Master-Fernstudiengang
Wirtschaftsrecht für die Unternehmenspraxis

Rechts- und Witschaftswissenschaftliche Fakultät der Universität des Saarlandes
in Kooperation mit dem
Distance & International Studies Center (DISC)
der Technischen Universität Kaiserslautern

Masterarbeit zum Thema:

Strafrechtliche Aspekte der Entwicklung von Open Source Software zur Qualitätssicherung von Kommunikationssystemen im Internet

Modul: Wirtschaftsstrafrecht

Eingereicht von: Olaf Bergmann
Matrikelnummer (UdS):
Straße:
Wohnort:
Tel.-Nr:
E-Mail:

Abgabedatum: 14. Dezember 2009

Inhaltsverzeichnis

Abkürzungsverzeichnis

BeckOK	Beck'scher Online-Kommentar Strafrecht (zitiert als BeckOK-*Bearbeiter*)
BNetzA	Bundesnetzagentur
DoS	Denial of Service
DSL	Digital Subscriber Line
ErfK	Erfurter Kommentar zum Arbeitsrecht (zitiert als ErfK-*Bearbeiter*)
GPL	GNU General Public License
IT	Informationstechnik
JR	Juristische Rundschau
JuS	Juristische Schulung
JZ	Juristenzeitung
MK	Münchener Kommentar zum Strafgesetzbuch (zitiert als MK-*Bearbeiter*)
MR-Int	Medien und Recht International Edition
NGN	Next Generation Network
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
NZA	Neue Zeitschrift für Arbeitsrecht
StGB a. F.	Strafgesetzbuch in der Fassung vor dem 41. StrÄndG (d. h. vor dem 11. August 2007)
ZUM	Zeitschrift für Urheber- und Medienrecht

A. Einleitung

Ist im Zusammenhang mit Computerkriminalität vom Internet als Tatmittel die Rede, so geht es in der überwiegenden Zahl der Beiträge um Betrug, Pornografie, Schutzrechtverletzungen oder strafbare Äußerungen. Während die absoluten Zahlen in der polizeilichen Kriminalstatistik (PKS) diese Wahrnehmung bestätigen,[1] scheinen die weiteren Delikte wie etwa Datenveränderung und Computersabotage, aber auch die Fälschung beweiserheblicher Daten aufgrund geringerer Fallzahlen eher in den Hintergrund zu treten. Die potentiellen schwerwiegenden Auswirkungen dieser Handlungen auf die Volkswirtschaft wurden bereits in den 1970er Jahren erkannt und haben den Gesetzgeber veranlasst, in das Strafgesetzbuch mit dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG[2]) erstmals entsprechende Tatbestände einzuführen.[3]

Der seit dem Inkrafttreten des 2. WiKG im Jahr 1986 vorangeschrittene technische Ausbau des Internets und die mittlerweile zumindest für sehr große Teile der Bevölkerung in den Industriestaaten allgegenwärtige Verfügbarkeit leistungsfähiger Computer und kostengünstiger Internetanbindungen hat in der jüngeren Vergangenheit jedoch dazu geführt, dass selbst technisch nicht besonders vorgebildete Täter in der Lage sind, Schadprogramme in Umlauf zu bringen, in fremde Computersysteme einzudringen oder Online-Dienste gezielt zu überlasten. Als Reaktion auf diese Entwicklung und in weitgehender Übereinstimmung mit internationalen Abkommen zur Bekämpfung von Computerkriminalität[4] wurde mit dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG[5]) vom 7. August 2007 bereits die Herstellung von Werkzeugen zur Durchführung bestimmter Tathandlungen im Bereich der Computerkriminalität als strafbare Handlung eingestuft.

[1] Laue 13/2009, S. 2; Köppen 2008; Köppen 2009.
[2] *BGBl. I Nr. 21 vom 23.05.1986, 721.*
[3] *BT-Drs. 10/5058*, S. 24, 33.
[4] Zu nennen ist hier insbesondere die *Convention on Cybercrime, ETS 185.*
[5] *BGBl. I Nr. 38 vom 10.08.2007, 1786.*

Zahlreiche Kommentierungen zum 41. StrÄndG haben auf die Probleme hingewiesen, die sich aus der Kriminalisierung dieser sogenannten *Hackertools* ergibt.[6] In der kontrovers geführten Diskussion sehen sich die Befürworter der Änderungen der Kritik u. a. von Informationstechnik-Firmen gegenüber, die eine Rechtsunsicherheit im Bereich der empirischen Sicherheitsüberprüfungen von Computersystemen befürchtet.

In der vorliegenden Arbeit werden die strafrechtlichen Aspekte der Herstellung und Verbreitung von *Dual-Use-Tools*[7] als Open Source Software analysiert. Im Vordergrund der Betrachtung steht die Rolle der verantwortlichen Personen innerhalb einer Unternehmenshierarchie. Wie im Folgenden dargelegt wird, besteht gerade in kleinen und mittleren Unternehmen ein besonderes Interesse an der Veröffentlichung von Software als sogenannte freie Software, da dies den eigenen Wartungsaufwand verringern kann. Als Beispiel für ein Dual-Use-Tool wird eine Open Source Software herangezogen, die bei einem Anbieter von Telekommunikationsdiensten zur Durchführung von Belastungstests seiner Telekommunikationseinrichtungen weiterentwickelt worden ist.

I. Zur Bedeutung von Open Source Software in der Internetwirtschaft

Der stetige Ausbau von Weitverkehrsdatennetzen, fallende Kosten für Computer und Kommunikationstechnik und eine innovationsfreundliche Wirtschaftspolitik haben seit den 1990er Jahren dazu geführt, dass das Internet in Deutschland eine erhebliche volkswirtschaftliche Bedeutung erlangt hat.[8] Während anfangs vor allem Skaleneffekte durch effizientere Kommunikation sowie Netzwerkeffekte für einen Produktivitätsanstieg der Internetwirtschaft gesorgt haben, bildeten sich mit der Zeit zahlreiche Dienstleistungsmärkte im Bereich *Information und Kommunikation* (I&K) heraus. Im Jahr 2006 umfasste der I&K-Sektor ca. 4,5 % des steuerbaren Umsatzes in Deutschland, wobei etwa die Hälfte der sozialversicherungspflichtigen Beschäftigten in kleinen und mittleren Unternehmen (KMU[9]) angestellt waren.[10]

[6] Popp 2007, S. 87; Laue 13/2009, S. 6; DFN 2006, S. 5; Wien 2009, S. 186; Schumann 2007, S. 678.

[7] Popp 2007, S. 87; Ernst 2007, S. 2663.

[8] Welfens u. a. 2004, S. 86; Günther 2008, 155 f., m. w. N.

[9] Nach der Klassifikation des Statistischen Bundesamts umfasst dies Unternehmen mit weniger als 250 Beschäftigten und einem Jahresumsatz von höchstens 50 Mio. €, vgl. Statistisches Bundesamt 2009, S. 491.

[10] Ebd., S. 493.

Mit der gleichzeitig von der Europäischen Kommission vorangetriebenen Liberalisierung des Telekommunikationsmarkts[11] sanken in der Folge die Markteintrittshürden auch für kleinere Anbieter.[12] Trotz einer seit etwa 2007 andauernden Tendenz zur Konsolidierung auf dem DSL-Markt[13] ist der Telekommunikationsdienstemarkt im Jahr 2009 weiterhin stark diversifiziert und zeigt trotz leicht rückläufiger Umsatzerlöse stetigen Wachstum der Wettbewerber, vgl. Abbildung A.1[14].

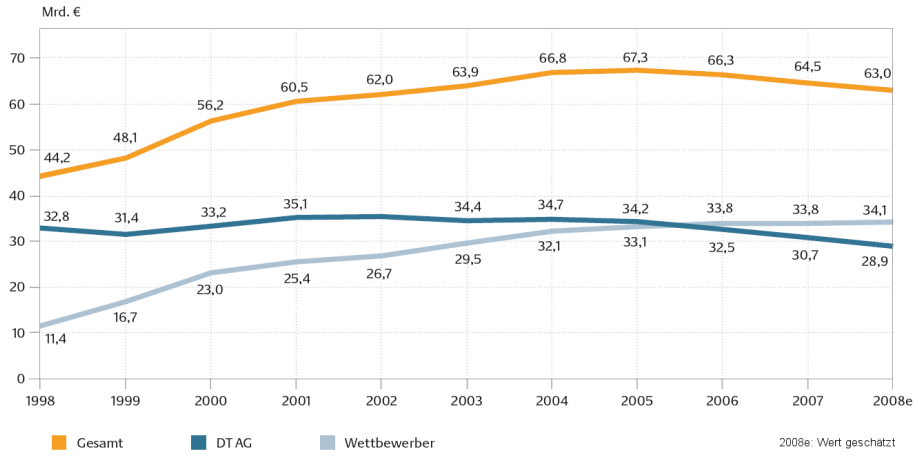

Abbildung A.1: Umsatzerlöse auf dem deutschen Telekommunikationsdienstemarkt (Quelle: BNetzA).

Die Bedeutung dieses Marktsegments für die deutsche Wirtschaft lässt sich an den Kennziffern des Statistischen Bundesamts ablesen: So umfassten die Dienstleistungen im Bereich Fernmeldedienste im Jahr 2006 25 % der Dienstleistungen im I&K-Sektor, bzw. 10 % des gesamten Dienstleistungssektors.[15] Mit etwa 18 % des Umsatzes und knapp 14 % der Beschäftigten stellte die Herstellung von Geräten und Einrichtungen der Telekommunikationstechnik einen weiteren bedeutenden Wirtschaftszweig innerhalb des I&K-Sektors dar.[16]

Kleine und mittlere Unternehmen sehen sich jedoch auch in diesem wachsenden Markt einem hohen Kostendruck ausgesetzt, und Unternehmensgründern mangelt es an Krediten für Anfangsinvestitionen.[17] Viele dieser Unternehmen setzen daher verstärkt auf Open Source Software und können so die Anschaffungskosten senken und eine Abhängigkeit ihrer IT-Prozesse von proprietärer Software minimieren.

[11] RL 90/388/EWG; RL 96/19/EG; RL 2002/77/EG.
[12] Welfens u. a. 2004, S. 64 ff.; Europäische Kommission 2002, S. 4 f.
[13] Vgl. u. a. Heise online 2007; Heise online 2008; ZDNet.de 2009, m. w. N.
[14] BNetzA 2008, S. 62.
[15] Statistisches Bundesamt 2009, S. 119.
[16] Ebd., S. 119.
[17] Welfens u. a. 2004, S. 62.

Unter *Open Source* wird dabei eine Lizenzform verstanden, die es jedem erlauben soll, die betreffende Software zu vervielfältigen, zu verbreiten, Änderungen vorzunehmen und die bearbeitete Fassung wiederum zu verbreiten.[18] Gleichzeitig wird der Schöpfer einer Bearbeitung jedoch verpflichtet, diese im Falle einer Veröffentlichung unter den gleichen Lizenzbedingungen zugänglich zu machen.[19] Die Quellen der Software – also der für Menschen vergleichweise leicht verständliche Programmtext vor der Übersetzung in eine maschinell ausführbare Repräsentation – werden dazu ebenfalls zugänglich gemacht.

Unter den zahlreichen Lizenzformen unter denen Open Source Software oder freie Software angeboten wird, ragt wegen ihres hohen Bekanntheitsgrads vor allem die GNU General Public License (GPL) heraus, vgl. Abbildung A.2 [20].

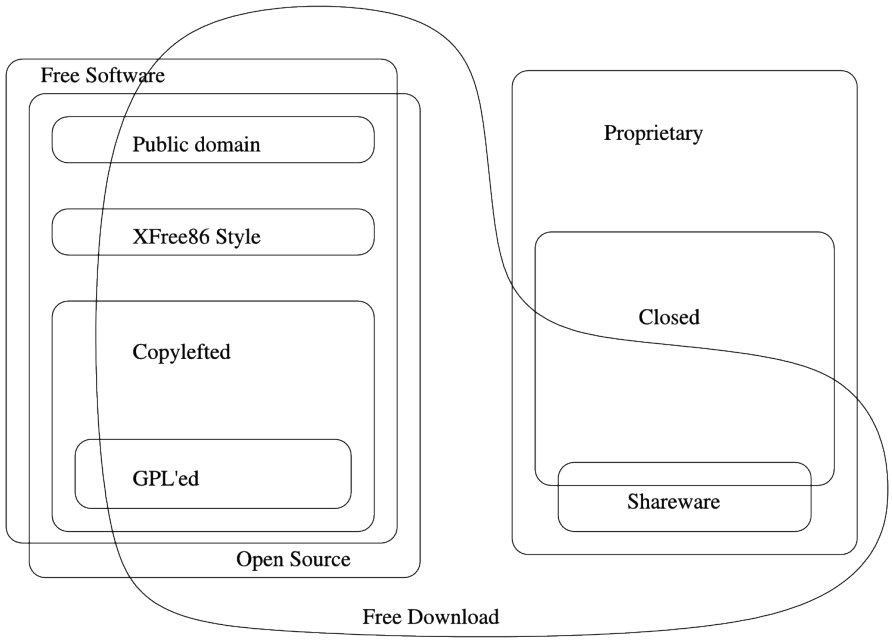

Abbildung A.2: Kategorisierung von Software nach Lizenzmodell (Quelle: FSF)

Darüber hinaus wird Open Source Software vor allem im I&K-Bereich gern von Lösungsanbietern als Bestandteil ihrer Leistung an Kunden weitergegeben. Im Vordergrund der wirtschaftlichen Betrachtung steht dabei allerdings weniger das Kostenargument, sondern interne Faktoren

[18] Wandtke/Bullinger-Grützmacher 2009, UrhG § 69c Rn 73.

[19] Metzger und Jaeger 1999, S. 840 f.

[20] FSF 2009; eine Übersicht über verschiedene Open-Source-Lizenzen und deren Wortlaut bietet die Open Source Initiative URL: `http://www.opensource.org/licenses/` (zuletzt besucht am 08.12.2009).

wie die Aneignung von Wissen aus der „Community“ und die Realisierung von Effizienzgewinnen durch gemeinschaftliche Entwicklungen und eine Durchsetzung von Eigenentwicklungen am Markt.[21] Zudem können externe Faktoren eine Rolle spielen, vor allem die Erwartungshaltung der Kunden in einem unvollkommenen Informationsmarkt: Als Anbieter im I&K-Bereich fehlt es jungen und vergleichsweise unbekannten Unternehmen oftmals an der notwendigen Reputation, um mit ihrem Produkt am Markt fußzufassen.[22]

Die Vertrauensbasis zwischen Anbieter und Kunde muss sich folglich aus dem Angebot selbst ergeben. Hier hilft der Einsatz von Standardsoftware, deren Vorteile und Einschränkungen vom Kunden leichter eingeschätzt werden können. Neben den Vorzeigeprodukten namhafter Softwarehersteller haben mittlweile auch einige Open-Source-Projekte diesen Status erreicht.[23] Der Einsatz von Open Source Software ermöglicht in solchen Fällen oftmals überhaupt erst den Markteintritt für kleine und mittlere Unternehmen, wird also zum „Business-Enabler“[24].

Beide Faktoren – interne und externe – bedeuten für die betreffenden Unternehmen einen Anreiz, ihrerseits einen Beitrag zur Weiterentwicklung der verwendeten Open Source Software zu leisten. Je nach Komplexität des (Open Source) Projekts und Anspruchsdenken der damit befassten öffentlichen Entwicklergemeinschaft ist dazu ggf. eine Unterordnung in die bestehende Projekthierarchie notwendig, Steuerungsfunktionen sind in erster Linie an die Reputation von beteiligten Softwareentwicklern geknüpft.[25]

Aus dieser Situation heraus ist es zu erklären, dass gerade hochqualifizierte Mitarbeiter in der Softwareentwicklung ihre eigene Reputation und den Spaßfaktor als wesentliche Gründe für eine Mitarbeit an Open-Source-Projekten sehen.[26] Eine Veröffentlichung der entwickelten Programme stellt für diese Mitarbeiter einen zusätzlichen Anreiz dar, sich über das normale Maß hinaus zu engagieren und auch in kurzer Zeit qualitativ hochwertige Ergebnisse einschließlich einer geeigneten Dokumentation zu liefern. Hinzu tritt außerdem das öffentliche Review von

[21] Günther 2008, S. 166; Wieland 2004, S. 114.

[22] Welfens u. a. 2004, S. 62.

[23] Einige Kennzahlen über große Projekte aus dem Bereich quelloffener und freier Software liefert Wheeler 2007; Vgl. auch Hasecke 2008; Rahemipour 2008.

[24] Welfens u. a. 2004, S. 139; West 2008, S. 84.

[25] Seifert und Wieland 2003, o. S.; Wieland 2004, S. 116.

[26] Luthiger 2004, S. 95–97; Wieland 2004, S. 116; Seifert und Wieland 2003, o. S.; Heinrich u. a. 2006, S. 61 ff., m. w. N.

sicherheitskritischen Programmteilen, das vor allem in den sensiblen Bereichen der Telekommunikationseinrichtungen eine wichtige Funktion einnimmt.

Im strafrechtlichen Sinne problematisch wird die Veröffentlichung von Software bereits dann, wenn die Software zur Begehung einer Straftat genutzt werden kann, es sich also mindestens um ein Dual-Use-Tool handelt. Mit der Aufnahme des neuen § 202c in das Strafgesetzbuch durch das 41. StrÄndG[27] kann bereits die Herstellung und Überlassung derartiger Werkzeuge den objektiven Tatbestand einer Vorbereitungshandlung erfüllen, wenn bei objektiver Betrachtung die Absicht zur Begehung einer Straftat gemäß §§ 202a, 202b, 303a oder 303b StGB vorliegt. Unternehmen sollten daher vor einer Veröffentlichung entsprechender Software eine ausführliche Prüfung auf eventuell einschlägige Normen durchführen, um eine strafrechtliche Verfolgung zu vermeiden.

II. Problemstellung

In der vorliegenden Arbeit wird diese Fragestellung anhand eines konkreten Anwendungsfalls auf dem Gebiet der Telekommunikation eingehend untersucht. Nach der Ausdehnung der Liberalisierung des Telekommunikationsmarkts auf die Erbringung von Sprachdiensten im Jahr 1998 und die in der Folge wettbewerbsrechtlich sichergestellte Verfügbarkeit von Mietleitungen mit ausreichender Bandbreite für die Sprachübertragung haben viele Zugangsanbieter in Deutschland die Möglichkeit wahrgenommen, ihr Angebot um einen Sprachtelefoniedienst auf der Basis von Internet-Technologien („Voice over Internet Protocol“, VoIP) zu erweitern.

Abbildung A.3[28] zeigt einen deutlichen Anstieg der Gesamtanzahl von Telefonanschlüssen, die über die neuen Teilnehmer auf dem Telekommunikationsmarkt nach 1998 realisiert worden sind.[29] Auffällig ist der Rückgang von ISDN- und Analoganschlüssen gegenüber einem signifikanten Wachstum von Sprachzugängen über entbündelte[30] Teilnehmeranschlüsse.

