EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

IT-SICHERHEIT UND § 202c StGB

STRAFBARKEIT BEIM UMGANG MIT IT-SICHERHEITSTOOLS NACH DEM 41. STRAFRECHTSÄNDERUNGSGESETZ ZUR BEKÄMPFUNG DER COMPUTERKRIMINALITÄT

von Dennis Jlussi*
entstanden aus einer Projektarbeit gemeinsam mit Christian Hawellek*
*candi. iur. an der Gottfried Wilhelm Leibniz Universität Hannover

Inhalt

Dennis Jlussi: IT-Sicherheit und § 202c StGB

Einleitung

Die Einführung des § 202c StGB durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität[1] (41. StrÄndG) ist in den Medien und von betroffenen Fachkreisen scharf kritisiert worden; Maßnahmen der IT-Sicherheit würden kriminalisiert und auch nach allgemeiner Anschauung gutartige Anwender von Hackertools seien „von der Gnade des Richters" abhängig.[2] Für die Unternehmen und Mitarbeiter im Bereich der IT-Sicherheit ist die Frage, ob ihr Tun strafbar ist, existenziell. Dies gilt aber nicht weniger für die Kunden, denn professionelle IT-Sicherheitschecks und Audits sind wichtige Bestandteile des betrieblichen Informationsschutzes und nicht zuletzt des unternehmerischen Risikomanagements, das spätestens seit Einführung des § 91 Abs. 2 AktG durch das KonTraG[3] für Aktiengesellschaften auch rechtlich geboten ist.

Das 41. StrÄndG ist im Juni 2007 im Deutschen Bundestag verabschiedet worden. Es ist am 10. August 2007 verkündet worden und am darauffolgenden Tag in Kraft getreten. Das Gesetz hat völker- und unionsrechtliche Hintergründe: Es dient zum einen der Umsetzung des Übereinkommens über Computerkriminalität des Europarates vom 23.11.2001 („Cybercrime Convention") und zum anderen der Umsetzung des EU-Rahmenbeschlusses 2005/222/JI über Angriffe auf Informationssysteme vom 24.02.2005. § 202c StGB setzt jedoch nur die Cybercrime Convention um und findet im Rahmenbeschluss keine Grundlage.

Das Gesetz ändert und ergänzt die Strafrechtsbestimmungen über Computerkriminalität: Beim Ausspähen von Daten (§ 202a StGB) kommt es nicht mehr auf einen Erfolg an, das heißt, es ist nunmehr unerheblich, ob der Täter tatsächlich Daten erlangt, es genügt die Möglichkeit des Zugangs zu Daten. Der Tatbestand des Abfangens von Daten (§ 202b StGB) ist neu geschaffen und der der Computersabotage (§ 303b StGB) ausgeweitet worden.

Zu Besorgnis und Kritik hat aber vor allem die Einführung des § 202c StGB geführt. Diese Untersuchung soll die rechtsdogmatischen Aspekte dieser Vorschrift klären und daraus Hinweise für den praktischen Umgang für die betroffenen Fachkreise, also insbesondere IT-Sicherheitsunternehmen und deren Mitarbeiter, geben.

Als Tätigkeiten, die unter § 202c StGB fallen könnten, kommen insbesondere die Beschaffung, Erstellung, Anpassung und Verwen-dung von Software in Frage, und zwar einerseits für die IT-Sicherheit designte Software zur Schwachstellenanalyse (z. B. AppScan, GFI Languard, Nessus). Solche Software versucht (unter anderem), Sicherheitslücken aufzuspüren, indem bestimmte potenziell schädliche Werte an das zu testende System übergeben und sodann Reaktionsmuster („Signaturen") ausgewertet werden. Andererseits kommt aber auch Schadsoftware (Viren, Trojaner, Würmer Exploits etc.) in Frage, die beschafft und angewendet wird, um zu testen, ob Computersysteme für bestimmte Angriffe anfällig sind oder ob die Systeme durch aktuelle Patches und Sicherheitssoftware (z. B. Virenscanner) ausreichend und wirksam geschützt sind. Häufig kommt es auch zum Austausch von angepassten Exploits etc. mit befreundeten Unternehmen oder im Rahmen von unternehmensübergreifenden Arbeitsgruppen[4] , sodass sich die dringende Frage stellt, ob derartige Maßnahmen in Zukunft als strafbar zu qualifizieren sind.
Frage stellt, ob derartige Maßnahmen in Zukunft als strafbar zu qualifizieren sind.

[1] BGBl I Nr. 38/2007, S. 1786 ff.
[2] Lischka, Gesetz kriminalisiert Programmierer, Spiegel Online, http://www.spiegel.de/netzwelt/web/0,1518,492932,00.html.
[3] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, BGBl I Nr. 24/1998, S. 786 ff.
[4] Z. B. im CERT-Verbund, sh. http://www.cert-verbund.de

B. Entstehung des § 202c StGB

§ 202c – 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.

I. Entstehung der Norm aus der Cybercrime Convention

Mit § 202c StGB setzt Deutschland Artikel 6 des Übereinkommens über Computerkriminalität des Europarates vom 23.11.2001 („Cybercrime Convention", auch „Budapest Convention") um. Die Cybercrime Convention war das weltweit erste multilaterale Übereinkommen über Computerkriminalität.[5] Umfangreiche Erläuterungen zum Übereinkommen sind im Explanatory Report des Europarates enthalten.[6] Die Vertragsstaaten verpflichten sich, zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen[7] bestimmte materielle Straftatbestände im Bereich der Computerkriminalität einzuführen sowie bestimmte Befugnisse für Strafermittlungsverfahren einzuführen. Deutschland hat die Cybercrime Convention unterzeichnet; die Bundesregierung plant, die Ratifizierung zeitnah nach der noch ausstehenden Umsetzung der prozessrechtlichen Ermittlungsbefugnisse[8] vorzunehmen.[9]

Artikel 6 – Missbrauch von Vorrichtungen

(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:

a) das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen

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;

ii.) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen, mit dem Vorsatz, sie zur Begehung einer nach den Artikeln 2 bis 5 um-schriebenen Straftat zu verwenden, und

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.

