Michael Albrecht

Die Kriminalisierung von Dual-Use-Software

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

in Fortführung der Reihe
„Beiträge und Materialien aus dem Max-Planck-Institut
für ausländisches und internationales Strafrecht Freiburg“
begründet von Albin Eser

Band S 144

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Die Kriminalisierung von Dual-Use-Software

Michael Albrecht

Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Alle Rechte vorbehalten
© 2014 Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
c/o Max-Planck-Institut für ausländisches und internationales Strafrecht
Günterstalstraße 73, 79100 Freiburg i.Br.
http://www.mpicc.de
Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin
http://www.duncker-humblot.de

Umschlagbild: © Kaspersky Lab
Foto des Autors: PHOTO-SERVICE-SHOP-Dammtorstraße, Hamburg, Inh. T. Schaaf
Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim
Printed in Germany
Gedruckt auf alterungsbeständigem (säurefreiem) Papier entsprechend ISO 9706 ∴

ISSN 1860-0093
ISBN 978-3-86113-812-9 (Max-Planck-Institut)
ISBN 978-3-428-14621-5 (Duncker & Humblot)
DOI https://doi.org/10.30709/978-3-86113-812-9
CC-Lizenz by-nc-nd/3.0

Vorwort

Cyberkriminelle handeln heute in international organisierten und hochspezialisierten Gruppierungen. Ihre „Wertschöpfungskette“ reicht von der Suche nach Schwachstellen über die Entwicklung von Schadsoftware bis zu deren Vertrieb. So kommt jede halbe Sekunde ein neues Schadprogramm auf den Markt. Neue Vorfeldtatbestände sollen dies eindämmen und stellen den Umgang mit gefährlichen Computerprogrammen unter Strafe. Doch auch IT-Sicherheitsexperten brauchen solche Software, um durch Tests und Analysen dieselben Schwachstellen zu finden und zu schließen. So stellt sich dem Gesetzgeber die *Dual-Use-Problematik*, um deren Lösung geht es in dieser Arbeit geht.

Die Arbeit wurde im April 2013 als Dissertation bei der Juristischen Fakultät der Albert-Ludwigs-Universität zu Freiburg i.Br. eingereicht. Rechtsprechung und Literatur sind auf dem Stand von März 2013. In Fußnoten sind wichtige Neuerungen noch bis Mitte 2013 berücksichtigt.

Mein Dank gilt an erster Stelle Herrn Professor Dr. Dr. h.c. mult. *Ulrich Sieber*, der mich in das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg i.Br. aufgenommen und beim Erarbeiten der Dissertation sehr gefördert hat. Seine Betreuung war vor allem bei der Konzeption des Forschungsprojekts, aber auch bei der Überarbeitung des Dissertationsmanuskripts äußerst wertvoll. Ausdrücklich danke ich für die Eigenverantwortung und Freiheit in allen inhaltlichen Entscheidungen.

Gleichfalls danke ich Herrn Professor Dr. *Walter Perron* für sein anregendes Zweitgutachten. Fruchtbar waren auch die vielen Diskussionen mit Kollegen am Max-Planck-Institut und Mit-Stipendiaten der International Max Planck Research School for Comparative Criminal Law.

Ich danke *Simone*, *Reiner*, *Liesel*, *Martin*, *Katharina* und *Gregor*, die mein Manuskript korrekturgelesen haben. *Simones* unerschütterliche Zuversicht half mir durch alle schwierigen Phasen und gab starken Rückhalt.

Mein ganz besonderer und größter Dank gebührt schließlich meinen *Eltern*. Sie waren mir nicht nur Ansporn durch ihr eigenes Vorbild, sondern ließen mich seit Schul- und Studienzeiten auch ihre bedingungslose Unterstützung spüren. Ihnen widme ich diese Arbeit.

München, im Oktober 2014 *Michael Albrecht*

Inhalt

Teil 4
Optimierung der Straftatbestände

Abkürzungsverzeichnis

a.A.	am Anfang
a.a.O.	am angegebenen Ort
a.M.	am Main
abl.	ablehnend
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AL	Ausfuhrliste
Am. J. Int'l L.	American Journal of International Law
AnwBl	Anwaltsblatt
Art.	Artikel
Aufl.	Auflage
AWV	Außenwirtschaftsverordnung
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BayObLG	Bayerisches Oberstes Landesgericht
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHSt	Amtliche Sammlung der Entscheidungen des Bundesgerichtshofs in Strafsachen
BKA	Bundeskriminalamt
BMWI	Bundesministerium für Wirtschaft
BSI	Bundesamt für Sicherheit in der Informationtechnik
bspw.	beispielsweise
BT-Drucks.	Drucksache des deutschen Bundestags
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
bzw.	beziehungsweise
CCC	Convention on Cybercrime
CIA	Confidentiality, integrity, availability (von Daten)
CoCom	Coordinating Committee for Multilateral Export Controls
COM	Document of the European Commission
CR	Computer und Recht

DDoS	Distributed Denial of Service
ders.	derselbe
DoS	Denial of Service
DRM	Digital Rights Management
Drucks.	Drucksache
DS	Der Sachverständige
DuD	Datenschutz und Datensicherheit
ebd.	ebenda
EG	Europäische Gemeinschaft(en)
etc.	et cetera
ETS	European Treaty Series
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
Fn.	Fußnote
FS	Festschrift
FTA	Free-to-air
FTP	File Transfer Protocol
GA	Goltdammer's Archiv für Strafrecht
ggf.	gegebenenfalls
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR-Int	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
HMD	HMD – Praxis der Wirtschaftsinformatik
HRRS	Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht
Hrsg.	Herausgeber
http	Hypertext Transfer Protocol
i.S.d.	im Sinne des/der
i.V.m.	in Verbindung mit
I/O	Input/Output
Info-RL	Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft
IT	Information Technology (Informationstechnologie)

ITRB	Der IT-Rechts-Berater
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
JuS	Juristische Schulung
JZ	JuristenZeitung
KOM	Dokument der Europäischen Kommission
K&R	Kommunikation und Recht
KWKG	Kriegswaffenkontrollgesetz
LG	Landgericht
Lit.	*littera* (Buchstabe)
m.w.N.	mit weiteren Nachweisen
MMR	MultiMedia und Recht
MR-Int	Medien und Recht International
NJW	Neue Juristische Wochenschrift
Nr./Nrn.	Nummer/Nummern
NStZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
P2P	peer-to-peer
pp.	perge, perge
RAM	Random-access memory
RB	Rahmenbeschluss
RL	Richtlinie
Rn.	Randnummer
ROM	Read-only memory
Rs.	Rechtssache
Rspr.	Rechtsprechung
S.	Seite
Slg.	Amtliche Sammlung des EuGH
sog.	sogenannt
st. Rspr.	ständige Rechtsprechung
StraFo	Strafverteidiger Forum
StGB	Strafgesetzbuch
StVG	Straßenverkehrsgesetz
SVR	Straßenverkehrsrecht
u.a.	unter anderem; und andere
u.U.	unter Umständen

UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
VG	Verwaltungsgericht
vgl.	vergleiche
WIPO	World Intellectual Property Organization
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WWW	World Wide Web
z.B.	zum Beispiel
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZKDSG	Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht

Einleitung

I. Forschungsgegenstand

Jede halbe Sekunde entsteht ein neues Schadprogramm.[1] Wie *Michael Hange*, der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), betont, wird solche Software nicht mehr von Einzeltätern geschrieben, sondern die Programmierer sind eingegliedert in internationale, arbeitsteilig organisierte Netzwerke mit enormer Innovationskraft. Deren Wertschöpfungskette reiche von der Suche nach Schwachstellen über die Programmierung von Schadsoftware bis hin zum Handel mit gestohlenen Daten. Die notwendigen Computerprogramme würden dabei von professionellen Cyberkriminellen im Stile eines Baukastensystems industriell gefertigt.[2]

Der deutsche Gesetzgeber hat der Verbreitung solch schädlicher Computerprogramme den Kampf angesagt und mehrere Straftatbestände geschaffen, die den Umgang mit bestimmten, als Schadsoftware eingestuften Computerprogrammen verbieten. Zum ersten Mal wurde ein Software-Delikt in diesem Sinne im Jahr 2002 im Zugangskontrolldiensteschutzgesetz definiert, hier wurde das Herstellen, Einführen und Verbreiten von sogenannten Umgehungsvorrichtungen unter Strafe gestellt (heute § 4 ZKDSG). Unter Umgehungsvorrichtungen wurden von Anfang an insbesondere „Hackerprogramme" verstanden, mittels derer sich z.B. verschlüsselte Pay-TV-Sender ohne großen Aufwand entschlüsseln lassen.[3] Anschließend normierte der Gesetzgeber Software-Delikte in den Bereichen der Geld- und Wertzeichenfälschung (§ 149 Abs. 1 Nr. 1 StGB), der Überwindung von Kopierschutz- und ähnlichen Maßnahmen (§ 108b Abs. 2 UrhG), des Computerbetrugs (§ 263a Abs. 3 StGB), des Missbrauchs von Wegstreckenzählern und Geschwindigkeitsbegrenzern (§ 22b Abs. 1 Nr. 3 StVG) und schließlich der *CIA-Delikte*, also der Delikte gegen Vertraulichkeit *(confidentiality)*, Intergrität *(integrity)* und Verfügbarkeit *(availability)* von Computerdaten (§ 202c Abs. 1 Nr. 2 StGB). Mittlerweile ergibt sich in diesen Bereichen insgesamt über ein Dutzend verschiedener Tatbe-

---

[1] Siehe „De Maizières Schutzwerk für den ‚Cyber-Raum'", Zeit online vom 23.2.2011, online abrufbar unter http://www.zeit.de/digital/internet/2011-02/cyber-abwehrzentrum [zuletzt abgerufen am 15.11.2014].

[2] Pressemitteilung des BKA und BSI vom 12.5.2010, online abrufbar unter https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/BKA_IuK-Kriminalitaet_120510.html [zuletzt abgerufen am 15.11.2014].

[3] BT-Drucks. 14/7229, S. 8.

standskombinationen, in denen der Umgang mit jeweils unterschiedlichen Computerprogrammen unter Strafe gestellt ist.

Obwohl der Gesetzgeber hier in völlig verschiedenen Sachgebieten aktiv geworden ist, bestehen weitreichende Gemeinsamkeiten: Durch die Schaffung dieser Software-Delikte will der Gesetzgeber Schwarzmärkte für schädliche Computerprogramme trockenlegen und eine befürchtete *Underground Economy* „an der Wurzel bekämpfen".[4] Daneben soll Massenkriminalität verhindert werden, die der Gesetzgeber befürchtet, weil solche Programme im Internet einfach, schnell und häufig kostenlos verfügbar seien. Neben den Ähnlichkeiten in den gesetzgeberischen Motiven bestehen aber auch strukturelle Gemeinsamkeiten zwischen den Tatbeständen: Computerprogramme werden jeweils als „digitale Werkzeuge" für spätere Straftaten umschrieben und tatbestandlich erfasst. Durch die Software-Delikte kriminalisiert der Gesetzgeber also das Vorfeld zu eigentlichen Rechtsgutsverletzungen, um solche Verletzungen möglichst zu verhindern. Diese Form der Kriminalitätsbekämpfung durch Vorfelddelikte ist Ausdruck eines neuen Sicherheits- und Präventionsgedankens, welcher einer ganzen Reihe jüngerer Tatbestände insbesondere in den Bereichen des Terrorismus und der Organisierten Kriminalität zugrunde liegt: Sinn und Berechtigung dieses neuen Präventionsstrafrechts werden nicht mehr in der *Ahndung* sozialschädlichen Verhaltens gesehen, sondern in dessen *Verhinderung*.[5] Die überkommene strafrechtliche Aufgabe der Repression gerät damit in den Hintergrund. Angesichts dieses Paradigmenwechsels ist die Diskussion um Legitimation und Grenzen des Strafrechts neu entflammt.

Dass aber die Kriminalisierung des Umgangs mit Computerprogrammen auch über die dogmatische Debatte hinaus erhebliche Verunsicherung schaffen kann, trat bei der Einführung des § 202c Abs. 1 Nr. 2 StGB offen zutage: Der sogenannte Hacker-Paragraph soll den Umgang mit „Hacking-Tools" in Vorbereitung bestimmter IT-Straftaten eigens unter Strafe stellen. Doch schon während des Gesetzgebungsverfahrens kamen Bedenken wegen des konkreten Wortlauts des Tatbestands auf, und zwar weit über die Grenzen der juristischen Fachwelt hinaus: Mit Inkrafttreten des Gesetzes im August 2007 wurde gegen den Präsidenten des Bundesamts für Sicherheit in der Informationstechnik Strafanzeige wegen Verbreitens von Hacking-Tools gemäß § 202c Abs. 1 Nr. 2 StGB erstattet, weil das BSI auf seiner Homepage die Software-Suite *BOSS* anbot, in der ein Programm zum Passwortknacken namens *John the Ripper* enthalten war – nur zu Testzwecken, versteht

---

[4] Siehe Explanatory Report zur CCC, Rn. 71.

[5] Kritisch hierzu *Hassemer*, HRRS 2006, 130 ff.; *Sieber*, NStZ 2009, 354 f.; *Jakobs* sieht hierin einen Wandel vom bürgerlichen zum Feindstrafrecht, ZStW 117 (2006), 845 ff., welches er aber nicht unter allen Umständen für illegitim hält, a.a.O., 847. Auch *Pawlik*, Der Terrorist und sein Recht, S. 41, plädiert für ein „Bekämpfungsrecht", das Terroristen „als Feinde anerkennt". Für eine Begrenzung der „Instrumentalisierung des Strafrechts zu Präventionszwecken" *Weißer*, ZStW 121 (2009), 160. Zweifelnd am Funktionswandel insgesamt *Zabel*, StraFo 2011, 21.

sich: der Nutzer solle die Sicherheit seiner Passwörter überprüfen können.[6] Mehrere Personen erhoben umgehend Verfassungsbeschwerden gegen den neuen Straftatbestand, darunter ein IT-Sicherheitsunternehmen, das Angriffssimulationen (sog. *Penetration Tests*) durchführt, ein Informatikprofessor, der zu Lehrzwecken Schadsoftware zugänglich machte, und ein Privater, dessen Linux-Distribution diverse „Sicherheitstools" enthielt. Sie alle befürchteten, dass durch den neu geschaffenen Tatbestand nicht nur Cyberkriminelle in ihren Vorbereitungshandlungen bestraft würden, sondern dass auch ein alltäglicher oder beruflich notwendiger, jedenfalls aber legitimer Umgang mit „Schadsoftware" oder „Analysesoftware" künftig nicht mehr möglich sei. Die *Dual-Use-Problematik* wurde prominent.

Im Mai 2009 erging in den Verfahren ein Nichtannahmebeschluss des Bundesverfassungsgerichts,[7] der aber aufgrund der konkret gestellten Anträge nur in einigen Auslegungsfragen Impulse setzen konnte, die neuralgischen Punkte jedoch unberührt ließ. Es blieb daher offen, wo die Grenze zwischen straflosem Umgang und krimineller Straftatvorbereitung verläuft. Unter dieser Unsicherheit leidet die IT-Sicherheitsbranche und es werden weiterhin massive *Chilling Effects* befürchtet.[8] Im Brennpunkt sind dabei zwei Fragen, nämlich erstens, nach welchen Kriterien Computerprogramme in „Analysetools", „Schadsoftware" und „Dual-Use-Tools" zu unterscheiden sind und welche davon tatbestandlich erfasst sein sollen, und zweitens, was genau unter dem Merkmal „Vorbereiten" zu verstehen ist. Hinter den Auslegungsschwierigkeiten stehen Zweifel daran, ob der Wortlaut tatsächlich das ausdrückt, was der Gesetzgeber historisch regeln wollte oder welche Regelung sinnvoll wäre. Insbesondere beim subjektiven Bezug des Vorfeldtäters zur Zieltat ist umstritten, welche Anforderungen de lege lata bestehen und ob diese de lege ferenda optimiert werden müssten. Die Untersuchung und Beantwortung dieser Fragen ist deshalb nicht nur mit Blick auf § 202c Abs. 1 Nr. 2 StGB bedeutsam, sondern hat sich hieran lediglich entzündet. Unter dem Schlagwort der *Dual-Use-Problematik* werden nämlich Probleme diskutiert, die sich bei allen Software-Delikten ergeben, weil in solchen Vorfeldtatbeständen der Umgang mit Computerprogrammen erfasst wird, mit denen neben kriminellen stets auch legitime Handlungen denkbar sind.

Auch in Zukunft werden diese Fragen kaum ihre Dringlichkeit verlieren: Nach BKA-Präsident *Jörg Ziercke* werden Computerprogramme mittlerweile in allen

---

[6] Siehe „Das BSI und § 202c: Der Hackerparagraf und das Bundesamt", online abrufbar unter http://www.tecchannel.de/sicherheit/management/1729025/das_bsi_und_202c_der_hackerparagraf_und_das_bundesamt/index.html [zuletzt abgerufen am 15.11.2014].

[7] BVerfG, Beschluss vom 18.5.2009, 2 BvR 2233/07; 2 BvR 1151/08; 2 BvR 1524/08.

[8] Siehe nur *Ladner/Schillo*, Neues zum Hackerparagrafen, CRN vom 25.2.2010, online abrufbar unter http://www.crn.de/service/recht/artikel-80263.html [zuletzt abgerufen am 15.11.2014]; *Muncan/Schreiber*, DuD 2009, 221.

Kriminalitätsbereichen unterstützend eingesetzt.[9] Insofern beunruhigt etwa die Meldung, dass es einem Team aus Informatikern, Elektrotechnikern und Kardiologen gelungen sei, an einen Herzschrittmacher per Funk den Befehl zur Erteilung von Elektrostößen auszusenden.[10] Unter dem Aspekt des *Ubiquitous Computing*, also der vollständigen digitalen Durchdringung des Alltags,[11] ergeben sich immer weitere Anwendungsgebiete für Schadsoftware. Möglicherweise wird also der Gesetzgeber schon bald neuen Handlungsbedarf sehen und in weiteren Kriminalitätsbereichen neue Software-Delikte entwerfen. Denn je stärker der Alltag der Menschen von Computertechnik durchdrungen ist, umso größer und vielfältiger sind die Angriffsflächen für Schadsoftware. Schon bislang wurden softwarespezifische Vorfelddelikte unter Verzicht auf eine systematische Herangehensweise in eher heterogenen Deliktsfeldern und in unterschiedlicher rechtstechnischer Ausprägung eingeführt. Künftig lassen sich nicht mehr nur im Vorfeld einer Urheberrechtsverletzung oder eines *Denial-of-Service*-Angriffs entsprechende digitale Tatwerkzeuge denken. Denn wenn von der Einbruchssicherung über den Stromzähler bis hin zum Herzschrittmacher alle Geräte digital arbeiten, lassen sie sich auch digital manipulieren. Der Gedanke an ein Software-Delikt im Vorfeld eines Hausfriedensbruchs oder gar eines Totschlags erscheint nicht mehr befremdlich, und für den Gesetzgeber wird spätestens mit dem Auftauchen neuer Kriminalitätsphänomene neuer Druck entstehen. Um weiterem strafrechtlichem Stückwerk, verunsichernden Vorfeldtatbeständen oder inhaltsleeren Symbolgesetzen vorzubeugen, muss daher die Grundfrage erörtert werden: Wie soll welcher Umgang mit welchen Computerprogrammen pönalisiert werden?

II. Forschungsziel

Ziel der Arbeit ist es, einen allgemeinen Modellstraftatbestand zu entwickeln, der den Umgang mit bestimmten Computerprogrammen im Vorfeld von Rechtsgutsverletzungen unter Strafe stellt. Dieser Tatbestand soll – ausgehend von den gesetzgeberischen Zielen – ein gerechtfertigtes Maß an Kriminalisierung erreichen, dabei jedoch legitimes Verhalten, insbesondere in der IT-Sicherheitsbranche, zuverlässig von der Strafbarkeit ausnehmen. Darüber hinaus soll er alle bisherigen

---

[9] Pressemitteilung des BKA und BSI vom 12.5.2010, online abrufbar unter https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/BKA_IuK-Kriminalitaet_120510.html [zuletzt abgerufen am 15.11.2014].

[10] „Hack ins Herz", Süddeutsche Zeitung vom 13.3.2008, online abrufbar unter http://www.sueddeutsche.de/digital/funksignal-an-herzschrittmacher-hack-ins-herz-1.297308 [zuletzt abgerufen am 15.11.2014].

[11] Vgl. zu den Anwendungsgebieten für Ubiquitous Computing *Mattern*, Ubiquitous Computing, S. 3 f.

Software-Delikte zusammenfassen und vereinheitlichen. Schließlich soll er so ausgestaltet sein, dass er ohne großen gesetzgeberischen Aufwand und ohne Systembrüche erweitert werden kann, falls neue Software-Delikte im Vorfeld weiterer Rechtsgutsverletzungen erforderlich und angemessen sein sollten.[12]

Hierfür muss die Dual-Use-Problematik in ihrem IT-spezifischen Einschlag untersucht werden. Der Begriff der Dual-Use-Problematik wird in der juristischen Fachliteratur uneinheitlich verwendet. Dies legt nahe, dass mehrere Aspekte eine Rolle spielen, die gedanklich noch nicht sauber voneinander getrennt werden. Deshalb soll der Frage nachgegangen werden, ob sich das Phänomen des Dual-Use allein aus den dem Computerprogramm immanenten Funktionen ergibt oder ob auch äußere Umstände eine Rolle spielen. Diese äußeren Umstände wären sodann zu identifizieren. Auf diese Weise muss ein Begriff von der Dual-Use-Problematik geschaffen werden, der ihre sämtlichen Aspekte abdeckt. Nur unter dieser Voraussetzung lässt sie sich angemessen regulieren.

Des Weiteren müssen die Grundsätze der Strafrechtslegitimation daraufhin untersucht werden, welche Vorgaben sie für eine Vorverlagerung der Strafbarkeit über das Versuchsstadium hinaus machen. Soweit möglich muss untersucht werden, welche konkreten Vorgaben sich aus dem aktuellen Stand der Diskussion um die Legitimation von Vorfelddelikten für die Kriminalisierung des Umgangs mit bestimmten Computerprogrammen ableiten lassen.

Schließlich sind die Regelungstechniken zu analysieren, die für eine legitime strafrechtliche Behandlung dieses Bereichs zur Verfügung stehen. Zu untersuchen ist, wie sie welchen Aspekt der Dual-Use-Problematik aufgreifen. Hier müssen alle unterschiedlichen Techniken der Software-Delikte im deutschen Strafrecht abstrakt analysiert werden. Da das IT-Strafrecht internationalen Harmonisierungsbestrebungen unterliegt, gehen viele deutsche Software-Delikte auf Vorgaben aus internationalen Instrumenten, etwa der Cybercrime-Konvention des Europarats (ETS Nr. 185), den Rahmenbeschlüssen 2000/383/JI und 2001/413/JI sowie dem Vorschlag der EU-Kommission für eine Richtlinie über Angriffe auf Informationssysteme KOM(2010) 517 zurück. Deshalb sind auch die Regelungstechniken dieser Regime beizuziehen. Schließlich finden sich insbesondere im Kriegswaffen- und Exportkontrollstrafrecht Regelungen, in denen sich der Gesetzgeber explizit mit Dual-Use-Aspekten auseinandergesetzt hat. Da hier Regelungstechniken vorzufinden sind, die in dieser Form weder in den deutschen Tatbeständen der Software-Delikte noch ihren internationalen Vorläufern eingesetzt wurden, sollen auch diese Gegenstand der Untersuchung werden.

---

[12] *Grunst*, GA 2002, 222 f. sieht in Straftatkatalogen eine Gefahr der Erweiterung. Nimmt man bei jeder Erweiterung Legitimationsfragen ernst, so ist in der einfachen Erweiterbarkeit eines Tatbestands jedoch eine Chance zu sehen.

III. Forschungsmethoden

Als Forschungsmethode wird ein funktionaler Rechtsvergleich angewandt. Verglichen werden gesetzgeberische Regelungstechniken zur Bewältigung der Dual-Use-Problematik. Diese entstammen dem deutschen Computerstrafrecht, dem deutschen Kriegswaffen- und Exportkontrollstrafrecht, EU-Rahmenbeschlüssen zur Harmonisierung nationalen Strafrechts, EG-Richtlinien zur Harmonisierung bestimmter Rechtsgebiete, einem Vorschlag für eine Richtlinie zur Harmonisierung des Informationsstrafrechts sowie der völkerrechtlichen Cybercrime Convention des Europarats. Hierbei wird funktional verglichen, wie die jeweiligen Regelungstechniken einzelne Aspekte der Dual-Use-Problematik aufgreifen und regeln. Die gefundenen Ergebnisse werden danach bewertet, wie effektiv sie bei konsequenter Vermeidung von *Chilling Effects* sind.

Hierfür werden die jeweiligen Normen samt ihren Begleitmaterialien wie Erwägungsgründen, Gesetzesbegründungen und Beratungsprotokollen analysiert. Ferner werden die Rechtsprechung und juristische Fachliteratur unter dem beforschten Aspekt ausgewertet. Ebenso werden relevante Publikationen zu den dogmatischen Grundlagen dargestellt. Zudem werden IT-spezifische Aspekte der Dual-Use-Problematik anwendungsorientiert kenntlich gemacht. Soweit dies möglich und erforderlich ist, wird auf Fachliteratur des IT-Sicherheitsmanagements zurückgegriffen. Erkenntnisse zu Herkunft und Verbreitungswegen bestimmter Schadprogramme stützen sich auf Recherchen in einschlägigen offenen und halboffenen Foren im Internet.

IV. Gang der Darstellung

Die Darstellung folgt dem Gedankengang, der im Forschungsziel entwickelt worden ist. In Teil 1 wird ein Begriff davon entwickelt, was Dual-Use bedeutet, in welchen Ausprägungen das Dual-Use-*Phänomen* in der Informationstechnik entsteht und inwiefern hieraus für den Gesetzgeber eine Dual-Use-*Problematik* im „Software-Strafrecht“ entsteht.

Darauf aufbauend wird in Teil 2 der aktuelle Stand der Debatte um die Strafrechtslegitimation im Vorfeld von Rechtsgutsverletzungen abgefragt. Dazu werden die Veröffentlichungen analysiert und zusammengeführt, die sich mit der Legitimation von Vorfelddelikten der einschlägigen Art auseinandersetzen. Es wird ein dogmatischer Rahmen entwickelt, in dem sich die Kriminalisierung des Umgangs mit Schadsoftware bewegen muss. Hieraus ergibt sich ein Legitimationsmaßstab für den Vergleich der Regelungstechniken.

Im Anschluss werden in Teil 3 die Rechtstechniken aller Tatbestände des deutschen Software-Strafrechts, der internationalen Harmonisierungsinstrumente sowie

des deutschen Kriegswaffen- und Exportkontrollstrafrechts auf ihren Regelungsinhalt und ihre Wirkweisen untersucht, sodass analysiert werden kann, wie sie welche Ausprägung des Dual-Use-Phänomens aufgreifen und lösen.

In Teil 4 erfolgt hierauf aufbauend der wertende Vergleich der Regelungstechniken aus dem Teil 3 hinsichtlich ihrer Rechtsklarheit und Legitimität in Bezug auf die verschiedenen Ausprägungen des Dual-Use-Phänomens. Dies ermöglicht den Entwurf eines optimierten Modellstraftatbestandes zur Kriminalisierung des Umgangs mit schädlicher Software im Vorfeld von Rechtsgutsverletzungen. Die Kernaussagen der Arbeit und die Vorzüge des Modellstraftatbestandes werden in einer abschließenden Zusammenfassung hervorgehoben.

Teil 1

Dual-Use als gesetzgeberische Herausforderung

Obwohl Computer und Internet den gesamten Lebensalltag der Menschen in Beruf und Freizeit durchdrungen haben, bleibt ihre konkrete technische Funktionsweise für den ganz überwiegenden Großteil ihrer Nutzer im Dunkeln. Da sich die Informationstechnik durch eine hohe Komplexität auszeichnet, sind auch IT-spezifische kriminelle Handlungen und Bedrohungen „aus dem Netz" in ihren Einzelheiten schwer nachvollziehbar. Zum besseren Verständnis solcher Bedrohungen werden deshalb häufig Analogien gesucht. Schadsoftware wird als digitale Waffe dargestellt: Der Tagesspiegel sprach mit Blick auf den Trojaner *Stuxnet* von einer „Sabotagewaffe",[1] der österreichische Standard von der „unsichtbaren Superwaffe"[2] und das Wochenblatt Spiegel von einer „Zauberwaffe".[3] Freilich ist schon der Begriff „Trojaner" eine Analogie, die verständlich machen soll, wie solche Computerprogramme funktionieren. Spätestens seitdem die USA im Jahre 2007[4] und im Jahre 2011 auch Deutschland[5] jeweils Cyber-Abwehrzentren gegründet und EU und USA in „Cyber-Manövern" den „digitalen Bündnisfall"[6] proben, tobt in den Medien der „Cyberwar",[7] der „Krieg 2.0",[8] wobei mit Stuxnet der „digitale Erstschlag" erfolgt,[9] und „Armeen von Zombie-Rechnern"[10] im Einsatz seien.

---

[1] Tagesspiegel vom 24.6.2011, online abrufbar unter http://www.tagesspiegel.de/meinung/sabotagewaffe-stuxnet-der-krieg-der-computer/1943838.html [zuletzt abgerufen am 15.11.2014].

[2] derStandard.at Webstandard-Feature vom 10.2.2011, online abrufbar unter http://derstandard.at/1296696529107/WebStandard-Feature-Stuxnet-Auf-der-Spur-der-unsichtbaren-Superwaffe [zuletzt abgerufen am 15.11.2014].

[3] Der Spiegel, Ausgabe 32/2011, 94 ff.

[4] heise.de vom 14.6.2007, online abrufbar unter http://heise.de/-139507 [zuletzt abgerufen am 15.11.2014].

[5] heise Security vom 1.4.2011, online abrufbar unter http://heise.de/-1220106 [zuletzt abgerufen am 15.11.2014].

[6] Spiegel online vom 3.11.2011, online abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/cyber-manoever-eu-und-usa-ueben-den-digitalen-buendnisfall-a-795604.html [zuletzt abgerufen am 15.11.2014].

[7] FAZ vom 5.12.2010, online abrufbar unter http://www.faz.net/-gsi-xpa5; Die Zeit Nr. 18/2012 vom 26.4.2012, online abrufbar unter http://www.zeit.de/2012/18/Interview-Cyber-Security [zuletzt abgerufen am 15.11.2014].

[8] Die Zeit, Ausgabe 40/2010, online abrufbar unter http://www.zeit.de/2010/40/Stuxnet-Computerwurm [zuletzt abgerufen am 15.11.2014].

[9] FAZ vom 22.9.2010, online abrufbar unter http://www.faz.net/-gsi-xua1 [zuletzt abgerufen am 15.11.2014].

Solche Analogien sind hilfreich, um ein erstes Verständnis für die Phänomenologie IT-spezifischer Bedrohungen zu entwickeln. Da jedoch solche Vergleiche nie in jeder Hinsicht passen, dürfen sie nicht handlungsleitend sein, wenn es darum geht, den Umgang mit bestimmter Software unter Strafe zu stellen. Computerprogramme können nicht einfach mit Kriegswaffen wie Drohnen oder anderer Hardware gleichgesetzt werden[11] – auch wenn gelegentlich ein Computerprogramm zu kriegerischen Zwecken eingesetzt werden mag. Deshalb müssen die Eigenheiten der IT-Sicherheit berücksichtigt werden, wenn eine angemessene Kriminalisierung des Umgangs mit gefährlichen Computerprogrammen erreicht werden soll.

In diesem 1. Teil der Arbeit wird aufgezeigt, dass die IT-Sicherheit vom Phänomen des Dual-Use bestimmt wird. In einem ersten Schritt wird Dual-Use als Phänomen vorgestellt und erörtert, in welchen Ausprägungen Dual-Use im Software-Strafrecht entsteht (I.). Im zweiten Schritt wird gezeigt, warum das Dual-Use-*Phänomen* für den Gesetzgeber bei der Schaffung maßvoller, aber effektiver Strafnormen zur Dual-Use-*Problematik* wird (II.).

Die Begriffe, die hier entwickelt werden, sind von zentraler Bedeutung für die Arbeit. Insbesondere die beiden Ausprägungen des Dual-Use-Phänomens sind grundlegend für die spätere rechtspolitische Würdigung und den Vergleich der Regelungstechniken im 3. und 4. Teil dieser Arbeit. Dort wird entscheidend sein, ob die einzelnen Regelungstechniken in den verschiedenen Ausprägungen des Dual-Use-Phänomens zu verständlichen (Rechtsklarheit) und vertretbaren (Legitimation) Ergebnissen führen.

I. Das Dual-Use-Phänomen

Der Begriff des Dual-Use entstammt nicht der Informationstechnik, sondern dem Bereich der Kontrolle von Kriegswaffen und Rüstungsgütern. Von dort wurde er verallgemeinert und dehnte sich in andere Rechtsgebiete aus (A.). Im Software-Strafrecht, also dem Recht zur strafrechtlichen Kontrolle gefährlicher Computerprogramme, bezeichnet der Begriff zwei verschiedene Ausprägungen des Phänomens (B.).

---

[10] Spiegel online vom 1.7.2011, online abrufbar unter http://www.spiegel.de/netzwelt/web/schadsoftware-tdl4-kriminelle-ruesten-armee-der-zombie-rechner-auf-a-771724.html [zuletzt abgerufen am 15.11.2014].

[11] So aber der Spiegel, Ausgabe 43/2011, 18, online abrufbar unter http://www.spiegel.de/spiegel/print/d-81136813.html [zuletzt abgerufen am 15.11.2014].

A. Dual-Use im Recht zur Kontrolle der Kriegswaffen und Rüstungsgüter

Herstellung, Handel und insbesondere Export von Kriegswaffen und übrigen Rüstungsgütern sind durch strenge Kontrollregime geregelt.[12] Da aber in kriegerischen Konflikten von Heugabeln und Messern bis hin zu Kampfhubschraubern und U-Booten eine Vielzahl von Gütern eingesetzt werden kann, müssen normative Abstufungen vorgenommen werden, um unterschiedlich strenge Kontrollregime an unterschiedliche Gegenstände zu knüpfen.

Das Recht der Kriegswaffen- und Rüstungsgüterkontrolle differenziert daher zwischen Kriegswaffen, die allein militärischen Zwecken dienen, und sogenannten Dual-Use-Gütern, die sowohl militärischen als auch zivilen Zwecken dienen können. Die EG-Dual-Use-Verordnung (Verordnung 498/2009/EG) spricht in der deutschen Fassung von „Gütern mit doppeltem Verwendungszweck" und definiert entsprechend:

> „Güter mit doppeltem Verwendungszweck" [sind] Güter, einschließlich Datenverarbeitungsprogramme und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können; darin eingeschlossen sind alle Waren, die sowohl für nichtexplosive Zwecke als auch für jedwede Form der Unterstützung bei der Herstellung von Kernwaffen oder sonstigen Kernsprengkörpern verwendet werden können.[13]

Im Recht der Kriegswaffen- und Rüstungsgüterkontrolle drückt der Dual-Use-Begriff also aus, dass ein Gegenstand objektiv so beschaffen ist, dass er sowohl für eine militärische als auch für eine zivile (Dual) Verwendung (Use) infrage kommt. Freilich muss die zivile Verwendung hierbei der Eigenart des Gegenstandes entsprechen: Dass man einen militärischen Flugzeugträger auch zivil als Museumsschiff nutzen kann, macht ihn nicht zum Dual-Use-Gut.[14] Der deutsche Terminus der Güter mit doppeltem Verwendungszweck rückt statt der doppelten Verwendbarkeit den doppelten Verwendungs*zweck* in den Fokus und macht damit deutlich, dass es bei der Bewertung des Umgangs mit solchen Gütern maßgeblich auf den Handelnden und die Zwecke, die er subjektiv verfolgt, ankommt.

Dieser militärische Dual-Use-Begriff wurde mehr und mehr verallgemeinert, sodass zuletzt „Dual-Use" in allerlei Konstellationen verwendet wurde, um etwas objektiv Ambivalentes zu bezeichnen. Das OLG Düsseldorf sprach zuletzt sogar im

---

[12] Zur detaillierten Analyse der Regelungen von GG, KWKG, AWG und AWV siehe unten Teil 3, III.

[13] *Schneier* berichtet allerdings, dass der Großteil der Güter, die tatsächlich militärisch verwendet werden, speziell hierfür entworfen oder umgebaut werden muss. Das gelte selbst für Toiletten des Militärs, siehe *Schneier*, America's Dilemma, wired.com am 5.1.2008, abrufbar unter http://archive.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0501 [zuletzt abgerufen am 15.11.2014].

[14] Beispiele bei *Kalinowski*, Zivil-militärisches Dual-Use am Beispiel des iranischen Nuklearprogramms, online abrufbar unter http://www.znf.uni-hamburg.de/Folien230408.pdf [zuletzt abgerufen am 15.11.2014].

Zusammenhang mit § 13 BGB davon, dass die „Regeln des Dual-Use“[15] anwendbar seien, wenn festzustellen ist, ob ein Rechtsgeschäft zum Zwecke einer gewerblichen oder selbstständigen beruflichen Tätigkeit abgeschlossen worden ist. Mit den „Regeln des Dual-Use“ meinte das OLG Düsseldorf offenbar allein die anschließend aufgestellte Faustregel, dass bei mehreren Zwecken derjenige maßgeblich ist, der die übrigen überwiegt. Mit dem Dual-Use-Begriff des Rechts zur Kontrolle der Kriegswaffen und Rüstungsgüter hat dies freilich nur noch wenig zu tun.

B. Dual-Use im Recht zur Kontrolle gefährlicher Computerprogramme

In mehreren Delikten des deutschen Computerstrafrechts stehen bestimmte Umgangsformen mit gefährlichen Computerprogrammen unter Strafe. Diesem wachsenden gesetzgeberischen Interesse für Software als Tatwerkzeug folgend, wird mittlerweile das Software-Strafrecht als eigenes Teilrechtsgebiet aufgefasst.[16] Dabei sind Software-Delikte bislang regelmäßig als Teilaspekt oder als Ergänzung zu Harmonisierungs- und Gesetzesinitiativen mit jeweils anderen Schwerpunktsetzungen (Urheberrecht, Schutz des Euro, Bekämpfung der Fälschung bargeldloser Zahlungsmittel etc.) normiert worden. Selbst in der Cybercrime Convention stellt das Software-Delikt des Art. 6 eine bloße Ergänzung zur Harmonisierung der eigentlichen CIA-Delikte dar.[17] Ein europäisches Instrument oder ein Gesetz „über den Umgang mit gefährlichen Tatwerkzeugen, insbesondere Computerprogrammen“, das diesen Bereich umfassend regulieren würde, gibt es bislang nicht. Dennoch soll im Folgenden vom Software-Strafrecht und von Software-Delikten gesprochen werden. Denn bei all diesen Delikten besteht nicht nur in der gesetzgeberischen Zielsetzung große Ähnlichkeit, sondern auch in den Herausforderungen aufgrund des IT-spezifischen Dual-Use-Phänomens.

In diesem Kapitel werden zunächst exemplarisch „gefährliche Computerprogramme“ vorgestellt, die im Fokus des Gesetzgebers stehen und diesen zur Schaffung von Software-Delikten veranlassten (1.). Sodann wird dargestellt, dass sich das Dual-Use-Phänomen bei Computerprogrammen in zwei verschiedenen Ausprägungen zeigt (2.). Diese Ausprägungen müssen für die Bewertung der Regelungstechniken (siehe 3. und 4. Teil dieser Arbeit) zwingend auseinandergehalten werden.

---

[15] Siehe OLG Düsseldorf, Urteil vom 17.7.2009, 16 U 168/08 Rn. 53.

[16] Siehe *Popp*, GA 2008, 375 ff., der den Begriff „Software-Delikt“ geprägt hat.

[17] Dies wird schon daraus ersichtlich, dass gegen Art. 6 CCC Vorbehalte zulässig sind, Art. 42 CCC.

1. Gefährliche Computerprogramme als Regelungsmaterie

Regelungsmaterie der Software-Delikte ist der Umgang mit bestimmten Computerprogrammen. Die Gesetz- und Normgeber stufen einzelne Computerprogramme nach bestimmten Kriterien als besonders gefährlich ein und stellen folglich insbesondere deren Herstellung, Beschaffung und Verbreitung unter Strafe. Welche Schadsoftware die Gesetzgeber bei der Schaffung von Software-Delikten konkret vor Augen hatten und worin ihr spezifisches Gefährdungspotential liegt, soll hier in einem groben Überblick dargestellt werden. Die Darstellung erfolgt dabei anwendungsorientiert. Technische Details werden nur erläutert, soweit sie der späteren juristischen Diskussion zuträglich sind. Insgesamt lassen sich den Software-Delikten zwei große Einsatzfelder für Schadsoftware zuordnen: der Bereich der geschützten Inhalte des UrhG und des ZKDSG (a)) sowie der Bereich des Hacking im engeren Sinne (b)).

a) Geschützte Inhalte: Keygens, Cracks, Fixes

Im Bereich der Urheberrechte und verwandten Schutzrechte werden die geschützten Inhalte in der Regel mit technischen Schutzmaßnahmen vor unbefugter Verwertung geschützt: Teilweise enthalten DVDs, Audio-CDs und Blu-ray-Discs unmittelbar Kopierschutzmaßnahmen, die das Kopieren der Disc verhindern, andere Mechanismen sollen sicherstellen, dass beim Aufruf des geschützten Inhalts keine Kopie, sondern die Original-DVD/CD/BD eingelegt ist. Wiederum andere Sicherungen setzen beim Kopiervorgang an, indem sie beim Versuch, eine Kopie des geschützten Materials herzustellen, signalisieren, dass der Rechtsinhaber in eine solche Vervielfältigung nicht eingewilligt hat, sodass das Brennprogramm den Kopiervorgang nicht startet.[18]

Bei geschützter Software, also insbesondere Office-Programmen, Computerspielen, Bild- und Videobearbeitungsprogrammen, die auf dem Computer des Nutzers installiert werden müssen, bieten sich weitere Möglichkeiten zur Sicherung der Interessen des Rechtsinhabers. Diese setzen meist bei der Programminstallation, beim Start und während der Nutzung des Programms an. Bei der Installation wird der Nutzer regelmäßig nach einer Seriennummer gefragt, die getrennt vom eigentlichen Datensatz etwa in einem dazugehörigen Handbuch oder der Originalverpackung zu finden ist. Hat er sich eine illegale Kopie verschafft, also etwa die Installationsdateien aus dem Internet heruntergeladen, so steht ihm die Seriennummer nicht zur Verfügung und das Programm lässt sich nicht installieren. Beim Start des Programms lassen sich Kopierschutzmaßnahmen dergestalt einbinden, dass das Programm zunächst prüft, ob die Original-DVD eingelegt ist oder ob die Installation von einer Original-DVD erfolgt ist. Alternativ kann das Programm

---

[18] Vgl. *Hänel*, Die Umsetzung des Art. 6, S. 115 ff.

auch eine Internetverbindung zu einem Server des Softwarelieferanten oder des Kopierschutzanbieters aufbauen und dort abgleichen, ob die auf dem Computer installierte Version wirksam und rechtmäßig lizenziert wurde und erst im Anschluss an eine solche Überprüfung das Computerprogramm aktivieren. Neuere Kopierschutzmaßnahmen setzen zudem in der Anwendung des Programms an: Das Programm lässt sich nur ausführen, solange eine Internetverbindung zum Server des Herstellers oder Kopierschutzanbieters besteht, sodass dieser die rechtmäßige Lizenzierung des Programms permanent überprüfen kann (sog. Online-DRM).[19]

Gegen jeden der genannten Schutzmechanismen gibt es jedoch Maßnahmen. Gegen Sicherungen, die beim Start des Programms ansetzen, lassen sich sogenannte *Fixes* oder *Cracked Exes* einsetzen: Hierbei handelt es sich um einzelne Dateien, die nach der Installation des gewünschten Programms in den Programmordner kopiert werden, wo sie einzelne Originaldateien ersetzen. Bei den ersetzten Dateien handelt es sich meist um die Exe-Datei, die das Programm startet. Bei der *Cracked Exe* handelt es sich um eine Kopie der originalen Exe-Datei, wobei die Befehle entfernt worden sind, die beim Start des Programms den Kopierschutzmechanismus auslösen. Gegen ein Online-DRM werden sogenannte Fixes eingesetzt, die einen Server emulieren, also dem geschützten Programm vorspiegeln, es würde Kontakt zu dem Server des Rechtsinhabers halten, obwohl es tatsächlich gar keine Online-Verbindung aufbaut.[20]

Die Seriennummernabfrage kann man mit Keygens und Serials umgehen. Serials sind keine Programme, sondern einfach Seriennummern, die von dem Cracker abgetippt und zur Verfügung gestellt werden. Bis vor einigen Jahren war es noch gängig, mit dem geschützten Programm auch eine passende Seriennummer in einer .nfo-Datei zu liefern, die der Nutzer dann bei der Installation auf seinem PC verwenden konnte. Diese Methode wurde jedoch in dem Moment unbrauchbar, ab dem jede Seriennummer nur noch einmalig verwendet werden konnte (etwa weil bei der Verwendung der Seriennummer eine Verbindung mit dem Server des Rechtsinhabers hergestellt und sichergestellt wurde, dass diese Seriennummer noch unbenutzt war). Seitdem haben sich Keygens etabliert. Dies sind kleine Programme, die darauf basieren, dass ihr Hersteller den Algorithmus kennt, nach dem der Rechtsinhaber seine Seriennummern generiert. Ist dieser Algorithmus bekannt, so können mithilfe des Keygens beliebig viele Seriennummern generiert werden. In der zentralen Datenbank des Rechtsinhabers werden diese dann nicht als gefälscht erkannt, weil dort nur überprüft wird, ob sie dem zugrunde liegenden Algorithmus entsprechen und noch unbenutzt sind.

---

[19] Einen Überblick über die Funktionsweisen der gängigsten Kopierschutzverfahren SecuROM, StarForce, SafeDisc sowie die genannte Internetaktivierung und die Seriennummer gibt *Mayer-Wegelin*, JurPC Web-Dok. 28/2009, Abs. 9 ff.

[20] Vgl. Toms Hardware vom 23.4.2010, online abrufbar unter http://www.tomshardware.com/news/assassins-creed-crack-hack-drm-ac2,10260.html [zuletzt abgerufen am 15.11.2014].

Gegen die Schutzmechanismen, die direkt am Datenträger ansetzen, also insbesondere Abspiel-, Brenn- und Kopierschutzmechanismen, gibt es Treiber, die entweder als selbstständige Programme verfügbar oder direkt in Brennprogramme implementiert sind. Beispiele dafür sind *Yasu* und *AnyDVD*, die alle gängigen Kopierschutzmechanismen und Benutzungsbeschränkungen quasi ausschalten. Der *AnyDVD*-Hersteller *Slysoft* stellt diese Eigenschaften des Treibers auf seiner Homepage explizit in den Vordergrund.[21] Anders verhält es sich beim *VLC media player*, einem kostenlosen, bekannten und beliebten Computerprogramm zur Wiedergabe von Multimedia-Inhalten,[22] insbesondere Audiodateien, Videodateien, DVDs, Video-CDs, Audio-CDs, Netzwerk-Streams und so weiter. Geschätzt wird das Programm vor allem dafür, dass es „schlank" ist, also wenige Ressourcen beansprucht, und beinahe alle Audio- und Videoformate wiedergeben kann, ohne auf zusätzliche Codecs Packs angewiesen zu sein. Neben der Wiedergabe ermöglicht es auch die Konvertierung von Mediendateien, das Implementieren von Untertiteln, das Verschieben von Bild- und Tonspur,[23] das nachträgliche Verändern der Medienlautstärke, das Abspielen unvollständiger Mediendateien ebenso wie das Abspielen gepackter Mediendateien und vieles mehr.[24] Der *VLC media player* enthält aber auch die Programmbibliothek *libdvdcss*, die es ermöglicht, die CSS-Verschlüsselung von DVDs zu umgehen und damit beispielsweise die Länderkodierung einer DVD mittels Brute-Force-Attacke auszuhebeln.[25] Die CSS-Verschlüsselung stellt eine wirksame technische Schutzmaßnahme im Sinne des § 95a UrhG dar, sodass deren Umgehung gemäß § 108b Abs. 1 i.V.m. § 95a Abs. 1 UrhG strafbar ist.[26]

Im Bereich zugangskontrollierter Dienste, also insbesondere dem verschlüsselten Pay-TV, wird in der Regel eine Kombination aus Hardware und Software zum Schutz des Dienstes verwendet: Hier wird das Signal verschlüsselt ausgesandt und auf einem bestimmten Receiver mittels eines Schlüssels, der sich auf einer Smart-

---

[21] „AnyDVD ist ein Treiber, der im Hintergrund automatisch und unbemerkt eingelegte DVD-Filme entschlüsselt", „Entfernt Kopierschutz (CSS) und Ländercode (RPC) von DVDs", „Entfernt analogen Kopierschutz (Macrovision)", siehe http://www.slysoft.com/de/anydvd.html [Stand: 14.5.2012, nunmehr abgewandelt, zuletzt abgerufen am 16.11.2014].

[22] Auf der Download-Seite des deutschsprachigen Computer-Portals CHIP Online wird der VLC media player bei über 180.000 Bewertungen von 98 % positiv bewertet. http://www.chip.de/downloads/VLC-media-player-32-Bit_13005928.html [Stand: 4.3.2013, zuletzt abgerufen am 16.11.2014].

[23] Vgl. die Angaben auf der Herstellerseite http://www.videolan.org/vlc/features.html [zuletzt abgerufen am 16.11.2014].

[24] Siehe http://www.chip.de/downloads/VLC-media-player-32-Bit_13005928.html, wo der Funktionsumfang als zu groß bezeichnet wird, als dass er dort hinreichend wiedergegeben werden könnte [Stand: 4.3.2013, zuletzt abgerufen am 16.11.2014].

[25] http://www.videolan.org/developers/libdvdcss.html; http://en.wikipedia.org/wiki/Libdvdcss, [zuletzt abgerufen am 15.11.2014].

[26] Siehe nur OLG München GRUR-RR 2009, 86 f.; Leupold/Glossner-*Wiebe*, Teil 3 Rn. 218; näher zur rechtlichen Beurteilung unten Teil 3, I.B.4.a).

card befindet, entschlüsselt.[27] Auch hier werden entsprechende Tools zum unautorisierten Empfang des Signals gehandelt. Mittels spezieller Programme kann man sodann das Betriebssystem eines unautorisierten Receivers für den unautorisierten Empfang aufrüsten (patchen) und einen Smartcard-Rohling mit den erforderlichen Schlüsseln bespielen.[28]

Häufig werden solche Umgehungstools von spezialisierten Hacker-Gruppierungen zusammen mit den geschützten Inhalten zugänglich gemacht („Release").[29] Dazu wird den Original-Inhalten ein Ordner hinzugefügt, in dem sich der benötigte *Crack* befindet. Solche Ordner heißen dann häufig „Crack" oder tragen den Namen der Hacker-Gruppierung, die den Release erstellt hat. Original-Inhalt und Crack-Ordner werden dann in einer Image-Datei (meist eine *Media Descriptor File* mit der Endung .mdf oder ein ISO-Abbild mit der Endung .iso) zusammengeführt. Da diese Datei aufgrund ihrer Größe für eine sichere und schnelle Verbreitung im Internet ungeeignet ist, wird sie häufig komprimiert und in kleinere Einzeldateien aufgeteilt, welche dann zum Download gestellt werden. Wer sich daraufhin die Original-Inhalte illegal besorgen möchte, kann die gepackten Dateien herunterladen, entpacken und das nun vorhandene Image mithilfe eines Emulators „mounten". Ein Emulator ist ein (vielfach kostenlos verfügbares) Programm, mit dem sich virtuelle Laufwerke betreiben lassen. Das bedeutet, dass dem Computer ein physikalisches Laufwerk vorgespiegelt wird, das sich aber softwareseitig steuern lässt. Im Explorer wird also ein weiteres Laufwerk angezeigt, dessen Inhalt man über den Emulator steuert.[30] Wenn man bei einem virtuellen Laufwerk ein DVD-Image „mountet", entspricht dies folglich dem Einlegen einer DVD in ein physikalisches Laufwerk.

In dem „gemounteten" Laufwerk findet der Downloader nun den gesamten Inhalt der Original-DVD sowie den Crack-Ordner. In dem Crack-Ordner befinden sich dann alle zur Umgehung notwendigen Dateien sowie häufig eine .nfo-Datei (zu öffnen bspw. mit dem *Editor* von Windows), in der sich neben Informationen zum heruntergeladenen Computerprogramm und verschiedenen Statements des Crackers (Grüße, Provokationen, „Stellenangebote", pp.) auch regelmäßig eine Installations- und Crackanleitung befindet. Sollte der Release keinen Crack enthalten, sondern etwa nur aus einer 1:1-Kopie der geschützten DVD bestehen („untouched release"), muss der illegale Downloader sich den Crack separat besorgen.

---

[27] Vgl. *Federrath*, in: Dressel/Scheffler, ZKDSG, S. 6 ff.

[28] A.a.O., S. 15 ff.

[29] Bekannte Hacker-Gruppierungen, die sich auf Releases spezialisiert haben, sind etwa POSTMORTEM, Razor1911, SKiDROW, PARADOX, Fairlight, Hatred (früher: DEViANCE) und Unleashed.

[30] Zeitgemäße Emulatoren wie etwa DAEMON Tools können bis zu 32 virtuelle Laufwerke gleichzeitig betreiben. Jedes Laufwerk lässt sich dabei unabhängig von den anderen als HD-, CD-, DVD-, oder BluRay-Laufwerk betreiben.

Der Download erfolgt über P2P-Netzwerke, Torrents, FTPs und im Usenet, sowie im WWW über große File- oder Sharehoster. Diese sind in der Regel nicht durchsuchbar, jedoch existieren große Internetcommunitys, deren Mitglieder in Online-Foren die Download-Links zu den Releases auf den Filehostern bereitstellen. Solche Foren sind in der Regel halböffentlich, das heißt, jedermann kann sich mit einer gültigen E-Mail-Adresse dort registrieren und hat dann Zugriff auf die Inhalte des Forums. Die größten deutschsprachigen Foren dieser Art sind wahrscheinlich www.boerse.bz und www.mygully.com. Daneben gibt es große Portale, die nur Cracks und Keygens zur Verfügung stellen, beispielsweise www.gamecopyworld .com, www.megagames.com sowie www.keygen.us.

b) Hackingtools im engeren Sinne

Als Hackingtools im engeren Sinne sollen hier solche Computerprogramme verstanden werden, die bei Aktivitäten im Sinne des Kern-Computerstrafrechts Verwendung finden. Zum Kern-Computerstrafrecht sollen Angriffe auf Vertraulichkeit, Integrität und Verfügbarkeit von Daten zählen („CIA-Delikte“) sowie der gesamte Bereich des Computerbetrugs.

Zu einer ersten Gruppe „klassischer“ Hackingtools gehören zunächst Spähprogramme, die darauf angelegt sind, Informationen über ein Zielsystem einzuholen. Hierzu zählen insbesondere Portscanner, Vulnerabilty Scanner und Sniffer. Portscanner ermitteln, welche Dienste auf dem Zielsystem auf welchem Port aktiv sind, also auf welchen Wegen Daten hinein- und herausfließen. Vulnerability Scanner erfassen darüber hinaus, ob auf dem Zielsystem bereits bekannte Schwachstellen vorhanden sind. Sniffer sind Programme, die den Datenverkehr in einem Netzwerk mitschneiden.[31]

In einer zweiten Gruppe von Hackingtools können sogenannte Crackingtools zusammengefasst werden. Mit ihrer Hilfe können Passwörter und Verschlüsselungen geknackt werden. Dabei können solche Tools auf verschiedene Methoden zurückgreifen, etwa indem sie alle logisch möglichen Passwörter (sogenannte *Brute-Force-Attacke*) oder besonders häufige Passwörter auf Grundlage eigens hierfür erstellter Listen ausprobieren. Neuere Tools greifen auf die sogenannte Pass-the-Hash-Methode zurück, bei der das Tool nicht das Passwort selbst benutzt, sondern den Hashwert, der aus dem Passwort generiert und in der Datenbank abgelegt wird.[32]

---

[31] Vgl. *Lindner*, Stellungnahme zum Gesetzentwurf BT-Drucks. 16/3656, S. 2 f.

[32] Siehe *Eweida*, Pass-the-hash attacks: Tools and Mitigation, S. 2 ff., online abrufbar unter http://www.sans.org/reading_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation_33283 [zuletzt abgerufen am 15.11.2014].

Eine dritte Gruppe typischer Hackingtools sind Würmer.[33] Ihr Charakteristikum besteht darin, dass sie sich selbst replizieren, sich also innerhalb des infizierten Computersystems oder auf weitere Computersysteme kopieren. Je nach den Intentionen des Programmierers kann ein Wurm etwa Schadensroutinen ausführen, Text verbreiten, Daten protokollieren oder alle infizierten Computer an einen Command-and-Control-Server rückkoppeln, über den sich sodann alle infizierten Computer als Netzwerk fernsteuern lassen – als sogenanntes Botnet.[34]

Da Botnets vielen Zwecken dienen können, werden sie gegenwärtig als eine der größten Bedrohungen der IT-Sicherheit angesehen.[35] So kann der Betreiber des Botnets über den Command-and-Control-Server alle Bots anweisen, Spam zu verschicken oder Bezahlvorgänge auf dem befallenen PC zu überwachen und dabei etwa Kreditkartendaten auszulesen und an den Botnet-Betreiber zurückzumelden. Botnets werden häufig auch für DDoS-Angriffe verwendet. Auch in diesem Kriminalitätsbereich ist die Arbeitsteilung mittlerweile so weit fortgeschritten, dass Botnets mitunter stundenweise gemietet werden können, etwa um DDoS-Angriffe auf eine bestimmte Seite auszuführen. Solche Angriffe sind häufig „maßgeschneidert“: Datum, Uhrzeit, Dauer und Art der Angriffe sind modulartig nach Belieben wählbar.[36] Auch das Bundesamt für Sicherheit in der Informationstechnik weist auf seinen Bürgerseiten intensiv auf die Gefahren durch Botnets hin[37] und hat in Kooperation mit dem Verband der deutschen Internetwirtschaft *eco* ein Anti-Botnet-Beratungszentrum gegründet, welches den Bürgern dabei hilft, ihre Computer darauf zu untersuchen, ob sie unbemerkt Teil eines Botnets geworden sind und gegebenenfalls vorhandene Infektionen auf dem jeweiligen Computer beseitigt.[38]

Freilich ist jede funktionale Systematisierung von Schadsoftware angreifbar. In der Regel kombinieren einzelne Computerprogramme auch mehrere Angriffsformen, sodass ein Programm etwa eine Sniffing-Funktion mit einer Cracking-Funktion kombiniert, auf diese Weise eine Schwachstelle auf dem Zielsystem ausnutzt, um dort Code zu hinterlegen, der das System an einen Command-and-Control-Server koppelt und sich selbst weiterverbreitet.[39] Solche Kombinationen werden als Exploits bezeichnet, weil sie eine erkannte Sicherheitslücke automatisch

---

33 Vgl. *Pohl*, DuD 2007, 684.

34 *Brodowski/Freiling*, Cyberkriminalität, S. 68 ff.

35 *Bernnat/Bauer/Zink/Bieber/Jost*, IT-Sicherheitsbranche in Deutschland, S. 236 ff.

36 Vgl. „DDoS-Attacken auf dem Vormarsch“, http://www.all-about-security.de/security-artikel/applikations-host-sicherheit/applikationen-web-services/artikel/14127-ddos-attacken-auf-dem-vormarsch/ [zuletzt abgerufen am 15.11.2014].

37 Siehe https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html [zuletzt abgerufen am 15.11.2014].

38 Siehe https://www.botfrei.de/ [zuletzt abgerufen am 15.11.2014].

39 Siehe auch *Lindner*, Stellungnahme zum Gesetzentwurf BT-Drucks. 16/3656, S. 4.

ausnutzen. Sie werden in sogenannten Exploit Frameworks teilweise im Baukastensystem zur Verfügung gestellt.[40]

Schon diese exemplarische Auflistung zeigt, dass Computerprogramme für die geschützten Rechtsgüter durchweg ein hohes Gefährdungspotential aufweisen. Mit ihrer Hilfe lassen sich Angriffe auf geschützte Rechtsgüter zum einen automatisiert durchführen, zum anderen wird das Bedrohungspotential durch Netzwerkeffekte erheblich verstärkt: Kleine Angriffe lassen sich millionenfach duplizieren und koordinieren, wodurch sie – etwa im Falle von Botnetzen – ein gewaltiges Schadenspotential entfalten können.

2. Ausprägungen des Dual-Use-Phänomens bei gefährlicher Software

Das Dual-Use-Phänomen zeigt sich bei gefährlicher Software unter zwei Aspekten, die im Folgenden erörtert werden: ein Multifunktions- (1.) und ein Mehrzweckaspekt (2.). Multifunktionsaspekt bedeutet, dass das Computerprogramm nicht nur schädliche, sondern auch nützliche Funktionen aufweist. Mehrzweckaspekt bedeutet, dass eine schädliche Funktion des Computerprogramms nicht nur zu kriminellen Zwecken, sondern auch zu Test- und Analysezwecken genutzt werden kann und genutzt wird.

a) Erste Ausprägung des Dual-Use-Phänomens: der Multifunktionsaspekt

Der erste Aspekt des Dual-Use-Phänomens resultiert aus der Multifunktionalität von Computerprogrammen. Er betrifft solche Computerprogramme, die unter *mehreren* Funktionen auch *eine* Funktion haben, die *ausschließlich schädlich* ist. Am oben genannten Beispiel des *VLC media player* wird dies deutlich: Das Programm hat eine Vielzahl von Funktionen, etwa das Abspielen von Videodateien, DVDs, Video-CDs, Audio-CDs und Netzwerk-Streams. All diese Funktionen sind nützlich und grundsätzlich legal. Zusätzlich hat das Programm aber auch die Funktion, die CSS-Verschlüsselung von DVDs zu umgehen. Diese Verschlüsselung darf aber als „technische Schutzmaßnahme“ nicht umgangen werden, § 95a Abs. 1 UrhG. Damit hat der *VLC media player* sowohl legale, unschädliche und nützliche Funktionen, als auch eine rechtswidrige, schädliche Funktion. In diesem Fall kann von einem Dual-Use-Programm gesprochen werden.

Dieser Multifunktionsaspekt des Dual-Use-Phänomens wirft bei der Schaffung eines Software-Delikts zunächst die Frage auf, ob das Verhältnis verschiedener

---

[40] *Lindner*, Stellungnahme zum Gesetzentwurf BT-Drucks. 16/3656, S. 4; siehe auch *Muncan/Schreiber*, DuD 2009, 220 f.; *Pohl*, DuD 2007, 685.

Funktionen des Computerprogramms zueinander grundsätzlich eine Rolle spielen soll. Bejaht man dies, so stellt sich die Frage, nach welchen Kriterien die schädliche Funktion zu den übrigen Funktionen ins Verhältnis gesetzt werden soll und ab welcher Schwelle der Umgang mit dem entsprechenden Computerprogramm tatbestandsmäßig sein soll. In den Tatbeständen des Software-Strafrechts finden sich mehrere rechtstechnische Modelle, die diesen Multifunktionsaspekt des Dual-Use-Phänomens im objektiven Tatbestand angehen.[41]

b) Zweite Ausprägung des Dual-Use-Phänomens: der Mehrzweckaspekt

Das Dual-Use-Phänomen zeigt sich aber auch darin, dass dieselbe technische Funktion eines Computerprogramms, die einerseits zu Angriffszwecken gegen ein Zielsystem verwendet werden kann, andererseits auch zu Simulationszwecken auf einem eigenen Testsystem eingesetzt werden kann. Es kommt also darauf an, welche Zwecke der Nutzer mit dem Computerprogramm verfolgen will, weshalb hier von einem Mehrzweckaspekt gesprochen wird.

Allen Schadprogrammen ist nämlich gemein, dass sie Sicherheitslücken in den angegriffenen Systemen ausnutzen. Jedes IT-System hat Schwachstellen, die jedoch vom Programmierer oder Systemadministrator beseitigt werden können, sobald sie entdeckt werden. Folglich liegt eine effektive Strategie zur Bekämpfung krimineller Angriffe darin, die Schwachstellen eines Systems noch vor dem Täter aufzuspüren, zu analysieren und zu beseitigen.[42] Deshalb empfiehlt das BSI bereits seit 1992, im Rahmen des IT-Sicherheitsmanagements solche Analysen vorzunehmen.[43] Heutzutage werden bei Sicherheitsstudien standardmäßig Schutzbedarfs-, Schwachstellen- und Bedrohungsanalysen durchgeführt.[44]

Eine wichtige Rolle spielen dabei simulierte Eindringversuche, sogenannte *Penetration Tests*. Hier schlüpft ein IT-Sicherheitsbeauftragter in die Rolle eines Angreifers, um Sicherheitslücken des betreuten Systems zu finden[45] und den Widerstandswert des Systems gegenüber Angriffen von Externen oder Internen zu beur-

---

[41] Eingehend dazu unten Teil 3, I.B. und II.B.

[42] Vgl. *Brodowski/Freiling*, Cyberkriminalität, S. 83 ff.; selbstverständlich ist es kein Fall von Dual-Use, wenn im Vorfeld einer Online-Durchsuchung Schwachstellenanalysen auf dem Zielsystem vorgenommen werden, vgl. zur Technik *Fox*, DuD 2007, 828 ff.; *Pohl*, DuD 2007, 685 ff.

[43] Vgl. BSI, IT-Sicherheitshandbuch, Kapitel 4.1.

[44] *Müller*, IT-Sicherheit, S. 453; *Schreiber*, Kosten und Nutzen von Penetrationstests, S. 4 f.

[45] Siehe *Aharoni*, Metasploit, S. 27 ff.; *Kersten/Reuter/Schröder*, IT-Sicherheits-management, S. 269; *Schreiber/Heinrich*, Penetrationstests als Instrument zur Qualitätssicherung, S. 453 f.

teilen.[46] Einige IT-Sicherheits-Zertifikate sehen solche Angriffssimulationen zwingend vor.[47] Dementsprechend werden offensive Methoden des *Penetration Testing* auch an Hochschulen gelehrt.[48]

Da Kriminelle und IT-Sicherheitsbeauftragte also dasselbe Zwischenziel verfolgen, nämlich das Aufspüren und Nachweisen von Sicherheitslücken, nehmen sie äußerlich dieselbe Handlung vor. Hierfür verwenden sie natürlich auch vergleichbare oder gar dieselben Tools. Der Sinn dieser Computerprogramme liegt einzig darin, Schwachstellen aufzuspüren und auszunutzen. IT-Sicherheitsbeauftragte sind hierauf zwingend angewiesen, um die Ausnutzbarkeit von Schwachstellen zu prüfen.[49] Damit wird ein zweiter Aspekt des Dual-Use-Phänomens ersichtlich, nämlich ein Mehrzweckaspekt: Eine allein schädliche Funktion des Computerprogramms ist zu legitimen Analyse-, Test- und Nachweiszwecken ebenso brauchbar wie zu kriminellen Zwecken. Selbst ein Computerprogramm, das nur eine einzige schädliche Funktion hat, also eine Schadensroutine, muss nicht in krimineller Absicht hergestellt worden sein. Zwar besorgen sich IT-Sicherheitsberater solche Programme häufig auch aus zwielichtigen Quellen, entwickeln sie nötigenfalls aber auch selbst.[50] Zudem handeln IT-Sicherheitsbeauftragte nicht immer im Auftrag der Rechtsgutsträger, etwa wenn sie eine Schwachstelle in einem System festgestellt haben und diese im Rahmen des *Full-Disclosure-Prinzips* veröffentlichen, damit andere Systembetreiber überprüfen können, ob sie auch betroffen sind und gegebenenfalls einstweilige Schutzvorkehrungen gegen Angriffe treffen können.[51]

Der Mehrzweckaspekt ist aber gar nicht auf Analysezwecke begrenzt, sondern zeigt sich grundsätzlich überall, wo mit Einwilligung des Rechtsgutsträgers legitimes Handeln zumindest denkbar ist: etwa bei Fernwartungssystemen, mittels derer man Zugriff auf entfernte, verbundene Computersysteme hat. Spielt man das Programm auf dem Zielsystem auf, um dort Daten zu löschen, so ist dies unproblematisch, solange es mit Einwilligung des Betreibers des Zielsystems etwa im Rahmen eines Fernwartungsvertrags erfolgt. Spielt man dagegen dasselbe Programm auf, um jenseits der Einwilligung des Betreibers Sabotageakte auf dem Zielsystem vorzunehmen, so ist dies keineswegs unproblematisch. Dabei ist die eine Handlung von der anderen zum Zeitpunkt des Aufspielens äußerlich nicht zu unterscheiden.

---

[46] Siehe *Kersten/Reuter/Schröder*, IT-Sicherheitsmanagement, S. 233; *Schreiber*, Kosten und Nutzen von Penetrationstests, S. 4 f.

[47] Siehe *Kersten/Reuter/Schröder*, IT-Sicherheitsmanagement, S. 12; vgl. auch BSI, Durchführungskonzept für Penetrationstests, S. 103 ff.

[48] *Mink*, Der richtige Weg für IT-Sicherheitsausbildung, S. 3 ff.

[49] Siehe *Kersten/Reuter/Schröder*, IT-Sicherheitsmanagement, S. 270; *Müller*, IT-Sicherheit, S. 456; *Vacca*, Computer and Information Security Handbook, S. 388.

[50] Siehe *Lindner*, Stellungnahme zum Gesetzentwurf BT-Drucks. 16/3656, S. 2, 4.

[51] Siehe *Canellopoulou-Bottis*, Disclosing Software Vulnerabilities, S. 258 f.; *Lindner*, Stellungnahme zum Gesetzentwurf BT-Drucks. 16/3656, S. 5; *Vacca*, Computer and Information Security Handbook, S. 391 ff.

Kennt man dagegen die mittelbaren Ziele des Handelnden, drückt sich der Mehrzweckaspekt schon sprachlich aus: Das eine Mal wird das Zielsystem durch das Löschen „gewartet", das andere Mal wird es „kompromittiert". Und auch hinsichtlich des Computerprogramms wird nun differenziert: Spricht man im einen Fall von einem Fernwartungsprogramm, so ist man im anderen Fall geneigt, von einer Backdoor, einem Rootkit oder Trojaner zu sprechen. Damit stellt sich die Frage, wie diese Wertung strafrechtlich normiert werden kann. Denn anders als der Multifunktionsaspekt ergibt sich der Mehrzweckaspekt des Dual-Use nicht aus mehreren unterschiedlichen Funktionen eines Computerprogramms, sodass der Gesetzgeber ersichtlich nicht den Umgang mit einem Löschprogramm unter Strafe stellen kann. Da der Dual-Use hier an *einer* Funktion entsteht, muss der Gesetzgeber einen Weg finden, die Kriterien im Tatbestand niederzulegen, die aus dieser Funktion ein „Warten" oder ein „Kompromittieren" machen.

Der Mehrzweckaspekt des Dual-Use-Phänomens wirft somit die Frage auf, welche subjektiven Ziele der Handelnde verfolgt, welche Zwecke er setzt. Will der Gesetzgeber diesen Mehrzweckaspekt des Dual-Use-Phänomens berücksichtigen, so muss er ein rechtstechnisches Mittel finden, welches das Geschehen konsequent nach den Intentionen des Handelnden unterscheidet. Der Mehrzweckaspekt ist in einigen Tatbeständen auf je unterschiedliche Weise berücksichtigt, in anderen Tatbeständen wird darüber hinweggegangen.[64] Sowohl der Multifunktionsaspekt als auch der Mehrzweckaspekt müssen bei der Schaffung von Software-Delikten beachtet werden. Der Gesetzgeber wird sich zunächst die Frage stellen müssen, ob er jedes Computerprogramm tatbestandlich erfassen will, das irgendeine schädliche Funktion aufweist, sei sie auch nebensächlich (Multifunktionsaspekt). Sodann wird er sich fragen müssen, ob er den Umgang mit einem gefährlichen Computerprogramm stets unter Strafe stellen möchte oder ob er Test- und Analysehandlungen von der Strafbarkeit ausnehmen will (Mehrzweckaspekt).