[27] *BGBl. I Nr. 38 vom 10.08.2007, 1786.*

[28] BNetzA 2008, S. 67.

[29] Die nationale Regulierungsbehörde bezeichnet diese als „alternativen Teilnehmernetzbetreiber“, da der Endkundenanschluss („Teilnehmeranschluss“ nach Art. 2 lit. c VO (EG) 2887/2000/EG) für den Sprachtelefoniedienst nicht von dem vorherrschenden Marktteilnehmer, der Deutschen Telekom, bereitgestellt wird.

[30] Vgl. Art. 2 lit. e VO (EG) 2887/2000/EG.

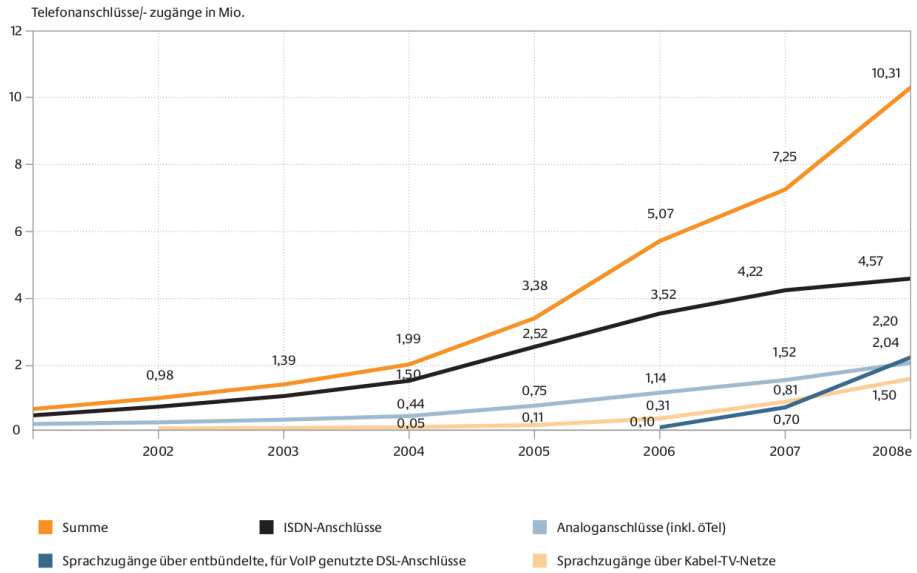

Abbildung A.3: Entwicklung der Telefonanschlüsse/-zugänge der alternativen Teilnehmernetzbetreiber (Quelle: BNetzA)

Als ein wesentliches Problem für die Markteinführung von Sprachtelefonie über VoIP galt lange Zeit die von einige etablierten Marktteilnehmern geförderte Erwartungshaltung vieler Endkunden, die zugrunde liegende Vermittlungstechnik führe zu einer geringeren Sprachqualität und sei zudem schlechter gegen Ausfälle des Telefondienstes abgesichert. Zwar könnten technische Unzulänglichkeiten und mangelnde Erfahrung beim Betrieb eines komplexen Echtzeit-Dienstes bei einigen der neu in den Markt eingetretenen Anbieter tatsächlich zu spürbaren Qualitätseinbußen gegenüber der nach jahrzehntelangem Betrieb bewährten leitungsvermittelten Technik geführt haben, doch zeigt die Marktentwicklung einen ungebrochenen Trend zur Umstellung auf die neue Technik, der sich auch etablierte Anbieter nicht mehr entziehen können.

Aufgrund dessen erreichen zumindest die überregional operierenden Teilnehmernetzbetreiber eine Ausfallsicherheit von rund 99,999 % und eine mit dem alten Telefonnetz vergleichbare Sprachqualität. Teilweise werben Anbieter von Geräten für den Heimgebrauch unter dem Stichwort „HD-Telefonie“[31] sogar mit dem Umstand, dass die hohe Bandbreiter heutiger Teilnehmeranschlüsse mit entsprechender Kodierungstechnik eine erheblich bessere Sprachqualität ermöglicht.

Zur Sicherstellung der Ausfallsicherheit werden an den neuralgischen Punkten im Telefonnetz mehrfach abgesicherte Systeme zur Durchleitung der Telefoniesignale eingesetzt. Die Vermittlungstechnik, auf der

[31] Vgl. Mansmann 2009.

der VoIP-Sprachdienst aufsetzt, bringt gegenüber dem klassischen Telefonnetz allerdings einige Änderungen mit sich, die vom Dienstanbieter beim Betrieb der Telekommunikationseinrichtungen beachtet werden müssen. Hierzu zählt unter anderem der Schutz der Einrichtungen vor Überlastung. Während im klassischen Telefonnetz vor allem die Anzahl der parallelen Leitungsverbindungen (und in begrenztem Umfang auch die Geschwindigkeit, mit der Gespräche auf diesen Leitungen durchgeschaltet werden können) von Bedeutung ist, wird die Kapazität eines VoIP-Netzes vor allem durch die Geschwindigkeit bestimmt, mit der einzelne Nachrichten verarbeitet werden können. Diese hängt einerseits von der Bandbreite des Netzes ab, stärker aber noch von der Leistungsfähigkeit der Netzknoten.[32]

Da die Leistungsfähigkeit von Netzknoten für das Next Generation Network[33] (NGN) stark von der jeweils realisierten Funktionalität sowie der Effizienz der eingesetzten Algorithmen abhängt, ist eine Bewertung nur anhand von Systemparametern wie Hardwareausstattung oder verwendeter Betriebssoftware sehr schwierig. Vor der erstmaligen Übernahme in den Wirkbetrieb und nach Aktualisierung der Software sind daher Belastungstests notwendig, um eine Destabilisierung des Gesamtsystems durch die vorgenommenen Änderungen ausschließen zu können.

Eine besonders kritische Funktion für den Sprachdienst ist die Registrierung von Telefonie-Endpunkten. Anders als im klassischen Telefonnetz, wo jeder Teilnehmeranschluss direkt über das angeschlossene Kabel erreicht wird, entsteht die Zuordnung zwischen der Rufnummer eines Teilnehmers und der Gerätekennung eines angeschlossenen Telefonie-Endpunkts dynamisch und wird in regelmäßigen Abständen automatisch aktualisiert. Dadurch wird unter anderem sichergestellt, dass ein Teilnehmer auch dann noch erreichbar ist, wenn die DSL-Verbindung unterbrochen worden ist und sich die (dynamisch zugewiesene) IP-Adresse[34] für

[32] An Übergängen ins klassische (leitungsvermittelte) Telefonnetz sowie bei der Zusammenschaltung zwischen Netzbetreibern kann es weitere Einschränkungen geben, die für die Betrachtung hier jedoch nicht wesentlich sind.

[33] Die Zusammenschaltung von Telekommunikationsdiensten erfolgt in Deutschland auf der Basis bilateraler Verträge zwischen Telekommunikationsnetzbetreibern. Für die technische Ausgestaltung der Netzzusammenschaltung wurde der gemeinsame Arbeitskreis für technische und betriebliche Fragen der Nummerierung und Netzzusammenschaltung (AKNN) eingerichtet. Dort wurde unter Zugrundelegung von ITU-T Rec. Y.2001 ein Konzept für die Zusammenschaltung paketvermittelter Netze in Deutschland entworfen (AKNN 2009).

[34] Adressierungsinformation auf der Ebene des Internet-Protokolls (IP). Für die derzeit vorherrschende Version 4 handelt es sich dabei um eine global eindeutige 32-Bit-Zahl, über die der betreffende Rechner im Internet erreicht werden kann (vgl. Postel

den betreffenden Teilnehmeranschluss nach der Wiederherstellung der Verbindung geändert hat.

Darüber hinaus ist diese Funktion Bestandteil der Vermittlung von Telefonanrufen an die darüber registrierten Teilnehmer. Belastungstests für diese Komponente umfassen daher nicht nur die regelmäßige Registrierung von Telefonie-Endpunkten, sondern auch die Anrufsignalisierung im Telefonnetz. Dies kann natürlich nicht im Wirkbetrieb erfolgen, sondern wird unter möglichst realen Bedingungen nachgestellt. Als Open Source Software finden hier vor allem die Programme `PROTOS`[35] und `SIPp`[36] im breiten Einsatz.

Bei `SIPp`, das in der folgenden Betrachtung im Vordergrund steht, handelt es sich um ein frei verfügbares Werkzeug, das in den wesentlichen Teilen unter der GPL in der Version 2 veröffentlicht worden ist, zwei Dateien des Quellcodes unterfallen der vereinfachten BSD-Lizenz.[37] Das Programm ermöglicht das Versenden von Signalisierungsinformationen für das verwendete Telefonie-Protokoll mit sehr hoher Geschwindigkeit, so dass damit das Registrierungsverhalten von weit über einer Million Telefonie-Endpunkten nachgestellt werden kann. Daneben bietet es noch Funktionen zum Simulieren von Telefonanrufen, einschließlich des Einspielens vorab aufgezeichneter Audiodatenströme.

Die Software erlaubt Tests mit sehr hoher Geschwindigkeit und eignet sich aufgrund eines flexiblen Konfigurationsmechanismus für die Erprobung der wichtigsten Funktionen der zuvor beschriebenen Telefonieeinrichtungen. Allerdings lassen sich damit nur Nachrichten mit der Senderadresse (bzw. den wenigen Senderadressen) des Systems erzeugen, auf dem die Software installiert ist. In der Praxis hat sich jedoch gezeigt, dass zahlreiche Gerätehersteller die Auswirkungen einer großen Anzahl von Nachrichten mit unterschiedlichen Quelladressen unterschätzen, beispielsweise indem interne Tabellen mit Millionen Einträgen nicht effizient aktualisiert werden können. `SIPp` wurde daher für interne Tests so erweitert, dass die versendeten Nachrichten zum Testen der Vermittlungssysteme beliebige IP-Adressen als Quelladresse aufweisen können. Eine eigens für die betreffenden Tests eingerichtete Routing-Infrastruktur ermöglicht zudem die Belastungsprüfung im Wirkbetrieb.

1981).

[35] Wieser, Laakso und Schulzrinne 2004, S. 166.

[36] Jacques und Gayraud 2004.

[37] Der Wortlaut beider Lizenzen ist zu finden unter URL: `http://www.opensource.org/licenses/` (zuletzt besucht am 08.12.2009).

III. Gang der Untersuchung

Aus dem Gesagten ergibt sich bereits, dass die Open Source Software `SIPp` geeignet ist, Telekommunikationssysteme unter hohe Last zu setzen und damit potentiell den von diesen Geräten erbrachten Dienst zu beeinträchtigen. Zusätzlich wurde das Programm um die Möglichkeit erweitert, die Quelladresse der versendeten Nachrichten beliebig abzuändern und dem Empfänger der Daten somit einen anderen Ursprung vorzutäuschen. Damit weist das veränderte Programm ein erheblich höheres Gefährdungspotential auf als das Original und ist somit noch kritischer vor dem Hintergrund der Vorbereitung einer Straftat gemäß §§ 303b Abs. 1 Nr. 2, Abs. 5 StGB i. V. m. § 202c StGB zu beurteilen. Die folgende Untersuchung zeigt allerdings, dass die mit dem 41. StrÄndG eingeführte Verschärfung des deutschen Strafrechts dem Open-Source-Gedanken hier nicht im Wege steht.

Zu Beginn unserer Untersuchung wird in Kapitel B. der Rechtsrahmen für die Beurteilung des Sachverhalts dargelegt. Dabei wird die grundsätzliche Vereinbarkeit der GPL mit den Regelungen zu allgemeinen Geschäftsbedingungen (AGB) gemäß §§ 305 ff. BGB vorausgesetzt,[38] da das Hauptaugenmerk auf den strafrechtlichen Aspekten einer nach deutschem Recht zu bewertenden Tat liegt.

Kapitel C. gibt einen Überblick über die einschlägigen Normen des Strafgesetzbuchs, die bei der Herstellung, der Veröffentlichung und schließlich dem Einsatz des abgeänderten Programms `SIPp` berührt werden. Durch Auslegung wird ermittelt, inwieweit die objektiven Tatbestandsmerkmale dieser Rechtsnormen erfüllt sind.

Darauf aufbauend erörtert Kapitel D. mögliche Tatbeteiligungen vor dem Hintergrund der üblichen Rollenverteilung innerhalb eines mittelständischen Unternehmens mit einer eigenen Software-Entwicklungsabteilung und unterstreicht die Forderung nach einer verstärkten Ausrichtung der Unternehmenslandschaft auf gesamtverantwortliches Handeln.

Kapitel E. beschließt diese Arbeit mit einer zusammenfassenden Würdigung der erzielten Ergebnisse und daraus abgeleiteten Handlungsempfehlungen an die Unternehmensführung.

[38] LG München I – 21 O 6123/04; mit Einschränkungen beim Haftungsausschluss: Sujecki 2005, Abs. 10 ff., m. w. N.; Spindler FS Bartsch, S. 13 f.; Schulz 2005, Rn 10–14.

B. Bekämpfung von Computerkriminalität

Als Reaktion auf den seit Jahren beobachteten statistischen Anstieg von Delikten, die im weitesten Sinne der Internet-gestützten Computerkriminalität zuzurechnen sind, hat der Gesetzgeber im Jahr 2007 die Vorbereitung entsprechender Tathandlungen unter Strafe gestellt. Diese mit dem *41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität*[39] eingebrachte Änderung des deutschen Strafgesetzbuchs ist eingebettet in eine Reihe internationaler Aktivitäten zahlreicher Staaten zur Bekämpfung der Computerkriminalität.

Diese sowohl innerhalb der EU als auch darüber hinaus auf globaler Ebene mittels völkerrechtlicher Verträge manifestierten Ziele stellen eine rechtsstaatliche Antwort auf die wachsende Kriminalität in einem virtuellen, zahlreiche Staatsgebiete berührenden Raum dar. Das deutsche Strafrecht zielt mit dem in § 3 StGB bestimmten Territorialitätsprinzip vor allem auf den Schutz inländischer Rechtsgüter.[40]

Schwierig ist die Bestimmung des anwendbaren materiellen Strafrechts für Tathandlungen im Internet, zumal § 9 StGB als Anknüpfungspunkte den Begehungsort oder Erfolgsort nennt.[41] Aufgrund dieser ubiquitären Sichtweise wäre jedwede Straftat im Internet bei wörtlicher Auslegung allerdings nach dem deutschen Strafrecht zu verfolgen.[42] Als problematisch gilt diese Sichtweise im Hinblick auf abstrakte Gefährdungsdelikte, da der Ort des Taterfolgs unbestimmt ist und somit eine nach § 3 StGB vorausgesetzte Bedrohung inländischer Rechtsgüter nicht unmittelbar ersichtlich ist.[43] Als Lösungsmöglichkeit werden daher in Anlehnung an den BGH Handlungen nach § 9 Abs. 1 3. Alt. StGB nur dann gemäß § 3

[39] *BGBl. I Nr. 38 vom 10.08.2007, 1786.*

[40] MK-Ambos 2003, StGB § 3 Rn 4–8; Schönke/Schröder-Eser 2006, StGB § 3 Rn 1–5.

[41] Schönke/Schröder-Eser 2006, StGB § 9 Rn 1, 3.

[42] Schönke/Schröder-Eser 2006, StGB § 9 Rn 7; Breuer 1998, S. 141.

[43] Breuer 1998, S. 142; Sieber 1999, S. 2067; MK-Ambos/Ruegenberg 2003, StGB § 9 Rn 27–32 m. w. N.

StGB nach dem deutschen Strafrecht zu beurteilen sein, wenn diese auch einen Inlandsbezug aufweisen.[44]

Ein solcher ist für die hier betrachtete Problemstellung der Beteiligung von inländischen Unternehmen an Open-Source-Projekten ohne weiteres zu bejahen. Der Rechtsrahmen ergibt sich daher wie im Folgenden beschrieben.

I. Convention on Cybercrime

Den grundsätzlichen Rahmen für die gemeinsame supranationale Bekämpfung gegen die „Cyberkriminalität“ bildet die am 21. November 2001 in Budapest vom Rat der Europäischen Union beschlossene *Convention on Cybercrime*,[45] in der ein Maßnahmenkatalog gegen Computer- und Internetdelikte zur Umsetzung in nationales Recht empfohlen wird. Die formale völkerrechtliche Verpflichtung zur Umsetzung geeigneter Maßnahmen gegen Angriffe auf Informationssysteme ergibt sich schließlich aus dem Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme.[46] Die innerstaatlich umzusetzenden Maßnahmen zielen nach der Cybercrime Convention auf die Abwehr folgender Gefahren:

- Rechtswidriger Zugang zu Computersystemen (Art. 2)
- Rechtswidriges Abfangen von nichtöffentlichen Daten (Art. 3)
- Unbefugter Eingriff in Daten (Art. 4)
- Unbefugter Eingriff in ein System (Art. 5)

Darüber hinaus bestimmt Art. 6 des Abkommens, dass bereits die Vorbereitung der vorgenannten Tathandlungen eine Straftat darstellen soll. Als Vorbereitung werden dabei das vorsätzliche Herstellen, Verkaufen, Verschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitiges Verfügbarmachen von Tatmitteln für die genannten Zwecke verstanden. Außerdem soll auch schon Besitz entsprechender Werkzeuge unter

[44] BGH 1 StR 184/00 (LG Mannheim) = NStZ 2001, 305; Sieber 1999, S. 2072 f.; Stegbauer 2005, S. 677; Laue 13/2009, S. 5.

[45] *Convention on Cybercrime, ETS 185*; *BGBl. II Nr. 30 vom 10.11.2008, 1242*.

[46] ABl. Nr. L 69 S. 67–71.

Strafe gestellt werden, wenn damit der Vorsatz zur Begehung einer der genannten Straftaten verbunden ist.

Die Reichweite dieser Regelung wird in Art. 6 Abs. 2 allerdings insoweit eingeschränkt, dass die genannten Handlungen nur dann als tatbestandsmäßig angesehen werden sollen, wenn damit auch der Zweck[47] der Begehung einer Straftat nach den Artikeln 2 bis 5 verbunden ist. Ausdrückliche Ausnahmen umfassen demnach auch das genehmigte Testen von Computersystemen oder den Einsatz zu deren Schutz.

Zusätzlich zu den genannten Tatbeständen nennt die Cybercrime Convention noch weitere Handlungen, die unter Strafe gestellt werden sollen, insbesondere Fälschung von Computerdaten, Computerbetrug, das Herstellen, Anbieten, Verfügbarmachen, Verbreiten oder Übermitteln, Beschaffen und den Besitz von Kinderpornographie, des Weiteren die Verletzung von Urheberrechten oder verwandten Schutzrechten.

Um die Durchsetzung von Sanktionen zu vereinfachen, sollen neben die strafrechtliche Verantwortlichkeit natürlicher Personen gesetzgeberische Maßnahmen zur Sanktionierung von juristischen Personen und ihren Organwaltern treten.