[5] Pocar, New Challenges for International Rules Against Cyber-Crime, European Journal on Criminal Policy and Research 2004, 27-37 [30].
[6] Vertragsbüro des Europarates, Explanatory Report on the Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
[7] Explanatory Report (Fn. 6), Abs. 71.
[8] Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtli-nie 2006/24/EG, BT-Drs. 16/5806.
[9] BT-Drs. 16/5806, S. 2.

B. Entstehung des § 202c StGB

(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.

(3) Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, sofern der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Verfügbarmachen der in Absatz 1 Buchstabe a Ziffer ii bezeichneten Mittel betrifft.

1. Regelungsgegenstand

Art. 6 Cybercrime Convention verpflichtet die Vertragsstaaten, eine selbständige Strafbewehrung von Vorbereitungshandlungen im Bereich der Artt. 2 – 5 vorzunehmen. Computerstraftaten erfordern typischerweise bestimmte Software („Hackertools"); den Umgang damit unter Strafe zu verbieten, erfasst bereits den Vorfeldbereich der Straftaten und wirkt daher präventiv. Ein ähnliches Vorgehen, nämlich das Verbot des Handels mit entsprechenden Mitteln zur Kriminalitätsbekämpfung im Vorfeld, ist auf internationaler Ebene bereits 1929 in der „Genfer Konvention über Geldfälschung" mit der Pönalisierung des Handels mit Druckmaschinen und anderem Geldfälschermaterial eingeschlagen worden.[10]

Abs. 1 lit. a Ziff. i stellt die genannten Umgangsweisen mit solchen Computerprogrammen unter Strafe, die „in erster Linie" zur Begehung von Computerstraftaten bestimmt sind. Das umfasst z. B. Programme, die dazu bestimmt sind, Computerdaten unbefugt zu verändern oder zu löschen oder das Betriebssystem zu stören, also etwa Viren oder Programme zur unbefugten Zugangsverschaffung.[11] Die Konferenzteilnehmer haben ausführlich darüber beraten, ob nur solche Programme erfasst werden sollen, die ausschließlich und spezifisch zur Begehung von Computerstraftaten bestimmt sind.

Letztlich wurde aber ein solcher Tatbestand für zu eng befunden, weil er die Vorschrift im Hinblick auf Beweisschwierigkeiten praktisch kaum anwendbar machen würde.[12] Ebenso wurde es aber abgelehnt, allein auf die objektive Eignung genügen zu lassen und als Strafbarkeitsfilter allein auf die subjektive Absicht zur Begehung von Computerstraftaten abzustellen.[13] Die Kompromisslösung besteht darin, Computerprogramme zu erfassen, die „in erster Linie" zur Begehung von Computerstraftaten erstellt wurden; dies soll „üblicherweise" Programme mit „dual use" ausschließen.[14]

Die Konferenzteilnehmer haben das Problem der drohenden Überkriminalisierung im Bereich der IT-Sicherheit gesehen. Daher erfasst Art. 6 Cybercrime Convention nur Taten, bei denen nicht bloß gewöhnlicher Vorsatz besteht, sondern ein spezifischer und direkter Vorsatz im Hinblick auf die Verwendung bei einer Computerstraftat besteht.[15] In Art. 6 Abs. 2 wird deutlich klargestellt, dass vom Anwendungsbereich der Cybercrime Convention nicht die genannten Umgangsweisen mit Computerprogrammen erfasst sind, wenn kein solcher Vorsatz besteht, sondern der Zweck des Umgangs beispielsweise in genehmigtem Testen oder zum Schutz von Computersystemen besteht.

[10] Spannbrucker, Convention on Cybercrime – Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht, diss. iur., Regensburg 2004, S. 79.
[11] Explanatory Report (Fn. 6), Abs. 72.
[12] Explanatory Report (Fn. 6), Abs. 73.
[13] Ebendort. [14] Ebendort.
[15] Explanatory Report (Fn. 6), Abs. 76.

B. Entstehung des § 202c StGB

2. Bedeutung des Art. 6 Cybercrime Convention für die Auslegung des § 202c StGB

Die Cybercrime Convention ist ein zwischenstaatliches Übereinkommen, das die Bundesrepublik Deutschland völkerrechtlich verpflichtet, entsprechende strafrechtliche Bestimmungen in das nationale Strafrecht einzuführen. Das Übereinkommen hat keinerlei Direktwirkung gegenüber den Bürgern, es bedarf der Umsetzung in ein deutsches Gesetz. Es ist dem deutschen Gesetzgeber durch das Übereinkommen auch nicht verwehrt, strengere als die im Übereinkommen vorgesehenen Vorschriften zu erlassen.

Gleichwohl hat der Gesetzgeber in der amtlichen Begründung zum Ausdruck gebracht, dass die Einführung des § 202c StGB gezielt der Umsetzung von Art. 6 Cybercrime Convention dient.[17] Abweichungen und Vorbehalte hat der Gesetzgeber jeweils besonders begründet,[18] sodass davon auszugehen ist, dass, soweit keine Abweichung besonders begründet ist, der Wille des Gesetzgebers darin besteht, die Cybercrime Convention exakt umzusetzen. Insoweit können das Übereinkommen und der Explanatory Report für die historische Auslegung des § 202c StGB herangezogen werden.