II. Die Dual-Use-Problematik: Symbolgesetze vs. Chilling Effects

Die zentrale Herausforderung für den Gesetzgeber ist daher, sowohl den Multifunktions- als auch den Mehrzweckaspekt des Dual-Use-Phänomens bei der Erschaffung eines Software-Delikts zu beachten. Er muss also einen Tatbestand schaffen, der einerseits auf unterschiedliche Funktionen des Computerprogramms eingeht (Multifunktionsaspekt), der aber gleichzeitig die subjektive Zwecksetzung des Handelnden hinreichend berücksichtigt (Mehrzweckaspekt). Dabei besteht

---

[64] Eingehend dazu unten Teil 3, I.C. und II.C.

freilich die Gefahr, den Tatbestand des Software-Delikts zu stark einzuschränken, sodass er erhebliche Teile seines Anwendungsbereichs verliert und damit zu einem Symbolgesetz verkommt, das nur scheinbar strafrechtlichen Schutz bietet.[65] Auf der Gegenseite besteht die Gefahr einer Kriminalisierung von Bereichen, die für die IT-Sicherheitsbranche essentiell sind: Wenn den IT-Sicherheitsbeauftragten kein konsequenter Ausweg aus der Kriminalisierung aufgezeigt wird, besteht die Gefahr, dass sie Sicherheitstests nicht mehr im Geltungsbereich des StGB vornehmen. Aus einer solchen Furcht vor Kriminalisierung stellte der Hersteller des Netzwerk-Sniffers KisMAC mit der Einführung des § 202c Abs. 1 Nr. 2 StGB seinen Betrieb in Deutschland ein und zog seine Server ins Ausland ab.[66] Diese Effekte können freilich schon dann eintreten, wenn für IT-spezifische berufstypische Handlungen lediglich die konkrete Furcht entsteht, sie könnten strafbar sein, auch wenn sie es tatsächlich gar nicht sind. Man spricht dann von *Chilling Effects*.[67]

Der Vorwurf der Symbolgesetzgebung erschüttert die Legitimität eines Software-Delikts, weil ein Strafgesetz ohne Anwendungsbereich überflüssig und nicht zu rechtfertigen ist. Ebenso wenig ist eine zu umfassende Kriminalisierung zu legitimieren, und die damit einhergehenden Chilling Effects laufen dem gesetzgeberischen Ziel sogar zuwider, die IT-Sicherheit insgesamt zu stärken. Die beiden Pole der Symbolgesetzgebung und der Chilling Effects sind im Software-Strafrecht durch das Dual-Use-Phänomen miteinander verbunden.

Der Gesetzgeber muss also zwei Probleme vermeiden (Überkriminalisierung und Symbolgesetzgebung), die auf demselben Phänomen beruhen (Dual-Use) und ineinandergreifen. Deshalb ist es gerechtfertigt, von einer Dual-Use-*Problematik* zu sprechen.[68] Dieser Begriff wird dem Rest der Arbeit, namentlich der Analyse der Rechtstechniken, mit denen der Gesetzgeber die Dual-Use-Problematik zu lösen versucht hat[69] sowie deren wertendem Vergleich[70] zugrunde gelegt.

---

[65] Vgl. zum Begriff des Symbolischen Strafrechts *Hefendehl*, Kollektive Rechtsgüter, S. 179 f.; *ders.*, in: ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 97.

[66] Auf der Seite http://kismac.de/ findet sich seither nur noch ein Abschiedsgruß.

[67] Vgl. *Borges/Stuckenberg/Wegener*, DuD 2007, 277; *Stuckenberg*, Stellungnahme BT-Drucks. 16/3656, S. 7; *Berinato*, CSO 2007, 18 ff.; siehe außerdem *Sieber*, NStZ 2009, 363, zu entsprechenden Effekten im Zusammenhang mit Vorfelddelikten der Terrorbekämpfung. Zum Ursprung des Begriffs in der amerikanischen Dogmatik zur Meinungsäußerungsfreiheit *Ladeur/Gostomzyk*, NJW 2012, 714.

[68] Eine *Problematik* entsteht erst durch das Ineinandergreifen mehrerer *Probleme*. Es wäre nicht präzise, von einer Problematik zu sprechen, wo nur einzelne Probleme erörtert werden.

[69] Siehe unten Teil 3.

[70] Siehe unten Teil 4.

Teil 2

Die Strafrechtslegitimation bei Software-Delikten

Durch einen Straftatbestand ordnet eine Gesellschaft das menschliche Miteinander: Sie stellt eine Verhaltensregel auf und knüpft an einen Verstoß gegen diese Verhaltensregel besonders drastische Konsequenzen. Wegen dieser drastischen Konsequenzen bedürfen Straftatbestände einer besonderen Rechtfertigung gegenüber dem einzelnen Mitglied der Gesellschaft und der Gesellschaft selbst – jedenfalls dann, wenn die Gesellschaft sich als freiheitlicher (Rechts-)Staat versteht und organisiert.[1] Es stellt sich also bei jedem Straftatbestand die Frage nach seiner Legitimation.

Die Frage nach der Strafrechtslegitimation drängt bei Software-Delikten besonders, weil diese wegen der Dual-Use-Problematik stets im Verdacht stehen, übliches und unauffälliges Verhalten, etwa von IT-Sicherheitsbeauftragten, zu kriminalisieren.[2] In dieser Arbeit muss deshalb zunächst erörtert werden, ob und inwiefern die Schaffung von Software-Delikten überhaupt gerechtfertigt werden kann, ehe die einzelnen Regelungstechniken der bestehenden Tatbestände analysiert und für einen neuen Modellstraftatbestand optimiert werden können.

In diesem Teil der Arbeit wird daher ein Referenzrahmen entwickelt, anhand dessen die Legitimität von Software-Delikten bewertet werden kann. Hierzu werden nach einführenden Überlegungen zur Verortung der Legitimationsfrage (I.) zunächst die Legitimationskonzepte vorgestellt, die für Vorfelddelikte der hier behandelten Art entwickelt worden sind (II.). In einem Zwischenschritt wird kategorisiert, welches Vorfeldverhalten sich in den Software-Delikten findet (III.). Darauf aufbauend können die Grundüberlegungen aus den bestehenden Legitimationskonzepten auf das Vorfeldverhalten der Software-Delikte übertragen werden, sodass ein Bewertungsmaßstab für ihre Legitimität bestimmt werden kann (IV.). Dieser Bewertungsmaßstab wird im 4. Teil der Arbeit angewandt.

---

[1] Vgl. *Hassemer*, HRRS 2006, 130 f.

[2] Siehe etwa *Duttge*, FS für Weber, S. 285 ff.; *Gierhake*, ZIS 2008, 398 f., 401 f.; *Weißer*, ZStW 121 (2009), 149.

I. Zur Verortung: Legitimation und Verfassung

Die Debatte um die Legitimation einer Strafnorm nimmt ihren Ausgangspunkt in dem auf *Binding* zurückgehenden, heute nicht mehr angezweifelten Postulat, dass die Aufgabe des Strafrechts im Schutz von Rechtsgütern besteht[3] und das Strafrecht daher nur dafür eingesetzt werden darf.[4] Im freiheitlichen Rechtsstaat wird dieser Gedanke in der verfassungsrechtlichen Prüfung eines Strafgesetzes verankert, genauer in der Verhältnismäßigkeitsprüfung: Der Gesetzgeber darf Grundrechte nur dann einschränken, wenn er damit einen *legitimen Zweck* (in geeigneter, erforderlicher und angemessener Weise) verfolgt, und dieser legitime Zweck besteht immer im Schutz bestimmter Rechtsgüter.[5]

Aufbauend hierauf besagt der – ebenso unumstrittene – Ultima-Ratio-Gedanke, dass das Strafrecht selbst zum Schutze von Rechtsgütern nicht beliebig eingesetzt werden darf, sondern dass der Gesetzgeber darauf erst zurückgreifen kann, wenn er alle anderen geeigneten Mittel ausgeschöpft hat. Denn das Strafrecht ist sein schärfstes Schwert, jenseits des Strafrechts hat er keine Mittel mehr.[6]

Der Schutz der Rechtsgüter soll dadurch erreicht werden, dass ihre Verletzung und ihre Gefährdung unter Strafe gestellt werden. Eine Strafnorm enthält deshalb zweierlei: Zum einen wird dem Bürger *verboten*, diese Rechtsgüter zu gefährden oder zu verletzen, zum anderen wird an die Verletzung dieses Verbots eine Sanktion geknüpft, nämlich die Strafe. Mit der Strafe wird ein sozialethisches Unwerturteil ausgedrückt: Dem delinquenten Bürger wird gesellschaftsfeindliches Ver-

---

[3] *Binding*, Normen, S. 189, verwendet den Begriff des Rechtsguts zuerst. Dogmengeschichtlich angelegt ist er jedoch schon bei *Birnbaum*, Neues Archiv des Kriminalrechts (1834), S. 175 f.; siehe auch *Anastasopoulou*, Deliktstypen, S. 6 ff. m.w.N.; einen aktuellen Überblick über auch alternative Legitimationstheorien liefert *Herbert*, Grenzen des Strafrechts bei der Terrorismusgesetzgebung, Teil 2, I.B.

[4] Stellvertretend für alle Jescheck/*Weigend*, Strafrecht AT, S. 7; *Roxin*, StrafR AT I, S. 14; mit dieser allgemeineren Aussage ist noch nicht die umstrittene „strafrechtliche Rechtsgutslehre" angesprochen, die dem Gesetzgeber weitere Grenzen setzen will, siehe dazu sogleich.

[5] Siehe nur BVerfG 2 BvR 392/07 (= Inzest = NJW 2008, 1137 ff.), Rz. 35. Konkret hat das BVerfG hier die Rechtsgüter familiäre Ordnung, Persönlichkeitsrecht und sexuelle Selbstbestimmung des „unterlegenen" Inzestpartners sowie Volksgesundheit (Vermeidung genetisch geschädigter Abkömmlinge aus Inzestbeziehungen) identifiziert, Rz. 41 ff. = NJW 2008, 1139 ff.; kritisch insbesondere zum Schutz der Volksgesundheit *Hörnle*, NJW 2008, 2087 f.

[6] BVerfG 2 BvR 392/07, ebd. („Strafrecht als ‚ultima ratio' des Rechtsgüterschutzes"); st. Rspr., siehe schon BVerfGE 39, 1 (= Schwangerschaftsabbruch = NJW 1975, 573 ff.), 47; Jescheck/*Weigend*, S. 3; freilich wäre das von *Jakobs*, ZStW 97 (1985), 751 ff., vorgeschlagene „Feindstrafrecht" ein gesetzgeberisches Mittel jenseits des bürgerlichen Strafrechts und würde diesem den Ultima-Ratio-Charakter nehmen. Dieser Vorschlag wird jedoch bislang nicht ernsthaft erwogen, sondern allenfalls werden in Teilen des bestehenden Strafrechts „feindstrafrechtliche Tendenzen" gewähnt und kritisiert, vgl. *Heinrich*, ZStW 121 (2009), 94 ff.

halten *vorgeworfen*, er wird also getadelt und neben einem Eingriff in seine Freiheit, sein Vermögen oder seine Freizeit (je nach Strafe) wird durch die Verurteilung insbesondere in sein soziales Ansehen eingegriffen.[7] Dieses sozialethische Unwerturteil markiert den zentralen Unterschied zwischen dem Strafrecht und anderen Sanktionsordnungen: Das Ordnungswidrigkeitenrecht belegt Ordnungsverstöße mit Bußen, also Ordnungsrufen oder „Denkzetteln", und das Polizeirecht hat die Aufgabe, Störungen und Gefahren schlicht zu beseitigen.[8]

Die Frage, welches Verhalten legitim mit Verbot *und Strafe* belegt werden kann, wirft zuerst die Frage auf, was Legitimation überhaupt ist. In jüngerer Zeit scheinen sich zwei Lager gebildet zu haben: Eine Gruppe von Autoren legt eine speziell verfassungsrechtliche Sicht zugrunde, nach welcher jeder Straftatbestand legitim ist, der nicht verfassungswidrig ist. Dementsprechend ist zu überprüfen, ob der fragliche Straftatbestand für den Gesetzgeber ein geeignetes, erforderliches und angemessenes (verhältnismäßiges) Mittel zum Erreichen des politischen (und verfassungsrechtlich zulässigen) Ziels darstellt, wobei insbesondere das Übermaßverbot Bedeutung entfaltet.[9] Erfüllt der Straftatbestand diese Anforderungen nicht, so ist er verfassungswidrig *und* illegitim.

Die Autoren im zweiten Lager nehmen keine solche verfassungsrechtliche Verankerung vor, sondern stützen ihre Legitimitätserwägungen auf überkommene Lehren der Strafrechtswissenschaft, maßgeblich die „strafrechtliche Rechtsgutslehre". Illegitim ist demnach ein Straftatbestand dann, wenn er einer überkommenen Legitimationslehre widerspricht.[10] Der Unterschied zum ersten Lager besteht also vor allem darin, dass die überkommenen Legitimationslehren nicht verfassungsrechtlich verankert werden.

Strukturell könnten die überkommenen Legitimationslehren an zwei Stellen einer verfassungsrechtlichen Prüfung integriert werden. Einerseits könnten sie in der Angemessenheitsprüfung ansetzen: Dies würde bedeuten, dass ein Verstoß gegen die jeweilige Legitimationslehre dazu führen würde, dass das Strafgesetz *unangemessen* und damit *verfassungswidrig* ist. Andererseits könnten die Legitimationslehren auch an der Einschätzungsprärogative ansetzen, die das Verfas-

---

[7] Siehe nur Jescheck/*Weigend*, Strafrecht AT, S. 65.

[8] Jescheck/*Weigend*, Strafrecht AT, S. 58 f.; *Roxin*, StrafR AT I, S. 3 f.

[9] So insbesondere *Appel*, Verfassung und Strafe, S. 514 ff., 574 ff.; *Bunzel*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 96 ff.; *Hassemer*, ZIS 2006, 268; *Hefendehl*, Kollektive Rechtsgüter, S. 42 ff.; *Lagodny*, Strafrecht vor den Schranken der Grundrechte, S. 275 ff.; *Puschke*, in: Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 23 ff.; *Radtke/Steinsiek*, ZIS 2008, 383 ff.; so auch das Bundesverfassungsgericht, siehe insbesondere BVerfG 2 BvR 392/07 (= Inzest = NJW 2008, 1137 ff.).

[10] So insbesondere *Duttge*, FS für Weber, S. 285 ff., 288 ff., 294 ff.; *von Hirsch/Wohlers*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 196 ff.; *Sieber*, NStZ 2009, 358 ff.; *Weber*, in: Jescheck (Hrsg.), Vorverlegung, S. 1 ff.; *Wohlers*, GA 2002, 15 ff.; *ders.*, Deliktstypen des Präventionsstrafrechts, S. 213 ff.

sungsrecht dem Gesetzgeber zugesteht. Verstößt der Gesetzgeber dann gegen eine Legitimationslehre, so führt dies nicht zur Verfassungswidrigkeit des Strafgesetzes, weil die Einschätzungsprärogative des Gesetzgebers verfassungsrechtlich gar nicht justiziabel ist. Der Gesetzgeber hat dann schlicht seine Einschätzungsprärogative „schlecht" ausgeübt. Mit anderen Worten: Der Verstoß gegen eine Legitimationslehre wäre in diesem Falle dem Gesetzgeber nur politisch vorzuwerfen, nicht aber rechtlich. Diese Haltung nimmt das Bundesverfassungsgericht ein, wenn es im Inzest-Verfahren in aller Deutlichkeit festhält, dass sich aus der „strafrechtlichen Rechtsgutslehre" keine besonderen verfassungsrechtlichen Anforderungen an Strafnormen ableiten lassen.[11]

Ziel dieser Arbeit ist es, in einem wertenden Vergleich der bestehenden Software-Delikte die angewandten Regelungstechniken unter dem Aspekt der Rechtsklarheit und Legitimation zu *optimieren*. Es soll nicht über die angewandten Regelungstechniken geurteilt werden. Deshalb bedarf es hier keiner weiteren Erörterung, ob ein Legitimationsmangel dem Gesetzgeber nur rechtspolitisch oder auch verfassungsrechtlich vorzuwerfen ist.

II. Legitimationskonzepte für Vorfelddelikte

Aus der mittlerweile 160-jährigen Diskussion um die Strafrechtslegitimation[12] ist ein „unübersehbares Schrifttum"[13] hervorgegangen, das hier nicht zusammengefasst werden kann. Für die Frage nach der Legitimität der Software-Delikte ist auch nur ein Teil dieser Literatur von Bedeutung. Der Gesetzgeber hat hier nämlich zwei spezielle Typen von Vorfelddelikten eingesetzt, die in der Literatur gesondert diskutiert werden. Die Konzepte, die sich mit der Legitimation dieser beiden Deliktstypen auseinandersetzen, werden im Folgenden erörtert.

Der erste Deliktstyp besteht im Vorbereiten einer späteren Rechtsgutsverletzung. Der zweite Deliktstyp erfasst jeglichen Umgang mit bestimmten (gefährlichen) Computerprogrammen – ohne einen konkretisierten Bezug zu einer späteren Rechtsgutsverletzung herzustellen. Delikte der ersten Gruppe beginnen regelmäßig mit dem Wortlaut „Wer eine Straftat [nach §§ …] *vorbereitet*, indem er ein Computerprogramm mit bestimmten Eigenschaften herstellt [etc.], wird bestraft." Delikte des zweiten Typs haben die Struktur „Wer ein Computerprogramm mit bestimmten Eigenschaften herstellt [etc.], wird bestraft."

---

[11] BVerfG 2 BvR 392/07, Rz. 39 = NJW 2008, 1138.

[12] *Koriath*, GA 2001, 51.

[13] *Roxin*, AT I, S. 64.

Mit diesen Deliktstypen haben sich insbesondere *Weber*, *Frisch*, *Wohlers* und *von Hirsch*, *Sieber*, *Puschke* und *Duttge* befasst. Nachfolgend wird dargestellt, welche Legitimitätskriterien sie jeweils entwickelt haben. Dabei ist der Terminologie der Autoren mit Zurückhaltung zu begegnen: Es hat sich noch keine einheitliche Begrifflichkeit herausgebildet. So fasst *Wohlers*[14] etwa unter dem Begriff „Vorbereitungsdelikte" andere Delikte zusammen als *Sieber*[15] unter seinen „Vorbereitungsdelikten", die wiederum nicht deckungsgleich sind mit den „Vorbereitungsdelikten im engeren Sinne" nach *Puschkes*[16] Terminologie.

A. Weber

Erste wegweisende Überlegungen stellte Weber im Jahre 1987 mit seinem Beitrag „Die Vorverlegung des Strafrechtsschutzes durch Gefährdungs- und Unternehmensdelikte"[17] an. Er liefert darin einen Überblick über viele unterschiedliche Problemfelder der Legitimation von Vorfelddelikten, vor allem aber erörtert er strukturelle Fragen der *Vorbereitungs*delikte.

1. Strukturierung bei Weber

Weber betrachtet „Gefährdungsdelikte i.e.S." und fasst darunter alle Delikte, zu deren Verwirklichung kein Verletzungserfolg und kein Verletzungswille des Täters erforderlich ist.[18] Er analysiert sodann, ob es bei dem jeweiligen Gefährdungsdelikt aus Sicht des Gesetzgebers legitim war, auf die Normierung eines Verletzungserfolgs oder Verletzungswillens zu verzichten: Ist der Verzicht des Gesetzgebers legitim, so ist es auch das Gefährdungsdelikt. Ist der Verzicht dagegen nicht legitim, so müsste ein Verletzungserfolg oder Verletzungswille zwingend (nach-)normiert werden. Die Schaffung des *Gefährdungs*delikts war dann illegitim. Anhand einzelner Delikte entwickelt Weber sodann Kategorien, in denen der Verzicht auf die Normierung eines Verletzungserfolgs oder Verletzungswillens legitim sein soll.

2. Legitimitätskriterien für einen Verletzungsverzicht

Der Gesetzgeber kann nach Weber etwa legitim auf die Normierung eines Verletzungserfolgs verzichten, wenn *mehrere Beteiligte* ein *schadensgeeignetes Verhalten* an den Tag gelegt haben, sicher ein *Verletzungserfolg eingetreten* ist und

---

[14] Siehe sogleich A.

[15] Siehe sogleich B.

[16] Siehe sogleich C.

[17] *Weber*, in: Jescheck (Hrsg.), Vorverlegung, S. 1 ff.

[18] A.a.O., S. 21.

nur die Verantwortlichkeit *eines einzelnen* Beteiligten nicht nachgewiesen werden kann. Der Verletzungserfolg müsse dann nicht vertatbestandlicht werden. Klassisches Beispiel für diese Kategorie sei § 231 StGB (Beteiligung an einer Schlägerei).[19] Die hier untersuchten Anschließungs- und Vorbereitungsdelikte des Software-Strafrechts setzen jedoch in einem Stadium an, in dem noch nicht abzusehen ist, ob jemals ein Verletzungserfolg eintritt (etwa wenn bereits das Herstellen eines Schadprogramms unter Strafe gestellt wird). Deshalb ist diese Legitimationskategorie Webers nicht auf Software-Delikte anwendbar.

Daneben ist nach Weber die Normierung eines Gefährdungsdelikts legitim, wenn sich ein tatsächlicher Deliktserfolg nur schwer feststellen lässt. Dies könne einerseits aufgrund *praktischer* Nachweisprobleme der Fall sein, etwa in multikausalen Gemengelagen wie der des Landesverrats gemäß § 94 StGB,[20] der Aussagedelikte gemäß §§ 153 ff. StGB,[21] des Lebensmittelstrafrechts und des Umweltstrafrechts.[22] Andererseits könnten Nachweisprobleme auch *theoretisch-wissenschaftlich* bedingt sein.[23] Eine solche Pönalisierung verzichtet also ganz auf einen Verletzungserfolg oder auf den Nachweis einer (Erfolgs-)Kausalität. Sie ist für *Weber* legitim zum Schutze wichtiger Rechtsgüter des Einzelnen (wie Leben und Gesundheit) oder der Allgemeinheit (wie die ökologischen Güter der Umwelt). Dies ist für Weber so unzweifelhaft, dass er sich damit begnügt, ohne Argument festzustellen, dass für den Grundsatz *in dubio pro libertate* „hier kein Platz" sei.[24] Auch diese Kategorie lässt sich nicht unmittelbar auf die Software-Delikte übertragen. Diese werden nämlich in der Regel normiert, weil man besonders schwere Rechtsgutsverletzungen verhindern möchte – nicht weil man potentielle Rechtsgutsverletzungen nicht nachweisen könnte.

Drittens und letztens sei der Verzicht auf die Normierung eines Verletzungserfolgs legitim, wenn dadurch das Zufallselement einer erfolgsbezogenen Haftung begrenzt werden solle: Bleibe bei einem vorsätzlichen Erfolgsdelikt zufällig der Erfolg aus, so werde das Täterverhalten jedenfalls bei hochstehenden Rechtsgütern legitim über die Versuchsstrafbarkeit erfasst. Ebenso sei es legitim, zu einem fahrlässigen Erfolgsdelikt ergänzend ein konkretes Gefährdungsdelikt für den Fall zu

---

[19] A.a.O., S. 23.

[20] A.a.O., S. 24: Das Herbeiführen eines „schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland" sei kaum einmal nachzuweisen.

[21] A.a.O., S. 24 f.: Nicht nachweisbar sei, ob eine gerichtliche Entscheidung falsch sei, und auch nicht, ob die einzelne Falschaussage hierfür kausal gewesen sei.

[22] A.a.O., S. 26 f.: Hier sei nicht nachweisbar, ob oder welche einzelnen Handlungen für die entstandenen Schäden kausal gewesen seien.

[23] A.a.O., S. 25: Nicht wissenschaftlich belegt sei etwa, ob es tatsächlich die geschlechtliche Entwicklung einer Person unter 18 Jahren störe, wenn ihr pornografische Schriften zugänglich gemacht würden (§ 184 Abs. 1 Nr. 1, 2, 5 StGB).

[24] A.a.O., S. 27.

schaffen, dass der Taterfolg zufällig ausbleibt.[25] Da aber auch bei konkreten Gefährdungsdelikten der Eintritt der konkreten Gefahr vom Zufall abhänge,[26] seien konkrete Gefährdungsdelikte wiederum nur dort legitim, wo das zugrunde liegende Verhalten auch abstrakt gefährlich und als Ordnungswidrigkeit oder Straftat erfasst sei.[27] Hier wird das Zusammenspiel von Erfolgs- und Gefährdungsdelikten geschildert, welches andernorts auch als Rechtsgüterschutz nach dem Bild konzentrischer Kreise beschrieben wird: Erfolgsdelikte, konkrete Gefährdungsdelikte, abstrakte Gefährdungsdelikte und Ordnungswidrigkeiten werden wie Schutzwälle um das Rechtsgut gezogen.[28] Freilich kann ein bestimmter Schutzwall nicht allein deshalb legitim sein, weil ihm ein engerer Schutzwall vorausgeht und ein weiterer Schutzwall nachfolgt. Weber führt dies zwar an dieser Stelle nicht weiter aus, trifft aber später die Aussage, abstrakt gefährliche Verhaltensweisen seien grundsätzlich durch (bloße) Bußgeldtatbestände zu verbieten. Bei *stärkerer Schadensneigung* könnten sie jedoch auch als Vergehen erfasst werden. Soweit es um Handlungen gehe, die für menschliches *Leben* und *Gesundheit* per se *hochgefährlich* seien, seien abstrakte Gefährdungsdelikte sogar zwingend.[29]

Nicht legitim sei es in jedem Falle, Vorfelddelikte zu schaffen, um eigentlich präventive Gefahrenabwehr zu betreiben, indem man durch eine weite Vorverlagerung der Strafbarkeit bereits in einem frühen Stadium strafprozessuale Zwangsmaßnahmen ermöglicht, deren Sinn dann nicht in der Aufklärung, sondern der Verhinderung von Straftaten besteht.[30] Die vielfach anzutreffende Begründung, dass andere Straftaten nur verhindert werden könnten, wenn bereits im Vorfeld strafprozessual ermittelt werde, sei „selbstverständlich" nicht legitim, da das inkriminierte Verhalten seine Gefährlichkeit in sich selbst tragen müsse; dies sei wiederum nur gegeben, wenn bereits im Vorfeld festgestellt werden könne, dass eine erste bestimmte Tat geplant werde.[31]

Diesen Gedanken greift Weber in seinen konkreteren Ausführungen zu den Vorbereitungsdelikten[32] erneut auf. Auch diese müssten *objektiv* eine Schadensneigung in sich tragen, weil eine Gefährdung nicht allein aus dem Planungszusammenhang

---

[25] A.a.O., S. 28.

[26] Aus diesem Grunde ordnen manche Autoren die konkreten Gefährdungsdelikte auch den Erfolgsdelikten zu, instruktiv siehe *Schulenburg*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 244 ff. m.w.N.

[27] A.a.O., S. 29.

[28] Vgl. *Koriath*, GA 2001, 57; legt man dieses Bild zugrunde, so liegt die Schwierigkeit jedoch darin, den zulässigen Radius der konzentrischen Schutzwälle zu bestimmen.

[29] *Weber*, in: Jescheck (Hrsg.), Vorverlegung, S. 32.

[30] A.a.O., S. 31.

[31] Ebd.

[32] Unter Vorbereitungsdelikten versteht er solche Delikte, die das „Vorbereiten" als Merkmal im Tatbestand tragen.

konstruiert werden dürfe.[33] Allerdings genügt es nach Webers Auffassung, wenn das objektiv begründete Gefährdungsunrecht als Ordnungsunrecht erfasst sei, denn sobald zu diesem ein deliktischer Vorsatz hinzutrete, liege *kriminelles* Unrecht vor.[34] Sei bekannt, dass Dritte bestimmte Vorrichtungen zu kriminellen Zwecken nutzten, so sei dies ein Indiz für die „Gefährlichkeit und damit Strafwürdigkeit" der Vorbereitungshandlungen (also Herstellung, Verbreitung etc. dieser Vorrichtungen).[35] Dies lasse sich aus der Idee der Ingerenzhaftung ableiten: Wenn jemand eine solche Gefahr verursache, dass er rechtlich dazu verpflichtet ist, ein Umschlagen der Gefahr in einen Verletzungserfolg zu verhindern, dann erscheine es legitim, schon die Gefahrschaffung als solche unter Strafe zu stellen.[36] Insbesondere gelte dies, weil der Gefahrverursacher in der Regel nicht wegen Begehung der Zieltat (durch Unterlassen) belangt werden könne. Üblicherweise habe er nämlich keine Möglichkeit zur Erfolgsabwendung, weil er die konkrete Zieltat gar nicht kenne.[37] Dass man strafrechtlich für die Gefahren verantwortlich sei, die man schaffe, lasse sich auch aus den Rücktrittsbestimmungen ableiten, da diese durchweg Gefahrabwendung verlangten.[38]

Unklar ist, ob Weber an dieser Stelle nur über die „objektive Gefährlichkeit" spricht, sodass also ein deliktischer Planungszusammenhang weiterhin erforderlich wäre (Gefährlichkeit = objektive Schadensneigung), oder ob er mit dem Schlagwort „Gefährlichkeit und damit Strafwürdigkeit" möglicherweise zum Ausdruck bringt, dass es seines Erachtens in diesen Fällen nicht mehr auf den Planungszusammenhang ankomme. Das Zweite scheint hier näher zu liegen, denn in der Folge spricht er nur noch empirisch messbare Phänomene an: Es lässt sich einfach feststellen, ob Dritte eine bestimmte Vorrichtung zu deliktischen Zwecken nutzen. Dies ist keine Wertungsfrage. Wenn diese Gefährlichkeit automatisch zur Strafwürdigkeit führen würde, käme es auf subjektive legitimierende Kriterien wie den Planungszusammenhang nicht mehr an. Da Weber zuvor aber davon spricht, dass „nicht *allein* aus dem Planungszusammenhang" die Gefährlichkeit eines Verhaltens konstruiert werden dürfe, spricht vieles dafür, dass er ihn weiterhin für notwendig erachtet. Abschließend lässt sich aber nicht klären, wie der Autor hier verstanden werden will.

Webers Rekurs auf die Ingerenzhaftung kann dagegen nicht vollends überzeugen: Die Ingerenzhaftung betrifft ja den Fall, dass der Gefahrverursacher für einen

---

[33] A.a.O., S. 15, mit Verweis auf *Jakobs*, ZStW 97 (1985), 767 ff.

[34] Ebd.

[35] Ebd.

[36] A.a.O., S. 16.

[37] Ebd. Ob *Weber* hier den besonderen Legitimationsgrund darin sieht, dass der Vorfeldtäter *nicht belangt werden kann* oder darin, dass er den Verletzungserfolg *faktisch nicht abwenden kann*, geht aus den Ausführungen nicht hervor.

[38] Ebd.

später eingetretenen Verletzungserfolg haftet, wenn dieser Verletzungserfolg aus der von ihm geschaffenen Gefahr resultiert.[39] Dies bedeutet aber gerade nicht, dass schon die Gefahrschaffung verboten oder gar strafbar gewesen wäre. Wäre es nicht zum Verletzungserfolg gekommen, so gäbe es gar keinen Zurechnungsgegenstand, für den der Gefahrschaffende über den Ingerenzgedanken die Verantwortung tragen müsste. Mit der Ingerenzhaftung lässt sich also allenfalls die Bestrafung eines Gefahrverursachers wegen tatsächlich eingetretener späterer Verletzungserfolge legitimieren. Es wäre jedoch zirkelschlüssig, wenn man mit dieser Idee auch noch die Pönalisierung der bloßen Gefahrschaffung legitimieren wollte. Vielmehr gilt das Gegenteil: Die „Weltrisikogesellschaft"[40] kann auf Gefahrschaffungen überhaupt nicht verzichten, sondern diese sind geradezu charakteristisch. Gefahrverursacher sind in der Weltrisikogesellschaft zumindest häufig vorhanden. Deshalb muss die isolierte Gefahrschaffung zunächst stets legitim sein. Eine Strafe kann nur dann verhängt werden, wenn zur Gefahrschaffung etwas hinzutritt. Auf dieses „Etwas" wurde – auch durch Webers Beitrag – der Fokus der Legitimationsdiskussion gelenkt.

Für die Vorfelddelikte nach Art der hier einschlägigen Software-Delikte lässt sich Weber also wie folgt zusammenfassen: Diese Vorfelddelikte sind dann legitim, wenn in ihnen ein abstrakt gefährliches Verhalten mit einer objektiv hohen Schadensneigung umschrieben wird. Die hohe Schadensneigung kann sich aus dem Planungszusammenhang des (Vorfeld-)Täters ergeben, aber auch aus dem sicheren Wissen um eine spätere deliktische Anknüpfungshandlung.

B. Frisch

Auch Frisch befasst sich mit der Kriminalisierung von Verhaltensweisen, die mittelbar Rechtsgüter verletzen (können) und erörtert deren Legitimation.[41] In einem eigenen Kapitel widmet er sich den „Verhaltensweisen, die rechtsgutsbeeinträchtigendes Verhalten Dritter, insbesondere die Begehung von Straftaten, ermöglichen, fördern oder veranlassen".[42] Darin stehen Verhaltensweisen in der Vorbereitungsphase im Fokus.[43]

1. Strukturierung bei Frisch

Frisch analysiert nicht bestimmte Vorbereitungs- oder Anschließungs*delikte*, sondern – losgelöst von einzelnen Delikten – jeweils ein bestimmtes Vorfeldverhal-

---

39 Siehe nur *Roxin,* Strafrecht AT II, S. 759, Rn. 143 ff.

40 Zum Begriff siehe *Sieber*, ZStW 119 (2007), 3 ff., 16 ff.

41 *Frisch*, Tatbestandsmäßiges Verhalten, S. 69 ff.

42 A.a.O., S. 230 ff.

43 A.a.O., S. 290 ff.

ten. Er legt zugrunde, dass ein Verhalten dann strafrechtlich missbilligt werden kann, wenn daran die Zurechnung eines etwaigen Deliktserfolgs geknüpft werden *könnte*. Nach Frischs Auffassung ist dies eben keine Frage der Zurechnung, sondern eine normative Vorfrage, die schon auf Ebene der Tatbestandsmäßigkeit zu entscheiden sei. Kriterien dieser normativen Vorfrage schlägt er in seiner Monografie vor.

Er betrachtet dabei explizit die Konstellationen der hier interessierenden Vorfelddelikte: Frisch spricht davon, dass der Vorfeldtäter (in seinen Worten der „mittelbar Gefährdende“[44]) seine Tathandlung vornimmt und dabei nicht zwingend weiß, ob ein Dritter bereits zur Zieltat entschlossen ist und diesen Entschluss umsetzt. Der Vorfeldtäter mag dies bei Vornahme seiner Handlung sogar nur wahrscheinlich finden oder für möglich halten, und auch objektiv mögen solche Zieltatentschlüsse mal mehr, mal weniger sicher sein.[45] Damit beschreibt Frisch exakt die Situation in den hier thematisierten Vorfelddelikten: Bei Anschließungsdelikten spielen Zieltaten und -täter keine Rolle, der Vorfeldtäter muss also nichts von den Tatentschlüssen Dritter wissen. Bei Vorbereitungsdelikten muss er dagegen irgendeine intellektuelle Beziehung zu einer irgendwie konkretisierten Zieltat haben.[46] Freilich sind die Ausführungen, die Frisch unter das Schlagwort der „Erweiterung der Macht des Dritten“[47] fasst, nur auf die Konstellation übertragbar, dass der Vorfeldtäter eine *fremde* Tat fördert. Die Tatbestände der Software-Delikte sind jedoch auch immer dann erfüllt, wenn der Täter auf seine *eigene* Zieltatbegehung hinarbeitet. Diese Konstellation ist nicht Gegenstand von Frischs Werk.

2. Legitimitätskriterien nach Frisch

Frisch geht davon aus, dass nicht jede Vorfeldhandlung, die das Risiko oder die Gefahr für das geschützte Rechtsgut erhöht oder schafft, auch tatbestandliches Unrecht darstellt. Die Risikoerhöhung ist notwendig,[48] jedoch müsse etwas hinzukommen.

Nicht ausreichend sei es, wenn bei der Weitergabe eines bestimmten Gegenstandes lediglich die *Möglichkeit* hinzukomme, diesen Gegenstand deliktisch (aus-) zunutzen. Ebenso genüge es nicht, wenn die Zieltatbegehung im Einzelfall etwa erfahrungsgemäß etwas näherliege, da auch dies im Ergebnis die Handlungsfreiheit „zu massiv“ einschränken würde.[49]

---

[44] A.a.O., S. 264.

[45] Ebd.

[46] Einzelheiten hierzu sind *de lege lata* völlig unklar, siehe dazu unten Teil 3, I.C.1.

[47] *Frisch*, Tatbestandsmäßiges Verhalten, S. 264.

[48] A.a.O., S. 293.

[49] A.a.O., S. 265. Hier könnte man auch formulieren, dass diese Möglichkeit ja erst zu der Risikoerhöhung führt. Fehlt die Möglichkeit deliktischer Verwendung, so fehlt es bereits an einer Risikoerhöhung für das Rechtsgut.

Des Weiteren genüge es nicht, wenn *objektiv konkrete Anhaltspunkte* für deliktisches Anschlussverhalten bestehen. Dies würde zu einer Misstrauensgesellschaft führen, in der sich jeder stets nach objektiven Anhaltspunkten für deliktisches Anschlussverhalten umsehen müsste.[50] Ebenso wenig sei es ausreichend, wenn der Vorfeldtäter *subjektiv konkrete Anhaltspunkte* dafür habe, dass „der Dritte" zu „einem bestimmten deliktischen Verhalten" bereits „entschlossen ist (oder sich entschließen wird)", was Frisch unter das Schlagwort „erkennbare Tatentschlossenheit oder Tatneigung" fasst.[51] Nach Frisch gibt es nämlich keine Maßstäbe dafür, wann man „konkrete Anhaltspunkte" in diesem Sinne hat.[52] Zudem bestehe die Gefahr, dass einzelne Personen vom Güterverkehr ausgeschlossen würden, weil sie nolens volens solch konkrete Anhaltspunkte schaffen oder in sich tragen (bspw. Vorbestrafte).[53]

Kein hinreichender Indikator sei außerdem die *Deliktswahrscheinlichkeit*. Denn es seien Fälle vorstellbar, in denen es sogar fast sicher sei, dass eine Straftat folge und dennoch das Verhalten nicht missbilligt werden könne. Dies sei etwa bei der Rückzahlung eines Darlehens an einen notorischen Devisenstraftäter der Fall.[54]

Schließlich sei auch nicht immer hinreichend, wenn die Tathandlung als solche schon *unbefugt* erfolge („sonstige Verbotenheit").[55] Dies begründet Frisch vor allem damit, dass der Schutzzweck der Verbotsnorm nicht zwingend in dieselbe Richtung weise wie die Strafnorm: Betrachtet man den Verkauf eines gefährlichen Gegenstandes, so kann man die Legitimität einer entsprechenden Strafnorm nicht daran knüpfen, ob dieser Verkauf während oder außerhalb der Ladenöffnungszeiten (=unbefugt) stattfindet.[56]

Nach Frisch ist der maßgebliche Indikator ein *eindeutig deliktischer Sinnbezug*.[57] Gemeint ist damit ein „zentraler Sinnbezug außerhalb des rechtlichen Handlungsspielraums". Liege dieser vor, so liege bereits in dem Vorfeldverhalten selbst ein ideeller Angriff auf das Rechtsgut.

Die Frage sei, wann dieser eindeutig deliktische Sinnbezug angenommen werden solle. Beim Umgang mit bestimmten Gegenständen in der Vorbereitungsphase einer Rechtsgutsverletzung könne man für den „deliktischen Sinnbezug" beispielsweise nicht fordern, dass ein Gegenstand „ausschließlich deliktisch verwertbar" sei:

---

[50] A.a.O., S. 269.

[51] A.a.O., S. 266 f.

[52] A.a.O., S. 268.

[53] A.a.O., S. 271.

[54] A.a.O., S. 275.

[55] A.a.O., S. 276 ff.

[56] A.a.O., S. 276 f. Hier ließe sich ergänzen, dass in manchen Bereichen solche vorstrafrechtlichen Befugnisnormen gar nicht existieren und schon deshalb nicht darauf abgestellt werden kann, ob die Tathandlung „unbefugt" vorgenommen wird.

[57] A.a.O., S. 281.

Dies würde nicht einmal auf „typische Verbrechenswerkzeuge wie Dietriche“ zutreffen.[58] Außerdem könnte der Dritte mit solchen Gegenständen unter Umständen auch bloße Erkenntnisinteressen befriedigen wollen.[59]

Maßgeblich sei unter dem Aspekt des „deliktischen Sinnbezugs“, dass das Vorfeldverhalten insgesamt darauf bezogen sei, das Zieldelikt zu ermöglichen oder zu erleichtern. Der deliktische Sinnbezug sei dabei ein objektives Kriterium: Er liege vor, wenn die Handlung objektiv nur Sinn ergebe, wenn sie als Ermöglichungs- oder Erleichterungshandlung interpretiert würde,[60] also wenn eine plausible rechtmäßige Alternativerklärung fehle.[61] Kein „deliktischer Sinnbezug“ liege daher bei Handlungen vor, die „unübersehbar als Verfolgung berechtigter Handlungsinteressen zu verstehen und dadurch regelmäßig auch motiviert“ seien.[62]

Besonderheiten bestehen nach Frisch bei Verhaltensweisen, an die zwar deliktisch angeknüpft werden kann, weshalb man sie auch deliktisch erklären könnte, die jedoch vom (theoretischen) Vorfeldtäter nicht als solche gewünscht sind, sondern vielmehr zu rechtmäßigen Zwecken vorgenommen werden.[63] Diese Verhaltensweisen haben nach Frisch keinen „deliktischen Sinnbezug“ und ein strafbewehrtes Verbot kann nur unter dem Gedanken einer notstandsmäßigen Aufopferung gerechtfertigt werden: Der (theoretische) Vorfeldtäter muss sich aufopfern und seine sozialadäquate und eigentlich akzeptable Handlung aufgeben, weil es Dritte gibt, die an diese Handlung deliktisch anknüpfen können.[64]

Grundsätzlich könnten solche Straftatbestände nur gerechtfertigt werden, wenn unverhältnismäßige Beeinträchtigungen des Rechtsguts drohen, die nicht anders abgewehrt werden können als durch das strafbewehrte Verbot.[65] Dies stützt Frisch auf systematische Ableitungen aus §§ 138 und 323c StGB: In diesen Tatbeständen sind Bedrohungslagen für bestimmte Rechtsgüter abgebildet und dem Bürger werden Pflichten zur Abwendung dieser Rechtsgutsbedrohungen auferlegt. Frisch folgert nun, dass es dann erst recht strafbar sein müsse, diese Bedrohungslage durch ein bestimmtes Vorfeldverhalten zu intensivieren.[66] Er stellt aber klar, dass nicht jede ambivalente Vorfeldhandlung zugleich die Bedrohungslage intensiviert:

---

[58] A.a.O., S. 290.

[59] Ebd., womit beinahe der Mehrzweckaspekt der Dual-Use-Problematik angesprochen ist. Der Unterschied besteht allerdings darin, dass dort nicht nur bloße Erkenntnisinteressen befriedigt werden, sondern dahinter stets das Fernziel steht, den technischen Schutz von IT-Systemen gegen Angriffe und Angriffswerkzeuge zu verbessern.

[60] A.a.O., S. 284.

[61] A.a.O., S. 289.

[62] A.a.O., S. 307.

[63] A.a.O., S. 310.

[64] A.a.O., S. 312.

[65] Ebd.

[66] A.a.O., S. 314 f.

Der potentielle Vorfeldtäter dürfe deliktserleichternde Vorfeldhandlungen jedenfalls noch vornehmen, solange er auch im Anschluss noch seinen Pflichten aus §§ 138 und 323c StGB nachkommen könne.[67]

Diese Fallgruppe ist gerade im Bereich der Software-Delikte hochinteressant: Wenn etwa „im Untergrund" zu einem hohen Preis ein Hackingtool verkauft wird, das eine bislang unentdeckte Sicherheitslücke im IT-System eines Krankenhauses ausnutzt und dem Angreifer damit die Kontrolle über bestimmte Operationsgeräte gibt, dann besteht eine Bedrohungslage für mehrere hochrangige Rechtsgüter. Wenn nun ein Rechtschaffener erfährt, dass dieser Verkauf stattgefunden hat, wird er möglicherweise die Sicherheitslücke bekanntmachen wollen, damit Krankenhäuser sich vor entsprechenden Angriffen schützen können. Möglicherweise wird er als *Proof-of-Concept* selbst ein entsprechendes Hackingtool schreiben und gemeinsam mit einer Anleitung zur vorläufigen Behebung der Sicherheitslücke *(Workaround)* veröffentlichen. In diesem Fall ermöglicht und fördert seine Handlung unmittelbar die Deliktsbegehung bezüglich der Krankenhäuser, die die Sicherheitslücke nicht sofort beheben. Mittelbar jedoch mildert die Handlung die Bedrohungslage, weil die Krankenhäuser sich nun gegen Angriffe dieser Art schützen können.

Nach Frisch liegt hier schon kein deliktischer Sinnbezug vor, weil es für das Gesamtgeschehen eine plausible rechtmäßige Interpretation gibt. Überdies werden die Risikoerhöhung und die Deliktserleichterung kompensiert durch die nun gestiegenen Chancen zur Tatverhinderung.[68] Diese objektive Kompensation soll sogar dazu führen, dass das konkrete Verhalten nicht einmal dann legitim bestraft werden könnte, wenn der potentielle Täter *in deliktischer Absicht* handelt.[69] Er soll also selbst dann straffrei bleiben, wenn er die Sicherheitslücke samt *Hackingtool* und *Workaround* veröffentlicht und dabei insgeheim hofft, dass die Krankenhäuser ihre Schutzsysteme nur langsam verbessern, sodass es noch zu einer Reihe von schwerwiegenden Rechtsgutsverletzungen kommt: Es liege objektiv schlicht keine Risikoerhöhung darin, dass Sicherheitslücke, Hackingtool und Workaround veröffentlicht werden.

Zusammenfassend sind nach Frischs Ausführungen also die Vorfelddelikte der hier einschlägigen Art dann legitim, wenn sie das Risiko für das geschützte Rechtsgut erhöhen und ein „deliktischer Sinnbezug" der Vorfeldhandlung besteht. Auf den „deliktischen Sinnbezug" der Vorfeldhandlung könne nur verzichtet werden, wenn sie unverhältnismäßige und irreversible Beeinträchtigungen der geschützten Rechtsgüter nach sich zieht.

---

[67] A.a.O., S. 317.

[68] Ebd.

[69] A.a.O., S. 319.

C. Wohlers und von Hirsch

Wohlers hat sich zunächst in seiner Habilitationsschrift „Deliktstypen des Präventionsstrafrechts“ aus dem Jahre 2000 detailliert mit der Legitimation von Vorfelddelikten der hier diskutierten Art auseinandergesetzt. Im Jahr 2003 hat er in dem Beitrag „Rechtsgutstheorie und Deliktsstruktur – zu den Kriterien fairer Zurechnung“ diese Gedanken gemeinsam mit von Hirsch fortgeführt. [70]

1. Strukturierung bei Wohlers und von Hirsch

Wohlers unterteilt die Menge aller abstrakten Gefährdungsdelikte in drei Gruppen: „Potentiell-konkrete Gefährdungsdelikte“ bilden Situationen ab, die potentiell in eine konkrete Gefährdung münden, ohne dass der Täter dies steuern könnte. Beispiel hierfür ist die Trunkenheitsfahrt gemäß § 316 StGB.[71] Die zweite Gruppe bilden die „Kumulationsdelikte“, bei denen das entsprechende Rechtsgut durch eine einzelne Deliktsbegehung nicht beeinträchtigt wird, bei denen jedoch mehrere gleichgerichtete Handlungen kumuliert zu einer Rechtsgutsbeeinträchtigung führen oder führen können. Hierunter fallen insbesondere die Umweltdelikte der §§ 324 ff. StGB.[72] Die dritte Kategorie stellen „Vorbereitungsdelikte“ dar, deren Tathandlungen so umschrieben sind, dass sie erst dann zu einer Beeinträchtigung eines Rechtsguts führen (können), wenn objektiv eine *selbstständige Zweithandlung* an sie anknüpft.[73] Dabei unterscheidet Wohlers nicht kategorial nach den subjektiven Intentionen des Vorfeldtäters. Es spielt deshalb für die systematische Einordnung eines Delikts noch keine Rolle, ob der Ersthandelnde subjektiv den späteren Erfolg fördern oder herbeiführen *will*. Solche subjektiven Bezüge des Ersttäters zu einer späteren Zieltat oder zum Deliktserfolg erörtern Wohlers und von Hirsch vielmehr als Gesichtspunkte der Legitimation des einzelnen Delikts.[74]

Damit können ihre Ausführungen auf alle hier thematisierten Software-Delikte gleichermaßen angewandt werden. Denn diese stellen alle ein abgeschlossenes Verhalten im Vorfeld einer Rechtsgutsverletzung dar, welches erst durch eine angeknüpfte selbstständige Zweithandlung in eine konkrete Gefährdung oder Verletzung des geschützten Interesses münden kann. Zwar bestehen in den Software-Delikten strukturelle Unterschiede auf der subjektiven Tatseite,[75] jedoch führt dies bei von Hirsch und Wohlers erst in der Frage der *Legitimation* des einzelnen Vorfelddelikts zu unterscheidbaren Ergebnissen.

---

[70] *von Hirsch/Wohlers*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 196 ff.

[71] *Wohlers,* Deliktstypen, S. 309.

[72] A.a.O., S. 309 f.

[73] A.a.O., S. 310.

[74] *von Hirsch/Wohlers*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 205, dazu sogleich.

[75] Siehe hierzu sogleich D. sowie unten Teil 3, I.C., II.C. und III.C.

Wohlers weist darauf hin, dass es sich bei der Frage nach der Legitimation von Vorfelddelikten in der Sache um ein Problem der Abgrenzung von Verantwortungsbereichen handelt.[76] Konkret gehe es darum, die Verantwortungsbereiche von Ersthandelndem und Zweithandelndem gegeneinander abzugrenzen und sodann festzustellen, ob eine (gedachte) deliktische Zweithandlung zumindest auch in den Verantwortungsbereich des Ersthandelnden fällt, wann also das „eigenverantwortliche Verhalten anderer Personen als ein handlungsleitender Faktor antizipiert wird".[77] Nur in diesem Fall sei eine Pönalisierung der Ersthandlung mit dem Selbstverantwortungsprinzip in Einklang zu bringen.[78] Dieses besagt, dass sich Verhaltenspflichten nur auf den *eigenen* Verantwortungsbereich beziehen und „man sich grundsätzlich nicht darauf einstellen muss, dass *andere* sich […] sorgfaltswidrig verhalten".[79] Die Frage nach den Grenzen des Verantwortungsbereichs ist nach Wohlers aber eine normative Frage und muss deshalb anhand normativer Maßstäbe bestimmt werden.[80]

Zur Annäherung an die Grenze der Legitimität solcher Vorfelddelikte prüft Wohlers zunächst, ob aus der Lehre von der objektiven Zurechnung und der Unterbrechung dieser Zurechnung Erkenntnisse zu gewinnen sind.[81] Auch hier werden nämlich Fälle diskutiert, in denen ein Ersthandelnder durch sein Verhalten eine Situation schafft, an die ein anderer anknüpft und den Deliktserfolg unmittelbar herbeiführt. Dort stellt sich also ebenso die Frage, in welchen Fällen dem Ersthandelnden das Herbeiführen des Erfolgs durch den Zweithandelnden noch zugerechnet werden darf und in welchen eine Zurechnung abzulehnen ist. Als Grundsätze, nach denen die objektive Zurechnung unterbrochen werden soll, stellt Wohlers den Vertrauensgrundsatz,[82] die Sozialadäquanz[83] und die (fehlende) Vorhersehbarkeit deliktischen Anschlussverhaltens[84] vor. In diesen Fallgruppen wird das Zweithandeln dem Ersthandelnden selbst dann nicht zugerechnet, wenn ein Deliktserfolg *tatsächlich eingetreten ist*. Daraus folge, dass solche Situationen *erst recht* nicht als abstrakte Gefährdungsdelikte konzipiert werden dürfen, denn dies würde bedeuten, dass die Zweithandlung eben doch zugerechnet würde, selbst wenn sie noch gar nicht stattgefunden hat, vielleicht nie stattfindet und ein Deliktserfolg von Anfang an nur hypothetisch vorliegt.[85] Allerdings unterstreicht Wohlers in der Folge, dass

---

[76] *Wohlers*, Deliktstypen, S. 311.

[77] Ebd.

[78] A.a.O., S. 329.

[79] *Schumann*, Handlungsunrecht, S. 5 (Hervorhebung nicht im Original).

[80] *Wohlers*, Deliktstypen, S. 331, 333.

[81] A.a.O., S. 330 ff.

[82] A.a.O., S. 331 f.

[83] A.a.O., S. 331.

[84] A.a.O., S. 332 f.

[85] A.a.O., S. 330.

sich die normative Frage der Abgrenzung von Verantwortungsbereichen bei Vorbereitungsdelikten abstrakt stelle, während bei den Fallgruppen der objektiven Zurechnung stets ein konkreter Einzelfall zugrunde liege, weshalb obige Grundsätze nicht eins zu eins übertragen werden könnten.[86]

In seinem eigenen Modell betont Wohlers vielmehr die Ambivalenz jeglichen Verhaltens und stellt deshalb für die Frage, ob eine Verhaltensweise legitim pönalisiert werden kann, darauf ab, welche *Funktion* dieser Verhaltensweise *bestimmungsgemäß zukommt*.[87] Daraus ergebe sich, ob das Vorverhalten einen *deliktischen Sinnbezug* habe. Wenn die Verhaltensweise gar keinen oder jedenfalls keinen eindeutigen deliktischen Sinnbezug habe, sei eine Pönalisierung des Vorverhaltens von vornherein ausgeschlossen.[88]

Eine genaue Abgrenzung zwischen *Funktion* und *Bestimmung* nimmt Wohlers sodann jedoch nicht hervor. Insbesondere ist unklar, auf wessen Sichtweise und Willensrichtung es ankommt. Vermutlich ist gemeint, dass der Vorfeldtäter seinem Verhalten eine *Bestimmung* gibt, aus der sich sodann die *Funktion* des Verhaltens ableiten lässt. Damit handelte es sich um eine Kombination aus einem subjektiven und einem objektiven Element. Ein deliktischer Sinnbezug ergäbe sich hier, wenn der Vorfeldtäter mit seinem Verhalten die Begehung oder den Erfolg einer Zieltat fördern *will* (Bestimmung) und wenn bei einer hinzugedachten Anknüpfungshandlung, die grob der Idee des Vorfeldtäters entspricht (bestimmungsgemäße Anknüpfungshandlung), das Ersthandeln insgesamt zur Vorbereitung der Zieltat nützlich ist (deliktische Funktion).

Bei „Verhaltensweisen, an die bestimmungsgemäß nur zu deliktischen Zwecken angeknüpft werden kann“,[89] sei eine Pönalisierung grundsätzlich möglich, da die Vorbereitung deliktischen Handelns ersichtlich keinen relevanten sozialen Wert habe. In der Frage des Dual-Use, also in Fällen, in denen auch die Möglichkeit einer nicht-deliktischen Anknüpfungshandlung bestehe, könne auf der Legitimationsebene keine Antwort gegeben werden.[90] Das Problem des Dual-Use sei vielmehr über eine präzise Ausgestaltung der Strafbarkeitsvoraussetzungen zu lösen: Eine Pönalisierung sei legitim, wenn sie – etwa bei Gegenständen, die vor allem als „Deliktswerkzeuge“ verwendet werden können – keine sozial werthaften Gebrauchsformen erfasse.[91]

---

[86] A.a.O., S. 335.
[87] Ebd.
[88] Ebd.
[89] A.a.O., S. 336.
[90] Ebd.
[91] Ebd.

2. Legitimitätskriterien des „normative involvement“

Zusammen mit von Hirsch präzisiert Wohlers den deliktischen Sinnbezug anhand von „Kriterien fairer Zurechnung“, nach denen ein Ersthandelnder für das Verhalten eines Zweithandelnden normativ verantwortlich gemacht werden könne, also ein „*normative involvement*“ des Ersthandelnden zu bejahen sei.[92]

(1) *Abzielen auf deliktisches Zweithandeln*. Legitim sei zum einen die Pönalisierung eines Verhaltens, das direkt und unmittelbar *darauf abziele*, eine andere Person zu ihrem deliktischen Verhalten zu bestimmen.[93] Da das *Verhalten* des Vorfeldtäters insgesamt darauf abzielen muss, einen Zweithandelnden zu einer deliktischen Anknüpfungshandlung zu bestimmen, ist es demnach nicht ausreichend, wenn der Ersthandelnde den Zweithandelnden allein subjektiv zu einer deliktischen Handlung bestimmen *will*. Er muss dies vielmehr in seinem Verhalten zum Ausdruck bringen. Als Beispiel nennen von Hirsch/Wohlers das „Auffordern zu Straftaten“ gemäß § 111 Abs. 1 StGB.[94]

(2) *Vermittlung von deliktischem Know-how*. Ferner sei es legitim, das Vermitteln deliktischen Know-hows unter Strafe zu stellen, selbst dann, wenn diese Wissensvermittlung keinen Aufforderungscharakter habe.[95] Dies gelte jedoch nur, wenn das „Telos“ der Wissensvermittlung darin liege, „*allein deliktisch verwertbares* Know-how zu vermitteln“.[96] An dieser Stelle wird jedoch nicht ganz klar, welche Funktion das „allein“ hier erfüllt: Soll das vermittelte Know-how *allein* deliktisch verwertbar sein? Oder soll *allein* solches Know-how vermittelt werden, das (unter anderem) deliktisch verwertbar ist? Außerdem ist klärungsbedürftig, wie das „Telos“ in Abgrenzung zu Bestimmung und Funktion aus der ersten Fallgruppe (Abzielen auf deliktisches Anschlusshandeln) einzuordnen ist. Deshalb lässt sich nur festhalten, dass nach von Hirsch/Wohlers das Vermitteln deliktisch verwertbaren Know-hows unter Umständen legitim pönalisiert werden kann.

Auch hier sei aber sozial werthaftes Verhalten von der Strafbarkeit auszunehmen. In diesen Fällen könne der Gesetzgeber jedenfalls Ausschlussklauseln verwenden, um etwa sicherzustellen, dass Kunst-, Wissenschafts- und Meinungsfreiheit nicht zu stark eingeschränkt würden.[97]

---

[92] *von Hirsch/Wohlers*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 196 ff.

[93] A.a.O., S. 205.

[94] § 111 Abs. 1 StGB ist in den infrage kommenden Mitteln sehr präzise, indem er eine „Kundgebung mit Appellcharakter“ an einen unbestimmten Adressatenkreis erfordert, siehe nur Schönke/Schröder-*Eser*, § 111 Rn. 3, 4. Daneben sind jedoch viele weitere Verhaltensformen denkbar, die auf deliktisches Zweithandeln abzielen und damit in diese Legitimationskategorie fallen würden.

[95] A.a.O., S. 205.

[96] Ebd.

[97] Ebd.

(3) *Unbefugter Umgang mit gefährlichen Produkten*. Der Umgang mit Produkten, die ihrer bestimmungsgemäßen Funktion nach von Privatpersonen *nur zu unerlaubten Zwecken* verwendet werden können (also etwa militärische Kampfmittel), könne unzweifelhaft unter Strafe gestellt werden.[98] Bei Produkten, die „von ihrem Telos her sowohl legitime als auch illegitime Gebrauchsmöglichkeiten bieten", sei eine Pönalisierung nur im Falle von „unbefugtem Handeln" legitim. Dies gelte etwa für Waffen und Gifte.[99] Auch hier ist wieder vom „Telos" die Rede, allerdings in einem anderen Bedeutungszusammenhang: Während in der zweiten Fallgruppe das „Telos" der Informationsvermittlung, also einer menschlichen Handlung, gemeint war, ist hier die Rede vom Telos von Gegenständen. Da bereitet es schon Schwierigkeiten, die Bedeutung des Begriffs überhaupt zu erfassen, da nicht ohne Weiteres klar ist, wonach bei einem multifunktionalen Gegenstand zu entscheiden ist, welche Funktionen dem Telos entsprechen und welche ihm zuwiderlaufen.[100]

Die von den Autoren angeführten Beispiele lassen jedoch darauf schließen, dass es um Produkte geht, deren *bestimmungsgemäße Funktion* sowohl einen *legalen* als auch einen *illegalen* Einsatz des Produkts ermöglicht. In diesen Fällen sei nur die Kriminalisierung unbefugten Handelns legitim. Damit wird die Grenze der Legitimität mit der Befugnisgrenze gleichgesetzt. Dies wiederum bedeutet, dass der Befugnisgeber zugleich über die Grenze legitimen Strafens bestimmt. Dies ist zwar nicht von vornherein abwegig, jedoch muss dann die Diskussion darüber geführt werden, wer zum Erteilen von Befugnissen berufen ist, insbesondere wenn die Befugnisse im Umgang mit den Produkten nicht schon ordnungsrechtlich geregelt sind.

Allerdings schränken von Hirsch und Wohlers ihr Modell dahingehend ein, dass es nur für das Vorbereiten von Straftaten *anderer* gelte.[101] Das Vorbereiten einer eigenen Straftat könne schon prinzipiell nicht pönalisiert werden, weil es der Konzeption vom mündigen Bürger widerspreche: Von einem mündigen Bürger sei nicht zu erwarten, dass er mit einem bestimmten Verhalten eine Straftat vorbereite, weil davon auszugehen sei, dass er seine Handlungsfreiheit gerade nicht missbraucht, auch wenn es ihm faktisch möglich sei, durch eine Zweithandlung ein Delikt zu begehen.[102]

Zusammenfassend sind nach Wohlers und von Hirsch also Vorfelddelikte der hier diskutierten Art dann legitim, wenn die Vorfeldhandlung einen deliktischen Sinnbezug aufweist, der es erlaubt, dem Vorfeldtäter eine potentielle Anschlusstat

---

[98] Ebd.

[99] Ebd.

[100] Diese Begriffskonstruktion ähnelt dem Tatbestandsmerkmal des „Zwecks eines Computerprogramms", das Eingang in die §§ 202c Abs. 1 Nr. 2, 263a Abs. 3 StGB und 22b Abs. 1 Nr. 3 StVG gefunden hat. Zu den dortigen Auslegungsschwierigkeiten siehe unten Teil 3, I.B.2.

[101] *von Hirsch/Wohlers*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 201.

[102] Ebd.

zuzurechnen. Der deliktische Sinnbezug müsse danach ermittelt werden, welche Funktion der Vorfeldhandlung bestimmungsgemäß zukommt. Konkret sei er demnach insbesondere zu bejahen, wenn die Vorfeldhandlung (1) darauf abziele, Dritte zu Anschlusstaten zu bestimmen, (2) Dritten allein deliktisch verwertbares Know-how vermitteln soll oder (3) einen unbefugten Umgang mit gefährlichen Gegenständen darstelle. In jedem Falle aber müsse sozial werthaftes Verhalten von der Strafbarkeit ebenso ausgenommen werden wie das Vorbereiten eigener Straftaten.

D. Sieber

Sieber befasste sich anlässlich des Entwurfs eines „Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten“,[103] der eine ganze Reihe unterschiedlicher Vorfelddelikte enthält, mit deren Systematik und Legitimation.[104] Siebers Strukturierung und Terminologie der Vorfelddelikte wird auch dieser Arbeit zugrunde gelegt.

1. Strukturierung bei Sieber

Sieber unterscheidet zwischen „Anschließungsdelikten“ und „Vorbereitungsdelikten“. Ein Anschließungsdelikt erfasst demnach eine abgeschlossene Handlung, die das Rechtsgut weder konkret gefährdet noch verletzt, an die aber ein Anschlusstäter mit einer deliktischen und rechtsgutsverletzenden Zweithandlung anknüpfen kann oder auf die er zur Rechtsgutsverletzung aufbauen kann. Für die Strafbarkeit des Ersttäters ist es dabei unerheblich, ob später tatsächlich ein Zweittäter deliktisch an das Verhalten des Ersttäters anknüpft. Auch ist kein konkreter Bezug der Ersthandlung zu einer bestimmten Zweithandlung erforderlich.[105]

In den Vorbereitungsdelikten wird ein Verhalten erfasst, mit dem der Täter eine bestimmte Zieltat *vorbereitet*. Da bei solchen Vorbereitungsdelikten die subjektiven Planungen des Ersthandelnden eine maßgebliche Rolle spielen, bestehe die Gefahr der Schaffung eines unzulässigen Gesinnungsstrafrechts, insbesondere wenn (neutrale) Alltagshandlungen zum Anlass genommen würden, subjektive Vorstellungen des Ersthandelnden zu erforschen und zu bestrafen.[106] Dieser Gefahr müsse im Rahmen der Legitimation Rechnung getragen werden.

---

[103] BT-Drucks. 16/12428 vom 25.3.2009.

[104] *Sieber*, NStZ 2009, 358 ff.

[105] A.a.O., 358.

[106] Abzulehnen sei deshalb etwa § 89a Abs. 2 Nr. 4 StGB, soweit er auch das *Ansparen von Vermögenswerten* als Vorbereiten einer schweren staatsgefährdenden Gewalttat erfasse, wenn beim Täter eine entsprechende Gesinnung vorliegt. *Sieber*, NStZ 2009, 360.

2. Legitimitätskriterien für Anschließungs- und Vorbereitungsdelikte

Bei Anschließungsdelikten sprechen gemäß Siebers Ausführungen das Prinzip der Eigenverantwortlichkeit des Anschlusstäters und der Vertrauensgrundsatz (Vertrauen in das rechtskonforme Verhalten anderer)[107] generell dagegen, dem Ersthandelnden eine hypothetische (!) deliktische Anschlusstat zuzurechnen.[108] Insbesondere bei einer *deliktsneutralen* Ersthandlung sei für den „Ersttäter" ein deliktisches Anschlussverhalten gar nicht vorhersehbar.[109] Daher könne nur bei Handlungen mit einem *deliktischen Sinnbezug* eine Kriminalisierung legitim sein. Ein solcher komme zunächst in Betracht, wenn der Ersthandelnde wie etwa im Waffenrecht eine *Sorgfaltspflicht* verletze, deren Telos es gerade sei, im konkreten Fall die Möglichkeit deliktischen Anschlusshandelns auszuschließen.[110] Ferner liege ein deliktischer Sinnbezug vor, wenn als Anschließungsdelikt ein Gegenstand weitergegeben werde, der nur „(oder ganz überwiegend) deliktisch genutzt" werden könne.[111] Schließlich sei auch ein deliktischer Sinnbezug gegeben, wenn der Gegenstand oder die Information *in besonderem Maße gefährlich* sei, wenn der Ersthandelnde und der Anschlusstäter *kollusiv zusammenwirkten*, wenn die Ersthandlung einen *spezifischen Aufforderungscharakter* habe oder wenn der Ersthandelnde *sicher wisse*, dass er durch sein Verhalten deliktisches Anschlussverhalten fördere.[112]

Zur Legitimation von Vorbereitungsdelikten reicht es nach Sieber nicht aus, nur darauf abzustellen, dass die Zieltat besonders gefährlich sei und nur durch frühes Eingreifen verhindert werden könne.[113] Vielmehr bedürfe es einer *eindeutigen objektiven Manifestation der Tatvorbereitung*, einer *besonderen Gefahrschaffung* sowie *spezieller Vorsatzmerkmale*.[114] Eine objektive Manifestation der Tatvorbereitung könne grundsätzlich in jedem Verhalten des Ersthandelnden liegen, jedoch könne dieses Verhalten nur dann als *Tat*vorbereitung gewertet werden, wenn es für die private oder berufliche Lebensgestaltung des Ersthandelnden keinen Sinn ergebe.[115] Die objektive Gefahr, welche der Täter – nach seiner Tatplanung – durch die Vorbereitungshandlung schaffe, müsse außerdem so erheblich sein, dass ihr erfah-

---

[107] Siehe *Roxin*, AT I, § 24 Rn. 21 ff., 26 ff.; *Duttge*, Zur Bestimmtheit des Handlungsunwerts von Fahrlässigkeitsdelikten, S. 468 ff. m.w.N.

[108] *Sieber*, NStZ 2009, 358.

[109] Als Beispiel hierfür nennt *Sieber* den Verkauf eines Brotmessers, ebd.

[110] A.a.O., 359.

[111] Ebd.

[112] Ebd.

[113] Ebd.

[114] Ebd.

[115] A.a.O., 361.

rungsgemäß zu einem späteren Zeitpunkt nicht mehr begegnet werden könne.[116] Als spezielles Vorsatzmerkmal sei schließlich erforderlich, dass der Täter einen unbedingten Entschluss zur Straftatbegehung gefasst habe oder jedenfalls mit Wissen hinsichtlich der Zieltat handle.[117] „In vielen Fällen" reiche es aufgrund der grundsätzlich fehlenden Tatnähe und der geringen Konkretisierung der Zieltat nicht aus, wenn der Vorsatz hinsichtlich der Zieltatbegehung in Form von dolus eventualis vorliege, vielmehr seien Absicht oder Wissen erforderlich.[118]

E. Puschke

Puschke[119] untersucht „Vorbereitungstatbestände im engeren Sinne" und fasst darunter Tatbestände mit solchen Handlungen, die selbst noch kein Rechtsgut beeinträchtigen, sondern eine „zukünftige, vorsätzliche Beeinträchtigung eines individuellen oder kollektiven Rechtsguts vorbereiten".[120] Davon werden unter anderem solche (Vorfeld-)Tatbestände ausgenommen, die zwar eine spätere Schädigungshandlung vorbereiten, jedoch keinen intentionalen Bezug des Vorbereitenden zu dieser Schädigungshandlung voraussetzen.[121] Puschkes Ausführungen lassen sich folglich nur auf die Vorbereitungsdelikte nach der hier gewählten Terminologie anwenden. Anschließungsdelikte im Sinne dieser Arbeit setzen den intentionalen Bezug zur späteren Schädigung gerade nicht voraus.

Zur Legitimation eines Vorbereitungsdelikts müssen laut Puschke insbesondere fünf Anforderungen erfüllt sein: Erstens müsse das gesetzgeberische Ziel (auch) bei Vorbereitungsdelikten darin bestehen, eine psychisch vermittelte Wirkung zu erzielen, also *abzuschrecken*. Es dürfe nicht das vorrangige Strafziel des Gesetzgebers sein, eine Interventionsmöglichkeit vor einer späteren Rechtsgutsverletzung zu schaffen.[122] Zweitens brauche es ein konkretes, *eng umrissenes Schutzgut*, welches als Anknüpfungspunkt für Geeignetheits- und Verhältnismäßigkeitserwägungen tauge.[123] Drittens müsse die Vorbereitungshandlung selbst für das Rechtsgut gefährlich sein, es bedarf also eines hinreichenden *Gefährlichkeitszusammenhangs*.[124] Viertens dürfe der *Kernbereich* privater Lebensgestaltung durch die Pönalisierung

---

116 Ebd.

117 Ebd.

118 Ebd.

119 *Puschke*, in: Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 ff.

120 A.a.O., S. 10 f.

121 A.a.O., S. 13 f., mit Verweis auf den Erwerb oder Besitz von Waffen und die Strafbestimmungen des Kriegswaffenkontrollgesetzes.