II. Umsetzung der Cybercrime Convention in das deutsche Strafrecht

Mit dem 41. StrÄndG erfolgte eine weitgehende Umsetzung des Maßnahmenkatalogs aus der Cybercrime Convention und damit auch deren (teilweise) Ratifizierung.[48] Die Grundlagen zur Bekämpfung von Delikten im Zusammenhang mit Computernutzung wurde im deutschen Strafrecht jedoch schon viel früher gelegt, insbesondere durch das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität.[49]

Die Regelungen des 2. WiKG zielten im Wesentlichen auf den Schutz wirtschaftlich bedeutsamer Rechtsgüter, indem etwa das Verändern von Daten (§ 303a StGB a. F.) oder die Computersabotage (§ 303b StGB a. F.) ausdrücklich auf wirtschaftlich bedeutsame Daten bezogen worden sind,[50]

[47] Vgl. Popp 2007, S. 87.
[48] Schumann 2007, S. 675; Hoeren 2009, S. 513.
[49] *BGBl. I Nr. 21 vom 23.05.1986, 721*; Schultz 2006, S. 784.
[50] *BT-Drs. 10/5058*, S. 34.

und das Ausspähen von Daten blieb straffrei, solange sich der Täter lediglich unbefugt Zugang zu den Daten verschafft hatte, ohne die Daten jedoch selbst zur Kenntnis zu nehmen oder einem Dritten zu verschaffen.[51]

Das 41. StrÄndG verschärft vor allem die bestehenden Normen §§ 202a, 303b StGB a. F., indem nun auch der Zugang zu fremden Daten untersagt ist (§ 202a StGB) und die Computersabotage nach § 303b StGB auf jegliche fremde Datenverarbeitung anwendbar ist.[52] Neu hinzugekommen sind außerdem § 202b StGB über das Abfangen von Daten und der Vorbereitungstatbestand in § 202c StGB, der qua Verweis auch für die §§ 303a, 303b StGB sinngemäß anwendbar ist.

III. „Dual-Use-Tools“ in der Rechtsprechung

Mit der Umsetzung der Cybercrime Convention in nationales Recht hat der Gesetzgeber konsequent versucht, Strafbarkeitslücken im Sinne der internationalen Verfolgung von Straftaten im Internet zu schließen. Dass dieser Wille auch von den Gerichten getragen wird, zeigt sich in einigen jüngeren Beschlüssen von Bundesverfassungsgericht und Bundesgerichtshof. In seiner Entscheidung zur Verfassungsmäßigkeit von verdeckten Ermittlungsmaßnahmen in Datennetzen stellte das BVerfG noch einmal die Bedeutung der informationellen Selbstbestimmung heraus und verwies auf das vom allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG umfasste Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme in Privaträumen sowie Betriebs- und Geschäftsräumen.[53]

Das BVerfG hatte sich nach Einführung des neuen Vorbereitungstatbestands in § 202c StGB außerdem mit der Frage zu beschäftigen, inwieweit diese Regelung in die Berufsfreiheit von Personen eingreife, die aufgrund ihrer beruflichen Tätigkeit mit Schadprogrammen und Hackertools zu tun haben.[54] Ein wesentlicher Punkt in der Ablehnung der Verfassungsbeschwerde stellt die Abgrenzung zwischen dem „Zweck“ einer Software i. S. d. § 202c StGB dar und ihrer „Eignung“ zur Begehung

[51] Schumann 2007, S. 676; Popp 2007, S. 85; *BT-Drs. 16/3656*, S. 9; *BT-Drs. 10/5058*, S. 28 f.

[52] *BT-Drs. 16/3656*, S. 13.

[53] BVerfG 1 BvR 370/07, 1 BvR 595/07 = MMR 2008, 315, S. 316 f.; Hoeren 2009, S. 538.

[54] BVerfG 2 BvR 2233/07 = ZUM 2009, 745.

einer Straftat. Demnach reiche es nicht aus, wenn sich ein Programm lediglich dazu eigne, auch strafbare Handlungen zu begehen. Es müsse vielmehr schon bei der Entwicklung des Programms eine entsprechende Absicht vorgelegen haben, die sich auch objektiv manifestiere und durch Auslegung zu ermitteln sei.[55]

Für die Auslegung objektiver Merkmale kann die Funktionsweise und Ausgestaltung der Software selbst herangezogen werden, aber auch äußere Umstände wie die Vermarktung können eine Rolle spielen. So kam das OLG München im Rahmen seiner Entscheidung über einen Hyperlink auf eine Software zur Umgehung technischer Kopierschutzmaßnahmen für Bild- und Tonträger zu der Auffassung, die betreffende Software AnyDVD sei Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen i. S. d. § 95a Abs. 3 Nr. 1 UrhG.[56]

Bereits vor dem 41. StrÄndG hatte das OLG Frankfurt a. M. darüber zu entscheiden, ob in der vorangekündigten Überlastung eines Web-Servers im Internet und der Zurverfügungstellung eines für diesen Zweck bereitgestellten Computerprogramms eine Datenunterdrückung i. S. d. § 303a StGB a. F. vorliegt bzw. eine Aufforderung dazu gemäß § 111 StGB a. F. erfolgt ist.[57] Zuvor hatte das AG Frankfurt a. M. entschieden, dass in dem durchgeführten Angriff eine strafbare Nötigung zu sehen sei und ferner der Tatbestand der öffentlichen Aufforderung zu einer Straftat erfüllt sei.[58]

Im Ergebnis sehr umstritten,[59] kann eine auf abschließende Wertung hier verzichtet werden, da mit dem neuen § 303b StGB in Zukunft eine einschlägige Strafnorm für Computersabotage durch Internet-Blockaden bzw. Denial-of-Service-Angriffe zur Verfügung steht.[60]

[55] BVerfG 2 BvR 2233/07 = ZUM 2009, 745; Ernst 2007, S. 2663.

[56] OLG München 29 – U 2887/05 = ZUM 2005, 896, S. 898 f.; Leupold/Glossner-Cornelius 2008, Teil 8 Rn 86.

[57] OLG Frankfurt a. M. – 1 Ss 319/05 = MMR 2006, 547.

[58] AG Frankfurt a. M. – 991 Ds 6100 Js 226314/01 = MMR 2005, 863.

[59] Hilgendorf 10/2006; Gercke 2006; Eichelberger 2006.

[60] Ernst 2007, S. 2665; Hoeren 2009, S. 530; Laue 13/2009, S. 7.

C. Untersuchung des objektiven Tatbestands

Wie im vorhergehenden Kapitel anhand der gesetzlichen Maßnahmen gegen Internetkriminalität erläutert, geht von Computerprogrammen eine bedeutende Gefahr für Datenverarbeitungsanlagen aus. Anhand des Programms `SIPp` und daran für den speziellen Einsatz bei einem alternativen Telekommunikationsanbieter vorgenommenen Erweiterungen für die Abänderung der Senderadressen wird in diesem Kapitel die Auslegung des objektiven Tatbestands der einschlägigen strafgesetzlichen Normen erläutert. Zuvor bietet Abschnitt C.I. einen kurzen Einblick in die Funktionsweise von `SIPp` und mögliche Einsatzszenarien bei der Qualitätssicherung von Telekommunikationsanlagen.

I. `SIPp` als Tatwerkzeug

Die Öffnung des Telekommunikationsmarkts für Sprachdienste eröffnete nicht nur neuen Anbietern den Eintritt zu diesem Dienstleistungsmarkt, sondern schaffte auch neue Betätigungsfelder für Hersteller von Infrastrukturkomponenten wie Vermittlungsanlagen oder Endgeräten. Die für Sprachtelefonie neue Technik auf der Basis des Protokolls SIP (Session Initiation Protocol[61]) zeichnet sich durch einen vergleichsweise einfachen Aufbau der ausgetauschten Nachrichten aus, daher können Funktionen für die Signalisierung bereits mit geringem Aufwand hergestellt werden.

`SIPp` eignet sich insbesondere für isolierte Funktionstests, da es die grundlegenden technischen Protokollmechanismen für die Kommunikation mittels SIP bereitstellt und darauf aufbauend lediglich die Anwendungslogik – von der Anrufsignalisierung bis hin zu komplexen Mehrwertdiensten – in einer einfachen Spezifikationssprache definiert werden muss. Die so definierten *Szenarien* lassen sich dann automatisch mit einer beliebigen Senderate wiederholen. Bei jeder Wiederholung können

[61] Rosenberg u. a. 2002.

variable Felder der Nachrichten verändert werden, so dass beispielsweise unterschiedliche Teilnehmerkennungen eingesetzt werden können.[62] Das Missbrauchspotential dieser Funktion wird üblicherweise durch kryptographische Sicherungsmechanismen[63] eingegrenzt, die eine Zuordnung empfangener Nachrichten zu den darin enthaltenen Anruferkennungen[64] erlauben.

Die Identifikation von Teilnehmern[65] erfolgt beim Teilnehmernetzbetreiber anhand der Anruferkennung innerhalb einer Nachricht. Neben der IP-Adresse der gesendeten Nachricht, mit deren Hilfe der betreffende Teilnehmeranschluss[66] ermittelt werden kann, erlaubt die Anruferkennung folglich Rückschlüsse auf den Teilnehmer selbst. Vor der Durchleitung von Anrufen wird eine Vermittlungseinrichtung daher die mitgesandte kryptographische Information auswerten und auf Basis der (authentischen) Teilnehmerkennung entscheiden, ob der Anruf an das gewählte Ziel zulässig ist. Auf diese Weise kann weitgehend sichergestellt werden, dass der angebotene Sprachdienst nur berechtigten Nutzern zur Verfügung steht.

Damit ein Teilnehmeranschluss auf diesem Weg erreicht werden kann, registrieren sich die angeschlossenen Endgeräte mit der Kennung des betreffenden Teilnehmers, indem sie in regelmäßigen Abständen[67] eine entsprechende Nachricht mit ihrer IP-Adresse und Kennung an die nächste erreichbare Vermittlungsstelle senden. Auch hier wird mittels kryptographischer Techniken sichergestellt, dass jeder Teilnehmer nur seine eigene Kennung anmelden kann, wobei jedoch keine Beschränkung der Registrierungen auf den eigenen Teilnehmeranschluss vorgesehen ist.

Je nach Anzahl der direkt angeschlossenen Endgeräte und der ausgegebenen Teilnehmerkennungen sind die betroffenen Vermittlungsstellen vergleichsweise hohen Anforderungen ausgesetzt. Jede eintreffende Registrierung erfordert im ersten Schritt eine Überprüfung der enthaltenen kryptographischen Information, die häufig in mehreren Schritten erfolgt und somit mehrere aufeinanderfolgende Nachrichten umfasst. Bei erfolgreicher Anmeldung wird schließlich die interne Registrierungsdatenbank

[62] Wieser, Laakso und Schulzrinne 2004, S. 167.

[63] Franks u. a. 1999, m. w. N.

[64] Anruferkennungen im NGN sind heute identisch mit Rufnummern nach ITU-T Rec. E.164. In Zukunft sind jedoch auch andere Formen von Anruferkennungen i. S. d. § 3 Satz 1 Nr. 18 TKG denkbar, wie Bergmann 2008 zeigt.

[65] § 3 Satz 1 Nr. 20 TKG

[66] § 3 Satz 1 Nr. 21 TKG

[67] Je nach Voreinstellung wenige Minuten bis zu einer Stunde.

des Dienstanbieters aktualisiert, so dass eingehende Anrufe fortan an den zuletzt gemeldeten Endpunkt weitergeleitet werden.

Wegen des hohen Nachrichtenaufkommens, das der Registrierungsprozess verursacht, stellt diese Komponente sehr hohe Anforderungen an die Ausfallsicherheit des Gesamtsystems. Eine besondere Schwierigkeit für den reibungslosen Betrieb des Systems und die Sicherung gegen Angriffe von außen ergibt sich aus der Stellung dieser Einrichtung als erster Anlaufpunkt für sämtliche Anrufsignalisierung aus dem eigenen Teilnehmernetz oder für einen Dienstanbieter ohne eigenes Netz sogar für das gesamte Internet.[68] Übliche Techniken zur Abwehr von Denial-of-Service-Angriffen[69] lassen sich hier nur sehr begrenzt einsetzen, da eine Einschränkung der Netzbereiche auf der IP-Ebene der weltweiten Erreichbarkeit entgegensteht. Als Hilfsmittel gegen eine Überlastung von Registrierungskomponenten kann eine Ratenkontrolle eingefügt werden, die zum einen eine obere Grenze für die Senderate eines jeden Endpunkts vorgibt, zum anderen eine systemweite obere Grenze festlegt.[70]

Die mit der Ratenkontrolle verbundene Speicherung von Zustandsinformationen in der Telekommunikationseinrichtung kann bei einer fehlerhaften Implementierung aufgrund der hohen Anzahl an sendenden Endgeräten leicht zu einer Überlastung des Systems führen. Um dies auszuschließen, sollen Lasttests mit `SIPp` durchgeführt werden. Allerdings ist das Programm in der veröffentlichten Version nicht in der Lage, eine erhebliche Anzahl an Endpunkten mit einer eigenen IP-Adresse zu simulieren. Es ist daher für den Einsatz bei einem alternativen Telekommunikationsanbieter derart erweitert worden, dass beliebige IP-Adressen als Absender eingetragen werden können und so die Notwendigkeit entfällt, auf dem sendenden Rechner die entsprechenden Netzschnittstellen vorab zu konfigurieren. Damit lassen sich auf einfache Weise Belastungstests durchführen, die in ihrer Ausgestaltung einem Denial-of-Service-Angriff gleichen. Dazu versendet das Programm SIP-Nachrichten mit unterschiedlichen Kennungen und unter Verwendung von unterschiedlichen IP-Adressen innerhalb eines vorgegebenen Adressbereichs. Die getestete Vermittlungsstelle kann anhand der Nachrichten nicht erkennen, dass sie von ein und demselben Sender stammen. Sie bearbeitet diese Nachrichten, als kämen sie von den angegebenen Absenderadressen.

[68] CERT/CC 2003.

[69] Vgl. Walsh und Kuhn 2005, S. 46 f.; zum Begriff siehe Ernst 2003, S. 3235; Eichelberger 2006, S. 491; Gercke 2006, S. 552.

[70] Zum Beispiel Ayuso 2006; Scholz 2006.

Um diese Tests im Labor sinnvoll durchführen zu können, muss ein zusammenhängender Adressbereich gewählt werden, der dem Initiator zugeordnet wird. Antworten der Vermittlungsstelle können dann mittels entsprechender Konfiguration der Routing-Infrastruktur an den `SIPp`-Prozess geleitet werden.

II. Einschlägige Normen des Strafgesetzbuchs

Aus der vorhergehenden Beschreibung lassen sich auf den ersten Blick einige strafrechtliche Tatbestände erkennen, die im Folgenden näher untersucht werden. Die Anwendung des abgeänderten `SIPp` könnte auf den ersten Blick die Tatbestände der Nötigung erfüllen (Abschnitt C.II.1.), der Fälschung beweiserheblicher Daten oder Täuschung im Rechtsverkehr bei Datenverarbeitung (Abschnitt C.II.2.) und der Störung von Telekommunikationsanlagen (Abschnitt C.II.7.).

Daneben sind die Regelungen des Strafgesetzbuchs über das Abfangen von Daten (Abschnitt C.II.3.), Datenveränderung (Abschnitt C.II.5.) und Computersabotage (Abschnitt C.II.6.) zu berücksichtigen. Aufgrund der abstrakten Gefährdung, die der Gesetzgeber in der Existenz der verwendeten Tatmittel – sogenannter *Hackertools* – sieht, sind bereits Vorbereitungshandlungen strafbar (Abschnitt C.II.4.).[71]

1. § 240 StGB: Nötigung

In der Literatur wird die Durchführung von DoS-Angriffen teilweise als Nötigung eingestuft.[72] Zu prüfen ist daher, ob das massenhafte Senden von SIP-Nachrichten mittels `SIPp` eine rechtswidrige Ausübung von Gewalt gegen einen Menschen darstellt, die diesen zur Duldung des damit erwirkten Zustands nötigt.

a) Gegen einen Menschen

Als Opfer des DoS-Angriffs mittels `SIPp` kommen vordringlich Betreiber von Telekommunikationseinrichtungen im NGN in Betracht. Als juristische Person fällt der Anbieter des Sprachdienstes und Betreiber der Vermittlungseinrichtung nicht darunter.

[71] *BT-Drs. 16/3656*, S. 12.

[72] Eichelberger 2006, S. 491 (zu AG Frankfurt am Main, Urt. v. 1.07.2005 – 991 Ds 6100 Js 226314/01, Online-Demo); a. A. Hilgendorf 10/2006, S. 2; Gercke 2006, S. 550.

Allerdings betrifft der DoS-Angriff auf eine Vermittlungsstelle und die damit einhergehende Störung des Telefoniedienstes auch die dort registrierten Nutzer, da ihre Erreichbarkeit herabgesetzt wird, und sie unter Umständen auch nicht selbst telefonieren können. Damit richtet sich die Handlung des Angreifers gegen einen oder mehrere Menschen.

b) Duldung

Die von dem Angriff betroffenen Menschen müssen den gegenwärtigen Zustand auch erdulden, da sie dessen Einwirkung unmittelbar ausgesetzt sind.

c) Ausübung von Gewalt

Fraglich ist, ob ein DoS-Angriff auf eine Vermittlungsstelle oder einen Teilnehmeranschluss und die damit verbundene Einschränkung des Sprachdienstes Gewalt i. S. d. § 240 Abs. 1 StGB darstellt. Der Gewaltbegriff der Nötigung ist jedoch umstritten in Fällen, bei denen keine unmittelbare Kraftentfaltung vorliegt, die eine körperliche Zwangswirkung auf das Opfer der Nötigung ausübt.[73]

Unzweifelhaft ist, dass die durch Überlast bewirkte Einschränkung des Sprachdienstes eine Zwangseinwirkung auf den Willen Dritter ausübt, der das betroffene Opfer nicht ohne erhebliche Anstrengungen entfliehen kann. Zu bezweifeln ist jedoch, dass dies bereits als physische Zwangseinwirkung auf den freien Willensentschluss zu werten ist, wie dies von einer Mindermeinung gefordert wird.[74]

d) Rechtswidrigkeit

Wird das Vorliegen von Gewalt bejaht, so ist schließlich noch zu prüfen, ob diese rechtswidrig eingesetzt worden ist. Gemäß § 240 Abs. 2 StGB ist dies der Fall, wenn die Anwendung der Gewalt für den angestrebten Zweck als verwerflich anzusehen ist. Dazu müsste das eingesetzte Nötigungsmittel in einem nicht angemessenen Verhältnis zum angestrebten Nötigungsziel stehen.

Keine Berücksichtigung bei der Bewertung der Verwerflichkeit der Handlung finden dabei nach h. M. die angestrebten Fernziele.[75] Eine Blockade

[73] Bejahend Otto 1992, S. 569; Eichelberger 2006, S. 491; a. A. Altvater 1995, S. 281; Gercke 2006.

[74] Eichelberger 2006, S. 491.