Gleichwohl sind die Möglichkeiten völkerrechtskonformer Auslegung begrenzt, gerade im Bereich des Strafrechts. Es sind besondere Anforderungen an die Bestimmtheit des Strafgesetzes zu stellen, die nicht durch völkerrechtskonforme Auslegung relativiert werden dürfen. Daher ist, anders als im europäischen Gemeinschaftsrecht, bei der Auslegung von Völker rechtsumsetzungen die konforme Auslegung zwar eine mögliche Methode, aber nicht die um der wirksamen Umsetzung Willen unbedingt zu bevorzugende Auslegungsmethode.

II. Umsetzung im deutschen Strafrecht

Der Gesetzgeber hat § 202c StGB bereits bestehenden strafrechtlichen Regelungen nachempfunden, bei denen es sämtlich darum geht, schon im Vorfeld bestimmte Vorbereitungshandlungen zu bestrafen, indem die Herstellung und Verschaffung wesentlicher für die Straftat erforderlicher Mittel strafbewehrt wird. Bereits früher hat der Gesetzgeber die Herstellung und Verschaffung von Mitteln zur Geldfälschung (§ 149 StGB), von Mitteln zur Ausweisfälschung (§ 275 StGB), von Software für den Computerbetrug (§ 263a Abs. 3 StGB) und von Software für die Tachomanipulation (§ 22b Abs. 1 Nr. 3 StVG) unter Strafe gestellt. Dass § 202c StGB der gleichen Systematik folgen soll, zeigt sich vor allem daran, dass er – genau wie §§ 263a, 275 StGB, 22b StVG – hinsichtlich des „Rücktritts" von der Vorbereitung auf § 149 Abs. 2 und 3 StGB verweist.

Erhellende höchstrichterliche oder obergerichtliche Rechtsprechung ist zu den Vorbildnormen – bis auf eine Entscheidung des BVerfG zu § 22b StVG, dazu sodann unter D.I. – jedoch praktisch nicht veröffentlicht.[19] Der Gesetzgeber hat daher nicht auf gefestigte Auslegungstendenzen Bezug nehmen können.

[16] Zur Entfaltung völkerrechtlicher Verbindlichkeit Spannbrucker (oben Fn. 10), S. 6.
[17] BT-Drs. 16/3656, S. 11f.
[18] Ebendort.
[19] Zu § 149 StGB: BGH wistra 2004, S. 265-267; zu § 275 StGB: OLG Köln, NStZ 1994, S. 289; beide Entscheidungen betreffen nur den Anwendungsbereich der jeweiligen Norm.

C. Der Tatbestand des § 202c StGB

I. Rechtsdogmatische Einordnung des § 202c StGB

1. Selbständiges Vorbereitungsdelikt

In Umsetzung der Cybercrime Convention stellt § 202c StGB ein selbständiges Vorbereitungsdelikt dar. Während eine Versuchsstrafbarkeit erst in Betracht kommt, wenn der Täter alles aus seiner Sicht wesentliche getan hat, um den Taterfolg eintreten zu lassen, begründet § 202c StGB eine Strafbarkeit bereits vor dem Versuchsstadium, wenn der Täter in der Absicht, eine Computerstraftat zu begehen, die entsprechenden Mittel herstellt, beschafft etc.

2. Abstraktes Gefährdungsdelikt

§ 202c stellt ein abstraktes Gefährdungsdelikt dar. Der Gesetzgeber will mit abstrakten Gefährdungsdelikten bestimmte Verhaltensweisen verbieten, aus denen sich typischerweise eine erhebliche Gefahr von Rechtsgutsverletzungen ergibt. Es wird gesetzlich unwiderleglich vermutet, dass diese Verhaltensweisen generell gefährlich sind. Eine Rechtsgutsgefährdung ist somit nicht Tatbestandsmerkmal und keine Voraussetzung für die Strafbarkeit, sondern rechtspolitischer Grund für die Strafnorm.[20] Die Strafbarkeit besteht daher gerade unabhängig von einer im Einzelfall tatsächlich bestehenden Gefahr für eine Person oder Sache. Die strafbewehrten Verhaltensweisen sind solche, die besonders leicht eine konkrete Gefahr auslösen können und dem Gesetzgeber deshalb bereits als solche strafwürdig erscheinen.

§ 202c StGB ist – im Gegensatz zu den übrigen Computerstraftaten des 41. StrÄndG – nicht von einem Strafantragserfordernis (§§ 205, 303c StGB) erfasst; § 202c StGB ist mithin Offizialdelikt und von Amts wegen zu verfolgen.

II. Der objektive Tatbestand

1. Tathandlung

Als Varianten der Tathandlung nennt das Gesetz das Herstellen, sich oder einem anderen Verschaffen, Verkaufen, einem anderen Überlassen, Verbreiten oder sonst Zugänglichmachen. Dabei meint „Verbreiten" die aktive Weitergabe, während „zugänglich machen" das passive Bereitstellen (insb. zum Download) meint.

„Verschaffen" umfasst dabei jede Form der Verschaffung, sei es per Download, per E-Mail, auf einem körperlichen Datenträger oder in anderer Weise. Auf eine Entgeltlichkeit kommt es nicht an, sodass auch kostenlose Software erfasst ist; ebenso wenig spielt es eine Rolle, ob die Software als Installationsdatei oder unmittelbar ausführbar vorliegt.