122 A.a.O., S. 26.

123 A.a.O., S. 28.

124 A.a.O., S. 29 ff.

nicht berührt sein,[125] und fünftens sei gemäß dem *Bestimmtheitsgrundsatz* genau zu klären, welchen Inhalt das Merkmal „vorbereiten" habe und welche Eigenschaften das Tatobjekt erfüllen müsse.[126] Die Kriterien der zwingend psychischen Vermittlung, des eng umrissenen Schutzguts, des unantastbaren Kernbereichs sowie des Bestimmtheitsgrundsatzes stellen zwar hinsichtlich der Formulierung und Begründung von Vorfeldtatbeständen wichtige Anforderungen an den Gesetzgeber; entscheidend ist aber in der Frage nach der Legitimität eines Vorfeldtatbestands, genauer: nach den *Grenzen legitimer Vorverlagerung* der Strafbarkeit, das Kriterium des „hinreichenden Gefährlichkeitszusammenhangs". Diesen Gefährlichkeitszusammenhang trennt Puschke in einen subjektiven und einen objektiven Aspekt, wobei eine hinreichende und strafbarkeitslegitimierende Risikoerhöhung für das geschützte Rechtsgut nur dann vorliegen soll, wenn beide Aspekte zugleich vorliegen.

1. Subjektiver Gefährlichkeitszusammenhang

Der subjektive Gefährlichkeitszusammenhang sei der Planungszusammenhang. Dieser stelle das konstituierende Merkmal aller Vorbereitungsdelikte dar.[127] Charakteristisch sei, dass der Täter seinen Vorsatz nicht nur auf die konkrete Vorbereitungshandlung beziehe, sondern darüber hinaus einen Angriff auf das Rechtsgut plane.[128] Der Planungszusammenhang sei also ein „überschießendes subjektives Element", welches bei der Bewertung des *objektiven* Gefährlichkeitszusammenhangs erst die Orientierung gebe. Daher müssten an den Planungszusammenhang hohe Anforderungen gestellt werden. Konkret formuliert Puschke drei Anforderungen an den Planungszusammenhang:[129] Erstens brauche die Vorbereitungshandlung eine *Rechtsgutsverletzung* als *materialen Bezugspunkt*. Anders ausgedrückt: Die Vorbereitungshandlung muss die Rechtsgutsverletzung selbst vorbereiten. Damit sollen solche Vorbereitungshandlungen ausgeschlossen werden, die selbst wiederum in weitere Vorbereitungshandlungen münden. Zweitens müsse der geplante Angriff *hinreichend konkret* sein. Eine rein formale Bezugnahme auf einen bestimmten Straftatbestand genüge nicht. Drittens müsse jedenfalls in den Fällen, in denen der Täter einen eigenen Angriff vorbereite, hinsichtlich der Durchführung seines Angriffs *Absicht* vorliegen. Es genüge nicht, wenn der Vorbereitungstäter lediglich dolus eventualis dahingehend habe, dass er später einmal den Angriff durchführe.

---

125 A.a.O., S. 36.
126 A.a.O., S. 37 f.
127 A.a.O., S. 29.
128 A.a.O., S. 30.
129 A.a.O., S. 30 f.

2. Objektiver Gefährlichkeitszusammenhang

Als objektiven Gefährlichkeitszusammenhang thematisiert Puschke den strukturellen Konnex zwischen dem Rechtsgut und dem Vorbereitungsdelikt, also den äußeren Zusammenhang zwischen der Vorbereitungshandlung und der späteren Rechtsgutsschädigung.[130] Auf diesen Zusammenhang komme es an, da er die Demarkation zum gemeinhin abgelehnten Gesinnungsstrafrecht darstelle.[131] Der objektive Gefährlichkeitszusammenhang besteht laut Puschke nur, wenn die inkriminierte Handlung zur Vorbereitung *geeignet* ist und *typischerweise* Rechtsgutsbeschädigungen vorbereitet.[132]

Unter der *Eignung zur Vorbereitung* ist dabei zu verstehen, dass die Tathandlung des Vorfelddelikts eine Rechtsgutsbeschädigung vorbereiten können muss. Der Gesetzgeber, der eine Handlung als Vorbereitungshandlung qualifizieren und unter Strafe stellen möchte, kann sich dabei nur an solche Handlungen halten, die auch tatsächlich eine Vorbereitung darstellen können. Negativ ausgedrückt, darf eine Handlung, die keine Rechtsgutsbeeinträchtigung vorbereiten kann, auch nicht als Vorbereitungshandlung qualifiziert und unter Strafe gestellt werden. Dies mag trivial erscheinen, ist aber deshalb wichtig, weil die Rede von der „Eignung zur Vorbereitung" auch so verstanden werden kann, als nähme sie den Bezug zwischen der Handlung und der Vorbereitung in den Blick, wobei die Vorbereitung quasi als Erfolg gedacht würde und gefragt würde, ob die Tathandlung imstande ist, eine Vorbereitung *eintreten* oder *folgen zu lassen*. Dann allerdings läge der Fokus auf dem Vorfeld der Vorbereitung. Darum geht es gerade nicht, denn der objektive Gefährlichkeitszusammenhang fragt nach dem Bezug der Vorbereitungshandlung zur Rechtsgutsbeeinträchtigung.[133] Anhand der *Eignung zur Vorbereitung* soll also gefragt werden, ob eine bestimmte Handlung imstande ist, eine Vorbereitungshandlung *zu sein*, also eine Rechtsgutsverletzung vorzubereiten.

Unter der Bezeichnung „tatbestandliche Typisierung"[134] führt Puschke die zweite Begrenzung ein: die inkriminierte Handlung müsse nicht nur geeignet sein, eine Rechtsgutsbeschädigung vorzubereiten, sondern sie müsse diese Beschädigung bei normativer Betrachtung *typischerweise* vorbereiten.[135] Es handelt sich hierbei also im Grunde um eine Schadensprognose aufgrund von Erfahrungssätzen. Das Erfordernis der „tatbestandlichen Typisierung" folge aus dem Grundsatz des Tatstrafrechts, aus dem Grundsatz *nullum crimen sine lege* und aus dem Bestimmtheits-

---

130 A.a.O., S. 31.

131 Ebd., mit Verweis auf BVerfG NJW 2010, 51; *Greco*, in: Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 73 (81 f.); *Hirsch*, FS für Lüderssen, S. 253 ff.; *Hoyer*, Eignungsdelikte, S. 53 f.

132 *Puschke*, in: Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 32.

133 A.a.O., S. 31.

134 A.a.O., S. 32.

135 A.a.O., S. 33.

gebot. Explizit leitet Puschke aus diesem Erfordernis auch ab, dass ein Computerprogramm, das auch das Einscannen und Bearbeiten von Geldscheinen zulässt, ebenso zur Erstellung eines Familienbildbandes diene und daher *kein typisches* Werkzeug für eine Geldfälschung im Sinne des § 149 Abs. 1 Nr. 1 StGB sei.[136]

Eignung zur Vorbereitung und *tatbestandliche Typisierung* sind nach Puschke notwendige Bedingungen der legitimen Vorfeldkriminalisierung. Daneben sei – jedenfalls im Rahmen der grundrechtlichen Erforderlichkeitsprüfung – ebenso der Aufwand von Vorbereitungshandlung und vorbereiteter Verletzungshandlung zu berücksichtigen: Nur wenn durch eine relativ aufwendige Vorbereitungshandlung die Verletzungshandlung erheblich vereinfacht und damit ihre Durchführung wahrscheinlicher werde, könne ein Vorbereitungsdelikt gerechtfertigt werden.[137] Neben diesem Aufwandsverhältnis seien auch das verbleibende Risiko und die veränderliche Hemmschwelle des Vorbereitungstäters zu berücksichtigen.[138] Unklar bleibt dagegen, ob auch Beweisschwierigkeiten bei der Zieltat als legitimierender Aspekt berücksichtigt werden können.[139]

Erst die Kombination aus einer subjektiven Schädigungsabsicht sowie einer objektiv geeigneten und typischen Vorbereitungshandlung ergebe einen hinreichenden rechtsgutsbezogenen Gefährlichkeitszusammenhang.[140]

F. Duttge

Duttge nimmt die Einführung des § 263a Abs. 3 StGB, also das Vorbereiten eines Computerbetrugs, zum Anlass, die Grenzen legitimen Strafens bei Vorbereitungsdelikten zu erörtern.[141] In seinem Beitrag stellt er zunächst die Faustformel auf, dass das tatbestandlich erfasste Verhalten zunächst ein spezifisches Schädigungspotential hinsichtlich eines „anerkannten ‚Kern-Rechtsguts'" aufweisen müsse. Schütze der Straftatbestand dagegen ein neu entworfenes Rechtsgut, so sei nicht auszuschließen, dass er in Wirklichkeit gar kein Rechtsgut oder zumindest ein nicht anerkennenswertes Rechtsgut schützen solle. Die Legitimität dieses Straftatbestands sei dann zweifelhaft.[142] Sodann postuliert Duttge, dass sich ein allgemeingültiger Legitimationsmaßstab nicht allein aus dem geltenden (hier: Vermögens-) Strafrecht ergeben könne, sondern gerade dem „vorfindlichen Normenbestand ent-

---

136 Ebd., Hervorhebung nicht im Original.

137 Mit Verweis auf das Herunterladen einer Bombenbauanleitung, das – jedenfalls im Vergleich zum Beschaffen der Materialen und zum Zusammenbau und mit Blick auf das tatsächliche Attentat – zu unbedeutend für eine eigenständige Pönalisierung sei, a.a.O., S. 34.

138 A.a.O., S. 35.

139 Zunächst zweifelnd, dann die Zweifel relativierend, a.a.O., S. 35 f.

140 A.a.O., S. 33.

141 *Duttge*, FS für Weber, S. 285 ff.

142 A.a.O., S. 295.

hoben“ sein müsse.[143] Unter Rückgriff auf das „gemäßigte Regressverbot“ in den sogenannten Drittbeteiligungsfällen[144] gewinnt Duttge die Regel, dass ein Vorfeldverhalten nur dann legitim unter Strafe gestellt werden könne, wenn sich dem Täter „triftige Anhaltspunkte darbieten, dass durch sein Verhalten eine hervorragende ‚Tatgelegenheit‘ geschaffen wird, die von anderen leicht in Richtung einer definitiven Beeinträchtigung des betreffenden Rechtsguts ausgenutzt werden kann“.[145] Andernfalls verbiete der Vertrauensgrundsatz eine entsprechende Pönalisierung. Damit stellt Duttge also ein Vorhersehbarkeitskriterium auf.

Am Beispiel des § 263a Abs. 3 StGB erörtert Duttge sodann, dass eine solche „qualifizierte Voraussehbarkeit“ der späteren Rechtsgutsschädigung jedenfalls nicht vorliege, wenn sich ein Computerprogramm zum deliktischen Einsatz lediglich *eigne*, daneben aber auch legal eingesetzt werden könne. Diskutabel wäre die Pönalisierung bei Computerprogrammen, die sich *ausschließlich* zu deliktischen Zwecken einsetzen ließen.[146] Dies entspräche dann der Kriminalisierung des Besitzes von Kriegswaffen, der unerlaubten Herstellung bestimmter Arzneimittel oder des unbefugten Umgangs mit Schusswaffen. In diesen Fällen liege ein „eindeutig schädigender bzw. schadensgeneigter Sinnbezug“ vor.[147] Dies liegt wohl hauptsächlich an der von Duttge festgestellten „herausragenden Wertigkeit“ der betroffenen Rechtsgüter.[148] Beim Rechtsgut Vermögen, das vom Computerbetrug und seinem Vorfeldtatbestand geschützt wird, zweifelt Duttge den ausreichenden Wert des Rechtsguts offenbar an, denn hier verlangt er zusätzlich eine „zeitlich-räumliche Komponente“, die zu einer „objektiv-situativen Verdichtung“[149] führt und damit die Pönalisierung rechtfertigt. Dem Vorbereitungsdelikt des § 263a Abs. 3 StGB spricht er diese Verdichtung ab.[150]

In Kurzform: Duttge fordert also, dass es für den Vorfeldtäter qualifiziert voraussehbar sein müsse, dass sein Verhalten zu einer Rechtsgutsschädigung führe. Diese „Voraussehbarkeit“ liege bei einem „eindeutig schädigenden bzw. schädigungsgeneigten Sinnbezug“ vor. Dieser könne sich aus besonders gefährlichen Tatmitteln oder besonders hochwertigen Rechtsgütern ergeben. Je weniger das Rechtsgut wert sei, umso „objektiv-situativ verdichteter“ müsse das Vorfeldverhalten sein. Mit anderen Worten: Umso näher muss das Vorfeldverhalten an der späteren Verletzung liegen.

---

143 A.a.O., S. 297.

144 Hier verweist er auf *Renzikowski*, Restriktiver Täterbegriff und fahrlässige Beteiligung, S. 262.

145 A.a.O., S. 299.

146 A.a.O., S. 300 f.

147 A.a.O., S. 301.

148 A.a.O., S. 303.

149 Ebd.

150 Ebd.

In Kapitel IV. dieses Teils sollen die Gemeinsamkeiten und Unterschiede der soeben vorgestellten Legitimationskonzepte betrachtet werden, damit darauf aufbauend ein Bewertungsmaßstab für Software-Delikte bestimmt werden kann. Zuvor muss jedoch ein Zwischenschritt erfolgen: Die unterschiedlichen Verhaltensweisen in den Software-Delikten müssen getrennt ausgewiesen werden, damit sie überhaupt in Bezug zu einzelnen Legitimitätskriterien gesetzt werden können.

III. Das Vorfeldverhalten in den Software-Delikten

Sieber hat dargelegt, dass innerhalb der Vorfelddelikte unterschieden werden kann zwischen solchen Delikten, die das Vorbereiten als Merkmal im Tatbestand führen und damit einen intentionalen Bezug zum Zieldelikt vertatbestandlichen (= Vorbereitungsdelikte) und solchen Delikten, die diesen Bezug nicht aufweisen, sondern ein in sich abgeschlossenes Vorfeldverhalten normieren (= Anschließungsdelikte). Der erforderliche deliktische Sinnbezug ist in Anschließungs- und Vorbereitungsdelikten offenkundig unterschiedlicher Natur. Deshalb muss in der Legitimationsfrage zwischen diesen Delikten unterschieden werden, und voraussichtlich sind unterschiedliche Maßstäbe anzulegen.

Hier lässt sich noch weiter differenzieren: Betrachtet man die Anschließungs- und Vorbereitungsdelikte des Software-Strafrechts, so stellt man fest, dass diese jeweils ein ganzes Bündel einzelner Tathandlungen aufweisen, die jeweils sehr unterschiedlich sind. Deshalb lässt sich das Vorfeldverhalten, so wie es in den einzelnen Tathandlungen der Software-Delikte aufgeführt ist, in Gruppen abbilden, denen eine jeweils unterschiedliche Art von Unrecht zugrunde liegt. Solche Unterschiede verdienen auch in der Legitimationsdiskussion Berücksichtigung. Bildet man nämlich solche Gruppen, so lassen sich daraus die unrechtsbildenden Faktoren abstrahieren, und die Konzepte zur Strafrechtslegitimation können entsprechend differenzierter auf die Software-Delikte übertragen werden.

Als Tathandlungen werden in den Software-Delikten aufgeführt: das Herstellen eines entsprechenden Computerprogramms,[151] das Sichverschaffen, das Einem-anderen-Verschaffen und das Einem-anderen-Überlassen eines solchen Computerprogramms,[152] das Einführen und das Verbreiten,[153] das Feilhalten,[154] das Verwahren,[155] das Verkaufen,[156] das Vermieten[157] und das Zugänglichmachen.[158] In den

---

[151] Als Tathandlung in allen Software-Delikten aufgeführt, siehe §§ 149 Abs. 1, 202c Abs. 1 Nr. 2, 263a Abs. 3 StGB, 22b Abs. 1 Nr. 3 StVG, 4 ZKDSG, 108b Abs. 2 UrhG.

[152] Nur in §§ 149 Abs. 1, 202c Abs. 1 Nr. 2, 263a Abs. 3 StGB, 22b Abs. 1 Nr. 3 StVG.

[153] Nur in §§ 202c Abs. 1 Nr. 2 StGB, 4 ZKDSG, 108b Abs. 2 UrhG.

[154] Nur in §§ 149 Abs. 1, 263a Abs. 3 StGB, 22b Abs. 1 Nr. 3 StVG.

[155] Nur in §§ 149 Abs. 1, 263a Abs. 3 StGB.

Vorbereitungsdelikten kommt freilich hinzu, dass der Täter durch die jeweilige Tathandlung eine Zieltat vorbereiten muss, wobei es sowohl strafbar ist, wenn er eine eigene Zieltat vorbereitet als auch wenn er die Zieltat eines anderen vorbereitet.

Wer nun ein gefährliches Computerprogramm verbreitet, verwirklicht offenkundig ein anderes Unrecht als derjenige, der sich selbst ein gefährliches Computerprogramm verschafft. Wiederum anderes Unrecht verwirklicht derjenige, der ein gefährliches Computerprogram herstellt. Nachfolgend sollen daher die Tathandlungen kategorisiert werden.

A. Vorbereiten einer eigenen Straftat

In einer ersten Gruppe soll dasjenige Vorfeldverhalten erfasst werden, welches nur unter dem Blickwinkel erklärt werden kann, dass der Täter selbst das Zieldelikt durchführen will und hierzu die entsprechenden Vorbereitungen trifft. Paradebeispiel dafür ist das Sichverschaffen in Vorbereitungsdelikten: Der Vorfeldtäter will ein bestimmtes Zieldelikt verwirklichen und verschafft sich das notwendige Werkzeug, nämlich ein entsprechend einsetzbares Computerprogramm.

Hier wird deutlich, dass das Vorbereiten einer eigenen Straftat im Grunde vorgelagertes Versuchsunrecht ist. Damit schaffen die Vorbereitungsdelikte des Besonderen Teils bereichsspezifische Ausnahmen zu der Grundregel des Allgemeinen Teils, dass Vorbereitungshandlungen straflos sind, und erst der Eintritt in das Versuchsstadium (ausnahmsweise) eine Strafbarkeit auslösen kann.[159] Diese Grenze markiert § 22 StGB, indem er voraussetzt, dass der Täter nach seiner Vorstellung von der Tat zur Tatbestandsverwirklichung unmittelbar ansetzt.[160] Die Vorbereitungsdelikte lockern dieses Erfordernis nun auf, soweit sie das Vorbereiten eigener Zieldelikte unter Strafe stellen. Strukturell betrachtet wird in den Vorbereitungsdelikten das unmittelbare Ansetzen ersetzt durch eine bestimmte Vorbereitungshandlung (etwa das Sichverschaffen eines gefährlichen Computerprogramms), welche so die Anforderungen des unmittelbaren Ansetzens nicht erfüllen würde.

Damit erschließt sich auch für die Legitimationsdiskussion bei Vorbereitungsdelikten eine neue und zugleich alte Erkenntnisquelle: die Strafbegründung des Versuchs. Nach der heute vorherrschenden und dem § 22 StGB zugrunde liegenden

---

156 Nur in §§ 202c Abs. 1 Nr. 2 StGB, 108b Abs. 2 UrhG.

157 Nur in § 108b Abs. 2 UrhG.

158 Nur in § 202c Abs. 1 Nr. 2 StGB.

159 *Sieber*, NStZ 2009, 359 f.

160 Statt aller Jescheck/*Weigend*, Strafrecht AT, S. 518 ff.; Schönke/Schröder-*Eser*, § 22 Rn. 11.

„individuell-objektiven Theorie“ liegt ein strafwürdiger Versuch nur dann vor, wenn der Täter hinsichtlich aller Tatbestandsmerkmale Vorsatz hat[161] und objektiv eine Handlung vornimmt, die nach seiner subjektiven Einschätzung der eigentlichen Tatbestandsverwirklichung unmittelbar vorangeht.[162] Damit muss ein Versuchstatbestand zwei Elemente aufweisen, um legitim zu sein: Erstens ein *subjektives*, nämlich den Vorsatz hinsichtlich der Merkmale der versuchten Tat. Bloße „Tatgeneigtheit“ also Neigung zur Tatbegehung reicht hier nicht aus.[163] Zweitens ein *objektives*, nämlich das Unmittelbare Ansetzen zur Tatbegehung, wobei es ausreicht, wenn sich die Unmittelbarkeit aus der subjektiven Täterperspektive ergibt. Objektiv muss sie nicht vorliegen. Dieses Kriterium wurde eingeführt, um der ausufernden Vorfeldkriminalisierung durch die in der Rechtsprechung angewandte „rein subjektive Theorie“ entgegenzutreten: Das Reichsgericht etwa hatte bereits das Herstellen einer falschen Bescheinigung zum Zwecke einer späteren Täuschung als Betrugsversuch gewertet.[164]

Stellt man nun das bloße *Vorbereiten* einer eigenen Straftat unter Strafe, so mindert man im Vergleich zu einem legitimen Versuchstatbestand die Anforderungen an das objektive Element. Damit der Vorbereitungstatbestand dennoch seine Legitimation erhält, muss diese Minderung möglicherweise in irgendeiner Art kompensiert werden. Zwar wird teilweise vertreten, dass dies schlechterdings unmöglich sei: So vertreten *von Hirsch/Wohlers* in aller Deutlichkeit, dass eine Vorbereitungsstrafbarkeit mit dem Leitbild des bürgerlichen Strafrechts schlicht unvereinbar sei, weil dieses davon ausgehe, dass der mündige Bürger seine Handlungsfreiheit im Rahmen des geltenden Rechts nutze.[165] Das Argument legt aber selbst offen, wann die These möglicherweise ihre Schlagkraft verliert: nämlich immer wenn man nicht davon ausgehen muss oder kann, dass der Bürger sich rechtstreu verhalten wird. Ein Vorbereitungstatbestand ist also denkbar und möglicherweise auch legitim, wenn *sicher feststeht*, dass der betreffende Vorbereitungstäter seine Handlungsfreiheit eben nicht im Rahmen des geltenden Rechts ausüben wird. Mit anderen Worten: Möglicherweise kann bei einem Vorbereitungstatbestand ein verfestigtes subjektives Element etwa in Form einer kriminellen Absicht aufwiegen, dass das objektive Element im Vergleich zum Unmittelbaren Ansetzen des Versuchs stark abgeschwächt worden ist.

---

161 Statt aller Jescheck/*Weigend*, Strafrecht AT, S. 515 m.w.N.

162 Statt aller Jescheck/*Weigend*, Strafrecht AT, S. 516, 518 ff. m.w.N.

163 BGH StV 1987, 528.

164 RGSt 51, 343; Beispiel entnommen aus Jescheck/*Weigend*, Strafrecht AT, S. 513.

165 *von Hirsch/Wohlers*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 201.; vgl. oben II.C.2.

B. Vorbereiten fremder Straftaten

Grundlegend anders ist es jedoch zu bewerten, wenn der Täter die Straftat eines anderen vorbereitet. Denn hierbei wird die Strafbarkeit nicht davon getragen, dass der Vorbereitungstäter einen kriminellen Plan gefasst hat und nun umzusetzen beginnt, vielmehr wird hier in Rechnung gestellt, dass der Täter den Tatplan eines anderen fördert. Er leistet also einen Beitrag zu fremdem Unrecht, wenn er einem anderen die Straftat ermöglicht oder doch zumindest erleichtert. Ein konkretes Beispiel hierfür liegt in den Software-Delikten etwa in der Tatvariante, in welcher der Täter ein Zieldelikt vorbereitet, indem er einem anderen ein deliktisch einsetzbares Computerprogramm verschafft.

Aus diesen Erwägungen wird bereits klar, dass das Vorbereiten einer fremden Straftat in der vorliegenden Form eine Abwandlung klassischer Beihilfe darstellt.[166] Die klassische Beihilfe gemäß § 27 Abs. 1 StGB erfasst die Konstellation, in der eine vorsätzliche und rechtswidrige Straftat eines anderen stattgefunden hat, zu der ein Vorfeldtäter objektiv einen irgendwie förderlichen und kausalen Hilfsbeitrag geleistet hat.[167] Auf der subjektiven Seite muss der Gehilfe dementsprechend einen Vorsatz hinsichtlich der Ausführung der vorsätzlichen und rechtswidrigen Haupttat haben, zum anderen aber auch hinsichtlich seines Hilfsbeitrages, den er als förderlich und kausal für die Haupttat in seinen Vorsatz aufgenommen haben muss.[168] Förderbeiträge zu fremden Straftaten können jedoch uferlos gedacht werden,[169] denn selbst der zeugende Vater und die gebärende Mutter eines späteren Straftäters leisten kausale Förderbeiträge zu dessen späteren Straftaten. Die Beihilfestrafbarkeit muss deshalb begrenzt werden, damit sie ihre Legitimität behält. Für eine solche Begrenzung der Beihilfestrafbarkeit auf ein legitimes Maß haben sich drei Stellschrauben entwickelt: Die Akzessorietät der Teilnahme,[170] die Limitierung der akzessorischen Haftung[171] und die Neutralisierung unverdächtiger Beihilfehandlungen.[172]

---

166 Vgl. *Heger*, ZIS 2008, 274.

167 Ob der Gehilfenbeitrag tatsächlich auch kausal geworden sein muss, ist umstritten. Die Rechtsprechung hält dies grundsätzlich nicht für erforderlich, siehe Jescheck/*Weigend*, Strafrecht AT, S. 693 f.

168 A.a.O., S. 695.

169 BayObLG NJW 1984, 1366.

170 Erst durch das Vorliegen einer vorsätzlichen und rechtswidrigen Haupttat kann auch die Teilnahmehandlung als Unrecht angesehen werden, vgl. Jescheck/*Weigend*, Strafrecht AT, S. 655.

171 Besondere persönliche Merkmale müssen für Täter und Teilnehmer jeweils gesondert berücksichtigt werden, vgl. Jescheck/*Weigend*, Strafrecht AT, S. 656.

172 Einzelne Beihilfehandlungen (etwa berufstypische Verhaltensweisen) müssen unter bestimmten Umständen strafrechtlich „neutralisiert" werden, sodass sie keine Beihilfestrafbarkeit auslösen, vgl. *Rackow*, Neutrale Handlungen, S. 71 ff.

Die Vorbereitungsdelikte erfassen in der Konstellation des Vorbereitens fremder Straftaten solche Beihilfekonstellationen.[173] Dabei lässt der Gesetzgeber jedoch im Unklaren, wie es mit den drei genannten Legitimations-Stellschrauben der Beihilfe in den Vorbereitungsdelikten zu halten ist. Hinsichtlich der Akzessorietät belässt es der Gesetzgeber bei dem Hinweis, dass es genüge, wenn der Täter mit dolus eventualis billigend in Kauf nehme, dass er eine fremde Straftat vorbereite.[174] Damit beschreibt der Gesetzgeber aber lediglich den Vorsatz des Vorbereitungstäters hinsichtlich des eigenen Förderbeitrages. Denn mit anderen Worten muss der Vorbereitungstäter den Vorsatz haben, dass seine Tathandlung den Charakter eines Förderbeitrags hat. Im Umkehrschluss ist damit gesagt, dass das Prinzip der limitierten Akzessorietät zu einer Haupt- oder Zieltat in den Vorbereitungsdelikten gerade nicht gelten soll. Aus den Äußerungen des Gesetzgebers, dass die Vorbereitungsdelikte gerade auch Konstellationen *versuchter* Beihilfe erfassen sollten, lässt sich weiter gehend ableiten, dass in den Vorbereitungsdelikten überhaupt keine Akzessorietät zu irgendeiner Zieltat herrschen soll. Es kommt schlicht nicht darauf an, ob es später zu einer Zieltat kommt oder nicht, und deshalb kann es auch nicht darauf ankommen, ob der Täter dies in seinen Vorsatz aufgenommen hat. Als einzige Begrenzung der Vorbereitungsstrafbarkeit bleibt folglich die Neutralisierung unverdächtiger Vorbereitungshandlungen.

Damit ergibt sich für die Legitimationsdebatte in den Vorbereitungsdelikten eine zweite neue und zugleich alte Erkenntnisquelle. Wenn zu der Kategorie der „unverdächtigen Beihilfehandlungen“ seit Langem Grundsätze entwickelt werden, nach denen bestimmte Tatbeiträge als „strafrechtlich neutral“ zu werten sind,[175] so lassen sich daraus möglicherweise rechtspolitisch verwertbare Grundsätze für die Neutralisierung von Vorbereitungshandlungen ableiten. Aus diesen ließe sich im Umkehrschluss entwickeln, welche Kriterien die konkreten Tatbestandshandlungen erfüllen müssen, damit der Gesetzgeber sie legitim als strafbare Vorbereitungshandlungen werten und in Gesetzesform gießen kann. Unter dem Schlagwort der Neutralisierung unverdächtiger Beihilfe finden sich viele der hier aufgeworfenen Fragen wieder: Auch dort wird etwa diskutiert, wann eine riskante Beihilfe erlaubt sein muss, wann sozialadäquate Jedermannsgeschäfte vorliegen, wann berufsbedingtes Verhalten neutralisiert werden muss, ob eine drittvermittelte fahrlässige Erfolgsverursachung straflos sein muss und insbesondere, welche Anforderungen an einen „deliktischen Sinnbezug“ zu stellen sind.[176]

---

[173] Vgl. *Hefendehl*, in: ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 99 f.

[174] Siehe dazu ausführlich unten Teil 3, I.C., II.C.

[175] Vgl. hierzu eingehend *Rackow*, Neutrale Handlungen, S. 71 ff., 129 ff., 508 ff.

[176] Vgl. hierzu insbesondere *Rackow*, Neutrale Handlungen, S. 129 ff., 281 ff., 367 ff., 507 ff. Kritisch zur „überragenden Funktion“ des subjektiven Tatbestands in solchen Konstellationen *Hefendehl*, in: ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 99.

Lenkt man die Debatte um die Legitimation der Vorfelddelikte in diese Richtung, so lässt sich auch diskutieren, inwiefern eine – möglicherweise abgeschwächte Form der – Akzessorietät in die Vorbereitungsdelikte eingeführt werden kann. Es ist durchaus zu erwägen, den Vorbereitungsvorsatz in den Software-Delikten so auszulegen, dass er sich auch auf die Ausführung eines – in den wesentlichen Umrissen entsprechend bestimmten – Zieldelikts durch einen anderen erstrecken muss.

C. Bewusster Kontrollverlust über gefährliche Gegenstände

Soweit es um Anschließungsdelikte geht, lassen sich unter Legitimationsgesichtspunkten ebenfalls zwei Kategorien unterscheiden. Diese Vorfelddelikte stellen nicht das Vorbereiten einer (eigenen oder fremden) Straftat unter Strafe, sondern ein konkretes Verhalten in Bezug auf ein bestimmtes Computerprogramm – losgelöst von etwaigen Zieltaten. Unterscheiden kann man deshalb erstens solche Fälle, in denen der Täter bewusst die Kontrolle über gefährliche Computerprogramme aufgibt und zweitens Fälle, in denen der Täter gefährliche Computerprogramme (noch) im eigenen Kontrollbereich hat.

In die Kategorie des bewussten Kontrollverlusts fallen Tathandlungen wie das Einem-anderen-Verschaffen und das Einem-anderen-Überlassen eines gefährlichen Computerprogramms. Auch das Verbreiten, Vermieten und Zugänglich-Machen solcher Computerprogramme fallen hierunter. In diesen Tatvarianten begibt sich der Vorfeldtäter bewusst der Kontrolle über ein potentielles Tatwerkzeug und überlässt es der Willkür anderer, eine Rechtsgutsverletzung herbeizuführen. Damit schafft also der Vorfeldtäter bereits eine Gefahrensituation für das Rechtsgut, die er selbst nicht mehr beherrscht. Die zentralen Legitimationsfragen sind in dieser Kategorie folglich, wann der konkrete Gegenstand tatsächlich gefährlich ist, wann ein hinreichender Kontrollverlust eingetreten ist und welchen intentionalen Bezug der Vorfeldtäter zu beidem haben muss.

Die Diskussion um die Legitimation der Vorfelddelikte konzentriert sich typischerweise auf diese Kategorie.[177] Regelmäßig vollziehen die Autoren dabei einen Zweischritt: Zunächst klassifizieren sie die Vorfelddelikte als abstrakte Gefährdungsdelikte, sodann erörtern sie die genannten Legitimationsfragen. Die Vorfelddelikte erfassen aber ein viel breiteres Spektrum von Verhaltensweisen.

---

[177] *Sieber*, NStZ 2009, 358; *Wohlers*, Deliktstypen des Präventionsstrafrechts, S. 281 ff.; *Zieschang*, Die Gefährdungsdelikte, S. 52 ff.

D. Gefährliche Gegenstände im eigenen Kontrollbereich

Eine letzte, aber sehr auffällige Kategorie ist die der gefährlichen Gegenstände im eigenen Kontrollbereich. Gemeint sind hiermit die Tatvarianten, in denen das Hantieren mit einem gefährlichen Gegenstand unter Strafe gestellt wird, obwohl der Handelnde die volle Kontrolle über den gefährlichen Gegenstand innehat und obwohl er keine kriminelle Intention hegt. Zu dieser Kategorie zählen freilich nur Varianten der Anschließungsdelikte, da Vorbereitungsdelikte stets (irgend-)eine kriminelle Intention voraussetzen. In den Anschließungsdelikten fallen die Tatvarianten des Herstellens, Sichverschaffens, des Besitzens und des Einführens gefährlicher Computerprogramme in diese Kategorie. In diesen Fällen ist aufgrund der Tathandlung davon auszugehen, dass der Vorfeldtäter die volle Kontrolle über den Gegenstand ausübt, zugleich sind keinerlei kriminelle Intentionen normiert, die der Vorfeldtäter verfolgen müsste, um sich strafbar zu machen.

Nach den überkommenen Legitimationslehren sind solche Vorfelddelikte, zu denen etwa auch die Strafbarkeit des illegalen Waffenbesitzes gemäß § 51 Abs. 1 WaffG zählt, besonders schwer zu rechtfertigen. Fordert man zur Legitimation eines Vorfelddelikts, dass seine Tathandlung zumindest abstrakt in irgendeiner Weise ein Rechtsgut gefährdet, so muss man beim „zweckfreien Besitz" die Legitimität verneinen.[178] Eine Gefährlichkeit des hier inkriminierten Geschehens kann nämlich nur aus einer Unterstellung resultieren, die gerade nicht vertatbestandlicht ist: Entweder man unterstellt dem Täter, dass er die Gefahrenquelle gerade nicht unter Kontrolle hat oder dass er seine Kontrolle demnächst einschränken wird, oder man unterstellt ihm sogar, dass er die Gefahrenquelle später deliktisch nutzen will.

Würde man die genannten Unterstellungen im Tatbestand normieren, so fiele dieses Vorfeldverhalten im ersten Fall in die obige Kategorie des bewussten Kontrollverlusts (Kapitel C.) oder in die Kategorien des Vorbereitens einer Straftat (Kapitel A. oder B.). Da vorliegend aber gerade nichts normiert ist, müssen diesen Tatvarianten abstrakte Unterstellungen zugrundeliegen: Entweder unterstellt man abstrakt, dass faktisch niemand diese Art der Gefahr beherrschen kann, oder man unterstellt, dass jeder, der eine solche Tathandlung vollzieht, stets eine Zieltat plant. Ohne diese Unterstellungen ist das normierte Verhalten objektiv *und* subjektiv völlig ungefährlich und die Legitimität der Strafnorm höchst fraglich.

Bislang wird dies in der Literatur nicht so klar differenziert. Das mag daran liegen, dass sich die Autoren bei dem Beispiel des illegalen Waffenbesitzes jedenfalls im Ergebnis einig sind und deshalb die (hilfsweise) angebotenen Legitimationsstränge weniger kritisch entworfen oder hinterfragt werden: *Hefendehl* verweist

---

[178] So *Lagodny*, Strafrecht vor den Schranken der Grundrechte, S. 333 ff., der allerdings ein ordnungsrechtliches Verbot für unproblematisch hält (S. 335).

etwa auf den „evidentermaßen gefährlichen Verlauf des inkriminierten Verhaltens“ und das „in den Vereinigten Staaten praktizierte Gegenmodell“.[179] Dabei ließe sich schon fragen, ob *Besitz* wirklich als *Verhalten* klassifiziert werden kann oder ob Besitz nicht eher eine Gegebenheit oder ein Zustand ist. Jedenfalls ist es kein *Verlauf*. Es ist deshalb nicht stimmig, wenn zur Legitimation der Besitzstrafbarkeit auf den „gefährlichen Verlauf des Besitzes“ verwiesen wird.[180] Gemeint ist freilich, dass Waffenbesitz gelegentlich in Rechtsgutsverletzungen umschlägt, was sich aber auf die einfache Aussage reduzieren lässt: Waffen sind gefährlich. Als Legitimation für ein strafrechtliches Verbot taugt ein solcher Erfahrungssatz nicht grundsätzlich, jedenfalls nicht jenseits des Waffenrechts.

Auch ein weiterer Legitimationsstrang lässt sich schwerlich auf vergleichbare Konstellationen des Software-Strafrechts übertragen: die Sicherung des staatlichen Gewaltmonopols.[181] Während bei Waffen nachvollziehbar ist, dass ihre weite Verbreitung das Gewaltmonopol des Staates theoretisch gefährden könnte, liegt dies bei Schadsoftware nicht so nahe. Dieser Gedankengang ist aber auch in sich kein Argument zur Legitimation eines Delikts: Das staatliche Gewaltmonopol besagt, dass es keine mächtigere Gewalt als die des Staates geben darf. Es garantiert also, dass der Staat den Bestand der Rechtsordnung mit höchster Gewalt durchsetzt.[182] Das Gewaltmonopol ist folglich dort verletzt, wo der Staat die Kontrolle verliert. Damit wird deutlich: Das staatliche Gewaltmonopol ist ein Rechtsgut, das der Öffentlichen Sicherheit ähnelt.[183] Wenn man also ausführt, die Strafbarkeit des Waffenbesitzes diene der Sicherung des staatlichen Gewaltmonopols, so stellt man lediglich fest, dass es ein Rechtsgut gibt, auf das sich die Strafbarkeit des Waffenbesitzes bezieht und dessen Gefährdung damit pönalisiert wird. Ob diese Pönalisierung legitim ist, bleibt aber unbeantwortet.

Obwohl oder gerade weil die Strafbarkeit des Waffenbesitzes wenig kritisiert wird, wurde bislang kein übertragbares Konzept für seine Legitimation gefunden. Der Besitz gefährlicher Computerprogramme kann nicht mit Verweis auf das staatliche Gewaltmonopol kriminalisiert werden, und auch ein „gefährlicher Verlauf“ ist beim zweckfreien, bloßen Besitz von Schadsoftware keineswegs evident. Die Legitimation dieser Deliktskategorie bleibt also schwierig.

---

[179] *Hefendehl*, Kollektive Rechtsgüter, S. 144; ähnlich *Nestler*, in: P.-A. Albrecht (Hrsg.), Zustand des Strafrechts, S. 70.

[180] Die Gefährlichkeit ist deshalb schon gar nicht „evident“; auch *Lüderssen*, ZStW 107 (1995), 902, auf den *Hefendehl* hier verweist, spricht selbst nur von „Erfahrbarem“ ohne aufzuschlüsseln, was da eigentlich im Einzelnen erfahrbar sei.

[181] *Lagodny*, Strafrecht vor den Schranken der Grundrechte, S. 333; *Hefendehl*, Kollektive Rechtsgüter, S. 144 m.w.N.

[182] *Hefendehl*, Kollektive Rechtsgüter, S. 145 f.

[183] A.a.O., S. 145.

IV. Bewertungsmaßstab für Software-Delikte

In den oben (II.) dargestellten Legitimationskonzepten hat sich gezeigt, dass die Frage nach der Legitimation von Vorfelddelikten eigentlich die normative Frage nach der Abgrenzung von Verantwortungsbereichen ist. Der Verantwortungsbereich eines Ersthandelnden kann nicht beliebig auf ein potentielles deliktisches Anschlussverhalten eines Zweithandelnden ausgedehnt werden, sondern es braucht ein Vehikel, welches das Vorfelddelikt zugleich legitimiert und begrenzt.

In dieser Arbeit sollen jedoch keine absoluten Legitimitätskriterien festgelegt werden, anhand derer einzelne Vorfelddelikte als legitim oder illegitim bezeichnet würden (A.). Vielmehr soll aus den übereinstimmenden Grundüberlegungen der Autoren ein Referenzrahmen gewonnen werden, anhand dessen die Regelungstechniken der Software-Delikte als *vergleichsweise* legitim oder illegitim bewertet werden können (B.).

A. Keine absoluten Legitimitätskriterien

In den dargestellten Konzepten zur Legitimation von Vorfelddelikten der hiesigen Art (II.) argumentieren die Autoren im Grunde in denselben Kategorien: Zur Legitimation eines solchen Vorfelddelikts ist erforderlich, dass der Täter durch seine Tathandlung eine objektive Risikoerhöhung für das geschützte Rechtsgut herbeiführt und er diese Risikoerhöhung subjektiv in Bezug zu einer späteren Straftat setzt.

Die Übereinstimmungen bestehen jedoch nur, wenn man über unterschiedliche Begrifflichkeiten großzügig hinwegsieht. Beim verbreiteten Begriff des „deliktischen Sinnbezugs“[184] etwa fällt auf, dass kaum ein Autor ihn definiert. Der Begriff wird in der Regel eingeführt und unmittelbar im Anschluss wird erwogen, in welchen Fällen dieser „deliktische Sinnbezug“ vorliegen soll. Auch wenn hierüber dann im Einzelnen häufig Einigkeit herrscht, ist ziemlich unklar, was ein „deliktischer Sinnbezug“ eigentlich ist. Es geht um einen Sinn, aber wovon? Und es geht um einen Bezug, aber geht es um den Bezug *des* Sinns (und wenn ja, seinen Bezug wozu)? Oder geht es um den Bezug *zum* Sinn (und wenn ja, wessen Bezug zum Sinn)? Und bezieht sich das „deliktisch“ eigentlich auf den Bezug oder auf den Sinn? Und was bedeutet „deliktisch“ in diesem Zusammenhang überhaupt, wann ist der Sinn oder der Bezug „deliktisch“? Nach Frischs Ausführungen[185] wird ein „deliktischer Sinnbezug“ aus einer Art Interpretation mit anschließender Vermutung gewonnen: Ein Geschehen wird von außen betrachtet und beurteilt. Wenn man am Ende die Vermutung aussprechen kann, dass der Vorfeldtäter eine Straftat

---

[184] Bei *Duttge* „schädigender bzw. schadensgeneigter Sinnbezug“, siehe oben II.F.

[185] Siehe oben II.B.

ermöglichen oder fördern wollte, bejaht man den „deliktischen Sinnbezug". Demnach ginge es hier aber nicht um einen „deliktischen Sinnbezug", sondern eigentlich um einen deliktsbezogenen Sinn: Der (vermutete) Sinn der Vorfeldhandlung ist deliktsbezogen, weil der Vorfeldtäter (vermutlich) seine Handlung auf eine spätere Deliktsbegehung ausgerichtet hat und diese Deliktsbegehung auch fördern oder ermöglichen wollte.

Frisch trennt zudem gedanklich zwischen der objektiven Risikoerhöhung und dem subjektiven, aber objektiviert zu ermittelnden „deliktischen Sinnbezug". Sieber fasst dagegen risikoerhöhende Momente auch unter das Schlagwort des „deliktischen Sinnbezugs": Er leitet einen „deliktischen Sinnbezug" bei Anschließungsdelikten etwa daraus ab, dass ein Gegenstand „nur (oder ganz überwiegend) deliktisch" genutzt werden kann[186] – was Frisch wohl als objektiv risikoerhöhendes Moment ansehen und nicht dem „deliktischen Sinnbezug" zuordnen würde. In Puschkes Ausführungen entspricht der „objektive Gefährlichkeitszusammenhang" eher der Risikoerhöhung bei Frisch, jedoch erinnert Puschkes hierbei angelegte „typisierende Betrachtungsweise"[187] an Frischs objektivierte Interpretation des „deliktischen Sinnbezugs". Duttges „eindeutig schädigender bzw. schadensgeneigter Sinnbezug" lehnt sich auch eher an objektive risikoerhöhende Momente an. Jedoch fordert auch er, dass der Täter (wohl subjektive) triftige Anhaltspunkte dafür habe, eine hervorragende Tatgelegenheit zu schaffen.[188]

Des Weiteren führt Frisch anhand konkreter Beispiele an, dass seines Erachtens aus einem „sicheren Wissen" des Vorfeldtäters um eine Zieltatbegehung nicht zwingend auf einen „deliktischen Sinnbezug" geschlossen werden könne.[189] Dagegen sehen andere Autoren das „sichere Wissen um die Zieltatbegehung" als zuverlässigen Beleg eines „deliktischen Sinnbezugs" an.[190]

Die Unschärfe des Begriffs zeigt sich aber auch innerhalb einzelner Werke, etwa wenn Frisch nicht nur vom „deliktischen Sinn*bezug*" spricht, sondern gelegentlich auch von „deliktischer Sinn*bezogenheit*" oder wenn er ein Verhalten als „deliktisch sinn*geprägt*" oder „deliktisch geprägt"[191] klassifiziert – damit aber offenbar immer dasselbe meint.[192]

Dies sind nicht nur kleinliche Begriffsstreitigkeiten, sondern in all dem wird ein Dilemma der Legitimationsdiskussion sichtbar: Man will eine absolute Grenze der Legitimität ziehen, hat dafür aber nur unscharfe Begriffe, also auch unscharfe

---

186 Siehe oben II.D.2.

187 Siehe oben II.E.2.

188 Siehe oben II.F.

189 *Frisch*, Tatbestandsmäßiges Verhalten, S. 283 ff.

190 So etwa *Weber* und *Sieber*, siehe oben II.A. bzw. II.D.

191 A.a.O., S. 291, 296, 310 etc.

192 A.a.O., S. 290.

Kriterien zur Hand: Zentrale Schlagwörter der Legitimationsdebatte sind im Grunde Platzhalter für wenig konturierte Ideen. Dies gilt für den „Vertrauensgrundsatz" und das „Regressverbot"[193] gleichermaßen wie für den „deliktischen Sinnbezug".

Zu dem förmlichen Problem unscharfer Begriffe tritt ein inhaltliches Problem hinzu: Soweit die Legitimationskonzepte bei absoluten Legitimitätskriterien im Maß abweichen, kann hierum vor allem mit politischen Argumenten gestritten werden, weniger mit rechtlichen. Sieber etwa trägt vor, dass der Vorfeldtäter bei Vorbereitungsdelikten in vielen Fällen dolus directus hinsichtlich der vorbereiteten Tat haben müsse, andernfalls sei das Vorfelddelikt wegen der fehlenden Tatnähe häufig illegitim.[194] Der Gesetzgeber stellt sich dagegen gelegentlich auf den Standpunkt, dass es bereits ausreiche, wenn der Vorfeldtäter die vorbereitete Tat lediglich „in Aussicht nehme"[195] – was wohl weniger als dolus eventualis ist.[196] Beide sind sich jedenfalls – in Übereinstimmung mit allen dargelegten Legitimationskonzepten – darin einig, dass das Vorfelddelikt illegitim wäre, wenn gar kein subjektiver (deliktischer Sinn-)Bezug erforderlich wäre. Ob sich dieser deliktische Sinnbezug nun aber schon einstellt, wenn der Vorfeldtäter die vorbereitete Tat bloß in Aussicht nimmt, oder ob hierfür dolus eventualis oder gar dolus directus 2. oder 1. Grades erforderlich ist, lässt sich mit *rechtlichen* Argumenten kaum noch fassen. *Politisch* mag es wünschenswert sein, dass der Gesetzgeber die Strafbarkeit auf Absichtsfälle beschränkt. Mit Blick auf die *rechtliche Legitimation* des Straftatbestandes lässt sich jedoch nur sagen: Je stärker der „deliktische Sinnbezug" sichtbar wird, desto eher ist das Vorfelddelikt legitim. Je schwächer der „deliktische Sinnbezug" ist, desto zweifelhafter ist die gesamte Legitimität des Vorfelddelikts.

Damit zeigt sich, dass es derzeit schlicht noch keinen absoluten Legitimitätsmaßstab gibt. Jedenfalls gibt es keinen Maßstab, der so praktikabel wäre, dass man ihn bloß an ein Software-Delikt anlegen müsste, um herauszufinden, ob dieses legitim oder illegitim ist.[197] Für den Gesetzgeber bedeutet dies, dass er sich in der Kriminalpolitik zwar die Frage stellen kann und muss, ob ein neu zu schaffender Straftatbestand *legitim* wäre – dass es hierauf jedoch keine endgültige Antwort geben kann. Vielmehr wird der Fokus auf die Rechtstechnik gelenkt:[198] Je stärker der Gesetzgeber Aspekte wie einen „deliktischen Sinnbezug" rechtstechnisch hervorhebt,

---

[193] Fundamentale Zweifel an deren Schärfe bei *Frisch*, Tatbestandsmäßiges Verhalten, S. 233 ff., der auch die Legitimation von Straftatbeständen nur relativ bestimmen will, siehe *Frisch*, FS für Stree/Wessels, S. 71 ff. Dagegen *Duttge*, FS für Weber, S. 297, der einen „dem Normenbestand enthobenen" Maßstab anlegen will.

[194] Siehe oben II.D.2.

[195] Siehe etwa BT-Drucks. 16/3656, S. 19 rechte Spalte.

[196] Ausführlich hierzu unten Teil 3, I.C.1.

[197] *Nestler*, in: P.-A. Albrecht (Hrsg.), Zustand des Strafrechts, S. 65, geht sogar so weit zu sagen, dass der einzige Konsens in der Legitimationsfrage darin bestehe, dass Strafrecht nur zum Schutze von Rechtsgütern legitim sei.

[198] Vgl. *Frisch*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 227 ff.

desto eher ist der Straftatbestand legitim. Je schwächer beispielsweise die Anforderungen an die Intentionen des Vorfeldtäters rechtstechnisch ausgestaltet werden, desto eher ist der Straftatbestand illegitim. Damit wird deutlich, dass nur solche Je-desto-Sätze als Maßstab für den wertenden Rechtsvergleich im 4. Teil dieser Arbeit bestimmt werden können.

B. Relative Legitimitätsindikatoren

Die oben (II.) dargestellten Legitimationskonzepte weisen in ihren Grundüberlegungen und Grundstrukturen Gemeinsamkeiten auf, aus denen sich ein Referenzrahmen gewinnen lässt, anhand dessen Tatbestandsmodelle als *vergleichsweise* legitim oder illegitim bewertet werden können (1.). Dementsprechend werden als Leitideen dieser relativen Legitimitätsbewertung die Risikoerhöhung und der „deliktische Sinnbezug“ festgelegt (2.).

1. Übereinstimmende Grundstrukturen der Legitimationskonzepte

Die Grundstruktur in den oben (II.) dargestellten Konzepten zur Legitimation von Vorfelddelikten ist im Wesentlichen gleich: Alle Autoren fordern erstens eine objektive Risikoerhöhung für das Rechtsgut und zweitens, dass der Täter einen subjektiven Bezug zu einem späteren Delikt vorweist.

Diese Struktur findet sich bei Weber, der ein „abstrakt gefährliches Verhalten“ in Kombination mit einem „deliktischen Planungszusammenhang“ für erforderlich hält. Bei Frisch setzt sie sich mit anderen Begriffen fort, wenn dieser eine „objektive Risikoerhöhung“ mit einem subjektiven „deliktischen Sinnbezug“ kombiniert. Auch Sieber beschreibt zur Legitimation von Anschließungsdelikten Kriterien der Risikoerhöhung in Kombination mit subjektiven Täteraspekten wie dem kollusiven Zusammenwirken, dem Aufforderungscharakter und dem sicheren Wissen um eine deliktische Anschlusstat. Dies wiederum deckt sich mit Wohlers’ und von Hirschs Forderung, dass das Vorfeldverhalten *bestimmungsgemäß* eine deliktische *Funktion* erfülle. Ebenso fügen sich Siebers Forderungen nach einer besonderen Gefahrschaffung und spezieller Vorsatzmerkmale in das Schema von Risikoschaffung und subjektivem Bezug. Gleiches gilt für Puschkes Forderung nach einem „subjektiven und objektiven Gefährlichkeitszusammenhang“. Ähnlich liegt es bei Duttge, der eine vorhersehbare „objektiv-situativ verdichtete“ Gefahr fordert, die einen „eindeutig schädigenden bzw. schadensgeneigten Sinnbezug“ herstelle.

Insgesamt lässt sich damit festhalten, dass in der Diskussion um die Grenzen legitimen Strafens darin Einigkeit herrscht, dass immer ein objektiver und ein subjektiver Aspekt zusammenkommen müssen. Es muss nämlich zunächst *objektiv* eine Gefahr oder ein Risiko entstehen. Sodann muss feststehen, dass diese objek-

tive Gefahr nicht zufällig, versehentlich oder funktionslos geschaffen wurde, sondern dass ein Subjekt, also ein Täter, diese Gefahr im Rahmen eines deliktischen Vorgangs geschaffen hat. Da dies äußerlich nicht zwangsläufig erkennbar ist, stellt also der Täter *subjektiv* den Bezug zu einer späteren Straftat her und gibt dem Gesamtgeschehen damit ein deliktisches Gepräge. Diese beiden Aspekte werden unter den Autoren unterschiedlich bezeichnet und auch die Einzelkriterien, nach denen der eine oder der andere Aspekt bejaht werden soll, decken sich nicht. Als Maßstab für einen wertenden Vergleich der Legitimität einzelner Tatbestandsmodelle lassen sie sich dennoch verwenden. So werden sie hier unter dem Schlagwort der (objektiven) „Risikoerhöhung" bzw. des (subjektiven) „deliktischen Sinnbezugs" zugrundegelegt.

2. Risikoerhöhung und „deliktischer Sinnbezug" als Legitimitätsindikatoren

Risikoerhöhung und „deliktischer Sinnbezug" sollen als Leitideen in dieser Arbeit die Legitimität eines Vorfelddelikts indizieren: Je stärker das Risiko für das Rechtsgut durch das tatbestandliche Verhalten erhöht wird, desto eher ist der Tatbestand legitimiert. Je offensichtlicher sich ein „deliktischer Sinnbezug" aus dem tatbestandlichen Verhalten ergibt, desto eher ist der Tatbestand legitimiert.

Der Indikator der Risikoerhöhung soll dabei vor allem in seiner negativen Bedeutung relevant sein: Ein Verhalten, das für das Rechtsgut unmittelbar und mittelbar völlig ungefährlich ist, soll nicht unter Strafe gestellt werden.[199] Für die Legitimität streitet dementsprechend, wenn der Straftatbestand so formuliert ist, dass er ausnahmslos ein Risiko für das Rechtsgut impliziert. Dazwischen liegen Tatbestände, die nur *potentielle* Risiken beschreiben, also etwa Situationen, in denen der Täter zwar eine Gefahrenquelle schafft, diese aber zugleich kontrolliert. Hier liegt noch kein Risiko vor, es kann aber eines entstehen, sobald der Täter seine Kontrolle einschränkt. Auch fallen Situationen in diesen Zwischenbereich, in denen der Täter demonstriert, wie ein Rechtsgut verletzt werden kann, um sogleich darzulegen, wie der Rechtsgutsträger sich gegen Angriffe dieser Art verlässlich schützen kann.

Das Schlagwort des „deliktischen Sinnbezugs" ist – wie oben (A.) beschrieben – unsauber und soll hier nur verwendet werden, weil es sich als Schlagwort bereits etabliert hat. Gemeint ist damit, dass geprüft wird, ob die im Tatbestand umschriebene Handlung *nur* dann Sinn ergibt, wenn sie zu einem gedachten Zieldelikt in Bezug gesetzt wird und deshalb selbst bereits *als* deliktische Handlung erscheint. Ist dies der Fall, so soll der „deliktische Sinnbezug" (eigentlich: deliktischer Handlungssinn) bejaht werden. Als Legitimitätsindikator bedeutet dies: Der Tatbestand muss idealerweise so formuliert sein, dass das tatbestandsmäßige Verhalten *objek-*

---

[199] Dies klingt trivial, wird aber noch relevant, siehe Teil 4, I.

tiv keinen anderen Sinn ergibt als den, dass der Vorfeldtäter sich und sein Handeln *subjektiv* in einen deliktischen Vorgang integrieren will. Gegen die Legitimität eines Vorfelddelikts spricht demnach, wenn das darin beschriebene Verhalten auch von rechtstreuen Bürgern verwirklicht wird, die keineswegs Teil krimineller Machenschaften sein wollen, sondern rechtmäßige Ziele verfolgen und dies plausibel erklären können. Damit wird deutlich, dass anhand des deliktischen Sinnbezugs bewertet werden kann, ob und inwieweit der Tatbestand sozialadäquates Verhalten miterfasst. Ein offenkundiger deliktischer Sinnbezug läge etwa vor, wenn im Tatbestand eine Deliktsbegehungsabsicht des Täters normiert ist. Hier würden nämlich nur Fälle erfasst, in denen das Subjekt sein Handeln in einen deliktischen Vorgang integrieren will. Ein deliktischer Sinnbezug kann sich aber auch aus einem Fördervorsatz des Täters ergeben. Er muss sich jedoch nicht zwingend aus dem Tätervorsatz ergeben, sondern kann zumindest theoretisch schon aus dem Tatobjekt folgen. Hierfür müsste das Tatobjekt so beschaffen sein, dass schon aus der Natur der Sache kein rechtmäßiger oder sozialadäquater Umgang mit diesem Gegenstand denkbar ist.

Bei der Bewertung der Software-Delikte nach den genannten Indikatoren kann freilich schon eine gewisse Vorwertung nach den im Zwischenschritt (III.) gebildeten Kategorien von Vorfeldverhalten vorgenommen werden. Die Risikoerhöhung hängt nämlich nicht nur davon ab, wie gefährlich das Tatobjekt ist, sondern auch davon, wie damit verfahren wird: beim „Verbreiten" eines gefährlichen Computerprogramms (Kategorie: Bewusster Kontrollverlust) ist die Risikoerhöhung etwa stärker als beim isolierten Herstellen oder Besitzen (Kategorie: Gefährliche Gegenstände im eigenen Kontrollbereich). Der Grad der Risikoerhöhung mag auch davon abhängen, ob eine fremde oder eigene Straftat vorbereitet wird: Solange nur eine eigene Tat vorbereitet wird, speist sich das Rechtsgutsrisiko vor allem aus den Plänen des Täters. Bereitet er dagegen eine fremde Tat vor, so mag in der Kollusion mit einem Dritten ein vergleichsweise erhöhtes Risiko zu sehen sein.

Der deliktische Sinnbezug variiert vor allem zwischen Vorbereitungs- und Anschließungsdelikten, weil er sich bei Anschließungsdelikten im Grunde nur aus Tatobjekt und Tathandlung in Kombination ableiten kann: Verschafft der Täter ein gefährliches Computerprogramm in seinen eigenen Kontrollbereich, so mag es dafür rechtmäßige Erklärungen geben – abhängig davon, um welche Art von Computerprogramm es sich handelt. Verbreitet der Täter das Computerprogramm dagegen unkontrolliert, fällt eine rechtmäßige Alternativerklärung dafür schwerer. Anhand des deliktischen Sinnbezugs als Indikator lässt sich vor allem die Forderung Wohlers' und von Hirschs berücksichtigen, dass „sozial werthafte Verhaltensweisen" straflos blieben: Für solche Verhaltensweisen kann stets eine rechtmäßige Alternativerklärung gegeben werden, sodass der deliktische Sinnbezug entfällt.

Verworfen wird für die Zwecke dieser Arbeit das Legitimitätskriterium des *unbefugten* Umgangs und der Sorgfaltspflichtverletzung bei von Hirsch und Wohlers beziehungsweise bei Sieber. Dieses Kriterium erscheint für Software-Delikte

weniger aussagekräftig als für andere Vorfelddelikte. Anders als beispielsweise im Waffenrecht gibt es nämlich im Software-Strafrecht keinen ordnungsrechtlichen Unterbau, der gesetzliche Verhaltensvorschriften im Umgang mit Computerprogrammen enthielte. Ein solcher ist zwar nicht zwingend erforderlich, da sich Sorgfaltspflichten auch aus nichtgesetzlichen beruflichen Standards und Kunstregeln ergeben, deren Verletzung auch als unbefugter Umgang beurteilt werden kann, jedoch haben IT-spezifische Sorgfaltspflichten in der Rechtswissenschaft und insbesondere der forensischen Praxis bislang wenig Beachtung gefunden. Deshalb ist das Kriterium des unbefugten Umgangs mit Computerprogrammen zum jetzigen Zeitpunkt noch recht vage. Solange dies so ist, kann die Legitimität eines Software-Delikts kaum dadurch gesteigert werden, dass eine Handlung nur dann für tatbestandsmäßig erklärt wird, wenn sie gegen vorstrafrechtliche Befugnisnormen verstößt.

Bei der Anwendung der Indikatoren Risikoerhöhung und deliktischer Sinnbezug sind stets die Besonderheiten der Informationstechnik zu beachten. Das Risiko eines Computerprogramms speist sich – anders als etwa bei einer Schusswaffe – nicht allein aus dem konkreten Schaden, den das einzelne Computerprogramm anrichten kann. Vielmehr muss zusätzlich in die Gefährlichkeitserwägung einbezogen werden, dass Computerprogramme häufig leicht repliziert und modifiziert werden können und dementsprechend äußerst rasch in ihrer Originalversion sowie in Abwandlungen online verbreitet werden können. Diese Verbreitung ist zudem häufig irreversibel, jedenfalls solange sich ein signifikanter Teil der Menschen für diese Computerprogramme interessiert („das Netz vergisst nichts“). Angesprochen ist damit die Gefahr von Massenkriminalität oder Massenschäden.

Teil 3

Regelungstechniken für Software-Delikte

Im nun folgenden Teil 3 der Arbeit wird untersucht, mit welchen rechtstechnischen Mitteln der Gesetzgeber die Grenzen festlegt, ab denen ein bestimmter Umgang mit bestimmten Computerprogrammen strafbar sein soll. Hierfür werden die maßgeblichen Software-Delikte des deutschen Haupt- und Nebenstrafrechts (I.) sowie ihre Vorläufer in internationalen Instrumenten (II.) analysiert. Der deutsche und die internationalen Gesetzgeber nutzen als regulative Stellschraube hier zum einen die objektive Umschreibung der zu erfassenden Computerprogramme (Typisierung der Computerprogramme), zum anderen die subjektive Tatseite, also den intentionalen Bezug des Vorfeldtäters zu einer späteren Zieltat. Folglich soll nach einem Überblick über die einschlägigen Normen (jeweils A.) zunächst die objektive Umschreibung der tatbestandlichen Software (jeweils B.), sodann der tatbestandlich festgelegte intentionale Bezug des Vorfeldtäters zur Zieltat (jeweils C.) analysiert werden. In den Kapiteln B. und C. werden jeweils die verwendeten rechtstechnischen Ansätze hinsichtlich ihrer inhaltlichen Weite und Schärfe analysiert, sodann wird untersucht, wie sich die jeweilige Regelungstechnik auf die Dual-Use-Problematik auswirkt. Dies wird auch Aufschluss darüber geben, welche Vorstellung der jeweilige Gesetzgeber von der Dual-Use-Problematik zugrunde gelegt hatte und wie er sie folglich lösen wollte. In Kapitel III. dieses Teils wird aufgezeigt, mit welchen Rechtstechniken der deutsche Gesetzgeber der Dual-Use-Problematik im Kriegswaffen- und Exportkontrollrecht begegnet. Diese Analysen liefern das Material für den funktionalen Rechtsvergleich im anschließenden Teil 4 dieser Arbeit.

Als Methode zu dieser Analyse der Regelungstechniken dient die Auslegung. Sie ist insbesondere deshalb die maßgebliche Methode, weil sie den Ausschlag darüber gibt, ob angesichts der Dual-Use-Problematik Chilling Effects drohen. Diese entstehen vornehmlich dann, wenn ein Bürger eine Strafnorm rechtskundig auslegt und zu dem Schluss kommt, dass sein geplantes, sozial nützliches Verhalten von einem Strafgericht möglicherweise als strafbar eingestuft würde, und er deshalb von seinem Vorhaben ablässt. Die Auslegung der gewählten Tatbestandsmerkmale ist also zentral für die Prognose, ob der Erlass einer Strafnorm *Chilling Effects* auslöst.

Einen ersten Schwerpunkt bildet dabei die grammatische Auslegung, da der Wortlaut der Norm ihrem Adressaten unmittelbar zugänglich ist. Besondere Berücksichtigung soll sodann der Wille des historischen Gesetzgebers finden. Die historische Auslegungsmethode spielt zwar üblicherweise eine weniger bedeutende

Rolle und nach Rechtsprechung des Bundesverfassungsgericht dient sie im Regelfall sogar nur dazu, ein bereits gefundenes Ergebnis zu bestätigen,[1] jedoch hat sie im vorliegenden Kontext ein größeres Gewicht: Zum einen sind Software-Delikte regelmäßig relativ junge Delikte, weshalb ein leichter Zugang zu den Gesetzgebungsmaterialien gegeben ist, die von Normadressaten – und später auch Gerichten – regelmäßig als Auslegungshilfe herangezogen werden. Hinzu kommt, dass im Gesetzgebungsverfahren häufig Normadressaten wie IT-Sicherheitsunternehmen selbst als Sachverständige gehört werden. Sie wirken folglich an der Entstehung der Gesetzesmaterialien mit. Schließlich wird zu sehen sein, dass bei einigen Tatbeständen ohne Rückgriff auf die Gesetzesmaterialien gar nicht ermittelt werden kann, welche Regelung der Gesetzgeber eigentlich treffen wollte. Gerade in solchen Fällen misst ihnen auch das Bundesverfassungsgericht erhebliches Gewicht bei[2] oder hält den Blick in die Gesetzesmaterialien zumindest für unbedenklich.[3]

Ergänzend werden die systematische und teleologische Auslegungsmethode herangezogen, damit die Reichweite des Tatbestands ermittelt werden kann.[4] Hier wird offengelegt, dass die teleologische Auslegung nicht immer weiterführt, da mitunter das Telos einer Norm nicht eindeutig festgestellt werden kann.

Schließlich sollen auch die unterschiedlichen Ergebnisse dargestellt werden, zu denen die Literatur und – soweit vorhanden – die Rechtsprechung in der Tatbestandsauslegung kommen. Hierbei soll es jeweils besonders deutlich gemacht werden, wenn Rechtsprechung und Literatur ihre Auslegungsergebnisse nicht mehr allein durch die aufgezeigten Auslegungsmethoden gewinnen, sondern beispielsweise grundrechtskonforme Beschränkungen vorschlagen. Dem liegt folgender Gedankengang zugrunde: Chilling Effects können nur dann zuverlässig ausgeschlossen werden, wenn anhand der beschriebenen Auslegungsmethoden ein eindeutiges Auslegungsergebnis gefunden werden kann. Führen diese Auslegungsmethoden dagegen zu einem zu weiten Ergebnis, das erst in einem zweiten Schritt wieder grundrechtskonform beschränkt wird, so liegen Chilling Effects bereits nahe. Denn für viele IT-Sicherheitsunternehmen wird es ein untragbares Wagnis darstellen, sich scheinbar tatbestandsmäßig zu verhalten, sich dabei auf die Verfas-

---

[1] BVerfGE 34, 269, 288 ff.

[2] BVerfGE 54, 277, 297.

[3] BVerfGE 1, 117, 127.

[4] *Gruber*, Einheitsrecht, S. 22 f., wendet sich dagegen, nationale Auslegungsmethoden auf solches nationales Recht anzuwenden, das aus der Umsetzung völkerrechtlicher Verträge hervorgegangen ist. Ihm zufolge müssten hier „international einheitliche methodische Regeln des internationalen Einheitsrechts“ in der Auslegung angewandt werden. Im Ergebnis dürfte dies jedoch keinen Unterschied machen, da auch bei Anwendung der nationalen Methoden im Rahmen der historischen und teleologischen Auslegung in vergleichbarem Maße berücksichtigt wird, dass die konkrete Norm durch ihren völkerrechtlichen Hintergrund geprägt ist. Dies erkennt *Gruber* auch an, S. 24.

sung zu berufen und darauf zu vertrauen, dass Staatsanwaltschaft und Gerichte den Tatbestand bei der Auslegung grundrechtskonform beschränken.

Dies gilt natürlich gleichermaßen, wenn solche Beschränkungen im Wege europarechts- oder völkerrechtskonformer Auslegung gewonnen werden sollen oder wenn Rechtsprechung oder Literatur gar auf nichtkanonisierte Auslegungsmethoden zurückgreifen, um das Verhalten aus dem fraglichen Tatbestand auszunehmen. Ob es in diesen Fällen tatsächlich zu Chilling Effects kommt, ist freilich eine kriminologische Frage, die hier nicht beantwortet werden kann. Sie muss es aber auch nicht, denn es geht in der vorliegenden Arbeit nicht darum, das Entstehen von Chilling Effects in bestimmten Fällen (positiv) festzustellen, sondern es geht (negativ) darum, eine Gesetzgebungstechnik zu finden, die das Entstehen von Chilling Effects zuverlässig verhindert.

I. Deutsches Strafrecht

Zunächst werden die Software-Delikte des deutschen Strafrechts untersucht. Nach einem Überblick über die bestehenden Strafnormen (A.) wird die erste Stellschraube, nämlich die objektive Umschreibung des Tatobjekts, also die Typisierung der erfassten Software, untersucht (B.). Daran knüpft die Analyse der zweiten Stellschraube, nämlich der subjektiven Tatseite mit dem intentionalen Bezug des Vorfeldtäters zur Zieltat, der zugleich dem Delikt seine Struktur gibt (C.).

A. Überblick

Im März 2002 wurde mit Erlass des Zugangskontrolldiensteschutzgesetzes[5] das erste Software-Delikt des deutschen Strafrechts geschaffen: §§ 3, 4 ZKDSG stellen den Umgang mit „Vorrichtungen zur Umgehung von Zugangskontrolldiensten“ unter Strafe. Ausweislich der Gesetzesbegründung waren von Anfang an insbesondere Computerprogramme als tatbestandliche „Vorrichtungen“ zu verstehen.[6] Im Juni desselben Jahres folgte die Aufnahme von Computerprogrammen als Tatobjekte in den Wortlaut des § 149 Abs. 1 Nr. 1 StGB.[7] Im Jahr 2003 wurde anlässlich der Reform des Urheberrechts durch § 108b Abs. 2 UrhG bereits das nächste, an

---

[5] Gesetz vom 19.3.2002 über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten, BGBl. I 2002, S. 1090.

[6] BT-Drucks. 14/7229, S. 7, rechte Spalte.

[7] Gesetz vom 22.8.2002 BGBl. I 2002, S. 3387.

§ 4 ZKDSG angelehnte Software-Delikt geschaffen.[8] Im selben Jahr folgte mit § 263a Abs. 3 StGB ein Software-Delikt im Vorfeld des Computerbetrugs.[9] Im Jahr 2005 trat § 22b Abs. 1 Nr. 3 StVG in Kraft, der auf Computerprogramme zum Verfälschen von Wegstreckenzählern abzielt.[10] Das vorläufig letzte Software-Delikt wurde 2007 mit § 202c Abs. 1 Nr. 2 StGB eingeführt,[11] der Vorbereitungshandlungen zu den sogenannten CIA-Delikten[12] bestrafen soll.