[75] Baumann 1987, S. 37; Eichelberger 2006, S. 492; Otto 1987, 213 m. w. N.; Miebach 1988, S. 132; BGHSt 1 StR 5/88 = NJW 1989, 362.

zu Demonstrationszwecken, die sich nicht unmittelbar gegen die Betroffenen richtet, wird daher regelmäßig als rechtswidrig einzustufen sein. Auch eine an sich gutgemeinte, aber ohne Einwilligung des Betreibers der Telekommunikationseinrichtung durchgeführte Lastprüfung ist vor diesem Hintergrund als verwerflich einzustufen.[76]

e) Fazit

Die Feststellung des Nötigungstatbestands stellt den Anwender des deutschen Strafrechts regelmäßig vor große Probleme, wenn es um die Auslegung des Gewaltbegriffs geht. Den vorläufigen Höhepunkt der Kontroverse um die Verfassungsmäßigkeit des § 240 StGB bildete der Beschluss des BVerfG zur Vereinbarkeit der Norm mit Art. 103 Abs. 2 GG.[77]

Wie die abweichende Stellungnahme von drei beteiligten Verfassungsrichtern zeigt, konnte in dieser Frage keine eindeutige Rechtsauffassung erzielt werden. Nach obigen Ausführungen kann davon ausgegangen werden, dass zumindest hinsichtlich der Ablehnung der Einbeziehung von Fernzielen in die Verwerflichkeitsprüfung weitgehende Einigkeit besteht. Die soziale Angemessenheit dieser nicht unmittelbar der Nötigungshandlung zugrundeliegenden Ziele soll demnach lediglich für die Strafzumessung eine Rolle spielen.

2. §§ 269, 270 StGB: Fälschung

Die Verwendung des modifizierten `SIPp` kann zudem unter den Tatbestand des § 269 Abs. 1 StGB fallen, soweit die verwendeten IP-Adressen des Senders und die Teilnehmerkennungen als beweiserhebliche Daten einzustufen sind und sich diese zur Täuschung des Empfängers oder eines Dritten eignen.

a) Beweiserhebliche Daten

Der Datenbegriff ist im Strafgesetzbuch nicht eindeutig bestimmt, sondern muss unter Berücksichtigung des jeweils betrachteten Tatbestands interpretiert werden.[78] Im Gegensatz zu § 202a Abs. 2 StGB, der mit der Art der Speicherung oder Übermittlung zumindest eingrenzende Merkmale von Daten nennt, die unter den betreffenden Tatbestand fallen sollen, lässt § 269 StGB dies weitgehend offen und stellt lediglich auf deren

[76] Zur Sozialadäquanz eigenmächtiger Handlungen siehe auch Ernst 2003, S. 87.
[77] BVerfG 1 BvR 718/89, 719/89, 722/89, 723/89.
[78] Dornseif und Schumann 2002, S. 53.

Beweiserheblichkeit ab. Eine Gleichbehandlung beider Begriffe ist daher nicht gerechtfertigt.[79]

Unter Einbeziehung des Merkmals „beweiserheblich“ ist jedoch sorgfältig von der urkundlichen Wahrnehmbarkeit und damit vom Tatbestand des § 267 StGB abzugrenzen, Dabei wird in der Literatur auf die Gesamtschau der potentiell urkundlich relevanten Daten abgestellt, bei der die Wirkung der Angaben auf einen Empfänger berücksichtigt wird.[80]

aa) IP-Spoofing

Hinsichtlich der Verwendung von falschen IP-Adressen (*IP-Spoofing*[81]) ist zu beurteilen, ob dadurch eine unechte Urkunde hergestellt wurde, die Nachricht also nicht von dem Aussteller stammt, der mit der IP-Adresse bezeichnet wird. Grundsätzlich trifft dies bei der Verwendung der „Spoofing-Funktion“ des hier betrachteten modifizierten Programms `SIPp` zu, soweit IP-Adressen verwendet werden, die dem Computer nicht zugeordnet sind. Im Gegensatz dazu ermöglicht die Originalfassung des Programms nur die Verwendung der auf dem System konfigurierten IP-Adressen,[82] so dass eine Fälschung der Adressen bereits auf der Ebene des Betriebssystems durchgeführt werden müsste und nicht durch die hier untersuchte Software erfolgt.

Zu verneinen ist die Ausstellung einer unechten Urkunde spätestens mit der Verwendung eines dem Sender zugeordneten Netzbereichs, da der Aussteller dann eindeutig erkennbar ist, selbst wenn die angegebenen IP-Adressen nicht auf den eigentlichen Schnittstellenkarten des Senderechners konfiguriert sind. Das Vorhandensein eines für die erfolgreiche Kommunikation erforderlichen Rückwegs durch das Internet ist hinsichtlich der Beweiserheblichkeit nicht gefordert und kann daher bei der Betrachtung vernachlässigt werden.

bb) Verwendung von Teilnehmerkennungen

Damit überhaupt eine syntaktisch korrekte SIP-Nachricht entsteht,[83] ist die Angabe einer Teilnehmerkennung für den Absender erforderlich. Diese bezeichnet den Aussteller der Nachricht, mithin also der fraglichen

[79] So auch Buggisch 2004, 3520 m. w. N.; *BT-Drs. 10/5058*, S. 34; offen: MK-Erb 2006, StGB § 269 Rn 14; a. A. Heghmanns 2009, Rn 1393.

[80] Dornseif und Schumann 2002, 53 ff.m. w. N.

[81] Hoeren 2009, S. 532; technisch fehlerhaft, aber i. E. korrekt Rinker 2002, S. 663.

[82] Beachte: Jede Schnittstellenkarte kann eine oder mehrere IP-Adressen besitzen, d. h. ein an das Internet angeschlossener Computer ist u. U. über mehrere IP-Adressen erreichbar.

[83] Rosenberg u. a. 2002, S. 26 ff.

Urkunde. Eine falsche Angabe würde folglich den Tatbestand der Urkundenfälschung erfüllen, da eine Teilnehmerkennung für den Sprachdienst – also eine Rufnummer – unzweifelhaft beweiserheblich ist.

b) Täuschung

Neben dem Vorliegen einer verfälschten oder unechten Urkunde ist jedoch im Einzelfall auch noch die Täuschungsabsicht zu prüfen. Eine Täuschung liegt vor, wenn der Sender der Nachricht dem Empfänger gegenüber unrichtige Tatsachen vorgibt oder wahre Tatsachen unterdrückt und den Empfänger damit zu einer Rechtshandlung veranlassen will.

Fraglich ist, ob das Senden der SIP-Nachrichten eine derartige Täuschung darstellt. Zweck der Nachrichten ist eine Zustandsänderung in der Vermittlungsstelle und ggf. damit verbundender Telekommunikationseinrichtungen. Ein rechtserhebliches Verhalten ist vordergründig nicht damit verbunden.[84] Allerdings führt die Registrierung von Endgeräten unter einer gefälschten Teilnehmerkennung zu einer fehlerhaften Annahme über die Identität des unter der Kennung erreichten Anschlussinhabers, so dass ein Dritter (nämlich ein Anrufer) in Unkenntnis der Wahrheit den Eindruck erhält, er würde mit dem echten Anschlussinhaber telefonieren. Unerheblich ist dabei, dass dies u. U. nur kurzzeitig der Fall sein wird oder dass der Anruf mangels eines angeschlossenen Endgeräts überhaupt nicht zustande kommt.

Für den Fall der mit fehlerhafter Teilnehmerkennung von `SIPp` erzeugten Anrufsignalisierung liegt ebenso eine Täuschung vor, wenn dieser „Anruf“ von der Vermittlungseinrichtung an einen anderen Teilnehmer weitergeleitet wird. Ein Beispiel für einen Angriff mit Täuschungsabsicht auf Teilnehmeranschlüsse mehrerer großer Sprachdienstanbieter in Deutschland im September 2008 zeigt, dass zahlreiche Teilnehmer auf diese Weise zum Rückruf an eine unbekannte Rufnummer veranlasst werden können.[85]

Die Täuschung von Dritten wird allerdings insoweit erschwert, dass Telekommunikationseinrichtungen für das NGN nur Nachrichten auswerten, die mittels kryptographischer Methoden einem Teilnehmer eindeutig zugeordnet werden können. Um diese zu fälschen und damit eine Täuschung herbeizuführen, müsste ein Angreifer folglich Kenntnis des zugehörigen Passworts besitzen. Ohne Nachweis der Authentizität werden

[84] MK-Erb 2006, StGB § 270 Rn 1.

[85] Eine technische Analyse des Vorgehens ist zu finden in Darilion 2008.

SIP-Nachrichten aus nicht vertrauenswürdiger Quelle aber an der ersten Vermittlungsstelle im Telekommunikationsnetz abgelehnt. Als Folge liegt keine Beeinflussung menschlicher Entscheidungen vor, was nach einer verbreiteten Meinung Voraussetzung für das Vorliegen eines Täuschungstatbestands nach § 269 StGB ist.[86]

Unabhängig von der Diskussion über die deklaratorische Funktion der Gleichstellungsklausel erfasst § 270 StGB auch den Fall der Täuschung einer Maschine,[87] so dass die Anwendbarkeit des § 269 StGB unter den vorgenannten Bedinungen erfüllt ist.

3. § 202b StGB: Abfangen von Daten

Im Zusammenhang mit gefälschten Registrierungen von Teilnehmeranschlüssen im NGN ist ferner an einen Tatbestand gemäß § 202b StGB zu denken. Da der Einsatz von `SIPp` wie bereits in Abschnitt C.II.2. dargelegt als Anwendung technischer Mittel zu werten ist, bleibt zu prüfen, inwieweit fremde Daten betroffen sind, die unbefugt aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft worden sind.

a) Fremde Daten

Nach dem Gesetzeswortlaut des § 202b Abs. 1 StGB fällt unter den Tatbestand nur das Sichverschaffen von Daten i. S. d. § 202a Abs. 2 StGB, an denen der Täter keine Verfügungsberechtigung besitzt. Der Datenbegriff ist dabei wie schon für § 269 StGB[88] nicht eindeutig festgelegt, ist aber wohl unterschiedlich aufzufassen.[89]

Nach dem ausdrücklichen Willen des Gesetzgebers soll das geschützte Rechtsgut des § 202a StGB – und damit qua Verweis auch des § 202b StGB – durch das ausdrücklich dokumentierte Geheimhaltungsinteresse des Verfügungsberechtigten charakterisiert werden.[90] Zwar zielt der Einsatz von `SIPp` in erster Linie auf die Änderung von Registrierungsdaten an der Vermittlungsstelle, doch ermöglicht gerade diese Änderung eine

[86] MK-Erb 2006, StGB § 270 Rn 1; a. A. Lackner-Kühl 2007, StGB § 270 Rn 1; Schönke/Schröder-Cramer/Heine 2006, StGB § 270 Rn 1 m. w. N.

[87] Heghmanns 2009, Rn 1400; Haft 1987, S. 9.

[88] Vergleiche Abschnitt C.II.2.

[89] Buggisch 2004, S. 3520 m. w. N.; *BT-Drs. 10/5058*, S. 34; a. A. Heghmanns 2009, Rn 1393.

[90] *BT-Drs. 10/5058*, S. 29; ebenso h. M. MK-Graf 2003, StGB § 202a Rn 2; Schönke/Schröder-Lenckner 2006, StGB § 202a Rn 1 m. w. N.

Umleitung von eingehenden Anrufen für den betreffenden Teilnehmer an das mittels SIPp registrierte Endgerät.

Auf diese Weise kann ein Täter nicht nur an die Inhaltsdaten eines Gesprächs gelangen (etwa unter Vorspiegelung eines angeschlossenen Anrufbeantworters des rechtmäßigen Anschlussinhabers), sondern auch an weitere nicht für ihn bestimmte Daten wie die Teilnehmerkennung des Anrufers und den Zeitpunkt des Gesprächs. Ein besonderes Geheimhaltungsinteresse für diese Telekommunikationsdaten ist bereits durch § 88 Abs. 1 TKG gesetzlich dokumentiert.[91]

b) Unbefugtes Sichverschaffen

Da der Sprachdienst im NGN wie das traditionelle Telefonnetz die Vermittlung von Gesprächen grundsätzlich nur an Teilnehmer ermöglicht, die zur Nutzung der verwendeten Teilnehmerkennung und des dazugehörigen Teilnehmeranschlusses berechtigt sind, stellt eine Umleitung von Anrufen mittels automatisierter Registrierung von Teilnehmerkennungen durch SIPp nur dann eine unrechtmäßige Handlung dar, wenn es sich um gefälschte Teilnehmerkennungen handelt, über die der Täter keine Verfügungsberechtigung besitzt.

c) Nichtöffentliche Übermittlung

Im Gegensatz zum leitungsvermittelten traditionellen Telefonnetz, das aufgrund des erschwerten Zugangs zu den Übertragungseinrichtungen unschwer als nichtöffentlich erkennbar ist, basiert das NGN auf Internet-Technologien, die in ihrer grundlegenden Konzeption bereits als unsicher gegenüber Datenveränderung und Manipulation einzustufen sind.[92] Das Zusammenschaltungsregime für VoIP-Netze in Deutschland[93] führt jedoch zu einer Abschottung der Kernnetze der Dienstanbieter vom öffentlichen Internet.

Soweit also Teilnehmeranschlüsse im NGN – wie in den meisten Fällen – eine Punkt-zu-Punkt-Verbindung mit dem jeweiligen Teilnehmernetzbetreiber aufbauen, ist eine dem traditionellen Telefonnetz vergleichbare Sicherheit gegen das Abhören der Übermittlung hergestellt. Trotz der Verwendung von Internet-Technologien muss der Sprachdienst im NGN also als nichtöffentliche Übermittlung angesehen werden.

[91] Zum Schutz von Telekommunikationsdaten nach Art. 10 Abs. 1 GG siehe auch BVerfG 1 BvR 370/07, 1 BvR 595/07 = MMR 2008, 315, S. 316.

[92] DFN 2006, S. 4; Sankol 2006, S. 364.

[93] AKNN 2009.

Diese Sichtweise wird ferner gestützt durch § 88 TKG, wonach ein Telefonanruf eine nichtöffentliche Übermittlung darstellt, unabhängig ob diese durch geeignete technische Maßnahmen gegen das Abhören Dritter geschützt ist.

d) Fazit

Hinsichtlich des Tatbestands aus § 202b StGB ist festzuhalten, dass das unbefugte Abfangen von Daten mittels `SIPp` immer einhergeht mit der Fälschung von Teilnehmerkennungen, die nach §§ 270, 269 StGB der Urkundenfälschung gleichgestellt ist. Zu beachten ist, dass der eigentlichen Tathandlung der unbefugten Entgegennahme von Telefongesprächen weitere deliktswürdige Handlungen vorausgehen müssen, insbesondere die Fälschung von Teilnehmerkennungen.

4. § 202c StGB: Vorbereitungshandlungen

Zusammen mit dem Tatbestand des Abfangens von Daten gemäß § 202b StGB hat der Gesetzgeber im 41. StrÄndG[94] zugleich mit § 202c StGB einen entsprechenden Vorbereitungstatbestand vorgesehen, und §§ 202a, 303a, 303b StGB entsprechend erweitert. Danach ist bereits das Herstellen, das Verschaffen und die Weitergabe von Computerprogrammen strafbar, deren Zweck von einem der vorgenannten Tatbestände erfasst wird.[95]

a) Herstellung und Weitergabe

Da diese Arbeit ausdrücklich den Einsatz von Open Source Software bei Dienstleistern in der Telekommunikationsbranche zum Gegenstand hat, ist bereits das Verschaffen von Software gegeben. Darüber hinaus wird auch die Bearbeitung und ggf. Veröffentlichung des Ergebnisses betrachtet, so dass die weiteren Handlungsalternativen des § 202c Abs. 1 StGB erfüllt sind.

Der bloße Besitz ist dabei ausdrücklich nicht erfasst,[96] sondern beim Täter muss der Wille zur eigenständigen Verfügung über das Programm als Akt des Sichverschaffens zum Ausdruck gebracht werden.[97] Dies ist

[94] *BGBl. I Nr. 38 vom 10.08.2007, 1786.*

[95] Schumann 2007, S. 678, weist zu Recht darauf hin, dass der Verkauf als schuldrechtliches Verpflichtungsgeschäft nicht erfasst sein kann.

[96] *BT-Drs. 16/3656*, S. 12.

[97] BGH 1 StR 558-97 (LG Karlsruhe) = NJW 1998, 2064, S. 2065.

im vorliegenden Szenario aufgrund des beabsichtigten Einsatzes für die Qualitätssicherung der Fall.

Mit der Erweiterung der Software um eine Funktionalität, die gemeinhin als *IP-Spoofing* bezeichnet wird, ist außerdem eine erhebliche Veränderung des ursprünglichen Programms eingetreten: Von nun an ist `SIPp` von sich aus (d. h. ohne besondere Konfigurationen auf dem ausführenden Rechner vornehmen zu müssen) in der Lage, beliebige IP-Adressen für das Versenden der Daten zu benutzen.

Als Lizenzmodell haben sich die ursprünglichen Autoren von `SIPp` für die GPL in der Version 2 entschieden. Eine Weitergabe des Programms ist daher an die Veröffentlichung unter eben dieser Lizenz vorgeschrieben.[98] Als Folge stellt die Veröffentlichung der neuen Funktionen als Open Source Software eine Verbreitung bzw. ein Zugänglichmachen im Sinne des § 202c Abs. 1 StGB dar.

b) Zweck

In der Begründung zum 41. StrÄndG weist der Gesetzgeber ausdrücklich darauf hin, dass Computersoftware als Tatobjekt nur insoweit erfasst werden soll, als sie nach der objektivierten Zweckbestimmung zur Begehung der erfassten Straftatbestände geeignet sind.[99] Die Vorbereitungshandlung wird damit zum abstrakten Gefährdungsdelikt aufgewertet, nachdem vormals die versuchte Beihilfehandlung im Fall des Ausbleibens einer Haupttat nicht strafrechtlich verfolgt werden konnte.[100]

Wie die Ausführungen im vorhergehenden Abschnitt zeigen, kann `SIPp` zu Handlungen eingesetzt werden, die grundsätzlich zu den Tathandlungen aus § 202b StGB gehören. Allerdings ist eine generelle Kriminalisierung derartiger Werkzeuge vom Gesetzgeber nicht intendiert, sondern es sei auf die *objektivierte Zweckbestimmung* abzustellen.[101]

Für die Bewertung des objektiven Zwecks ist daher zu hinterfragen, ob ein Programm gerade für die zuvor genannten Tathandlungen konzipiert worden ist.[102] Software-Werkzeuge, die zwar auch für strafbare Handlungen verwendet werden können, in ihrem eigentlichen Einsatzumfeld

[98] GPLv2, Art. 3.

[99] *BT-Drs. 16/3656*, S. 12; vgl. auch BVerfG 2 BvR 2233/07 = ZUM 2009, 745, S. 749.

[100] Schumann 2007, S. 678; Ernst 2007, S. 2663; *BT-Drs. 16/3656*, S. 11.

[101] BeckOK-Weidemann 2009, StGB §202c Rn 7; Schumann 2007, S. 678; Popp 2007, S. 86; Ernst 2007, S. 2663.