Der Gesetzgeber geht in seiner Begründung nicht weiter darauf ein, ob – wie im Europarats-Abkommen vorgesehen – davon auch die Einfuhr erfasst ist und scheint dies vorauszusetzen; dabei erscheint allerdings sehr zweifelhaft, ob z. B. allein das Verbringen von Software, die man bereits in unmittelbarem Besitz hat, in den räumlichen Geltungsbereich des StGB unter „verschaffen" subsumiert werden kann. Ob der Eintritt der abstrakten Gefährdungslage im räumlichen Geltungsbereich des StGB einen Erfolgsort i. S. d. § 9 StGB begründet, ist nämlich umstritten. Da bei abstrakten Gefährdungsdelikten gerade keine konkrete Gefahr oder ein sonstiger Taterfolg erforderlich

[20] Wessels / Beulke, Strafrecht AT, Rn. 29.

C. Der Tatbestand des § 202c StGB

ist, werden sie häufig als schlichte Tätigkeitsdelikte angesehen.[21]

Nur vereinzelt wird schon in der abstrakten Gefahr ein tatbestandlicher Erfolg i. S. d. § 9 StGB gesehen;[22] dies überzeugt jedoch nicht, denn eine abstrakte Gefahr ist gerade kein „zum Tatbestand gehörender Erfolg". Darunter fallen nur solche Erfolge, die Tatbestandsmerkmal sind, während aber bei abstrakten Gefährdungsdelikten der „Erfolg" der abstrakten Gefährdung eben nur rechtspolitischer Strafwürdigkeitsgrund ist. Wenn aber weder der Tatort (Ort des Verschaffens) im Geltungsbereich des StGB liegt noch überhaupt ein Erfolgsort – und somit auch keiner im Geltungsbereich des StGB – besteht, ist die Einfuhr im Ausland beschaffter Mittel nach deutschem Recht straflos, jedenfalls sofern die Tathandlung nicht auch im jeweiligen ausländischen Staat mit Strafe bedroht ist (§ 7 Abs. 2 StGB). Da eine völkerrechtskonforme Auslegung nicht unbedingt – um den Preis der Einhaltung strafrechtsdogmatischer Grundsätze – geboten ist und außerdem die Einfuhr schon wortlautmäßig nicht mehr unter „verschaffen" subsumiert werden kann, hat der Gesetzgeber insoweit die Umsetzung verfehlt.

2. Tatobjekte

Als Tatobjekte kommen Passwörter und sonstige Sicherheitscodes (§ 202c Abs. 1 Nr. 1) sowie Computerprogramme (Nr. 2) in Betracht.

Passwörter und sonstige Sicherheitscodes umfassen alle Kennungen, die den Zugang zu Daten ermöglichen. Neben klassischen Passwörtern fallen darunter auch z. B. PINs, TANs, Authentifizierungszertifikate oder digitalisierte biometrische Merkmale (z. B. für die Täuschung eines Fingerabdrucksensors) unabhängig davon, wie sie zur Zugangserlangung an die Hardware übergeben werden (Tastatureingabe, Chipkarte, RFID, elektrische Signalübergabe etc.).

Was ein Computerprogramm ist, ist nicht legal definiert. Nach landläufiger Definition sind Computerprogramme Abfolgen von Befehlen, die auf einem Computer zur Ausführung gebracht werden, um eine bestimmte Funktionalität zur Verfügung zu stellen.[23] § 202c selbst erfasst die Vorbereitung der Straftaten §§ 202a, 202b als Schutzzweck; §§ 303a, 303b verweisen zusätzlich auf § 202c. Computerprogramme i. S. d. § 202c können also zunächst all solche sein, die ihrem Wesen nach geeignet sind, diese Straftaten zu begehen.

Über die schlichte Eignung hinaus erfordert § 202c noch, dass der Zweck des Computerprogramms, also seine Bestimmung, die Begehung solcher Straftaten ist. Auch dies lässt aber eine Grauzone, denn zweifelhaft ist dies für Anweisungen, die lediglich ein anderes Programm aufrufen, das dann den Schaden verursacht. Ob z. B. eine Batch-Datei, die allein *format c:* als Anweisung enthält, oder eine HTML-Datei, die Schadsoftware nur einbettet, überhaupt Computerprogramme im Sinne der Vorschrift sind und wenn ja, solche, deren Zweck die Begehung der einschlägigen Computerstraftaten ist, erscheint fraglich. Es müssen daher einerseits Computerprogramme überhaupt definiert und von Nicht-Computerprogrammen abgegrenzt werden und andererseits muss bestimmt werden, wann eine dem objektiven Tatbestand entsprechende Zweckbestimmung vorliegt.

[21] Tiedemann / Kindhäuser, NStZ 1988, S. 337-346 [346]; Ostendorf, JuS 1982, S. 429; Jescheck / Weigend, Lehrbuch des Strafrechts, S. 178; Lackner/Kühl, § 9 Rn 2; Sch/Sch-Eser, § 9 Rn. 6.
[22] OLG Saarbrücken, NJW 1975, S. 506-509 [507]; Martin, Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen, 1989, S. 119.
[23] Wikipedia: Computerprogramm; ganz ähnlich Zimmermann (Hrsg.), Das Lexikon der Datenverarbeitung.