Insgesamt handelt es sich also um sechs Paragraphen, in denen ein bestimmter Umgang mit bestimmten Computerprogrammen unter Strafe gestellt wird. Dabei pflegt der Gesetzgeber die Angewohnheit, diese Tatbestände als eine Art „allgemeine Vorfelddelikte" zu behandeln und sie in verschiedenen spezielleren Delikten für entsprechend anwendbar zu erklären: § 202c Abs. 1 Nr. 2 StGB nennt etwa die §§ 202a, 202b StGB als Zieldelikte, erfasst aber auch das Vorbereiten einer Tat nach § 303a oder § 303b StGB, da der Gesetzgeber in den dortigen Abs. 3 bzw. 5 jeweils die entsprechende Geltung des § 202c StGB anordnet. § 149 Abs. 1 Nr. 1 StGB verweist selbst nur auf die §§ 146, 148 StGB, jedoch verweisen wiederum die §§ 151, 152, 152a Abs. 5 und 152b Abs. 5 StGB ihrerseits auf § 149 StGB. § 22b Abs. 1 Nr. 3 StVG ist dagegen allein auf die im Tatbestand genannten Nrn. 1 und 2 desselben Absatzes anwendbar. Ebenso erfahren § 4 ZKDSG, § 108b Abs. 2 UrhG und § 263a Abs. 3 StGB keine entsprechende Anwendbarkeit für weitere Zieldelikte. Daraus folgt das wenig elegante Ergebnis, dass einerseits ein Vorfelddelikt auf die einschlägigen Zieldelikte verweisen kann, andererseits aber auch Zieldelikte ihrerseits ein bestimmtes Vorfelddelikt für entsprechend anwendbar erklären können. Insgesamt ergeben sich aus den sechs genannten Tatbeständen somit – je nach Zählweise – bis zu 15 Software-Delikte.

B. Die objektive Umschreibung tatbestandlicher Computerprogramme

Der Gesetzgeber hat bei den bestehenden Software-Delikten jeweils unterschiedliche Formulierungen und Typisierungen verwandt, um die zu erfassenden Computerprogramme tatbestandlich zu umschreiben. Mal ist die Eignung eines Computerprogramms ausschlaggebend, mal seine Bestimmung, sein Zweck, sein Nutzen oder sein Design. Hier lassen sich sechs rechtstechnische Modelle zur Typisierung des Tatobjekts unterscheiden, die im Folgenden einzeln analysiert werden.

---

[8] Gesetz vom 10.9.2003 zur Regelung des Urheberrechts in der Informationsgesellschaft, BGBl. I 2003, S. 1774.

[9] 35. StrÄndG vom 22.12.2003, BGBl. I 2003, S. 2838.

[10] Gesetz vom 14.8.2005, BGBl. I 2005, S. 2412.

[11] 41. StrÄndG vom 7.8.2007, BGBl. I 2007, S. 1786.

[12] CIA-Delikte sind Delikte gegen Vertraulichkeit (**C**onfidentiality), Integrität (**I**ntegrity) und Verfügbarkeit (**A**vailability) von Daten.

1. „Der Art nach zur Begehung [der Zieltat] geeignet“

In einem ersten Modell stellt der Gesetzgeber den Umgang mit Computerprogrammen unter Strafe, die *ihrer Art nach zur Begehung einer bestimmten Straftat geeignet* sind. Diese Tatobjektformulierung kommt nur in § 149 Abs. 1 Nr. 1 StGB zur Anwendung:

> **§ 149 Abs. 1 Nr. 1 StGB Vorbereitung der Fälschung von Geld und Wertzeichen**
> Wer eine Fälschung von Geld oder Wertzeichen **vorbereitet, indem er**
> 1. Platten, Formen, Drucksätze, Druckstöcke, Negative, Matrizen, **Computerprogramme** oder ähnliche Vorrichtungen, **die ihrer Art nach zur Begehung der Tat geeignet sind**,
> 2. […]
> 3. […]
> herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überläßt, wird, **wenn er eine Geldfälschung vorbereitet**, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe, sonst mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 149 Abs. 1 StGB stellt Vorbereitungshandlungen zu § 146, § 148, § 151, § 152, § 152a und § 152b StGB unter Strafe, also Vorbereitungshandlungen zur Fälschung von Geld (§ 146 StGB), Wertzeichen (§ 148 StGB) und Wertpapieren des eigenen Währungsgebiets (§ 151 StGB) und fremder Währungsgebiete (§ 152 StGB) sowie von Zahlungskarten ohne Garantiefunktion, Schecks, Wechseln (§ 152a StGB) und Zahlungskarten mit Garantiefunktion (§ 152b StGB). Soweit die Zieldelikte nicht in § 149 StGB genannt sind, verweisen sie selbst auf § 149 StGB und erklären seine entsprechende Geltung.[13]

In der vorliegenden Arbeit soll die Regelungstechnik analysiert werden, die diesem Tatbestand zugrunde liegt. Zu dieser Regelungstechnik gelangt man, indem man § 149 Abs. 1 Nr. 1 StGB sprachlich bereinigt und von dem konkreten Deliktsbereich abstrahiert. Dann lautet der Tatbestand in diesem „Eignungsmodell“: Wer eine bestimmte Zieltat vorbereitet, indem er *Computerprogramme, die ihrer Art nach zur Begehung der (Ziel-)Tat geeignet sind*, herstellt (etc.) wird, wenn er eine Zieltat vorbereitet, bestraft.

a) Charakteristika dieses Regelungsmodells

Fraglich ist, was unter einem Computerprogramm zu verstehen ist, welches seiner Art nach zur Begehung einer bestimmten Zieltat geeignet ist. In der Auslegung des Merkmals „geeignet“ wird der Blick auf Eigenschaften oder Funktionen des Computerprogramms gelenkt. Konkretisiert man diesen Befund, so lassen sich mehrere Abstufungen treffen.

---

[13] Auf diese Art bestimmt der Gesetzgeber auch den Anwendungsbereich des § 202c StGB, siehe etwa § 303a Abs. 3 oder § 303b Abs. 5 StGB.

aa) „Geeignet“

Grammatisch naheliegend wäre es zunächst, den Ausdruck „geeignet zur Begehung“ so auszulegen, dass ein Computerprogramm dann erfasst ist, wenn es selbst die Zieltat begehen oder doch zumindest herbeiführen oder auslösen kann. Allerdings ist die Begehung einer Zieltat untrennbar an eine Handlung im strafrechtlichen Sinne geknüpft und damit an ein willensgetragenes *menschliches* Verhalten.[14] Ein Computerprogramm kann deshalb keine Straftat begehen, und auch die Idee, dass es ein willensgetragenes menschliches Verhalten auslöst oder herbeiführt, ist noch Science Fiction. Die „Begehung der Zieltat“ muss durch den Verwender geschehen.

Da im Rahmen des Vorfelddelikts ein Computerprogramm hergestellt (o.Ä.) werden muss, welches „*für das Zieldelikt* geeignet“ ist, muss das Programm in irgendeiner engeren Beziehung zur Zieltat stehen. Dementsprechend wäre es sinnvoll, das Merkmal „geeignet“ als „passend“ oder „recht“ auszulegen. Zwar ist damit keine Konkretisierung des „Geeignet“-Merkmals gewonnen, jedoch wird die inhaltliche Richtung klarer: Erfasst sind Computerprogramme, die bei der Begehung einer Zieltat verwendbar, einsetzbar, nützlich oder dienlich sind.[15] Dass das Computerprogramm ausweislich der Tatbestandsformulierung „seiner Art nach“ zur Begehung einer Zieltat geeignet sein muss, lenkt den Blick auf die Funktionen. Denn diese bestimmen maßgeblich seine Art. Es braucht also mindestens eine Funktion, welche für die Begehung einer Zieltat nützlich ist oder durch die das Computerprogramm zur Begehung einer Zieltat verwendet werden kann.[16]

bb) „Unmittelbar“

Bereits 1914 hat das Reichsgericht festgehalten, dass darüber hinaus ein Unmittelbarkeitskriterium einzuführen ist: Nur solche Vorrichtungen sind vom Tatbestand erfasst, mit deren Hilfe Falsifikate *unmittelbar* hergestellt werden können.[17] Als Tatobjekt des Vorfelddelikts kommen also nur solche Werkzeuge in

---

[14] Heute überwiegende Auffassung, siehe nur Jescheck/*Weigend*, AT, S. 223. Darüber hinaus sind die Einzelheiten des strafrechtlichen Handlungsbegriffs seit jeher umstritten, vgl. die Überblicke bei *Hirsch*, ZStW 93 (1981), 836 ff.; NK-*Puppe*, Vor § 13, Rn. 41 ff.

[15] Vgl. auch Duden, Synonymwörterbuch, S. 426, „geeignet“, wo unter 3. folgende Synonyme aufgeführt werden: anwendbar, brauchbar, dienlich, einsetzbar, nutzbar, nützlich, praktikabel, praktisch, tauglich, verwendbar, verwendungsfähig, zweckmäßig.

[16] Die Gesetzesbegründung BT-Drucks. 7/550, S. 229, spricht hier von einer „spezifischen Verwendbarkeit“; ebenso *Husemann*, NJW 2004, 108 f.

[17] Ständige Rechtsprechung, siehe nur RGSt 48, 165; RGSt 55, 47; RGSt 55, 284; RG LZ 1922, 163; RGSt 65, 203; zuletzt wiederholt in BGH 1 StR 297/03 (= wistra 2004, 266), wo allerdings (versehentlich?) vice versa argumentiert wurde: Das fragliche Kartenlesegerät habe nicht unmittelbar der Fälschung gedient, *weil* es nicht zur Herstellung eines Falsifikats geeignet gewesen sei.

Betracht, durch deren Einsatz der Täter des Zieldelikts unmittelbar den Taterfolg des Zieldelikts herbeiführen kann. Dieses Kriterium präzisiert das andernfalls zu weite Tatbestandsmerkmal des Geeignet-Seins im Vorfeldtatbestand, worunter sonst jegliche Gegenstände gefasst werden könnten, die irgendwann auf dem Weg zum Taterfolg der Zieltat Verwendung finden können. Die Fälschungsmittel (hier also: Computerprogramme) müssen daher gebrauchsfertig sein und keiner weiteren Bearbeitung bedürfen.[18] Die Literatur hat dies übernommen und leitet das Kriterium entweder aus dem Tatbestandsmerkmal „geeignet"[19] oder aus dem Merkmal „herstellen"[20] ab, wobei Letzteres unnötig die Bezüge verwischt.

Das Unmittelbarkeitskriterium bedeutet freilich nicht, dass das Computerprogramm den Taterfolg *allein* herbeiführen können müsste. Schon aus praktischer Sicht wäre dies ungewöhnlich: Computerprogramme bauen in aller Regel auf bestimmten Betriebssystemen auf. Diese Betriebssysteme, etwa Windows oder Linux, haben den Sinn, die Systemressourcen des Computers zu verwalten und durch bestimmte Basisdienste den Computer betriebsbereit zu halten. Da ein Betriebssystem hierfür seinerseits viele einzelne Computerprogramme einsetzt, ist es untypisch (wenn auch nicht unvorstellbar), dass ein Computerprogramm *allein*, also ohne Betriebssystem und ohne jedes andere Computerprogramm überhaupt funktioniert. Gerade in dieser Konstellation wird aber auch der Sinn des Unmittelbarkeitskriteriums deutlich: Die Computerprogramme des Betriebssystem können in der Regel nicht *unmittelbar* den Deliktserfolg herbeiführen. Sie schaffen lediglich die Voraussetzungen dafür, dass ein unmittelbar deliktsgeeignetes Computerprogramm auf dem Computer ausgeführt werden kann.

cc) Weitere Einschränkungen?

Mancherorts wird über das Erfordernis einer spezifischen, *unmittelbaren* und finalen Verwendbarkeit hinaus gefordert, dass die Vorrichtung auch *ausschließlich* für Fälschungen verwendbar sein müsse,[21] oder dass die Vorrichtung keine weitere gleich spezielle Funktion haben dürfe.[22] Eine Begründung dafür, dass diese weitere Einschränkung notwendig sei, wird jedoch nicht geliefert. Dieser Vorschlag überzeugt auch deshalb nicht, weil er den Tatbestand über die Maßen einengen würde: Ein Tatverdächtiger müsste nur darlegen, dass die von ihm benutzte Vorrichtung auch zu irgendeinem anderen Zweck als dem einer Geldfälschung verwendet werden kann, um die Vorrichtung dem Anwendungsbereich des § 149 Abs. 1 Nr. 1

---

[18] Statt aller RGSt 48, 165.

[19] LK-*Ruß,* § 149 Rn. 3; MK-*Erb*, § 149 Rn. 3; Schönke/Schröder-*Sternberg-Lieben*, § 149 Rn. 3.

[20] NK-*Puppe*, § 149 Rn. 6.

[21] So etwa MK-*Erb*, § 149 Rn. 3; NK-*Puppe*, § 149 Rn. 4.

[22] So SK-*Rudolphi/Stein*, § 149 Rn. 2.

StGB zu entziehen. Überdies wird diese Tatbestandsbeschränkung weder durch den Gesetzeswortlaut („geeignet") noch durch die Gesetzesbegründung („spezifische Verwendbarkeit"[23]) nahegelegt.

Ebenso überzeugt es nicht, Computerprogramme nur dann unter den Tatbestand zu fassen, wenn sie ein *abgrenzbares Programmmodul* enthalten, welches sich ausschließlich zu Fälschungshandlungen verwenden lässt.[24] Es ist schon nicht ersichtlich, weshalb es rechtliche Auswirkungen haben soll, ob ein Software-Entwickler die Funktionen seines Programms in abgrenzbare Module unterteilt und welche Funktionen in welche Module gruppiert werden. Außerdem ist es seitens des Gesetzgebers ja gerade gewollt, *alle* unmittelbar fälschungsgeeigneten Computerprogramme zu erfassen, unabhängig davon, welcher Teil des Programms (oder genauer: welcher Abschnitt des Programmcodes) letztlich die Fälschungsfunktion beinhaltet. Dementsprechend ist es nur dann konsistent, „allgemeine Graphikprogramme" vom Tatbestand auszunehmen,[25] wenn man davon ausgeht, dass sich mit allgemeinen Grafikprogrammen Falsifikate *nicht unmittelbar* herstellen lassen.[26]

Dennoch verwischt diese Argumentation die Kriterien: Es kommt nicht darauf an, wie speziell oder allgemein die Software ist, sondern allein darauf, ob sich Falsifikate damit *unmittelbar* herstellen lassen. Aus diesem Grunde ist es auch nicht richtig, die „spezifische Verwendbarkeit" zu Fälschungen bei „leistungsfähigen Farbkopierern" zu verneinen.[27] Wenn ein leistungsfähiger Farbkopierer dazu taugt, entsprechendes Papier so zu bedrucken, dass als unmittelbares Ergebnis ein täuschend echtes Falsifikat entsteht, so kann kein Zweifel daran bestehen, dass der leistungsfähige Farbkopierer eine Vorrichtung ist, die zur Begehung von Fälschungsdelikten verwendbar, also geeignet im Sinne des § 149 Abs. 1 Nr. 1 StGB ist.

Für Computerprogramme kann also nichts anderes gelten als für die anderen explizit genannten Fälschungsmittel und die ähnlichen Vorrichtungen des § 149 Abs. 1 Nr. 1 StGB. Computerprogramme sind somit geeignet im Sinne des § 149 Abs. 1 Nr. 1 StGB, wenn sie für die Begehung der Zieltaten spezifisch verwendbar

---

[23] BT-Drucks. 7/550, S. 229.

[24] So aber *Fischer*, § 149 Rn. 3; SK-*Rudolphi/Stein*, § 149 Rn. 2.

[25] So Schönke/Schröder-*Sternberg-Lieben*, § 149 Rn. 3; wohl auch MK-*Erb*, § 149 Rn. 3.

[26] Dafür wiederum mag man anführen, dass viele Software- und Hardwarehersteller in ihren Produkten softwareseitige Sperren einrichten, welche das (Nach-)Bearbeiten von Banknoten, Ausweisen etc. verhindern sollen. Siehe etwa das „Counterfeit Deterrence System" der Central Bank Counterfeit Deterrence Group, welches bspw. in der Bildbearbeitungssoftware „Adobe Photoshop CS" eingesetzt wird, siehe http://helpx.adobe.com/photoshop/cds.html (zuletzt aufgerufen am 15.11.2014).

[27] So aber BeckOK-*Weidemann*, § 149 Rn. 6; Lackner/*Kühl*, § 149 Rn. 2; MK-*Erb*, § 149 Rn. 3; NK-*Puppe*, § 149 Rn. 4; SK-*Rudolphi/Stein*, § 149 Rn. 2; Schönke/Schröder-*Sternberg-Lieben*, § 149 Rn. 3.

sind, wenn der Täter also unter Verwendung des Computerprogramms Falsifikate unmittelbar herstellen kann.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Dieser Vorfeldtatbestand enthält im Vergleich zu den anderen Software-Delikten die Besonderheit, dass das tatbestandliche Computerprogramm dazu eingesetzt werden soll, körperliche Gegenstände herzustellen (Zahlungskarten, Geld, Wertzeichen, …). In den anderen Vorfelddelikten wird es um Computerprogramme gehen, mittels derer in irgendeiner Weise auf Computersysteme oder Daten kompromittierend eingewirkt werden soll. Im vorliegenden Fall ergibt sich daher auch mit Blick auf die Dual-Use-Problematik die Besonderheit, dass grundsätzlich keine IT-gestützten Abwehrmechanismen zum Schutz gegen Angriffe dieser Art vorliegen. Für eine computergestützte Geldfälschung muss keine IT-Schwachstelle ausgenutzt und kein IT-Sicherheitsmechanismus gehackt werden. Will man beispielsweise beim sogenannten *Skimming* gefälschte Zahlungskarten herstellen, so gibt es hiergegen keine technische Sicherungsvorkehrung, die etwa auf einem Kartenrohling vorgesehen wäre, um zu verhindern, dass aus dem Rohling durch eine unautorisierte Beschreibung mit Daten ein Falsifikat wird. Es existiert lediglich der strafrechtliche Normappell, aus dem Rohling kein Duplikat herzustellen.

Deshalb zeigt sich hier auch das Dual-Use-Phänomen nicht in beiden Ausprägungen, die in Teil 1 der Arbeit dargelegt wurden:[28] Oben wurde unter dem Schlagwort des Mehrzweckaspekts ausgeführt, dass eine Ausprägung des Dual-Use-Phänomens daher rührt, dass zum Schutz gegen und zur Abwehr von IT-Angriffen auch IT-Sicherheitsbeauftragte auf das Angriffswerkzeug angewiesen sind, die solche Angriffe selbst simulieren. Dies gilt hier nicht: Es gibt ja gar keinen IT-Sicherheitsbeauftragten, der etwa Kartenrohlinge davor schützen wollte, dass sie mit falschen Daten beschrieben werden. Deshalb können die Konsequenzen der Regelungstechnik des § 149 Abs. 1 StGB für diese Ausprägung der Dual-Use-Problematik nicht am Beispiel der konkreten Zieldelikte, sondern lediglich abstrakt erörtert werden.

Konkret ist hier jedoch zunächst der Multifunktionsaspekt des Dual-Use-Phänomens relevant: Computerprogramme haben in aller Regel mehrere Funktionen. Im vorliegenden rechtstechnischen Modell werden alle Computerprogramme als taugliche Tatobjekte erfasst, wenn sie die oben dargelegte spezielle „deliktische Eignung“ aufweisen – unabhängig davon, ob und wie viele weitere Funktionen sie haben und ob diese weiteren Funktionen legitim sind. Konkret bedeutet das, dass auch solche Computerprogramme erfasst werden, mit denen autorisierte Personen arbeiten. Kreditkartenunternehmen, die ihre Kreditkartenrohlinge mit korrekten

---

[28] Siehe oben Teil 1, I.B.2.

Datensätzen beschreiben müssen, benötigen hierfür bestimmte Hard- und Software. Da hier stets auch ein abredewidriger oder unbefugter Gebrauch der Software vorstellbar ist, sind die entsprechenden Computerprogramme auch zur Herstellung von unautorisierten Duplikaten im Sinne des § 152b Abs. 1 StGB geeignet. Diese Regelungstechnik versucht also nicht, den Unterschied zwischen kriminellem und legitimem Verhalten bereits im objektiven Tatbestand im Tatobjekt zu verankern. Taugliche Tatobjekte sind zunächst alle deliktisch einsetzbaren Werkzeuge und angesichts der umfassenden Tathandlungen des § 149 Abs. 1 StGB (herstellen, sich verschaffen, einem anderen verschaffen oder überlassen, feilhalten, verwahren)[29] kommt grundsätzlich eine Vielzahl der Personen, die irgendwie am Produktionsprozess von Kreditkarten oder anderen Schutzobjekten der §§ 146, 148, 151, 152, 152a, 152b beteiligt sind, als Täter des Vorfelddelikts in Betracht. Die Unterscheidung zwischen kriminellem und nichtkriminellem Verhalten hängt bei Verwendung dieser Regelungstechnik allein am Tatbestandsmerkmal des *Vorbereitens* einer Zieltat.[30]

Gleiches gilt freilich, wenn man *abstrakt* betrachtet, welche Auswirkungen diese Regelungstechnik unter dem Mehrzweckaspekt der Dual-Use-Problematik hätte, also in den Fällen, in denen ein Computerprogramm sowohl von einem Kriminellen zum deliktischen Einsatz benötigt wird als auch von einem IT-Sicherheitsbeauftragten zum Suchen und Beheben von Schwachstellen im Computersystem erforderlich ist. Ein solches Computerprogramm ist nach vorliegender Regelungstechnik stets tatbestandsmäßig. Deshalb ist etwa das Herstellen eines solchen Computerprogramms eine tatbestandsmäßige Handlung, unabhängig davon, ob der IT-Sicherheitsbeauftragte das Programm nur für sich selbst herstellt oder ob der Kriminelle es für seinen späteren Einsatz programmiert oder ob etwa ein „ehrenamtlicher" Hacker ein solches Programm als *Proof of Concept* entwickelt, um zu beweisen, dass eine bestimmte Sicherheitslücke bei bestimmten Systemen existiert und ausgebeutet werden kann. Auch in diesen Fällen hängt eine Strafbarkeit der jeweils infrage kommenden Personen lediglich davon ab, ob sie eine Zieltat *vorbereiten*.

2. Begehung der Zieltat als Zweck

In einem zweiten Modell stellt der Gesetzgeber den Umgang mit Computerprogrammen unter Strafe, „deren Zweck die Begehung einer Zieltat ist". Dieses Tatbestandsmodell ist Gegenstand lebhafter Diskussion in Rechtsprechung und wissenschaftlicher Literatur sowie vor allem auch in der Zivilgesellschaft. Ange-

---

[29] *Scheffler* kritisiert diese unspezifische Aufzählung von Tathandlungen als gesetzgeberische Schrotschusstechnik, ZStW 117 (2006), 796.

[30] Siehe dazu unten C.1.

wandt wurde es in § 263a Abs. 3 StGB, § 202c Abs. 1 Nr. 2 StGB und in § 22b Abs. 1 Nr. 3 StVG. Exemplarisch sei hier § 202c Abs. 1 Nr. 2 StGB wiedergegeben:

> **§ 202c Vorbereiten des Ausspähens und Abfangens von Daten**
> Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
> 1. […]
> 2. **Computerprogramme, deren Zweck die Begehung einer solchen Tat ist**,
> herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 202c Abs. 1 Nr. 2 StGB stellt Vorbereitungshandlungen zu § 202a, § 202b, § 303a und § 303b StGB unter Strafe, also Vorbereitungshandlungen zum Ausspähen von Daten (§ 202a StGB), Abfangen von Daten (§ 202b StGB) zur rechtswidrigen Datenveränderung (§ 303a StGB) und zur Computersabotage (§ 303b StGB). Ähnlich wie § 149 Abs. 1 StGB erklärt auch § 202c StGB selbst nur seine Geltung für das Vorfeld der § 202a und § 202b StGB. Das Vorbereitungsdelikt gilt aber auch im Vorfeld der § 303a und § 303b StGB, weil dort die entsprechende Geltung explizit normiert ist, siehe § 303a Abs. 3 bzw. § 303b Abs. 5 StGB. § 263a Abs. 3 StGB stellt ein Vorfelddelikt allein zu § 263a Abs. 1 StGB (Computerbetrug) dar, und § 22b Abs. 1 Nr. 3 StVG erfasst das Vorfeld zu den Delikten des § 22b Abs. 1 Nr. 1 und § 22b Abs. 1 Nr. 2 StVG („Missbrauch" von Wegstreckenzählern bzw. Geschwindigkeitsbegrenzern). Folglich kommt dieses „Zweckmodell" als Regelungstechnik im Vorfeld von sieben verschiedenen Straftaten zum Einsatz.

Bereinigt man die Vorfelddelikte dieses rechtspolitischen Modells sprachlich für die Ziele der vorliegenden Arbeit, so lautet der Tatbestand: Wer eine bestimmte Zieltat vorbereitet, indem er *Computerprogramme, deren Zweck die Begehung der Zieltat ist*, herstellt (etc.), wird bestraft.

a) Charakteristika dieses Regelungsmodells

Der Begriff des Zwecks wird in diesen Tatbeständen unter sprachlichen Gesichtspunkten sehr ungewöhnlich verwendet, weshalb sich die grammatische Auslegung schwierig gestaltet. Der Wortlaut spricht von Computerprogrammen, deren *Zweck* die Begehung einer Zieltat *ist*. Folglich geht es um einen Zweck, den das Computerprogramm *hat*, also einen „Zweck des Computerprogramms". Semantisch ist dies äußerst ungewöhnlich, weil mit dem Begriff „Zweck" üblicherweise das Ziel oder der Sinn einer *Handlung* ausgedrückt wird. Vorliegend wird „Zweck" jedoch strukturell so verwandt, dass er sich auf einen Gegenstand bezieht (nämlich das Tatobjekt), nicht etwa auf eine Handlung (etwa die Tathandlung).

aa) Das semantisch-sprachlogische Problem

Durch die gewählte Formulierung erscheint der „Zweck eines Computerprogramms" als eine Eigenschaft eines Gegenstandes.[31] Es stellt sich damit die Frage, wie man die eigentliche Bedeutung des Begriffs „Zweck" in das vorliegende rechtstechnische Modell „übersetzen" kann, sodass daraus auch in dieser ungewöhnlichen Verwendung als Eigenschaft eines Gegenstandes ein Sinn gewonnen werden kann. Hierfür soll zunächst eine typische Zweckkonstellation untersucht werden, um zu klären, welche Funktionen darin die Begriffe „Zweck", „Mittel", „Objekt", „Subjekt" und „Handlung" erfüllen.

Üblicherweise beschreibt der Zweck eine Beziehung zwischen dem Subjekt und seiner Handlung sowie dem gegebenenfalls eingesetzten Objekt (=Mittel):[32] Der Zweck ist das Ziel oder der Sinn, den das Subjekt mit der Handlung verfolgt. Er ist damit causa finalis für die Handlung des Subjekts und seine Auswahl und Anwendung der Mittel.[33]

Etymologisch bezeichnete das alt- und mittelhochdeutsche Wort *zwec* ursprünglich einen Pflock, insbesondere den Pflock, der die Mitte einer Zielscheibe markiert.[34] Spätestens seit dem 15. Jahrhundert wird dies sinnbildlich verwandt, sodass „Zweck" heute als Synonym zu „Ziel" verstanden wird und nicht nur das Ziel eines Schusses, sondern jeglicher Handlung ausdrücken kann.[35]

Einen Zweck wird man deshalb zunächst festlegen, bestimmen oder setzen; sodann verfolgt man ihn, um ihn schließlich zu erreichen oder zu verfehlen.[36] Der Zweck kann also ein erklärender Gedanke sein, etwa wenn eine Person einen Zweck setzt, mit dem sie ihre Handlungen rechtfertigen oder nachvollziehbar

---

[31] Vgl. BT-Drucks. 16/5449, S. 4 rechte Spalte; *Popp*, MR-Int 2007, 87.

[32] *Hegel*, Logik für die Mittelklasse, spricht in §§ 128, 129, 131 jedoch auch von einer „inneren Zwekmäßigkeit", die vorliege, wenn „ein Daseyendes seinen Begriff in sich selbst hat, und zugleich Zwek, Mittel, und sich realisirender und realisirter Zwek an ihm selbst ist." Dies deutet jedoch auf das philosophische Großthema der Reflexion auf ontologische, kosmologische oder theologische Zweckursachen der Dinge, siehe dazu zusammenfassend *Ritter/Gründer/Gabriel*, Historisches Wörterbuch der Philosophie, S. 1486 ff.; vgl. auch *Popp*, GA 2008, 381.

[33] *Grimm*, Deutsches Wörterbuch Band 32, S. 959 linke Spalte; *Jhering*, der Zweck im Recht, S. 1; *Luhmann*, Zweckbegriff und Systemrationalität, S. 7; *Regenbogen/Meyer,* Wörterbuch der philosophischen Begriffe, S. 753; *Wahrig*, Deutsches Wörterbuch, S. 1446, wo allerdings auch in einem Beispielsatz von einem *Gerät* die Rede ist, das „seinen Zweck" erfülle. Dies dürfte jedoch eine umgangssprachliche Beispielformulierung sein.

[34] *Grimm*, Deutsches Wörterbuch Band 32, S. 958 linke Spalte; *Regenbogen/Meyer,* Wörterbuch der philosophischen Begriffe, S. 753.

[35] *Kluge*, Etymologisches Wörterbuch, S. 1020.

[36] Vgl. auch Duden, Synonymwörterbuch, S. 1133, „Zweck", wo als Synonyme neben Bedeutung und Sinngehalt vor allem Absicht, Bestreben, Intention u.Ä. genannt werden.

machen kann. Auch kann ein Zweck „von außen“ interpretiert oder auf ihn geschlossen werden, etwa wenn ein Dritter das Verhalten einer Person beobachtet und Vermutungen darüber anstellt, welchen Zweck die Person verfolgt.[37] Der Zweck ist damit etwas Vergeistigtes, Erläuterndes, das zwingend mit der Handlung einer Person verknüpft ist. Diese Handlungen haben den Zweck, den das handelnde Subjekt vor oder während der Handlung autonom setzt. Objekte haben dagegen keine intrinsischen Zwecke.[38] Sie sind als Werkzeuge des handelnden Subjekts vielmehr *Mittel* (zum Zweck).

Bei einer strengen grammatischen Auslegung im vorliegenden Tatbestandsmodell ergibt sich beim „Zweck eines Computerprogramms“ somit ein doppeltes Paradoxon: Zwecke werden immer *subjektiv* gesetzt und mit *Handlungen* verknüpft, während der objektive Tatbestand hier einen *objektiven* Zweck voraussetzt, der einem *Gegenstand* wie eine Eigenschaft anhaftet. Semantisch steht man damit vor dem Problem, dass diese Paradoxien nicht auflösbar sind. Wenn der Tatbestand grammatisch keinen Sinn ergibt, muss man bei sehr strenger Wortlautauslegung folglich zu dem Schluss kommen, dass dieses Delikt keinen Anwendungsbereich hat. Da die Wortlautgrenze jedoch nicht durch Wörterbücher und Lexika bestimmt wird, sondern weithin der Auslegung zugänglich ist,[39] soll nachfolgend untersucht werden, was der Gesetzgeber teleologisch-historisch eigentlich zu regeln versucht hat. Sodann ist zu fragen, ob das gefundene Ergebnis unter Beachtung von Art. 103 Abs. 2 GG noch in den tatsächlichen Wortlaut der hier interessierenden Tatbestände hineingelesen werden kann.

In diesem Zusammenhang kann man dann von einem „Zweck des Computerprogramms“ sprechen, wenn man von vornherein anerkennt, dass es nicht darum geht, eine Eigenschaft des Computerprogramms zu untersuchen und als dessen Zweck zu bezeichnen oder zu bewerten. Vielmehr ist von Anfang an davon auszugehen, dass eine *Beziehung* untersucht wird, welche zwischen drei Eckpunkten besteht:[40] Der Zweck ist die Beziehung zwischen erstens dem Gegenstand (Computerprogramm), zweitens einem Subjekt (etwa dem Programmierer, dem Verwender oder auch jedermann) und drittens einer Handlung.

Um sinnvoll von einem „kriminellen Zweck des Computerprogramms“ sprechen zu können, muss man einen Zweischritt vollziehen: In einem *ersten* Schritt müssen die Eckpunkte dieser dreistelligen Zweckbeziehung konkret festgelegt werden. Es muss also definiert werden, welches Subjekt und welche Handlung zu dem Computerprogramm (= Objekt) in Beziehung gesetzt werden. Dies ist essentiell dafür, dass

---

[37] Vgl. *Grimm*, Deutsches Wörterbuch Band 32, S. 959 linke Spalte; *Prechtl*, Philosophie-Lexikon, S. 592.

[38] So auch *Popp*, GA 2008, 380.

[39] Siehe *Kudlich/Christensen*, JR 2011, 148 f.

[40] Vgl. *Popp*, GA 2008, 381 („dreistellige Beziehung“).

überhaupt ein Zweck ermittelt werden kann (Zweckermittlung). In einem *zweiten* Schritt lässt sich sodann das normative Urteil fällen, ob die drei Endpunkte so zusammenwirken, dass das Gesamtgeschehen auf die Begehung von Straftaten ausgerichtet ist – ob also das festgelegte Subjekt, die festgelegte Handlung und das Computerprogramm in einer solchen Beziehung zueinander stehen, dass sie gleich einer „unheilvollen Allianz" als kriminelle Zweckbeziehung bezeichnet werden kann. Konkret ausgedrückt: das Subjekt muss bei seiner Handlung mit dem Objekt ein kriminelles Ziel verfolgen, und es muss aus der Beziehung von Subjekt, Handlung und Gegenstand objektiv zu schließen sein, dass dies so ist.

Bei Software-Delikten ist der maßgebliche Gegenstand immer das Computerprogramm. Deshalb muss vor dem ersten Schritt der Zweckermittlung lediglich präzisiert werden, welches Subjekt und welche Handlung in den Blick genommen und bewertet werden sollen.

Als *Subjekt* kommen im Grunde alle Personen in Betracht, die mit dem Computerprogramm zu tun hatten oder haben. Funktional lassen sich diese jedoch in zwei Gruppen teilen: Eine erste Gruppe könnten etwa die „historischen Hersteller" bilden, die zu der gegenwärtigen Form des Computerprogramms beigetragen haben. Dies ist bewusst so unscharf formuliert, da die Herstellergruppe in diesem weiteren Sinne auch den Designer, Entwickler, Programmierer, möglicherweise auch einen Modifizierer des Computerprogramms erfassen soll. Andererseits kann auch „der Vorfeldtäter" maßgebliches Subjekt sein. Stellt man auf Vorfeldtäter ab, so kann dies im konkreten Einzelfall freilich auch der Hersteller sein. Es kann aber auch ein Intermediär sein – etwa im Falle des Verkaufens, Einem-Anderen-Verschaffens und Vermietens. Schließlich mag der Vorfeldtäter auch zugleich Endverwender sein. Da das Subjekt in diesem Gedankenspiel der maßgebliche Zwecksetzer ist, muss man in diesen Konstellationen jeweils fragen, ob das Subjekt durch seine Handlung Straftaten bezweckt, also deren Begehung herbeiführen will.

Die maßgebliche *Handlung* muss freilich immer eine des gedachten Subjekts sein, da ja nur das Subjekt den Zweck setzen kann. Um im vorliegenden „Zweckmodell" die Frage zu beantworten, ob ein konkretes Computerprogramm tatbestandsmäßig ist, muss dann immer gefragt werden, ob das hinzugedachte Subjekt mit seiner hinzugedachten Handlung bezweckt hat, dass eine Straftat begangen werde. Dies soll nachfolgend veranschaulicht werden.

Beim maßgeblichen Subjekt kann man – wie gesagt – differenzieren zwischen dem *historischen Hersteller*, einem *Intermediär* und dem *Endverwender*. Legt man erstens als entscheidungserhebliches Subjekt den *historischen Hersteller* fest, so ermittelt man den kriminellen Zweck unabhängig von etwaigen anderen Vorfeldtätern (etwa den Zwischenhändlern) und unabhängig vom späteren Täter eines Zieldelikts. Ein Computerprogramm ist in diesem Gedankenexperiment immer tatbestandsmäßig, wenn sein Hersteller mit der Herstellung des Programms ursprünglich den kriminellen Zweck verfolgt hat, dass (irgendjemand) das Compu-

terprogramm bei der Begehung von Straftaten einsetzt. In dieser Konstellation würde der Hersteller ein Computerprogramm quasi in der Herstellungsphase mit dem kriminellen Zweck versehen, der dem Computerprogramm in der Folge stets anhaftet, auch wenn es sich in den Händen eines Zwischenhändlers, eines Endverwenders oder einer sonstigen Person befindet.

Legt man dagegen zweitens den *Intermediär* als maßgebliches Subjekt fest, so liegt ein krimineller Zweck vor, wenn dieser Intermediär mit der Weiterleitung des Programms bezweckt, dass Straftaten begangen werden – unabhängig davon, welche Zwecke der Hersteller des Programms ursprünglich verfolgt und ebenso unabhängig davon, welche Zwecke der Endverwender, also der Abnehmer des Computerprogramms am Ende tatsächlich verfolgt. In diesem Gedankenexperiment kann ein Computerprogramm selbst dann tatbestandsmäßig sein, wenn es ursprünglich von einem gutwilligen Hersteller entworfen worden ist. Es ist in diesem Gedankenexperiment sogar bereits in der Herstellungsphase tatbestandsmäßig, eben weil schon in diesem Moment ein böswilliger Intermediär gedacht wird, der dieses Programm in krimineller Absicht weitervermitteln wird. Hierbei ist freilich nicht nötig, dass der Intermediär selbst eine Straftat zu verwirklichen beabsichtigt: Es genügt bereits, wenn er will, dass ein anderer im Anschluss an die Vorfeldhandlung eine Straftat begeht.

Stellt man dagegen drittens auf einen gedachten *Endverwender* ab, so spielen Absichten des Herstellers und des Intermediärs keine Rolle. Ausschlaggebend ist allein, ob der gedachte Endverwender kriminelle Zwecke verfolgt. Ist dies zu bejahen, so ist nach diesem Gedankenexperiment das Computerprogramm ein taugliches Tatobjekt, auch schon in dem Moment, in dem es sich noch in den Händen eines gutwilligen Herstellers und möglicherweise ebenso gutwilligen Intermediärs befindet.

Hier wird also deutlich: In dem „Zweckmodell“ wird ein konkretes Computerprogramm zum Anlass genommen, Gedankenexperimente durchzuspielen. Darin nehmen gedachte Subjekte gedachte Handlungen vor, die in einem Bezug zu dem konkreten Computerprogramm stehen. Sobald in einem dieser Gedankenexperimente eine kriminelle Absicht verzeichnet wird, liegt ein krimineller Zweck vor, der dann – in der Realität – dem konkreten Computerprogramm „angeheftet“ wird. In der Diktion des Gesetzgebers: Das Computerprogramm hat dann einen kriminellen Zweck. Es ist folglich tatbestandsmäßig.

bb) Die Gesetzesmaterialien

In den Gesetzesmaterialien finden sich keine präzisierenden Ausführungen zur Frage, was hier mit dem „Zweck eines Computerprogramms“ gemeint ist. Zu der Frage, wie der Zweck strukturell zu ermitteln ist, also auf *wen* und auf *welche Handlung* es ankommt, finden sich in den Materialien nur verklausulierte Ausführungen: Vor allem irritiert es, dass der Gesetzgeber in seinen Ausführungen zum

„Zweck des Computerprogramms“ weitere Begriffe mit ähnlichem Abstraktionsgrad einführt: So ist etwa von der „Bestimmung des Computerprogramms“, von seiner „(objektivierten) Zweckbestimmung“, der „objektiven Zweckbestimmung“,[41] dem „funktionalen Zweck“[42] oder dem „objektiven Zweck“[43] die Rede. Dabei wird nicht klar, ob der Gesetzgeber mit dem Begriff „Bestimmung“ bewusst ein Aliud zum „Zweck“ verwendet, etwa um das Tatbestandsmerkmal inhaltlich in die Nähe einer Widmung zu rücken und damit den Fokus auf den Schöpfer des Programms – oder irgendeinen anderen Widmungsgeber – zu legen. Möglicherweise sieht der Gesetzgeber „Zweck“ und „Bestimmung“ aber auch schlicht als Synonyme an. Beim Begriff der Zweckbestimmung ist darüber hinaus unklar, ob damit die „Bestimmung des Programms durch seinen Zweck“ oder das „Bestimmen des Programmzwecks“ (etwa durch oben genannte Subjekte oder sogar den *Rechts*anwender) gemeint ist. Gleichermaßen ungeklärt ist, ob der Gesetzgeber einen Unterschied zwischen der „objektivierten“ Zweckbestimmung und der „objektiven“ Zweckbestimmung sieht und falls ja, worin dieser läge.[44] Der Begriff des objektiven Zwecks schließlich ist eine Contradictio in adiecto[45] und ohne weiter erklärende Ausführungen dazu, unter welchem Aspekt ein Zweck als objektiv angesehen werden soll, völlig unbrauchbar.

Später führt der Gesetzgeber jedoch aus, dass dem Computerprogramm „die illegale Verwendung immanent“[46] sein müsse, was wiederum der Fall sei, wenn das Computerprogramm „nach Art und Weise des Aufbaus oder [der] Beschaffenheit auf die Begehung von Computerstraftaten *angelegt*“ sei.[47] Damit wird das „Anlegen“ des Computerprogramms also wohl das Entwerfen oder Designen als maßgebliche *Handlung* betont. Als relevantes *Subjekt* kämen hier entsprechend nur die historischen Hersteller in Betracht, die das Computerprogramm entworfen, entwickelt und geschrieben haben. Dies wird zwar in der Begründung zum Gesetzesentwurf nicht ausdrücklich gesagt, jedoch heißt es auch in der Beschlussempfehlung des Rechtsausschusses, dass solche Computerprogramme einen kriminellen Zweck haben, die „in erster Linie dafür ausgelegt oder hergestellt [werden], um damit Straftaten nach den §§ 202a, 202b StGB zu begehen“.[48] Wird demnach der *Hersteller* in den Fokus gerückt, so müssten die Absichten eines gedachten *Verwenders* unberücksichtigt bleiben.

---

41 Alle BT-Drucks. 16/3656, S. 12 linke Spalte.

42 BT-Drucks. 16/3656, S. 19 linke Spalte.

43 BT-Drucks. 15/1720, S. 11.

44 Gegen eine unterschiedliche Bedeutung *Valerius*, JR 2010, 86.

45 Vgl. *Popp*, GA 2008, 381.

46 BT-Drucks. 16/3656, S. 19 linke Spalte.

47 Ebd.

48 BT-Drucks. 16/5449, S. 4 rechte Spalte.

An dieser Stelle ist jedoch noch zu vermerken, dass der Rechtsausschuss seine Auffassung auf Art. 6 des Übereinkommens über Computerkriminalität stützt, der in seiner deutschen Übersetzung eine leichte Akzentverschiebung erfahren hat: Im englischen Originaltext geht es um ein „computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5". In der deutschen Sprachfassung wurde die Stellung des „primarily" verändert und Art. 6 übersetzt mit: „[ein Computerprogramm, das] *in erster Linie* dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen."[49] Während also im Englischen das „primarily" sich auf die Begehung von Straftaten bezieht und somit ausdrückt, dass unter mehreren denkbaren Verwendungszwecken die kriminelle Verwendung im Vordergrund stehen muss („dafür ausgelegt, in erster Linie der Begehung von Straftaten zu dienen"), bezieht sich das „in erster Linie" in der deutschen Sprachfassung auf das Anlegen oder Herrichten des Computerprogramms („in erster Linie dafür ausgelegt, zu Straftaten eingesetzt zu werden"). Ob diese feinsinnigen Variationen tatsächlich im Einzelfall zu unterschiedlichen Ergebnissen in der Sache führen, mag hier dahinstehen. Jedenfalls legt die deutsche Sprachfassung im Vergleich zur englischen Sprachfassung eine leichte Akzentuierung auf den Herstellungs- oder Anpassungsvorgang. Diese übersetzungsbedingte Akzentverschiebung hat der Rechtsausschuss offenbar nicht gesehen, sonst hätte er in seiner Argumentation hierzu Stellung nehmen müssen.

Legt man also ein Zweckverständnis zugrunde, wonach der Zweck eine Beziehung zwischen einem Subjekt, einem Objekt und einer Handlung ist, und diese Beziehung ausdrückt, zu welchem Ende Subjekt, Objekt und Handlung zusammenwirken, so lässt sich als schlüssiges Zweckkonzept aus den Gesetzesmaterialien ableiten: Maßgebliches Subjekt sollen wohl die *historischen Hersteller* des Computerprogramms sein. Entscheidend ist, welches Ziel diese mit dem Entwerfen und Herstellen des Computerprogramms ursprünglich verfolgt haben. Dies ist anhand des Aufbaus oder Designs und insbesondere der Funktionen des Computerprogramms objektiviert zu ermitteln. Auf die Absichten eines *Verwenders* kommt es dagegen nicht an. Ist die kriminelle Intention der Programmhersteller in einer Gesamtbetrachtung festgestellt worden, so *hat* das Computerprogramm quasi als Eigenschaft einen kriminellen Zweck. Es wird also in der Folge stets vom objektiven Tatbestand erfasst.

Freilich finden sich in der Gesetzesbegründung auch Aussagen, die sich diesem Ergebnis entgegenhalten ließen. Insgesamt liegt daher die Vermutung nahe, dass der Gesetzgeber das semantische Problem seiner Regelungstechnik gar nicht erkannt hat,

---

[49] Dass daneben die Konstruktion „zu begehen" grammatisch falsch ist, weil nicht das Computerprogramm eine Straftat begehen kann, sondern nur sein Verwender, soll hier nicht weiter interessieren. Gemeint ist hier offensichtlich, dass Computerprogramme darauf ausgelegt oder dafür hergestellt sein müssen, *dass damit* Straftaten (von irgendjemandem) begangen werden.

sondern sich vielmehr „aus dem Bauch heraus“ dazu eingelassen hat, was als „Zweck“ infrage kommt. Der Sinn dieser Regelungstechnik erschließt sich deshalb nicht unmittelbar.

Von der strukturellen Frage, auf welches Subjekt und welche Handlung es überhaupt ankommt, ist die normative Frage zu unterscheiden, *ab wann* davon gesprochen werden kann, dass das festgelegte Subjekt mit der festgelegten Handlung einen *kriminellen* Zweck verfolgt. Hier geht es also nicht um die Ermittlung des Zwecks, sondern um seine *Bewertung* als kriminell. Insbesondere in den Fallvarianten, in denen ein potentieller Vorfeldtäter ein Computerprogramm aus dem eigenen Machtbereich entlässt,[50] wird für ihn diese Frage erheblich, denn in diesem Moment muss er wissen, ob sein Computerprogramm tatbestandsmäßig ist.

Zu dieser Frage hält die Gesetzesbegründung nur Andeutungen bereit: der Zweck des Computerprogramms müsse eindeutig,[51] aber nicht ausschließlich[52] auf die Begehung von Straftaten gerichtet sein.[53] Zudem wird der Begriff des „*funktionalen* Zwecks“ eingeführt.[54] Allerdings ist eine (objektive) Funktion zunächst etwas anderes als ein Zweck. Wenn der Gesetzgeber dennoch vom „funktionalen Zweck“ spricht, will er damit wohl sagen, dass für die Beurteilung des Programmzwecks die Funktionen des Computerprogramms eine Rolle spielen. So ist es auch kein Widerspruch, dass der funktionale Zweck *eindeutig* aber *nicht ausschließlich* deliktisch sein soll: Es genügt demnach, wenn das Computerprogramm *eine* Funktion beinhaltet, deren Zweck *eindeutig* in der Begehung von Straftaten liegt.

Damit ist das Schema zur Bewertung des Programmzwecks geklärt: Ein Computerprogramm „hat einen kriminellen Zweck“, wenn es zumindest *eine* Funktion beinhaltet, mit der *die historischen Hersteller* (= maßgebliches Subjekt) eindeutig die *Begehung von Straftaten* bezweckt haben.

Es bleibt freilich die normative Frage offen: Wann bezweckt ein Hersteller die Begehung von Straftaten? Muss er die Begehung von Straftaten nur vorhersehen? Muss er sie wünschen oder gar beabsichtigen? Genügt es, wenn er sie in Kauf nimmt? Gibt es ein erträgliches Maß an Straftaten, das der Hersteller noch vorhersehen und in Kauf nehmen darf, ohne dass man ihm unterstellen kann, er würde gerade diese Straftaten bezwecken? Dies wird in den Gesetzesmaterialien offengelassen und damit der Wissenschaft und Rechtsprechung anheimgestellt.

---

[50] Also Varianten verkaufen, verbreiten, einem anderen verschaffen oder überlassen und sonst zugänglich machen.

[51] BT-Drucks. 16/3656, S. 19 linke Spalte: Nicht erfasst werden Programme, deren Zweck „nicht eindeutig ein krimineller ist“.

[52] BT-Drucks. 16/3656, S. 12 linke Spalte, Ziffer 3 a.E.: „*auch* die Begehung […]“.

[53] Ebenso LG Karlsruhe NStZ-RR 2007, 19; *Cornelius*, CR 2007, 687; vgl. auch *Schuster*, DuD 2009, 743 f.

[54] BT-Drucks. 16/3656, S. 19 linke Spalte.

cc) Die Literatur

In der Literatur werden die Ausführungen des Gesetzgebers aufgegriffen und teilweise abgewandelt. Im Folgenden soll ein Überblick über die vertretenen Meinungen gegeben werden. Soweit die Autoren dem obigen Zweischritt folgen, wird dies hier wiedergegeben: Es wird zunächst erläutert, welches Subjekt, welches Objekt und welche Handlung in Beziehung gesetzt werden oder mit anderen Worten: wer durch welche Handlung den Zweck des Computerprogramms setzt. Sodann werden die normativen Anforderungen geschildert, die gestellt werden, um einen Zweck als kriminell zu werten und damit das Computerprogramm als tatbestandsmäßig zu beurteilen. So wird sichtbar, dass manch Widerspruch in Gesetzesmaterialien und Literaturmeinungen auf eine unterschiedliche Zweckkonstruktion zurückzuführen ist. Solch unterschiedliche Zweckkonstruktionen führen ebenso zu einem unterschiedlichen Verständnis des Begriffs „Dual-Use", sodass in Argumentationssträngen mit Verweis auf die Dual-Use-Problematik besondere Vorsicht walten muss.

Ein Teil der Literatur hält es von vornherein für unmöglich, den Zweck eines Computerprogramms zu ermitteln.[55] Dies wird vor allem mit dem *Mehr*zweckaspekt des Dual-Use-Phänomens begründet: Auch autorisierte Sicherheitstests sind nur mit solchen Programmen möglich, die auch zu unautorisierten Angriffen verwendet werden können. Konsequenterweise müsste man demnach den Tatbestand für obsolet halten oder ein engeres Auslegungskriterium als den Zweck entwickeln.

Einige dieser Autoren wenden dagegen eine weitere Auslegung an und halten die bloße deliktische Eignung oder Funktion für ausreichend.[56] Vor allem in den frühen Veröffentlichungen zu § 202c Abs. 1 Nr. 2 StGB wird diese Eignungs-Auslegung häufig aus der Not vertreten, weil man befürchtete, dass der Tatbestand sonst leerliefe.[57] Dies kann jedoch nicht überzeugen: Die kriminelle Eignung stellt offensichtlich eine niedrigere Anforderung dar als der kriminelle Zweck.[58] Man

---

[55] So *Ernst*, DS 2007, 338; *ders.*, NJW 2007, 2663; *Hassemer/Ingeberg*, ITRB 2009, 85 f.; im Ergebnis auch *Gröseling/Höfinger*, MMR 2007, 629, die (nur) deshalb auf die ausschließlich deliktische Verwendbarkeit abstellen, damit aber den Wortlaut des Tatbestands überdehnen.

[56] SK-*Hoyer*, § 202c Rn. 6 – interessanterweise kommentiert derselbe Autor im selben Werk zur selben Regelungstechnik bei § 263a, dass das Computerprogramm konkret so gestaltet sein müsse, dass die einzig plausible Erklärung sei, dass das Programm unmittelbar zur Begehung der Zieltat verwendet werden solle, siehe SK-*Hoyer*, § 263a Rn. 59; ähnlich *Popp*, JuS 2011, 392.

[57] *Ernst*, DS 2007, 338; *ders.*, NJW 2007, 2663; *Böhlke/Yilmaz*, CR 2008, 262; *Gercke,* in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 194; *Gröseling/Höfinger*, MMR 2007, 629; *Höfinger*, ZUM 2009, 752; *Husemann*, NJW 2004, 108; *Marberth-Kubicki*, Computer- und Internetstrafrecht, Rn. 123; *Popp*, MR-Int 2007, 86; vgl. auch *Cornelius*, CR 2007, 687; *Holzner*, ZRP 2009, 178.

[58] Vgl. BVerfG NJW 2006, 2319; *Hassemer/Ingeberg*, ITRB 2009, 86; *Popp*, MR-Int 2007, 87. Vgl. auch im Zusammenhang mit dem unten erörterten Tatbestandsmodell,

würde mit einer solchen Auslegung also über den Wortlaut des Tatbestands hinausgehen und damit gegen den Grundsatz *nulla poena sine lege* gemäß Art. 103 Abs. 2 GG verstoßen.[59]

Diesen Bedenken wird auch nicht abgeholfen, wenn man fordert, dass das Computerprogramm zur Begehung von Straftaten „spezifisch geeignet" ist,[60] was bei „Ausspähungs- und Crackingprogrammen" oder „Entschlüsselungsprogrammen mit speziellen Funktionen" zu bejahen sei.[61] Dies ist nämlich ein Zirkelschluss: Es stellt sich ja gerade die normative Frage, wann ein Entschlüsselungsprogramm als Crackingprogramm zu bezeichnen ist. Man dreht sich im Kreis, wenn man feststellt, dass ein Entschlüsselungsprogramm als tatbestandsmäßiges Crackingprogramm anzusehen ist, wenn es die spezifische Eignung eines Crackingprogramms hat. Hier ist ja gerade nach den Kriterien gefragt, nach denen ein Entschlüsselungsprogramm als Crackingprogramm zu bewerten ist: Wann liegt der Zweck des Computerprogramms im Cracken und nicht im Entschlüsseln?

Der Zweck des Computerprogramms wird in der Literatur teilweise *rein objektiv* auf Grundlage der Funktionen oder objektiven Gestaltung des Computerprogramms beurteilt. Zwecksetzende Subjekte werden dabei nicht festgelegt, sondern es wird das Computerprogramm isoliert betrachtet.[62] Damit kann jedermann den Zweck des Computerprogramms bestimmen. Auch eine mit dem Zweck verknüpfte Handlung wird hier nicht abstrakt festgelegt. Der Zweck des Computerprogramms soll nur anhand der Funktionen oder der Gestaltung ermittelt werden.

Ein weiterer Teil der Literatur konturiert dies stärker, indem eine „objektive Zweckbestimmung" vorgenommen wird, bei der das zwecksetzende Subjekt festgelegt wird: Es sei von äußeren Merkmalen des Computerprogramms darauf zu schließen, ob *sein Schöpfer* oder *Inhaber* deliktische Ziele verfolgt.[63] Ähnlich ist die Forderung, dass das Computerprogramm gerade im Hinblick auf eine spezielle

---

3.a)aa): OLG Hamburg GRUR-RR 2010, 156 (bloße Möglichkeit reicht nicht aus, um eine entsprechende „objektive Zweckbestimmung" anzunehmen).

[59] BeckOK-*von Heintschel-Heinegg*, § 202c Rn. 7.1 f.; *Fischer*, § 263a Rn. 31, § 202c Rn. 5; Schönke/Schröder-*Cramer/Perron*, § 263a Rn. 33; Schönke/Schröder-*Eisele*, § 202c Rn. 4; ebenso Lackner/*Kühl*, § 202c Rn. 3, widersprüchlich dagegen noch in § 263a Rn. 26b.

[60] MüKo-*Wohlers*, § 263a Rn. 68.

[61] So etwa MüKo-*Wohlers*, § 263a Rn. 68.

[62] *Böhlke/Yilmaz*, CR 2008, 262, unter expliziter Ablehnung eines Modells, das auf Entwickler oder Nutzer des Computerprogramms abstellt; *Gercke,* in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 122; *Hassemer/Ingeberg*, ITRB 2009, 86; NK-*Kindhäuser*, § 263a Rn. 43; SK-*Hoyer*, § 263a Rn. 59; ebenso *Popp*, GA 2008, 381, der hierfür den Begriff „objektivierter Zweck" schöpft, diesen aber unter dem Schlagwort „Bestimmung eines Gegenstandes" ausführt.

[63] *Borges/Stuckenberg/Wegener*, DuD 2007, 276; *Cornelius*, CR 2007, 687; Schönke/Schröder-*Cramer/Perron*, § 263a Rn. 33; *Schumann*, NStZ 2007, 678.

Tatmodalität einer Zieltat geschrieben worden sein muss.[64] Mit dieser Auslegung kann eine Reihe von Aspekten berücksichtigt werden, die darauf schließen lassen, dass die historischen Entwickler, die Intermediäre oder Endabnehmer des Computerprogramms deliktische Ziele verfolgt hatten, ohne dass es in dieser Auslegung auf die subjektiven Ziele einer Einzelperson tatsächlich ankäme – es geht ja um eine objektive Bestimmung des Programmzwecks anhand des Programmäußeren.

Ein weiterer Teil der Literatur vertritt eine noch stärkere Subjektivierung: Es solle nicht objektiviert ein Zweck ermittelt werden, sondern maßgeblich sei eine *spezifische Widmung* des *Schöpfers*, *Inhabers* oder *Verwenders* des Computerprogramms.[65] Der maßgebliche Zeitpunkt muss dabei wohl die Vornahme der Vorfeldhandlung sein. Demnach hat das Computerprogramm einen deliktischen Zweck, wenn sein Schöpfer, Inhaber oder Verwender mit der Vornahme der Tathandlung deliktische Ziele verfolgt. Zu ähnlichen Ergebnissen kommt man wahrscheinlich, wenn man im Zweifel auf die „Gesinnung des Urhebers“[66] abstellt.

Hat man mit den soeben dargestellten Konzepten ermittelt, wer welchen Zweck gesetzt hat, stellt sich die Frage nach dem Maßstab: Führen die ermittelten Zwecke dazu, dass das Computerprogramm insgesamt einen deliktischen Zweck hat?

Auch hierzu werden – meist ohne argumentative Auseinandersetzung – Vorschläge unterschiedlicher Intensität unterbreitet: So soll der deliktische Zweck zu bejahen sein, wenn die Begehung von Straftaten die *einzig* plausible Erklärung ist,[67] dass also mit anderen Worten der Zwecksetzer offensichtlich nicht auch einen rechtmäßigen Zweck verfolgt. Anderen wiederum genügt es, wenn der Zwecksetzer *primär* oder sogar nur *wesentlich* bezweckt, dass Zieltaten begangen werden.[68] Noch geringer ist die Schwelle wohl, wenn der Zwecksetzer bezweckt, dass das Computerprogramm *regelmäßig* zu Straftaten eingesetzt wird.[69] Am geringsten ist die Forderung, der Zwecksetzer müsse lediglich bezweckt haben, dass das Computerprogramm *überhaupt* zur Begehung von Straftaten eingesetzt wird.[70]

Neben diesen subjektiven Kriterien gibt es auch eher objektive Maßstäbe: Der deliktische Programmzweck liege vor, wenn die Vertriebspolitik oder das Marke-

---

[64] *Fischer*, § 263a Rn. 32.

[65] So *F. Albrecht*, SVR 2005, 286; *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, Rn. 158; NK-*Kargl*, § 202c Rn. 7; *Schreibauer/Hessel*, K&R 2007, 619; siehe auch BeckOK-*von Heintschel-Heinegg*, § 263a Rn. 48, der auf den „Willen des Täters“ abstellt.

[66] *Schultz*, DuD 2006, 782, wobei mit dem Urheber offenbar der Vorfeldtäter gemeint ist.

[67] SK-*Hoyer*, § 263a Rn. 59, ähnlich *Schreibauer/Hessel*, K&R 2007, 619.

[68] *Schumann*, NStZ 2007, 678.

[69] *Hassemer/Ingeberg*, ITRB 2009, 86.

[70] NK-*Kindhäuser*, § 263a Rn. 43.

ting des Programmherstellers oder sein Leumund dafür sprechen,[71] oder wenn ein sachkundiger Empfängerkreis dies feststellt.[72]

Unglücklich ist dagegen der Vorschlag, einen deliktischen Prorammzweck zu bejahen, wenn der Zwecksetzer „hauptsächlich nur" die Begehung von Straftaten verfolge.[73] „Hauptsächlich" und „nur" schließen einander schon sprachlich aus.

Zusammenfassend lässt sich also festhalten, dass die Meinungen in der Literatur in zwei Fragen weit auseinander gehen. Dies betrifft zum einen die Frage nach dem Zwecksetzer: Vertreter des einen Extrems lassen hier völlig offen, wer die Zwecke setzt und ordnen einem Computerprogramm allein anhand seines objektiven Erscheinungsbilds einen „deliktischen Zweck" zu. Im anderen Extrem betrachtet man die subjektiven Intentionen von Einzelpersonen aus der Gruppe der historischen Hersteller, Intermediäre oder Endverwender des Computerprogramms. Dazwischen gibt es subjektiv-objektiv gemischte Auslegungskonstrukte. Ein beträchtlicher Teil der Literatur lehnt das Zweckmodell insgesamt als impraktikabel ab. Die zweite Frage, in der große Meinungsvielfalt herrscht, betrifft die Schwelle, ab der ein Computerprogramm aufgrund eines deliktischen Zwecks als tatbestandsmäßig beurteilt wird: Während Vertreter des einen Extrems für ausreichend halten, dass überhaupt ein deliktischer Zweck des Computerprogramms vorliegt, wird im anderen Extrem gefordert, dass dieser deliktische Zweck der einzige verfolgte Zweck ist.

dd) Das Bundesverfassungsgericht

Das Bundesverfassungsgericht wurde aufgrund von Verfassungsbeschwerden sowohl mit § 202c Abs. 1 Nr. 2 StGB als auch mit § 22b Abs. 1 Nr. 3 StVG befasst, fasste wegen fehlender unmittelbarer Betroffenheit jeweils Nichtannahmebeschlüsse und griff dabei die vom Gesetzgeber vorgezeichnete Auslegung auf. Dieser zufolge drücke das Tatbestandsmerkmal „Zweck" eine finale Dimension aus und erfordere mehr als die bloße Eignung oder auch spezifische Eignung des Computerprogramms zum Einsatz bei Zieltaten.[74] Dies folge nicht nur aus dem Wortlaut, sondern auch aus einem systematischen Abgleich mit den Tatbeständen im „Eignungsmodell"[75] sowie aus der Entstehungsgeschichte des § 202c Abs. 1 Nr. 2 StGB.[76]

---

71 *Cornelius*, CR 2007, 687.

72 *Popp*, GA 2008, 381, der allerdings nicht angibt, nach welchen Maßstäben der sachkundige Empfängerkreis eigentlich urteilt.

73 Ebd.

74 BVerfG, 2 BvR 1589/05, Rz. 8; BVerfG, 2 BvR 2233/07, Rz. 61.

75 BVerfG, 2 BvR 1589/05, Rz. 8; BVerfG, 2 BvR 2233/07, Rz. 62; zur *spezifischen* Eignung/Verwendbarkeit vgl. oben, I.B.1.

76 BVerfG, 2 BvR 2233/07, Rz. 63.

Für diese finale Dimension seien die Absichten des Entwicklers ausschlaggebend.[77] Dies folge daraus, dass der Rechtsausschuss in seiner Beschlussempfehlung darauf hinweise, dass § 202c StGB „hinsichtlich der Zweckbestimmung" im Sinne des Art. 6 Abs. 1 lit. a Nr. i des Übereinkommens über Computerkriminalität auszulegen sei.[78] Interessant ist dabei jedoch, dass auch die Kammer nicht die deutsche Übersetzung des Übereinkommens über Computerkriminalität hinterfragt und damit – wie der Rechtsausschuss – die „Primarily"-Übersetzung „in erster Linie" auf das Auslegen und *Herstellen* des Computerprogramms bezieht, nicht auf die *Verwendung* zur Begehung von Straftaten.[79] Unter Heranziehung der Gesetzgebungsmaterialien, des Erläuternden Berichts zum Übereinkommen über Computerkriminalität sowie einzelnen Literaturmeinungen gewinnt die Kammer in einer historischen, teleologischen, pragmatischen und völkerrechtskonformen Auslegung das zusätzliche Erfordernis, dass die (kriminelle) Absicht des Programmentwicklers *äußerlich feststellbar manifestiert* ist. Diese äußerlich feststellbare Manifestation könne etwa in der Gestaltung des Programms, der Vertriebspolitik oder Werbung des Herstellers liegen, wobei diese Feststellung im Einzelnen Sache der Fachgerichte sei.[80]

Da es in diesem Kapitel darum geht, die deutsche Rechtstechnik als solche zu analysieren, wird hier keine völkerrechtskonforme Auslegung der deutschen Zweck-Tatbestände vorgenommen. Dennoch soll auf einen augenfälligen Unterschied zu den internationalen Vorläufern der deutschen Zweck-Tatbestände vorgegriffen werden:[81] Die völkerrechtlichen und europarechtlichen Akte sprechen nicht vom „Zweck des Programms", sondern vom Zweck seiner Verwendung. Damit liegt ihnen eine andere Rechtstechnik zugrunde, welche im deutschen Recht auch in anderen Software-Delikten zur Anwendung kam.[82]

ee) Zusammenfassung

Zusammenfassend ist festzuhalten, dass die grammatische Auslegung dieses Tatbestandsmodells in einem Zweischritt erfolgen muss. Da der Zweck immer eine Beziehung zwischen einem Subjekt, einem Objekt und einer Handlung ausdrückt, muss dieser im vorliegenden Modell zunächst *ermittelt* werden. Hierzu muss man festlegen, auf welches Subjekt und welche Handlung es in vorliegenden Tatbeständen ankommen soll, also *wer* durch *welche Handlung* den maßgeblichen Zweck

---

77 BVerfG, 2 BvR 2233/07, Rz. 65.

78 Ebd. mit wörtlichem Zitat aus BT-Drucks. 16/5449, S. 4 rechte Spalte.

79 BVerfG, 2 BvR 2233/07, Rz. 65.

80 BVerfG, 2 BvR 2233/07, Rz. 66.

81 Einzelheiten hierzu siehe unten II.

82 Siehe unten 5.

setzt. Im zweiten Schritt muss man dann normativ bewerten, ob diese Beziehung als kriminell einzustufen ist, ob also der ermittelte Zweck in der Begehung von Straftaten liegt.

Die Gesetzesmaterialien legen – trotz einer wirren Terminologie – im Ergebnis nahe, dass es strukturell auf den historischen Hersteller als zwecksetzendes Subjekt und sein Herstellen als Handlung maßgeblich ankommt. Das Bundesverfassungsgericht entnimmt den Gesetzesmaterialien dieselbe Festlegung und führt ergänzend aus, dass nur dann von einem *kriminellen* Zweck zu sprechen ist, wenn äußerlich feststellbar manifestiert ist, dass der Hersteller kriminelle Absichten verfolgt hat. Dabei sei etwa auf die Gestaltung des Computerprogramms selbst, seine Bewerbung oder die Vertriebswege abzustellen.

In der Literatur werden im ersten Schritt der Zweckermittlung unterschiedliche Schwerpunkte gesetzt: Nach einer rein objektiven Ansicht wird von jeglichem Subjekt abstrahiert und allein anhand der objektiven Funktionen des Computerprogramms ermittelt, „welche Ziele das Computerprogramm verfolgt“. Eine subjektive Ansicht fragt nach der Widmung, die der einzelne Hersteller oder Verwender dem Computerprogramm gibt. Dazwischen lässt sich die Ansicht verorten, die – ähnlich wie das Bundesverfassungsgericht – zwar nach den subjektiven Zielen des Herstellers fragt, diese aber objektiviert aus dem Erscheinungsbild des Computerprogramms ermittelt. Schließlich gibt es auch Autoren, die es ablehnen, nach dem „Zweck des Computerprogramms“ zu fragen, stattdessen auf seine Eignung abstellen und sich damit über den engeren Wortlaut des Tatbestands hinwegsetzen.

Zur *Bewertung* des ermittelten Zwecks wird in der Literatur häufig der Horizont eines objektiven Empfängerkreises herangezogen. Danach sei zu entscheiden, ob der Zweck des Computerprogramms einzig, primär, wesentlich, regelmäßig oder überhaupt in der Begehung von Straftaten liege, was dann – nach Auffassung des jeweiligen Autors – für die Tatbestandsmäßigkeit des Computerprogramms ausreicht.

Festzuhalten ist jedoch, dass viele Literaturmeinungen vor den Verfassungsbeschwerdeverfahren gegen § 202c Abs. 1 Nr. 2 StGB veröffentlicht wurden. Es ist daher noch nicht abzusehen, ob sie aufrechterhalten werden.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Im folgenden Kapitel wird untersucht, wie sich dieses „Zweckmodell“ auf das Dual-Use-Phänomen auswirkt. Bei gefährlicher Software zeigt sich das Dual-Use-Phänomen in zweierlei Hinsicht: einem Multifunktionsaspekt und einem Mehrzweckaspekt. Der Multifunktionsaspekt besagt, dass ein Computerprogramm mehrere Funktionen haben kann, von denen nicht jede schädlich ist. Der Mehrzweck-

aspekt besagt, dass auch eine schädliche Funktion für legitime Zwecke nützlich und erforderlich sein kann (Test- und Analysezwecke).[83]

Relativ unproblematisch ist in diesem „Zweckmodell" der Multifunktionsaspekt der Dual-Use-Problematik, nämlich dass ein Programm mehrere Funktionen haben kann, von denen manche legitim, andere jedoch auf einen deliktischen Einsatz ausgelegt sind. Im vorliegenden Regelungsmodell wird es als normative Frage betrachtet, ob solche Computerprogramme tatbestandsmäßig sind, und diese normative Frage wird den Fachgerichten überlassen. Dies mag zwar anfangs einige Rechtsunsicherheit schaffen, liegt aber in der Natur strafrechtlicher Gesetzgebung, da der Gesetzgeber nicht im Detail alle normativen Einzelentscheidungen vorwegnehmen kann.

Größere Schwierigkeiten bereitet dagegen der Mehrzweckaspekt der Dual-Use-Problematik, nämlich dass für IT-Sicherheitsexperten ein Zugriff selbst auf höchstschädliche Computerprogramme zu Test-, Analyse- und Demonstrationszwecken zwingend erforderlich ist. Insbesondere § 202c Abs. 1 Nr. 2 StGB verbreitete wegen dieses Mehrzweckaspekts von Anfang an große Unsicherheit, weil der Gesetzgeber hier versucht hat, den Mehrzweckaspekt beim Tatobjekt zu berücksichtigen, obwohl er eigentlich untrennbar mit der Tathandlung verknüpft ist.

Hintergrund ist, dass in den Zieldelikten häufig ein Verhalten beschrieben ist, welches äußerlich unauffällig ist und allein dadurch zu strafrechtlich vorwerfbarem Verhaltensunrecht wird, dass ein oder mehrere normative Merkmale mitverwirklicht sind: Die §§ 202a Abs. 1, 202b Abs. 1 StGB setzen etwa voraus, dass Daten betroffen sind, welche *nicht für den Täter bestimmt* sind. § 202a Abs. 1 StGB erfordert daneben, dass der Täter *unbefugt* handelt. § 22b Abs. 1 Nr. 1 StVG setzt voraus, dass bestimmte Messdaten *verfälscht* werden. In § 303a StGB wurde das erforderliche normative Merkmal gar nicht festgeschrieben, sodass der Tatbestand an sich überhaupt kein vertyptes Unrecht beschreibt. Jedoch setzt eine Bestrafung aus § 303a StGB nach einhelliger Auffassung voraus, dass der Täter in die Integrität von Daten eingreift, an denen er *keine Verfügungsbefugnis* hat.[84] Bei § 263a Abs. 1 StGB muss das Ergebnis eines Datenverarbeitungsvorgangs beeinflusst und dadurch das Vermögen eines anderen geschädigt werden, und diese Beeinflussung muss wiederum durch Verwendung *unrichtiger* oder *unvollständiger* Daten, durch *unbefugte* Verwendung von Daten oder durch eine sonstige *unbefugte* Einwirkung auf den Ablauf geschehen.

