis, dass der Täter nach § 15 StGB auch mit dem Vorsatz handeln muss, eine Tat nach §§ 202a bzw. 202b StGB vorzubereiten.

Die praktische Relevanz der Vorschrift zum vorgelagerten Schutz vor Systemeinbrüchen mag gering sein. § 202c I Nr. 1 StGB dürfte aber in der geplanten Fassung – auch wenn die Begründung daran zweifeln lässt, dass dies primäre Absicht der Verfasser war – nicht zuletzt auch einen relativ weit reichenden Schutz gegen das Phishing gewähren, wenn man § 202a StGB so auslegt, dass das ungeschriebene (von der h.M. aber zu Recht geforderte und auch im Entwurf vorausgesetzte) Überwinden der Zugangssicherung auch dann vorliegt, wenn ein Passwort unbefugt verschafft worden ist und dann eingesetzt wird, obwohl dann

der Zugriff ja eigentlich nicht unter „Überwindung der Sicherung“ erfolgt. Freilich erscheint eine solche Interpretation des § 202a StGB gerade mit Blick auf die Strafbarkeit nach § 202c StGB nahezu zwingend, da anderenfalls die Vorschrift insoweit meist leer laufen würde.

II. Abs. 1 Nr. 2

1. Das Herstellen, Sichverschaffen usw. vom „Computerprogramm, deren Zweck die Begehung“ von Straftaten nach §§ 202a, 202b StGB ist (sog. Hacker-Pools), ist nach dem Bekanntwerden des Gesetzesentwurfes (und auch bereits nach Verabschiedung der Europarechts-Konvention) rasch zum Gegenstand einer kritischen Diskussion in der Fachöffentlichkeit geworden. Die Kritik zielt insbesondere darauf hin, dass auch solche Personen (Sicherheitsbeauftragte, Systemadministratoren etc.), welche die entsprechenden Pools nur zum Testen ihrer Systeme benötigten, in die Gefahr einer Strafverfolgung geraten könnten. Das Gleiche gilt für den Schutz des eigenen Systems sowie für das Erproben von Systempenetrationen etwa in der Ausbildung.

2. Unter Verhältnismäßigkeitsgesichtspunkten mag man in der Tat fragen, ob eine solche abstrakte Vorfeldpönalisierung unverzichtbar ist, obwohl das entsprechende Verhalten für den Fall, dass mit dem Tool tatsächlich eine Straftat begangen wird, unproblematisch als Beihilfe unter Strafe steht. Insofern wäre es für einen rationalen Gesetzgebungsbeschluss hilfreich, Klarheit über zwei rechtstatsächliche Umstände zu gewinnen:

- Zum einen darüber, ob ein entsprechendes Verbot wirklich geeignet ist, Straftaten zu verhindern oder ob nicht professionelle Hacker ohnehin nicht auf die auf mehr oder weniger öffentlichen Vertriebswegen zugänglichen Programme zurückgreifen.
- Zum anderen wäre nach den Erfahrungen zu fragen, welche mit der ähnlich strukturierten und vor kurzem neu eingeführten Strafvorschrift des § 22b I Nr. 3 StVG bisher gemacht worden sind, in welcher die Vorbereitung einer Wegstreckenzähler- bzw. Geschwindigkeitsbegrenzermanipulation dadurch unter Strafe gestellt wird, dass der Täter „Computerprogramme, deren Zweck die Begegnung einer solchen Tat ist, herstellt, sich über einen anderen verschafft“ usw.

Sollte man zu beiden Fragen keine überzeugenden Ergebnisse finden können, ist in der Tat fraglich, ob nicht die negativen Sekundäreffekte überwiegen.

3. Strafrechtsdogmatisch sind mit der Vorschrift zwei Problemkreise verbunden:

- Zunächst ist trotz der gut gemeinten Absicht der Entwurfsverfasser fraglich, ob sich die „objektive Eignung“ zur Begehung von Straftaten nach §§ 202a, 202b StGB (unter gleichzeitigem Ausschluss von „harmlosen“ Programmen, aber unter offenbar erwünschtem gleichzeitigem Einschluss von „nicht ausschließlich für die Begehung einer Computerstraftat bestimmten“ Programmen [dual-use-Programme, vgl. S. 20 der Entwurfsbegründung]) trennscharf möglich ist. Die Erfahrungen etwa mit dem 1998 durch das 6. Strafrechtsreformgesetz eingeführten Merkmal des „gefährlichen Werkzeugs“, das beim Diebstahl oder Raub als Qualifikationsmerk-

mal mitgeführt werden kann, zeigen, dass eine Bestimmung spezifisch „deliktsanfälliger“ Tatwerkzeuge für die Rechtsanwender schwierig ist, wenn vom Gesetzgeber kein hinreichend bestimmter Katalog zur Verfügung gestellt wird.