C. Der Tatbestand des § 202c StGB

a) Computerprogramm

„Computerprogramm" ist als Rechtsbegriff bisher vorwiegend im Hinblick auf den urheberrechtlichen Schutz von Computerprogrammen diskutiert worden. Dort ist der Begriff umstritten: Eine Ansicht knüpft an DIN-Normen an, wonach ein Computerprogramm eine Folge von Befehlen ist, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind, mittels einer informationsverarbeitenden Maschine eine bestimmte Funktion oder Aufgabe auszuführen oder ein bestimmtes Ergebnis herbeizuführen, anzuzeigen oder zu erzielen.[24] Die herrschende Gegenauffassung verlangt eine gewisse algorithmische Ablauflogik und lässt es nicht genügen, wenn auf dem letztlich ausführenden Computer nur vorgegebene Darstellungen erzeugt werden (z. B. HTML).[25]

Die in der urheberrechtlichen Diskussion angeführten Argumente sind jedoch nicht gänzlich übertragbar. Im Urheberrecht ist vor allem entscheidend, dass triviale Abläufe, die keine logischen algorithmischen Unterscheidungen treffen, sowie Code in reinen Auszeichnungssprachen keinen urheberrechtlichen Schutz genießen sollen, weil ein Freihaltebedürfnis für die Allgemeinheit besteht. Dem gegenüber hat das Strafrecht einen anderen Schutzzweck; auch Programme, die nicht urheberrechtlich schutzfähig sind, können zur Begehung von Computerstraftaten geeignet und bezweckt sein. Daher ist der Begriff des Computerprogramms i. S. d. § 202c teleologisch am Schutzzweck der Strafnorm auszulegen. Auf eine gewisse Ablauflogik kann jedoch für die Erfüllung des Wortlautes nicht verzichtet werden.

Vom Schutzzweck erfasst sind daher auch solche Skripte, die (z. B. Betriebssystem-) Funktionen am Computer anstoßen, die für sich genommen neutrale Zwecke verfolgen, durch das Skript aber in ausschließlich bösartiger Absicht ausgelöst oder kombiniert werden. Das exemplarisch genannte Batch-Skript, das die Festplatte formatiert, wäre also erfasst.

Den Wortlaut „Computerprogramm" überschreiten dürften hingegen reine Verweise auf Schadsoftware, die von einer Anwendung eigenständig interpretiert werden müssen und lediglich eine Darstellung beeinflussen. Eine HTML-Seite, die Schadsoftware einbettet, ist für sich genommen daher kein Computerprogramm, da sie lediglich auf Schadsoftware verweist.

Dazwischen liegen Programme, die mit Middleware, Interpretern oder Virtual Machines interpretiert und ausgeführt werden. Java-Programme werden z. B. von der Java Virtual Machine, ausgeführt. Die „physikalische" Ausführung der Befehle auf dem Computer erfolgt dabei nicht durch die Java-Anwendung, sondern durch die Virtual Machine. Bei solchen Programmen handelt es sich, obwohl sie nur mittelbar auf dem Computer ausgeführt werden, jedoch nach allgemeiner Verkehrsanschauung um Computerprogramme und nicht bloß um Verweise, die nur eine Darstellung einer Anwendung steuern.

Gleichwohl ist die Abgrenzung nicht in jedem Fall eindeutig zu ziehen. Die Abgrenzung zwischen Code, der lediglich die Darstellung einer Anwendung beeinflusst, und solchem, der Funktionen des Betriebssystems, und sei es mittelbar über Middleware o. ä., auslöst, muss im Einzelfall vorgenommen werden.

Keine Computerprogramme sind hingegen allgemeinsprachliche Beschreibungen, also bloße Umschreibungen bestimmter Algorithmen, ohne dass diese in

[24] Koch, GRUR 1997, 417 [420]; Cichon, ZUM 1998, 898
[25] Gaster, MMR 1999, 734; Köhler, ZUM 1999, 548

C. Der Tatbestand des § 202c StGB

einer Programmiersprache umgesetzt sind. Auch die urheberrechtliche Lizenz als solche ist kein Computerprogramm, denn ein Nutzungsrecht an einem Computerprogramm stellt für sich genommen kein Computerprogramm dar; allein der Erwerb einer Lizenz, ohne dass die Software in Form des Programmcodes beschafft wird, genügt für eine Strafbarkeit also nicht.

b) Objektivierte Zweckbestimmung

Es sind nur solche Computerprogramme von der Strafvorschrift erfasst, deren Zweck die Begehung einer Tat nach §§ 202a, 202b, 303a, 303b StGB ist. Dabei soll auf die objektivierte Zweckbestimmung abgestellt werden.[26] Nach dem Willen des Gesetzgebers sollen nur solche Programme erfasst sein, denen *„die illegale Verwendung immanent ist, die also nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind“*,[27] wobei nach dem Wortlaut des Gesetzes nicht die Bestimmung für irgendwelche Computerstraftaten genügt, sondern sich die objektivierte Zweckbestimmung auf diejenigen Computerstraftaten beziehen muss, die in § 202c StGB genannt sind oder sich auf § 202c StGB beziehen.

Dies soll Computerprogramme ausschließen, die der Sicherheitsüberprüfung dienen und auch solche Computerprogramme nicht unter den objektiven Tatbestand fallen lassen, die nicht eindeutig zu einem kriminellen Zweck eingesetzt werden sollen und erst durch ihre Anwendung entweder kriminell oder legal eingesetzt werden *(dual use tools)*.