---

[83] Vgl. oben Teil 1, I.B.2.

[84] Dieses Erfordernis wird stellenweise in das Tatbestandsmerkmal Daten mit hineingelesen, siehe nur *Fischer*, § 303a Rn. 14; Schönke/Schröder-*Stree/Hecker*, § 303a Rn. 3; vielerorts wird dagegen „rechtswidrig" als eigenes Tatbestandsmerkmal in diesem Sinne ausgelegt, vgl. Lackner/*Kühl*, § 303a Rn. 4. Zum Streit um die richtige Verortung der Tatbestandseinschränkung siehe Übersicht bei *Fischer*, § 303a Rn. 14.

Denkt man in diesen Delikten die kursiv geschriebenen normativen Merkmale hinweg, so beschreiben die Tatbestände kein vertyptes Unrecht mehr. Das Auslesen, Eingeben, Verändern, Löschen und Verwenden von Daten sowie jedes sonstige Einwirken auf Datenverarbeitungsvorgänge ist rechtlich neutral und für jeden IT-Nutzer völlig alltäglich. Erst wenn dies unbefugt, unrichtig, verfälschend oder bestimmungswidrig erfolgt, erhält das Geschehen seinen typischen Unrechtscharakter.

Dies aber sind normative Merkmale, welche einem Computerprogramm nicht immanent sein können. Ein Computerprogramm kann immer nur Funktionen ausführen, kann Daten eingeben, verändern, löschen, auslesen und so fort. Ob der Programmverwender im Einzelfall die Befugnis hat, solche Funktionen auszuführen, kann man dem Computerprogramm nicht ansehen. Deshalb müssen selbst Rootkits und vergleichbare Software immer als Dual-Use-Programme gelten, sogar wenn sie ausschließlich Schadensroutinen ausführen können. Denn auch für sie ist charakteristisch, dass sie immer auch mit dem Willen des jeweils Berechtigten eingesetzt werden können und zu Testzwecken verwendet werden müssen.

Dieses Argument wird auch bei Kriegsgütern, Waffen oder chemisch-biologischen Kampfstoffen vorgetragen,[85] jedoch hat es in der Informationstechnik besonderes Gewicht: IT-Systeme können mit vergleichsweise geringem Aufwand und vernachlässigbaren Kosten gespiegelt, also reproduziert werden, sodass man Angriffe auf ein gespiegeltes System oder in einer *Sandbox* unter Echtzeitbedingungen ablaufen lassen kann, ohne dadurch einen Schaden an dem zu schützenden (Original-)System anzurichten. „Angriffstools“ oder Computerprogramme mit Schadensroutinen werden also in der IT sehr viel häufiger und intensiver zu rechtmäßigen, legitimen Zwecken eingesetzt als dies bei vergleichbaren Gegenständen aus der körperlichen Welt der Fall ist. Da also das Dual-Use-Phänomen in den Vorfelddelikten des IT-Strafrechts nicht von den objektiven Funktionen des Tatobjekts abhängt, sondern vom Vorliegen normativer Merkmale bei Begehung eines hinzugedachten Zieldelikts, wie etwa einem entgegenstehenden Willen oder einer fehlenden Verfügungsbefugnis, kann die Dual-Use-Problematik auch nicht durch eine konkretisierende Beschreibung der Computerprogramme im Tatbestand bewältigt werden. Eine Rechtstechnik, die diesen Weg wählt, führt zwangsläufig zu inkonsistenten Ergebnissen.

In dieser Hinsicht halfen auch die Beschlüsse des Bundesverfassungsgerichts nicht weiter. Diese haben lediglich in der Auslegung einzelner Tatbestandsmerkmale Rechtssicherheit geschaffen, das Dual-Use-Problem aber liegt in der Konzeption des Tatbestands: De lege lata definiert nämlich der Hersteller eines Computerprogramms beim Schaffen des Computerprogramms dessen möglicherweise kriminellen Zweck. Spätere Intermediäre oder Verwender können in dieser Hin-

---

[85] Dazu näher unten Teil 4, I.

sicht nichts mehr ändern.[86] Damit hat der historische Hersteller faktisch die Bestimmungshoheit über die Tatbestandsmäßigkeit eines Computerprogramms, und wenn es einmal zu einem kriminellen Zweck geschrieben worden ist, bleibt es stets objektiv tatbestandsmäßig, unabhängig davon, durch wessen Hände es im Anschluss läuft.

Dadurch entstehen zwei Gruppen von Computerprogrammen: solche, die zu kriminellen Zwecken hergestellt wurden und solche, die zu legalen (evtl. Test-) Zwecken hergestellt wurden. Dabei können die technischen Funktionen der einen und der anderen Programmgruppe sogar identisch sein. Jedoch werden die Computerprogramme, die *ursprünglich* mit kriminellen Intentionen geschaffen worden sind, zu einer Art „bemakelter Software". Der kriminelle Zweck haftet ihnen über ihre ganze Lebensdauer hinweg wie ein Makel an. Da ein späterer Besitzer diesen Makel auch nicht mehr beheben kann, ist der Umgang mit solcher Software nur noch dann straflos möglich, wenn der subjektive Tatbestand einen Ausweg aus der Strafbarkeit bietet.[87]

Im gleichen Zug entsteht eine Gruppe „makelloser Software", mit der jeder Umgang per se straflos ist, selbst wenn der „Täter" (eigentlich: Nichttäter) dabei die Begehung von Straftaten beabsichtigt: Es fehlt am tauglichen Tatobjekt.[88] Fälle dieser Art sind keineswegs fernliegend, da etwa ein Rootkit von zwei unterschiedlichen Herstellern, aber mit denselben Funktionen einmal als Angriffstool (bemakelt) und einmal als eine *Penetration-Testing*-Software (makellos) eingestuft werden kann. Dies führt zu dem bizarren Ergebnis, dass IT-Sicherheitsexperten untereinander „bemakelte Software" nicht mehr verbreiten können, wenn sie nicht ausschließen können, hiermit auch Straftaten vorzubereiten. Deshalb sind sie darauf angewiesen, sich etwa Angriffstools selbst zu beschaffen, in der Regel aus zwielichtigen Quellen im Internet. Damit erfreut sich die *Underground Economy* eines breiten Stamms eigentlich rechtstreuer Kunden und wird durch die Vorfeldtatbestände, mittels derer der Gesetzgeber den Handel mit Schadsoftware eigentlich bekämpfen wollte, sogar gestärkt. Gleichzeitig kann beispielsweise *Penetration-Testing*-Software uneingeschränkt verbreitet werden, auch wenn jedermann weiß, dass diese Software sich auch ohne Weiteres zu kriminellen Zwecken einsetzen

---

[86] Dies übersieht *Seeger*, DuD 2010, 477 f.

[87] In den Tatbeständen des „Zweckmodells" soll dies dadurch erreicht werden, dass der Vorfeldtäter subjektiv ein Zieldelikt *vorbereiten* muss. Dies wird aber häufig nicht zur Straflosigkeit führen, wenn Computerprogramme öffentlich zugänglich gemacht, also etwa zum Download angeboten oder an einen nicht überschaubaren Personenkreis weitergegeben werden, so auch explizit das BVerfG 2 BvR 2233/07 Rz. 77. Zum Merkmal des *Vorbereitens* im Detail siehe unten C.1.

[88] Dies gilt jedenfalls, solange die vorbereiteten Straftaten in der Vorstellung des „Vorfeldtäters" so vage bleiben, dass eine Beihilfestrafbarkeit noch nicht infrage kommt.

lässt. Einem Kriminellen müsste man daher raten, auf *Penetration-Testing*-Software zurückzugreifen, da er somit die Vorbereitungsstrafbarkeit umschifft.

Im vorliegenden Regelungsmodell besteht also unter dem Mehrzweckaspekt weiterhin ein Dual-Use-Problem. Insofern ist die in der Literatur gegebene „(vorsichtige) Entwarnung“[89] etwas voreilig, und der Feststellung, dass die befürchtete „Kriminalisierung von IT-Sicherheitsunternehmen […] nicht eingetreten“ sei, ist in dieser Pauschalität nicht zuzustimmen.

3. „Dazu bestimmt oder entsprechend angepasst, [die Zieltat] zu ermöglichen“

In einem dritten Modell stellt der Gesetzgeber das Herstellen, Einführen oder Verbreiten von „Vorrichtungen“ unter Strafe, „die dazu bestimmt oder entsprechend angepasst sind“ die Zieltat zu ermöglichen. Angewandt wurde dieses Modell in § 4 ZKDSG i.V.m. §§ 3 Nr. 1, 2 Nr. 3 ZKDSG. § 4 ZKDSG lautet:

> **§ 4 Strafvorschriften**
>
> Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen § 3 Nr. 1 eine **Umgehungsvorrichtung herstellt, einführt oder verbreitet**.

In § 3 Nr. 1 ZKDSG heißt es:

> **§ 3 Verbot von gewerbsmäßigen Eingriffen zur Umgehung von Zugangskontrolldiensten**
>
> Verboten sind
>
> 1. die Herstellung, die Einfuhr und die Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken
>
> […]

§ 2 Nr. 3 ZKDSG besagt:

> **§ 2 Begriffsbestimmungen**
>
> Im Sinne dieses Gesetzes bezeichnet der Ausdruck
>
> […]
>
> 3. „Umgehungsvorrichtungen“ technische Verfahren oder Vorrichtungen, die **dazu bestimmt oder entsprechend angepasst sind, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen**
>
> […]

Das „Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten“ soll verschlüsselte Radio- und Fernsehsendungen (insbesondere also das Pay-TV) sowie bestimmte Dienste der Informationsgesellschaft schützen, indem es bereits das Vorfeld einer unerlaubten Nutzung dieser Dienste umfassend kriminalisiert. Das Gesetz soll also entgegen seinem missverständlichen Titel primär die verschlüsselten Inhalte selbst schützen, nicht etwa die Techniken,

---

[89] Siehe Leupold/Glossner-*Cornelius*, Teil 10 Rn. 127.

mit denen die Inhalte verschlüsselt werden.[90] Hierzu pönalisiert § 4 ZKDSG den Umgang mit „Umgehungsvorrichtungen".

Da der Paragraph das pönalisierte Verhalten nicht selbst vollständig nennt, sondern den Verstoß gegen eine andere, nichtstrafrechtliche Verbotsnorm, nämlich § 3 ZKDSG, unter Strafe stellt, handelt es sich bei § 4 ZKDSG um einen Blankettstraftatbestand.[91] Auch § 3 ZKDSG beschränkt sich darauf, „Umgehungsvorrichtungen" als Verbotsgegenstand zu benennen, ohne zu erklären, was darunter zu verstehen ist. Dies folgt schließlich erst aus der Begriffsbestimmung des § 2 Nr. 3 ZKDSG. Führt man die Wortlaute der aufeinander verweisenden Paragraphen für die Ziele der vorliegenden Arbeit zu einem einzelnen Straftatbestand zusammen, so lautet dieser: Wer ein technisches Verfahren oder eine Vorrichtung, das oder die *dazu bestimmt oder entsprechend angepasst ist, die Zieltat zu ermöglichen*, zu gewerbsmäßigen Zwecken herstellt, einführt oder verbreitet, wird bestraft.[92]

Die genannten Normen erfassen „Vorrichtungen" und zielen damit insbesondere auf Computerprogramme ab.[93] Unter dieser Prämisse soll nachfolgend die Analyse des Tatobjekts erfolgen.

a) Charakteristika dieses Regelungsmodells

Im vorliegenden Modell muss die Vorrichtung entweder dazu bestimmt (aa)) oder entsprechend angepasst (bb)) sein, die Zieltat zu ermöglichen (cc)).

aa) „Dazu bestimmt"

Begrifflich steht die *Bestimmung* oder genauer das *Bestimmt-Sein* einer Vorrichtung in der Nähe des oben thematisierten Zwecks[94] und drückt aus, dass die Vorrichtung nach Maßgabe einer bestimmten Person einem kriminellen Ziel dienen soll. Da im Gesetzestext kein Bestimmungsgeber spezifiziert ist, wird in der Literatur teilweise vertreten, dass die Vorrichtung allein von ihrem Hersteller die jeweilige Bestimmung erhalten kann.[95] Begründet wird dies damit, dass in der englischen Sprachfassung der zugrunde liegenden Conditional-Access-Richtlinie[96] solche Vorrichtungen erfasst werden, die „designed or adapted" sind, den unautori-

---

[90] BT-Drucks. 14/7229, S. 7 linke Spalte; siehe auch *Bär/Hoffmann*, MMR 2002, 655.

[91] Vgl. *Sieber*, in: Hoeren/Sieber, Teil 19, AT Kapitel C I 2; E III.

[92] Zieltat ist hier die unerlaubte Nutzung eines zugangskontrollierten Dienstes.

[93] BT-Drucks. 14/7229, S. 7 rechte Spalte.

[94] Siehe oben I.B.2.

[95] *Strobel*, in: Dressel/Scheffler, ZKDSG, S. 124.

[96] Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten.

sierten Zugang zu ermöglichen.[97] Daraus ergebe sich ein temporales Gegenpaar aus „*ursprünglich* dazu entworfen“ (designed) und „*nachträglich* dazu angepasst“ (adapted), welches in der deutschen Sprachfassung nur nicht so deutlich zutage trete. Deshalb seien nur solche Computerprogramme bestimmt (*designed*), die schon zum Herstellungszeitpunkt durch den Hersteller dazu bestimmt worden sind, die Zieltat zu ermöglichen.[98]

Das Begriffspaar in § 2 Nr. 3 ZKDSG (Bestimmt-Sein, Angepasst-Sein) lässt sich jedoch auch als subjektiv-objektives Gegensatzpaar interpretieren. Dementsprechend wird das „Bestimmen“ überwiegend als zeitlich unabhängiges, subjektives Element ausgelegt.[99] Da das Gesetz dabei den Kreis der möglichen Bestimmungsgeber nicht eingrenzt, kann grundsätzlich jeder dem Computerprogramm seine deliktische Bestimmung geben, also der Hersteller, aber auch ein Intermediär (z.B. ein Zwischenhändler) oder der Endverwender. Ungeklärt ist dann allerdings, ob eine einmal vorliegende deliktische Bestimmung, die etwa vom Hersteller stammt, durch eine konträre Bestimmung eines Intermediärs wieder aufgehoben werden kann und wonach dann das Computerprogramm etwa in den Händen des Endverwenders beurteilt werden soll.

Ob jemand dem Computerprogramm die deliktische Bestimmung gegeben hat, und folglich das Computerprogramm *dazu bestimmt ist*, eine Zieltat zu ermöglichen, muss nach einhelliger Auffassung aus Sicht des Verkehrs, also des verständigen Durchschnittsnutzers, beurteilt werden.[100] Somit bleibt es bei dem Erfordernis, dass das Bestimmtsein des Computerprogramms nach außen sichtbar und damit für den verständigen Durchschnittsnutzer überhaupt erst erkennbar ist. Die Herstellerangaben sind diesbezüglich ein wichtiges Indiz, können jedoch auch durch das technische Vorverständnis des Verkehrs, durch bestehende Gepflogenheiten oder durch Hinweise von Dritten überlagert werden.[101]

Nicht ausreichend ist es dagegen, wenn ein äußerlich neutrales Computerprogramm rein subjektiv vom Hersteller oder einem Verwender dazu bestimmt wird, eine Zieltat zu ermöglichen. Dies folgt aber nicht zwingend aus dem Verbot des Gedankenstrafrechts, denn dieses verlangt nach übereinstimmender Meinung nur

---

[97] *Strobel*, in: Dressel/Scheffler, ZKDSG, S. 125.

[98] A.a.O., S. 126.

[99] Vgl. OLG Hamburg GRUR-RR 2010, 155 („innere Tatsache“).

[100] Siehe OLG Frankfurt a.M. GRUR-RR 2003, 287, OLG Hamburg GRUR-RR 2010, 156; *Arlt*, in: Hoeren/Sieber, Teil 7.7 Rn. 81; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 134; *Meschede*, Schutz digitaler Musik- und Filmwerke, S. 166.

[101] OLG Frankfurt a.M. GRUR-RR 2003, 287. Wenn das Gericht im Folgenden doch den Hersteller wieder als maßgeblich ansieht, weil es darauf ankomme, ob die deliktische Verwendung noch von dessen Willen getragen sei, so liegt dies wohl daran, dass im konkreten Fall allein der Hersteller betroffen war, weil er selbst die Vorrichtungen angeboten und vertrieben hatte, was ihm untersagt werden sollte.

irgendeine objektive Manifestation der kriminellen Intention,[102] welche vorliegend auch in der Tathandlung, also dem Herstellen, Einführen oder Verbreiten der (neutralen) Vorrichtung gesehen werden kann. Erforderlich ist das Nach-außen-Treten allein deshalb, weil die deliktische Bestimmung des Computerprogramms oder der Vorrichtung vom Verkehr, also Dritten, erkannt und als solche bewertet werden muss.

Konkret tritt eine solche Bestimmung beispielsweise dann schon nach außen, wenn der Vorfeldtäter das Computerprogramm so mit anderen Geräten kombiniert, dass das Ensemble die Zieltat ermöglicht.[103] Vertreibt ein Händler beispielsweise an einen unbestimmten Empfängerkreis ein Paket aus einem bestimmten FTA-Receiver, einem passenden Smart-Card-Rohling und einem Computerprogramm, mit dem man die Smart-Card-Rohlinge mit Empfangsschlüsseln beschreiben kann, so tritt durch das Verhalten dieses Händlers in der Gesamtschau nach außen, dass das Computerprogramm dazu bestimmt ist, den unautorisierten Empfang des verschlüsselten Fernsehsignals zu ermöglichen. In diesem Fall gibt es schlicht keine andere plausible Erklärung dafür, weshalb er die genannten Gegenstände im Paket vertreibt.

Für die Auslegung als temporaler Gegensatz (*ursprünglich* entworfen – *nachträglich* angepasst) werden schlüssige Argumente vorgetragen, und tatsächlich wurde später in Art. 6 Nr. 2 c) der Richtlinie 2001/29/EG[104] das englische *designed* in der deutschen Sprachfassung mit „entworfen" wiedergegeben – und wortgleich in den deutschen § 95a Abs. 3 Nr. 2 UrhG übernommen.[105] Dennoch ist diese Auslegung des Merkmals „bestimmt" keineswegs zwingend, insbesondere, da es dem Gesetzgeber von Anfang an freistand, den temporalen Gegensatz zu unterstreichen, etwa indem er schon im hiesigen § 2 Nr. 3 ZKDSG die Formulierung verwendet, die er später in § 95a Abs. 3 Nr. 2 UrhG gewählt hat. Überdies hätte er mit der Umsetzung der Richtlinie 2001/29/EG ins deutsche UrhG auch die Formulierung in § 2 Nr. 3 ZKDSG angleichen können, wenn er dies hätte klarstellen wollen.

Das Auslegungsergebnis ist hier davon abhängig, auf welche Auslegungsmethode man den Schwerpunkt legt: Mit einer grammatischen und historischen Auslegung kann man einen temporalen Gegensatz der Merkmale „bestimmt" und „angepasst" vertreten. Mit einer systematischen und teleologischen Auslegung gelangt man zu einem subjektiv-objektiven Gegensatz der Merkmale. Gegen die historische Auslegung spricht eine traurige Befürchtung: Möglicherweise hat der nationale

---

[102] So *Strobel*, in: Dressel/Scheffler, ZKDSG, S. 124; vgl. dagegen oben Teil 2, I.C.

[103] So auch *Arlt*, in: Hoeren/Sieber, Teil 7.7 Rn. 80.

[104] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

[105] Dazu sogleich eingehend, siehe I.B.4.

Gesetzgeber sich wenig Gedanken über die konkrete Bedeutung einzelner Tatbestandsmerkmale gemacht, weil er sich verpflichtet sah, die entsprechenden europäischen Vorgaben umzusetzen und daher schlicht die deutsche Sprachfassung der EG-Richtlinie eins zu eins in Gesetzesform gegossen hat.

Unabhängig davon, welche der beiden Auslegungsarten man wählt, gilt jedoch, dass das Bestimmt-Sein nicht zwingend bedeutet, dass das Computerprogramm auch *tatsächlich* die Zieltat ermöglicht.[106] Vielmehr kann auch ein objektiv ungeeignetes Computerprogramm dem Wortsinne nach vom Hersteller, Verwender etc. dazu bestimmt sein, die Straftat zu ermöglichen. Diese gesetzgeberische Entscheidung ist insofern nachvollziehbar, als der Vorfeldtäter häufig nicht mit letzter Sicherheit wissen wird, ob sein *Tool* tatsächlich funktionieren wird. Dessen Eignung hängt nämlich möglicherweise von Umständen ab, die der Täter gar nicht selbst in der Hand hat, wie etwa dem *Patch-Level* des Zielsystems oder der Verschlüsselungstechnik des zugangskontrollierten Dienstes.

So nutzte etwa der Pay-TV-Anbieter *Premiere*[107] bis 2008 das Verschlüsselungssystem *Nagravision*, welches ab November 2005 mit einer speziellen Smart-Card, später auch mit einem Software-Emulator umgangen werden konnte.[108] Ab August 2008 setzte *Premiere* eine neue Verschlüsselungstechnik ein, welche bis heute als nicht überwindbar gilt.[109] Obwohl also die Smart-Card und die Emulationssoftware heute faktisch nicht mehr ermöglichen, die Pay-TV-Verschlüsselung des *Premiere*-Nachfolgers *Sky Deutschland* zu umgehen, waren sie jedenfalls ursprünglich dazu entworfen, die Umgehung zu ermöglichen. Auch wenn man die subjektivierte Auslegung bevorzugt, können solche faktisch unbrauchbaren Smart-Cards und Emulationssoftware ohne Weiteres von einem Vorfeldtäter zum Ermöglichen der Zieltat bestimmt sein: Dies ist etwa der Fall, wenn der Vorfeldtäter über das Verschlüsselungsupdate seitens *Premiere* nicht im Bilde ist und die Emulationssoftware zum unautorisierten Empfang der Pay-TV-Sender einsetzen will.

In der subjektivierten Auslegung ähnelt die Konstellation dem untauglichen Versuch: Der Vorfeldtäter bestimmt ein Computerprogramm dazu, die Zieltat zu ermöglichen, das Programm taugt hierzu objektiv aber nicht. Wie beim untauglichen Versuch legt der Täter also ein Verhalten an den Tag, das auf eine Rechtsgutsverletzung ausgerichtet ist, und obwohl dies vom Täter intendiert ist, ist das Gesamtgeschehen objektiv nicht geeignet, die Rechtsgutsverletzung tatsächlich herbeizuführen.

---

[106] Vgl. auch *Entelmann*, Verbot von Vorbereitungshandlungen, S. 66; dagegen offenbar *Stadler*, JurPC Web-Dok. 126/2005 Abs. 4, 9.

[107] Heute: Sky Deutschland.

[108] Vgl. http://heise.de/-156259 [zuletzt abgerufen am 15.11.2014].

[109] Vgl. http://heise.de/-211918 [zuletzt abgerufen am 15.11.2014].

Der Unterschied zwischen dem deliktischen Bestimmen einer untauglichen Vorrichtung und dem Ausführen einer untauglichen Versuchshandlung liegt freilich in der Nähe zur Rechtsgutsverletzung: Beim untauglichen Versuch setzt der Täter unmittelbar zur Tatausführung an, § 22 StGB. Dagegen ist der Vorfeldtäter des Software-Delikts von der Ausführung des Zieldelikts unter Umständen noch weit entfernt. Möglicherweise will er das Zieldelikt gar nicht selbst ausführen, sondern bereitet eine fremde Tat vor. Der Umgang mit einer deliktisch bestimmten, aber untauglichen Vorrichtung kann jedoch regelmäßig nur in einen untauglichen Versuch der Zieltat münden.

Ein solcher untauglicher Versuch ist im Umkehrschluss aus § 23 Abs. 2 StGB grundsätzlich strafbar.[110] Die Strafbarkeit lässt sich rechtfertigen, indem man neben der Gefährdung, die zumindest ex ante besteht (dass der Versuch untauglich ist, stellt sich ja erst ex post heraus), auch auf den Gedanken eines rechtserschütternden Normbruchs durch die Vorfeldtat abstellt.[111] Konkret bedarf es jedoch in jedem Einzelfall einer gesonderten Begründung, wenn der Gesetzgeber über den tauglichen Versuch hinaus auch den untauglichen Versuch unter Strafe stellen will.[112]

Im hiesigen Regelungsmodell wird freilich die untaugliche Vorbereitung unter Strafe gestellt, sodass ein doppelt erhöhter Begründungsbedarf für ein solches Delikt entsteht: Zunächst muss der Gesetzgeber gesondert begründen, weshalb eine einfache Versuchsstrafbarkeit nicht ausreicht, sondern die Strafbarkeit weiter ins Vorfeld ausgedehnt werden muss. Sodann muss er auch begründen, weshalb es nicht ausreicht, nur taugliche Vorbereitungshandlungen unter Strafe zu stellen, sondern auch die lediglich deliktisch intendierten, aber von vornherein untauglichen Vorbereitungshandlungen strafbar sein sollen.

Im vorliegenden Falle des § 4 ZKDSG i.V.m. § 2 Nr. 3 ZKDSG hat der Gesetzgeber sich mit dem pauschalen Verweis auf die einfache Verbreitung von „Hackerwerkzeugen wie z.B. Entschlüsselungsprogrammen“ im Internet begnügt.[113] Im Ergebnis mag dieses Argument eine derart weite Vorverlagerung der Strafbarkeit tatsächlich tragen, jedoch ist bedauerlich, dass der Gesetzgeber sich nicht veranlasst sah, zu dieser brennenden Frage mehr auszuführen. Möglicherweise war aber auch die Umsetzungsverpflichtung aus der zugrunde liegenden Conditional-Access-Richtlinie für den Gesetzgeber bewusstseinsdominant, sodass er etwaige Legitimationsfragen und insbesondere die Problematik der untauglichen Vorbereitungshandlung schlicht übersehen hat.

Zusammenfassend kann das Bestimmt-Sein der Vorrichtung also auf zweierlei Arten ausgelegt werden. Entweder ist es temporal zu verstehen als das, wofür das

---

110 Vgl. zum Ganzen statt aller Schönke/Schröder-*Eser*, § 22 Rn. 60 ff.

111 Vgl. hierzu statt vieler *Roxin*, Strafrecht AT II, S. 336 ff.

112 Vgl. a.a.O., S. 340.

113 BT-Drucks. 14/7229, S. 8 linke Spalte.

Computerprogramm ursprünglich entworfen worden ist. Oder es ist – wie in der Auslegung der Gerichte und der überwiegenden Literaturmeinungen – ein zeitlich unabhängiges, subjektives Merkmal, demzufolge die Zielsetzung eines Subjekts, in der Regel des Herstellers, Händlers oder Verwenders, maßgeblich ist. Freilich muss dieses subjektive Merkmal an objektiven Umständen festgemacht werden.[114] Auf ein Vorliegen der deliktischen Bestimmung muss aus Sicht des verständigen Durchschnittsnutzers erkannt werden. Auch objektiv untaugliche Computerprogramme können deliktisch bestimmt sein. Inhaltlich würde dieses Merkmal damit dem obigen Zweckmodell in der Auslegung des Bundesverfassungsgerichts sehr nahe kommen.[115]

bb) „Entsprechend angepasst"

Neben dem Merkmal des Bestimmt-Seins enthält der vorliegende Tatbestand auch ein deskriptives Merkmal, durch das der Umgang mit bestimmten Vorrichtungen unabhängig davon unter Strafe gestellt wird, welche Ziele der Hersteller oder der Vorfeldtäter aktuell verfolgt. § 4 ZKDSG verbietet i.V.m. § 2 Nr. 3 ZKDSG nämlich auch das Herstellen, Einführen und Verbreiten von Vorrichtungen bei Strafe, die *entsprechend angepasst* sind, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen. Das „Angepasst-Sein" wird nicht nur im vorliegenden Tatbestand, sondern in einer Abwandlung auch in § 108b Abs. 2 i.V.m. § 95a Abs. 3 Nr. 2 UrhG als maßgebliches Merkmal eingesetzt, um zwischen „legitimen" und tatbestandsmäßigen Computerprogrammen zu unterscheiden.

„Angepasst" bedeutet dem Wortsinne nach, dass ein Gegenstand, der zuvor nicht oder nicht vollständig passt, so verändert wird, dass er vollständig passt. Hier geht es also um Vorrichtungen, welche die Zieltat an sich nicht ermöglichen, jedoch so modifiziert worden sind, dass sie die Zieltat nun möglich machen. In diesem Falle ist ihr Einführen und Verbreiten – egal zu welchen Zwecken – strafbar. Ein solches Anpassen der Vorrichtung erfordert dem Wortsinne nach, dass die Vorrichtung selbst verändert wird. Es liegt folglich sicher dann vor, wenn diese für deliktische Ziele *in ihrer Gestalt* verändert wird. Bei einem Computerprogramm ist das etwa der Fall, wenn die Dateien, aus denen es besteht, so manipuliert werden, dass das Programm Straftaten ermöglicht.

Beispielsweise ist Brennsoftware regelmäßig so programmiert, dass sie kopiergeschützte DVDs nicht kopiert, sondern den Kopierschutz „respektiert", auch wenn er technisch leicht umgangen werden könnte. Eine solche einprogrammierte Sicherung im Brennprogramm ließe sich jedoch entfernen, indem man das Programm *patcht*.[116] Führt man einen solchen *Patch* aus, so verändert man in der Regel ein-

---

[114] Vgl. *Entelmann*, Verbot von Vorbereitungshandlungen, S. 133 f.

[115] Siehe dazu oben 2.a)dd).

[116] Siehe zu *Patches*, *Cracks* und *Fixes* oben Teil 1, I.B.1.a).

zelne Dateien der Brennsoftware oder fügt in dem Installationsordner des Brennprogramms einzelne Dateien hinzu. Damit verändert man das Computerprogramm so, dass es die Begehung von Straftaten ermöglicht. Eine solche äußerliche Veränderung im Dateibestand ist aber nicht zwingend nötig.[117] Für die Tatbestandsmäßigkeit im vorliegenden Modell kann es jedoch auch schon genügen, wenn man ein grundsätzlich unverdächtiges Computerprogramm gemäß dessen regulären Funktionen nur so *konfiguriert*, dass es eine Straftat ermöglicht.

Ferner kann ein tatbestandliches Anpassen darin erblickt werden, dass zwei Vorrichtungen, die jeweils nicht unmittelbar zur Ausführung der Zieltat eingesetzt werden können, so zusammengefügt werden, dass sie die Zieltat unmittelbar ermöglichen. Ein gängiges Beispiel dieser Art dürfte bestimmte Hardware sein, die nur noch mit einer speziellen Soft- oder Firmware bespielt werden muss, um unmittelbar eingesetzt werden zu können. So liegt es etwa bei Digitalreceivern, die zum unautorisierten Empfang verschlüsselter Fernsehsignale erst verwendet werden können, wenn sie zuvor *gepatcht* worden sind. Dann können sie die Schlüssel einer (illegal beschriebenen) Smartcard auslesen und so das Fernsehsignal entschlüsseln.[118] Der Receiver allein stellt hier noch keine Umgehungsvorrichtung dar, da er nicht unmittelbar das Entschlüsseln ermöglicht.[119] Durch das Aufspielen des Patchs wird das Gerät jedoch so angepasst, dass es das Signal entschlüsseln kann, also die Zieltat ermöglicht. Entsprechend gilt dies für die eingesetzten Smartcards: Die Kartenrohlinge (Blanko-Smartcards, OPOS-Karten o.Ä.) müssen nämlich mit den passenden Schlüsseln beschrieben werden, bevor sie das Entschlüsseln des kryptischen Fernsehsignals im Receiver ermöglichen.[120] Der *ungepatchte* Receiver und die Blanko-Smartcard werden also durch das Aufspielen des Patchs bzw. das Beschreiben mit passenden Schlüsseln so angepasst, dass sie den unautorisierten Empfang eines verschlüsselten Signals in verständlicher Form ermöglichen.

Damit wird auch deutlich, dass es eine *objektive Eigenschaft* der Vorrichtung ist, so angepasst zu sein, dass sie die Zieltat ermöglicht.[121] Natürlich ist davon auszugehen, dass derjenige, der die Vorrichtung entsprechend angepasst hat (also den Kartenrohling beschrieben oder den Receiver gepatcht hat), bei seinem Tun auch subjektiv das Ziel hatte, das Zieldelikt zu ermöglichen. Nur insofern ist auch denjenigen Autoren zuzustimmen, die von dem subjektiven Element einer Ermög-

---

[117] Freilich ist dies ein etwas realitätsfernes Lehrbuchbeispiel, da heute die wesentlich einfachere Variante ist, gleich eines der unzähligen kostenlosen Brennprogramme zu benutzen, welche von Anfang an jeden Kopierschutz ignorieren. Bekannte Programme dieser Art sind etwa „CloneCD“ und „Alcohol 120%“, vgl. oben Teil 1, I.B.1.a).

[118] So auch im Sachverhalt von OLG Hamburg GRUR-RR 2010, 153, geschildert. Dort wurde jedoch nach § 95a Abs. 3 UrhG vorgegangen.

[119] LG Karlsruhe NStZ-RR 2007, 19; *Ernst*, CR 2004, 41; näher zum Kriterium der Unmittelbarkeit siehe unten dd).

[120] LG Karlsruhe NStZ-RR 2007, 19.

[121] So auch *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 113.

lichungsabsicht oder Intention des „Anpassers“ sprechen.[122] Sofern diese Autoren aber die Intentionen des „Anpassers“ zum entscheidenden Kriterium erheben wollen, entfernen sie sich von dem Schwerpunkt, den der Gesetzgeber semantisch gesetzt hat: Er spricht davon, dass die Vorrichtungen angepasst *sind* und beschreibt somit objektivierend eine Eigenschaft der Vorrichtung. Hätte der Gesetzgeber zum Ziel, die Absicht des Anpassers zum maßgeblichen Kriterium zu erheben, so würde er sinnvollerweise den Anpassungsvorgang und die damit verbundenen Intentionen im Gesetzeswortlaut hervorheben. Hierzu könnte er beispielsweise die Formulierung „Vorrichtungen, die *mit dem Ziel* angepasst *worden* sind, […]“ oder „Vorrichtungen, die *mit der Absicht* angepasst *worden* sind, […]“ verwenden. In grammatischer Auslegung ist also nicht die konkrete Intention des „Anpassers“ für die Strafbarkeit ausschlaggebend und muss vom Rechtsanwender deshalb auch nicht näher untersucht werden. Untersuchungsgegenstand sind vielmehr die Eigenschaften der Vorrichtung, insbesondere ihre Versions-Geschichte, aus der sich ablesen lässt, wie die Vorrichtung verändert wurde.

Schließlich ist fraglich, welche Auswirkungen es hat, dass die Vorrichtung im vorliegenden Modell *entsprechend* angepasst sein muss. Möglicherweise ist die Tatbestandsformulierung hier redundant. Semantischer Bezugspunkt von „entsprechend“ ist hier das „Bestimmt-Sein“ („dazu bestimmt oder entsprechend angepasst“). Dies würde bedeuten, dass die Vorrichtung so angepasst sein muss, dass ihr Angepasst-Sein einem Bestimmt-Sein entspricht.

Eine solche Regelung ergibt Sinn, wenn zwischen den beiden Tatbestandsalternativen grundsätzlich ein Stufenverhältnis besteht, welches durch die gewählte Formulierung ausgeglichen werden soll: das (grundsätzlich niedrigschwellige) Angepasst-Sein soll nur dann die Strafbarkeit auslösen, wenn es auch dem (höherschwelligen) Bestimmt-Sein entspricht. Ein solches Stufenverhältnis liegt im vorliegenden Tatbestandsmodell jedoch keineswegs auf der Hand. Auch finden sich in den Gesetzesmaterialien keine Ausführungen zum Verhältnis der Tatbestandsalternativen des Bestimmt-Seins und des Angepasst-Seins zueinander. Solche Ausführungen wären aber zu erwarten, wenn der Gesetzgeber tatsächlich von einem Stufenverhältnis ausginge. Daher ist vielmehr davon auszugehen, dass es sich bei dem Wort „entsprechend“ um eine überflüssige sprachliche Unschärfe handelt.

Dafür spricht auch ein sprachlicher Vergleich der englischen Fassung der Richtlinie 1998/84/EG, ihrer deutschen Fassung sowie dem daraus hervorgegangenen deutschen Gesetzestext: Während die englische Fassung von „any equipment […] designed or adapted to give access […]“ spricht, lautet der deutsche Richtlinientext

---

[122] Vgl. *Entelmann*, Verbot von Vorbereitungshandlungen, S. 66; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 85. Folgt man diesen Ansichten konsequent, so wären die Intentionen des „Anpassers“ maßgeblich, während die Intentionen des „Einführers“ oder „Verbreiters“, also des Vorfeldtäters irrelevant wären. Man erzeugte damit dasselbe Problem wie in obigem „Zweckmodell“, siehe oben I.B.2.

„jedes Gerät, das dazu bestimmt oder entsprechend angepasst ist, *um* den Zugang […] zu ermöglichen". Hieraus entstand wiederum der deutsche Gesetzestext „Vorrichtungen, die dazu bestimmt oder entsprechend angepasst sind, die […] Nutzung […] zu ermöglichen." Hier zeigt sich, dass bei der Übersetzung der englischen Richtlinienfassung einige sprachliche Unschärfen in die deutsche Version der Richtlinie geraten sind. So wurde das englische „designed" mit „dazu bestimmt" übersetzt, wodurch der Bezug zum schöpferischen Akt des Entwerfens oder Herstellens des jeweiligen Geräts bereits verwischt wird. Dieser Unterschied wird offenbar, wenn man die Übersetzung Art. 2 lit. e) der Richtlinie 1998/84/EG mit der Übersetzung von Art. 6 Abs. 2 c) der Richtlinie 2001/29/EG[123] vergleicht: Dort wird nämlich in einem ganz ähnlichen Zusammenhang[124] das englische „designed for the purpose of" im Deutschen mit „*entworfen*, um […] zu" übersetzt – womit der Bezug zur Produktion des Computerprogramms gewahrt bleibt.

Auch das Wort „entsprechend" findet sich nur in der deutschen Fassung der Richtlinie 1998/84/EG, während es in der englischen Sprachfassung keinen Gegenpart hat. Es liegt also nahe, dass dies auch in die Kategorie der übersetzungsbedingten sprachlichen Unschärfen einzuordnen ist. Im deutschen Gesetzestext wurde dann diese Redundanz übernommen, dafür wurde aber immerhin die umständliche und grammatisch fragwürdige Konstruktion „bestimmt oder entsprechend angepasst, *um* den Zugang […] zu ermöglichen" nicht übertragen, sondern der eleganteren Form ohne „um" Vorzug gegeben.

cc) „Zu ermöglichen"

Seine Begründung findet das Vorfelddelikt darin, dass durch das inkriminierte Verhalten breite Bevölkerungsschichten in die Lage versetzt werden, ohne großen Aufwand und mit relativ geringer Entdeckungsgefahr Straftaten zu begehen. Dies wird durch das tatbestandliche Erfordernis ausgedrückt, dass die Vorrichtung dazu bestimmt oder angepasst ist, die Begehung der Zieltat *zu ermöglichen*. Dies bedeutet eine Abgrenzung nach oben wie nach unten: Es genügt nicht, wenn die Vorrichtung dazu bestimmt oder angepasst ist, die Zieltat lediglich zu erleichtern, vielmehr muss es darum gehen, eine andernfalls unüberwindbare Hürde auszuschalten. Andererseits muss die Vorrichtung jedoch auch nicht dazu bestimmt oder angepasst sein, die gesamte Zieltat vollumfänglich selbst auszuführen. Damit hat das Ermöglichen auf den ersten Blick deskriptiven Charakter.

Fraglich ist aber, ob es vom Gesetzgeber ursprünglich als normatives Merkmal angesehen wurde und als solches zu interpretieren ist. In der Gesetzesbegründung findet sich nämlich die Klarstellung, dass es genüge, wenn die Vorrichtungen „*un-*

---

[123] Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

[124] Vgl. hierzu näher unten I.B.5.

ter anderem der Umgehung [des Zugangskontrolldienstes] *dienen*", da man sonst die Strafbarkeit zu leicht vermeiden könnte, indem man der Software gemischte Funktionen anfügt.[125] Dieser Klarstellung, die sich in ähnlicher Form auch bei den anderen Kriminalisierungsmodellen in den jeweiligen Gesetzesbegründungen findet, hätte es hier eigentlich gar nicht bedurft: Da der Gesetzeswortlaut vom Ermöglichen der Zieltat spricht, sind Vorrichtungen mit gemischten Funktionen von vornherein miterfasst. Ist nämlich ein Computerprogramm so angepasst, dass man mit ihm einen zugangskontrollierten Dienst unerlaubt nutzen kann, so ist es nach dem Gesetzeswortlaut völlig unerheblich, welche Funktionen es darüber hinaus hat. Selbst wenn die kriminelle Funktion angesichts einer Fülle an legitimen und legalen Funktionen völlig in den Hintergrund tritt, bleibt es dabei, dass das Computerprogramm (so angepasst ist, dass es) die Zieltat möglich macht und damit den Tatbestand erfüllt.[126]

Auffällig an der Wortwahl in der Begründung des Gesetzgebers ist aber, dass er von Vorrichtungen spricht, die der Umgehung *dienen*. Denn der Gesetzestext lässt bereits das Ermöglichen genügen. Genaugenommen sagt der Gesetzgeber hier also, dass Vorrichtungen dann tatbestandsmäßig sind, wenn sie daran angepasst sind, die Zieltat zu ermöglichen, und zwar dergestalt, dass sie der Begehung der Zieltat dienen, wobei es genügt, wenn sie unter anderem dazu dienen. Dies mutet zunächst kryptisch an, weist aber auf ein Problem dieses Kriminalisierungsmodells hin: Das zu kriminalisierende Phänomen erfordert eigentlich wertende Abstufungen. Denn offenkundig sollen nicht alle Vorrichtungen erfasst werden, die rein deskriptiv so angepasst sind, dass sie auch eine Straftat (hier die konkrete Zieltat) ermöglichen, sondern darunter nur diejenigen Vorrichtungen, die gerade in der Begehung der Zieltat ihren Sinn haben.[127] In der Auslegung und Anwendung der deskriptiven Tatbestandsmerkmale „angepasst" und „ermöglichen" lassen sich solche Wertungsstufen jedoch nicht abbilden. Der Gesetzgeber hatte dies offenbar erkannt und hat versucht, das deskriptive Merkmal des Ermöglichens normativ aufzuladen, indem er davon spricht, dass die jeweilige Vorrichtung eben nicht nur angepasst sein soll, die Zieltat zu ermöglichen, sondern dass auch sie der Begehung der Zieltat *dienen* müsse.

In der Gesetzesbegründung verwebt der Gesetzgeber damit einen normativen Aspekt in das deskriptive Tatbestandsmerkmal „ermöglichen", der zu erheblichen systematischen Friktionen führt. Denn es ist eine Wertungsfrage, wozu eine Vorrichtung dient und insbesondere, ob sie der Begehung einer *Straftat* dient. Ob die Vorrichtung die Straftat *ermöglicht*, ist dagegen gerade keine Wertungsfrage. Da

---

[125] BT-Drucks. 14/7229, S. 7 rechte Spalte.

[126] Dies übersieht offenbar das OLG Frankfurt a.M. GRUR-RR 2003, 287.

[127] Dieses Problem stellt sich in der Tatbestandsalternative „dazu bestimmt, […] zu ermöglichen" nicht, da das Bestimmt-Sein ein normatives Merkmal ist, welches aus Sicht des Verkehrs beurteilt wird, vgl. oben aa).

das Tatbestandsmerkmal des „Angepasst-Seins“ ebenfalls rein deskriptiv zu verstehen ist, leidet die Tatvariante „dazu angepasst, die Zieltat zu ermöglichen“ also daran, dass sie kein normatives Tatbestandsmerkmal bietet, in welchem Wertungsfragen verankert werden könnten. In der anderen Tatbestandsvariante des Bestimmt-Seins werden normative Wertungen aus Sicht des Verkehrs dagegen bereits berücksichtigt.[128] Würde man also im Merkmal des „Ermöglichens“ entgegen dem natürlichen Wortsinn eine weitere normative Stellschraube sehen, so führte dies zu einem Ungleichgewicht: In der Variante des „Bestimmt-Seins, die Zieltat zu ermöglichen“ wären zwei Wertungen zu treffen, während in der Alternative des „Angepasst-Seins, die Zieltat zu ermöglichen“ nur ein normativer Filter vorläge. Außerdem ergäbe sich ein normatives „Ermöglichen im Rechtssinne“, welches vom eigentlichen Wortsinn von „ermöglichen“ deutlich abweicht. Dies ist nicht wünschenswert.

Möchte man normative Aspekte auch in der Variante des „Angepasst-Seins“ berücksichtigen, um Vorrichtungen adäquat zu beurteilen, die so umgestaltet sind, dass sie legale und illegale Funktionen nebeneinander bieten, so muss man diese Kriterien in das Merkmal des „Angepasst-Seins“ einarbeiten. In diese Richtung geht die oben beschriebene subjektivierte Auslegung des Tatbestandsmerkmals „angepasst“.[129] Allerdings ergeben sich in dieser Auslegung weitgehende Überschneidungen mit dem Merkmal des Bestimmt-Seins. Dies wiederum lässt sich vermeiden, wenn man das Begriffspaar „bestimmt oder angepasst“ von vornherein als „ursprünglich entworfen oder nachträglich angepasst“ interpretiert.[130] Allerdings hat der Gesetzgeber diese Formulierung aus der Conditional-Access-Richtlinie gerade nicht übernommen. Im Modell des § 95a Abs. 3 UrhG[131] hat er dieses Problem von vornherein vermieden: Einerseits hat er ein anderes Begriffspaar gewählt, andererseits aber auch deskriptive und normative Tatbestandsmerkmale nebeneinander verwendet und diese sauber voneinander getrennt: Dort muss die Vorrichtung hauptsächlich (normativ) dazu angepasst sein (deskriptiv), die Zieltat zu ermöglichen (deskriptiv).[132]

Auf eine letzte Besonderheit des vorliegenden „Kriminalisierungsmodells“ ist noch hinzuweisen: Der Gesetzgeber hat hier darauf verzichtet, die handelnden Personen zu konkretisieren. Damit ist insbesondere unerheblich, wer die Vorrichtung anpasst, wer ihr die Bestimmung gibt und wem sie die Zieltat ermöglicht. Diese Personen müssen auch nicht identisch sein. In der Konsequenz werden auch Mehrpersonenverhältnisse vom Wortlaut erfasst: Wenn ein Computerprogramm aus Sicht der Verkehrs von *irgendjemandem* (z.B. dem Hersteller) dazu bestimmt wor-

---

128 Siehe oben aa).

129 Siehe oben bb).

130 Siehe die entsprechende Ansicht oben aa).

131 Siehe dazu sogleich I.B.4.

132 Siehe eingehend I.B.4. a).

den ist, *irgendeinem* Dritten die unautorisierte Nutzung zugangskontrollierter Dienste zu ermöglichen, so macht sich jeder strafbar, der diese Vorrichtung (zu gewerbsmäßigen Zwecken) einführt oder verbreitet.

dd) „Unmittelbar"?

Eine Vorrichtung, die in einer langen Kette von Vorbereitungshandlungen nur dazu bestimmt ist, den nächsten Vorbereitungsschritt zu ermöglichen, ist denklogisch zugleich dazu bestimmt, die spätere Zieltat zu ermöglichen – auch wenn sie bei der Zieltat selbst nicht eingesetzt werden soll. Da diese Vorrichtung aber im vorliegenden Kriminalisierungsmodell auch als tatbestandsmäßig angesehen werden müsste, droht bei sturer Auslegung und Subsumtion eine übermäßige Vorverlagerung der Strafbarkeit. Deshalb ist zu erwägen, wie die Vorfeldstrafbarkeit normativ begrenzt werden kann. Im „Eignungsmodell" wurde zu diesem Zweck das Unmittelbarkeitskriterium im Rahmen einschränkender Gesetzesauslegung eingeführt.[133] Wendet man dieses Kriterium auch hier an, so sind nur noch Vorrichtungen erfasst, welche dazu bestimmt oder entsprechend angepasst sind, die Zieltat *unmittelbar* zu ermöglichen, also die letzte Hürde auf dem Weg zur Ausführungshandlung des Zieldelikts zu nehmen.

In der Entscheidung des OLG Hamburg zu den FTA-Receivern[134] wurde diese Frage thematisiert, aber letztlich nicht entschieden: Das Instanzgericht ging offenbar von der Geltung dieses Unmittelbarkeitskriteriums aus, stellte aber klar, dass es nicht entgegenstehe, wenn die Vorrichtung erst im Zusammenspiel mit weiteren Bestandteilen die Zieltat (hier: die Umgehung technischer Schutzmaßnahmen) ermögliche.[135] Damit liegt es auf der Linie der vom Reichsgericht begründeten und bis heute aufrechtgehaltenen Rechtsprechung zur Unmittelbarkeit bei § 149 Abs. 1 Nr. 1 StGB. Im Februar 1914 entwickelte das Reichsgericht dieses Kriterium in einer Entscheidung zum damaligen § 151 StGB, dem Vorläufer des heutigen § 149 Nr. 1 StGB.[136] Hierbei ging es um Stempel zur unautorisierten Prägung von Münzgeld. Die Unmittelbarkeit wurde in der Entscheidung bejaht, obwohl auch die Stempel erst im Zusammenspiel mit weiteren Tatwerkzeugen wie einer Presse, einer Rändelmaschine und passendem Prägemetall die Zieltat (§ 146 StGB in der Fassung vom 1. Januar 1872) insgesamt ermöglichten.[137]

---

[133] Siehe oben I.B.1. a).

[134] OLG Hamburg GRUR-RR 2010, 153 ff. (= ZUM 2010, 63 ff.; MMR 2009, 851 ff.).

[135] OLG Hamburg GRUR-RR 2010, 155.

[136] RGSt 48, 161 ff., dort ging es zwar nicht um das *Ermöglichen der Zieltat*, sondern um Gegenstände, die *zum Zwecke der Zieltat dienlich* sind, jedoch spielt dies für die Frage der Unmittelbarkeit keine Rolle; vgl. auch oben I.B.1.a)bb).

[137] RGSt 48, 165.

Es ging also in der Frage der Unmittelbarkeit nie darum, ob die fragliche Vorrichtung bei der Durchführung der Zieltat das *einzige* eingesetzte Tatwerkzeug ist. Vielmehr ging es allein darum, ob die Vorrichtung *unmittelbar bei der Ausführung* der Zieltat eingesetzt wird – gegebenenfalls auch im Zusammenspiel mit anderen Tatwerkzeugen. Dennoch deutet das OLG Hamburg in seinem Urteil Zweifel hieran an, wenn es sagt, es könne dahinstehen, „ob dieser weitreichenden Umgehungsdefinition zuzustimmen ist".[138] Irritierend ist allerdings, dass das Gericht die Ausführungen der Vorinstanz offenbar als Ausführungen zum Zieldelikt auffasst. In der Tat wird auch beim Zieldelikt teilweise diskutiert, ob eine Umgehung der technischen Schutzmaßnahme nur dann vorliegt, wenn die Schutzmaßnahme durch die Tathandlung *unmittelbar beeinträchtigt* wird[139] oder ob es genügt, wenn die Tathandlung lediglich *darauf gerichtet* ist, die Schutzmaßnahme abzuschwächen.[140] Auf diesen (vermeintlichen) Streitstand bezogen sich die Ausführungen des LG Hamburg aber nicht.

Festzuhalten ist damit, dass sich das Unmittelbarkeitskriterium beim Vorfelddelikt allein darauf bezieht, ob die Vorrichtung als solche für die Zieltat gebrauchsfertig ist. Dies ist unabhängig davon zu beurteilen, ob die Vorrichtung bei der Ausführung der Zieltat mit anderen Tatwerkzeugen zusammengeschaltet oder kombiniert werden muss. Strikt zu trennen ist dieses Unmittelbarkeitskriterium im Vorfelddelikt außerdem von etwaigen Unmittelbarkeitskriterien beim Zieldelikt. Die zögerliche Haltung des OLG Hamburg ist insofern wohl einem Missverständnis geschuldet. Aus dem Wortlaut des Vorfelddelikts folgt ein Unmittelbarkeitskriterium nicht zwingend, jedoch geht das LG Hamburg offenbar[141] von seiner Geltung auch im vorliegenden Tatbestandsmodell aus.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Mit Blick auf den Multifunktionsaspekt und den Mehrzweckaspekt des Dual-Use-Phänomens ergeben sich bei dieser Regelungstechnik deutliche Abweichungen

---

138 GRUR-RR 2010, 155.

139 Siehe Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 28.

140 So die vom OLG Hamburg zitierte Gegenansicht bei Schricker/Loewenheim-*Götting*, § 95a Rn. 10. Tatsächlich aber handelt es sich dort wohl nur um eine unglückliche Formulierung, denn schon im Folgesatz führt *Götting* aus, dass unter der Umgehung einer Schutzmaßnahme jede Ausschaltung oder Manipulation der Maßnahme zu verstehen sei. Dieser finale Duktus legt nahe, dass auch hier von einer *unmittelbaren* Umgehung ausgegangen wird. Lediglich eines der aufgeführten Beispiele ist missverständlich: Der Einsatz eines Passwortknackers stellt tatsächlich nur dann eine Umgehung dar, wenn das Programm das geknackte Passwort automatisch verwendet und so die Passwortabfrage aushebelt. Solange das Passwort durch den Knacker nur „identifiziert", nicht aber verwendet wird, liegt noch keine Umgehung der technischen Schutzmaßnahme vor.

141 Die vorinstanzliche Entscheidung des LG Hamburg (Urteil vom 13.2.2008, Az. 308 O 3/08) ist bislang nicht im Volltext veröffentlicht.

zum Tatobjekt im zuvor erörterten „Zweckmodell". Dies liegt am Verzicht auf die Festlegung eines Bestimmungsgebers, an der Ergänzung um eine rein deskriptive Tatvariante und an der Anknüpfung an das bloße „Ermöglichen" der Zieltat. Zwar ähnelt das „Bestimmt-Sein des Computerprogramms" grundsätzlich dem „Zweck des Computerprogramms", jedoch kann das Computerprogramm im hiesigen „Bestimmungsmodell" sein deliktisches Bestimmt-Sein nicht nur durch den historischen Hersteller, sondern durch jeden beliebigen Bestimmungsgeber erhalten. Ob ein ursprüngliches deliktisches Bestimmt-Sein durch einen neuen Bestimmungsgeber später aufgehoben oder abgewandelt werden kann und welcher Bestimmungsgeber in solchen Konfliktfällen maßgeblich ist, ist unklar.

In der Tatvariante eines „deliktisch bestimmten" Computerprogramms tritt aber auch das Phänomen „bemakelter und makelloser Software"[142] auf: Computerprogramme werden nicht aufgrund ihrer Funktionen oder Eigenschaften, sondern aufgrund eines subjektiven Bestimmungsaktes durch einen abstrakten Bestimmungsgeber losgelöst vom konkreten Einzelfall als tatbestandsmäßig beurteilt. Diese Beurteilung haftet den Computerprogrammen sodann gleich einer Eigenschaft an und entzieht ihnen die Verkehrsfähigkeit. Wenn ein Computerprogramm aus Sicht des Verkehrs von *irgendjemandem* (z.B. dem Hersteller) dazu bestimmt worden ist, *irgendeinem* Dritten die unautorisierte Nutzung zugangskontrollierter Dienste zu ermöglichen, so macht sich *jeder* strafbar, der solche Vorrichtungen (zu gewerbsmäßigen Zwecken) einführt oder verbreitet. Er hantiert mit bemakelter Software und das ist nach diesem Regelungsmodell strafbar, ohne dass es darauf ankäme, welche Zwecke eigentlich der Einführende oder Verbreitende verfolgt.

Da diese Tatbestandsmodelle nur in Anschließungsdelikten verwendet worden sind, gibt es auch für IT-Sicherheitsbeauftragte keinen Ausweg aus der Strafbarkeit. Der Umgang mit diesen Programmen ist auch strafbar, wenn man keine Straftat vorbereitet.[143] Die Kehrseite dieses Phänomens ist, dass ein Computerprogramm, welches aus Sicht des Verkehrs nicht mit dem Makel einer deliktischen Bestimmung versehen ist, frei zirkulieren kann – auch wenn der Einführende oder Verbreitende um die deliktische Verwendbarkeit weiß und absichtlich Straftaten vorbereitet. Denn ob das Programm sich kriminell einsetzen lässt, spielt ebenso wenig eine Rolle wie die tatsächliche Intention des Vorfeldtäters. Maßgeblich ist allein die subjektive Bestimmung durch irgendeinen Bestimmungsgeber, welche sich irgendwie objektiv manifestiert haben muss.

In der Tatvariante des Angepasst-Seins wird unter dem Multifunktionsaspekt der Dual-Use-Problematik nicht differenziert: Jedes Computerprogramm mit einer deliktsermöglichenden Funktion ist tatbestandsmäßig, selbst wenn diese Funktion nebensächlich ist oder beiläufig oder zu ganz anderen Zwecken in das Computer-

---

142 Siehe dazu bereits oben 2.b).

143 Zu Vorbereitungsdelikten und Anschließungsdelikten ausführlich unten C.

programm eingebaut worden ist. Dies liegt daran, dass die Entscheidung über die Tatbestandsmäßigkeit der Software allein anhand deskriptiver Erwägungen erfolgt. Deshalb kann auch ein Computerprogramm tatbestandsmäßig sein, dessen deliktische Nutzung sich als Missbrauch darstellen würde. Diese Regelungstechnik orientiert sich damit an der Gefährlichkeit, die durch die Anpassung des Programms entstanden ist und verhindert somit, dass ein Computerprogramm frei zirkulieren kann, nachdem gefährliche Anpassungen vorgenommen worden sind. Programme, die von Anfang an deliktisch nutzbare Funktionen aufweisen, also nicht erst angepasst werden mussten, fallen jedoch nicht unter diese Regelung, sondern können nur nach obiger Variante des Bestimmt-Seins tatbestandsmäßig sein. Die Regelung des Angepasst-Seins macht mit ihrer weiten Kriminalisierung jedoch weitere Tatbestandsmerkmale erforderlich, damit danach differenziert werden kann, welche Ziele jemand verfolgt, der mit solchen Programmen umgeht. Werden – wie in § 4 ZKDSG i.V.m. § 3 Nr. 1, § 2 Nr. 3 ZKDSG – solche zusätzlichen Tatbestandsmerkmale nicht normiert, führt dieses Regelungsmodell zu einer unbedingten und unabwendbaren Gefährdungshaftung.

Ein IT-Sicherheitsbeauftragter, der auf gefährliche oder schädliche Software zwingend angewiesen ist, muss davon ausgehen, dass in diesem „Bestimmungs- und Anpassungsmodell“ die benötigte Software stets tatbestandsmäßig ist. Zumindest liegt es sehr nahe, dass sich irgendein Bestimmungsgeber konstruieren lässt, der dem jeweils genutzten Programm einmal eine deliktische Bestimmung gegeben hat. Zusätzlich lässt sich wohl auch häufig beweisen, dass ein bestimmtes Computerprogramm dazu angepasst ist, (auch) Straftaten zu ermöglichen. Da in den genannten Tatbeständen das „Vorbereiten einer Straftat“ nicht als Tatbestandsmerkmal aufgeführt ist, besteht für einen IT-Sicherheitsbeauftragten der einzige Weg aus der Strafbarkeit der vorliegenden Delikte darin, nicht die Tathandlungen des Einführens und Verbreitens zu verwirklichen. Wer sich *Cracking*-Software zu Testzwecken besorgen muss, sollte dies also unbedingt von inländischen Servern tun. Lädt er ein solches Programm zu Test-, Analyse- und Demonstrationszwecken von einem ausländischen Server herunter, macht er sich unzweifelhaft des Einführens einer Umgehungsvorrichtung strafbar.

4. „Hauptsächlich entworfen, hergestellt oder angepasst, um [die Zieltat] zu ermöglichen oder zu erleichtern“

Ein viertes Modell, welches in kleinen, aber erheblichen Details vom dritten hier vorgestellten Modell abweicht, liegt dem § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 3 UrhG zugrunde.[144] § 95a Abs. 3 Nr. 3 UrhG lautet:

---

[144] Vgl. die Übersicht zu den Strafvorschriften des Urheberrechts bei *Wang*, Strafrechtlicher Schutz des Urheberrechts, S. 36 ff. Zur historischen Entwicklung aus dem internationalen Recht, siehe *Wand*, Technische Schutzmaßnahmen, S. 23 ff.; *Entelmann*, Verbot

§ 95a Schutz technischer Maßnahmen

(3) Verboten sind die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und der gewerblichen Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen, die

[…]

3. **hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern**.

§ 108b Abs. 2 UrhG besagt:

§ 108b Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen

(1) Wer […], [wird] mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer **entgegen § 95a Abs. 3 eine Vorrichtung**, ein Erzeugnis oder einen Bestandteil **zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet**.

Zunächst fällt auf, dass die Tathandlungen in diesem Modell eine Weitung erfahren haben: Während im vorstehend erörterten Modell des § 4 ZKDSG i.V.m. §§ 3 Nr. 1, 2 Nr. 3 ZKDSG nur das Herstellen, Einführen und Verbreiten der Umgehungsvorrichtungen unter Strafe gestellt waren, erfasst § 108b Abs. 2 UrhG auch das Verkaufen und Vermieten.

Auch § 108b Abs. 2 UrhG stellt einen Blankettstraftatbestand dar, der seinen wesentlichen Inhalt durch den Verweis auf die Verbotsnorm des § 95a Abs. 3 UrhG erhält. Unglücklich ist dabei die Formulierung „entgegen § 95a Abs. 3 UrhG", denn die Verweisnorm des § 108b Abs. 2 UrhG bezieht sich nur auf Umgehungsmittel, während die Referenznorm § 95a Abs. 3 UrhG auch die Erbringung von Dienstleistungen zum Gegenstand hat. Das dortige Merkmal „*erbracht werden*, um die Umgehung […] zu ermöglichen" bezieht sich schon sprachlich nur auf die Erbringung von Dienstleistungen und ist damit im Rahmen des § 108b Abs. 2 UrhG obsolet. Dieser rechtstechnische Mangel hätte durch eine einfache Umformulierung vermieden werden können: Ebenso wird bestraft, wer eine Vorrichtung, ein Erzeugnis oder einen Bestandteil „im Sinne des § 95a Abs. 3" zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet. Auf die Dual-Use-Problematik hat dies jedoch keinen Einfluss.

In diesem Modell wird der Umgang mit solchen Vorrichtungen[145] unter Strafe gestellt, die die Zieltat[146] ermöglichen oder erleichtern sollen, und gerade hierzu

---

von Vorbereitungshandlungen, S. 21 ff.; überblicksartig zu den Umgehungsverboten im UrhG *Ernst*, CR 2004, 39 ff.

[145] Aus Gründen der Verständlichkeit wird hier wie im Folgenden darauf verzichtet, immer auch die Erzeugnisse und Bestandteile zu nennen. Die gesetzgeberische Intention ist offensichtlich eine möglichst breite und lückenlose Erfassung aller Geräte und Bauteile, vor allem aber von Software, vgl. *Arlt*, in: Hoeren/Sieber, Teil 7.7 Rn. 65; *Gercke*, in:

hauptsächlich entworfen, hergestellt oder angepasst werden. Vom vorstehend erörterten „Bestimmungs- und Anpassungsmodell" unterscheidet es sich dadurch, dass mit den Merkmalen des Entwerfens und Herstellens der gesamte Entstehungsprozess der Umgehungsvorrichtung stärker in den Fokus gerückt wird. Man kann deshalb auch vom „Entstehungsmodell" sprechen.

Außerdem ist nicht weiter erforderlich, dass die Vorrichtung die Zieltat ermöglichen soll, sondern es genügt bereits, wenn sie die Zieltat erleichtern soll. Das Merkmal des Bestimmt-Seins findet sich in diesem Modell nicht mehr, sondern wurde durch die Merkmale „entworfen" oder „hergestellt" ersetzt. Ein ganz erheblicher Unterschied liegt darin, dass in diesem Modell das normative Merkmal *hauptsächlich* eingefügt wurde, sodass wertende Betrachtungen unmittelbar im Tatbestand verankert werden können.

a) Charakteristika dieses Regelungsmodells

Soweit es auch hier um das *Anpassen* eines Computerprogramms geht, gilt das oben Gesagte.[147] Zu thematisieren sind an dieser Stelle deshalb nur die Tatbestandsvarianten, nach denen Vorrichtungen erfasst werden, die entworfen oder hergestellt werden, um die Zieltat zu erleichtern. Die Auswirkungen des normativen Merkmals „hauptsächlich" sind freilich mit Blick auf alle drei Tatbestandsvarianten zu diskutieren. Dem Merkmal des „Ermöglichens" kommt im Rahmen des § 108b Abs. 2 UrhG keine ausgrenzende Funktion mehr zu, da das Ermöglichen ein Mehr ist als das bloße Erleichtern. Somit ist hier das Tatbestandsmodell zu diskutieren, wonach jede Vorrichtung erfasst ist, die hauptsächlich entworfen oder hergestellt ist, um die Zieltat zu erleichtern.

aa) „[Dazu] entworfen oder hergestellt"

Das *Entwerfen* bezeichnet die Phase, in der eine ursprüngliche Idee so weit ausgearbeitet wird, dass mit der eigentlichen Produktion begonnen werden kann. In der Entwurfsphase werden beispielsweise Flussdiagramme, Programmablaufpläne sowie Grob- und Feinkonzepte angefertigt.[148] Die Entwurfsphase mündet in die eigentliche Herstellung, also das Programmieren, die Implementierung des Entwurfs in einen Quellcode sowie dessen Übersetzung in Maschinensprache.

Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 529; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 71.

146 Hier die Umgehung wirksamer technischer Schutzmaßnahmen gemäß § 108b Abs. 1 Nr. 1 i.V.m. § 95a Abs. 1 UrhG.

147 Siehe oben, I.B.3.a).

148 Vgl. *Chiampi Ohly*, SoftwareRecht, S. 41; *Kruth*, Grundlagen der IT, S. 64; *Redeker*, IT-Recht, S. 2.

Durch die Merkmale *entworfen* und *hergestellt* werden in diesem Tatbestand die Motive des ursprünglichen Software-Designers, Software-Entwicklers, Programmierers, Software-Ingenieurs etc.[149] mit seinem jeweiligen schöpferischen Akt verknüpft.[150] Die Finalität, mit der die Vorrichtung hergestellt worden ist, muss sich nämlich *vom schöpferischen Akt* der jeweiligen Person ablesen lassen. Daraus muss bereits erkenntlich werden, dass die Vorrichtung später eine Zieltat ermöglichen oder erleichtern soll, denn nur dann kann davon gesprochen werden, dass das Computerprogramm *dazu* entworfen oder hergestellt worden ist.

Teilweise wird diese Finalität auch als Absichtsmerkmal ausgelegt: Es müsse die Absicht des Herstellers im weiteren Sinne gewesen sein, durch seine Vorrichtung die Zieltat zu erleichtern.[151] Dafür spreche die Formulierung „entworfen oder hergestellt, *um […] zu*", die auch in anderen Tatbeständen als Hinweis auf einen erforderlichen dolus directus gelesen werde.[152] Dieser Analogschluss ist jedoch zweifelhaft, da die Um-zu-Konstruktion in den referenzierten Absichtsdelikten an die Tathandlung selbst anknüpft: Dort verknüpft der Täter mit seiner abgeschlossenen Handlung weitergehende Absichten. Im vorliegenden Modell geht es jedoch nicht um die Absichten des Täters (also des Vorfeldtäters, da hier ein Vorfelddelikt in Rede steht), sondern um die Intentionen des Tatobjekt-Herstellers oder Tatobjekt-Entwicklers. Es ist daher keineswegs zwingend, die Wertungen aus den Straftatbeständen des StGB hierher zu übertragen.

Im vorliegenden Fall würde ein Absichtsmerkmal die Beweisführung auch erheblich erschweren: Man müsste nicht nur nachweisen, dass der historische Hersteller im weiteren Sinne die maßgebliche Absicht hatte, sondern man müsste zusätzlich nachweisen, dass der Vorfeldtäter diesbezüglich zumindest dolus eventualis hatte. Freilich sind Beweisschwierigkeiten kein materiales Argument. Hier wird jedoch deutlich, dass vorliegend eine andere Konstruktion einschlägig ist: Während üblicherweise das Absichtsmerkmal eine erhöhte Gefährlichkeit der Tathandlung belegt und ein subjektiv erhöhtes Unrecht abbildet, ist dies hier nicht zwingend der Fall. Der Vorfeldtäter würde mit einem Gegenstand hantieren, mit dem ein Dritter einmal kriminelle Absichten verfolgt hat. Das erhöht nicht zwingend das subjektiv verwirklichte Unrecht und spricht auch nicht unbedingt für eine erhöhte Gefährlichkeit des Verhaltens des Vorfeldtäters.

---

[149] Im Folgenden soll immer dann vom Hersteller im weiteren Sinne gesprochen werden, wenn alle am Entwurf und an der Produktion des Computerprogramms Beteiligten gemeint sind.

[150] *Cornelius,* CR 2007, 686; Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 101.

[151] Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 101; *Hänel*, Umsetzung des Art. 6, S. 165; *Trayer*, Technische Schutzmaßnahmen, S. 116, 132; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 85.

[152] Vgl. *Sieber*, NStZ 2009, 359 f. mit Verweis auf §§ 96 und 265 StGB und m.w.N.

Anknüpfungspunkt für die Ermittlung dieser Finalität oder Absicht des Herstellers ist das objektive Erscheinungsbild der Vorrichtung oder ihr Design: Die Vorrichtung ist tatbestandsmäßig, wenn sich aus ihrem objektiven Design schließen lässt, dass ihr Hersteller sie gerade zur Erleichterung von Zieltaten entworfen, hergestellt oder angepasst hat. Dieser Schluss ist auch dann möglich, wenn der Hersteller nicht offen bekennt, dass es sich um eine Umgehungsvorrichtung handelt. Zwar werden Umgehungsvorrichtungen häufig auch als solche bezeichnet, jedoch soll es unter dem vorliegenden Regelungsmodell auch möglich sein, etwaige Schutzbehauptungen des Herstellers außer Acht zu lassen.

Im Gegenzug ist fraglich, wie damit umzugehen ist, wenn sich aus dem Design objektiv keine kriminelle oder legitime Tendenz ablesen lässt, und einzig eine Selbstbezichtigung des Herstellers vorliegt. Nach *Gercke* soll auch hier die Vorrichtung tatbestandsmäßig sein, weil sie ihre Ausrichtung auf Straftaten *auf beliebige Art* vom Hersteller im weiteren Sinne erhalten könne.[153] Dies strapaziert den Wortlaut sehr, denn dieser verlangt ja weiterhin, dass die Vorrichtung als Umgehungstool entworfen oder hergestellt worden ist. Es erscheint daher zweifelhaft, dass ein Hersteller am Ende des gesamten Produktionsprozesses allein durch die Bezeichnung der Vorrichtung quasi ex tunc festlegen kann, mit welchem Ziel das gesamte Geschehen zuvor abgelaufen ist. Indes erscheint dies auch nicht unvertretbar, denn ein Hersteller, der seine Motive offen bekennt, wird sich zumindest daran festhalten lassen. Allerdings könnte der Hersteller in diesem Falle die Vorrichtung durch eine bloße Umbenennung wieder dem Tatbestand entziehen, ohne dass er an der Programmgestaltung irgendeine Änderung vornehmen müsste.