- Strukturell zeigt das vorliegende Problem ferner Ähnlichkeit mit dem in der Rechtsprechung und Literatur der letzten Jahre kontrovers diskutierten Problem der „neutralen Beihilfe“, also der Beihilfestrafbarkeit durch die Erbringung von alltäglichen Dienstleistungen. Hier ist die Situation gewissermaßen eine „reziproke“, da es eben nicht (oder jedenfalls nicht nur) um alltäglich auch legal nutzbare Programme, sondern um die möglicherweise ebenfalls bestehende Möglichkeit einer legalen Nutzung von „an sich gefährlichen Programmen“ geht. Das Spannungsverhältnis zwischen vorgelagertem Rechtsgüterschutz einer- und Respekt vor der allgemeinen Handlungs- bzw. Berufsfreiheit andererseits ist jedoch ein vergleichbares.

Im Entwurfstext ist freilich zugleich auch eine Lösung durch das Merkmal der Vorbereitung einer Tat nach §§ 202a, 202b StGB angedeutet. Dabei kommt es weniger auf die „objektive Vorbereitungseignung“ an, da diese bei den in Nr. 2 genannten Programmen generell gegeben sein wird, sondern auf die subjektive Komponente: Nach § 15 StGB muss dem Täter bewusst sein, dass er durch sein Verhalten eine Straftat vorbereitet. Damit hat derjenige (etwa Sicherheitsbeauftragte oder Systemadministrator), der ausschließlich legale Zwecke verfolgt, ebenso wie derjenige Softwarehersteller, der ausschließlich zu solchen Zwecken Systemadministratoren mit Programmen versorgt, jedenfalls keinen hinreichenden Vorsatz, so dass eine Strafbarkeit nicht begründet wird.

Problematisch ist hierbei jedoch insbesondere für den Hersteller und Vertreiber solcher Programme die Möglichkeit einer Strafbarkeit auch wegen nur bedingten Vorsatzes, welcher bei der Lieferung eines solchen Programms in der Praxis im Einzelfall nicht verbindlich ausgeschlossen werden kann. Insoweit könnte es sich anbieten, den Tatbestand etwa durch die Formulierung „zur Vorbereitung einer Tat nach …“ so zu fassen, dass deutlich wird, dass ein bedingter Vorsatz zur Strafbarkeitsbegründung nicht ausreicht. Alternativ könnte vor die Tathandlung auch das Merkmal der „Unbefugtheit“ gesetzt werden, welches dann aber wohl ein verwaltungsrechtliches Verfahren zur Bestimmung einer entsprechenden „Vertriebsberechtigung“ voraussetzen würde.

Vor dem Hintergrund dieser Schwierigkeiten sollte nochmals genau geprüft werden, ob mit diesem Teil der Vorschrift tatsächlich etwas „gewonnen“ wird, d.h. eine Abschätzung ihrer Effektivität erfolgen. Dies nicht zuletzt auch vor dem Hintergrund, dass die Konvention des Europarates insoweit eine Nichtumsetzung auch zulassen würde. Sollte man allerdings zum Ergebnis kommen, dass eine solche Strafbarkeit hier politisch gewünscht ist, erscheinen die angedeuteten dogmatischen Probleme nicht so schwerwiegend und auch die Sorgen der „Software- und System-Administratoren-Lobby“ nicht so begründet, dass man aus rechtlichen Gründen davon Abstand nehmen müsste.

D. Geplante Änderung des § 205 StGB

In der geplanten Ergänzung des § 205 StGB wird auch für die neu gefassten §§ 202a und 202b StGB grundsätzlich ein Strafantragserfordernis statuiert. Dass es hier von in Fällen des § 202a StGB in der neuen Fassung nun eine Ausnahme bei besonderem öffentlichem Interesse geben soll, überrascht zwar etwas, wenn man sieht, dass sein Anwendungsbereich zugleich erweitert wurde, ist als politische Entscheidung aber sicher hinzunehmen. Eine „Entmündigung des Geschädigten eines Computereinbruchs“ (so der CCC auf http://www.ccc.de/press/releases/2006/20060925/forderungen.xml) ist darin nicht mehr zu sehen als bei allen anderen Offizialdelikten gegen Rechtsgüter der Person. Auf Grund der typischen Vernetzung von Computersystemen mag vorliegend wegen der Gefährdung Dritter die Einschränkung des Antragserfordernisses sogar um so näher liegen.