[102] Gercke 2007, S. 283; BVerfG 2 BvR 2233/07 = ZUM 2009, 745.

aber für legale Zwecke entwickelt worden sind, sollen demnach nicht in die Kategorie der „Hackertools“ fallen.[103]

Der Hauptanwendungsbereich für `SIPp` liegt im Testen der Grundfunktionalität und der Störanfälligkeit von Telekommunikationseinrichtungen. Dies zeigt sich insbesondere an einer Vielzahl zusätzlicher Funktionen, die speziell auf dieses Anwendungsgebiet abgestimmt sind. Dazu gehören beispielsweise die Erzeugung von Fehlerstatistiken, Anpassung der Nachrichtenwiederholrate während der Testläufe und die dynamische Report-Erstellung.[104]

Die in dieser Arbeit diskutierte Modifikation von `SIPp` bietet jedoch erstmals die Möglichkeit, ohne besondere Kenntnisse des unterliegenden Betriebssystems die Absenderadresse der versendeten IP-Pakete beliebig zu verändern. so dass sich dadurch auch der Charakter des Programms ändert. Zwar dient es weiterhin zur Erfüllung der zuvor genannten Aufgaben, jedoch erhöht diese neue Funktion auch sein Gefährdungspotential. Ferner erfordert die korrekte Benutzung der neuen Funktion besondere Kenntnisse und Fertigkeiten bezüglich der Konfiguration weiterer Netzkomponenten, um auch die zurückgesendeten Antwortnachrichten zu erhalten.

Bei dieser Art der Abänderung ist davon auszugehen, dass eine Eignung zur Begehung von Computerstraftaten im vorliegenden Fall gegeben ist. Zu untersuchen ist demnach im Einzelfall, ob die Entwicklung derartiger Änderungen auch in der Absicht der Begehung einer solchen Tathandlung erfolgt ist, da die bloße Eignung nicht genügen soll.[105] Als problematisch angesehen wird dabei die grundsätzliche Schwierigkeit der Unterscheidung zwischen den von der Vorschrift nicht erfassten Dual-Use-Tools und solchen Programmen, die mit böser Absicht entwickelt worden sind.[106]

c) Rechtswidrigkeit

Für Software, die nach objektiven Kriterien der Vorbereitung von Computerstraftaten dient, sind schließlich noch legale Rechtfertigungsgründe

[103] So auch ausdrücklich Art. 6 Abs. 2 sowie Rn 72 der *Convention on Cybercrime, ETS 185*; siehe auch *BGBl. II Nr. 30 vom 10.11.2008, 1242*, S. 1248.

[104] Eine ausführliche Beschreibung des Programms ist zu finden unter `http://sipp.sourceforge.net/` (besucht am 08.12.2009).

[105] *BT-Drs. 16/3656*, S. 18 f.; BVerfG 2 BvR 2233/07 = ZUM 2009, 745.

[106] So insbesondere die Stellungnahmen des Chaos Computer Club und der Gesellschaft für Informatik e. V., zusammengefasst in BVerfG 2 BvR 2233/07 = ZUM 2009, 745, S. 748; Gröseling und Höfinger 2007, S. 629.

zu berücksichtigen. Mangels einer akuten Gefahrenlage ist keine Notwehrsituation gegeben. Fraglich ist, ob eine ausdrückliche Einwilligung des Betreibers einer Vermittlungseinrichtung die Rechtswidrigkeit entfallen lässt oder ob eine Lösung der Problematik auf Tatbestandsebene erforderlich ist.[107]

Für § 202c StGB führt das Bundesverfassungsgericht aus, dass eine Einwilligung zu Penetrationstests an Computeranlagen durch ein auf die Aufdeckung von Sicherheitslücken spezialisiertes Unternehmen bereits das Tatbestandsmerkmal der Unbefugtheit entfallen lässt und sich somit eine Prüfung des subjektiven Tatbestands erübrige.[108]

5. § 303a StGB: Datenveränderung

§ 303a StGB stellt die rechtswidrige Zerstörung von Daten i. S. d. § 202a Abs. 2 StGB unter Strafe. Die strafbare Handlung zielt dabei auf ein gezieltes Vorenthalten der Daten gegenüber einem Verfügungsberechtigten durch Löschen, Verändern oder auch Unbrauchbarmachen oder Unterdrücken, und schließt den Vorbereitungstatbestand mit ein.

a) Daten

Für den Datenbegriff verweist die Norm auf § 202a Abs. 2 StGB, wobei insbesondere fremde Daten im Fokus stehen.[109] Im konkreten Fall geht es also um die Registrierungsdaten einer Vermittlungsstelle im NGN (vgl. Abschnitt C.II.3.a), durch die die Erreichbarkeit von Teilnehmern gewährleistet wird.

b) Tathandlung

Der Katalog der Tathandlungen des § 303a StGB umfasst eine große Bandbreite an Beeinträchtigungen, die im Ergebnis eine Einschränkung in der Verwendbarkeit der Daten für den Verfügungsberechtigten bewirken.[110]

Im vorliegenden Fall verhindert eine mittels `SIPp` herbeigeführte Überlastung, dass reguläre Registrierungsnachrichten von anderen Teilnehmern verzögert oder gar nicht bearbeitet werden. Dies kann zur Nichterreichbarkeit des betreffenden Teilnehmers während dieses Zeitraums

[107] BeckOK-Weidemann 2009, StGB § 202c Rn 9b.
[108] BVerfG 2 BvR 2233/07 = ZUM 2009, 745.
[109] Schönke/Schröder-Stree 2006, StGB § 303a Rn 3.
[110] Schönke/Schröder-Stree 2006, StGB § 303a Rn 4; Lackner-Kühl 2007, StGB § 303a Rn 1, 3 m. w. N.

führen, da der interne Registrierungsstatus einer Vermittlungsstelle für jeden Teilnehmeranschluss regelmäßig aktualisiert werden muss, damit diese Zustandsinformation nicht automatisch verfällt. Bei einer Überlastung des Systems können Nachrichten nicht so schnell verarbeitet werden oder werden gar von den vorgesehenen Mechanismen zum Schutz vor Überlastungen herausgefiltert.[111]

Das Verfallen der Registrierung ist in diesem Fall eine kausale Folge des Ausbleibens der Auffrischungsnachricht. Die Überlastung der Vermittlungsstelle führt damit zumindest zum Unbrauchbarmachen der bestehenden Daten.[112] Dem Verfügungsberechtigten – hier dem Systembetreiber zur Zustellung eingehender Anrufe – sind diese Daten entzogen, so dass der betreffende Teilnehmer telefonisch nicht mehr erreichbar ist.

Anders als im Fall der sogenannten Online-Demonstrationen, bei denen eine Überlastung eines Servers im World Wide Web mittels eines DoS-Angriffs herbeigeführt wird,[113] handelt es sich bei den betroffenen Daten um flüchtige Daten, die mit einem Verfallsdatum versehen sind. Eine regelmäßige Aktualisierung ist folglich notwendig, um den angebotenen Dienst aufrecht zu erhalten. Das Verhindern dieser Aktualisierung gleicht damit dem zeitweisen Entzug einer Urkunde[114].

In seiner Urteilsbegründung weist das OLG Frankfurt a. M. ausdrücklich auf diesen Unterschied in der Rechtsprechung des Reichsgerichts hin, nach der das vorsätzliche Vorenthalten einer Urkunde dem Straftatbestand des Unterdrückens genügen könne.[115] Mit diesem Hinweis unterstützt das OLG Frankfurt a. M. die hier vertretene Auffassung, dass bereits die zeitweise Nichtverfügbarkeit der Registrierung aufgrund der daraus erwachsenden Nachteile für die Verfügungsberechtigten als Unbrauchbarmachen zu werten ist.

c) Rechtswidrigkeit

Wie zuvor bereits gesehen, entfällt die Rechtswidrigkeit bei Vorliegen einer Erlaubnis des Betreibers der Vermittlungseinrichtung.

---

[111] Etwa *ratelimit*, s. o.

[112] *BT-Drs. 10/5058*, S. 35.

[113] Siehe Eichelberger 2004, S. 491; Hilgendorf 10/2006; Gercke 2006, S. 547; a. A. Laue 13/2009, S. 7.

[114] Zur Urkundeneigenschaft der SIP-Nachrichten siehe Abschnitt C.II.2..

[115] Gercke 2006, S. 551.

d) Vorbereitungshandlung

Gleichzeitig mit der Einfügung des § 202c in das Strafgesetzbuch (vgl. Abschnitt C.II.4.) wurde auch § 303a StGB um einen entsprechenden Vorbereitungstatbestand ergänzt, da nach §§ 303a, 303b StGB a. F. bei Ausbleiben der Haupttat auch die Vorbereitungshandlung straffrei bleiben musste.[116] Mit dieser neuen Regelung ist bei der Untersuchung der Tatbestandmäßigkeit der Herstellung und Verbreitung von potentiell gefährlicher Software wiederum auf die objektivierte Zweckbestimmung abzustellen.

Angewandt auf `SIPp` wird schnell klar, dass die zeitweise Unbrauchbarkeit der Daten zwar eine Folge der Server-Überlastung ist, die mittels `SIPp` hervorgerufen werden kann. Allerdings ist dies nur ein möglicher Seiteneffekt, der bei der Anwendung des Programms auftreten kann, nicht aber der Hauptzweck des Programms. Das Vorliegen einer Vorbereitungshandlung i. S. d. § 303a StGB ist im Falle von `SIPp` somit zu verneinen.

6. § 303b StGB: Computersabotage

Vor dem Hintergrund der Ausführungen zu § 303a StGB in Abschnitt C.II.5. ist des Weiteren an die Tatalternativen aus § 303b Abs. 1 StGB zu denken. Die aufgezählten Alternativen betreffen den rechtswidrigen Eingriff in ein System in Form einer erheblichen Störung durch Datenveränderung (1), DoS-Angriffe (2) oder physische Einwirkung auf die Hardware.

a) Datenverarbeitung von wesentlicher Bedeutung

Die wesentliche Änderung, die sich mit dem 41. StrÄndG hinsichtlich der Computerkriminalität ergeben hat, ist die Ausdehnung des Begriffs der Datenverarbeitung in § 303b StGB. Nachdem vormals grundsätzlich das Interesse von Wirtschaft und öffentlicher Verwaltung an einer ordnungsgemäß funktionierenden Datenverarbeitung im Vordergrund stand, soll nunmehr jedwede fremde Datenverarbeitung inbegriffen sein, soweit sie für den anderen von wesentlicher Bedeutung ist.[117] Für betriebliche Datenverarbeitung oder Behörden wurde allerdings die strafverschärfende Vorschrift des § 303b Abs. 2 StGB eingefügt.

[116] Eichelberger 2004, S. 597.
[117] *BT-Drs. 16/3656*, S. 13; Schumann 2007, S. 679; Ernst 2007, S. 2664 f.

Gemäß der Gesetzesbegründung dient das Merkmal der „wesentlichen Bedeutung“ lediglich dem Ausschluss von Bagetellfällen.[118] Da die Vermittlungseinrichtung eines Telekommunikationsdienstleisters unmittelbar für das Funktionieren des Sprachdienstes verantwortlich ist, erfüllt sie ohne Zweifel das Kriterium der wesentlichen Bedeutung.

b) Fremdheit

Zur Beurteilung der Fremdheit der Datenverarbeitung ist auf die eigentumsrechtlichen Verhältnisse abzustellen.[119] Für Qualitätssicherungsmaßnahmen innerhalb eines Betriebs ist demnach zu prüfen, in welchem vermögensrechtlichen Verhältnis der Täter zu der betroffenen Datenverarbeitung steht. Strittig ist hierbei, inwieweit vertretungsberechtigte Organe eines Betriebs als fremd anzusehen sind. Nach einer strikten Auslegung gelten bereits solche Datenverarbeitungsanlagen und -prozesse als fremd, die zumindest auch zu einem Teil dem Vermögen eines anderen zugerechnet werden müssen.[120] Danach wären lediglich Alleingesellschafter eines Unternehmens und deren vertretungsberechtigte Repräsentanten nicht fremd.[121]

Hinsichtlich der innerbetrieblichen Organisation vor allem von Kapitalgesellschaften ist diese Definition zu eingeschränkt, da dann eine Einwilligung zu Qualitätssicherungsmaßnahmen immer durch die vorgenannte Personengruppe erfolgen müsste. Einem angestellten Geschäftsführer wären wesentliche Handlungsbefugnisse in diesem Bereich genommen. Daher wird teilweise auch die hier eingenommene Sichtweise vertreten, dass der Betrieb auch für diejenigen Personen nicht als fremd zählt, die für diesen handlungsbevollmächtigt sind, beispielsweise angestellte Geschäftsführer einer GmbH.[122]

c) Erhebliche Störung

Zudem müsste eine erhebliche Störung der Datenverarbeitung vorliegen, also eine nicht als unerheblich einzustufende Beeinträchtigung ihres reibungslosen Ablaufs.[123] Für den Sprachdienst im NGN ist zwischen den

[118] *BT-Drs. 16/3656*, S. 13; Schumann 2007, S. 679; krit. Lackner-Kühl 2007, StGB § 303b Rn 2.
[119] MK-Wieck-Noodt 2006, StGB § 303b Rn 7.
[120] Lackner-Kühl 2007, StGB § 303b Rn 2; Schönke/Schröder-Stree 2006, § 303b StGB Rn 6; MK-Wieck-Noodt 2006, § 303b StGB Rn 7.
[121] Lackner-Kühl 2007, StGB § 303b Rn 2.
[122] MK-Wieck-Noodt 2006, StGB § 303b Rn 7; Schönke/Schröder-Stree 2006, StGB § 303b Rn 6.
[123] *BT-Drs. 16/3656*, S. 13.

Signalisierungsdaten und den Audiodaten zu unterscheiden. Während in der Echtzeitkommunikation bereits eine Unterbrechung von 250 ms eines interaktiven Audiodatenstroms als Qualitätseinbuße wahrgenommen wird, sind erst Verzögerungen oder Unterbrechungen im Sekundenbereich als erhebliche Beeinträchtigung anzusehen.

Unabhängig davon ist die Signalisierung zu betrachten, insbesondere im Hinblick auf die Erreichbarkeit von Teilnehmern, die durch die regelmäßige Aktualisierung der Registrierungen sichergestellt wird. In Deutschland weit verbreitet ist die Verwendung des auf IP aufsetzenden *User Datagram Protocols* (UDP[124]) zur Übertragung von SIP-Nachrichten zwischen Teilnehmeranschlüssen und der Vermittlungsstelle. Aufgrund der Eigenschaften von UDP werden die Nachrichten in kurzen Abständen wiederholt, wenn innerhalb einer bestimmten Zeit keine Antwort empfangen worden ist. Rechtzeitiges Senden der Nachrichten zur Auffrischung der Registrierungen stellt sicher, dass auch kurzzeitige Beeinträchtigungen der Übertragung oder der Vermittlungsstelle durch diese Wiederholungen überbrückt werden können, bevor die Registrierung des Teilnehmeranschlusses als fehlgeschlagen abgebrochen wird. Eine erhebliche Störung, die zur Nichterreichbarkeit einzelner Teilnehmer führt, wird daher je nach Konfiguration der beteiligten technischen Komponenten nicht bei Beeinträchtigungen von weniger als einer Minute eintreten.

d) Datenveränderung

Hinsichtlich einer Tathandlung gemäß § 303b Abs. 1 Nr. 1 StGB sei auf die Ausführungen in Abschnitt C.II.5. verwiesen.

e) Übermittlung von Daten

Mit Blick auf DoS-Angriffe wurde § 303b StGB im 41. StrÄndG um die Regelung in Abs. 1 Nr. 2 erweitert.[125] Das Übermitteln von Daten bezieht sich dabei auf das Weiterleiten von Daten vom Rechner des Angreifers (oder ggf. weitere fremde Rechner, über die der Täter die Kontrolle übernommen hat) über ein Rechnernetz auf das zu störende System.[126] Bei der Überlastung von Vermittlungsstellen mittels des Programms `SIPp` werden auf dem Sende-Rechner einfache Spezifikationen für Abfolgen von SIP-Nachrichten erstellt und beim Programmstart von `SIPp` eingelesen. Das Ziel der versendeten Nachrichten ergibt sich aus den Parametern, mit denen `SIPp` gestartet worden ist, und den Angaben in dem

[124] Postel 1980.
[125] Schumann 2007, S. 679; Ernst 2007, S. 2665; Laue 13/2009, S. 7.
[126] BeckOK-Weidemann 2009, StGB § 303b Rn 12.

Szenario. Da die in schneller Folge versendeten Daten ursächlich sind für eine eventuelle Überlastung des Empfängers dieser Nachrichten, erfüllt `SIPp` bei entsprechender Verwendung ohne weiteres das Tatbestandsmerkmal der Beeinträchtigung durch Übermittlung von Daten. Die Absicht wird im Einzelfall als subjektives Tatbestandsmerkmal zu prüfen sein.

f) Vorbereitungshandlungen

Mit § 303c Abs. 5 StGB wird auch die Vorbereitung zur Computersabotage als Straftat gewertet und wie bereits der Tatbestand des § 303a StGB nach der objektivierten Zweckbestimmung des § 202c StGB beurteilt (siehe Abschnitt C.II.4.).

Hinsichtlich des Straftatbestands aus § 303a Abs. 1 StGB wurde in Abschnitt C.II.5. bereits das Vorliegen eines Vorbereitungsdelikts verneint.

Der (ursprüngliche) Hauptzweck des Programms besteht allerdings in dem massenhaften Versenden von SIP-Nachrichten, um eine möglichst hohe Last auf Seiten des Empfängers zu verursachen. Wie bereits in Abschnitt C.II.4. ausgeführt, lässt der Funktionsumfang und die Art der Nutzung allerdings nicht auf eine Missbrauchsabsicht schließen, so dass das Vorliegen einer Vorbereitungshandlung i. S. d. § 303b Abs. 1 StGB im Falle von `SIPp` ebenfalls zu verneinen ist.

7. § 317 StGB: Störung von Telekommunikationsanlagen

Zur Sicherstellung eines grundsätzlich allgemein zugänglichen und funktionierenden Telefonnetzes umfasst § 317 StGB Tathandlungen, die den Betrieb negativ beeinflussen können. Darunter fallen auch die Veränderung von Betriebsanlagen sowie die Beeinträchtigung ihrer Funktionalität.

a) Telekommunikationsanlage

Als wesentliche Komponente eines Teilnehmernetzes im NGN ist eine Vermittlungseinrichtung, an der SIP-Nachrichten zur Registrierung von Teilnehmern entgegengenommen und verarbeitet werden, als Telekommunikationsanlage im Sinne dieser Norm zu betrachten.[127]

[127] Zur weitgefassten Auffassung der Merkmale „Telekommunikationsanlage“ siehe *BT-Drs. 13/8016*, S. 28; Schönke/Schröder-Sternberg-Lieben 2006, StGB § 317 Rn 2/3.

b) Öffentlicher Zweck

Ein öffentlicher Zweck liegt bereits dann vor, wenn der Betrieb der betreffenden Anlage im künftigen Allgemeininteresse liegt.[128] Als Teil des privatisierten Telefonnetzes erfüllt die Vermittlungseinrichtung diese Aufgabe, da viele Nutzer bereits heute nur noch über einen Teilnehmeranschluss im NGN auf der Basis von Voice-over-IP verfügen.

c) Dem Betrieb dienend

Mit der Rolle der betrachteten Vermittlungseinrichtung wird auch bereits deutlich, dass diese einen integralen Bestandteil des Telekommunikationsnetzes ausmacht. Eine Einschränkung des Betriebs ergibt sich nach den Ausführungen zu § 303a StGB in Abschnitt C.II.5. bereits durch eine Überlastung, die eine Aktualisierung der Registrierungsdaten verhindert.