Ein kleiner Unterschied zum verwandten Tatbestandsmodell der §§ 4, 3, 2 Nr. 3 ZKDSG besteht darin, dass dort die Rede von Vorrichtungen ist, die bestimmt oder angepasst *sind*, während es im hiesigen Modell um Vorrichtungen geht, die entworfen, hergestellt oder angepasst *werden*. Da der Gesetzgeber keine Ausführungen zu diesem abweichenden Detail macht, ist nicht zwingend anzunehmen, dass er damit inhaltliche Veränderungen vornehmen wollte. Zwar ließe sich argumentieren, dass durch die Verwendung des „sind" der Zustand oder die Beschaffenheit der Vorrichtung betont wird, während durch das „werden" stärker die Handlung des Herstellers im weiteren Sinne in den Vordergrund rückt. Am schlüssigsten erschiene ohnehin die Formulierung „entworfen, hergestellt oder angepasst *worden sind*", denn es handelt sich hierbei ja um eine Voraussetzung, die bereits erfüllt sein muss, wenn der Vorfeldtäter zur Tat schreitet. Es lässt sich jedoch nicht endgültig auflösen, ob es sich hier nicht eher um Unregelmäßigkeiten handelt, die dem hohen Arbeitsaufkommen in den zuständigen Ministerien geschuldet ist.

---

[153] *Gercke*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 533; unklar ist jedoch, wie das weitere dort aufgeführte Beispiel, nämlich dass ein *Anbieter* das Produkt als Umgehungstool *bewirbt*, mit den Attributen „entworfen, hergestellt oder angepasst" verknüpft werden kann. *Gercke* bringt hier eher ein Beispiel für § 95a Abs. 3 Nr. 1. Siehe dazu unten I.B.6.a).

Die größte Unsicherheit besteht zusammenfassend ohnehin in der Frage, wie die Intention des Herstellers im weiteren Sinne beschaffen sein muss. Insbesondere ist unklar, ob es sich dabei um einen eigenen deliktischen Vorsatz eines Dritten handelt, der hier vertatbestandlicht wird, welche Vorsatzform dann erforderlich ist und wie stark der Vorsatz konkretisiert sein muss, also welche Art von Zieldelikten der Hersteller im weiteren Sinne in seinen Vorsatz aufgenommen haben muss. Es ist auch nicht zu erwarten, dass diese Fragen in Kürze höchstrichterlich geklärt werden. Wahrscheinlicher ist, dass die Gerichte das Vorliegen dieses Tatbestandsmerkmals pauschal nach objektiven Kriterien aus Sicht des verständigen Durchschnittsnutzers einer solchen Vorrichtung bejahen oder verneinen werden, ohne sich gezielt mit den Intentionen eines einzelnen Herstellers und ihrer Verankerung in einzelnen Tatbestandsmerkmalen auseinanderzusetzen.[154]

bb) „Erleichtern"

Weiterhin zeichnet sich dieses Tatbestandsmodell dadurch aus, dass die Vorrichtungen nicht mehr dazu hergestellt (etc.) sein müssen, die Zieltat zu ermöglichen, sondern dass es bereits genügt, wenn sie die Zieltat erleichtern sollen. Freilich ist die Formulierung „zu ermöglichen oder zu erleichtern" dann redundant, denn das Ermöglichen ist ein Mehr zum Erleichtern, und eine Vorrichtung, die eine Zieltat ermöglichen soll, soll die Zieltat erst recht erleichtern.

Im Vergleich zum vorstehend erörterten Modell des § 4 ZKDSG i.V.m. § 3 Nr. 1, § 2 Nr. 3 ZKDSG ist dies also nochmals eine Erweiterung. Damit erübrigt sich auch die Diskussion um die Unmittelbarkeit, also die Frage, ob die Vorrichtung dazu hergestellt (etc.) sein muss, die Zieltat *unmittelbar* zu ermöglichen.[155] Denn der Begriff des Erleichterns erfasst typischerweise das mittelbare Ermöglichen. Damit ist jede Vorrichtung erfasst, die hergestellt (etc.) wird, um die Zieltat irgendwie zu fördern.

cc) „Hauptsächlich"

Die Vorrichtung muss *hauptsächlich* dazu entworfen, hergestellt oder angepasst sein, die Zieltat zu erleichtern. Damit werden die überwiegend deskriptiven Merkmale dieses Tatbestands um ein normatives Merkmal ergänzt, welches die Wertungen des Rechtsverkehrs direkt im Wortlaut verankert. Hier wird die Trennung zwischen der Analyse der Vorrichtungsfunktionen und der Bewertung dieser Funktionen offensichtlich: Die Vorrichtung muss hauptsächlich (normativ, Funktionsbewertung) dazu angepasst sein, die Zieltat zu ermöglichen (deskriptiv, Funktionsanalyse).

---

[154] Vgl. die Parallele oben I.B.3. a) aa) und *Entelmann*, Verbot von Vorbereitungshandlungen, S. 133 f.

[155] Vgl. oben I.B.3.a)dd).

Deshalb besteht kein Widerspruch zwischen der Feststellung, dass es genügt, wenn ein Computerprogramm so angepasst ist, dass es *auch* eine Straftat ermöglicht und der Forderung, dass das Programm *hauptsächlich* für die Begehung dieser Straftat hergestellt worden sein müsse. Beides ist schon nach dem Wortlaut erforderlich. *Arnold* betont den zweiten, normativen Aspekt und sagt mit Blick auf die BGH-Entscheidung im Clone-CD-Verfahren,[156] die Feststellung des deskriptiven Aspekts allein wäre „deutlich zu kurz gegriffen".[157] Letztlich tritt er dem BGH damit aber gar nicht entgegen: Dieser musste sich mit dem normativen Merkmal nämlich gar nicht auseinandersetzen, da von der Revision nicht angegriffen worden war, dass die Vorrichtung hauptsächlich dazu hergestellt wurde, die Zieltat zu ermöglichen.[158] Deshalb ist bis heute ungewiss, auf welche Kriterien man abstellen kann, wenn praktikabel bewertet werden soll, ob die Vorrichtung *hauptsächlich* für die Zieltat entworfen oder hergestellt worden ist. Die Schwierigkeiten ergeben sich vor allem daraus, dass die subjektiven Motive des Entwicklers oder Herstellers in diesem Modell den Ausschlag geben.[159] Im einfachsten Falle macht der Hersteller keinen Hehl daraus, illegale Ziele zu verfolgen. Beruft er sich aber darauf, dass sein Programm hauptsächlich wegen seiner legitimen Funktionen hergestellt wurde, die womöglich tatsächlich ein Alleinstellungsmerkmal gegenüber Konkurrenzprodukten darstellen, so wird der Gegenbeweis enorm aufwendig.

Dies soll an einem Beispiel verdeutlicht werden: Bei dem vom LG München I und OLG München beurteilten Programm *AnyDVD* der Firma *Slysoft*[160] handelt es sich um einen Treiber, welcher alle gängigen Kopierschutzmechanismen und Benutzungsbeschränkungen quasi ausschaltet.[161] Läuft dieser Treiber im Hintergrund, so lässt sich jede kopiergeschützte DVD oder CD mit einem beliebigen Brennprogramm kopieren. Zweifellos ist dieses Programm hauptsächlich dazu entworfen und hergestellt, die Umgehung wirksamer technischer Schutzmaßnahmen zu erleichtern. Es hat gar keine andere Funktion als die Umgehung technischer Schutzmaßnahmen. Damit erfüllt es § 95a Abs. 3 Nr. 3 UrhG.[162]

Wäre dieser Treiber aber in ein vollumfängliches Brennprogramm, etwa das Programm *CloneDVD* vom selben Anbieter, integriert,[163] so fiele die Beurteilung wesentlich schwerer: *CloneDVD* ist grundsätzlich dazu entworfen, DVDs zu kopie-

---

156 BGH NJW 2008, 3565.

157 *Arnold*, NJW 2008, 3545

158 Siehe BGH NJW 2008, 3566.

159 *Hänel*, Umsetzung des Art. 6, S. 165, spricht gar von der Absicht des Herstellers.

160 LG München I MMR 2008, 192 ff.; OLG München MMR 2009, 118; die Revisionsinstanz BGH MMR 2011, 391, setzte sich nicht mehr mit § 95a UrhG auseinander.

161 Vgl. oben Teil 1, I.B.1.a) und Fn. 33.

162 Die Münchener Gerichte haben ihre Urteile darauf gestützt, dass AnyDVD als Umgehungssoftware *beworben* wird und damit gegen § 95a Abs. 3 Nr. 1 UrhG verstößt. Siehe zu dieser Variante unten I.B.6.

163 Dass dies technisch möglich ist, sei hier unterstellt.

ren, und bietet daneben eine Vielzahl von zusätzlichen Funktionen an, zum Beispiel das Schneiden und Splitten des kopierten Films, das Entfernen von Menüs oder Extras einer DVD, die Veränderung der Datenausgabegröße, das Entfernen der *Layer Break Flag*, usw.[164] Wenn nun eine dieser vielen Zusatzfunktionen darin besteht, Kopierschutzmaßnahmen auszuschalten, muss diese Funktion so dominant sein, dass sie den Vorwurf an den Hersteller rechtfertigt, er habe eigentlich das gesamte Brennprogramm CloneDVD *hauptsächlich* hergestellt, um das Brennen kopiergeschützter DVDs zu ermöglichen. Der Hersteller wird sich immer darauf berufen, dass er sein Programm hauptsächlich wegen dessen legaler Funktionen entworfen habe (z.B. wegen besonders ansprechender Menüführung, besonders einfacher Bedienbarkeit oder weil das Programm besonders ressourcenschonend arbeitet etc.).

Freilich kann der Hersteller das Computerprogramm nicht einfach durch Schutzbehauptungen dem Tatbestand entziehen. Aber der Tatrichter muss Anhaltspunkte von einem solchen Gewicht feststellen, dass sie die Schutzbehauptung des Herstellers als solche erkennbar machen und ins Gegenteil verkehren. Der Tatrichter muss davon überzeugt sein, dass der verständige Durchschnittsnutzer[165] zu dem Schluss kommt, dass dieses Programm entgegen den Behauptungen des Herstellers hauptsächlich zur Umgehung von Kopierschutzmaßnahmen entworfen oder hergestellt worden ist. Liest man in die Tatbestandsvariante „hergestellt oder angepasst, um […] zu" ein Absichtsmerkmal hinein, so müssen die Umstände, welche die Herstelleraussagen widerlegen und seine Erleichterungs*absicht* beweisen sollen, umso gewichtiger sein.[166]

Die Frage, nach welchen Kriterien der verständige Durchschnittsnutzer zu einem solchen Schluss kommen kann, wird nur von einem Teil der Literatur weiter konkretisiert. Ein großer Teil überlässt diese Frage den Gerichten zur Entscheidung im Einzelfall.[167]

Nach *Arnold* ist dagegen eine Vorrichtung dann *hauptsächlich* für die Zieltat entworfen, hergestellt oder angepasst, wenn ein *hoher Anreiz* dazu besteht, die Vorrichtung rechtswidrig einzusetzen.[168] Um dies zu beurteilen, zerlegt er zunächst die

---

[164] Vgl. http://www.slysoft.com/de/clonedvd.html [Stand: 16.11.2014].

[165] OLG Frankfurt a.M. GRUR-RR 2003, 287, OLG Hamburg GRUR-RR 2010, 156; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 166; *Meschede*, Schutz digitaler Musik- und Filmwerke, S. 166; dagegen auf die allgemeine Lebenserfahrung abstellend: *Gutman*, K&R 2003, 493; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 84.

[166] Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 101; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 70; *Trayer*, Technische Schutzmaßnahmen, S. 116; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 85.

[167] *Entelmann*, Verbot von Vorbereitungshandlungen, S. 70; *Hänel*, Umsetzung des Art. 6, S. 165; *Meschede*, Schutz digitaler Musik- und Filmwerke, S. 166; *Pleister/Ruttig*, MMR 2003, 764.

[168] *Arnold*, MMR 2008, 145.

Vorrichtung in ihre einzelnen Funktionen und betrachtet jede Funktion isoliert. Die Funktionen sollen dabei so weit isoliert werden wie dies technisch möglich ist.[169] Befindet sich unter den herausgearbeiteten Funktionen eine illegale, so ist weiter zu prüfen, ob diese der Vorrichtung gezielt hinzugefügt worden ist. Hierfür soll auf objektive Indizien abgestellt werden: Für einen hohen kriminellen Anreiz und damit die Tatbestandsmäßigkeit der Vorrichtung spreche es, wenn die rechtswidrige Funktion trotz eines besonderen Gestaltungs- oder Programmieraufwands in die Vorrichtung verbaut worden ist.[170] Ein zweites Indiz für die Tatbestandsmäßigkeit sei es, wenn die rechtswidrige Funktion im Vergleich zu den rechtmäßigen Funktionen besonders einfach zu benutzen ist.[171] Dagegen soll eine Vorrichtung dann nicht *hauptsächlich* dazu entworfen (etc.) sein, die Umgehung von Schutzmaßnahmen zu erleichtern, wenn sich die Produktgestaltung allein am legalen Einsatz orientiert. Dies sei bei einem Computerprogramm etwa dann der Fall, wenn bei seinem legalen und illegalen Einsatz exakt dieselbe Funktionskette aktiviert werde. Es sei dann ein bloßer Reflex, dass die Vorrichtung auch illegal einsetzbar ist.[172] *Dreyer* schließt sich *Arnolds* Indizienkatalog an: Es müsse aus der Produktgestaltung der Schluss gezogen werden, dass der Hersteller (im weiteren Sinne) die Erleichterung der Zieltat *schwerpunktmäßig* bezweckt habe und es gerade nicht ausreiche, wenn er nur damit rechne oder in Kauf nehme, dass seine Vorrichtung die Zieltat erleichtert.[173]

Damit präsentieren *Arnold* und *Dreyer* überzeugende Indizien, welche zur Bewertung der Vorrichtung herangezogen werden können. Zweifelhaft ist einzig, ob die Vorrichtung für die rechtliche Analyse tatsächlich so weit in ihre einzelnen Funktionen aufgeflochten werden muss, wie dies *technisch möglich* ist. Zumindest Computerprogramme lassen sich technisch bis in die einzelnen Algorithmen oder sogar einzelne Zeilen eines Algorithmus trennen. Dies kann ersichtlich nicht gemeint sein, denn einzelne Algorithmen könnten nicht mehr sinnvoll auf einen Verstoß gegen § 95a Abs. 1 UrhG untersucht werden. Es erscheint dagegen zielführender, Vorrichtungen nur so weit in ihre Einzelfunktionen zu zerlegen, wie diese Einzelfunktionen noch einer rechtlichen Bewertung unterzogen werden können. Man muss die Vorrichtung also nicht so weit zerlegen, wie dies *technisch möglich* ist, sondern so weit, wie dies *rechtlich sinnvoll* ist. Ob man dabei den technischen Ansatz *Arnolds* wählt und ein Computerprogramm also in Programmcode-Abschnitte zerlegt oder ob man von vornherein einen gröberen Ansatz wählt, ist dann unerheblich. Allerdings ist darauf zu achten, dass nicht in der Unterteilung der Vorrichtungsfunktionen schon die spätere rechtliche Bewertung präjudiziert wird.

---

169 A.a.O., 146.

170 Ebd.

171 Ebd.

172 A.a.O., 146 f.; das Argument identischer Funktionsketten findet sich auch bei *Stickelbrock*, GRUR 2004, 739.

173 Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 101.

Gutman schlägt vor, man solle einerseits auf die bloße Eignung („Geeignetheit") zur Umgehung abstellen, andererseits auch auf den Hauptzweck nach allgemeiner Lebenserfahrung.[174] Die bloße Eignung ist jedoch weiter als der Wortlaut des Tatbestandes, da das Merkmal „hauptsächlich entworfen, hergestellt oder angepasst" ersichtlich höhere Anforderungen stellt. Das Abstellen auf die allgemeine Lebenserfahrung führt zudem kein normatives Merkmal ein, sondern sagt nur etwas über die Perspektive aus, nach der zu urteilen ist (ähnlich beim Abstellen auf einen verständigen Durchschnittsnutzer).

Götting vertritt, dass die Formulierung des § 95a Abs. 3 Nr. 3 UrhG lediglich ausdrücke, dass insgesamt eine objektive Zwecksetzung hinsichtlich der Umgehung einer technischen Schutzmaßnahme erforderlich sei und deshalb kaum wesentliche Unterschiede zu Nr. 1 und 2 bestünden.[175] Dieser Ansicht ist insofern beizupflichten, als die Nrn. 1–3 tatsächlich Vorrichtungen beschreiben, die jeweils in irgendeiner Weise besonders zu einem deliktischen Einsatz „neigen". Dabei darf man aber nicht übergehen, dass die Varianten an völlig unterschiedliche Charakteristika der Vorrichtung anknüpfen: Dies sind die Werbung in Nr. 1, wirtschaftliche Aspekte in Nr. 2 und die Motivation für die Produktion in Nr. 3. Daher ergeben sich sehr wohl wesentliche Unterscheide zwischen den Varianten.

Teilweise wird auch vertreten, § 95a Abs. 3 Nr. 3 UrhG sei ein Auffangtatbestand: Hier solle aus dem Gesamteindruck und der mutmaßlichen Tätermotivation geschlossen werden, ob die Vorrichtung zur Umgehung einer technischen Schutzmaßnahme erstellt worden ist.[176] Auch *Spindler/Leistner* gehen von einem Auffangtatbestand aus, der maßgeblich darauf abstelle, ob die Tathandlung eine Umgehung ermöglichen soll.[177] Diesen Auffassungen kann jedoch in jedem Punkt entgegengetreten werden: Erstens handelt es sich bei § 95a Abs. 3 Nr. 3 UrhG keineswegs um einen Auffangtatbestand zu den Nrn. 1 und 2, da die jeweils unterschiedlichen Nrn. 1–3 mitnichten in einem Stufenverhältnis zueinander stehen, wie dies für einen Auffangtatbestand typisch und erforderlich wäre. Die Nr. 3 ist daher schlicht ein *zusätzlicher* Tatbestand. Zweitens kommt es nicht auf die *Täter*motivation an, sondern auf die Motivation des Designers, Herstellers oder Anpassers. Dieser ist aber nicht zwingend identisch mit dem Täter, der die inkriminierten Tathandlungen (neben dem Herstellen auch das Einführen, Verbreiten, Verkaufen und Vermieten der Vorrichtung) vornimmt.[178] Drittens geht es nicht nur darum, ob die

---

[174] *Gutman*, K&R 2003, 493; auch auf die allgemeine Lebenserfahrung abstellend Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 84.

[175] Schricker/Loewenheim-*Götting*, § 95a Rn. 36 f.

[176] *Arlt*, in: Hoeren/Sieber, Teil 7.7 Rn. 68; *ders.*, DRM-Systeme, S. 83 f.

[177] *Spindler/Leistner*, GRUR-Int 2005, 793.

[178] Insofern inkonsequent *Spindler/Leistner*, GRUR-Int 2005, 793, die bei Verkaufsfördermaßnahmen nach § 95a Abs. 3 Nr. 1 UrhG noch korrekt feststellen, dass Vorfeldtäter und Werbetreibender auseinanderfallen können, bei Nr. 3 aber den Vorfeldtäter und den Hersteller in einen Topf werfen.

Vorrichtung zur Umgehung erstellt worden ist, sondern ausweislich des Wortlauts auch darum, ob sie dafür entworfen oder angepasst wird oder worden ist.

Einige der vorgestellten Ansichten sind eher kursorisch gehalten[179] oder fassen alle Tatbestandsvarianten des § 95a Abs. 3 Nr. 1–3 UrhG in eine einzige Gesamtabwägung nach nicht weiter spezifizierten objektiven Kriterien oder nach dem Gesamteindruck.[180] Häufig finden sich auch tautologische Ausführungen, etwa wenn gesagt wird, dass DVD-Ripper oder Crackprogramme das Tatbestandsmerkmal erfüllen, während normale Brennprogramme nicht dem Tatbestand unterfallen:[181] Hier wird die normative Frage einfach einer terminologischen Scheinlösung zugeführt, denn es ist ja gerade die Frage, woran man feststellen kann, ob ein Brennprogramm als Ripper oder Crackprogramm bezeichnet werden kann. Vor allem das von *Arnold* ausgearbeitete Anreizmodell bietet hierfür eine Reihe von Anhaltspunkten, die als Abwägungskriterien herangezogen werden können.

Auffällig ist, dass fast alle Ansichten allein das fertige Programm und seine Funktionen oder Verwendungsmöglichkeiten als Indizienquelle für die Abwägung heranziehen. Dabei dürfte es wesentlich einfacher sein, die Herstellermotivation zu ermitteln, wenn man auf die Entwurfs- und Herstellungsunterlagen für das Computerprogramm zugreift. Flussdiagramme, Programmablaufpläne, Grob- und Feinkonzepte sowie Workflows der Software-Entwickler und Syntax-Ingenieure dürften deutlich ergiebigere Informationsquellen dafür sein, welche Ziele der Hersteller bei der Erstellung seiner Software verfolgt hat.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Auch im vorliegenden Regelungsmodell tritt das Phänomen „bemakelter und makelloser Software“[182] auf: In der ersten Tatvariante werden Computerprogramme nicht nach ihren Funktionen oder Eigenschaften beurteilt, sondern maßgeblich ist die Zielsetzung des Programmentwicklers und Herstellers. Auch hier wird diese persönliche Zielsetzung des Herstellers im weiteren Sinne gleichsam als objektive Eigenschaft auf das Computerprogramm projiziert und entzieht ihm fortan die Verkehrsfähigkeit. Der Unterschied zum Vormodell ist, dass hier durch die Merkmale des Herstellens und Entwerfens der Programmentwickler als Bestimmungsgeber festgelegt worden ist. Welche Zwecke der Vorfeldtäter verfolgt, ist dagegen auch hier irrelevant. Er hantiert mit bemakelter Software und das ist nach diesem Rege-

---

[179] Sogar insgesamt unverständlich *Kröger*, CR 2001, 321.

[180] *Arlt*, in: Hoeren/Sieber, Teil 7.7 Rn. 68; *ders.*, DRM-Systeme, S. 83 f.; Fromm/Nordemann-*Czychowski*, § 95a Rn. 46; Dreier/Schulze-*Dreier*, § 95a Rn. 18; Spindler/Schuster-*Spindler*, UrhG § 95a Rn. 14 ff.

[181] Vgl. *Meschede*, Schutz digitaler Musik- und Filmwerke, S. 166; *Stickelbrock*, GRUR 2004, 739; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 84.

[182] Siehe dazu bereits oben 2.b) und 3.b).

lungsmodell ohne Weiteres strafbar, auch wenn er gar keine Straftat vorbereitet.[183] Die Kehrseite dieses Phänomens ist, dass ein Computerprogramm, welches nicht mit dem Makel eines „deliktischen Geburtsfehlers" versehen ist, frei zirkulieren kann –auch wenn es zu kriminellen Zwecken eingesetzt werden kann und etwa sein Verkäufer tatsächlich Straftaten wissentlich oder willentlich vorbereitet.

Das normative Merkmal „hauptsächlich" dürfte in der ersten Tatvariante regelmäßig durch die Finalität der Merkmale „hergestellt/entworfen, um […] zu" mitverwirklicht sein. In der zweiten Tatvariante des Angepasst-Seins wird dadurch jedoch eine normative Einschränkung vorgenommen, die diese Tatvariante an die erste annähert. Das oben Gesagte[184] gilt nun nämlich nicht mehr, da hier nicht mehr jedes Computerprogramm mit einer deliktserleichternden Funktion unter den Tatbestand gefasst werden kann. Vielmehr muss die deliktserleichternde Funktion hier den Hauptgrund für die Anpassung ausmachen. Dies lässt sich freilich nur unter Rückgriff auf die Intentionen des Anpassers beurteilen. Damit wird aber auch das Problem „bemakelter und makelloser Software" auf diese Tatvariante ausgedehnt.

Ein IT-Sicherheitsbeauftragter, der auf deliktisch verwendbare Software zwingend angewiesen ist, muss damit im vorliegenden Regelungsmodell stets prüfen, welche Intentionen der historische Hersteller, Entwickler oder Anpasser eines Programms verfolgt hat. Da in den genannten Tatbeständen das „Vorbereiten einer Straftat" nicht als Tatbestandsmerkmal normiert ist, besteht der einzige straflose Weg darin, lediglich auf Computerprogramme anerkannter Sicherheitsunternehmen oder anerkannter Sicherheitsexperten zurückzugreifen. Cracking-Software aus Hackerforen ist in der Regel tatbestandsmäßig, sodass sich die Strafbarkeit ihrer Einfuhr, Verbreitung, Vermietung und ihres Verkaufs auch für einen IT-Sicherheitsexperten, der in guter Absicht handelt, nicht vermeiden lässt.

Für den Verbotstatbestand des § 95a Abs. 3 UrhG ist in Abs. 4 eine Ausschlussklausel vorgesehen, durch die das Handeln öffentlicher Stellen zum Schutze der öffentlichen Sicherheit oder der Strafrechtspflege vom Verbot des Abs. 3 ausgenommen wird. In der Strafvorschrift des § 108b Abs. 2 UrhG wird zwar auf § 95a Abs. 3 UrhG verwiesen, allerdings in etwas umständlicher Form,[185] sodass sich die Frage stellt, ob die Ausschlussklausel des § 95a Abs. 4 UrhG auch im Rahmen der Strafvorschrift des § 108b Abs. 2 UrhG gelten soll und dort einen Tatbestandsausschluss in den genannten Fällen bewirkt.

Dafür sprechen systematisch-teleologische Erwägungen: Was schon nicht verboten sein soll, kann erst recht nicht strafbar sein. Der Wortlaut und die Struktur des § 108b Abs. 2 UrhG sprechen jedoch dagegen: Es wird dort nämlich explizit nur

---

[183] Zu Vorbereitungsdelikten und Anschließungsdelikten ausführlich unten C.

[184] Vgl. oben 3.b).

[185] Vgl. hierzu oben I.B.4. am Anfang.

auf Abs. 3 des § 95a UrhG verwiesen, nicht jedoch auf Abs. 4. Zudem findet sich der Verweis in einem Satzteil, der die tatgegenständlichen Vorrichtungen, Erzeugnisse und Bestandteile konkretisieren soll. Dies spricht dafür, nicht einmal den gesamten § 95a Abs. 3 UrhG im Rahmen des § 108b Abs. 2 UrhG heranzuziehen, sondern lediglich die tatbestandliche Umschreibung der Verbotsobjekte in den Nrn. 1–3 des § 95a Abs. 3 UrhG.

Hiergegen ließe sich wiederum einwenden, dass § 108b Abs. 2 UrhG gerade nicht von „Vorrichtungen, Erzeugnissen oder Bestandteilen *im Sinne des § 95a Abs. 3 Nr. 1–3 UrhG*" spricht, sondern durch die Wortwahl „entgegen § 95a Abs. 3" einen pauschalen Verweis macht, und gegen § 95a Abs. 3 UrhG eben nur das verstößt, was nicht von Abs. 4 privilegiert ist. Folglich gälte die Ausschlussklausel des Abs. 4 auch im Rahmen des § 108b Abs. 2 UrhG.

Erklärt man hier die Ausschlussklausel für anwendbar, so verschafft sie nur den öffentlichen Stellen und den Personen, derer sich die privilegierten öffentlichen Stellen bedienen, einen Tatbestandsausschluss.[186] Der private Bereich, namentlich die IT-Sicherheitsbranche, die zu Test-, Analyse- und Demonstrationszwecken auf tatbestandsmäßige Software angewiesen ist, wird dagegen nicht erfasst.

Ausschlussklauseln können jedenfalls ein effizientes und präzises Mittel zur Eingrenzung der Strafbarkeit darstellen, insbesondere bei der Feinjustierung der Dual-Use-Bereiche. Im Kriegswaffen- und Exportkontrollrecht finden sich Tatbestandsmodelle, die maßgeblich auf Ausschlussklauseln als Regelungstechnik für das Dual-Use-Phänomen setzen.[187]

Im Urheberstrafrecht zeigt sich hinsichtlich der Dual-Use-Problematik eine Besonderheit: Aus § 95a Abs. 1 UrhG folgt, dass das Verbot der Umgehung wirksamer technischer Schutzmaßnahmen nur für solche Werke gilt, die gemäß § 2 UrhG geschützt sind. Das Umgehungsverbot für technische Schutzmaßnahmen ist also kein Selbstzweck, sondern dient dem Schutz der Werke und Leistungen der Rechtsinhaber.[188] In dem Moment, in dem ein ursprünglich geschütztes Werk gemeinfrei wird, verliert also auch das Umgehungsverbot seine Legitimation und kann nicht fortbestehen.[189] Auslegungstechnisch löst man dies, indem man die Schutzmaßnahme als nicht mehr wirksam im Sinne des § 95a UrhG betrachtet, da sie kein Schutzziel mehr sicherstellen kann.[190] Entfällt das Umgehungsverbot, so verliert

---

[186] Statt aller Dreier/Schulze-*Dreier*, § 95a Rn. 19.

[187] Siehe hierzu unten III.E.

[188] BGH NJW 2008, 3566.

[189] Siehe nur *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 30, 99, 109; Dreier/Schulze-*Dreier*, § 95a Rn. 3; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 41; Schricker/Loewenheim-*Götting*, § 95a Rn. 3; *Schäfer*, Kartellrechtliche Kontrolle, S. 112; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 52 und 68.

[190] Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 25; Schricker/Loewenheim-*Götting*, 95a Rn. 20; *Trayer*, Technische Schutzmaßnahmen, S. 132.

auch die technische Maßnahme zum Schutz dieses Umgehungsverbots ihre Daseinsberechtigung.[191] Dennoch ist umstritten, wie sich der Ablauf der Schutzfrist im Rahmen des § 95a Abs. 3 UrhG auswirkt.[192]

In konsequenter Auslegung lassen sich nach Schutzfristablauf die Umgehungsvorrichtungen nicht mehr unter § 95a Abs. 3 Nr. 1–3 UrhG fassen, da sie nicht (mehr) entworfen, hergestellt oder angepasst sind, die Umgehung *wirksamer* technischer Schutzmaßnahmen im Sinne des Abs. 1 zu erleichtern.[193] Wenn die Umgehungsvorrichtungen bereits vor Ablauf der Schutzfrist hergestellt worden sind, waren sie zwar möglicherweise tatbestandsmäßig, solange die technische Schutzmaßnahme wirksam war, also die Schutzdauer anhielt. Verliert aber das Werk seinen urheberrechtlichen Schutz, so ist das Umgehungsmittel nur noch dafür hergestellt, eine ehemals wirksame technische Schutzmaßnahme zu umgehen, also eine Schutzmaßnahme, die nicht mehr existiert. Damit ist das Umgehungsmittel nicht tatbestandsmäßig. Dies gilt freilich nur, wenn die konkrete Umgehungvorrichtung allein auf die Umgehung der Schutzmaßnahmen *freier* Werke angelegt ist.

Hieraus erwächst im Urheberrecht ein besonderer Mehrzweckaspekt des Dual-Use-Phänomens: Jede Vorrichtung, die sich deliktisch, also zur Umgehung einer wirksamen technischen Schutzmaßnahme, einsetzen lässt, lässt sich unabhängig von einer Einwilligung des Rechtsinhabers legal einsetzen – spätestens wenn die Schutzdauer des Werkes abläuft. Während in den anderen Rechtsgebieten also der Mehrzweckaspekt des Dual-Use-Phänomens vor allem deshalb besteht, weil IT-Sicherheitsbeauftragte auf schädliche Computerprogramme zu Test- und Analysezwecken zugreifen müssen, mag man im Urheberrecht womöglich auf ursprünglich schädliche Computerprogramme zugreifen, weil die Schutzfrist des Werkes abgelaufen ist.

In den anderen Rechtsgebieten hängt die Unterscheidung zwischen rechtmäßig und rechtswidrig von normativen Tatbestandsmerkmalen ab. Im Urheberrecht hängt sie zusätzlich vom maßgeblichen *Zeitpunkt* ab. Allein aufgrund des anstehenden Schutzfristablaufs kann man also im Urheberrecht jede Umgehungsvorrichtung als Dual-Use-Vorrichtung bezeichnen.[194] Eine rein deliktische Umgehungs-

---

[191] OLG München MMR 2009, 119; siehe auch Erwägungsgründe 47 und 48 zur Richtlinie 2001/29/EG; siehe auch *Enders*, ZUM 2004, 600.

[192] Dieses Problem stellt sich nur bei Ablauf der Schutzfrist, nicht aber wenn der Verwender einer Umgehungsvorrichtung sich darauf beruft, Schrankenbestimmungen der §§ 45 ff. UrhG mittels Umgehungsvorrichtung durchzusetzen. Das Urheberrecht gewährt dem Schrankenprivilegierten kein Selbsthilferecht, vgl. *Meschede*, Schutz digitaler Musik- und Filmwerke, S. 168 ff.

[193] So *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 101 f.; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 42; *Kauert*, in: Wandtke (Hrsg.), Urheberrecht, S. 278.

[194] So *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 102; *ders.*, MMR 2008, 145.

vorrichtung kann es demnach nur geben, *solange* bei dem entsprechenden Werk die Schutzfrist noch nicht abgelaufen ist.

Dieses Problems kann man sich entledigen, indem man entgegen obiger Darstellung einfach alle Umgehungsvorrichtungen unter § 95a Abs. 3 UrhG fasst, unabhängig davon, ob sie darauf angelegt sind, die Schutzmaßnahmen freier Werke oder geschützter Werke zu umgehen. In einigen Publikationen wird dies vertreten,[195] obwohl selbst deren Autoren klarstellen, dass von § 95a Abs. 3 UrhG nur solche Vorrichtungen erfasst sind, die *wirksame* technische Maßnahmen im Sinne des § 95a Abs. 1 UrhG umgehen.[196] Zwar verstehen auch sie nur solche technischen Maßnahmen als wirksam, die verhindern sollen, dass *geschützte* Werke oder andere *Schutz*gegenstände rechtswidrig genutzt werden,[197] jedoch wird ein pauschales Verbot von Umgehungsvorrichtungen damit begründet, dass mit der Regelung des Abs. 3 eine weitreichende und effektive Kontrolle der Rechtsinhaber angestrebt worden sei.[198]

Diese Behauptung stützt sich vornehmlich auf Erwägungsgrund 51 der Info-RL, wonach der Rechtsschutz technischer Schutzmaßnahmen pauschal gelte und die Ausnahmen- und Schrankenregelungen des Art. 5 Info-RL durch freiwillige Maßnahmen der Rechtsinhaber durchgesetzt werden sollen.[199] Allerdings spricht Erwägungsgrund 51 nur abstrakt davon, dass der „Rechtsschutz technischer Maßnahmen" unbeschadet des Allgemeininteresses und der öffentlichen Sicherheit gelte, und auch die darauffolgenden Ausführungen zu den freiwilligen Maßnahmen der Rechtsinhaber müssen nicht zwingend dahingehend verstanden werden, dass der Rechtsschutz grundsätzlich über die Urheberrechtsschranken hinausreicht.

Ebenso wenig findet sich eine solche gesetzgeberische Intention in den Gesetzesmaterialien zum deutschen § 95a UrhG wieder. Auch in der Sache würde ein pauschales Verbot von Umgehungsvorrichtungen nicht überzeugen. Bei freien Werken geht es schließlich um einen Bereich, in dem der Rechtsinhaber gerade *keine* Rechte mehr hat. Ein berechtigtes Interesse des (vormaligen) Rechtsinhabers an einer effektiven und weitreichenden Kontrolle kann hier also gar nicht bestehen.[200]

---

[195] *Arlt,* DRM-Systeme, S. 84, 141; *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 117; Schricker/Loewenheim-*Götting*, § 95a Rn. 24; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 68; wohl auch *Gutman*, K&R 2003, 493.

[196] Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 71.

[197] Schricker/Loewenheim-*Götting*, § 95a Rn. 3; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 12.

[198] *Auer*, FS für Dittrich, S. 18; Schricker/Loewenheim-*Götting*, § 95a Rn. 24 unter Verweis auf *Reinbothe*, GRUR-Int 2001, 741, der sich a.a.O. aber nicht zur Dual-Use-Problematik äußert, sondern lediglich konstatiert, dass die speziellen Schranken und Ausnahmen des Umgehungsverbots nicht auch für das Vorfeld gelten.

[199] Vgl. EG 51, Richtlinie 2001/29/EG.

[200] So auch *Entelmann*, Verbot von Vorbereitungshandlungen, S. 42; *Trayer*, Technische Schutzmaßnahmen, S. 117.

Außerdem würde das pauschale Verbot einen systematischen Bruch bedeuten: Der mittelbare Urheberrechtsverletzer würde schlechter gestellt als der unmittelbare Urheberrechtsverletzer, denn dieser kann sich auf die Gemeinfreiheit berufen.[201] Auch würde die mittelbare Urheberrechtsverletzung nach § 95a Abs. 3 UrhG umfassender geahndet als die anderen mittelbaren Urheberrechtsverletzungen, bei denen Schrankenregelungen und die Gemeinfreiheit berücksichtigt werden.[202]

Möglicherweise liegt hier auch ein Missverständnis vor: Die Argumentation der Gegenseite wäre dann schlüssiger, wenn es im vorliegenden Modell darauf ankäme, wozu das Umgehungsmittel *geeignet* ist. Wären in diesem Falle alle Umgehungsmittel vom Tatbestand ausgenommen, die *zumindest auch* bei freien Werken Schutzmaßnahmen umgehen *können* (also auch dazu geeignet sind), so liefe der Tatbestand leer. Um dies zu verhindern, müsste man tatsächlich erwägen, alle Dual-Use-Vorrichtungen einzubeziehen. Im Kriminalisierungsmodell des Urheberrechts geht es aber gerade nicht um die deskriptive Frage, wozu eine Umgehungsvorrichtung geeignet ist, sondern um die normative Frage, wofür sie hauptsächlich entworfen, hergestellt oder angepasst wird oder worden ist.[203] Und in dieser Frage ist das Gesetz eindeutig.

Nach überzeugender Ansicht werden daher Vorrichtungen, die dafür entworfen, hergestellt oder angepasst werden, *ausschließlich bei freien Werken* technische Schutzmaßnahmen zu umgehen, nicht vom Tatbestand der §§ 108b Abs. 2, 95a Abs. 3 UrhG erfasst. Dies folgt zwingend aus dem Gesetz. Die überwiegend vertretene Gegenmeinung, welche § 95a Abs. 3 UrhG auch auf Vorrichtungen zur Umgehung der Schutzmaßnahmen freier Werke ausdehnen will, stellt – jedenfalls sofern man diese Meinung auch i.V.m. § 108b Abs. 2 UrhG vertritt – eine täterbelastende Analogie dar und verstößt gegen Art. 103 Abs. 2 GG. Sicherlich kann man sich fragen, wie praxisrelevant diese Gedankenspiele sind. Angesichts des rasanten technischen Fortschritts ist es kaum absehbar, ob die Schutzmaßnahmen von heute überhaupt noch als wirksame Schutzmaßnahmen angesehen werden, wenn die heute geschützten Werke einst gemeinfrei werden. Nicht weniger fraglich ist, ob es dann überhaupt noch die Umgehungsvorrichtungen von heute gibt.

Umgehungsmittel, die dazu geeignet sind, zugleich wirksame und unwirksame technische Schutzmaßnahmen zu umgehen, sind also weder von vornherein dem Tatbestand entzogen[204] noch unterfallen sie automatisch dem Tatbestand.[205]

---

[201] *Haedicke*, FS für Dietz, S. 362.

[202] Vgl. a.a.O., S. 361.

[203] Vgl. oben I.B.4. a).

[204] So aber *Kauert*, in: Wandtke (Hrsg.), Urheberrecht, S. 278; dagegen *Dreier*, ZUM 2002, 38.

[205] So aber *Arlt*, DRM-Systeme, S. 84, 141; *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 117; Schricker/Loewenheim-*Götting*, § 95a Rn. 24; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 68.

Auch ist nicht richtig, dass man zwingend entweder der ersten oder der zweiten Ansicht folgen müsste.[206] Solch apodiktische Auslegungen der §§ 108b Abs. 2, 95a Abs. 3 UrhG würden auch zu inkonsistenten Ergebnissen führen, in Anbetracht der Tatsache, dass jede Umgehungsvorrichtung (zumindest nach Ablauf der Schutzfrist) auch legal einsetzbar ist. Es kommt in diesen Fällen vielmehr auf die wertende Betrachtung durch den Verkehr an, der beurteilt, wozu eine ambivalent einsetzbare (oder „zweckneutrale“) Vorrichtung hergestellt, entworfen oder angepasst worden ist.[207] Deshalb ist auch die Befürchtung nicht gerechtfertigt, dass in diesen Fällen die Rechtsinhaber durch Verwenden technischer Schutzmaßnahmen auch die Nutzung gemeinfreier Werke diktieren könnten[208] – vielmehr diktiert der Verkehr.

Zusammenfassend ist festzuhalten, dass dieses „Entstehungsmodell“ den Blick auf die historischen Hersteller im weiteren Sinne lenkt. Sie geben dem Computerprogramm durch ihren jeweiligen schöpferischen Akt eine erste Bestimmung, die sich freilich im Lauf des Produktlebens durch ein Anpassen des Computerprogramms auch ändern kann. Der Multifunktionsaspekt des Dual-Use-Phänomens wird durch das Merkmal „hauptsächlich“ berücksichtigt. Auf den Mehrzweckaspekt des Dual-Use-Phänomens wirkt sich das „Entstehungsmodell“ lediglich insofern aus, als es die historischen Hersteller im weiteren Sinne oder spätere Anpasser zum jeweils maßgeblichen Bestimmungsgeber macht – nicht den Endnutzer des Computerprogramms. Der Endnutzer und seine Intentionen haben damit keinen Einfluss auf die Tatbestandsmäßigkeit des Computerprogramms.

5. Begrenzter wirtschaftlicher Zweck oder Nutzen neben der Zieltat

In einem fünften Modell wird nun der Fokus weg von der Herstellung der Software hin zu ihrem Einsatz verschoben. Hier ist nicht erheblich, wozu das Umgehungsmittel aus Hersteller- oder Händlersicht eingesetzt werden soll,[209] sondern wozu es wirtschaftlich sinnvoll eingesetzt werden kann oder worin sein besonderer wirtschaftlicher Nutzen liegt. Damit rückt anstelle des Herstellers der Programm-Nutzer in den Blick. Dieses Modell liegt dem § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 2 UrhG zugrunde. Letzterer lautet:

> **§ 95a Schutz technischer Maßnahmen**
> (3) Verboten sind die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und der gewerblichen

---

206 So aber *Arnold*, Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht, S. 117: „tertium non datur“.

207 So auch die überzeugende Auffassung in der Rechtsprechung, vgl. oben I.B.3.a) und 4.a).

208 Befürchtung bei *Kauert*, in: Wandtke (Hrsg.), Urheberrecht, S. 278.

209 Vgl. Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 98.

> Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen, die
>
> […]
>
> 2. **abgesehen von der Umgehung wirksamer technischer Maßnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben**
>
> […]

§ 108b Abs. 2 UrhG besagt:

> **§ 108b Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen**
>
> (1) Wer […], [wird] mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
>
> (2) Ebenso wird bestraft, wer **entgegen § 95a Abs. 3 eine Vorrichtung, ein Erzeugnis oder einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet**.

Dieses Tatbestandsmodell lenkt den Blick auf wirtschaftliche Erwägungen und kann deshalb als „ökonomisches Modell" bezeichnet werden. Es erweckt mit seiner Rede vom *begrenzten* wirtschaftlichen Zweck auf den ersten Blick einen etwas saloppen Eindruck. Da eine Vorrichtung mit *unbegrenztem* wirtschaftlichem Nutzen schwer vorstellbar ist, liegt es zumindest nicht auf der Hand, welche Bedeutung diesem – eigentlich ausgrenzenden – Merkmal zukommen soll. Dies wird im Folgenden genauer untersucht.

a) Charakteristika dieses Regelungsmodells

Zur Unterscheidung zwischen schädlichen und legitimen Vorrichtungen setzt der Gesetzgeber hier auf eine wirtschaftliche Betrachtungsweise. Entscheidend ist der wirtschaftliche Zweck oder der wirtschaftlichen Nutzen der Vorrichtung. Dieser muss – abgesehen vom Zweck und Nutzen der Vorrichtung bei *illegalem* Einsatz – begrenzt sein, damit die Vorrichtung vom Tatbestand erfasst ist.

aa) Wirtschaftlicher Zweck

Der wirtschaftliche Zweck einer Vorrichtung lässt sich in einer freien Auslegung umschreiben als ein wirtschaftlich ertragreiches Ziel, welches durch eine bestimmte Einsatzart der Vorrichtung erreicht werden soll. Oben wurde gezeigt, dass sich ein *Zweck* immer aus dem Zusammenspiel dreier Fixpunkte ergibt („dreistrahlige Beziehung"):[210] erstens eines Subjekts, zweitens dessen Handlung und drittens des eingesetzten Mittels, hier also der Vorrichtung. Vorliegend geht es um den *wirtschaftlichen* Zweck, also sind von allen verfolgbaren Zielen nur die wirtschaftlich relevanten zu untersuchen.

---

[210] Vgl. oben, I.B.2.a).

Möglicherweise soll das vorliegende Tatbestandsmodell jedoch gar nicht so feinsinnig ausgelegt werden. Bei der Formulierung „wirtschaftlicher Zweck oder Nutzen" könnte es sich insgesamt um eine umgangssprachliche Spreizung handeln. Denkbar ist nämlich, dass der Gesetzgeber angesichts der Dual-Use-Problematik durch diese Wortwahl schlicht einen Abwägungsmechanismus nach Wirtschaftlichkeitskriterien einfügen wollte und die Begriffe „Zweck" und „Nutzen" folglich als Platzhalter hierfür fungieren.[211] Diese Vermutung liegt auch deshalb nahe, weil weder die zugrunde liegende Richtlinie 2001/29/EG noch die Gesetzesbegründung irgendwelche Einzelheiten zu Sinn und Bedeutung der Tatbestandsmerkmale „Zweck" und „Nutzen" sowie ihrer Abgrenzung voneinander enthalten. Auch in der Literatur konzentrieren sich die Ausführungen auf den wirtschaftlichen Nutzen oder allgemein wirtschaftliche Erwägungen, die unter dem zusammengezogenen Begriffspaar „Zweck und Nutzen" angestellt werden.

bb) Wirtschaftlicher Nutzen

Der Tatbestand erfasst auch eine Vorrichtung, deren wirtschaftlicher Nutzen neben der Umgehung wirksamer technischer Schutzmaßnahmen begrenzt ist. Es ist also zunächst zu untersuchen, welchen wirtschaftlichen Nutzen die Vorrichtung überhaupt hat. Ein wirtschaftlicher Nutzen ist jeder wirtschaftliche Vorteil, den das Verwenden der Vorrichtung bringt.[212] Im Falle der Umgehung eines Kopierschutzes liegt der Nutzen für den Verwender also in der Möglichkeit, eine Kopie des geschützten Werks anzufertigen. Der *wirtschaftliche* Nutzen liegt damit in den ersparten Aufwendungen, die der Verwender bei rechtmäßiger Anfertigung einer Kopie des Werks hätte aufbringen müssen. Also hat der wirtschaftliche Nutzen etwa die Höhe einer normalerweise erforderlichen Lizenzgebühr. Eine Vorrichtung, deren einziger Nutzen für den Verwender in dieser Umgehung liegt, ist unzweifelhaft vom Tatbestand des § 95a Abs. 3 Nr. 2 UrhG erfasst. Denn dann hat diese Vorrichtung abgesehen von der Umgehung gar keinen wirtschaftlichen Nutzen.

Lässt sich die Vorrichtung aber auch anderweitig einsetzen und bringt sie dem Verwender auch bei einem solch anderweitigen Einsatz einen wirtschaftlichen Nutzen, so muss dieser Nutzen laut Tatbestand begrenzt sein.

cc) „Begrenzt"

Der wirtschaftliche Zweck oder Nutzen, den die Vorrichtung dann hat, wenn sie *nicht* zur Umgehung wirksamer technischer Schutzmaßnahmen eingesetzt wird, muss also begrenzt sein. Mit anderen Worten darf der legale Einsatz der Vorrichtung dem Verwender keine *wirtschaftlich unbegrenzten* Vorteile einbringen.

---

211 Ähnlich *Arlt*, in: Hoeren/Sieber, Teil 7.7 Rn. 67.

212 *Arnold*, MMR 2008, 148.

Nimmt man den Wortlaut genau, so ist also eine Vorrichtung, die sich zur Umgehung von technischen Schutzmaßnahmen einsetzen lässt, nur dann nicht tatbestandsmäßig, wenn es sich dabei um einen legal einsetzbaren „Goldesel" handelt. Oder anders gewendet: Ein legal einsetzbarer „Goldesel" darf auch dann noch hergestellt, eingeführt, verbreitet, verkauft und vermietet werden, wenn er unter anderem auch wirksame technische Schutzmaßnahmen umgeht. Der Gesetzgeber hält sich hier an den Wortlaut des Art. 6 Abs. 2 b) der Richtlinie 2001/29/EG und übernimmt damit die unfreiwillig komische Formulierung des Europäischen Parlaments und des Rates. Bei strenger, humorloser Bindung an den Wortlaut ist die Folge dieses Tatbestandsmerkmals, dass es schlicht seine Ausgrenzungsfunktion verliert. *Jede* Vorrichtung ist erfasst, wenn sie dem Verwender *irgend*einen wirtschaftlichen Nutzen durch die Umgehung wirksamer technischer Schutzmaßnahmen bringt.

In der Literatur wird dieses Kriterium eines begrenzten oder unbegrenzten wirtschaftlichen Nutzens entweder von vornherein nicht wörtlich genommen oder allgemein als unbillig angesehen, weshalb einige Autoren eigene Kriterien entwickelt haben. Da diese Kriterien gegenüber dem „Unbegrenztheits-Kriterium" des geltenden § 95a Abs. 3 Nr. 2 UrhG eine Einschränkung bedeuten, sind sie täterbegünstigend und verstoßen deshalb nicht gegen Art. 103 Abs. 2 GG.

Vielfach wird die Tatbestandsformulierung als Relation interpretiert: Der legale wirtschaftliche Nutzen soll im Verhältnis zum illegalen Nutzen nicht begrenzt, sondern vernachlässigbar oder unerheblich sein – nur dann ist eine Vorrichtung tatbestandsmäßig.[213] Denn selbst ein Betriebssystem wie Windows hat keinen unbegrenzten wirtschaftlichen Nutzen.[214] Es bietet aber eine solche Fülle von (legalen) Funktionen, dass eine möglicherweise illegal nutzbare Funktion[215] ohne Weiteres aufgewogen wird. Die Frage ist nur, wie stark die legale Funktion die illegale Funktion überwiegen muss, damit die Vorrichtung vom Tatbestand ausgenommen

---

[213] So auch *Hänel*, Umsetzung des Art. 6, S. 164; ähnlich Dreier/Schulze-*Dreier*, § 95a Rn. 18, der dort aber Nr. 2 und 3 des § 95a Abs. 3 UrhG gleichsetzt und eine allgemeine Abwägung fordert, ohne jedoch Abwägungskriterien und Abwägungsmaßstab zu konkretisieren. Vgl. außerdem *Gercke*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 532, der im Folgenden jedoch allgemeine Schwerpunktbetrachtungen vorschlägt und auf eine Abwägung wirtschaftlicher Nutzen verzichtet. Ebenso wohl Spindler/Schuster-*Spindler*, UrhG § 95a Rn. 14 ff.

[214] So aber *Schippan*, ZUM 2006, 855, der sagt, Windows habe „ganz offensichtlich nicht nur einen ‚begrenzten wirtschaftlichen Zweck oder Nutzen'."

[215] Laut *Stickelbrock* ließ sich – zumindest im Jahre 2003 – ein Kopierschutz bei bestimmten Musik-CDs umgehen, indem man die Autorun-Funktion in Windows deaktivierte, *Stickelbrock,* GRUR 2004, 739, mit Verweis auf *Minhardt*, Spiegel-Online vom 22.10.2003, abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,270719,00.html [zuletzt abgerufen am 16.11.2014]. In diesem Beispiel ist aber schon zweifelhaft, worin Erzeugnis, Bestandteil oder Vorrichtung i.S.d. § 95a Abs. 3 UrhG gesehen werden soll. Da die Autorun-Funktion hier Voraussetzung des Kopierschutzes war, müsste man argumentieren, dass es ein krimineller Bestandteil von Windows ist, dass man die Autorun-Funktion abschalten kann. *Stickelbrock*, a.a.O., S. 739, zweifelt an der Wirksamkeit der technischen Schutzmaßnahme.

wird. *Wandtke/Ohst* halten eine Vorrichtung für nicht tatbestandsmäßig, wenn diese nach Entfernen der Umgehungskomponente überhaupt noch einen anderen wirtschaftlichen Nutzen hat.[216] *Entelmann* fordert weitergehend, dass die Vorrichtung (nach Abwägung im Einzelfall) einen *genügenden* sonstigen wirtschaftlichen Nutzen aufweist.[217] *Götting* stellt darauf ab, welcher (wirtschaftliche) Zweck *im Vordergrund* steht.[218] Nach *Dreyer* muss der wirtschaftliche Gesamtnutzen der Vorrichtung *ganz überwiegend* aus ihrer deliktischen Verwendbarkeit resultieren,[219] und auch *Stickelbrock* vertritt, dass es jedenfalls nicht ausreiche, wenn die Vorrichtung neben illegalen Funktionen „noch wesentlich mehr kann".[220] Andernorts wird vertreten, dass jede Vorrichtung mit illegaler Funktion erfasst ist, sofern sie ansonsten einen wirtschaftlich geringen Eigenwert hat.[221] Hiermit ist vermutlich gemeint, dass der wirtschaftliche Nutzen der Vorrichtung maßgeblich aus ihrer deliktischen Einsetzbarkeit resultieren muss. Es ist nämlich nicht nachvollziehbar, welche Erkenntnis aus dem *Wert* der Vorrichtung – selbst wenn man eine konsensfähige Methode zu dessen Ermittlung fände – für die vorliegende Frage zu gewinnen wäre. *Arnold* setzt den wirtschaftlichen Nutzen durch den rechtswidrigen Einsatz ins Verhältnis zu den Anschaffungskosten der Umgehungsvorrichtung und bejaht die Tatbestandsmäßigkeit der Vorrichtung umso eher, je stärker der wirtschaftliche Nutzen die Anschaffungskosten überwiegt.[222] Dies hat der Gesetzgeber aber wohl nicht gemeint. Der Wortlaut legt eher einen Vergleich zwischen rechtswidrigem und rechtmäßigem Nutzen nahe, sodass allenfalls der wirtschaftliche Nutzen bei rechtswidrigem Einsatz mit den Anschaffungskosten zu saldieren ist und dies dann ins Verhältnis zum Saldo aus Anschaffungskosten und wirtschaftlichem Nutzen bei rechtmäßigem Einsatz zu setzen ist.

Da es in jedem Einzelfall äußerst schwierig sein dürfte, jeweils den wirtschaftlichen Nutzen bei rechtmäßigem bzw. rechtswidrigem Einsatz genau zu beziffern, bestehen pragmatische Bedenken gegen alle Ansätze, die diese beiden Zahlenwerte gegeneinander abwägen wollen. Pragmatischer erscheint es, alle Vorrichtungen zu erfassen, die bei kriminellem Einsatz überhaupt einen wirtschaftlich erheblichen Nutzen bringen. Dass sie auch bei rechtmäßigem Einsatz einen wirtschaftlichen Nutzen haben, soll dem dann nicht entgegenstehen. Es ist nicht ausgeschlossen, dass der Gesetzgeber genau dies ausdrücken wollte, weshalb sich dieses Ergebnis in teleologischer Auslegung auch vertreten lässt.

---

216 Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 84; wohl auch *Ernst*, CR 2004, 41.

217 *Entelmann*, Verbot von Vorbereitungshandlungen, S. 69;

218 Schricker/Loewenheim-*Götting*, § 95a Rn. 35.

219 So wohl Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 99.

220 *Stickelbrock*, GRUR 2004, 739.

221 *Arlt*, DRM-Systeme, S. 83; *Spindler*, GRUR 2002, 116.

222 *Arnold*, MMR 2008, 148.

Die Beurteilung einer Vorrichtung nach wirtschaftlichen Maßstäben wird wie bei den Varianten des § 95a Abs. 3 Nr. 2 und 3 grundsätzlich objektiviert aus Sicht des verständigen Durchschnittsnutzers vorgenommen.[223] Der Tatrichter kann dessen Perspektive in eigener Wertung einnehmen, kann jedoch auch Verbraucherumfragen als Indiz berücksichtigen.[224]

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Mit Blick auf die Dual-Use-Problematik wird in diesem „ökonomischen Modell" nun ein ganz anderer Ansatz gewählt: Es sollen nicht mehr einzelne Funktionen des Computerprogramms bewertet werden, sondern es wird das gesamte Computerprogramm als Wirtschaftsgut betrachtet. Dies erscheint für den Multifunktionsaspekt der Dual-Use-Problematik sachgerecht: Ein Programm mit legitimen und schädlichen Funktionen wird danach beurteilt, was seinen wirtschaftlichen Wert konstituiert. Damit trägt auch der oben stets angeführte Kritikpunkt, dass nicht auf die kriminelle Eignung eines Computerprogramms abgestellt werde,[225] hier nicht mehr. Denn einen kriminellen wirtschaftlichen Nutzen kann ein Computerprogramm nur dann haben, wenn es überhaupt kriminell einsetzbar ist. Problematisch ist hier allerdings, dass der Hersteller das Risiko trägt, dass sich eine Vorrichtung, die er ursprünglich nur für den legalen Einsatz entworfen hat, als geeignetes Umgehungsmittel herausstellt und vielfach hierfür angeschafft wird. Denn ab diesem Zeitpunkt ist auch das weitere Herstellen der Vorrichtung strafbewehrt. [226]

Für den Mehrzweckaspekt der Dual-Use-Problematik ergibt sich indes keine Änderung: IT-Sicherheitsbeauftragte benötigen regelmäßig Schadsoftware zur Simulation von Angriffen. Realistischerweise fallen darunter insbesondere solche Programme, deren wirtschaftlicher Nutzen gerade in der rechtswidrigen Verwendung liegt. Denn eben diese Programme dürften von potentiellen Angreifern genutzt werden. Es ist deshalb davon auszugehen, dass IT-Sicherheitsbeauftragte regelmäßig mit Computerprogrammen Umgang haben, die nach diesem Regelungsmodell taugliche Tatobjekte sind. Verwendet man also diese Regelungstechnik zur Umschreibung des Tatobjekts, so muss man sicherstellen, dass eine Strafbarkeit von IT-Sicherheitsbeauftragten an anderer Stelle scheitert. Denkbar sind hier etwa besondere Vorsatzerfordernisse eines Vorfeldtäters. Im vorliegenden Fall des § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 2 UrhG wurden solche Sicherungen

---

[223] Vgl. OLG Frankfurt a.M. GRUR-RR 2003, 287, OLG Hamburg GRUR-RR 2010, 156; Fromm/Nordemann-*Czychowski*, § 95a Rn. 46; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 134; *Gercke*, in: Gerke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 532; *Meschede*, Schutz digitaler Musik- und Filmwerke, S. 166; *Pleister/Ruttig*, MMR 2003, 764; *Spindler/Leistner*, GRUR-Int 2005, 793.

[224] Vgl. Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 99.

[225] Siehe oben 2.b); 3.b); 4.b).

[226] So auch *Trayer*, Technische Schutzmaßnahmen, S. 116.

nicht normiert, weshalb sich IT-Sicherheitsbeauftragte de lege lata regelmäßig nach diesem Tatbestand strafbar machen. Zur Ausschlussklausel des § 95a Abs. 4 UrhG und deren Geltung im Rahmen des § 108b Abs. 2 UrhG gilt das oben Gesagte.[227]

6. „Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel [einer Zieltat]"

In einem sechsten Modell wird erneut der Fokus verschoben. Hier spielt es keine Rolle mehr, wozu das Computerprogramm eingesetzt werden soll oder welchen Nutzen sein Einsatz bringt. Maßgeblich ist hier, wie es vermarktet wird. Damit rückt anstelle des Herstellers und Users nun der Werbetreibende in den Blick. Man kann deshalb von einem „Marketing-Modell" sprechen. Dieses Modell liegt dem § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 1 UrhG zugrunde. § 95a Abs. 3 Nr. 1 UrhG lautet:

> **§ 95a Schutz technischer Maßnahmen**
>
> (3) Verboten sind die Herstellung, die Einfuhr, die Verbreitung, der Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und der gewerblichen Zwecken dienende Besitz von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen, die
>
> 1. Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind
>
> […]

§ 108b Abs. 2 UrhG besagt:

> **§ 108b Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen**
>
> (1) Wer […], [wird] mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
>
> (2) Ebenso wird bestraft, wer entgegen § 95a Abs. 3 eine Vorrichtung, ein Erzeugnis oder einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet.

Einige Autoren sind der Ansicht, § 95a Abs. 3 Nr. 1 UrhG beziehe sich insgesamt nicht auf Vorrichtungen, Erzeugnisse und Bestandteile, sondern ausschließlich auf „Dienstleistungen aus dem Bereich der kommerziellen Kommunikation", weshalb diese Tatbestandsvariante im Zusammenhang mit § 108b Abs. 2 UrhG eine untergeordnete Rolle spiele.[228] Für diese Annahme gibt es jedoch keinen Grund. Der Wortlaut spricht unzweideutig aus, dass neben dem Erbringen von

---

[227] Siehe oben 4.b).

[228] So explizit *Gercke*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 531; zumindest missverständlich *Dreier*, in Dreier/Schulze, § 95a Rn. 17, der zunächst nur von Vorrichtungen, Erzeugnissen und Bestandteilen spricht, ohne die Tatbestandsmerkmale der Nr. 1–3 hierauf zu beziehen, sodann die Merkmale der Nr. 1–3 nur auf die Erbringung von Dienstleistungen anwendet, um sich schließlich in Rn. 18 doch auch zum „wirtschaftlichen Zweck oder Nutzen" (Nr. 2) von *Umgehungswerkzeugen* einzulassen.

Dienstleistungen, welche der Nr. 1 entsprechen, auch ein bestimmter Umgang mit Vorrichtungen, Erzeugnissen und Bestandteilen, welche der Nr. 1 entsprechen, verboten ist („sowie"). Auch in der Gesetzesbegründung kommt an keiner Stelle eine Intention des Gesetzgebers zur Sprache, § 95a Abs. 2 Nr. 1 UrhG auf Dienstleistungen zu beschränken. Daneben besteht auch in systematischer Auslegung kein Anlass, bei Nr. 1 andere Bezüge herzustellen als bei Nr. 2 und Nr. 3 des § 95a Abs. 3 UrhG. Auch diese Nummern beziehen sich auf Vorrichtungen *und* Dienstleistungen, was in Nr. 3 explizit daran zu erkennen ist, dass neben den für Dienstleistungen unpassenderen Attributen „entworfen, hergestellt oder angepasst" auch das Attribut „erbracht werden" eingefügt ist.

Von alledem abgesehen ist teleologisch ohnehin das Gegenteil von obiger Ansicht richtig: Gerade die ungehemmte Verbreitung von Umgehungsmitteln (Vorrichtungen, Erzeugnissen, Bestandteilen) birgt die größere Gefahr für die (faktische) Wirksamkeit technischer Schutzmaßnahmen. Dies kommt nicht nur in der Gesetzesbegründung zum Ausdruck,[229] sondern auch darin, dass die Strafnorm des § 108b Abs. 2 UrhG nur auf Vorrichtungen, Erzeugnisse und Bestandteile abzielt, während das Erbringen entsprechender Dienstleistungen lediglich als Ordnungswidrigkeit in § 111a Abs. 1 Nr. 1 b) UrhG ausgestaltet ist. Die Ansicht, wonach sich § 95a Abs. 3 Nr. 1 UrhG nur auf Dienstleistungen, nicht aber auf Vorrichtungen, Erzeugnisse und Bestandteile bezieht, ist also zu verwerfen.[230]

a) Charakteristika dieses Regelungsmodells

Erfasst ist eine Vorrichtung, die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung (aa)) ist, welche das Ziel der Umgehung wirksamer technischer Schutzmaßnahmen (bb)) verfolgt. Im Kern geht es hier um Vorrichtungen, die als Umgehungsvorrichtungen vermarktet werden. Sie sollen taugliche Tatobjekte des Vorfelddelikts sein. In § 95a Abs. 3 Nr. 1 UrhG wird also nicht das Vermarkten der Vorrichtung selbst verboten, vielmehr ist das Vermarktet-Werden der Vorrichtung die Voraussetzung für das Verbot des Umgangs mit der Vorrichtung.[231] Freilich enthält § 95a Abs. 3 UrhG a.A. auch ein Verbot der Werbung für eine Vorrichtung

---

[229] BT-Drucks. 15/38, S. 28 rechte Spalte.

[230] Auch *Gercke* liefert a.a.O. letztlich gar kein Argument für seinen Standpunkt, sondern verweist lediglich auf Schricker/Loewenheim-*Götting*, § 95a Rn. 34, der dort etwas kryptisch formuliert, „die verbotenen Handlungen müssen Gegenstand einer Verkaufsförderung […] sein", und in der von *Gercke* zitierten 3. Aufl. 2006 steht zusätzlich, dass entscheidend sei, „ob die Absatzförderung […] auf die Vermarktung […] gerichtet" sei. Richtig ist aber, dass die Vorrichtungen Gegenstand einer Verkaufsförderung sein müssen, also der Absatz der Vorrichtungen gefördert werden soll. Siehe dazu sogleich.

[231] Insofern missverständlich LG München I MMR 2008, 194 und OLG München ZUM 2005, 900.

im Sinne der Nrn. 1–3.[232] Der funktionale Unterschied liegt aber darin, dass im ersten Halbsatz des Abs. 3 die Verbots*handlung* umschrieben ist, während Abs. 3 Nr. 1 den Verbots*gegenstand* umschreibt.[233] Dies soll nachfolgend im Einzelnen dargelegt werden.

aa) „Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung"

Die Vorrichtungen müssen Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung sein. Diese Begriffe werden weder in der zugrunde liegenden Richtlinie 2001/29/EG noch in den Gesetzesmaterialien zu § 95a UrhG näher erläutert. Allen Varianten ist jedoch gemein, dass sie auf die Absatzförderung des Produkts gerichtet sind. Teilweise wird angenommen, dass Werbung sich auf Äußerungen beschränke, während Vermarktung und Verkaufsförderung grundsätzlich alle Maßnahmen zur Absatzförderung umfassten.[234] Schon daran wird jedoch deutlich, dass die Varianten jedenfalls nicht trennscharf voneinander abzugrenzen sind. Deshalb ist wohl jede Form der Absatzförderung erfasst.[235] Eine Begrenzung auf kommerzielle *Kommunikation* ist dabei nicht zwingend,[236] da etwa der Begriff der Verkaufsförderung schon im Wortsinn gerade nicht auf Kommunikation beschränkt ist. Unerheblich sind grundsätzlich auch die Intensität, Häufigkeit oder Professionalität der einzelnen Marketingmaßnahme. Als Beispiele für verkaufsfördernde Maßnahmen werden Verkaufsveranstaltungen, Verpackung und Gestaltung des Produkts[237] sowie der Internetauftritt des Herstellers[238] genannt. Tatsächlich dürften alle Instrumente des betriebswirtschaftlichen Marketing-Mix darunter fallen, also insbesondere Produktpolitik, Kommunikationspolitik, Distributionspolitik und Kontrahierungspolitik (Preis-, Lieferkonditionen- und Absatzfinanzierungspolitik).[239]

---

232 Dieses Verbot ist aber nicht von der Strafnorm des § 108b Abs. 2 UrhG umfasst, sondern lediglich um die Ordnungswidrigkeitsnorm des § 111a Abs. 1 Nr. 1 b) UrhG erweitert.

233 Dies führt freilich dazu, dass es gemäß § 95a Abs. 3 Nr. 1 UrhG auch verboten ist, für eine Vorrichtung zu werben, die als Umgehungsvorrichtung beworben wird.

234 Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 88–90.

235 So auch OLG Hamburg GRUR-RR 2010, 155 („Vermarktung").

236 So aber *Hänel*, Umsetzung des Art. 6, S. 163; *Wand*, Technische Schutzmaßnahmen, S. 111.

237 Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 88; *Spindler/Leistner*, GRUR-Int 2005, 793.

238 LG München I MMR 2005, 385, bestätigt durch OLG München ZUM 2005, 898, nicht beanstandet durch BGH MMR 2011, 391 ff.; ebenso LG München I MMR 2008, 194, OLG München MMR 2009, 120.

239 Vgl. *Kirchgeorg*, in: Gabler Wirtschaftslexikon, „Marketingpolitische Instrumente", online abrufbar unter http://wirtschaftslexikon.gabler.de/Archiv/1493/marketingpolitische-instrumente-v6.html [zuletzt abgerufen am 16.11.2014].

Ungeklärt ist, ob die Verkaufsförderung, Werbung oder Vermarktung im Sinne des § 95a Abs. 3 Nr. 3 UrhG anders interpretiert werden muss als die „Werbung im Hinblick auf Verkauf oder Vermietung" aus § 95a Abs. 3 UrhG a.A. In diesem Zusammenhang ist vor allem umstritten, ob das Anpreisen einer Vorrichtung durch *Verbraucher* auch als Werbung in dem einen oder anderen Sinne angesehen werden kann. Mit Blick auf die Dual-Use-Problematik ist dies besonders relevant.[240]

Eine Definition der *Werbung* findet sich in Art. 2 Nr. 1 der Europäischen Irreführungsrichtlinie 84/450/EWG. Erfasst ist dort jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen zu fördern. Für die „Werbung im Hinblick auf Verkauf oder Vermietung" im Sinne des § 95a Abs. 3 UrhG a.A. hat der BGH entschieden, dass die Definition aus der Irreführungsrichtlinie zwar anwendbar, aber jedenfalls dahingehend zu weiten ist, dass auch das nichtgewerbliche, ggf. auch einmalige Handeln Privater grundsätzlich erfasst wird.[241] Ob diese Auslegung auch auf den Begriff der „Verkaufsförderung, Werbung oder Vermarktung" des § 95a Abs. 3 Nr. 1 UrhG anzuwenden ist, wird bezweifelt. Jedenfalls aber müsste diese Begriffsgruppe in ihrer Gesamtheit weiter reichen als der bloße Werbebegriff, da anderenfalls die Aufnahme der Verkaufsförderung und Vermarktung in den Tatbestand redundant wäre.