Nicht unter den objektiven Tatbestand fallen daher einerseits Programmier- und Skriptsprachen, die sich lediglich dazu eignen, Malware zu programmieren, sowie Programme, bei denen es sich um in Verkehrskreisen anerkannte Sicherheitssoftware handelt, die zur Erkennung, nicht aber zum Ausnutzen von Sicherheitslücken dient. Prinzipiell kann jedoch jedes Programm, auch Malware, zu gutartigen Testzwecken eingesetzt werden, sodass es reine „single use tools“ praktisch gar nicht gibt. Der Gesetzgeber stellt daher auf eine „objektivierte“ Zweckbestimmung ab. Während eine Zweckbestimmung an sich naturgemäß subjektiv ist, will der Gesetzgeber diese Zweckbestimmung objektivieren. Dabei wird es auf die Anschauung der Verkehrskreise ankommen. Programme, deren eigene Funktionalität nur „bösartig“ ist, werden unter den Tatbestand fallen, denn auch wenn sie im Einzelfall zu gutartigen Testzwecken eingesetzt werden, so bleibt es bei ihrer objektivierten strafwürdigen Zweckbestimmung. Malware, also insbesondere Viren, Würmer und Spyware, fallen daher unter den objektiven Tatbestand.

Auch hier bleibt daher eine Grauzone, in der nur einzelfallbezogen eine Einordnung vorgenommen werden kann. Ein Exploit ist z. B. an sich nach objektivierter Zweckbestimmung strafwürdig. Ob das aber etwa auch für Exploits gilt, die von IT-Sicherheitsmitarbeitern erstellt werden und Sicherheitslücken testweise ausnutzen, die bekannt sind und geschlossen sein sollten, ist sehr fraglich; diese können möglicherweise bereits nach objektivierter Bestimmung auch zur gutartigen Verwendung bestimmt sein.

Hinsichtlich der Zweckbestimmung ist auch zu berücksichtigen sein, in welcher Weise das Ausnutzen der Sicherheitslücke geschieht. Besteht die Lücke z. B. darin, unbefugt eine Datei auf der Festplatte zu hinterlegen, so scheint es sachgerecht, die objektivierte

[26] BT-Drs. 16/3656, S. 12.
[25] BT-Drs. 16/3656, S. 19.

C. Der Tatbestand des § 202c StGB

Zweckbestimmung des Exploits auch daran zu messen, ob eine Datei hinterlegt wird, die weiteren Schaden anrichten kann, oder aber eine ungefährliche Datei, etwa eine reine Textdatei mit einem Sicherheitshinweis.

III. Der subjektive Tatbestand

1. Allgemeiner Vorsatz

Der allgemeine Vorsatz besteht im Wissen um die und Wollen der objektiven Tatbestandsmerkmale. Der Täter muss also wissen, dass es sich um ein Computerprogramm im beschriebenen Sinn handelt und es sich verschaffen (etc.) wollen.

2. Vorbereitung einer Computerstraftat

Die Vorbereitung einer Computerstraftat ist neben der objektivierten Zweckbestimmung des Computerprogramms der zweite wesentliche „Filter", mit dem der Gesetzgeber gutartige Nutzung straffrei halten will. Im Wortlaut *„Wer eine Straftat [...] vorbereitet, indem er [...]"* ist „indem" nicht so zu verstehen, dass die Vorbereitung einer Straftat bereits darin besteht, dass die Tathandlungen begangen werden, sondern es handelt sich um unterschiedliche Tatbestandsmerkmale.[28] Der Täter muss die Tathandlung also begehen, weil er mit der Tathandlung eine in Aussicht genommene Straftat (§§ 202a, 202b, 303a, 303b) vorbereiten will. Wann von einer Vorbereitung auszugehen ist, ist fraglich und vom Gesetzgeber offen gelassen worden.

a) Überschießende Innentendenz

Umstritten ist, ob die Vorbereitung einer Straftat objektiv vorliegen muss oder ob sich bei dem Tatbestandsmerkmal allein auf die Intention des Täters richtet (überschießende Innentendenz).

Nach e. A. soll es sich um ein objektives Tatbestandsmerkmal handeln, weil es objektiv formuliert sei.[29] Nach h. M. jedoch handelt es sich um eine überschießende Innentendenz, da es insoweit nur auf die Vorstellung des Täters ankomme.[30]

Dies ist auch überzeugend, weil es auf die objektive Vorbereitung einer Straftat nicht ankommt. Im hier von der Strafbarkeit erfassten Vorbereitungsstadium ist die Vorbereitung ohnehin nur anhand der Vorstellung des Täters festzumachen. Die Vorbereitung als objektives Tatbestandsmerkmal würde auch Strafbarkeitslücken entstehen lassen, nämlich dort, wo es (insbesondere beim Zugänglichmachen an unbestimmte Dritte) objektiv zu keiner Vorbereitung gekommen ist (denn diese liegt nicht allein in der Tathandlung, s. o.), diese aber subjektiv gewollt wurde: Mangels Erfüllung des objektiven Tatbestandes und mangels Versuchsstrafbarkeit wäre dann, obwohl eine abstrakte Gefahr geschaffen wurde, der Täter straffrei. Für die Annahme eines nur subjektiven Tatbestandsmerkmals spricht letztlich auch die Cybercrime Convention, in deren Art. 6 von Vorsatz die Rede ist, also ein *„intent that the device is used for the purpose of committing [...] offences"*.[31]

b) Erforderliche Vorsatzform

Bei der überschießenden Innentendenz genügt, soweit der Gesetzgeber nicht die „Absicht" zur wortlautmäßigen Tatbestandsvoraussetzung macht, an sich dolus eventualis.[32] Es würde also genügen wenn

[28] BT-Drs. 16/3656, S. 19.
[29] NK -Puppe, § 149 Rn. 3.
[30] LK -Ruß, § 149 Rn. 4.
[31] Explanatory Report (Fn. 6), Abs. 76.
[32] LG München I, NJW 2003, S. 2328-2331 [2329].

C. Der Tatbestand des § 202c StGB

der Täter es ernsthaft für möglich hält und billigend in Kauf nimmt, dass seine Tathandlung der Vorbereitung einer der genannten Computerstraftaten dient.