Fraglich ist, ob diese Überlastung auch als Beeinträchtigung im Sinne der Norm zu verstehen ist. Da keine physische Einwirkung vorgenommen wird, liegt keine Zerstörung oder Beschädigung einer Sache vor. Auch Telefonterror wird nicht als Tathandlung i. S. d. § 317 StGB angesehen, während eine Blockade eines Servers durch das Versenden unerwünschter Massen-Mails teilweise schon als solche aufgefasst wird.[129]

Aufgrund des öffentlichen Interesses an der Funktionsfähigkeit des Telefonnetzes reiche jedoch die konkrete Gefahr einer Störung des Betriebs bereits aus. Ein Eingriff in die physische Substanz der Anlage ist nicht erforderlich.[130] Damit erfüllt ein DoS-Angriff vermöge `SIPp` folglich auch den objektiven Tatbestand des § 317 StGB.

III. Zusammenfassung

In diesem Kapitel wurde untersucht, inwieweit der Einsatz einer um die Funktion des IP-Spoofing erweiterten Programms `SIPp` zur Erzeugung massenhafter SIP-Nachrichten und deren Versand an eine nahegelegene Vermittlungseinrichtung die objektiven Tatbestände einschlägiger Strafrechtsnormen erfüllt. Vorrangig wurden dabei die mit dem 41. StrÄndG

[128] *BT-Drs. 13/8016*, S. 28; Schönke/Schröder-Sternberg-Lieben 2006, StGB § 317 Rn 4.

[129] Schönke/Schröder-Sternberg-Lieben 2006, StGB § 317 Rn 2/3; Lackner-Kühl 2007, StGB § 317 Rn 3.

[130] BeckOK-Valerius 2009, StGB § 317 Rn 4 m. w. N.

neu aufgenommenen Straftatbestände zur Bekämpfung von Computerkriminalität betrachtet und die einschlägigen Normen diskutiert, die vor dieser Strafrechtsnovelle von der Rechtsprechung und in der Literatur zur Beurteilung von strafrechtlich relevanten Tatsachen herangezogen wurden.

Im Vordergrund stand dabei die Frage nach der grundsätzlichen Deliktswürdigkeit vor dem Hintergrund der Ausgangsfrage. Auf Konkurrenzen und die für manche Tatbestände erforderliche Strafantragserfordernis wurde bewusst nicht eingegangen.

Ein besonderer Schwerpunkt lag ferner auf der Untersuchung der Strafwürdigkeit der Erweiterung von `SIPp` um eine Funktion zur Verwendung beliebiger Absenderadressen (IP-Spoofing) und deren Veröffentlichung als Open Source Software. Spätestens mit dieser Funktion fällt das Programm in die Klasse der Dual-Use-Tools, die auch für schädliche Zwecke eingesetzt werden können. Vor dem Hintergrund der Änderungen im Zuge der Strafrechtsnovelle durch das 41. StrÄndG war daher vor allem die Frage nach der Strafbarkeit der Entwicklung, Weitergabe und Sichverschaffens als Vorbereitungshandlung zu beurteilen.

Im Ergebnis zeigte sich, dass die vielgestaltige Kritik an den neuen Vorschriften zur Bekämpfung von Computerkriminalität vor allem hinsichtlich einer Vorfeldkriminalisierung der Verwendung und Entwicklung von Dual-Use-Tools unbegründet gewesen ist. Als Software stellt ein Programm wie `SIPp` nach objektivierter Zweckbestimmung kein Hackertool dar und kann somit im Rahmen eines Open-Source-Projekts legal veröffentlicht werden. Selbst die Erweiterung um eine Funktion zum IP-Spoofing für breit angelegte Belastungstests von Telekommunikationseinrichtungen ändert diese Einschätzung nicht.

Dennoch besteht gerade in vielen Open-Source-Projekten weiterhin große Unsicherheit über die rechtliche Einordnung der entwickelten Software. Vor allem im gewerblichen Bereich ist daher eine genaue Kenntnis der strafrechtlichen Verantwortung jedes Einzelnen für die Wahrung des Rechtsfriedens unverzichtbar. Im folgenden Kapitel wird daher ein Blick auf den potentiellen Täterkreis innerhalb einer Unternehmenshierarchie geworfen und eine potentielle Beteiligung an deliktswürdigen Handlungen diskutiert.

D. Verantwortlichkeit bei der Entwicklung von Qualitätssicherungswerkzeugen

Nachdem zuvor der Einsatz von `SIPp` für die Qualitätsprüfung von Telekommunikationseinrichtungen hinsichtlich der objektiven Tatbestände einschlägiger Strafrechtsnormen bewertet worden ist, soll darauf aufbauend ein Blick auf den beteiligten Personenkreis im Unternehmen geworfen werden. Der Schwerpunkt der Betrachtung liegt dabei auf der Tatherrschaft für die im vorherigen Kapitel diskutierten Tatbestände. Wie gezeigt, ist bei der Entwicklung und dem tatsächlichen Einsatz von Dual-Use-Software besondere Sorgfalt bei der Beurteilung der Außenwirkung dieser Tätigkeiten erforderlich.

Die Beteiligung eines Anbieters von Telekommunikationsdienstleistungen an Open-Source-Projekten bringt daher weitere Verantwortung hinsichtlich des Einsatzes und der Weitergabe solcher Werkzeuge mit sich. Mit der in Abschnitt C.II.4. diskutierten Ausgestaltung der gesetzlich geforderten objektivierten Zweckbestimmung, nach der die Unterscheidung zwischen legaler Software und schädlichen Hackertools bereits Teil des objektiven Tatbestands ist, hat sich die anfängliche Unsicherheit vieler Rechtsanwender mittlerweile gelegt. Dennoch ist es notwendig, die zugrunde gelegten Kriterien auch innerhalb der Unternehmenshierarchie zu kommunizieren und so Rechtssicherheit bei der Beteiligung an Open-Source-Projekten zu gewinnen.

Die folgende Betrachtung zeigt daher individuelle Verantwortlichkeiten innerhalb der Organisationsstruktur eines Unternehmens auf. Die Ausführungen beschränken sich dabei auf eine für kleine und mittlere Unternehmen typische Rollenverteilung zwischen ausführenden Fachkräften, Kontrollinstanzen und Mitarbeitern mit Weisungsbefugnis. Die Hauptverantwortung für das Unternehmen liegt schließlich bei der Unternehmensführung bzw. Inhabern. Im Vordergrund steht dabei die Kapitalgesellschaft als vorherrschende Gesellschaftsform im I&K-Bereich.

Für eine eindeutige Beurteilung der persönlichen Verantwortung ist zunächst einmal wichtig, die Rollen der Beteiligten zu untersuchen. Da das deutsche Strafrecht an individuelles Verschulden einer natürlichen Person während einer aktiven Handlung anknüpft, ist das Unternehmen als juristische Person nicht strafbar,[131] jedoch sieht § 14 StGB eine Zurechnung von tatbestandserheblichen persönlichen Merkmalen und Handlungen einer juristischen Person zu den jeweils bestellten Vertretern vor.

I. Softwareentwickler

An der Herstellung von Computerprogrammen sind in erster Linie Softwareentwickler aktiv beteiligt. Eine Vorbereitung einer Straftat i. S. d. § 303a Abs. 3 StGB bzw. § 303b Abs. 5 StGB jeweils i. V. m. § 202c Abs. 1 Nr. 2, Abs. 1 1. Alt StGB liegt nach den Ausführungen in Kapitel C. objektiv bereits dann vor, wenn ein bestehendes Programm derart abgeändert wird, dass es nach objektivierter Zweckbestimmung auch illegalen Zwecken dienen kann.[132]

Die Tätigkeit eines Programmierers bei der Softwareentwicklung kann ohne weiteres als aktives Tun angesehen werden, denn ohne dessen Handlung würden die fraglichen Programmfunktionen nicht realisiert, und es käme in der Folge nicht zu einer Gefährdung von Datenverarbeitungsanlagen durch Einsatz des Programms.

Dem jeweiligen Programmierer einer potentiellen Schadroutine müsste bei Vorliegen einer durch die Software objektiv manifestierten Schädigungsabsicht im konkreten Einzelfall allerdings auch Vorsatz nachgewiesen werden.[133] Zu unterscheiden ist hier zwischen angestellten Programmierern, die in eine Unternehmenshierarchie eingebunden sind und aufgrund ihrer Weisungsgebundenheit als Arbeitnehmer angesehen werden, und den in der Softwareentwicklung häufig anzutreffenden freien Mitarbeitern, die zumindest hinsichtlich ihrer zeitlichen und örtlichen Ausgestaltung der Arbeitsbedingungen nicht unmittelbar den Weisungen ihres Auftraggebers unterworfen sind.[134]

[131] Wabnitz/Janovsky-Raum 2007, Kap. 4 Rn 2; MK-Joecks 2003, StGB § 25 Rn. 16.
[132] Ernst 2007, S. 2663.
[133] BeckOK-Weidemann 2009, StGB § 202c Rn 9 m. w. N.; BVerfG 2 BvR 2233/07 = ZUM 2009, 745.
[134] Vgl. ErfK-Koch 2010, BetrVG § 5 Rn. 18–22; Hromadka 2003, S. 1848; Moll-Reiserer 2009, Rn. 7; BAG 5 AZR 644/98 = NZA 2000, 1102, S. 1102.

1. Entwickler im Angestelltenverhältnis

Kommt ein Softwareentwickler als persönlich abhängiger Arbeitnehmer lediglich seiner vertraglich geschuldeten Hauptpflicht nach, ist regelmäßig nicht von dolus directus auszugehen. Ein Eventualvorsatz (dolus eventualis) könnte jedoch darin bestehen, dass ein Programmierer sehr wohl um die Gefährlichkeit der von ihm entwickelten Software weiß, da er ausdrücklich wegen seines Spezialwissens mit der betreffenden Entwicklungsaufgabe betraut worden ist. Dazu müsste der Entwickler jedoch nicht nur die Eignung seines Programms zur Verwirklichung einer Straftat ernstlich für möglich halten, sondern den Taterfolg auch billigend in Kauf nehmen.[135]

Bezogen auf die Vorbereitung einer Straftat im Zusammenhang mit den in Abschnitt C.II. aufgezeigten Tatbeständen nach §§ 202a, 202b StGB und §§ 303a, 303b StGB (jeweils i. V. m. § 202c StGB) müsste also in der Handlung des Programmierers ein deliktförderndes Verhalten vorliegen.[136] Seine Entwicklungstätigkeit bezieht sich aber gerade auf die Herstellung von Werkzeugen für die legale Verwendung, soweit die Qualitätssicherungsmaßnahmen im eigenen Betrieb durchgeführt werden. Da in diesem Fall das Unternehmen sowohl Betreiber der betroffenen Datenverarbeitungssysteme ist als auch Auftraggeber der Programmentwicklung, ist regelmäßig von einem Vorliegen des erforderlichen Einverständnisses auszugehen. Mangels Täterwillens scheidet auch eine Mittäterschaft nach § 25 Abs. 1 Nr. 2 StGB mit weiteren Tatbeteiligten – etwa der Unternehmensleitung (s. u.) aus.[137] Aufgrund der Weisungsgebundenheit des Mitarbeiters ist ggf. auch an Beihilfe zu denken. Dazu müsste der Softwareentwickler nach dem Wortlaut des § 27 Abs. 1 StGB allerdings vorsätzlich handeln, was zuvor bereits verneint worden ist. Für die Behandlung von berufstypischen Handlungen stellt der BGH stellt für die Beurteilung von Beihilfehandlungen auf die Kenntnis des Gehilfen von der Handlung des Haupttäters ab.[138] Danach würde der Entwickler zum Tatgehilfen, wenn er positive Kenntnis von einer geplanten Nutzung des von ihm entwickelten Programms zur (versuchten) Ausführung einer Straftat hätte. Ein Erkennen der bloßen Möglichkeit, dass sein Arbeitsergebnis zum Begehen einer Straftat genutzt werden könnte, reiche hingegen aus.[139]

[135] Ständige Rechtsprechung, statt vieler: BGHSt 36,1 = NJW 1989, 781, S. 783.
[136] Popp 2007, S. 87.
[137] MK-Joecks 2003, StGB § 25 Rn. 169, 203.
[138] MK-Joecks 2003, StGB § 27 Rn. 47.
[139] MK-Joecks 2003, StGB § 27 Rn. 47.

2. Freier Mitarbeiter

Für die Beurteilung der Tatherrschaft bei einem freien Mitarbeiter ist zu prüfen, inwieweit eine fachliche Weisungsbindung durch den Auftraggeber vorliegt. Dies wird vorwiegend bei einer Auftragsentwicklung auf der Basis eines Dienstvertrags der Fall sein. Hier wird vornehmlich Art und Umfang der zu leistenden Arbeit festgelegt, während die herzustellende Software in ihrer Funktion nur grob umrissen wird. Genauere Festlegungen und Spezifikationen erfolgen dann im Rahmen der vertraglich vereinbarten Tätigkeiten unter Weisung des Auftraggebers.

Die Tatherrschaft liegt bei dieser Konstellation kraft Organisationsherrschaft wiederum beim Auftraggeber, der vom Auftragnehmer lediglich berufstypische Handlungen einfordert. Eine strafrechtliche Andersbehandlung zwischen freiem Mitarbeiter und Arbeitnehmer ist daher im Falle eines Dienstvertrages abzulehnen.

Kritischer zu beurteilen ist die Sachlage bei einer freien Mitarbeit auf der Basis eines Werkvertrags. Hier ist regelmäßig davon auszugehen, dass eine detaillierte inhaltliche Ausgestaltung des zu liefernden Arbeitsergebnisses bereits Teil des Vertragsdokuments ist. Beide Parteien können daher schon vor Vertragsschluss die Deliktwürdigkeit der zu entwickelnden Software weitgehend einschätzen.

Problematisch ist hier wiederum die Abgrenzung zwischen der gutgläubigen Herstellung und Verbreitung eines Dual-Use-Tools zu legalen Zwecken und der fahrlässigen Herstellung und Verbreitung von Software, die in objektiven Tatbeständen aus Kapitel C. entspricht. Die Gutgläubigkeit des Auftragnehmers ist vor allem aufgrund der Entfernung zum Auftraggeber denkbar. Ein vorsatzausschließender Tatbestandsirrtum gemäß § 16 Abs. 1 Satz 1 StGB läge etwa vor, wenn der Auftraggeber den Eindruck erweckt, er wolle lediglich seine eigene im Testbetrieb befindliche Telekommunikationsanlage einer Qualitätsprüfung unterziehen, insgeheim aber auf die Vermittlungsanlage eines Mitbewerbers abzielt.

Besitzt der Auftragnehmer hingegen positive Kenntnis von der sozialschädlichen Gesinnung des Auftraggebers, so handelt er bei der Herstellung der Software im Wissen um die Gefahr, die von dem entwickelten Produkt ausgeht. Er handelt folglich bedingt vorsätzlich, da er den Taterfolg nicht nur für möglich hält, sondern diesen auch billigend in Kauf nimmt, und macht sich somit der Vorbereitung einer Straftat schuldig.

II. Tester und Qualitätssicherungsbeauftragte

Eine wichtige Funktion innerhalb der Unternehmenshierarchie nimmt die Qualitätssicherung ein, da sie das reibungslose Funktionieren der betriebenen Anlagen sicherstellen soll. Da die Aufgaben der Qualitätssicherung regelmäßig nicht die Herstellung der Prüfsoftware umfassen, trifft hier höchstens das Sichverschaffen i. S. d. § 202c Abs. 1 Nr. 2 StGB zu. Tatbestandmäßig ist allerdings nur Software, die bereits mit der Absicht entwickelt oder modifiziert worden ist, eine strafbare Handlung im Sinne der einschlägigen Normen zur Bekämpfung der Computerkriminalität zu begehen.[140]

Da es sich bei der Vorbereitungshandlung um ein eigenständiges Delikt handelt, kommen Tester und Qualitätssicherungsbeauftragte in dieser Hinsicht auch als Täter in Frage. Bei der Prüfung des subjektiven Tatbestands ist wiederum auf Eventualvorsatz abzustellen.[141] Als Angestellte des Unternehmens führt die hier betrachtete Personengruppe ähnlich wie Softwareentwickler lediglich berufstypische Handlungen im Rahmen ihrer weisungsgebundenen Tätigkeit aus. Insoweit ist bei Einhaltung der gebotenen üblichen Sorgfalt im Rahmen ihrer Tätigkeit ein (bedingter) Vorsatz zur Ausführung einer strafbaren Handlung regelmäßig zu verneinen.

Eng verbunden mit der ausgeübten Tätigkeit ist auch die Durchführung der Lasttests mit Werkzeugen wie dem erweiterten `SIPp`, wodurch die Testbeauftragten unmittelbar an der Tathandlung beteiligt sind. Mit dem Starten des Programms beschränkt sich die deliktspezifische Handlung folglich nicht mehr allein auf die Vorbereitung einer Straftat gemäß § 202c StGB i. V. m. §§ 303b, Abs. 5, 303a Abs. 3 StGB, sondern erfüllt potentiell die in Kapitel C. diskutierten Straftatbestände der (versuchten) Fälschung beweiserheblicher Daten (§ 269 StGB), der Täuschung im Rechtsverkehr (§ 270 StGB), (versuchter) Nötigung (§ 240 StGB), (versuchter) Datenveränderung (§ 303a StGB), (versuchter) Computersabotage (§ 303b StGB) oder der (versuchten) Störung von Telekommunikationsanlagen (§ 317 StGB).

Dabei ist wiederum auf den Tatvorsatz abzustellen, für den im Allgemeinen die gleichen Beobachtungen hinsichtlich der Ausführung beruflicher Tätigkeiten gelten.

[140] BeckRS 2009, S. 457.
[141] BeckOK-Weidemann 2009, StGB § 202c Rn 9 m. w. N.

III. Weisungsbefugte Mitarbeiter unterhalb der Leitungsebene

Innerhalb der Verantwortungskette zwischen der Führungsebene und dem Fachpersonal nimmt die Bereichs- und Abteilungsleiterebene eine Mittlerposition ein. Sie sind regelmäßig im Rahmen ihres Aufgabengebiets weisungsbefugt gegenüber der untergeordneten Hierarchieebene. Innerhalb dieser Organisationsstruktur tragen die Mitarbeiter Verantwortung für eine sorgfältige und gewissenhafte Ausführung der übertragenen Arbeiten sowie für die Einhaltung der gebotenen Sicherheitsstandards. Sie sind in ihrem Aufgabenbereich zuständig für die Auswahl geeigneter Mitarbeiter, deren sorgfältige Anleitung sowie eine hinreichende Beaufsichtigung.