Fraglich ist auch, worin der maßgebliche Strafgrund des Abs. 3 Nr. 1 zu sehen ist. Zum Teil wird hier auf die Streuwirkung der Werbung abgestellt. Argumentiert man in dieser Weise, so müsste man jedenfalls den einmaligen Verkauf einer Umgehungsvorrichtung bei *einmaliger* Bewerbung als Umgehungsvorrichtung von der Strafbarkeit ausnehmen, da hier ersichtlich keine Streuwirkung vorliegt.[242] Tatsächlich aber ist die Streuwirkung wohl eher der Grund für das (ordnungsrechtliche) Verbot der Bewerbung einer Vorrichtung als Umgehungsvorrichtung, nicht aber für das (strafrechtliche) Verbot des Umgangs mit entsprechend beworbenen Vorrichtungen. Der Strafgrund für das Verbot von Verkauf, Herstellung etc. kriminell beworbener Vorrichtungen liegt wohl vielmehr darin, dass der Vorfeldtäter in den vorliegenden Tatvarianten des Herstellens, Einführens, Verbreitens, Verkaufens und Vermietens davon ausgehen muss, dass die kriminell beworbene Vorrichtung später tatsächlich zu kriminellen Zwecken eingesetzt wird und er zu diesem Einsatz einen kausalen Unterstützungsbeitrag leistet. Für diese Frage ist es dann lediglich von Belang, ob der Vorfeldtäter Kenntnis von der Vermarktung der Vorrichtung als

---

240 Dazu ausführlich sogleich unter b).

241 BGH NJW 2008, 3566 f.; vgl. auch schon die Vorinstanz LG Köln MMR 2006, 416.

242 So Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 89.

Umgehungsmittel hat, und damit kann auch ein einmaliger Verkauf einer einmalig kriminell beworbenen Vorrichtung dem Tatbestand unterfallen.[243]

Redaktionelle Berichterstattung von Online-Medien ist grundsätzlich keine Werbung, solange sie eine kritische Distanz erkennen lässt. Dies gilt auch dann, wenn die Online-Berichterstattung durch Hyperlinks direkt auf illegale Inhalte verweist.[244] Auch wissenschaftliche Veröffentlichungen stellen keine Werbung dar.[245] Damit unterfallen auch Vorrichtungen, über deren kriminelle Einsatzmöglichkeit redaktionell berichtet wird, nicht dem Tatbestand des § 95a Abs. 3 Nr. 1 UrhG.

bb) „Mit dem Ziel der Umgehung wirksamer technischer Schutzmaßnahmen"

Nach dem Wortlaut müsste eigentlich die Verkaufsförderung, Werbung oder Vermarktung zum Ziel haben, dass wirksame technische Maßnahmen umgangen werden.[246] Dies ist jedoch allem Anschein nach nicht gemeint, denn das Ziel einer Verkaufsförderung, Werbung oder Vermarktung liegt – wie der Name bereits sagt – in der Regel darin, dass der Verkauf gefördert oder der Absatz gesteigert wird. Dem Hersteller, Verkäufer oder Werbetreibenden wird es kaum darauf ankommen, wozu der Erwerber die Vorrichtung tatsächlich einsetzt.

Gemeint ist hier vielmehr, dass die Umgehung technischer Schutzmaßnahmen den *Gegenstand* oder *Inhalt* der Verkaufsförderung ausmachen muss. Mit einfachen Worten: Die Vorrichtung muss als Umgehungsmittel vermarktet oder beworben werden.[247] Dies wird anhand der Werbeaussagen nach objektiven Kriterien aus Sicht des Durchschnittsadressaten bewertet.[248] Ebenso relevant wie die Werbeaussage selbst sind das Werbeforum und der Kreis der Adressaten: Wird kriminell einsetzbare Analyse-Software oder zu Analysezwecken einsetzbare Schadsoftware in einer Zeitschrift für IT-Sicherheit beworben, so spricht dies eher gegen die Tatbestandsmäßigkeit solcher Software, da das Werbeforum und der Empfängerkreis dafür sprechen, dass das Computerprogramm mit dem Ziel der Verbesserung der IT-Sicherheit beworben wird. Wird die Software in einer Publikumszeitschrift be-

---

[243] Vgl. BGH NJW 2008, 3567.

[244] BGH MMR 2011, 392; siehe auch die Zusammenfassung bei *Schippan*, ZUM 2006, 857.

[245] Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 91.

[246] So tatsächlich Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 83; wohl auch Schricker/Loewenheim-*Götting*, § 95a Rn. 34, der diesbezüglich einerseits sogar Absicht des Werbetreibenden fordert, andererseits ausreichen lässt, wenn die Werbung auf die Umgehung „abzielt", ebenso *Hänel*, Umsetzung des Art. 6, S. 163.

[247] LG Köln MMR 2006, 412; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 68; *Spindler/Leistner*, GRUR-Int 2005, 793; *Trayer*, Technische Schutzmaßnahmen, S. 115, 132.

[248] *Arnold*, Umgehungsmittel nach Urheberrecht und Wettbewerbsrecht, S. 111.

worben, so liegt es näher, sie als Umgehungsmittel einzustufen,[249] zumindest dann, wenn es sich – wie bei der Umgehung technischer Schutzmaßnahmen – nicht um technisch anspruchsvollste Hacking-Straftaten, sondern vielmehr um einfache Massenkriminalität handelt.

Ausreichen soll es außerdem, wenn der Software-Hersteller auf seiner Homepage eine Blickfangwerbung mit dem Slogan „… knackt fast jeden DVD-Kopierschutz" placiert.[250] Distanzierungserklärungen, in denen der Werbetreibende darauf hinweist, dass das beworbene Produkt nur zu rechtmäßigen Zwecken eingesetzt werden solle, können auch einen entgegengesetzten Effekt haben: Wenn dies aus Sicht des Verkehrs eher eine süffisante Scheindistanzierung darstellt, die in Wirklichkeit erst auf die rechtswidrige Verwendbarkeit hinweisen soll, so ist die Distanzierungserklärung zumindest unwirksam,[251] kann aber ebenso als Werbung mit dem Ziel der Umgehung technischer Schutzmaßnahmen anzusehen sein.[252]

Der Vorfeldtäter des § 108b Abs. 2 UrhG muss nicht zwingend identisch sein mit dem Werbetreibenden des § 95a Abs. 3 Nr. 1 UrhG. Freilich muss der Vorfeldtäter zumindest mit dolus eventualis annehmen, dass die einschlägige Vorrichtung als Umgehungsvorrichtung beworben wird, also ihre kriminelle Einsetzbarkeit besonders hervorgehoben wird.[253]

Umstritten ist, ob die als Umgehungsmittel beworbene Vorrichtung auch tatsächlich zur Umgehung technischer Schutzmaßnahmen imstande sein muss. Dies wird zum einen mit dem Argument bejaht, dass es nicht im Schutzbereich der Norm liege, den Umgang mit ungeeigneten Vorrichtungen zu verbieten, die nur *fälschlicherweise* als Umgehungsmittel beworben werden.[254] In diesem Fall sei die technische Schutzmaßnahme gerade nicht gefährdet, bedürfe also auch keines rechtlichen Schutzes.[255] Aus dem Wortlaut geht dies jedoch nicht zwingend hervor, sodass auch vertreten wird, es sei unerheblich, welche Eigenschaften die Vorrichtung hat – entscheidend sei allein die Zielsetzung der Werbung.[256]

Trotz aller offenen Fragen finden sich auch zu diesem Modell vielfach nur kursorische Ausführungen in der Literatur, in denen die Autoren – wie auch in Nr. 2 und Nr. 3 des § 95a Abs. 3 UrhG – lediglich eine Gesamtabwägung nach abstrakteren Kriterien wie der allgemeinen Lebenserfahrung oder dem Gesamteindruck im Ein-

---

249 *Arnold*, MMR 2008, 147.

250 OLG München ZUM 2005, 898.

251 OLG Frankfurt a.M. GRUR-RR 2003, 287.

252 *Arnold*, MMR 2008, 147.

253 Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 91; *Trayer*, Technische Schutzmaßnahmen, S. 115, 132. Zum subjektiven Tatbestand der Vorfelddelikte siehe auch sogleich I.C.

254 Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 83.

255 *Entelmann*, Verbot von Vorbereitungshandlungen, S. 68.

256 LG München I MMR 2008, 194; *Arnold*, Umgehungsmittel nach Urheberrecht und Wettbewerbsrecht, S. 29; Schricker/Loewenheim-*Götting*, § 95a Rn. 34.

zelfall vornehmen, um zu entscheiden, ob eine Vorrichtung tatbestandsmäßig ist.[257] *Wand* abstrahiert Abs. 3 Nr. 1 zu „kommerzieller Kommunikation mit dem Ziel der Umgehung" ohne nähere Ausführung, worauf es dann ankommen soll.[258] *Wandtke/Ohst* äußern sich ausschließlich zur Vermarktung, welche unter anderem die „Werbung bis zum Verkauf" einschließe, verweisen dann aber auf Rechtsprechung zur Werbung gemäß § 95a Abs. 3 UrhG a.A., nicht aber zu „Verkaufsförderung, Werbung und Vermarktung" nach § 95a Abs. 3 Nr. 1 UrhG.[259] *Spindler* macht nur allgemeine Ausführungen zu Werbung („Ankündigung und Anpreisung mit dem Ziel der Absatzförderung") und bezieht dies offenbar sowohl auf § 95a Abs. 3 UrhG a.A. als auch auf Abs. 3 Nr. 1, da er im Anschluss nur noch Nr. 2 und Nr. 3 erläutert.[260] *Arlt* interpretiert den zugrunde liegenden Art. 6 Abs. 2 a) der Richtlinie 2001/29/EG sogar dahingehend, dass die Vorrichtungen dem Ziel der Umgehung dienen müssten,[261] und löst sich damit vollends vom Wortlaut.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Auch dieses Regelungsmodell[262] setzt am Multifunktionsaspekt der Dual-Use-Problematik an. Computerprogramme mit mehreren Funktionen, von denen mindestens eine auch zur Begehung von Straftaten eingesetzt werden kann, sollen dann tatbestandsmäßig sein, wenn diese „kriminelle Funktion" des Programms beworben wird. Unter diesem Multifunktionsaspekt der Dual-Use-Problematik soll regelmäßig ausgeschlossen werden, dass ein Computerprogramm dem Tatbestand unterfällt, dessen krimineller Einsatz sich als Missbrauch des Programms darstellt.

Als Beurteilungskriterium, wann ein solcher Missbrauch vorliegt, wird also im vorliegenden Regelungsmodell herangezogen, zu welchem Gebrauch das Computerprogramm beworben wird. Damit hat zunächst der Hersteller die Deutungs- und Entscheidungshoheit über die Tatbestandsmäßigkeit des Computerprogramms, denn er dürfte regelmäßig entscheiden, wie das Programm beworben wird.

Diese Deutungshoheit kann der Hersteller aber im Lauf der Zeit auch verlieren. Denn in diesem Regelungsmodell ist nicht festgelegt, *von wem* das Produkt als Umgehungsmittel beworben werden muss, damit es dem Tatbestand unterfällt.[263]

---

[257] Fromm/Nordemann-*Czychowski*, § 95a Rn. 46; Dreier/Schulze-*Dreier*, § 95a Rn. 17 f.; *Gutmann*, K&R 2003, 493; *Pleister/Ruttig*, MMR 2003, 764.

[258] *Wand*, Technische Schutzmaßnahmen, S. 111.

[259] Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 83.

[260] Spindler/Schuster-*Spindler*, UrhG § 95a Rn. 13.

[261] *Arlt*, DRM-Systeme, S. 83.

[262] Auf die Ausschlussklausel des § 95a Abs. 4 UrhG soll hier nicht mehr eingegangen werden. Zu ihrer Geltung im Rahmen des § 108b Abs. 2 UrhG gilt das oben Gesagte, siehe I.B.4. b).

[263] Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 93; *Entelmann*, Verbot von Vorbereitungshandlungen, S. 68; *Trayer*, Technische Schutzmaßnahmen, S. 116.

Infolgedessen kann auch ein Computerprogramm, welches von seinem Hersteller mit guten Intentionen entworfen, auf den Markt gebracht und beworben wird, tatbestandsmäßig werden, wenn Dritte die illegalen Einsatzmöglichkeiten des Programms bewerben. Dies ist insbesondere dann bedeutsam, wenn man annimmt, dass der Begriff der „Verkaufsförderung, Werbung oder Vermarktung" nicht grundsätzlich ein unternehmerisches Handeln voraussetzt, sondern auch Privatpersonen und Verbraucher in diesem Sinne handeln können. Dann kommen hierfür nämlich insbesondere Blogger, Forenbetreiber und Forennutzer in Betracht.

Ein Computerprogramm kann dann allein dadurch den Tatbestand des § 95a Abs. 3 Nr. 1 UrhG erfüllen, dass es in einschlägigen Foren als Umgehungstool angepriesen wird. Dies liegt teleologisch auch nahe, denn wenn es als Umgehungstool beworben wird, macht es für den Unrechtsgehalt und das Gefährdungspotential für das Rechtsgut keinen Unterschied, *von wem* die entsprechende Marketingmaßnahme getroffen wird. Dies hat allerdings zur Konsequenz, dass ein Hersteller, der um solche Anpreisungen in Blogs und Foren weiß, sich gemäß § 108b Abs. 2 UrhG strafbar macht, wenn er die Software weiter herstellt.[264] Dies wird mit dem Argument gerechtfertigt, dass dem Hersteller schon im Voraus klar sein muss, wozu sein Programm geeignet ist, und er deshalb das Risiko kennt.[265]

Diese Argumentation macht freilich kenntlich, dass das Regelungsmodell den Mehrzweckaspekt der Dual-Use-Problematik nicht berücksichtigt: Es kann legitime Interessen geben, mit solchen Computerprogrammen umzugehen, und im Moment des Umgangs mit einem solchen Programm spielt die *Intention* des Handelnden eine maßgebliche Rolle. Dies gilt insbesondere für IT-Sicherheitsunternehmen, die sich auf Angriffe mittels dieses Programms vorbereiten müssen und deshalb gerade solche Computerprogramme benötigen, die in einschlägigen Kreisen als Umgehungsmittel beworben werden. Aber wie gesehen kann es auch für den Hersteller solcher Software ein legitimes Interesse an der Fortführung seiner Tätigkeit geben, wenn er etwa den großen Teil seiner Kundschaft bedienen will, der das Computerprogramm legitim einsetzt. Es erschiene unverhältnismäßig, hier das Strafrechtsschwert gegen den Programmhersteller einzusetzen, allein weil eine – möglicherweise sehr kleine – Gruppe Krimineller das Schadenspotential der Software in einschlägigen Kreisen bewirbt.

Dies ist dann wenig problematisch, wenn die hier erörterte objektive Regelungstechnik um ein subjektives Kriterium ergänzt wird, das etwa einem rechtschaffenen Programmhersteller einen Ausweg aus der Strafbarkeit ermöglicht. Die Vorfelddelikte des § 108b Abs. 2 i.V.m. § 95a Abs. 3 UrhG kranken allerdings daran, dass sie diesen Mehrzweckaspekt der Dual-Use-Problematik nicht berücksichtigen, son-

---

[264] So auch *Spindler/Leistner*, GRUR-Int 2005, 793; *Trayer*, Technische Schutzmaßnahmen, S. 116.

[265] Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 93.

dern das Tatobjekt als einziges Kriterium zur Abgrenzung legitimen Handelns von kriminellem Handeln dient. Im Folgekapitel wird diese subjektive Seite der Vorfelddelikte eingehend analysiert.

C. Die subjektive Tatseite der Software-Delikte

Wie gezeigt handelt es sich bei allen Software-Delikten um Delikte im Vorfeld eigentlicher Rechtsgutsverletzungen. Deshalb besteht in jedem dieser Vorfelddelikte ein gewisser subjektiver, intentionaler Bezug des Täters zum Zieldelikt. Dieser Bezug kann sich in einem separaten Tatbestandsmerkmal niederschlagen, etwa wenn besonderes Wissen oder Wollen des Vorfeldtäters hinsichtlich der Ausführung oder des Erfolgs eines Zieldelikts vertatbestandlicht wird. Ein subjektiver Bezug kann sich jedoch auch aus den Besonderheiten des Tatobjekts ergeben, etwa wenn dem Tatobjekt eine gewisse Bestimmung gegeben worden ist oder besondere Zwecke mit dem Tatobjekt ursprünglich verfolgt worden sind oder werden.[266] Es handelt sich dann freilich um eine andere Form eines intentionalen Bezugs, der sich aus dem bewussten Umgang mit einem „zweckgebundenen Gegenstand" ergibt.

Die Art des subjektiven Bezugs ergibt sich aus den rechtstechnischen Entscheidungen des Gesetzgebers. Denn bei der Frage, wie er den subjektiven Tatbestand der Software-Delikte regelt, legt er zugleich deren Deliktsstruktur fest. Bei einigen Vorfelddelikten hat der Gesetzgeber den intentionalen Bezug des Vorfeldtäters kenntlich gemacht, indem er das *Vorbereiten* eines Zieldelikts explizit in den Wortlaut des Tatbestands aufgenommen hat.[267] In den anderen Tatbeständen[268] fehlt es an einem solchen Merkmal. Damit ergeben sich strukturell zwei Gruppen von Software-Delikten: *Vorbereitungs*delikte einerseits, deren Strafwürdigkeit erst aus ihrem vertatbestandlichten Konnex zur vorbereiteten Zieltat folgt, und *Anschließungs*delikte andererseits, die ein in sich geschlossenes Verhalten unter Strafe stellen, sodass zur Verwirklichung der Zieltat erneut ein in sich geschlossenes Verhalten anschließen muss.[269] Nachfolgend wird die unterschiedliche inhaltliche Reichweite der Vorfelddelikte in beiden Tatbestandsstrukturen analysiert (jeweils a)). Sodann wird dargestellt, wie sich die jeweilige Rechtstechnik in der Dual-Use-Problematik auswirkt (jeweils b)).

---

[266] Vgl. hierzu die Erörterungen oben, C.

[267] §§ 149 Abs. 1, 202c Abs. 1 Nr. 2, 263a Abs. 3 StGB und § 22b Abs. 1 Nr. 3 StVG.

[268] §§ 108b Abs. 2 i.V.m. § 95a Abs. 3 UrhG und § 4 ZKDSG i.V.m. § 3 Nr. 1 ZKDSG.

[269] Terminologie nach *Sieber*, NStZ 2009, 358 ff.; gegen den Begriff der unfertigen oder unvollkommenen Delikte *Popp*, GA 2008, 390.

1. Vorbereitungsdelikte

Vorbereitungsdelikte zeichnen sich dadurch aus, dass das Vorbereiten der Zieltat eigens als Tatbestandsmerkmal formuliert ist. Dogmatisch zählen sie zur Kategorie deliktischer Planung, bei der die Gefährdung des Rechtsguts im Wesentlichen aus den Planungen und Absichten des Täters resultiert – äußerlich sind diese Delikte aufgrund des fehlenden Deliktserfolgs „unfertig" *(inchoate offences)*.[270] Wenn der Gesetzgeber diese Delikte mitunter als abstrakte Gefährdungsdelikte bezeichnet,[271] so ist dies wohl dahingehend zu verstehen, dass für die Verwirklichung des Tatbestands weder eine Rechtsgutsverletzung noch eine konkrete Rechtsgutsgefährdung erforderlich ist.[272] Dass der Gesetzgeber damit weiter gehende dogmatische Festlegungen treffen wollte, ist zu bezweifeln.[273]

a) Charakteristika dieses Regelungsmodells

In den Software-Delikten der vorliegenden Arbeit hat der Gesetzgeber die Formulierung gewählt: „wer eine [Zieltat] vorbereitet, *indem* er […], wird bestraft." In anderen Vorbereitungsdelikten finden sich auch die Formulierungen „wer eine [Zieltat] vorbereitet, *und dadurch* […], wird […] bestraft" (§ 80 StGB) sowie das knappe „wer eine [Zieltat] vorbereitet, wird […] bestraft" (§ 83 Abs. 1 und § 234a Abs. 3 StGB). Ebenso findet sich die Formulierung „Wer *zur Vorbereitung* [einer Zieltat …], wird bestraft" (§§ 310 Abs. 1, 316c Abs. 4 StGB). Es ist unklar, ob diese scheinbar minimalen Abwandlungen in der Tatbestandsformulierung auch inhaltliche Auswirkungen haben. Im Einzelnen ist die Bedeutung des Merkmals „Vorbereiten" nämlich äußerst umstritten. Dies betrifft insbesondere Inhalt, Reichweite und Anknüpfungspunkt des Merkmals. Inhaltlich ist zunächst unklar, ob das Wort „Vorbereiten" überhaupt als Tatbestandsmerkmal mit eigenständiger Bedeutung anzusehen ist. Die zweite, anschließende Frage ist, ob das „Vorbereiten" als objektives Tatbestandsmerkmal zu verstehen ist, das lediglich vom Vorsatz umfasst sein muss, oder ob das „Vorbereiten" eine erforderliche Intention des Vorfeldtäters beschreibt, also eine über den objektiven Tatbestand schießende Innentendenz ausdrückt. Drittens ist ungeklärt, wie stark die Zieltat in der Vorstellung des Vorfeldtäters konkretisiert sein muss. Alle Fragen werden nachfolgend erörtert.

---

[270] Vgl. *Sieber*, NStZ 2009, 359.

[271] Vgl. BT-Drucks. 16/3656, S. 12 rechte Spalte.

[272] Diese negative Definition der abstrakten Gefährdungsdelikte findet sich auch bei *Kindhäuser*, Gefährdung als Straftat, S. 225; siehe zur Deliktsstruktur von Gefährdungsdelikten *Schulenburg*, in: Hefendehl (Hrsg.), Rechtsgutstheorie, S. 246 ff.

[273] Dazu sogleich unten.

aa) Eigene Bedeutung des „Vorbereitens“?

Zunächst ist fraglich, ob dem Vorbereiten überhaupt ein eigener Bedeutungsgehalt zukommt. Der Wortlaut spricht davon, dass der Täter eine Zieltat vorbereitet, *indem* er eine bestimmte Handlung vornimmt (etwa ein Hackingtool verbreitet, § 202c Abs. 1 Nr. 2 StGB). Legt man diese Formulierung grammatisch eng aus, so folgt aus der Konjunktion „indem“, dass derjenige, der den zweiten Halbsatz verwirklicht, automatisch die Zieltat *vorbereitet*. Der Indem-Halbsatz stellt demgemäß eine Legaldefinition des Vorbereitens dar. Deshalb bliebe nach dieser strengen Wortlaut-Auslegung kein Raum mehr für eine eigenständige Bedeutung des Merkmals „vorbereiten“, die über den Bedeutungsgehalt des zweiten Halbsatzes hinausgeht.[274]

Der Gesetzgeber argumentiert in den Gesetzesmaterialien zu § 202c StGB jedoch ambivalent. Dort heißt es zunächst, dass der Vorfeldtäter eine eigene oder fremde Computerstraftat in Aussicht genommen haben müsse.[275] Dies spricht für einen eigenen (subjektiven) Gehalt des Merkmals „vorbereiten“. Gleich im Folgesatz heißt es aber, dass der Vorfeldtäter dann keine Computerstraftat in Aussicht nimmt, wenn das Computerprogramm zu Ausbildungszwecken in der IT-Sicherheitsbranche hergestellt, erworben oder einem anderen überlassen wurde.[276] Hier wird also allein mit den (objektiven) Merkmalen des Indem-Halbsatzes argumentiert: Sind die Kriterien des Indem-Halbsatzes (Zweck des Computerprogramms: Begehung einer Computerstraftat) objektiv nicht erfüllt, so ist auch das „Vorbereiten“ zu verneinen. Diese Argumentation spricht also gegen eine eigenständige Bedeutung des Vorbereitens.

Gleich im Anschluss bringt der Gesetzgeber jedoch wieder ein entgegengesetztes Beispiel: Wird ein ursprünglich zu kriminellen Zwecken hergestelltes Computerprogramm ausschließlich *zu legalen Zwecken verbreitet*, so werde wiederum keine Computerstraftat in Aussicht genommen[277] – hier ist also das Vorbereiten mit der Tathandlung verknüpft und wird interpretiert als „Ausführen der Tathandlung zu einem kriminellen Zweck“, mithin als eigenständiges (subjektives) Merkmal. Auch der letzte Satz der Gesetzesbegründung deutet in diese Richtung: Allein die Tathandlung (Herstellen etc. eines tatbestandsmäßigen Computerprogramms) stelle noch kein „Vorbereiten“ dar.[278]

In der Literatur wird dagegen zum Teil vertreten, dass das Vorbereiten keine eigenständige Bedeutung habe.[279] Dabei wird jedoch nicht mit dem Wortsinn, son-

---

274 Vgl. auch *Gehrig*, Absichtsmerkmal, S. 96.

275 BT-Drucks. 16/3656, S. 19 linke Spalte.

276 Ebd.

277 BT-Drucks. 16/3656, S. 19 rechte Spalte.

278 Insgesamt ebenso *Böhlke/Yilmaz*, CR 2008, 263.

279 NK-*Puppe*, § 149 Rn. 2, 3.

dern mit der (gesetzgeberisch intendierten) Dogmatik argumentiert: Der Gesetzgeber habe das Vorbereitungsdelikt als abstraktes Gefährdungsdelikt konzipiert, dessen abstrakte Gefahr sich allein in der Herstellung der tatgegenständlichen Vorrichtung erschöpfe, mittels derer beispielsweise im Falle des § 149 Abs. 1 Nr. 1 StGB theoretisch unbegrenzt viele Falsifikate hergestellt werden könnten.[280]

Dieses Argument ist zumindest für die Tatvarianten, in denen der Vorfeldtäter die Computerprogramme einem nicht überschaubaren Personenkreis zugänglich macht, von einigem Gewicht, denn hier besteht die abstrakte Gefahr für das Rechtsgut tatsächlich allein in der Verfügbarkeit der hergestellten Fälschungsmittel. Dann macht es auch keinen Unterschied, ob der Vorfeldtäter darüber hinaus noch gezielt zur Vorbereitung von Straftaten handelt oder nicht. Für die Tatvarianten des Einführens, Sichverschaffens und des hier explizit erwähnten Herstellens lässt sich dies jedoch nicht aufrechterhalten. In diesen Fällen begründet die Tathandlung isoliert noch überhaupt keine Gefahr für das Rechtsgut. Diese entsteht erst unter Berücksichtigung eines etwaigen Planungszusammenhangs des Vorfeldtäters, welcher dann in das Merkmal „vorbereiten" hineinzulesen wäre.

Auch in der Literatur wird eine eigenständige Bedeutung des Vorbereitens abgelehnt, allerdings wird hierfür vereinzelt die Begründung vorgetragen, dass der Tatbestand seinen Anwendungsbereich verlöre, wenn man dem Vorbreiten eine eigenständige Bedeutung beimäße: Wäre erforderlich, dass der Vorbereitungstäter eine Zieltat in Aussicht nimmt, so müssten Vorbereitungstäter und Zieltäter identisch sein.[281] Ohne diese Täteridentität hätte der Vorfeldtäter schließlich keinen Einfluss auf die Zieltat.[282] Dann aber würde dem § 202c StGB insgesamt der Anwendungsbereich entzogen, weshalb auf das Merkmal „vorbereiten" insgesamt zu verzichten sei.[283]

Dieser Argumentation ist aber schon deshalb nicht zuzustimmen, weil nicht ersichtlich ist, weshalb bei Täteridentität der Anwendungsbereich des Vorbereitungsdelikts entfallen soll. Im Übrigen stimmt schon die Grundannahme nicht: Vorbereitungstäter und Zieltäter müssen keineswegs identisch sein. Der Vorfeldtäter kann ohne Weiteres einen irgendwie gearteten Vorsatz hinsichtlich der Zieltat haben, ohne dass er zugleich späterer Täter des Zieldelikts sein müsste. Es dürfte sogar besonders häufig vorkommen, dass der Hersteller eines tatbestandsmäßigen Computerprogramms (= Vorfeldtäter) nicht auch die spätere Straftat (bspw. Ausspähen von Daten) begeht. Diese Literaturstimme ist auch in den Gesetzesmaterialien an keiner Stelle reflektiert. Sie widerspricht im Übrigen auch systematischen Erwä-

---

280 NK-*Puppe*, § 149 Rn. 2.

281 *Böhlke/Yilmaz*, CR 2008, 264.

282 Ebd.

283 Ebd., allerdings führen *Böhlke/Yilmaz* sodann als begrenzendes Merkmal ein, der Täter dürfe hinsichtlich der Zieltat keine Befugnis zur Tatausführung vom Rechtsgutsinhaber erhalten haben, 264–266.

gungen: Schließlich verlangt man auch beim Gehilfen gemäß § 27 Abs. 1 StGB Vorsatz hinsichtlich der Haupttat, ohne dass der Gehilfe und der Haupttäter identisch sein müssten. Es lässt sich deshalb keine plausible Stütze für diese Literaturansicht finden.

Für eine eigenständige Bedeutung des Vorbereitens spricht auch die Tatsache, dass etwa § 149 Abs. 1 Nr. 1 StGB bis auf das Merkmal des Vorbereitens inhaltlich deckungsgleich mit § 127 Abs. 1 Nr. 1 OWiG ist. Folglich muss gerade das Merkmal des Vorbereitens die qualitative Grenze zwischen kriminellem Unrecht und Ordnungsunrecht markieren. Das Gegenargument, § 127 OWiG erfasse schlicht *andere* Fälle als § 149 StGB und sei nur bei Gegenständen mit einer „speziellen andersartigen Zweckbestimmung" einschlägig,[284] verfängt schon deshalb nicht, weil es ausweislich der jeweiligen Tatbestände sowohl bei § 149 Abs. 1 Nr. 1 StGB als auch bei § 127 Abs. 1 Nr. 1 OWiG maßgeblich auf die *Eignung* der Gegenstände ankommt. Diese Eignung wird von etwaigen Zweckbestimmungen gar nicht tangiert, sodass eine Zweckbestimmung auch nicht den Ausschlag über die Tatbestandsmäßigkeit geben kann.[285]

In teleologischer Argumentation wird für die eigene Bedeutung des Vorbereiten-Merkmals ebenso angeführt, dass sich kriminelles Vorverhalten eben nur dadurch von legitimem Verhalten der IT-Sicherheit unterscheide, dass nur bei Ersterem der Vorsatz hinsichtlich des Vorbereitens einer Straftat gegeben sei.[286] Der IT-Sicherheitsbeauftragte bereitet keine Straftaten vor, sondern will sie verhindern. Auch historisch, also mit der Gesetzesbegründung, lässt es sich vereinbaren, im Vorbereiten ein eigenständiges Merkmal zu sehen, wenn man annimmt, dass das Vorbereiten *objektiv* durch den zweiten Halbsatz definiert wird, *subjektiv* aber im Sinne einer überschießenden Innentendenz höhere Anforderungen stellt. Legt man diese Auslegung zugrunde, so sind die oben dargestellten Ausführungen in den Gesetzesmaterialien auch schlüssig. Fraglich ist dann allerdings, *welche* Bedeutung das Vorbereiten im subjektiven Tatbestand genau hat.

Vereinzelt wird auch vertreten, dass das Vorbereiten über den eigenen (subjektiven und objektiven) Bedeutungsgehalt hinaus noch eine weitere objektive Bedeutung habe: Vorbereiten setze voraus, dass eine Zieltat bereits konkret geplant sei.[287] Dies sei jedenfalls dann ein objektives Merkmal, wenn die Zieltat eines anderen vorbereitet werde – nur beim Vorbereiten einer eigenen Zieltat handle es sich um ein ausschließlich subjektives Merkmal.[288] Darüber hinaus müsse „das Vorhaben"

---

[284] NK-*Puppe*, § 149 Rn. 3.

[285] Vgl. oben B.2.

[286] *F. Albrecht*, SVR 2005, 286. Ob dann der Verweis auf allgemeine Vorsatzregeln, also zumindest Eventualvorsatz genügt, ist freilich fraglich, siehe sogleich unten bb).

[287] SK-*Rudolphi/Stein*, § 149 Rn. 6; Schönke/Schröder-*Sternberg/Lieben*, § 149 Rn. 7.

[288] SK-*Rudolphi/Stein*, § 149 Rn. 6.

objektiv erfolgstauglich sein.[289] Mit dem „Vorhaben" ist in diesem Zusammenhang wohl die konkrete Zieltat gemeint, welche auf die konkrete Vorfeldhandlung aufbaut. Gegen diese objektiven Auslegungen des Vorbereitens spricht zunächst der Wortlaut. Denn durch den Indem-Halbsatz wird legaldefiniert, worin das Vorbereiten objektiv besteht.

Freilich könnte man die Ausführungen dieser Autoren auch als Argumentation für eine teleologische Einschränkung des objektiven Tatbestands verstehen. Dann allerdings ist höchst zweifelhaft, ob diese Einschränkung tatsächlich dem Telos des Delikts folgt. Denn die Vorbereitungsdelikte haben gerade zum Ziel, Massenkriminalität zu verfolgen und verhindern.[290] Es sollen also auch Fälle erfasst werden, in denen etwa der Hersteller eines schädlichen Computerprogramms einer unübersehbaren Menge Dritter eine bestimmte Art von Zieltaten ermöglicht. In diesen Fällen ist es aber typischerweise nicht so, dass der unübersehbare Personenkreis bereits Zieltaten planen würde und der Vorfeldtäter hierfür dann das Mittel bereitstellt. Der umgekehrte Fall dürfte die Regel sein.

bb) Vorsatz hinsichtlich des objektiven Vorbereitens

Überwiegend wird also vertreten, dass das Vorbereiten objektiv in den aufgeführten Tathandlungen (Herstellen, Überlassen etc.) aufgeht, subjektiv jedoch eine eigenständige Bedeutung haben soll.[291] Dementsprechend ist im subjektiven Tatbestand nicht nur erforderlich, dass der Vorfeldtäter die Tathandlung, also das Herstellen, Überlassen etc. des Computerprogramms vorsätzlich vornimmt, sondern dass er diese Vorfeldhandlung auch vorsätzlich *als Vorbereitungs*handlung für die Begehung eines (eigenen oder fremden) Zieldelikts vornimmt. Dies bedeutet mindestens, dass der Vorfeldtäter auch in seinen Vorsatz aufgenommen haben muss, dass man zur Verwirklichung einer Zieltat auf seine Vorfeldtat aufbauen kann, also seine Vorbereitungshandlung eine günstigere Ausgangslage für die Begehung der Zieltat schafft. Dies bedeutet allerdings nicht zwingend, dass der Täter auch hinsichtlich der Begehung oder des Taterfolgs des Zieldelikts Vorsatz haben muss.

Zunächst wird hier deshalb die überwiegend thematisierte Konstellation vorgestellt, in der objektiv das Vorbereiten als „Schaffen einer günstigeren Ausgangslage" verstanden und stets bejaht wird, wenn der zweite Halbsatz des Vorbereitungsdelikts („indem er […]") objektiv verwirklicht ist, während sich der Vorsatz gerade nicht auf diese objektiven Merkmale des zweiten Halbsatzes beschränkt,

---

289 Ebd.

290 BT-Drucks. 16/3656, S. 12 linke Spalte.

291 *Fischer*, § 149 Rn. 5, § 202c Rn. 7, § 263a Rn. 33 f.; LK-*Hilgendorf*, § 202c Rn. 27; Lackner/*Kühl*, § 149 Rn. 5, § 202c Rn. 5, § 263a Rn. 26c; NK-*Kargl*, § 202c Rn. 12 und NK-*Kindhäuser*, § 263a Rn. 44 (die damit in Widerspruch treten zu NK-*Puppe*, § 149 Rn. 3); LK-*Ruß*, § 149 Rn. 6; widersprüchlich *Böhlke/Yilmaz*, CR 2008, 264.

sondern darüber hinausschießt. Die Stimmen in der Literatur, die zusätzlich einen Vorsatz hinsichtlich Tatbegehung oder Taterfolg des Zieldelikts fordern, werden im anschließenden Kapitel diskutiert.[292]

Popp spricht treffend davon, der Vorbereitungstäter müsse seinem Verhalten eine „subjektiv deliktsfördernde Tendenz verleihen".[293] *Stree/Sternberg-Lieben* konkretisieren dies dahingehend, dass der Vorbereitungstäter wissen oder damit rechnen müsse, dass sein Verhalten eine Zieltat fördert.[294] Lediglich *Rudolphi/Stein* konkretisieren dies noch weiter und führen aus, dass der Vorsatz sich darauf erstrecken müsse, dass bereits eine Zieltat geplant sei, die auch durch die Vorbereitungshandlung gefördert werden könne.[295] Sofern der Vorfeldtäter eine eigene Zieltat vorbereite, bedeute dies, dass er bereits einen Tatentschluss zur Begehung der Zieltat gefasst haben müsse, der qualitativ den Anforderungen des § 22 StGB entspricht. Bereite er dagegen eine fremde Zieltat vor, so müsse sein Vorbereitungsvorsatz umfassen, dass der andere einen Tatentschluss gemäß § 22 StGB bereits gefasst habe.[296] Diese Auffassung engt den subjektiven Tatbestand stark ein und erfasst vor allem solche Konstellationen, in denen der Vorfeldtäter und der Zieltäter kollusiv zusammenarbeiten. Jedoch sind hiernach regelmäßig Konstellationen ausgeschlossen, in denen der Vorfeldtäter durch sein Verhalten einem größeren Kreis Dritter die Zieldelikte erst ermöglicht oder erheblich erleichtert, da wohl in vielen solchen Fällen die Zieltatplanung der anderen erst nach der abgeschlossenen Vorfeldhandlung einsetzt.

Ganz überwiegend wird deshalb angenommen, dass sich der Vorsatz lediglich auf das Fördern der Zieltat erstrecken müsse und diesbezüglich dolus eventualis genüge. Damit reicht aus, wenn der Täter ernstlich davon ausgeht und sich damit abfindet, dass sein Verhalten eine Straftat fördert.[297]

Popp dagegen hält unter Verweis auf die englische Fassung der *Cybercrime Convention* Absicht für erforderlich. Das dortige „intent" sei nämlich mehr als der deutsche dolus eventualis.[298] Ebenso – wenn auch ohne Begründung – verlangt

---

[292] Siehe dazu unten cc).

[293] *Popp*, MR-Int 2007, 87.

[294] Schönke/Schröder-*Stree/Sternberg-Lieben*, § 149 Rn. 7.

[295] SK-*Rudolphi/Stein*, § 149 Rn. 6a.

[296] Ebd.

[297] MüKo-*Erb*, § 149 Rn. 6; *Ernst*, NJW 2007, 2664; *ders*., DS 2007, 338; *Fischer*, § 149 Rn. 5 und § 202c Rn. 8, einschränkend in § 263a Rn. 34, wo er dolus eventualis nur hinsichtlich der Tatgegenstände und der Tathandlung genügen lässt; *Gröseling/Höfinger*, MMR 2007, 629; *Höfinger*, ZUM 2009, 753; Lackner/*Kühl*, § 149 Rn. 5, § 202c Rn. 5, § 263a Rn. 26c; NK-*Kargl*, § 202c Rn. 13; NK-*Kindhäuser*, § 263a Rn. 44; *Schreibauer/Hessel*, K&R 2007, 619; *Schumann*, NStZ 2007, 679.

[298] *Popp*, MR-Int 2007, 87.

Wohlers Absicht bezüglich des Vorbereitens.[299] Auch *Gercke* hält zumindest bei § 263a Abs. 3 StGB hinsichtlich der Vorbereitung der Zieltat explizit Absicht für erforderlich.[300]

Ebenso vertritt *Gehrig*, dass das Vorbereiten als zielgerichtetes Vorbereiten im Sinne von dolus directus mindestens zweiten Grades zu verstehen sei: Ihm zufolge ist der Unrechtsgehalt in der Konstellation, in der etwa der „Vorfeldtäter" einem anderen mit bloßem dolus eventualis ein Computerprogramm überlässt, derart gering, dass die Tat besser dadurch abgebildet würde, dass man sie als Beihilfe zum Sichverschaffen des anderen qualifiziert und dem durch § 27 Abs. 2 Satz 2 StGB geminderten Strafrahmen unterwirft.[301] Diesem Vorschlag kann freilich immer nur dann gefolgt werden, wenn beweisbar ist, dass ein Sichverschaffen eines anderen vorliegt. In der schon mehrfach erörterten, vom Bundesverfassungsgericht nicht angenommenen Verfassungsbeschwerde[302] hatte etwa der Informatikprofessor seinen Studenten zu Studienzwecken Hacking-Programme verfügbar gemacht. Dolus eventualis hinsichtlich des Vorbereitens einer Straftat durch einen der Studenten wäre hier zu bejahen. Beihilfe zum Sichverschaffen eines Hacking-Programms liegt dagegen nur vor, wenn auch nachgewiesen werden kann, dass ein Student tatsächlich selbst eine Straftat vorbereitet und sich hierfür ein Hacking-Programm vom Professor verschafft.

Auch der Verweis auf die Cybercrime Convention ist nur insofern überzeugend, als dort das Vorbereiten gerade kein Tatbestandsmerkmal darstellt. Hier wird das Vorfelddelikt stattdessen als isolierte Tathandlung konstruiert (Herstellen, Verkaufen etc. eines bestimmten Computerprogramms), welche mit der *Absicht* verknüpft wird, dass dieses Computerprogramm zur Begehung von Zieltaten verwendet wird („with intent that it be used for the purpose of committing any of the offences"), Art. 6 Abs. 1 a CCC.[303] Die Cybercrime Convention spricht hier also – anders als *Popp* und *Gercke* – von einer *Verwendungs*absicht, nicht von einer Vorbereitungsabsicht.[304]

Diese Verwendungsabsicht geht aber über eine Vorbereitungsabsicht hinaus: Vorbereitungsabsicht läge schon vor, wenn der Vorfeldtäter willentlich oder wissentlich eine günstigere Ausgangslage für die Begehung einer Zieltat schafft. Er müsste dagegen nicht beabsichtigen, dass das Computerprogramm tatsächlich zur

---

[299] MüKo-*Wohlers*, § 263a Rn. 70; der folglich Stellung bezieht gegen MüKo-*Erb*, § 149 Rn. 6.

[300] *Gercke,* in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 195; beim insoweit gleichlautenden § 202c StGB lässt er dann jedoch Eventualvorsatz genügen, ohne diese Ungleichbehandlung zu begründen, vgl. ebenda, Rn. 126.

[301] *Gehrig*, Absichtsmerkmal, S. 97.

[302] BVerfG 2 BvR 2233/07.

[303] Siehe dazu ausführlich unten II.C.1.

[304] Siehe zu dieser Auslegung des Vorbereiten-Merkmals nachfolgend cc).

Begehung einer Zieltat verwendet wird. Der Auslegung *Popps* und *Gerckes* wäre also zuzustimmen, wenn der Gesetzgeber die Vorgaben aus der CCC inhaltsgleich umsetzen wollte.

Dies ist aber fraglich, da der deutsche Gesetzgeber Umsetzung des Art. 6 Abs. 1 CCC mit § 202c Abs. 1 StGB explizit eine andere Tatbestandskonstruktion gewählt hat. Zwar spricht er in der Gesetzesbegründung ausdrücklich die Vorgaben der CCC an, was möglicherweise für eine Auslegung des Vorbereiten-Merkmals als Verwendungsabsicht spräche. Zudem zitiert er in der Begründung zu § 202c Abs. 1 Nr. 1 und Nr. 2 StGB auch deren jeweilige Vorgaben, nämlich Art. 6 Abs. 1 CCC lit. a ii. beziehungsweise lit. a i. Interessanterweise zitiert er bei der Vorgabe zu § 202c Abs. 1 Nr. 1 (!) StGB nun einen Teil des Art. 6 Abs. 1 CCC, den er beim Zitieren der Vorgabe zu § 202c Abs. 1 Nr. 2 StGB weglässt: „mit dem Vorsatz, sie zur Begehung bestimmter Computerstraftaten zu verwenden".[305] Dies ist aber genau der Zusatz, der für die Frage der Vorbereitungs- oder Verwendungsabsicht relevant ist. Die unterschiedliche Zitierung mag ein Versehen gewesen sein, aber auch im Folgenden führt der Gesetzgeber aus, dass die Tathandlung (also das Herstellen etc.) zwar „*zur Vorbereitung*" einer Zieltat vorgenommen werden müsse, dass hierfür aber ein „In-Aussicht-Nehmen" einer Zieltat genüge.[306] Damit liegt ein Vorbereiten nach der Gesetzesbegründung bereits vor, wenn der Vorfeldtäter die Tathandlung (Herstellen etc.) vornimmt und dabei eine Zieltat „in Aussicht nimmt". Dass damit weniger als Absicht gemeint ist, folgt schon daraus, dass ein Absichtserfordernis im Gesetzgebungsverfahren angeregt, aber nicht übernommen wurde und der Gesetzgeber dieses in den Materialien an keiner Stelle diskutiert.[307]

Einen ganz anderen Standpunkt vertritt *Hoyer*: Er interpretiert im Rahmen des § 263a Abs. 3 StGB den Vorbereitungsvorsatz als Vorsatz des Vorbereitungstäters hinsichtlich der „Kausalität seiner Tathandlung für einen Computerbetrug".[308] Unter teleologischen Gesichtspunkten ist zweifelhaft, dass eine solche (u.U. auch falsche) Vorstellung des Vorfeldtäters die Strafwürdigkeit begründen soll. Die Vorbereitungsdelikte sollen zudem ausweislich der jeweiligen Gesetzesbegründungen das konkrete Vorfeldverhalten unabhängig davon unter Strafe stellen, ob es überhaupt zum Zieldelikt kommt. Mit Hoyers Auslegung müsste es also genügen, wenn der Täter sich vorstellt, dass sein Handeln kausal für ein vorgestelltes Zieldelikt wird. Dies rückt das Vorbereitungsdelikt in die Nähe der versuchten Anstiftung gemäß § 30 Abs. 1 Var. 1 StGB.

Unerheblich ist zu diesem Zeitpunkt freilich, ob später tatsächlich eine Zieltat ausgeführt wird. Denn hier geht es nur um die subjektive Seite des Vorbereitens,

---

[305] BT-Drucks. 16/3656, S. 11 rechte Spalte Nr. 1 und 2.

[306] BT-Drucks. 16/3656, S. 18 rechte Spalte.

[307] Siehe *Borges/Stuckenberg/Wegener*, DuD 2007, 277.

[308] SK-*Hoyer*, § 263a Rn. 61.

und Vorbereitungsdelikte sollen gerade solches Verhalten erfassen, welches bei Ausbleiben einer Zieltat als versuchte Beihilfe straflos wäre.[309]

cc) Vorsatz hinsichtlich der Begehung der Zieltat?

Wie bereits angeklungen wird zum Teil über den Vorbereitungsvorsatz hinaus ein weiteres Vorsatzmerkmal eingeführt und diskutiert. Alle bisher dargestellten Ansichten thematisieren den Vorsatz hinsichtlich des Vorbereitens, also des Schaffens einer günstigeren Ausgangslage für die Begehung einer Zieltat.

Vereinzelt wird nun zusätzlich gefordert, dass der Vorbereitungstäter auch die *Begehung* der Zieltat oder zumindest die *Verwendung* des Computerprogramms zur Begehung der Zieltat in seinen Vorsatz aufgenommen haben müsse. So plädieren *Borges/Stuckenberg/Wegener* dafür, dass der Vorbereitungstäter zusätzlich die Absicht haben müsse, dass die Zieltat begangen werde. Dies fordern auch *Gazeas/Grosse-Wilde/Kießling*, allerdings bei der Einführung des § 89a StGB,[310] wobei sie jedoch einschränken, dass es zur Bejahung des Vorbereitens jedenfalls genüge, wenn der Vorfeldtäter dolus eventualis hinsichtlich der Begehung der Zieltat habe.

Auch die englische Sprachfassung der CCC fordert beim Vorfeldtäter die *Absicht*, dass das Computerprogramm zum Zwecke der Begehung einer Zieltat verwendet wird, Art. 6 Abs. 1 a CCC a.E. („with intent that it be used for the purpose of committing any of the offences"). Die deutsche Sprachfassung macht daraus den Vorsatz, das Computerprogramm zur Begehung einer Zieltat „zu verwenden", wonach in grammatisch korrekter Auslegung der Vorfeldtäter planen müsste, die Vorrichtung *selbst* zu verwenden. Das ist aber ersichtlich ein Übersetzungsfehler oder ein grammatisches Redaktionsversehen, da nach der Ratio des Art. 6 CCC gerade auch der Vorfeldtäter erfasst werden soll, der fremde Zieltaten vorbereitet, indem er Computerprogramme in Umlauf bringt, die einem unübersehbaren Kreis Dritter die Begehung der Zieltaten ermöglichen.[311]

Rudolphi/Stein differenzieren danach, ob der Vorfeldtäter eine eigene oder eine fremde Zieltat vorbereitet.[312] Wie beschrieben legen sie zunächst die Annahme zugrunde, dass der Vorbereitungsvorsatz sich darauf beziehen müsse, dass eine Zieltat bereits geplant sei und das eigene Vorfeldhandeln geeignet sei, diese Zieltat zu fördern.[313] Die Planung des Zieldelikts müsse dabei den Anforderungen des § 22 StGB entsprechen. Bereite der Vorfeldtäter in dieser Konstellation eine fremde

---

[309] BT-Drucks. 16/3656, S. 12 linke Spalte; *Fischer*, § 149 Rn. 5, § 263a Rn. 34; NK-*Kargl*, § 202c Rn. 12; LK-*Ruß*, § 149 Rn. 6.

[310] *Borges/Stuckenberg/Wegener*, DuD 2007, 277 f.; *Gazeas/Grosse-Wilde/Kießling*, NStZ 2009, 595; siehe auch *Sieber*, NStZ 2009, 359.

[311] Siehe dazu ausführlich unten II.C.1.

[312] Siehe SK-*Rudolphi/Stein*, § 149 Rn. 6a.

[313] Vgl. die entsprechende Erläuterung oben bb).

Zieltat vor, so brauche er keinen Vorsatz hinsichtlich der Begehung dieser Zieltat, sondern lediglich dahingehend, dass der andere einen solchen Vorsatz bereits gefasst hat. Bereite der Vorfeldtäter dagegen eine eigene Zieltat vor, so müsse er selbst den Zieltatvorsatz haben.[314] Da dieser die Anforderungen des § 22 StGB entsprechen soll, muss also der Vorfeldtäter schon vor Versuchsbeginn *zur Zieltat entschlossen* sein.

Gegen eine *Absicht* des Vorbereitungstäters hinsichtlich der Begehung der Zieltat wird das Argument vorgetragen, dass der Vorfeldtäter häufig kein besonderes Interesse an der Begehung der Zieltat habe, sondern dass sich sein Interesse regelmäßig auf den eigenen Profit beschränke, der sich aber – jedenfalls in den Tatvarianten des Herstellens, Verkaufens, Feilhaltens, Überlassens etc. – durch die Vorbereitungshandlung selbst einstellt und nicht abhängig ist von der Begehung des Zieldelikts.[315] Dieses Argument gegen ein *Absichts*erfordernis wird freilich als Argument für den dolus eventualis vorgetragen.

Im Ergebnis wird also vereinzelt gefordert, dass der Vorbereitungstäter auch einen Vorsatz hinsichtlich der Begehung einer Zieltat hat. Dies mag *politisch* wünschenswert sein, *rechtliche* Argumente gibt es für eine solche Tatbestandsreduktion de lege lata jedoch nicht. Dies gilt insbesondere, weil der Gesetzgeber kein solches subjektives Merkmal normiert hat, obwohl er die Möglichkeit vor Augen hatte: In internationalen Vorgaben der Software-Delikte findet sich ein solches Vorsatzmerkmal. Man muss deshalb davon ausgehen, dass der Gesetzgeber sich bewusst dagegen entschieden hat.

dd) Vorbereiten einer bestimmten Zieltat oder vieler unbestimmter Zieltaten?

Neben der Frage, wie intensiv der Vorbereitungsvorsatz sein muss und worauf er gerichtet sein muss, wird ebenso kontrovers diskutiert, *wie konkret* die Zieltat(en), die der Vorfeldtäter vorsätzlich vorbereitet, in seiner Vorstellung ausgeformt sein müssen. Diese Frage stellt sich freilich unabhängig davon, ob man das Vorbereiten als „Absicht hinsichtlich der Begehung irgendwie konkretisierter Zieltaten" versteht oder ob man es als „Vorsatz hinsichtlich der Schaffung einer günstigeren Ausgangslage für irgendwie konkretisierte Zieltaten" versteht.

Die weiteste denkbare Auslegung würde hier den subjektiven Tatbestand bejahen, wenn der Tätervorsatz umfasst, dass *irgendjemand* anknüpfend an das Vorfeldverhalten *irgendeine* Zieltat begeht. In einer sehr engen Auslegung müsste sich der Vorsatz des Vorfeldtäters dagegen auf eine nach Zeit, Ort, Täter und Opfer

---

314 SK-*Rudolphi/Stein*, § 149 Rn. 6a.

315 Vgl. *Popp*, GA 2008, 391, mit Verweis auf die entsprechende Diskussion bei § 267 StGB, wo „*zur* Täuschung im Rechtsverkehr" gehandelt werden muss und sich entsprechende Fragen stellen. Das Argument zitiert *Popp* aus LK-*Tröndle*, 10. Aufl. 1982, § 267 Rn. 199.

genau bestimmte Zieltat beziehen. Möglicherweise liegt die Lösung in der Mitte, nämlich darin, dass der Vorfeldtäter die Zieltat in ihren wesentlichen Umrissen oder in Grundzügen – wenn auch nicht in allen Einzelheiten – in Aussicht genommen hat. Diese Formel wird weithin vertreten,[316] allerdings wird nicht immer dasselbe darunter verstanden.

Einer sehr weiten Ansicht zufolge müssen Gegenstand, Zeit, Ort oder Begehungsweise der Zieltat noch nicht konkretisiert sein, auch nicht in Grundzügen.[317] Vielmehr genüge es, wenn die Zieltat ihrem *rechtlichen* Wesen nach in Aussicht genommen ist.[318] Dies scheint auch der Gesetzgeber neuerdings zu vertreten, wenn er in den Gesetzesmaterialien zur Vorbereitung einer schweren staatsgefährdenden Gewalttat gemäß § 89a Abs. 1, 2 StGB ausführt, dass es bereits genüge, wenn für den Täter „der *Deliktstyp* der vorbereiteten Tat hinreichend bestimmt ist".[319] Diese Auslegung dürfte aber inhaltlich kaum noch zu unterscheiden sein von der Ansicht, die von vornherein *keinen überschießenden Vorbereitungsvorsatz* in den Tatbestand hineinliest. Letztlich fordert sie nämlich lediglich Vorsatz dahingehend, dass durch die Tathandlung „eine der Zieltaten" vorbereitet oder gefördert wird.[320]

Der Vorfeldtäter muss aber in den §§ 149 Abs. 1, 263a Abs. 3, 202c Abs. 1 StGB und 22b Abs. 1 StVG ohnehin Vorsatz hinsichtlich der tatgegenständlichen Vorrichtung haben und damit auch hinsichtlich ihrer Eignung zu bestimmten Straftaten beziehungsweise ihres auf Straftaten gerichteten Einsatzzweckes. Wer aber ein Computerprogramm, dessen Zweck die Begehung bestimmter Zieltaten ist, vorsätzlich verbreitet, zugänglich macht oder Ähnliches, der hat auch zwangsläufig mindestens dolus eventualis dahingehend, dass das Computerprogramm die Begehung solcher Zieltaten fördert. In der Regel dürfte er sogar sicheres Wissen haben, dass die Herstellung eines deliktisch einsetzbaren Computerprogramms die Begehung entsprechender Straftaten erleichtert. Der Vorfeldtäter könnte sich zwar darauf berufen, dass er die eigentliche *Begehung* solcher Straftaten nicht wolle – dass er sie faktisch begünstigt, auch wenn er das Computerprogramm beispielsweise allein in guter Absicht verfügbar macht, kann er aber nicht bestreiten.

Andernorts wird in einer deutlich engeren Auslegung gesagt, der Täter müsse eine konkrete Tat vor Augen haben, wobei lediglich Zeit, Ort und Einzelheiten offen bleiben dürften.[321] Eine noch engere Auffassung lehnt auch dies ab und legt

---

316 Siehe BT-Drucks. 16/3656, S. 19 linke Spalte; MüKo-*Erb*, § 149 Rn. 6; *Fischer*, § 263a Rn. 34; NK-*Kargl*, § 202c Rn. 12; NK-*Kindhäuser*, § 263a Rn. 44; Lackner/*Kühl*, § 149 Rn. 5; SK-*Rudolphi/Stein*, § 149 Rn. 6; Schönke/Schröder-*Sternberg/Lieben*, § 149 Rn. 7.

317 Lackner/*Kühl*, § 149 Rn. 5.

318 Ebd.

319 BT-Drucks. 16/12428, S. 14 rechte Spalte.

320 So auch NK-*Puppe*, § 149 Rn. 3.

321 LK-*Ruß*, § 149 Rn. 6.

als Maßstab für die wesentlichen Umstände der Zieldelikte die Wertungen der §§ 26, 27 StGB an.[322] Begründet wird dies damit, dass der Anwendungsbereich der Norm (hier: § 202c StGB) ohnehin rechtsstaatlich bedenklich weit und daher einschränkend auszulegen sei.[323]

Am engsten schließlich ist die Auffassung von *Rudolphi/Stein*. Danach ist jedenfalls beim Vorbereiten eigener Zieltaten ein Konkretisierungsgrad zu verlangen, der dem Konkretisierungsgrad in § 22 StGB entspricht.[324]

Als Argument für das Erfordernis einer Konkretisierung „jedenfalls in den Grundzügen" führt *Fischer* die Tätige-Reue-Vorschrift des § 149 Abs. 2 Nr. 1 StGB an. Diese findet aufgrund von Verweisungen auch in den anderen Vorbereitungsdelikten Anwendung, siehe §§ 202c Abs. 2, 263a Abs. 4 StGB und § 22b Abs. 2 StVG.[325] Ihr zufolge wird nicht bestraft, wer die Ausführung „der vorbereiteten Tat" aufgibt[326] und die Gefahr abwendet, dass andere „die Tat" weitervorbereiten oder ausführen. Der Wortlaut spricht also von „der Tat" und legt damit laut Fischer das Erfordernis einer *konkretisierten* einzelnen Tat nahe.

In systematischer Auslegung relativiert sich dieses Argument jedoch. Kumulativ zu § 149 Abs. 2 Nr. 1 StGB muss nämlich Abs. 2 Nr. 2 erfüllt sein (siehe „und" bei Abs. 2 Nr. 1 a.E.), und dieser konstatiert, dass der Vorfeldtäter straffrei ausgeht, wenn er die die Fälschungsmittel vernichtet, unbrauchbar macht, ihr Vorhandensein einer Behörde anzeigt oder sie dort abliefert. Legt man Nr. 1 und Nr. 2 im Zusammenhang aus, so ergibt sich, dass ein Vorbereitungstäter straffrei ausgeht, wenn er die Tatwerkzeuge aus dem Verkehr zieht und die Gefahr abwendet, dass andere an seine Tatvorbereitung anknüpfen. Dies bedeutet aber, dass der Vorbereitungstäter auch in den Genuss der Tätige-Reue-Vorschrift kommen muss, wenn eine Gefahr im Sinne der Nr. 1 gar nicht bestanden hat. Denn wenn der Vorbereitungstäter straffrei ausgeht, wenn er eine geschaffene Gefahr abwendet, so muss er erst recht straffrei ausgehen, wenn er die Gefahr gar nicht erst geschaffen hat. Dies wird insbesondere auch dadurch gestützt, dass der Tatbestand des § 149 Abs. 1 StGB eine solche Gefahrschaffung nicht voraussetzt. Es ist also nicht zulässig, aus der speziellen Privilegierung des Abs. 2 Nr. 1 einen Umkehrschluss auf die Voraussetzungen der Strafbarkeit nach Abs. 1 zu ziehen. Dementsprechend präzisiert *Fischer* auch, dass jedenfalls keine Konkretisierung des Vorbereitungsvorsatzes im Sinne der §§ 26, 27 erforderlich sein könne.[327]

---

322 LK-*Hilgendorf*, § 202c Rn. 28.

323 Ebd.

324 SK-*Rudolphi/Stein*, § 149 Rn. 6.

325 *Fischer*, § 149 Rn. 5.

326 Was freilich nur in den Fällen Sinn ergibt, in denen der Vorbereitungstäter eine *eigene* Tat vorbereitet.

327 *Fischer*, § 202c Rn. 8.

Gegen den Vorsatz hinsichtlich einer *konkretisierten* Zieltat spricht außerdem, dass in den Tatvarianten, in denen das Computerprogramm einem nicht näher eingeschränkten Personenkreis überlassen wird (also: Verfügbarmachen, Verbreiten, Überlassen etc.) oder in denen die Zieltat noch relativ fern ist (also: Feilhalten, Verwahren etc.) eine Konkretisierung hinsichtlich Tatzeit, Tatort oder Umfang der Zieltaten praktisch nie vorliegen wird.[328] Die Tätervorstellung kann hier regelmäßig nur dahingehend konkretisiert sein, dass das Computerprogramm zu allen *möglichen* Zieltaten verwendet wird. Würde man im Straftatbestand dennoch die Konkretisierung verlangen, so würde man ihm per Auslegung den Anwendungsbereich entziehen.

Zudem sollen Vorbereitungsdelikte historisch und teleologisch betrachtet solche Fälle erfassen, die andernfalls als versuchte Beihilfe straflos wären.[329] Demnach können auch die Anforderungen an den Konkretisierungsgrad des Vorbereitungsvorsatzes nicht höher sein als die Anforderungen an den Konkretisierungsgrad des Gehilfenvorsatzes. Beim Gehilfen ist aber gerade ausreichend, dass er die Dimension des Unrechts erfasst, also den wesentlichen Unrechtsgehalt und die Angriffsrichtung.[330] Angesichts der Tatsache, dass Vorbereitungsdelikte gerade auch einer befürchteten Massenkriminalität entgegenwirken sollen, die aus der Streuwirkung öffentlich zugänglicher Schadsoftware resultiert, wäre im Sinne des Gesetzgebers wohl zu erwägen, ob die subjektiven Voraussetzungen bei Vorbereitungsdelikten gegenüber den subjektiven Voraussetzungen der Beihilfe nicht sogar zu lockern sind.[331]

ee) Zusammenfassung

Es lässt sich also festhalten, dass dem Merkmal des Vorbereitens nach herrschender und überzeugender Ansicht eine eigenständige, subjektive Bedeutung zukommt. Der Täter muss also nicht nur die Merkmale des objektiven Tatbestands (Tathandlung, Tatgegenstand) vorsätzlich verwirklichen, sondern er muss darüber hinaus mindestens dolus eventualis dahingehend haben, dass er mit der Vornahme seiner Handlung die Begehung einer Straftat begünstigt oder irgendwie fördert. Diese geförderte Straftat muss nach der Vorstellung des Vorbereitungstäters in ihren wesentlichen Umrissen oder Grundzügen konkretisiert sein. Es herrscht jedoch keine Einigkeit darüber, welches Maß an Konkretisierung genau zu fordern ist. Eine Absicht hinsichtlich der tatsächlichen Begehung von Zieltaten wird nur von einem Teil der Autoren in das Vorbereiten-Merkmal hineingelesen und entspricht wohl nicht dem Willen des historischen Gesetzgebers.

---

328 So auch *Fischer*, § 202c Rn. 8 und § 263a Rn. 34.

329 BT-Drucks. 16/3656, S. 12 linke Spalte.

330 Statt aller siehe Schönke/Schröder-*Heine*, § 27 Rn. 19.

331 So auch *Fischer*, § 202c Rn. 8 und § 263a Rn. 34.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Der subjektiven Tatseite kommt im Rahmen der Dual-Use-Problematik besondere Bedeutung zu. Denn Kriminelle und IT-Sicherheitsbeauftragte nehmen häufig äußerlich identische Handlungen vor. Unterschiede bestehen regelmäßig allein in den subjektiven Einstellungen der Handelnden. Der Gesetzgeber hat bei der Normierung der Vorbereitungsdelikte diesen Umstand gekannt, und so ist das Vorbereiten-Merkmal als Versuch zu sehen, vor allem unter dem Mehrzweckaspekt des Dual-Use-Phänomens eine adäquate Lösung zu finden. Es ist jedoch fraglich, ob das Merkmal rechtstechnisch tatsächlich dazu geeignet ist, das gesetzgeberische Ziel zu verwirklichen, nämlich kriminelles Verhalten von erwünschten Handlungen in der IT-Sicherheitsbranche zu unterscheiden.

Ein IT-Sicherheitsbeauftragter, der mit tatbestandsmäßiger Software hantiert, wird vor allem den Vorwurf fürchten, er bereite *fremde* Straftaten vor. Dieser Vorwurf drängt sich auf, sobald der IT-Sicherheitsbeauftragte die alleinige Kontrolle über eine tatbestandsmäßige Software aufgibt. Der Vorwurf kann jedoch schon drohen, wenn der IT-Sicherheitsbeauftragte noch die alleinige Kontrolle über sein Computerprogramm ausübt.

Angenommen ein IT-Sicherheitsbeauftragter ist für die Server-Sicherheit in einem Unternehmen zuständig, findet eine Schwachstelle in einem Computerprogramm, das auf dem betreuten Server läuft und möchte nun testen, wie sich diese Schwachstelle ausnutzen lässt. Er schreibt ein Programm, welches unter Ausnutzung der Schwachstelle dem Verwender Zugriff auf die Daten verschaffen soll, die auf dem Server abgelegt sind. Dieses Programm schreibt er als *Proof of Concept*, um dreierlei Ziele zu verwirklichen: erstens will er sich selbst vergewissern, dass die Schwachstelle existiert und wie weit sie ausgenutzt werden kann. Zweitens will er dem Hersteller der Serversoftware, in der sich die Schwachstelle befindet, nachvollziehbar darlegen, worin die Schwachstelle in dessen Produkt besteht, damit dieser sie mit einem Update beheben kann. Drittens will er seinen Kollegen Existenz und Reichweite der Sicherheitslücke demonstrieren, damit diese überprüfen können, ob die Lücke auf ihrem System in gleicher Weise besteht und ausgenutzt werden kann und wie sie kurzfristige Behelfslösungen (sog. *Workarounds*) finden können, bis ein *Patch* vom Hersteller der Serversoftware erscheint und die Sicherheitslücke schließt.[332]

Hier stellt sich nun die Frage, ob der IT-Sicherheitsbeauftragte faktisch nicht auch fremde Straftaten vorbereitet, wenn er diesen *Proof of Concept* programmiert und gegebenenfalls anderen IT-Sicherheitsbeauftragten, dem Hersteller der Serversoftware oder der Öffentlichkeit zugänglich macht. Bei objektiver Betrachtung wird man dies häufig bejahen müssen: Die Ausgangslage zur kriminellen Ausnutzung der Sicherheitslücke wird ohne Zweifel durch die Veröffentlichung eines

---

[332] Vgl. *Muncan/Schreiber*, DuD 2009, 220 f., sowie oben Teil 1, I.B.2.b).

deliktisch einsetzbaren *Proof of Concepts* verbessert. Der IT-Sicherheitsbeauftragte, der den *Proof of Concept* herstellt, *weiß* dies auch, hat also nicht nur einen Fördervorsatz, sondern sogar dolus directus 2. Grades hinsichtlich der Schaffung einer besseren Ausgangslage für die Begehung von Straftaten.

Auch mit der Ansicht, dass die vorbereiteten Zieltaten einigermaßen konkretisiert sein müssten, zeigt sich dem IT-Sicherheitsbeauftragten kein Weg aus der Strafbarkeit. Die vorbereiteten Zieltaten sind ja aus seiner Sicht regelmäßig konkretisiert, denn der *Proof of Concept* wurde für eine spezielle Angriffsform unter Ausnutzung einer speziellen Sicherheitslücke in einer speziellen Systemkonfiguration entwickelt. Es ist also regelmäßig bestimmt, welche Art von Systemen auf welche genaue Art angegriffen werden. Dass die Opfer im Einzelnen noch nicht individualisiert sind, dürfte den Vorbereitungsvorsatz nicht entfallen lassen, da an diesen nach Intensität und Bestimmtheit keine höheren Anforderungen zu stellen sind als an den Gehilfenvorsatz, möglicherweise sogar niedrigere Anforderungen.[333]

In einem strukturell vergleichbaren Fall hat das Bayerische ObLG dies ausdrücklich festgehalten: In dem Fall hatte ein Gehilfe dem späteren Täter „Spezialdrähte" verkauft, mit denen dieser Spielautomaten einer bestimmten Marke ausleeren konnte. Der Drahtverkäufer wusste nicht, wann und wo der Täter die Drähte einsetzen würde, welche konkreten Automaten er ausleeren würde und zu wessen Schaden er das Geld aus den Automaten entwenden würde. Das BayObLG hielt fest, dass dies Einzelheiten der Tat seien, die der Gehilfe gerade nicht zu kennen brauche.[334]

Im Falle des IT-Sicherheitsbeauftragten sind die vorbereiteten Taten ganz ähnlich konkretisiert: Die Angriffsart ist bekannt, ebenso das eingesetzte Angriffsmittel und die Art der Angriffsziele. Der Unterschied besteht darin, dass der IT-Sicherheitsbeauftragte darüber hinaus regelmäßig nicht weiß, *wer* sein Computerprogramm deliktisch einsetzt. Ob damit der Vorbereitungsvorsatz entfällt, ist aber höchst fraglich. Für den Gehilfenvorsatz wird jedenfalls vertreten, dass es unschädlich sein kann, wenn der Gehilfe den Haupttäter nicht persönlich identifiziert hat.[335] Vorbereitungsdelikte unterschieden sich von Beihilfekonstellationen nun regelmäßig dadurch, dass sie einem unbestimmten Personenkreis die Begehung von Zieltaten ermöglichen. Demnach liegt eine entsprechende Weitung des subjektiven Tatbestands gerade im Telos der Vorbereitungsdelikte. Dementsprechend ist es nur konsequent, wenn es dem Vorbereitungstäter nicht zugutekommt, dass sich sein Vorbereitungsvorsatz nicht auf individualisierte Einzeltäter bezieht.

Im Anschluss hieran erübrigt sich allerdings auch die Diskussion, welche Form des Vorsatzes der IT-Sicherheitsbeauftragte bezüglich seines Förderbeitrags haben

---

333 Siehe oben ausführlich, a)–dd).

334 BayObLG NJW 1991, 2585, mit Verweis auf BGHSt 11, 66; BGH, bei *Dallinger*, MDR 1955, 143; BGH GA 1967, 115; BGH GA 1981, 133; BGH NJW 1982, 2454.

335 Schönke/Schröder-*Heine*, § 27 Rn. 19.

muss. Es trägt zur Lösung der Dual-Use-Problematik nichts bei, hinsichtlich des Vorbereitens (= die objektive Ausgangslage verbessern oder die Zieltat erleichtern) den dolus eventualis für unzureichend zu erklären.[336] Der IT-Sicherheitsbeauftragte *weiß* in aller Regel, dass sein *Proof of Concept* auch Straftaten ermöglicht oder erleichtert, denn er schreibt ihn ja gerade, um dies zu beweisen (das ist sozusagen das Beweisthema). Mithin weiß er auch sicher, dass er mit der Veröffentlichung des Computerprogramms eine günstigere Ausgangslage für die Begehung von Zieltaten schafft, sie also *vorbereitet*. Folglich hat der IT-Sicherheitsbeauftragte immer dolus directus 2. Grades hinsichtlich der Vorbereitung.

Eine Begrenzung des Wortlauts auf Absicht („wer in der Absicht, eine Zieltat vorzubereiten, bestimmte Computerprogramme herstellt, verbreitet …“ oder „wer absichtlich eine Zieltat vorbereitet, indem er …“) würde hier nur dann mit der gewünschten Rechtssicherheit das Handeln des IT-Sicherheitsbeauftragten von der Strafbarkeit ausnehmen, wenn unter Absicht nur dolus directus 1. Grades verstanden würde. Dann ließe sich argumentieren, dass es dem IT-Sicherheitsbeauftragten nicht zielgerichtet darauf ankomme, eine Zieltat zu fördern, sondern vielmehr sei sein primäres und überwiegendes Motiv, die konkrete Sicherheitslücke lege artis zu demonstrieren.[337] Das Fördern einer fremden Zieltat wäre hier bloß Nebenfolge, sodass dolus directus 1. Grades – jedenfalls mit der herrschenden Meinung – hier zu verneinen wäre.[338]

Allerdings bedeutet das Merkmal Absicht in den Straftatbeständen des StGB nicht immer allein dolus directus 1. Grades, sondern kann – in Abhängigkeit von Sinn und Zweck der Vorschrift – von allgemeinem Vorsatz über dolus directus bis hin zu dolus directus 1. Grades alles bedeuten.[339] Es herrscht lebhafter Streit über die Merkmale, nach denen unterschieden werden soll, ob in einem konkreten Tatbestand Absicht im Sinne von dolus directus 1. Grades erforderlich ist oder ob auch dolus directus 2. Grades ausreicht. Nach *Roxin* kommt es etwa darauf an, ob die deliktische Absicht den ganzen Deliktstyp prägt, wie etwa beim Betrug, der durch die Aneignungsabsicht sein Gepräge als Bereicherungsdelikt erhalte.[340] Hier sei dolus directus 1. Grades erforderlich, während in Delikten, die ihr Gepräge vornehmlich durch die tatbestandsmäßige Rechtsgutsverletzung erhalten, etwa § 164 Abs. 1 und § 257 StGB, dolus directus 2. Grades ausreichen soll.[341] Nach *Lenckner* kommt es darauf an, ob das Absichtsmerkmal den strafrechtlichen Schutz ausweiten oder begrenzen

---

336 Vgl. oben unter a)bb).

337 Zur schwierigen Abgrenzung zwischen dolus directus 1. Grades und 2. Grades in diesem Bereich siehe *Bung*, Wissen und Wollen, S. 220 ff.