Das geht über die Vorgabe der Cybercrime Convention hinaus, die eine Absicht im technischen Sinn, also dolus directus 1. Grades erfordert.[33] Allerdings ist die Cybercrime Convention nur ein Instrument der Mindestharmonisierung, sodass es dem deutschen Gesetzgeber unbenommen ist, schärfere Vorschriften einzufügen. Der Gesetzgeber hat davon Abstand genommen, den technischen Begriff der Absicht im Wortlaut oder der Begründung zu verwenden und stellt auf eine Inaussichtnahme ab und darauf, dass bei der Tathandlung keine Anhaltspunkte für eine eigene oder fremde Computerstraftat bestehen.[34] Wenn es genügen soll, dass der Täter Anhaltspunkte für eine Computerstraftat sieht, so spricht dies dafür, dass dolus eventualis im Hinblick auf die Vorbereitung einer Computerstraftat genügt.

c) Konkretisierung des vorbereiteten Delikts

Fraglich ist dann noch, wie sehr die in Aussicht genommene Computerstraftat konkretisiert sein muss. Dies ist bei ähnlichen Delikten umstritten: Nach e. A. muss der Täter eine konkrete Tat vor Augen sehen, die in ihren wesentlichen Umrissen Gestalt hat; ein völlig vager Plan genügt nach dieser Ansicht nicht, jedoch müssen Einzelheiten der Tatbegehung noch nicht endgültig festgelegt sein.[35] Nach a. A. soll es genügen, wenn der Täter in dem Bewusstsein handelt, dass die Tatobjekte irgendwann einmal einer Computerstraftat dienen könnten.[36]

Letztgenannte Auffassung ließe jedoch die Strafbarkeit den Bereich der bewussten Fahrlässigkeit umfassen; eine Fahrlässigkeitsstrafbarkeit ist aber weder dem Wortlaut zu entnehmen noch vom Gesetzgeber gewollt. Man wird daher verlangen müssen, dass der Täter eine Computerstraftat vorbereitet, die er oder ein Dritter zum Zeitpunkt der Tathandlung schon ins Auge gefasst hat. Das ist der Fall, wenn zumindest einige wesentliche Eckpunkte feststehen, etwa das anzugreifende Computersystem oder die Person des Opfers oder eine bestimmbare Zielgruppe (z. B. die Anwender eines bestimmten Betriebssystems oder einer bestimmten Applikation). Beim Zurverfügungstellen (zum Download) genügt es, wenn der Täter zum Zeitpunkt der Tathandlung damit rechnet und billigend in Kauf nimmt, dass sich andere zur Begehung einer Straftat das Hackertool so beschaffen. Der Täter muss also wissen oder damit rechnen, dass seine Handlung ein geplantes Delikt fördert,[37] ohne dass alle konkreten Tatmodalitäten feststehen müssen.[38]

Steht nicht fest, welche Computerstraftat begangen werden soll, und ist die Tat dennoch ins Auge gefasst (wenn z. B. das Opfer schon feststeht und das Tatobjekt zu mehreren Straftaten geeignet ist) ist Wahlfeststellung möglich, also eine Verurteilung unter Offenlassung der Frage, ob der Täter eine Straftat nach § 202a, § 202b, § 303a oder § 303b vorbereitet hat.

[33] Explanatory Report, Abs. 76: „direct intent"; a. A. ohne besondere Begründung Spannbrucker, S. 81; zur englischen Terminologie Burgess, For sight of Consequences is not the same as intent, http://www.peterjepson.com/law/burgess%20A2-1.htm.
[34] BT-Drs. 16/3656, S. 19.
[35] LK -Ruß, § 149 Rn. 6; Sch/Sch-Stree / Sternberg-Lieben, § 149 Rn. 5.
[36] NK -Puppe, § 149 Rn. 3.
[37] Sch/Sch- Sternberg-Lieben, § 149 Rn. 8.
[38] Lackner/Kühl, § 263a Rn. 26c.

D. Stellungnahme und Lösungsmöglichkeiten

Die Tatbestände des Computerstrafrechts – insbesondere diejenigen, die neu durch das 41. Strafrechtsänderungsgesetz eingeführt wurden – haben für Aufregung unter IT-Sicherheitsleuten gesorgt. Nicht ganz zu Unrecht, denn auf den ersten Blick sind die Normen unklar und selbst bei genauem Hinsehen lassen sich nicht alle Strafbarkeitsrisiken völlig verneinen. Gleichwohl haben der Europarat und auch der deutsche Gesetzgeber ganz deutlich gemacht, dass mit den Regelungen die Arbeit der IT-Sicherheit nicht unter Strafe gestellt werden soll, und mit einigen wenigen zur Vorsicht gebotenen Verhaltensweisen lassen sich die Strafbarkeitsrisiken minimieren.

Der Gesetzgeber hat § 202c StGB ähnlich gefasst wie bestehende Vorfelddelikte und hat dabei nicht auf eine gefestigte Rechtsprechung zurückgreifen können: Es gibt fast keine höchstrichterliche oder obergerichtliche Rechtsprechung. Zugleich werden hinsichtlich mehrerer entscheidender Aspekte, wie im einzelnen soeben dargelegt, in der Literatur unterschiedliche Meinungen vertreten. Dazu kommen noch Begriffe („Computerprogramm"), die nicht legal definiert sind.