Gemäß § 14 Abs. 2 Nr. 2 StGB sind grundsätzlich auch auf diese Mitarbeiter eines Unternehmens die persönlichen Merkmale des Inhabers oder dem zur Übertragung von Aufgaben Befugten anzuwenden, die sonst beim Inhaber vorliegen würden.[142] Nach dem Gesetzeswortlaut stehen damit auch solche Mitarbeiter einer hierarchischen Organisation in der Verantwortung für auftragsbezogene Entscheidungen der Betriebsleitung, die sich eher am unteren Ende dieser Hierarchie befinden. Für diese Personengruppe mit sehr eng begrenztem Verantwortungsbereich und geringem Einfluss auf unternehmerische Entscheidungen ist diese Norm regelmäßig nicht einschlägig.[143]

Daneben kann teilweise eine Schuld kraft Organisationsherrschaft ausgeschlossen werden. Dazu ist nach einer Entscheidung des BGH im Rahmen der Mauerschützenprozesse eine hinreichende Organisationstiefe erforderlich, aus der sich eine Austauschbarkeit der Tatmittler ergibt.[144] Danach müsste der Handlungserfolg auch dann erzielt werden, wenn statt des beauftragten Mitarbeiters eine beliebige andere Person an derselben Stelle der Organisationshierarchie den rechtswidrigen Entschluss umgesetzt hätte.

Umstritten ist eine Anwendbarkeit dieser Rechtsfigur auf andere Organisationsstrukturen mit dem Argument, in einer rechtmäßigen Organisation könne der Vollzug einer Straftat dem Hintermann überhaupt nicht

[142] Schönke/Schröder-Perron 2006, StGB § 14 Rn 38; Wabnitz/Janovsky-Raum 2007, Kap. 4 Rn 12.
[143] Schönke/Schröder-Lenckner 2006, StGB § 14 Rn 32.
[144] Jakobs 1995, S. 27.

garantiert werden.[145] Vertreter der gegenteiligen Auffassung – darunter der BGH – wollen im Kampf gegen die Wirtschaftskriminalität bei einer hinreichend engen Auslegung die Anwendung auf komplexe Organisationsstrukturen von Wirtschaftsunternehmen zulassen.[146]

Vor dem Hintergrund des Einsatzes und der Weiterentwicklung von Dual-Use-Tools im Rahmen von Open-Source-Projekten ist der zuletzt verbreiteteren Haltung der Vorzug zu geben. Insbesondere stellt die aktive Beteiligung an entsprechenden Open-Source-Projekten eine strategische Entscheidung auf der Leitungsebene dar, deren Tragweite über den Aufgabenbereich des einzelnen Mitarbeiters in der Organisationsstruktur weit hinausgeht. So ist vor allem die Zweckbestimmung nach objektiven Kriterien dem Einzelnen oft nicht möglich, so dass eine Strafbarkeit nach § 202c StGB unter diesen Umständen nicht angemessen erscheint.

Ungeachtet dessen steht es natürlich in der Verantwortung jedes Betriebsangehörigen, die Allgemeinheit vor Gefahren zu bewahren, die durch ihre Tätigkeit in dem Unternehmen entstehen könnten. Dazu gehört insbesondere Pflicht zur Sorgfalt und die Beaufsichtigung delegierter Aufgaben.

IV. Leitende Angestellte und Inhaber

Wie zuvor erläutert worden ist, sind Tathandlungen weisungsgebundener Angestellter nicht vorsätzlich begangen, soweit sie im Rahmen der übertragenen berufstypischen Aufgaben erfolgt sind. Eine Strafbarkeit liegt in diesen Fällen nur bei einem Ausführungs- oder Übernahmeverschulden vor, auf der Seite des Weisungsberechtigten ist an Auswahlverschulden, Instruktionsverschulden oder gar Beaufsichtigungsverschulden zu denken.

Unabhängig davon befindet sich am Ende der Verantwortungskette die Betriebsleitung, insbesondere der Inhaber und dessen rechtmäßige Vertreter. Neben der persönlichen Strafbarkeit aus Jedermannsdelikten sowie aus Sonderdelikten, die sich unmittelbar aus dem Nebenstrafrecht ergeben, müssen sich vertretungsberechtigte Angehörige juristischer Personen gemäß § 14 Abs. 1 StGB auch straftatbegründende Eigenschaften

[145] Fleischer-Spindler, § 15 Rn 92–93, 126.

[146] Wabnitz/Janovsky-Raum 2007, Kap. 4 Rn 60–61; BeckOK-Kudlich 2009, StGB § 25 Rn 34 m. w. N.; BGHSt 5 StR 98/94 = NJW 1994, 2703, S. 2706 m. w. N.

zurechnen lassen, wenn die juristische Person selbst Normadressat ist.[147] Gleiches gilt nach § 14 Abs. 2 StGB für leitende Angestellte, soweit sie innerhalb ihrer Befugnis und aufgrund der ihnen übertragenen Aufgaben handeln.

Bedeutsam wird diese Zurechnung persönlicher Merkmale insbesondere im Hinblick auf die Vorbereitung einer Straftat i. S. d. § 202c StGB, wenn es um die objektivierte Zweckbestimmung bei der Entwicklung und Weitergabe von Open Source Software geht. Dort, wo zur Zweckbestimmung neben rein objektiven Kriterien wie der Gestaltung oder Funktionalität von Programmen die persönliche Verwendungsabsicht herangezogen wird, ist nach h. M. zumindest auch auf das Unternehmen und seine Produktwerbung abzustellen.[148] Damit wird der subjektive Anteil der Zweckbestimmung gerade in Kapitalgesellschaften weitgehend durch die Führungsebene bestimmt, so dass diese kraft Organstellung bzw. der ihr übertragenen Aufgaben für die legale Ausrichtung der hergestellten und vertriebenen Software verantwortlich ist.

Für Betreiber von Sprachdiensten ergibt sich außerdem eine besondere Verantwortung der Betriebsleitung gegenüber der Allgemeinheit aus dem öffentlichen Interesse an der Funktionsfähigkeit des Telefonnetzes[149]. Dabei ist jedoch fraglich, inwieweit dies eine Verschärfung der bestehenden Pflichten bewirkt. So hat der BGH im Lederspray-Fall auf strafrechtlich bedeutsame Pflichten hingewiesen, die sich aus pflichtwidrigem Vorverhalten ergeben können. Demnach kann sich eine strafrechtliche Schadensabwendungspflicht bereits aus der zivilrechtlich bestehenden Verkehrssicherungspflicht ergeben.[150]

Zu beachten ist jedoch, dass der BGH hier vor allem für gefährliche Güter eine Parallele zur Produkthaftung schaffen wollte. Eine daraus grundsätzlich aus der zivilrechtlichen Verkehrssicherungspflicht erwachsende Garantenstellung wird in der Literatur mangels pflichtwidrigen Vorverhaltens jedoch zurecht abgelehnt.[151]

---

[147] Fleischer-Spindler, § 15 Rn 3–4; Wabnitz/Janovsky-Raum 2007, Kap. 4 Rn 6–10.

[148] OLG München 29 – U 2887/05 = ZUM 2005, 896, S. 898 f.; Leupold/Glossner-Cornelius 2008, Teil 8 Rn 88; BeckOK-Weidemann 2009, StGB § 202c Rn 7.2; BeckRS 2009; mit krit. Anm. LG München I – 21 O 3220/05 = MMR 2005, 385, S. 386.

[149] Vgl. *BT-Drs. 13/8016*, S. 28; Schönke/Schröder-Sternberg-Lieben 2006, StGB § 317 Rn 4.

[150] BGH 2 StR 549/89 (LG Mainz) = NJW 1990, 2560, S. 2562 f., m. w. N.

[151] Fleischer-Spindler, § 13 Rn 48; Schönke/Schröder-Stree 2006, StGB § 13 Rn 32, 37 m. w. N.; BGH 4 StR 179/91 (LG Saarbrücken) = NStZ 1991, 490, S. 490.

Die strafrechtliche Haftung trifft somit für die in Kapitel C. aufgeführten Tatbestände in erster Linie den jeweiligen Verursacher. Entsprechend der Unternehmenshierarchie sind weisungsbefugte Mitarbeiter im Rahmen der üblichen Sorgfaltspflicht und abhängig von ihren persönlichen Fähigkeiten und Kenntnissen haftbar. Dies gilt grundsätzlich genauso für die Leitungsebene eines Unternehmens, wobei die aus der Organstellung abgeleitete Allzuständigkeit eine Haftungserweiterung im Rahmen der betrieblichen Organisation begründet.

Bedeutsam wird dies für Organwalter vor allem bei Kollegialentscheidungen, die zu einer Mittäterschaft nach § 25 Abs. 2 StGB führen können.[152] Führt eine mehrheitlich getroffene Entscheidung eines Gesamtorgans also zu strafbarem Verhalten der juristischen Person, so haben grundsätzlich alle beteiligten Organmitglieder dafür einzustehen. Schuldfreiheit kommt im Einzelfall in Betracht, wenn von dem Beteiligten nachgewiesen werden kann, dass er den Beschluss nicht mitgetragen hat.[153]

Abschließend sei schließlich auf die mit dem 41. StrÄndG erfolgte Änderung des Gesetzes über Ordnungswidrigkeiten (OWiG[154]) hingewiesen. Die Abänderung des § 130 Abs. 1 Satz 1 OWiG soll vor dem Hintergrund der §§ 202a, 202b, 202c, 303a und 303b StGB die Verantwortlichkeit eines Betriebsinhabers für tatbestandsmäßige Handlungen der unterstellten Mitarbeiter klarstellen, soweit diese im Rahmen ihrer Befugnisse gehandelt haben und zusätzlich eine Aufsichtspflichtverletzung vorlag.[155]

Mit dieser Änderung unterstreicht der Gesetzgeber die aus der Eröffnung eines Betriebs abgeleitete Verantwortung des Inhabers für das gesetzeskonforme Wohlverhalten seiner Angestellten im Rahmen ihrer betrieblichen Aufgaben.[156] Die geäußerte Kritik an dieser Tendenz zielt vor allem auf die Entwicklung moderner Organisationsformen, in denen sich eine strikt hierarchisch organisierte Struktur als nicht effizient erwiesen hat.[157] Werden beispielsweise Entscheidungsbefugnisse einem gesamten Entwicklungsteam übertragen, ohne zuvor klare Zuständigkeiten und Verantwortungsbereiche abzugrenzen und diese in geeigneter Weise zu kon-

[152] Wabnitz/Janovsky-Raum 2007, Kap. 4 Rn 29; MK-Joecks 2003, StGB § 25 Rn 211; BGH 2 StR 549/89 (LG Mainz) = NJW 1990, 2560.

[153] Wabnitz/Janovsky-Raum 2007, Kap. 4 Rn 31.

[154] *BGBl. I Nr. 15 vom 25.02.1987, 602–629*, zuletzt geändert durch Art. 2 G. v. 29.07.2009, *BGBl. I Nr. 49 vom 3.08.2009, 2353–2354*.

[155] *BT-Drs. 16/3656*, S. 16; *BR-Drs. 676/06*, S. 8.

[156] OLG Jena – 1 Ss 242/05 = NStZ 2006, 533, S. 534; Többens 1999, S. 3; krit. Fleischer-Spindler, § 15 Rn 92.

[157] Fleischer-Spindler, § 15 Rn 120.

trollieren, so bedeutet dies automatisch eine Verletzung der Aufsichtspflicht, mithin einen Organisationsmangel.

Zur Stärkung solcher flexibler Organisationsformen wird in der Literatur die Anwendung des § 30 OWiG ohne Bezugnahme auf individuelle Pflichtverletzungen im Unternehmen vorgeschlagen.[158] Dieser Sichtweise ist allerdings nicht uneingeschränkt zu folgen, da die juristische Person als Normadressat ansonsten unter Umständen für rechtswidrige Handlungen von Angestellten einzustehen hätte, die nicht im Rahmen ihrer betrieblichen Aufgaben durchgeführt worden sind. Hier wäre wiederum eine Parallelbehandlung von Straftat und Ordnungswidrigkeit vorzuziehen.

V. Zusammenfassung

In diesem Kapitel wurde die Unternehmensorganisation näher auf potentielle Strafbarkeitsrisiken untersucht, die mit einer Beteiligung an der Nutzung und Weiterentwicklung von Dual-Use-Tools im Rahmen von Open-Source-Projekten entstehen können. Die aus der Betriebseröffnung hergeleitete Allgemeinzuständigkeit des Unternehmensinhabers für alle von seinem Betrieb ausgehenden Gefahren erfordert eine sorgfältige Planung und Umsetzung organisatorischer Vorkehrungen, um Pflichtverletzungen innerhalb des Unternehmens frühzeitig erkennen zu können und entsprechende Gegenmaßnahmen für die Zukunft zu entwickeln.

Anhand der wesentlichen Personengruppen, die unmittelbar für die Entwicklung von Software zuständig sind und diese auch zu betriebsspezifischen Zwecken innerhalb des Unternehmens einsetzen, wurden konkrete Strafbarkeitsrisiken am Beispiel eines modifizierten Programms zur Qualitätsprüfung von Telekommunikationseinrichtungen im NGN gezeigt. Dabei wurde deutlich, dass gerade die objektivierte Zweckbestimmung zur Beurteilung einer Handlung vor dem objektiven Tatbestand des § 202c StGB hohe Anforderungen an die Instruktion und Beaufsichtigung weisungsgebundener Mitarbeiter stellt. Denn die Absicht der Programmentwicklung ist Teil der Unternehmensstrategie und somit nicht ohne weiteres bis in die untersten Ebenen der Organisationsstruktur ersichtlich. Die Aufklärung über den bezweckten Einsatz der Dual-Use-Software und eine deutliche Klarstellung unerlaubter Aktivitäten hilft somit der proaktiven Gefahrenabwehr und stellt somit einen wesentlichen Baustein der Sicherheitsorganisation dar.

[158] Fleischer-Spindler, § 15 Rn 96.

E. Fazit

Freie Software und Open Source haben vor allem im Bereich kleiner und mittlerer Unternehmen der Internetwirtschaft Kostenvorteile gebracht oder den Markteintritt sogar erst ermöglicht. Nach der Öffnung des Telekommunikationsmarkts für Sprachdienste und der beginnenden Umstellung aller Teilnehmernetzbetreiber auf VoIP-Technologien hat sich außerdem ein vielgestaltiger Markt für Dienstleistungen und Produkte rund um das Next Generation Network (NGN) entwickelt.

Eine unerwünschte Folge der technischen Entwicklung und der damit zusammenhängenden zunehmenden wirtschaftlichen Nutzung des Internets ist jedoch die gleichzeitig rasant steigende Computerkriminalität. Einige Delikte, wie etwa der Computerbetrug, erfahren dabei im wesentlichen eine Verlegung des Tatorts – etwa vom Bankautomaten an der Ecke auf einen entfernten Server einer Bank. Andere Tatbestände wie etwa die „Online-Demonstration“ sind hingegen neu und waren somit lange Zeit nur schwer in das bestehende Normenwerk des Strafgesetzbuchs einzuordnen.

Besonders bedenklich erschien dabei vor allem auch die Leichtigkeit, mit der selbst technisch mittelmäßig begabte Jugendliche mit entsprechenden im Internet erhältlichen Werkzeugen Schadprogramme erzeugen und in Umlauf bringen konnten. Um den Zugang zu diesen Programmsammlungen zu erschweren, wurde mit dem 41. StrÄndG unter anderem ein neuer Vorbereitungstatbestand in das Strafgesetzbuch aufgenommen, nach dem die Herstellung und Weitergabe solcher „Hackertools“ strafbar ist. Wesentliches Merkmal zur Abgrenzung von Dual-Use-Tools, die unter anderem auch für die unter Strafe gestellten Handlungen eingesetzt werden können, ist die Absicht, in der das betreffende Programm entwickelt, beschafft, weitergegeben oder sonstwie zugänglich gemacht wurde. Als Instrument hat sich die objektivierte Zweckbestimmung herauskristallisiert, also eine Betrachtung der Gesamtumstände, unter denen diese Tathandlungen ausgeführt worden sind.

Als Folge der neuen Gesetzeslage ist der Entschluss zur Verwendung und ggf. Weiterentwicklung und Veröffentlichung von Open Source Software im eigenen Unternehmen auch auf die Risiken einer Strafbarkeit aus § 202c StGB zu bewerten. Anhand eines Anwendungsbeispiels aus dem Bereich der Telekommunikation wurden in dieser Arbeit Kriterien für eine solche Bewertung aufgezeigt und mögliche strafbare Handlungen einzelner Funktionsträger in einem typischen mittelständischen Unternehmen identifiziert. Dabei hat sich gezeigt, dass es der Betriebsleitung obliegt, eine geeignete Sicherheitsorganisation auch dann vorzusehen, wenn der objektive Tatbestand des § 202c StGB (noch) nicht erfüllt ist.

An die Unternehmensorganisation stellt dies hohe Anforderungen, da stärker als zuvor ein gesamtverantwortliches Handeln gefordert ist. Zu den bereits bestehenden Pflichten des Inhabers[159] hinsichtlich Personalauswahl, Leitung des Personals, transparenter Aufgabenverteilung und gewissenhafter Kontrolle der Einhaltung von Vorschriften, tritt nun die sachgerechte Dokumentation der hergestellten oder eingesetzten Software hinsichtlich ihres objektiven Zwecks. Im Zusammenhang damit sollten die mit dieser Software befassten Mitarbeiter frühzeitig über ihre Aufgaben und Pflichten – vor allem im Hinblick auf die Gefahrenabwehr – hingewiesen werden. Ferner sollte eine lückenlose Dokumentation der Anforderungen an die zu entwickelnde Software, der geforderten Funktionalität, ihres Einsatzzwecks, und ggf. einer geplanten Veröffentlichung im Rahmen von Open-Source-Projekten angefertigt werden, um bereits in frühen Planungsphasen den Einsatzzweck zu dokumentieren. Ausführliche Testdokumentationen bei der Qualitätssicherung sowie die Dokumentation des tatsächlichen Einsatzes können ebenfalls als Beleg legaler Anwendungszwecke dienen.

Im Ergebnis manifestiert § 202c StGB und dessen Auslegung die gesellschaftliche Tendenz, Unternehmern als Teile der Gesellschaft mehr gesamtverantwortliches Handeln abzuverlangen. Während Großunternehmen dies bereits mit der Einrichtung einer Compliance-Organisation umsetzen, besteht hier für mittelständische Unternehmen noch Aufholbedarf. Für kleine und Kleinstunternehmen ist jedoch davon auszugehen, dass die Distanz zwischen Inhaber und Fachpersonal gering genug ist, um auch ohne einen komplexen Überbau eine hinreichende Sicherheitsorganisation gewährleisten zu können.

[159] Vgl. Többens 1999, S. 4; Fleischer-Spindler, § 15 Rn 105.

Literaturverzeichnis

AKNN, Konzept für die Zusammenschaltung von Next Generation Networks, Version 2.0.0, Stand 31.03.2009, hg. v. Arbeitskreis für technische und betriebliche Fragen der Nummerierung und Netzzusammenschaltung – Unterarbeitskreis Next Generation Networks (UAK-NGN), März 2009, URL: http://aknn.de/fileadmin/uploads/oeffentlich/Konzept_Next_Generation_Network_V_2_0_0.pdf (besucht am 08. 12. 2009).