Nur auf den ersten Blick ist widersprüchlich, dass für die an sich weniger schwerwiegende bloße Vorbereitungshandlung des § 202c StGB kein Antragserfordernis vorgesehen ist; dies ist damit zu erklären, dass sich bei diesem abstrakten Vorfelddelikt nur schwer ein Verletzter benennen lässt, der antragsberechtigt sein könnte. Ähnliche Konstruktionen sind auch sonst im Zusammenhang mit abstrakt-gefährlichen Verhaltensweisen etwa im Vorfeld einer Körperverletzung zu beobachten, bei denen kein Strafantrag erforderlich ist, während etwa die einfache sowie die fahrlässige Körperverletzung ihrerseits Antragsdelikte sind.

E. Geplante Änderung des § 303b StGB

§ 303b StGB soll zum einen dahingehend geändert werden, dass nicht nur Datenverarbeitungsanlagen von Betrieben, Unternehmen oder Behörden, sondern auch von jeder Privatperson grundsätzlich geschützte Tatobjekte sein können; ferner hinzugekommen ist die Tathandlungsvariante des Eingebens oder Übermittelns von Daten in Nachteilszufügungsabsicht:

I. Im Grundsatz ist die Erweiterung der tauglichen Tatobjekte uneingeschränkt zu begrüßen. Wie schon aus den einleitenden Überlegungen klar geworden ist, spielen Computer mittlerweile auch für Privatpersonen eine derart zentrale Rolle, dass eine strafrechtliche Schutzlosigkeit jenseits der § 303 StGB erreichenden Substanzverletzungen nicht mehr zeitgemäß ist.

II. Das aus der Vorläuferfassung übernommene Merkmal der „wesentlichen Bedeutung“ erscheint dabei aber aus mehreren Gründen zweifelhaft: Zunächst sind Abgrenzungsschwierigkeiten damit (wie auch schon bisher, aber für den privaten Bereich vielleicht noch schwieriger zu lösen) vorherzusehen; des weiteren erscheint auch systematisch keinesfalls selbstverständlich, warum etwa bagatellhafte Sachbeschädigungen im Grundsatz strafrechtlich erfasst werden sollen, während das Tatobjekt bei § 303b StGB bereits für den Grundtatbestand für einen anderen „von wesentlicher Bedeutung“ sein müssen. Zuletzt ist auch fraglich, ob diese Einschränkung den europäischen Vorgaben gerecht wird. Denn die dort vorgesehene Beschränkung auf Fälle „nicht leichter“ Beeinträchtigungen etc. betrifft eigentlich eher Qualität bzw. Quantität der Beeinträchtigung, welche im

Entwurfstext durch das Merkmal „erheblich stört“ noch einmal eigens genannt ist. Eine zusätzliche – und zwar offenbar über eine bloße allgemeine Bagatellschwelle hinausgehende – Einschränkung der Tatobjekte auf solche von „wesentlicher Bedeutung“ erscheinen dagegen durch die europäischen Vorgaben nicht gedeckt.

In den Qualifikationsfällen des Abs. 2, die insoweit über die europarechtlichen Minimalanforderungen hinausgehen, ist dagegen das zusätzliche Korrektiv der „wesentlichen Bedeutung“ für die Strafrahmenschärfung sicherlich vorstellbar.

III. Die Tathandlung der Dateneingabe bzw. -übermittlung in Nachteilszufügungsabsicht ist zur Erfassung sog. „Denial-of-Service-Attacks“ eine sinnvolle Ergänzung, deren Strafwürdigkeit durchaus diskutabel erscheint und deren strafrechtliche Erfassung bisher doch erhebliche Schwierigkeiten hervorruft. Dogmatisch erscheint die Tathandlung für den Rechtsanwender – nicht zuletzt auch durch das vor die Klammer gezogene einschränkende Merkmal der „erheblichen Störung“ – durchaus handhabbar.

Erlangen, 14.03.2007

Prof. Dr. Hans Kudlich