Der Gesetzgeber hat sich offenbar – wie schon der Europarat [39] – außerstande gesehen, gutartige Tätigkeiten wie im Bereich der IT-Sicherheit klar im Wortlaut auszunehmen, ohne Strafbarkeitslücken für böswillige Tätigkeiten entstehen zu lassen. Der Gesetzgeber vertraut auf eine angemessene, einzelfallbezogene Anwendung des § 202c StGB durch die Staatsanwaltschaften und Gerichte und mutet den im IT-Sicherheitsbereich Beschäftigten persönlich sowie den Unternehmen (i. V. m. §§ 30, 130 OWiG) zu, entsprechende Strafbarkeits- bzw. Ordnungswidrigkeitsrisiken auf sich zu nehmen und es „darauf ankommen zu lassen".

Auch wenn es angesichts dessen keineswegs völlig neben der Sache ist, von einer Abhängigkeit „von der Gnade des Richters"[40] , so dürfte nach hier vertretener Auffassung bei richtiger Anwendung und (insb. teleologischer und historischer) Auslegung des § 202c StGB durch die Staatsanwaltschaften und Gerichte eine Strafbarkeit im Rahmen der IT-Sicherheit bei Einhaltung weniger Maßgaben nicht bestehen. Es ist jedoch nicht völlig auszuschließen, dass dies in der Praxis in Teilen – und gerade hinsichtlich der umstrittenen Aspekte – anders gehandhabt würde und es wenigstens zu Ermittlungsverfahren und -maßnahmen, Anklageerhebungen und unterinstanzlichen Verurteilungen kommen könnte. Selbst wenn am Ende eines solchen Verfahrens keine Verurteilung stünde, so wäre allein mit der Aufnahme des Verfahrens und der Durchführung von Ermittlungsmaßnahmen (z. B. Durchsuchung, Sicherstellung oder Beschlagnahme von Computern) eine erhebliche Beeinträchtigung der Arbeitsfähigkeit im Bereich der IT-Sicherheit zu besorgen.

Es lassen sich daher die folgenden Vorsichtsmaßnahmen ergreifen, um die skizzierten Risiken zu minimieren:

I. Möglichkeit der Anrufung des BVerfG

Hinsichtlich der ähnlichen (und ähnlich unklaren) Strafbarkeit des Herstellens und Vertreibens von Computerprogrammen für die Kilometerzählerverfälschung (§ 22b I Nr. 3 StVG) hat ein Hersteller Verfassungsbeschwerde zum BVerfG erhoben. Das BVerfG hat durch seinen Beschluss zumindest etwas mehr Rechtssicherheit im Hinblick auf die Strafbarkeitsgren-

[39] Explanatory Report (oben Fn. 6), Abs. 73.
[40] Oben Fn. 2.

D. Stellungnahme und Lösungsmöglichkeiten

zen hergestellt.[41] Es wäre daher überlegenswert, eine wenigstens teilweise Klärung der Rechtsfragen auch im Hinblick auf § 202c StGB durch das BVerfG anzustreben.

II. Umgang mit Hackertools und Malware

Zur Minimierung der Strafbarkeitsrisiken führt auch die Beachtung einiger Maßgaben im Umgang mit Hackertools:

1. Sorgfalt

Im Umgang mit Hackertools und Malware, die zu Testzwecken beschafft oder erstellt wird, ist besondere Sorgfalt geboten. Solche Software sollte an niemanden weitergegeben werden, bei dem nicht sicher ist, dass er die Software zu gutartigen Testzwecken einsetzen will. Eine Weitergabe sollte nur an bekannte und zuverlässige Partner erfolgen. Keinesfalls sollte solche Software einem unbestimmten Empfängerkreis zugänglich gemacht werden.

Die betroffenen Computerprogramme sollten überdies sicher gehalten werden, und zwar sowohl was eventuelle Installations-Datenträger angeht, als auch hinsichtlich der Sicherung der Computer, auf denen sie installiert sind.

2. Dokumentation

Wenn ein Hackertool oder Malware beschafft – gleichgültig, ob kostenlos oder kommerziell – oder erstellt wird, sollte nachvollziehbar protokolliert werden, für welche Test- und Sicherheitszwecke das Programm beschafft wird und welche Verwendung des Programms vorgesehen ist. Aus der Dokumentation sollte sich zweifelsfrei ergeben, dass die Software nicht beschafft wurde, um Straftaten zu begehen, sondern um gutartige Tätigkeiten auszuüben. Auch der Einsatz des Programms ist entsprechend – schriftlich und veränderungssicher – zu dokumentieren.

3. Einwilligung

Da § 202c StGB ein abstraktes Gefährdungsdelikt ist und es daher naturgemäß keinen konkret betroffenen Rechtsgutsträger gibt, kommt eine Einwilligung nicht in Betracht. Jedoch ist eine Einwilligung hinsichtlich derjenigen Straftaten möglich, zu deren Vorbereitung die Tathandlung des § 202c StGB dienen soll, nämlich §§ 202a, 202b, 303a, 303b StGB. Liegt von dem jeweils Berechtigten, auf dessen Computersysteme oder Daten zu Testzwecken Angriffe verübt werden sollen, eine Einwilligung in die Maßnahmen vor, so entfällt die Strafbarkeit der vorbereiteten Tat und mithin auch die Strafbarkeit der Vorbereitung. Die Einwilligung sollte möglichst schriftlich erfolgen und hinreichend konkret die Maßnahmen nennen, in die eingewilligt wird. Es ist auf eine geschlossene Legitimationskette von der Unternehmensleitung (Vorstand) bis hin zu derjenigen Person zu achten, die die Einwilligung gibt.Dabei sind auch die Arbeitnehmerbeteiligungsrechte zu wahren, die von den konkreten Umständen (z. B. erlaubte Privatnutzung) abhängen können und daher im Einzelfall zu prüfen sind.

[41] BVerfG NJW 2006, 2318.