Altvater, G., Gewaltbegriff der Nötigung, in: NStZ 6 1995, Anmerkung zu BVerfG, Beschluss vom 10.01.1995 – 1 BvR 718/89, 1 BvR 719/89, 1 BvR 722/89, 1 BvR 723/89 = NVwZ 1995, 576 = NJW 1995, 1141, S. 275–282.

Ayuso, Pablo Neira, Netfilter's Connection Tracking System, in: LOGIN: The USENIX magazine 31.3 2006, S. 34–39.

Baumann, Jürgen, Demonstrationsziel als Bewertungsposten bei der Entscheidung nach § 240 II StGB?, in: NJW 1–2 1987, S. 36–38.

BeckRS, Schadsoftware – Hacker-Tools und Berufsfreiheit, in: NJW-Spezial 14 2009, S. 457.

Bergmann, Olaf, Portierungsdatenaustausch für VoPSTN, Version 2, Stand 11.03.2008, hg. v. Arbeitskreis für technische und betriebliche Fragen der Nummerierung und Netzzusammenschaltung – Unterarbeitskreis Signalisierung (UAK-S), Diskussionsbeitrag zur 88. Sitzung des UAK-S am 11.03.2008, Dokument 88.1, zugreifbar im internen Bereich unter http://www.aknn.de (Zugangsberechtigung erforderlich, zuletzt besucht am 16.12.2008).

BNetzA, Jahresbericht 2008, hg. v. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 2008.

Breuer, Barbara, Anwendbarkeit des deutschen Strafrechts auf exterritorial handelnde Internet-Benutzer, in: MMR 1998, S. 141–144.

Buggisch, Walter, Fälschung beweiserheblicher Daten durch Verwendung einer falschen E-Mail-Adresse?, in: NJW 49 2004, S. 3519–3522.

CERT/CC, CERT Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP), Feb. 2003, URL: http://www.cert.org/advisories/CA-2003-06.html (besucht am 08. 12. 2009).

Convention on Cybercrime, ETS 185, URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (besucht am 08. 12. 2009).

Darilion, Klaus, Analysis of a VoIP Attack, Okt. 2008, URL: http://www.ipcom.at/fileadmin/public/2008-10-22_Analysis_of_a_VoIP_Attack.pdf (besucht am 08. 12. 2009).

DFN, Forschungsstelle Recht im, Stellungnahme zum Regierungsentwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität vom 20. September 2006, Dez. 2006, URL: http://www.dfn.de/fileadmin/3Beratung/Recht/Stellungnahme06-11-24.pdf (besucht am 08. 12. 2009).

Dieterich, Thomas, Peter Hanau und Günter Schaub (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 10. Aufl., 2010.

Dornseif, Maximillian und Kay H. Schumann, Probleme des Datenbegriffs im Rahmen des § 269 StGB, in: JR 2 2002, S. 52–57.

Eichelberger, Jan, Das Blockieren einer Internet-Seite als strafbare Nötigung Zugleich eine Besprechung von AG Frankfurt am Main, Urt. v. 1.7.2005 -— 991 Ds 6100 Js 226314/01 (Online-Demo), in: Datenschutz und Datensicherheit (DuD) 30.8 Aug. 2006, S. 490–496.

Ders., Sasser, Blaster, Phatbot & Co. – alles halb so schlimm? – Ein Überblick über die strafrechtliche Bewertung von Computerschädlingen, in: Multimedia und Recht 9 2004, S. 594–597.

Ernst, Stefan, Das neue Computerstrafrecht, in: NJW 37 2007, S. 2661–2666.

Ders., Hacker und Computerviren im Strafrecht, in: NJW 45 2003, S. 3233–3239.

Europäische Kommission (Hrsg.), Achter Bericht der Kommission über die Umsetzung des Reformpakets im Telekommunikationssektor: Telekommunikation in Europa – Regulierung der Märkte 2002, KOM (2002) 695 endgültig, 2002.

Fleischer, Holger (Hrsg.), Handbuch des Vorstandsrechts, 2006.

Franks, John u. a., HTTP Authentication: Basic and Digest Access Authentication, Juni 1999, URL: http://www.ietf.org/rfc/rfc2617.txt (besucht am 08. 12. 2009).

Free Software Foundation (FSF), Categories of Free and Non-Free Software, zuletzt aktualisiert im November 2009, URL: http://www.gnu.org/philosophy/categories.html (besucht am 08. 12. 2009).

Dies., GNU General Public License, version 2, Juni 1991, URL: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html (besucht am 08. 12. 2009).

Gercke, Marco, Die Entwicklung des Internetstrafrechts 2006, in: ZUM 4 2007, S. 282–294.

Ders., Strafbarkeit einer „Online-Demo“, in: MMR 8 2006, Anmerkung zu OLG Frankfurt/M. Beschluss. vom 22.5.2006 – 1 Ss 319/05, S. 547–553.

Graf, Annika und Volker Briegleb, DSL-Markt: Kommt 2009 die Konsolidierung?, heise online, Artikel vom 22.12.2008, URL: http://www.heise.de/newsticker/meldung/DSL-Markt-Kommt-2009-die-Konsolidierung-191951.html (besucht am 08. 12. 2009).

Gröseling, Nadine und Frank Michael Höfinger, Computersabotage und Vorfeldkriminalisierung – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, in: MMR 10 2007, S. 626–630.

Günther, Jochen, Die Bedeutung von Open Source in der öffentlichen Verwaltung und der IT-Branche, in: Open Source Jahrbuch 2008, S. 155–168.

Haft, Fritjof, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), in: NStZ 1987, S. 6–10.

Hasecke, Jan Ulrich, Anwenderemanzipation Wie Nutzer die Softwareentwicklung beeinflussen können, in: Open Source Jahrbuch 2008, S. 7–18.

Heghmanns, Michael, Strafrecht für alle Semester: Besonderer Teil, Bd. 2, 2009.

Heinrich, Hartmut u. a., Open-Source-Software und ihre Bedeutung für Innovatives Handeln, hg. v. Friedrich-L. Holl, Metastudie im Auftrag des Bundesministeriums für Bildung und Forschung, 2006.

Heintschel-Heinegg, Bernd von (Hrsg.), Beck'scher Online-Kommentar, 2009.

Hilgendorf, Eric, Denial of service-Angriffe straflos?, in: Heckmann, Dirk (Hrsg.), jurisPR-ITR, Anm. 2, 10/2006.

Hoeren, Thomas, Internetrecht, 2009.

Hromadka, Wolfgang, Arbeitnehmer oder freier Mitarbeiter?, in: NJW 26 2003, Anmerkung zu BAG Urt. vom 29.05.2002 - 5 AZR 161/01, S. 1847–1849.

International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), Recommendation E.164: The international public telecommunication numbering plan. Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, Feb. 2005.

Dies., Recommendation Y.2001: General overview of NGN. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks, Dez. 2004.

Jacques, Olivier und Richard Gayraud, SIPp, 2004, URL: `http://sipp.sourceforge.net/` (besucht am 08. 12. 2009).

Jakobs, G., Mittelbare Täterschaft der Mitglieder des Nationalen Verteidigungsrats, in: NStZ 1 1995, Anmerkung zu BGH Urt. vom 26.07.1994 – 5 StR 98/94 = NStZ 1994, 537, S. 26–27.

Joecks, Wolfgang und Klaus Miebach (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, Bd. 1, 2006.

Köppen, Hajo, Computerkriminalität im Jahr 2008, in: Datenschutz und Datensicherheit (DuD) 33.7 Juli 2009, S. 409–410.

Ders., Entwicklung der Computerkriminalität in den Jahren 2004 bis 2007, in: Datenschutz und Datensicherheit (DuD) 32.12 Dez. 2008, S. 409–410.

Lackner, Karl und Kristian Kühl (Hrsg.), Strafgesetzbuch, 26. Aufl., 2007.

Laue, Christian, Strafrecht und Internet – Teil 1, in: Janssen, Gerhard (Hrsg.), jurisPR-StrafR, Anm. 2, 13/2009.

Leupold, Andreas und Silke Glossner (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 2008.

Luthiger, Benno, Alles aus Spaß? Zur Motivation von Open-Source-Entwicklern, in: Open Source Jahrbuch 2004, S. 93–106.

Lutterbeck, Bernd, Matthias Bärwolf und Robert A. Gehring (Hrsg.), Open Source Jahrbuch 2004. Zwischen freier Software und Gesellschaftsmodell, 2004.

Ders. (Hrsg.), Open Source Jahrbuch 2008. Zwischen freier Software und Gesellschaftsmodell, 2008.

Mansmann, Urs, Knackiger Sound, in: c't 6 2009, S. 194–195.

Marwan, Peter, Studie: Konsolidierung im deutschen Breitbandmarkt steht bevor, ZDNet.de, Artikel vom 19.10.2009, URL: http://www.zdnet.de/news/wirtschaft_unternehmen_business_studie_konsolidierung_im_deutschen_breitbandmarkt_steht_bevor_story-39001020-41516026-1.htm (besucht am 08. 12. 2009).

Metzger, Axel und Till Jaeger, Open Source Software und deutsches Urheberrecht, in: GRUR Int 10 1999, S. 839–848.

Miebach, Klaus, Berücksichtigung von Fernzielen bei Sitzblockaden, in: NStZ 3 1988, Anmerkung zu OLG Stuttgart, Vorlagebeschluss vom 17.12.1987 – 4 Ss 361/87.

Moll, Wilhelm (Hrsg.), Münchener Anwaltshandbuch Arbeitsrecht, 2. Aufl., 2009.

Murphy, Martin und Jürgen Kuri, Preiskampf auf DSL-Markt treibt Konsolidierung an, heise online, Artikel vom 7.08.2007, URL: http://www.heise.de/newsticker/meldung/Preiskampf-auf-DSL-Markt-treibt-Konsolidierung-an-160387.html (besucht am 08. 12. 2009).

Otto, Harro, Sitzdemonstrationen und strafbare Nötigung in strafrechtlicher Sicht, in: NStZ 5 1987, S. 212–213.

Ders., Strafbare Nötigung durch Sitzblockaden in der höchstrichterlichen Rechtsprechung und die Thesen der Gewaltkommission zu § 240 StGB, in: NStZ 12 1992, S. 568–573.

Popp, Andreas, Zur Umsetzung der „Convention on Cybercrime“ in Deutschland und Österreich, in: MR-Int 2007, S. 84–88.

Postel, John, Internet Protocol, Sep. 1981, URL: http://www.ietf.org/rfc/rfc791.txt (besucht am 08. 12. 2009).

Ders., User Datagram Protocol, Aug. 1980, URL: http://www.ietf.org/rfc/rfc768.txt (besucht am 08. 12. 2009).

Rahemipour, Jacqueline, OpenOffice.org – Aus dem Alltag eines nicht alltäglichen Open-Source-Projekts, in: Open Source Jahrbuch 2008, S. 27–40.

Rinker, Mike, Strafbarkeit und Strafverfolgung von „IP-Spoofing“ und „Portscanning“, in: MMR 2002, S. 663–666.

Rosenberg, Jonathan u. a., SIP: Session Initiation Protocol, Juni 2002, URL: http://www.ietf.org/rfc/rfc3261.txt (besucht am 08. 12. 2009).

Sankol, Barry, Die Qual der Wahl: § 113 TKG oder §§ 100g, 100h StPO? – Die Kontroverse über das Auskunftsverlangen von Ermittlungsbehörden gegen Access-Provider bei dynamischen IP-Adressen, in: MMR 12 2006, S. 361–365.

Scholz, Hendrik, ratelimit, 2006, URL: http://www.iptel.org/ser/doc/modules/ratelimit (besucht am 08. 12. 2009).

Schultz, Alexander, Neue Strafbarkeiten und Probleme – Der Entwurf des Strafrechtsänderungsgesetzes (StrafÄndG) zur Bekämpfung der Computerkriminalität vom 20.09.2006, in: Datenschutz und Datensicherheit (DuD) 30.12 2006, S. 778–784.

Schulz, Carsten, Die GPL kommentiert und erklärt, in: 2005, Kap. Ziffer 5 GPL, S. 96–103.

Schumann, Kay H., Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, in: NStZ 12 2007, S. 675–680.

Schönke, Adolf und Horst Schröder (Hrsg.), Strafgesetzbuch, 27. Aufl., 2006.

Seifert, Tilman und Thomas Wieland, Prerequisites For Enterprises To Get Involved In Open Source Software Development, in: 1st Workshop of Open Source Software in Industrial Environments, Proceedings of Net.ObjectDays, Erfurt, 2003.

Sieber, Ulrich, Internationales Strafrecht im Internet – Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace, in: NJW 29 1999, S. 2065–2073.

Spindler, Gerald, Softwarebeschaffung, Rechtsmängelhaftung und IT-Riskmanagement, in: Heymann/Schneider (Hrsg.): Festschrift für Michael Bartsch zum 60. Geburtstag 2006.

Statistisches Bundesamt (Hrsg.), Statistisches Jahrbuch für die Bundesrepublik Deutschland, 2009.

Stegbauer, Andreas, Rechtsprechungsübersicht zu den Propaganda- und Äußerungsdelikten, in: NStZ 12 2005, S. 677–683.

Sujecki, Bartosz, Vertrags- und urheberrechtliche Aspekte von Open Source Software im deutschen Recht, in: JurPC Web-Dok. 145 2005, URL: http://www.jurpc.de/aufsatz/20050145.htm (besucht am 08. 12. 2009).

Többens, Hans W., Die Bekämpfung der Wirtschaftskriminalität durch die Troika der §§ 9, 130 und 30 des Gesetzes über Ordnungswidrigkeiten, in: NStZ 1 1999, S. 1–8.

Verordnung (EG) Nr. 2887/2000 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 über den entbündelten Zugang zum Teilnehmeranschluss, ABl. Nr. L 336 vom 30.12.2000, S. 4—8.

Wabnitz, Heinz-Bernd und Thomas Janovsky (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 2007.

Walsh, Thomas J. und D. Richard Kuhn, Challenges in Securing Voice over IP, in: IEEE Security & Privacy 3.3 2005, S. 44–49.

Wandtke, Artur-Axel und Winfried Bullinger (Hrsg.), Praxiskommentar zum Urheberrecht, 20109.

Welfens, Paul J. J. u. a., Internetwirtschaft 2010 – Perspektiven und Auswirkungen, Techn. Ber., Europäisches Institut für internationale Wirtschaftsbeziehungen (EIIW) in Zusammenarbeit mit dem Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI) im Auftrag des Bundesministeriums für Wirtschaft und Arbeit, 2004, URL: http://www.bmwi.de/BMWi/Navigation/Service/publikationen,did=72096.html (besucht am 08. 12. 2009).

West, Joel, Unternehmen zwischen Offenheit und Profitstreben, in: Open Source Jahrbuch 2008, S. 77–90.

Wheeler, David A., Why Open Source Software / Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers!, Apr. 2007, URL: http://www.dwheeler.com/oss_fs_why.html (besucht am 08. 12. 2009).

Wieland, Thomas, Stärken und Schwächen freier und Open-Source-Software im Unternehmen, in: Open Source Jahrbuch 2004, S. 107–120.

Wien, Andreas, Computerkriminalität und Strafrecht, 2009, S. 177–194.

Wieser, Christian, Marko Laakso und Henning Schulzrinne, SIP robustness testing for large-scale use, in: SOQUA/TECOS, Bd. 58, 2004, S. 165–178.

Gesetzestexte und Drucksachen

BGBl. I Nr. 15 vom 25.02.1987, 602–629.

BGBl. I Nr. 21 vom 23.05.1986, 721.

BGBl. I Nr. 38 vom 10.08.2007, 1786.

BGBl. I Nr. 49 vom 3.08.2009, 2353–2354.

BGBl. II Nr. 30 vom 10.11.2008, 1242.

BR-Drs. 676/06.

BT-Drs. 10/5058.

BT-Drs. 13/8016.

BT-Drs. 16/3656.

Richtlinie 2002/77/EG der Kommission vom 16. September 2002 über den Wettbewerb auf den Märkten für elektronische Kommunikationsnetze und -dienste (Text von Bedeutung für den EWR, ABl. Nr. L 249 vom 17.09.2002 S. 21–26.

Richtlinie 90/388/EWG der Kommission vom 28. Juni 1990 über den Wettbewerb auf dem Markt für Telekommunikationsdienste (Open Network Provision, ONP), ABl. Nr. L 192 vom 24.7.1990, S. 10–16.

Richtlinie 96/19/EG der Kommission vom 13. März 1996 zur Änderung der Richtlinie 90/388/EWG hinsichtlich der Einführung des vollständigen Wettbewerbs auf den Telekommunikationsmärkten, ABl. Nr. L 74 vom 22.03.1996 S. 13–24.

Entscheidungsregister

AG Frankfurt a. M., Urt. v. 1.07.2005 – 991 Ds 6100 Js 226314/01 = MMR 2005, 863 (m. Anm. v. Gercke).

BAG, Urt. v. 19. 1. 2000 – 5 AZR 644/98 = NZA 2000.

BGH, Urt. v. 04.07.1991 – 4 StR 179/91 (LG Saarbrücken) = NStZ 1991, 490.

Ders., Urt. v. 04.11.1988 – 1 StR 262/88 = NJW 1989, 781.

Ders., Urt. v. 05.05.1988 – 1 StR 5/88 = NStZ 1988 = NJW 1988, 362.

Ders., Urt. v. 06.07.1990 – 2 StR 549/89 (LG Mainz) = NJW 1990, 2560.

Ders., Urt. v. 12.12.2000 – 1 StR 184/00 (LG Mannheim) = NStZ 2001, 305.

Ders., Urt. v. 24.03.1998 – 1 StR 558-97 (LG Karlsruhe) = NJW 1998, 2064.

Ders., Urt. v. 26.07.1994 – 5 StR 98/94 (LG Berlin) = NJW 1994, 2703.

BVerfG, Beschluss. v. 10.01.1995 – 1 BvR 718/89, 719/89, 722/89, 723/89 = NJW 1995, 1141 = NStZ 1995, 275.

Dass., Urt. v. 18.5.2009 – 2 BvR 2233/07 = K&R 2009, 632 = CR 2009, 673 = ZUM 2009, 745.

Dass., Urt. v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822 = MMR 2008, 315 (m. Anm. von Bär).

LG München I, Urt. v. 19.05.2004 – 21 O 6123/04 = DZWIR 2004, 391 = MMR 2004, 693.

LG München I, Urt. v. 7.03.2005 – 21 O 3220/05 (nicht rechtskräftig) = MMR 2005, 385 = GRUR-RR 2005, 214.

OLG Frankfurt a. M., Beschluss v. 22.5.2006 – 1 Ss 319/05 = MMR 2006, 547 (m. Anm. v. Gercke).

OLG Jena, Beschluss vom 2.11.2005 – 1 Ss 242/05 = NStZ 2006, 533.

OLG München, Urt. v. 28.07.2005 — 29 U 2887/05 = ZUM 2005, 896 = CR 2005, 821 = K&R 2005, 467.