338 Vgl. Dölling/Duttge/Rössner-*Duttge*, § 15 Rn. 13; *Gehrig*, Absichtsbegriff, S. 28.

339 Siehe nur BGHSt 16, 1.

340 So *Roxin*, Strafrecht AT I, S. 440 f. mit weiteren Beispielen.

341 *Roxin*, Strafrecht AT I, S. 442; vgl. auch Schönke/Schröder-*Sternberg-Lieben*, § 15 Rn. 70.

soll: Im ersten Fall, zu dem vor allem die Delikte zählen, in denen der Rechtsgüterschutz durch das Absichtsmerkmal vorverlagert wird, soll nach der ratio legis jeweils dolus directus 2. Grades genügen.[342]

Die Diskussion um die Absichtsdelikte soll hier nicht in ihren Einzelheiten wiedergegeben werden. Es soll nur veranschaulicht werden, dass die entscheidende Demarkationslinie beim Vorsatz hinsichtlich des Vorbereitens nicht zwischen dolus directus und dolus eventualis verläuft, sondern zwischen dolus directus 1. Grades und dolus directus 2. Grades. Dieses Problem löst man aber nicht dadurch, dass man „Absicht" als tatbestandliches Erfordernis normiert, da man damit nur die Tür zu einer weiteren Streitfrage öffnet, die in der Literatur lebhaft diskutiert und von der Rechtsprechung von Fall zu Fall entschieden wird.[343] Sie würde also in der Rechtswirklichkeit zunächst Rechtsunsicherheit hervorrufen. Eine weitere Einschränkung des Vorsatzes hinsichtlich des *Förderns der Zieltat* („vorbereiten") führt also nicht zu dem gewünschten Ergebnis, dass ein IT-Sicherheitsbeauftragter mit Sicherheit von der Strafbarkeit ausgeschlossen ist.

Das eigentliche Problem der Vorbereitungsdelikte ist also, dass mit dem Vorbereiten ein Tatbestandsmerkmal eingeführt worden ist, welches schon objektiv gar nicht den entscheidenden Unterschied zwischen kriminellem Vorfeldtäter und IT-Sicherheitsbeauftragten ausmacht, da beide unter Umständen gleichermaßen die Begehung von Straftaten ermöglichen oder erleichtern. Dieses Problem kann folglich auch nicht auslegungstechnisch im subjektiven Tatbestand gelöst werden. De lege lata findet ein IT-Sicherheitsbeauftragter nur einen Ausweg aus der Strafbarkeit, indem er das Computerprogramm, welches er eigentlich als *Proof of Concept* geschrieben hat, nicht aus den Händen gibt.

Um dennoch die Sicherheitslücke nachzuweisen, könnte er das Computerprogramm auf seinem System testen und diesen Test dokumentieren. Die Dokumentation könnte er sodann dem Hersteller der Server-Software, in der sich die ausgebeutete Sicherheitslücke befindet, sowie den Kollegen oder der Öffentlichkeit zur Verfügung stellen.[344] Zwar wird man dann immer noch bejahen können, dass er Zieltaten vorbereitet, da er immerhin Schwachstellen nachweist und belegt, dass diese auch ausgenutzt werden können. Allerdings tut er dies nicht mehr, indem er ein tatbestandsmäßiges Computerprogramm herstellt und verbreitet, sondern indem er die Dokumentation hierüber verbreitet. Dies wiederum ist nicht tatbestands-

---

342 *Lenckner*, NJW 1967, 1894.

343 Siehe nur Lackner/*Kühl*, § 15 Rn. 20 mit Verweis auf RGSt 59, 314 ff., und BGHSt 16, 1; siehe auch die Übersicht bei *Witzigmann*, JA 2009, 488 ff.

344 So hat etwa der französische Sicherheitsdienstleister *VUPEN* einen Zero-Day-Exploit entworfen, ausgeführt und ein Video hiervon auf Youtube zur Verfügung gestellt: https://www.youtube.com/watch?v=c8cQ0yU89sk [zuletzt aufgerufen am 16.11.2014].

mäßig.[345] Allerdings ist eine solche Dokumentation auch kein vollwertiger *Proof of Concept*, weil hieraus regelmäßig nicht alle Hintergründe erschlossen werden können, insbesondere wie das Schadprogramm (der *Exploit*) genau funktioniert und welche Sicherheitsfunktionen genau ausgehebelt werden.[346]

Der in der Literatur geäußerte Rat an die betroffenen IT-Sicherheitsunternehmen, sie sollten ihre Aktivitäten fortführen, aber im Detail protokollieren, hilft hier nicht weiter, weil ein tatbestandsmäßiges Verhalten selbstverständlich nicht dadurch straflos wird, dass man es protokolliert – möge das Protokoll auch noch so detailreich sein. Wenn in Teil 4 dieser Arbeit die einzelnen Regelungstechniken verglichen werden, wird man nicht umhin kommen festzustellen, dass das Konzept der Vorbereitungsdelikte insgesamt nicht dazu taugt, die Dual-Use-Problematik angemessen zu lösen. Man wird deshalb eine Alternative finden müssen.[347]

2. Anschließungsdelikte

Nicht in allen Software-Delikten hat der Gesetzgeber den intentionalen Bezug zur Zieltat explizit normiert. Nimmt man die Vorbereitungsdelikte weg, so bleiben Delikte, in denen schlicht ein bestimmter Umgang mit bestimmten Computerprogrammen unter Strafe gestellt wird. Hierzu zählen neben § 4 ZKDSG i.V.m. § 3 Nr. 1, § 2 Nr. 3 ZKDSG auch die Delikte des § 108b Abs. 2 i.V.m. § 95a Abs. 3 UrhG. In Anlehnung an *Sieber* werden diese Delikte hier Anschließungsdelikte genannt. Dieser Begriff macht deutlich, dass ein eigenständiges Verhalten eines anderen an das Verhalten des Vorfeldtäters anschließen muss, damit es zur Verletzung des Rechtsguts kommt.[348]

Dogmatisch lassen sich diese Delikte in die Kategorie der „Gefährdung durch Schaffung unbeherrschter objektiver Gefahrensituationen“ einordnen, zu der sich auch die konkreten und abstrakten Gefährdungs-, Eignungs- und Kumulationsdelikte zählen lassen.[349] Der Strafgrund besteht hier jeweils darin, dass der Vorfeldtäter eine Handlung vornimmt, an die zu deliktischen Zwecken angeknüpft werden kann, ohne dass der Täter hierüber die Kontrolle behielte.[350]

---

345 Anderes könnte allenfalls gelten, wenn man das Merkmal „Computerprogramm“ durch „Vorrichtungen“ ersetzt und hierunter auch Dokumentationen fassen möchte. Diese Auslegung erscheint allerdings sehr weit.

346 Vgl. hierzu auch die Meldung zum VUPEN-Video bei *heise Security*, http://heise.de/-1240321 [zuletzt aufgerufen am 16.11.2014]

347 Siehe dazu unten Teil 4, I.C.

348 *Sieber*, NStZ 2009, 358.

349 Systematisierung nach *Sieber*, NStZ 2009, 358 f.

350 So auch *Wohlers*, Deliktstypen, S. 328, der die Anschließungsdelikte jedoch auch zu den Vorbereitungsdelikten (in einem weiteren Sinne) zählt.

Bei den Anschließungsdelikten des Software-Strafrechts besteht diese Handlung im Umgang mit gefährlichen Computerprogrammen – wobei deren Gefährlichkeit und Unbeherrschbarkeit den fehlenden intentionalen Bezug des Vorfeldtäters zur Zieltat kompensieren soll. Es wird jedoch zu zeigen sein, dass nicht alle Anschließungsdelikte in diesem Bereich rechtstechnisch so gestaltet worden sind, dass sie ein unbeherrscht gefährliches Verhalten abbilden.[351] Im Anschluss an diese Erörterung der tatbestandlichen Charakteristika des Regelungsmodells werden seine konkreten Auswirkungen in der Dual-Use-Problematik erläutert.

a) Charakteristika dieses Regelungsmodells

Die Anschließungsdelikte unter den Software-Delikten zeichnen sich also dadurch aus, dass sie ein in sich abgeschlossenes Verhalten unter Strafe stellen. In der vorliegenden Arbeit wird regelmäßig vom Umgang mit bestimmten Computerprogrammen gesprochen, wobei Umgang weit zu verstehen ist und insbesondere die Herstellung der Computerprogramme einschließt. Anschließungsdelikte setzen gerade nicht voraus, dass der Vorfeldtäter seine Handlung mit einem bestimmten intentionalen Bezug zu einer Zieltat vornimmt (aa)). Dies bedeutet jedoch nicht, dass sie völlig frei von intentionalen Bezügen zu den jeweiligen Zieltaten wären, vielmehr sind diese intentionalen Bezüge häufig im Tatobjekt statt in der Tathandlung verankert. Damit sind sie zugleich losgelöst von der Person des Vorfeldtäters (bb)).

aa) Kein intentionaler Bezug des Vorfeldtäters zum Zieldelikt

Bei Anschließungsdelikten ist nicht erforderlich, dass der Täter mit seiner Handlung wissentlich oder willentlich irgendeine Zieltat vorbereitet, fördert oder ihre Begehung sonstwie beabsichtigt. Ausschlaggebend ist allein, dass er seine abgeschlossene Tathandlung vorsätzlich vornimmt.

So wird etwa in § 4 ZKDSG bestraft, wer eine Umgehungsvorrichtung herstellt, einführt oder verbreitet. Aus welchen Gründen der Vorfeldtäter dies tut oder welche Ziele er damit verfolgt, spielt für die Strafbarkeit nach § 4 ZKDSG keine Rolle. Insbesondere ist nicht erforderlich, dass der Vorfeldtäter die Umgehung eines Zugangskontrolldienstes plant oder beabsichtigt. Auch in § 108b Abs. 2 UrhG sind etwaige Intentionen des Vorfeldtäters hinsichtlich des Zieldelikts unerheblich. Interessant ist dabei, dass das Zieldelikt, nämlich die Umgehung der technischen Schutzmaßnahme gemäß § 108b Abs. 1 Nr. 1 UrhG im Grunde selbst ein Vorfelddelikt zur späteren Rechtsgutsverletzung darstellt und selbst auch in diesem Sinne eine überschießende Absicht hinsichtlich der Rechtsgutsverletzung

---

[351] Siehe sogleich a).

erfordert.[352] Das Vorfelddelikt des Abs. 2 ist aber als Anschließungsdelikt formuliert und normiert gerade keinen intentionalen Bezug zur Zieltat.[353] Es genügt vielmehr allein, dass der Täter vorsätzlich eine Umgehungsvorrichtung herstellt, einführt etc.[354]

Dieser Verzicht auf einen intentionalen Bezug des Vorfeldtäters kann auf zwei Weisen erklärt werden: Einerseits kann sich in dem Verzicht ausdrücken, dass der Gesetzgeber den intentionalen Bezug unwiderleglich präsumiert. Andererseits kann der Gesetzgeber den intentionalen Bezug für vernachlässigbar halten, etwa dann wenn dem tatbestandlichen Verhalten auch ohne intentionalen Bezug eine solche Gefährlichkeit innewohnt, dass diese allein ein strafbewehrtes Verbot des Verhaltens rechtfertigt.

bb) Andere intentionale Bezüge zum Zieldelikt

Dennoch sind die Anschließungsdelikte nicht völlig frei von intentionalen Bezügen zum Zieldelikt. Vielmehr finden sich zieltatbezogene Intentionen, oft solche anderer Personen, in den gesetzlichen Umschreibungen der Tatobjekte.

So werden unter den Umgehungsvorrichtungen des § 4 ZKDSG solche Vorrichtungen verstanden, die dazu bestimmt oder angepasst sind, die unerlaubte Nutzung eines zugangskontrollierten Dienstes zu ermöglichen, § 2 Nr. 3 ZKDSG. Damit ist eine Vorrichtung nur dann tatbestandsmäßig, wenn ein Bestimmungsgeber oder ein Anpasser die Intention verfolgt hat, dass diese Vorrichtung Zieltaten ermöglicht.

Hier ist also ein intentionaler Bezug normiert, der dem Merkmal des Vorbereitens in den Vorbereitungsdelikten ähnelt. Während dort der Vorsatz des Vorfeldtäters erforderlich ist, eine Zieltat zu fördern, ist hier die Intention des Bestimmungsgebers erforderlich, eine Zieltat zu ermöglichen. Der Unterschied besteht einerseits offensichtlich in der Intensität (fördern vs. ermöglichen), vor allem aber darin, dass in dem Anschließungsdelikt der Bestimmungsgeber oder Anpasser grundsätzlich nicht mit dem Vorfeldtäter identisch sein muss und dies häufig auch nicht ist. Die Intentionen des Vorfeldtäters sind hier deshalb durchweg unerheblich.[355]

In § 95a Abs. 3 Nr. 1 UrhG wird i.V.m. § 108b Abs. 2 UrhG der Umgang mit Vorrichtungen unter Strafe gestellt, die mit dem Ziel der Umgehung wirksamer technischer Maßnahmen vermarktet werden. Auch hier ist wieder kein intentionaler

---

[352] Nämlich die Absicht, sich oder einem Dritten Zugang zu einem nach dem UrhG geschützten Werk oder einem anderen nach dem UrhG geschützten Schutzgegenstand oder deren Nutzung zu ermöglichen.

[353] Ungenau: *Enders*, ZUM 2004, 599.

[354] Die gewerblichen Zwecke, die der Täter in § 4 ZKDSG und § 108b Abs. 2 UrhG verfolgen muss, sollen außer Betracht bleiben, weil sie jedenfalls keinen intentionalen Bezug der hier relevanten Art darstellen.

[355] Vgl. auch die ausführliche Erörterung dieses Tatbestandskonstrukts oben, I.B.3.

Bezug zur Zieltat beim Vorfeldtäter erforderlich, der solche Vorrichtungen herstellt, einführt, verbreitet, verkauft oder vermietet (§ 108b Abs. 2 UrhG). Dagegen ist ersichtlich erforderlich, dass *der Werbetreibende* das Ziel verfolgt, dass mit den Vorrichtungen technische Schutzmaßnahmen umgangen werden.[356] Entsprechendes gilt für § 95a Abs. 3 Nr. 3 UrhG, der eine Vorrichtung dann für tatbestandsmäßig erklärt, wenn sie hauptsächlich entworfen, hergestellt oder angepasst wird, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern. Hier ist also erforderlich, dass der Designer, Hersteller oder Anpasser den Zieltaterfolg intendiert.[357]

Die inhaltliche Bedeutung dieser intentionalen Bezüge ist im Detail weitgehend ungeklärt. Die Rechtsprechung begnügt sich bislang damit, deren Vorliegen anhand objektiver Anhaltspunkte aus Sicht des verständigen Durchschnittsnutzers zu bejahen oder verneinen – ohne eingehend zu erörtern, *was* sie da eigentlich bejaht oder verneint.[358] Allerdings gab es auch bislang keinen gerichtlichen Streit, in dem es auf eine inhaltliche Klärung solcher Einzelheiten angekommen wäre.

Einige Autoren verlangen im Modell des § 95a Abs. 3 Nr. 3 UrhG die *Absicht* des Herstellers, Designers oder Anpassers der tatgegenständlichen Vorrichtung.[359] Begründet wird dies allein damit, dass die Tatbestandsformulierung „um […] zu" an anderer Stelle auch als Absichtsmerkmal interpretiert werde. Mit einer solchen Auslegung würden die Beweisanforderungen jedoch sehr stark erhöht, vor allem in Drei-Personen-Konstellationen: Angenommen ein Vorfeldtäter T verkauft ein Computerprogramm an einen Kunden K, welches von einem Hersteller H programmiert worden ist. Für eine Bestrafung nach § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 3 UrhG müsste hier zunächst nachgewiesen werden, dass H das Computerprogramm hauptsächlich in der *Absicht* hergestellt hat, hinreichend konkretisierte Zieltaten zu erleichtern. Sodann müsste nachgewiesen werden, dass T zumindest billigend in Kauf nimmt, dass H diese Absicht beim Herstellen des Computerprogramms verfolgt hatte.[360]

Diese Konstruktion ist ungewöhnlich. In abstracto müssen in diesem Modell vier Voraussetzungen gegeben sein: ein Tatgegenstand, eine Tathandlung, die deliktische Absicht eines Dritten und der Vorsatz des Täters hinsichtlich der drei vorgenannten Merkmale. Das Ungewöhnliche an der Konstruktion ist, dass die deliktische Absicht nicht beim Täter vorliegen muss, sondern bei einem Dritten – der

---

356 Vgl. die ausführliche Erörterung dieses Tatbestandskonstrukts oben, I.B.6.

357 Vgl. die ausführliche Erörterung dieses Tatbestandskonstrukts oben, I.B.4.

358 Vgl. oben I.B.3.a)aa), I.B.4.a)aa), I.B.6.a)bb).

359 Dreyer/Kotthoff/Meckel-*Dreyer*, § 95a Rn. 101; *Hänel*, Umsetzung des Art. 6, S. 165; *Trayer*, Technische Schutzmaßnahmen, S. 116, 132; Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 85.

360 Vgl. auch oben I.B.4.

Täter muss diesbezüglich lediglich Vorsatz haben. Das StGB kennt Straftatbestände, in denen eine deliktische Absicht dem Gesamtgeschehen das kriminelle Gepräge gibt,[361] allerdings muss diese kriminelle Absicht stets beim Täter vorliegen und wird nicht von einem Dritten beigesteuert.

Würde man hieraus einen allgemeinen Grundsatz entwickeln, dass eine deliktsprägende Absicht immer beim Täter selbst vorliegen muss, so müsste in den Anschließungsdelikten die kriminelle Absicht des Dritten irgendwie dem Vorfeldtäter zugerechnet werden, damit sie dessen Bestrafung trägt. Es geht hier also um die Konstruktion eines Delikts, in dem ein Täter den subjektiven Tatbestand nicht vollständig selbst verwirklicht, sondern teilweise durch einen anderen. Das StGB kennt die Konstruktion, in der ein Täter den *objektiven* Tatbestand nicht vollständig selbst verwirklicht, sondern teilweise durch einen anderen: Bei mittelbarer Täterschaft gemäß § 25 Abs. 1 Var. 2 StGB werden objektive Tatbestandsmerkmale vom Tatmittler verwirklicht und dem Täter zugerechnet.[362] Auch bei Mittäterschaft, die im gemeinsamen Tatentschluss und Tatplan ein starkes Fundament wechselseitiger Zurechnung bietet,[363] werden ausschließlich *objektive* Tatbeiträge zugerechnet, während die subjektiven Tatbestandsmerkmale von jedem Mittäter in eigener Person verwirklicht werden müssen.[364]

Bei der vorliegenden Konstruktion besteht aber zwischen Vorfeldtäter und Hersteller oder Werbetreibendem nicht einmal ein Zurechnungsfundament wie die Gemeinschaftlichkeit, die bei der Mittäterschaft die Zurechnung erlaubt. Erst recht hat der Vorfeldtäter keine Willensherrschaft, wie dies bei der Zurechnung der Tatbeiträge in mittelbarer Täterschaft der Fall ist.[365] Unabhängig von der Frage, ob eine Zurechnung *subjektiver* Tatbeiträge überhaupt denkbar ist, wäre in den Anschließungsdelikten nur ein äußerst schwaches Zurechnungsvehikel vorhanden: der Vorsatz des Vorfeldtäters, also dass der Vorfeldtäter es ernstlich für möglich hält und billigend in Kauf nimmt, dass ein Software-Hersteller ursprünglich kriminelle Intentionen bei der Herstellung eines Computerprogramms verfolgt hat. Dogmatisch lässt sich hier also nur sehr schwer nachzeichnen, worin genau der Unrechtsgehalt dieses Vorfelddelikts liegt und inwiefern er verändert wäre, wenn der Vorfeldtäter keinen dolus eventualis hinsichtlich der Intentionen des historischen Herstellers hätte.

Alternativ könnte man auch versuchen, die Anschließungsdelikte als Teilnahme an fremdem Unrecht zu rekonstruieren. Die im Allgemeinen Teil des StGB gere-

---

[361] Etwa die Absicht rechtswidriger Zueignung in § 242, die Besitzerhaltungsabsicht in § 252 oder die Absicht rechtswidriger Bereicherung in § 263 StGB, die Nachteilzufügungsabsicht in § 303b StGB pp.

[362] Vgl. hierzu *Roxin*, AT II, S. 22 ff.; LK-*Schünemann*, § 25 Rn. 60 ff.

[363] Siehe nur *Roxin*, AT II, S. 78 ff.; abl. *Lesch*, ZStW 105 (1993), 292 ff. m.w.N.

[364] Siehe nur LK-*Schünemann*, § 25 Rn. 155, 168.

[365] Vgl. *Roxin*, AT II, S. 22 ff.

gelten Fälle der Teilnahme setzen objektiv jeweils eine vorsätzliche rechtswidrige Haupttat eines anderen und einen eigenen Beitrag des Teilnehmers hierzu voraus, subjektiv ist Vorsatz hinsichtlich der vorsätzlich rechtswidrigen Haupttat und hinsichtlich des Teilnehmerbeitrags erforderlich.[366] Bei Anschließungsdelikten knüpft der Vorfeldtäter an deliktisch intendiertes Verhalten des Herstellers oder Werbetreibenden an und leistet eben dadurch mit seiner Tathandlung einen Beitrag zu der vorweggenommenen und nicht normierten Zieltat eines anderen. Da die Zieltat nicht im objektiven Tatbestand verankert ist, ist auch kein diesbezüglicher Vorsatz des Vorfeldtäters erforderlich. Vorsatz ist nur hinsichtlich der Tathandlung *als Teilnahmebeitrag* erforderlich. Da die Tathandlung nur deshalb einen „Teilnahmebeitrag" darstellt, weil sie an deliktisch intendiertes Verhalten des Herstellers oder Werbetreibenden anknüpft, muss sich also auch der Vorsatz allein darauf beziehen, dass die Tathandlung an deliktisch intendiertes Verhalten anknüpft.

Rekonstruiert man das Anschließungsdelikt auf diese Weise, so wird deutlich, dass es sich hierbei – anders als bei den Vorbereitungsdelikten – nicht um den Spezialfall einer ausnahmsweise strafbaren versuchten Beihilfe handelt. Bei versuchter Beihilfe wäre weiterhin ein doppelter Gehilfenvorsatz erforderlich, also müsste sich dieser mutatis mutandis auch im entsprechenden Vorfelddelikt abzeichnen. Da dies in den Anschließungsdelikten nicht der Fall ist, sondern diese sich dadurch auszeichnen, dass sie die Zieltat weder im objektiven noch im subjektiven Tatbestand materialisieren, handelt es sich bei ihnen vielmehr um eine Form *nicht-akzessorischer Beihilfe*. Beim Anschließungsdelikt braucht der Vorfeldtäter nur einen Förderbeitrag zu leisten, ohne dass Akzessorietät zu irgendeiner Haupttat bestünde. Durch das Tatobjekt werden die Umstände präzisiert, unter denen die Tathandlung als Förderbeitrag anzusehen ist. In den Varianten des § 2 Nr. 3 ZKDSG und des § 95a Abs. 3 Nr. 1 und 3 UrhG liegen diese Umstände darin, dass der Vorfeldtäter es billigt, an deliktisch intendierte Handlungen des Herstellers oder Werbetreibenden anzuknüpfen. In der Variante des § 95a Abs. 3 Nr. 2 UrhG wird die Tathandlung allein wegen der objektivierten wirtschaftlichen Bewertung des Computerprogramms bereits als deliktischer Förderbeitrag eingestuft.

Damit gibt es bei den Anschließungsdelikten – anders als bei den Vorbereitungsdelikten – kein Problem der Rechtssicherheit in dem Sinne, dass gerichtliche Entscheidungen schwer vorhersehbar wären. Das Problem der Anschließungsdelikte besteht vielmehr darin, dass im Umgang mit Dual-Use-Software die gesetzgeberisch gewollten und sich abzeichnenden gerichtlichen Entscheidungen in Teilen unbillig sind.

---

366 Siehe nur *Roxin*, AT II, S. 128 ff.; LK-*Schünemann*, Vor § 26 Rn. 19 ff.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Vor allem der Mehrzweckaspekt der Dual-Use-Problematik, nämlich dass dasselbe Computerprogramm sowohl zu deliktischen als auch zu legalen (Test-)Zwecken verwendet werden kann und muss, wird in den Anschließungsdelikten völlig missachtet. Auf die Intention desjenigen, der mit tatbestandsmäßigen Computerprogrammen umgeht, wird in den Anschließungsdelikten überhaupt nicht abgestellt. In Dreipersonenverhältnissen aus Hersteller, Verkäufer (als Vorfeldtäter) und Verwender wird darüber hinaus auch nicht berücksichtigt, welchen intentionalen Bezug der Verkäufer (= Vorfeldtäter) zu den möglichen Absichten des Verwenders hat. Mit anderen Worten ist es egal, wenn der Verkäufer beabsichtigt oder sicher weiß, dass der Verwender mit dem verkauften Computerprogramm Zieldelikte begehen will. Ausschlaggebend sind allein die Intentionen früherer Glieder in der Kette, also des historischen Herstellers oder des Werbetreibenden.

Diese Konstruktion führt dazu, dass bestimmten Computerprogrammen die Verkehrsfähigkeit völlig entzogen wird, weil ihnen der Makel eines kriminellen historischen Herstellers anhaftet. Andere Computerprogramme, die von seriösen Herstellern produziert worden sind, können völlig frei zirkulieren. Dies verursacht sowohl unter dem Multifunktions- als auch dem Mehrzweckaspekt des Dual-Use-Phänomens Probleme. Dies soll an zwei Beispielen demonstriert werden: einerseits dem *VLC media player* der *VideoLAN Organization*, andererseits *AnyDVD* von *Slysoft*.

Der Multifunktionsaspekt wird am oben bereits erwähnten[367] *VLC media player* deutlich. Dieser ist ein Computerprogramm zur Wiedergabe von Multimedia-Inhalten (Mediaplayer). Er stellt neben einer Vielzahl von Funktionen auch die Programmbibliothek *libdvdcss* zur Verfügung, mittels derer die CSS-Verschlüsselung von DVDs umgangen werden kann, sodass man damit etwa die Länderkodierung einer DVD aushebeln kann. Da diese CSS-Verschlüsselung grundsätzlich als wirksame technische Schutzmaßnahme im Sinne des § 95a UrhG angesehen wird, ist ihre Umgehung gemäß § 108b Abs. 1 i.V.m. § 95a Abs. 1 UrhG strafbar.[368]

Ein Vorfeldtäter T, der um diese spezielle Eignung des *VLC media player* weiß und möglicherweise sogar gerade deshalb seinem Kunden K dieses Computerprogramm im Rahmen gewerblicher Software-Betreuung vermietet, macht sich dadurch aber nicht zwingend gemäß § 108b Abs. 2 UrhG strafbar – auch dann nicht, wenn er billigend in Kauf nimmt, dass sein Kunde das Programm urheber-

---

[367] Siehe Teil 1, I.B.1.a).

[368] Siehe nur OLG München GRUR-RR 2009, 86 f.; Leupold/Glossner-*Wiebe*, Teil 3 Rn. 218; ausführlich zur Auslegung des Tatbestands siehe oben I.B.4.a).

rechtswidrig zur Entschlüsselung des CSS nutzen werde.[369] Denn diese deliktische Eignung des Programms alleine ist in den Tatobjektbeschreibungen des § 95a Abs. 3 Nrn. 1–3 UrhG nicht ausreichend. Auch die deliktischen Intentionen des Vorfeldtäters T geben aufgrund der gewählten Deliktsstruktur keinen Ausschlag. Maßgeblich sind vielmehr die Ziele der Werbetreibenden (Nr. 1)[370] oder des Herstellers im weiteren Sinne (Nr. 3), hier also der *VideoLAN Organization*.

Dass die *VideoLAN Organization* den *VLC media player* im Sinne des § 95a Abs. 1 Nr. 3 UrhG hauptsächlich zur Umgehung technischer Schutzmaßnahmen hergestellt hat ist nicht anzunehmen. Hervorgegangen ist die Organisation aus einem studentischen Projekt an der École Centrale Paris.[371] Es ist anzunehmen, dass die hauptsächlichen Ziele der Programmierer das waren, wofür sie das Programm nun hervorheben: Es ist schlicht, schnell, leistungsfähig, gratis, spielt fast alle Formate ab und ist kompatibel mit vielen Betriebssystemen.[372] Auch nach wirtschaftlicher Betrachtungsweise (§ 95a Abs. 3 Nr. 2 UrhG) macht die Programmbibliothek *libdvdcss* nicht den ganz überwiegenden finanziellen Wert des Programms aus.

Damit macht sich T nur dann strafbar, wenn der *VLC media player* als Umgehungsvorrichtung beworben wird (§ 95a Abs. 3 Nr. 1 UrhG) und T dies in seinen Vorsatz aufgenommen hat. Dass der Hersteller selbst den Mediaplayer nicht als Umgehungsvorrichtung bewirbt, ist dabei noch unerheblich. Als Werbetreibender im Sinne des § 95a Abs. 3 Nr. 1 UrhG kommt grundsätzlich jeder in Betracht, da der Tatbestand hier keine einschränkenden Vorgaben macht.[373] Ließe sich also beweisen, dass der *VLC media player* beispielsweise in einem Internetforum oder auf einer bestimmten Homepage als Umgehungsvorrichtung beworben wird und T davon Kenntnis hatte, so erfüllt T den Tatbestand des § 108b Abs. 2 i.V.m. § 95a Abs. 3 Nr. 1 UrhG durch das Vermieten des Players.

Für das Rechtsgut ist es in der vorliegenden Konstellation aber völlig unerheblich, ob das Computerprogramm irgendwo als Umgehungssoftware beworben wird und noch unwichtiger ist es, ob T von der Werbung Kenntnis genommen hat. Entscheidend für die Gefährdung des Rechtsguts ist hier, dass T um die deliktische Eignung des Computerprogramms weiß, dass für ihn absehbar ist, dass das Computerprogramm deliktisch eingesetzt wird und dass er es dennoch vermietet. Vertat-

---

[369] Der *VLC media player* ist zwar kostenlos auf der offiziellen Produkthomepage erhältlich, sodass dessen Vermietung zu gewerblichen Zwecken allenfalls im Rahmen betrieblicher Software-Betreuung realistisch ist – dies ist für das vorliegende Argument jedoch nicht störend.

[370] Die Werbetreibenden müssen nicht zwingend im Auftrag des Herstellers agieren, vgl. oben I.B.6.a). Das Programm kann beispielsweise auch in Internetforen von Dritten als Umgehungsvorrichtung beworben werden.

[371] http://www.videolan.org/videolan/ [zuletzt abgerufen am 16.11.2014].

[372] Siehe http://www.videolan.org/vlc/ [zuletzt abgerufen am 16.11.2014].

[373] Vgl. oben I.B.6.

bestandlicht sind diese Kriterien aber nicht. Vielmehr hängt die Strafbarkeit davon ab, ob der Verkäufer oder Vermieter der Software zumindest billigend in Kauf nimmt, dass *die Werbetreibenden* illegale Ziele verfolgt hatten. Der *VLC media player* ist unter diesem Regelungsmodell ein deliktsgeeignetes, aber „makelloses" Computerprogramm und kann daher frei zirkulieren.

Eine unmittelbare Konsequenz ergibt sich auch für den Hersteller: Sobald der Player irgendwo als Umgehungssoftware beworben wird, verliert er seine Makellosigkeit. In dem Moment, in dem der Hersteller hiervon Kenntnis erlangt, macht er sich gemäß § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 1 UrhG strafbar, weil er ein Computerprogramm zu gewerblichen Zwecken herstellt, das als Umgehungsmittel beworben wird.[374] Ihm bleibt in diesem Moment nur der Ausweg, das Programm künftig ohne die inkriminierte Funktion weiter herzustellen. Bei *libdvdcss* und dem *VLC media player* mag dies angesichts der Tatsache, dass einige Linux-Distributionen von vornherein eine funktionsfähige Programmversion ohne *libdvdcss* beinhalten,[375] noch problemlos möglich erscheinen. Dramatisch aber ist es, wenn die inkriminierte Funktion integraler Bestandteil des Computerprogramms ist und nicht ohne weiteres vom Rest des Programms abgelöst werden kann. Nach geltender Rechtslage muss der Hersteller in diesem Moment die Produktion einstellen.

Der Mehrzweckaspekt wird am Beispiel *AnyDVD* sichtbar: *AnyDVD* ist ein Treiber, der alle gängigen Kopierschutzmechanismen und Benutzungsbeschränkungen auf DVDs, CDs und Blu-ray Discs quasi ausschaltet.[376] Anders als der *VLC media player* wird *AnyDVD* vom Hersteller *Slysoft* auch gerade für das Umgehen wirksamer technischer Schutzmaßnahmen beworben[377] und aus dem Gesamteindruck ergibt sich, dass *AnyDVD* gerade hierfür hergestellt wird.[378] Damit unterfällt *AnyDVD* dem § 95a Abs. 3 Nr. 1 und Nr. 3 UrhG, sodass gemäß § 108b Abs. 2 UrhG das Herstellen, Einführen, Verbreiten, Verkaufen und Vermieten strafbar ist, sofern es zu gewerblichen Zwecken erfolgt. Auch hier gilt dies wieder unabhängig von der Intention des Täters.

Ein Programmierer, der in einem auf Kopierschutzmaßnahmen spezialisierten Unternehmen an der Weiterentwicklung bestehender Schutzmaßnahmen arbeitet,

---

374 Vorausgesetzt, die *VideoLAN Organization* verfolgt gewerbliche Zwecke.

375 Siehe http://www.videolan.org/vlc/download-debian.html [zuletzt abgerufen am 16.11.2014].

376 Vgl. oben Teil 1, III.B.1a).

377 „AnyDVD ist ein Treiber, der im Hintergrund automatisch und unbemerkt eingelegte DVD-Filme entschlüsselt", „Entfernt Kopierschutz (CSS) und Ländercode (RPC) von DVDs", „Entfernt analogen Kopierschutz (Macrovision)", pp., siehe http://www.slysoft.com/de/anydvd.html [Stand: 14.5.2012, nunmehr abgewandelt, zuletzt abgerufen am 16.11.2014].

378 Siehe LG München I MMR 2008, 192 ff.; OLG München MMR 2009, 118; ausführliche Besprechung oben I.B.4.a)cc).

kann also *AnyDVD* nicht herunterladen, ohne sich strafbar zu machen. Dies gilt auch, wenn er nur die Funktionsweise von *AnyDVD* analysieren oder es auf den Prototypen einer neuen Schutzmaßnahme testweise anwenden will.[379]

Eine Lösung dieses Problems könnte in dem Merkmal „zu gewerblichen Zwecken" gesucht werden. Nach ständiger Rechtsprechung handelt derjenige zu gewerblichen Zwecken, der sich aus wiederholter Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang verschaffen möchte.[380] Für den Vorfeldtäter muss hier also die Einnahmequelle gerade aus dem Vermieten oder Einführen stammen.

Für den Kopierschutzprogrammierer, der sich einen Kopierschutzknacker zu Testzwecken von einem ausländischen Server herunterlädt, kann die Gewerblichkeit jedoch nicht schon deshalb verneint werden, weil aus dem Einführen noch keine unmittelbare finanzielle Einnahme resultiert. Dies gälte nämlich auch für den eigentlich anvisierten deliktisch gesinnten Vorfeldtäter. Vielmehr ließe sich hier argumentieren, dass der Programmierer seine Einnahmequelle nicht in dem wiederholten Einführen von Kopierschutzknackern hat, sondern erst in dem anschließenden Weiterentwickeln der Kopierschutzmaßnahmen. Beim deliktisch gesinnten Vorfeldtäter resultiert die Einnahme dagegen aus dem Einsatz der Software oder dem Weiterhandel mit ihr. Diese Argumentation ist allerdings zweischneidig, denn wenn man den Gesamtvorgang aus Einführen und Anschlusshandlung betrachtet und nach der rechtlichen Bewertung der Anschlusshandlung entscheidet, ob bereits das *Einführen* „zu gewerblichen Zwecken" erfolgt, entfernt man sich zum einen weit vom eigentlichen Wortlaut, zum anderen führt man einen deliktischen intentionalen Bezug im Anschließungsmodell „durch die Hintertür" ein. Dies ist vom Gesetzgeber jedoch offensichtlich nicht gewollt, sonst hätte er kein Anschließungsdelikt konzipiert.

Für den deliktisch gesinnten Vermieter „makelloser" Software (wie oben des *VLC media player*) gibt das Merkmal der Gewerblichkeit ohnehin keine Handhabe. Selbstverständlich handelt er zu gewerblichen Zwecken, jedoch kann dies nicht darüber hinweghelfen, dass kein taugliches Tatobjekt vorliegt. Der deliktisch gesinnte Vermieter oder Einführer „makelloser" Software geht daher immer straffrei aus.

---

[379] *Ziemann/Ziethen* sehen zumindest bei der Aufgabe des Besitzes von Waffen und Drogen einen Weg aus dem strafbewehrten Umgangsverbot darin, die zuständige Behörde zu informieren und zur Abholung aufzufordern, JR 2011, 67. Im IT-Strafrecht scheitert dieser Ansatz daran, dass es mehr legitime Tathandlungen gibt als die bloße Besitzaufgabe und vor allem daran, dass es keine zuständige Behörde zur Genehmigung eines Umgangs mit Schadsoftware gibt.

[380] Siehe nur BGHSt 1, 383; BGH NJW 2004, 1679.

II. Europäische Instrumente

Im vorstehenden Kapitel wurden die Regelungstechniken der Software-Delikte im deutschen Strafrecht erörtert. Die Analyse hat gezeigt, dass in den nationalen Software-Delikten sehr unterschiedliche Techniken eingesetzt wurden, um die Weite der Tatbestände zu bestimmen. Dabei ist häufig nicht klar, weshalb der Gesetzgeber sich für oder gegen eine Regelungstechnik entscheidet, und gelegentlich ist gänzlich unklar, ob die konkrete Regelung überhaupt das wiedergibt, was der Gesetzgeber regeln wollte. Eine übergreifende Systematik, Konzeption oder Strategie zur Regulierung gefährlicher Computerprogramme konnte jedenfalls nicht festgestellt werden.

Beinahe allen Software-Delikten ist gemein, dass sie Vorläufer in internationalen Harmonisierungsinstrumenten haben. Sowohl der Europarat als auch die Europäische Union haben Konventionen beziehungsweise Rahmenbeschlüsse und Richtlinien angenommen, in denen die konkreten Software-Delikte des deutschen Strafrechts vorgezeichnet wurden.

In diesem Kapitel II sollen deshalb die Normen aus dem Recht der genannten europäischen Institutionen untersucht werden, in denen die Mitgliedsstaaten verpflichtet wurden, einen bestimmten Umgang mit bestimmten Computerprogrammen zu sanktionieren. Dies soll aufzeigen, welche abweichenden Ansätze der Europarat und die Europäische Union bei der Regulierung gefährlicher Software angesichts der Dual-Use-Problematik verfolgt haben. Darüber hinaus kann dies möglicherweise erklären, worauf manche Eigenart der Regelungstechniken im deutschen Software-Strafrecht zurückzuführen ist. Unter diesen beiden Aspekten liefert die Analyse weiteres Material für den wertenden Vergleich von Regelungstechniken für Software-Delikte in Teil 4 dieser Arbeit.

Soweit im Folgenden von „Software-Delikten“ des „europäischen Strafrechts“ gesprochen wird, sind beide Begriffe nur bei einem weiten Verständnis zutreffend. Internationale Instrumente beinhalten offensichtlich keine Tatbestände, aus denen ein Bürger unmittelbar bestraft werden könnte.[381] Vielmehr erfordern sie alle eine irgendwie geartete Umsetzung in nationales Recht, um dort zu Delikten im eigentlichen Sinne zu werden. Dennoch handelt es sich schon bei den internationalen Normen um Regelungen, die von Anfang an darauf ausgerichtet sind, zu nationalen Verbotsnormen oder Straftatbeständen umgesetzt zu werden. Meist sind diese Normen so detailliert ausgestaltet, dass es den nationalen Gesetzgebern offen steht, sie wortgetreu als Straftatbestände ins nationale Recht zu übernehmen. Insofern stellt sich den internationalen Normgebern beim Erlass solch konkreter Harmonisierungsinstrumente dieselbe Herausforderung in Anbetracht der Dual-Use-Problematik, der sich auch nationale Gesetzgeber beim Erlass von Straftatbeständen

---

[381] So auch *Vogel*, GA 2002, 517.

gegenüber sehen: eine Formulierung der Norm zu finden, die illegitimes Verhalten erfasst, ohne legitimes Verhalten zu verbieten. Internationale und nationale Gesetzgeber stehen also vor demselben Sachproblem, sodass ihre Mittel – die unterschiedlichen Regelungstechniken zur Bewältigung dieses Problems – vergleichbar sind.

Das „europäische IT-Strafrecht" ist dabei schon deshalb kein homogenes Rechtsgebiet, weil es aus den Federn unterschiedlicher Normgeber stammt. Die Rechtsnatur der Instrumente ist unterschiedlich und ihre Bindungswirkung für die Mitgliedsstaaten verschieden. Gemein ist den Instrumenten, dass sie das Sanktionenrecht (nicht zwingend: Strafrecht) der jeweiligen Mitgliedsstaaten harmonisieren sollen, indem sie diese verpflichten, bestimmte Verhaltensweisen zu verbieten und für Verstöße Sanktionen vorzusehen. Nur teilweise wird zwingend Strafe angeordnet.

Bei dieser europäischen Strafrechtsharmonisierung ergänzen sich kooperative und integrative Modelle: In kooperativen Modellen verstärken Staaten vor allem ihre institutionelle Zusammenarbeit, etwa in der Rechtshilfe; in integrativen Modellen gleichen die Staaten überdies ihre nationalen Rechtsordnungen einander an.[382] An einer internationalen Strafrechtsdogmatik fehlt es dagegen noch.[383]

In diesem Kapitel werden zunächst die internationalen Instrumente genannt, in denen sich Regelungen zu Software-Delikten finden (A.). Anschließend werden wie schon in Kapitel I die unterschiedlichen Regelungstechniken für das Tatobjekt (B.) und für die subjektive Tatseite (C.) erläutert. Die jeweiligen Tatbestände werden in ihrer englischen und deutschen Sprachfassung analysiert, da sich oftmals Unregelmäßigkeiten in den deutschen Übersetzungen der englischen Ausgangstexte finden. So sollen Missverständnisse aufgrund von Übersetzungsfehlern vermeiden werden. Zugleich finden sich dadurch Lösungsansätze für Unregelmäßigkeiten und Missverständnisse, wenn diese sich nicht nur in der deutschen Fassung eines internationalen Instruments finden, sondern sich auch in der Implementation ins nationale deutsche Recht fortgesetzt haben.

In der Auslegung muss methodisch freilich berücksichtigt werden, dass es sich bei den Normen nicht um nationale Gesetze, sondern um Normen des Völkerrechts und des europäischen Sekundärrechts handelt.[384] Besonderes Gewicht kommt dabei der grammatischen Auslegung des Normtextes zu.[385] Die verwendeten Begriffe

---

382 Siehe *Sieber*, Rechtstheorie 41 (2010), 180 ff; *ders.*, ZStW 119 (2007), 7 ff.

383 *Mylonopoulos*, ZStW 121 (2009), 68 ff., plädiert für die Entwicklung einer solchen Dogmatik, namentlich um unabdingbare Rechtsprinzipien der nationalen Rechtsordnungen auch auf internationaler Ebene zur Geltung zu bringen, S. 85; *Vogel* hält sie für bereits existent, fordert aber eine Konzentration auf konkrete Sachfragen, nicht auf Systematisierungen und Kategorisierungen, GA 2002, 519 ff.

384 So auch *Schroeder*, JuS 2004, 181; *von Westphalen*, AnwBl 2008, 5.

385 *Kohler-Gehrig*, JA 1998, 809; *von Westphalen*, AnwBl 2008, 5.

sind hier nicht an nationalstaatliches Vorverständnis gebunden, sondern es ist jeweils von einem autonomen Wortsinn aus objektivierter internationaler Sicht auszugehen.[386] Die ebenso anzuwendende systematische Auslegungsmethode verlangt, dass europäisches Sekundärrecht primärrechtskonform ausgelegt wird und dass im systematischen Zusammenhang mit anderen Normen Widersprüche innerhalb der Rechtsordnung durch Auslegung vermieden werden.[387]

Ergänzend wird schließlich die teleologische Auslegungsmethode herangezogen, die bei Richtlinien der EG besonders durch die Orientierung am *effet utile* geprägt ist.[388] Freilich steht es immer im Vordergrund internationaler Harmonisierungsinstrumente, die Rechtsvorschriften innerhalb der Mitgliedsstaaten anzugleichen.[389] Dieses Telos ist jedoch bei der Auslegung des internationalen Instruments weniger ergiebig als bei der Auslegung des nationalen Umsetzungsgesetzes.[390] Aufschlussreicher ist es, das bereichsspezifische Telos des internationalen Instruments festzustellen und daran die Auslegung anzulehnen. In den vorliegenden Normen liegt dieses bereichsspezifische Telos – jeweils mit eigenen Nuancen – in der Eindämmung der Verbreitung von Schadsoftware und wird in den Erwägungsgründen im Einzelnen ausgeführt.[391] Bei mehreren Sprachfassungen sind zumindest im EU-Recht alle Versionen verbindlich.[392]

Allerdings ist ebenso zu berücksichtigen, dass in der vorliegenden Arbeit andere Ziele verfolgt werden als dies bei der Auslegung internationaler Instrumente typischerweise der Fall ist. Harmonisierende Rahmenbeschlüsse, Konventionen oder Richtlinien verpflichteten und verpflichten ihre Mitgliedsstaaten, eine bestimmte rechtliche Regelung zu treffen. Deshalb ist das Ziel der Auslegung internationalen Rechts typischerweise, das Maß und den Inhalt der rechtlichen Bindung zu ermitteln, etwa um zu überprüfen, ob die nationalen Regelungen eines Staates den internationalen Vorgaben entsprechen. In dieser Arbeit geht es jedoch darum, Regelungstechniken zu analysieren, mit denen der Normgeber die Dual-Use-Problematik bewältigen will. Insbesondere mit dieser Zielsetzung werden die Tatbestandsmerkmale nachfolgend ausgelegt.

---

386 Vgl. EuGH Slg 1980, 75, 84; EuGH Slg 1983, 987, 1002; Die Entscheidungen beziehen sich zwar auf Gemeinschaftsrecht, jedoch kann für Unionsrecht auch nach dem Vertrag von Lissabon und für Rechtsakte des Europarats diesbezüglich nichts anderes gelten.

387 *Kohler-Gehrig*, JA 1998, 810.

388 *Herdegen*, Europarecht 13. Aufl., S. 184; *Kohler-Gehrig*, JA 1998, 810.

389 *von Westphalen*, AnwBl 2008, 5.

390 Missverständlich insoweit *von Westphalen*, AnwBl 2008, 5.

391 Vgl. *Frenz*, Handbuch Europarecht, Bd. 6 Rn. 414; *Leisner*, EuR 2007, 698 ff.

392 *Schroeder*, JuS 2004, 185.

A. Überblick

Internationale Vereinbarungen zum Erlass von Software-Delikten finden sich in zwei Konventionen des Europarats, in Rahmenbeschlüssen des Rates der EU, in Richtlinien des Europäischen Parlaments und des Rates der EU sowie in einem Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates.

1. Instrumente des Europarats

Auf Ebene des Europarats haben die Unterzeichnerstaaten zweier Konventionen die Einführung von Software-Delikten vereinbart, nämlich in Art. 2 der Conditional-Access-Konvention sowie in Art. 6 des Übereinkommens über Computerkriminalität (Cybercrime Convention, CCC). Die Conditional-Access-Konvention des Europarats vom 24. Januar 2001, ETS Nr. 178, soll im Wesentlichen das Pay-TV schützen, also verschlüsselte Rundfunkdienste und ähnliche Dienste, zu denen der Kunde nur gegen ein Entgelt Zugang erhält. Die Konvention sieht ein Software-Delikt in Art. 4, Art. 2 lit. (d) vor, in dem der Umgang mit bestimmten Entschlüsselungsprogrammen unter Strafe gestellt wird. Das Übereinkommen über Computerkriminalität des Europarats vom 23. November 2001, ETS Nr. 185, ist das erste und bis heute prägendste Instrument zur international koordinierten Bekämpfung der Computerkriminalität.[393] Die Cybercrime Convention[394] enthält Regelungen zum materiellen Strafrecht (Art. 2–13 CCC), Strafprozessrecht (Art. 14–21 CCC), zur Gerichtsbarkeit (Art. 22 CCC) und zur internationalen Zusammenarbeit (Art. 23–35 CCC). In Art. 6 CCC enthält sie den Tatbestand des „Misuse of devices", in der deutschen Fassung „Missbrauch von Vorrichtungen" genannt, der den Umgang mit bestimmten Computerprogrammen im Vorfeld von CIA-Delikten unter Strafe stellt.

Der Europarat ist eine klassische internationale Organisation, die sich in Art. 1 lit. a ihrer Satzung die Aufgabe gegeben hat, einen engeren Zusammenschluss unter ihren Mitgliedern zu verwirklichen, um die Ideale und Grundsätze, die ihr gemeinsames Erbe sind, zu schützen und zu fördern, um ihren wirtschaftlichen und sozialen Fortschritt zu begünstigen.[395] Gemäß Art. 1 lit. b der Satzung setzt sie zu diesem Zweck verschiedene Mittel ein, darunter den Abschluss von Abkommen. Derzeit sind 47 europäische Staaten Mitglied des Europarats, darunter alle 27 EU-Mitgliedsstaaten.[396] Als traditionelle internationale Organisation kann der Europa-

---

393 *Hilgendorf/Frank/Valerius*, Computerstrafrecht, S. 29.

394 In manchen Ländern auch nach dem Unterzeichnungsort als Budapest-Konvention bezeichnet.

395 Vgl. *Hecker*, Europäisches Strafrecht, S. 77; *Herdegen*, Europarecht, S. 8; *Jung*, JuS 2000, 418.

396 http://www.coe.int/de/web/portal/47-members-states [zuletzt abgerufen am 16.11. 2014].

rat nicht selbst Rechtsvorschriften mit unmittelbarer Geltung in den Mitgliedsstaaten erlassen. Vielmehr ist er darauf beschränkt, ein Forum für die Aushandlung von völkerrechtlichen Verträgen zu bieten und als Moderator zu fungieren, um Kompromisse zu ermöglichen, die von allen Mitgliedsstaaten unterzeichnet und ratifiziert werden können.[397]

In Art. 36 CCC tritt auch die Rechtsnatur der Cybercrime Convention zutage. Es handelt sich um ein völkerrechtliches Übereinkommen, das am 23. November 2001 zur Unterzeichnung durch die Mitgliedsstaaten und alle Nichtmitgliedsstaaten, die sich an seiner Ausarbeitung beteiligt haben, aufgelegt wurde (Abs. 1). Es bedarf der Ratifikation, Annahme oder Genehmigung (Abs. 2) und tritt in Kraft, nachdem mindestens fünf Staaten, darunter mindestens drei Mitgliedsstaaten des Europarats unterzeichnet und ratifiziert haben (Abs. 3). Dies war zum 1. Juli 2004 der Fall. Zu den unterzeichnenden Nichtmitgliedsstaaten zählen heute Kanada, Japan, Südafrika und die Vereinigten Staaten von Amerika.[398] Drittstaaten, die weder Mitglied des Europarats sind noch an der Ausarbeitung des Übereinkommens beteiligt waren, können gemäß Art. 37 CCC auf Einladung des Ministerkomitees des Europarats und nach Konsultation und einhelliger Zustimmung der Vertragsstaaten beitreten. Die Bundesrepublik Deutschland hatte das Übereinkommen bereits am 23. November 2001 unterzeichnet, es jedoch erst zum 9. März 2009 ratifiziert. Gemäß Art. 36 Abs. 4 CCC trat es für die Bundesrepublik zum 1. Juli 2009 in Kraft, womit es völkerrechtliche Bindungswirkung entfaltete,[399] die nur durch Kündigung nach Art. 47 CCC wieder zu beseitigen ist.[400]

Für die Auslegung eines internationalen Rechtsinstruments sind seine amtlichen Fassungen unmittelbar maßgebend und stehen gleichberechtigt nebeneinander. Amtliche Übersetzungen dieser ursprünglichen Fassungen können allenfalls mittelbar als Auslegungshilfe herangezogen werden.[401] Amtssprachen des Europarats sind Englisch und Französisch, für die Cybercrime Convention liegt jedoch eine amtliche Übersetzung ins Deutsche vor.[402] Daher wird hier die englische Ausgangsfassung besonders im Vordergrund stehen.

---

397 Vgl. *Gercke*, in: Gercke/Brunst, Praxishandbuch Internetstrafrecht, Rn. 63 f; *Hecker*, Europäisches Strafrecht, S. 80; *Hilgendorf/Frank/Valerius*, Computerstrafrecht, S. 28.

398 Vgl. Übersicht des Europarats, online abrufbar unter http://conventions.coe.int/Treaty/ Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [zuletzt abgerufen am 16.11.2014].

399 Vgl. *Dahm*, Völkerrecht I/3, S. 600 ff.

400 Die Wiener Vertragskonvention verwendet bei multilateralen Verträgen den Terminus „Rücktritt", siehe *Dahm*, Völkerrecht I/3, S. 721; siehe auch *Ipsen*, Völkerrecht, S. 124 ff., 136 f., 194 ff.

401 *von Westphalen*, AnwBl 2008, 5.

402 Siehe http://www.conventions.coe.int/Default.asp?pg=Treaty/Translations/TranslationsChart_en.htm#185 [zuletzt abgerufen am 16.11.2014].

2. Instrumente der Europäischen Union

Im Rahmen der EU wurde das Software-Strafrecht bislang nach dem Recht *vor* Inkrafttreten des Vertrags von Lissabon harmonisiert. Zu dieser Zeit hatte die EU keine Ermächtigung zur Harmonisierung des Strafrechts durch den Erlass von Richtlinien. Vielmehr war dies allein in der Polizeilichen und Justiziellen Zusammenarbeit angesiedelt, war also Teil der Dritten Säule, die stark intergouvernemental geprägt war. In Art. 29 Abs. 1 EUV-*vor-Lissabon* war die Schaffung eines „Raumes der Freiheit, der Sicherheit und des Rechts" als Ziel ausgegeben worden. Die strafrechtliche Harmonisierung fand hier durch völkerrechtliche Rahmenbeschlüsse statt, welche nach dem Einstimmigkeitsprinzip getroffen werden mussten.[403] Gemäß Art. 34 Abs. 2 lit. b) Satz 1 EUV-*vor-Lissabon* waren Rahmenbeschlüsse für die Mitgliedsstaaten hinsichtlich der zu erreichenden Ziele, nicht aber hinsichtlich der Wahl der Form und Mittel der Umsetzung verbindlich.[404] Gleiches galt für Richtlinien gemäß Art. 249 Abs. 3 EGV-*vor-Lissabon*. Für Rahmenbeschlüsse war in Art. 34 Abs. 2 lit. b) Satz 2 EUV-*vor-Lissabon* ausdrücklich festgehalten, dass sie nicht unmittelbar wirksam sind. Dies galt jedoch grundsätzlich auch für Richtlinien,[405] sodass beide Instrumente einer Umsetzung in nationales Recht bedurften und hierzu auch die Mitgliedsstaaten verpflichteten.[406]

Durch den Vertrag von Lissabon wurden zum Teil Bereiche vergemeinschaftet, die zuvor der Polizeilichen und Justiziellen Zusammenarbeit zugehörig waren.[407] Art. 3 Abs. 2 EUV statuiert nun, dass die Union ihren Bürgern den „Raum der Freiheit, der Sicherheit und des Rechts" bietet. Die Justizielle Zusammenarbeit in Strafsachen ist nun in den Art. 82 f. AEUV geregelt. Gemäß Art. 83 Abs. 1 Satz 1 AEUV können das Europäische Parlament und der Rat „durch Richtlinien Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität festlegen, die aufgrund der Art oder der Auswirkungen der Straftaten oder aufgrund einer besonderen Notwendigkeit, sie auf einer gemeinsamen Grundlage zu bekämpfen, eine grenzüberschreitende Dimension haben". Hierzu zählen nach Satz 2 unter anderem die hier relevanten Fälschungen von Zahlungsmitteln, die Organisierte Kriminalität und vor allem die Computerkriminalität. Nach Art. 83 Abs. 3 AEUV kann ein Mitglied des Rates der EU ein Gesetzgebungsverfahren aussetzen, wenn es der Auffassung ist, dass der Richtlinienentwurf grundlegende Aspekte der eigenen Strafrechtsordnung berühren würde. Hierzu muss es beantragen, dass der Europäische Rat mit dem Entwurf befasst wird. Die Rechtswirkung von Richtlinien hat sich durch den Vertrag von Lissabon nicht

---

403 *Herdegen*, Europarecht, 11. Aufl., S. 439.

404 Vgl. ebd.; *Streinz*, Europarecht, Rn. 433.

405 Mit Ausnahme individuell begünstigender Richtlinien unter bestimmten Voraussetzungen, vgl. *Satzger*, Europäisierung des Strafrechts, S. 90 f.

406 *Herdegen*, Europarecht, 11. Aufl., S. 440.

407 *Herdegen*, Europarecht, 13. Aufl., S. 316.

geändert, sie sind weiterhin nur hinsichtlich ihres Ziels verbindlich, machen aber keine Vorgaben zu Form und Mittel der Umsetzung.[408]

Rahmenbeschlüsse und Richtlinien, die noch nach altem Recht, also vor Inkrafttreten des Vertrags von Lissabon, erlassen worden sind, gelten fort, bis sie unter Anwendung des neuen Rechts aufgehoben, für nichtig erklärt oder geändert werden, Art. 9 Satz 1 des Protokolls (Nr. 36) über die Übergangsbestimmungen.[409] Eine erste strafrechtsharmonisierende Richtlinie nach neuem Recht über Angriffe auf Informationssysteme befindet sich gerade in der Entwurfs- und Verhandlungsphase.[410]

a) Rahmenbeschlüsse

Für die vorliegende Arbeit sind zwei Rahmenbeschlüsse relevant. Dies ist erstens der Rahmenbeschluss 2000/383/JI des Rates der Europäischen Union vom 29. Mai 2000 über die Verstärkung des mit strafrechtlichen und anderen Sanktionen bewehrten Schutzes gegen Geldfälschung im Hinblick auf die Einführung des Euro. Dieser stellt den Vorläufer des deutschen § 149 Abs. 1 StGB dar und sieht in Art. 3 Abs. 1 lit. d, 1. Spiegelstrich ein Delikt für den betrügerischen Umgang mit bestimmten Geldfälschungswerkzeugen vor. Zweitens ist der Rahmenbeschluss 2001/413/JI des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln relevant. Dieser ist der Vorläufer des deutschen § 263a Abs. 3 StGB sowie des § 149 Abs. 1 i.V.m. §§ 151, 152a und 152b StGB. Der Rahmenbeschluss sieht zum einen ein Delikt für den betrügerischen Umgang mit bestimmten Computerprogrammen zur Fälschung anderer Zahlungsinstrumente als Geld vor, Art. 4 Abs. 2, 1. Spiegelstrich, sowie ein Delikt für den betrügerischen Umgang mit Computerprogrammen, deren Zweck ein Computerbetrug ist, Art. 4 Abs. 2, 2. Spiegelstrich.

b) Richtlinien

Relevante Richtlinien sind hier zum einen die Richtlinie 98/84/EG des Europäischen Parlaments und des Rates vom 20. November 1998 über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (Conditional-Access-Richtlinie). Diese ist Vorläufer des deutschen ZKDSG und enthält in Art. 4 ein Verbot bestimmter Handlungen in Bezug auf Umgehungsvorrichtungen für geschützte Dienste. Die zweite relevante Richtlinie ist die Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte

---

[408] *Satzger,* in: Sieber, Europäisches Strafrecht, S. 110.

[409] Vgl. *Herdegen*, Europarecht, 13. Aufl., S. 317.

[410] KOM(2010), 517 endgültig. Siehe Näheres dazu unten b).

in der Informationsgesellschaft. Diese ist das Vorbild für den deutschen § 108b Abs. 2 i.V.m. § 95a Abs. 3 UrhG[411] und enthält ein Verbot des Umgangs mit Umgehungsvorrichtungen für technische Schutzmaßnahmen in Art. 6 Abs. 2.

Wie oben beschrieben, können diese Richtlinien aus der Zeit vor dem Vertrag von Lissabon das Strafrecht nicht harmonisieren. Ihr Ziel bestand darin, aus der Binnenmarkt-Perspektive der EG einige Aspekte der grenzüberschreitenden Rundfunkdienste und „Dienste der Informationsgesellschaft" beziehungsweise des Urheberrechts in der Informationsgesellschaft zu harmonisieren. Dementsprechend schreiben beide Richtlinien lediglich wirksame, verhältnismäßige und abschreckende Sanktionen als Harmonisierungsziel vor.[412] Dies ließe sich grundsätzlich auch durch rein zivilrechtliche Regelungen erreichen, jedoch hat sich der deutsche Gesetzgeber dafür entschieden, die Verbotsnormen aus den Richtlinien mit dem rechtspolitischen Mittel des Strafrechts umzusetzen.[413]

In der Literatur wird teilweise vertreten, dass die Wahl des Strafrechts bei der Richtlinie zum Urheberrecht in der Informationsgesellschaft nicht nötig gewesen wäre. So wird darauf hingewiesen, dass schon nach Rechtslage *vor* der Umsetzung der Richtlinie das Herstellen und Vertreiben von Umgehungsmitteln als mittelbare Rechtsgutsverletzung anzusehen war, sodass der Rechtsinhaber bei konkret drohender Erstbegehungsgefahr bereits einen Unterlassungsanspruch gegen den „Vorfeldtäter" gemäß § 97 Abs. 1 UrhG hatte.[414] Die Neuregelung einer entsprechenden Verbotsnorm hatte demnach lediglich klarstellende Funktion und war überflüssig.[415]

Gegen diese Ansicht wird eingewandt, dass der Gesetzgeber wegen seiner Entscheidung für Strafnormen bei der Umsetzung der Conditional-Access-Richtlinie auch bei der Umsetzung des Art. 6 Abs. 2 Info-RL zwingend zu Strafvorschriften greifen musste. Das Gleichstellungsgebot aus der EuGH-Rechtsprechung erfordere, dass Verstöße gegen Gemeinschaftsrecht sachlich und verfahrensrechtlich gleichartig geahndet werden.[416] Da sich der deutsche Gesetzgeber beim Erlass des ZKDSG dazu entschlossen habe, die Vorgaben der Conditional-Access-Richtlinie als Strafvorschrift umzusetzen (§ 4 ZKDSG), sei der Ermessensspielraum bei der Umsetzung der Info-RL entsprechend reduziert gewesen. Sowohl Conditional-

---

411 Zur Entstehungsgeschichte siehe *Hilty*, ZUM 2003, 983 ff.; *Hoeren*, MMR 2000, 515 ff.; *Mayer*, EuZW 2002, 325 ff.

412 Vgl. Erwägungsgrund 18 der Richtlinie 1998/84/EG und Erwägungsgrund 58 der Richtlinie 2001/29/EG.

413 Bei der Umsetzung einer Richtlinie ist der Gesetzgeber in der Wahl der Mittel frei, vgl. oben II.A.2. a.A.

414 *Haedicke*, FS für Dietz, S. 359.

415 Ebd.

416 *Hänel*, Umsetzung des Art. 6, S. 197 mit Verweis auf EuGH Rs. 102/79, Slg. 1980, 1473 Rn. 10; EuGH Rs. 68/88, Slg. 1989, 2965 Rn. 24; EuGH Rs. 326/88, Slg. 1990, I-2911 Rn. 17; EuGH Rs. 186/98, Slg. 1999, I-4883 Rn. 14.

Access- als auch die Richtlinie zum Urheberrecht in der Informationsgesellschaft schützen nämlich Einnahmequellen eines Diensteerbringers bzw. Urhebers, für die es zwingend erforderlich sei, dass die Integrität der technischen Maßnahmen zum Schutze dieses Dienstes gewahrt werde. Die Bedrohung sei in beiden Fällen ähnlich intensiv. Da beide Vorgaben zudem aus gleichartigen Quellen, nämlich EU-Richtlinien, stammen, erfordere das Gleichstellungsgebot hier eine Umsetzung der Verbotstatbestände aus der Info-RL als Strafnormen.[417]

Diese Frage soll hier jedoch nicht weiter vertieft werden. Vielmehr soll im Folgenden untersucht werden, welche gesetzestechnischen Mittel die europäischen Normgeber (Europarat, Rat der EU, Europäisches Parlament mit dem Rat der EU) angewandt haben, um in ihren jeweiligen Instrumenten die Dual-Use-Problematik angemessen zu lösen.

B. Die objektive Umschreibung tatbestandlicher Computerprogramme

Die Normgeber der internationalen Instrumente haben in den Software-Delikten jeweils unterschiedlich nuanciert, welche Computerprogramme als taugliche Tatobjekte erfasst werden sollen. Sechs verschiedene rechtstechnische Modelle zeichnen sich hierbei ab. Diese werden nachfolgend erörtert, damit aufgezeigt werden kann, inwiefern sie sich jeweils in der Handhabung der Dual-Use-Problematik auf Ebene des Tatobjekts unterscheiden.

Wie in Teil 3, Kapitel I. der Arbeit werden auch hier jeweils die Charakteristika eines Regelungsmodells herausgearbeitet (a). Sodann wird erörtert, wie sich diese Charakteristika auf die Dual-Use-Problematik auswirken (b). Dies soll freilich ohne Würdigung der europäischen Kriminalpolitik erfolgen.[418]

1. "A computer program which is designed or adapted to [the offence]"

In einem ersten Modell werden Computerprogramme als Tatobjekte erfasst, die für die Verwirklichung der Zieltat entworfen *(designed)* oder angepasst *(adapted)* sind. Dieses Tatobjektmodell wird in Art. 4, Art. 2 lit. (e) der Richtlinie 98/84/EG (Conditional-Access-Richtlinie) vom 20. November 1998 verwendet und wurde später in einer entsprechenden Conditional-Access-Konvention des Europarats vom 24. Januar 2001 (ETS Nr. 178) übernommen. In beiden Instrumenten werden die Mitgliedsstaaten verpflichtet, bestimmte Handlungen im Umgang mit *illicit devices*

---

417 *Hänel*, ebd.

418 Siehe hierzu die scharfe Kritik an der EU-Kriminalpolitik von *Duttge*, FS für Weber, S. 285 ff.; vermittelnd *Vogel*, GA 2002, 517 ff.

zu verbieten. Art. 2 lit. (e) der Richtlinie 98/84/EG und der insoweit übereinstimmende Art. 2 lit. (d) der Conditional-Access-Konvention des Europarats spezifizieren das Tatobjekt *illicit device*, während jeweils die übrigen Tatbestandsmerkmale in Art. 4 RL 98/84/EG beziehungsweise Art. 4 der Conditional-Access-Konvention enthalten sind. Beispielhaft sei für die Rechtstechnik hier ein Auszug aus der Richtlinie 98/84/EG im Wortlaut wiedergegeben:

Article 4 Infringing activities

Member States shall prohibit on their territory all of the following activities:

(a) the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices;

(b) the installation, maintenance or replacement for commercial purposes of an illicit device;

(c) the use of commercial communications to promote illicit devices.

Art. 2 lit. (e) RL 98/84/EG statuiert, was mit *illicit device* gemeint ist:

Article 2 Definitions

For the purposes of this Directive […]

(e) *illicit device* shall mean any equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorisation of the service provider;

Die deutsche Fassung des Art. 4 RL 98/84/EG hält sich weitgehend wortgleich an die englische Vorgabe:

Artikel 4 Zuwiderhandlungen

Die Mitgliedstaaten verbieten in ihrem Hoheitsgebiet folgende Handlungen:

a) Herstellung, Einfuhr, Vertrieb, Verkauf, Vermietung oder Besitz illegaler Vorrichtungen zu gewerblichen Zwecken;

b) Installierung, Wartung oder Austausch illegaler Vorrichtungen zu gewerblichen Zwecken;

c) Einsatz der kommerziellen Kommunikation zur Förderung des Inverkehrbringens illegaler Vorrichtungen.

In der Begriffsbestimmung des Art. 2 lit. (e) RL 98/84/EG finden sich allerdings inhaltliche Abweichungen:

Artikel 2 Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck […]

e) „*illegale Vorrichtung*“ jedes Gerät oder Computerprogramm, das dazu bestimmt oder entsprechend angepaßt ist, um den Zugang zu einem geschützten Dienst in verständlicher Form ohne Erlaubnis des Diensteanbieters zu ermöglichen;

a) Charakteristika dieses Regelungsmodells

Die deutsche Fassung der Richtlinie wurde im deutschen ZKDSG wortgetreu übernommen. In der Analyse der Rechtstechniken dieses Tatbestandsmodells stellen sich auf europäischer Ebene daher keine anderen Probleme als im nationalen

Recht.[419] Anders als das deutsche ZKDSG definieren die Conditional-Access-Richtlinie und die Conditional-Access-Konvention jeweils nicht nur das „illicit device“ (illegale Vorrichtung), sondern zuvor deren legitime Variante, nämlich das „conditional access device“ (Zugangskontrollvorrichtung), Art. 2 lit. (c) RL 98/84/EG und Art. 2 lit. c Conditional-Access-Konvention. Dort heißt es im Wesentlichen übereinstimmend: “‘[C]onditional access device’ shall mean any equipment or software designed or adapted to give access in an intelligible form to a protected service in an intelligible form.”

Interessanterweise weicht aber die amtliche deutsche Fassung der Richtlinie von der amtlichen englischen Fassung in zwei Punkten entschieden ab: Erstens spricht die englische Fassung vom *Design* der Umgehungsvorrichtung, nicht von ihrer *Bestimmung*. Zweitens muss die Vorrichtung in der englischen Fassung dazu entworfen oder angepasst sein, Zugang zu kontrollierten Diensten zu *verschaffen (give access)*, statt den Zugang zu den Diensten zu *ermöglichen*.

Durch die erste Abweichung in der deutschen Fassung wird die schwierige Frage aufgeworfen, welchen genauen Inhalt das Bestimmen hat und insbesondere ob es als subjektives oder objektives Tatbestandsmerkmal zu interpretieren ist.[420] Die amtliche englische Fassung stellt dagegen auf das Design des Computerprogramms ab. Es ist also aus der objektiven Beschaffenheit, der Ausrichtung und dem Zusammenspiel der Programmfunktionen, also der Gesamtkonzeption des Computerprogramms zu ermitteln, wozu es geschaffen worden ist. Damit entspricht dieses Merkmal dem Merkmal „[dazu] entworfen“, das im deutschen Recht als „Entstehungsmodell“ dem § 108b Abs. 1 UrhG i.V.m. § 95a Abs. 3 Nr. 3 UrhG zugrunde liegt und oben erörtert wurde.[421]

Auch durch die zweite Abweichung wirft die deutsche Fassung eine Frage auf, die in der englischen Fassung von vornherein nicht besteht: Eine Vorrichtung, die in einer langen Kette von Vorbereitungshandlungen nur dazu bestimmt ist, den nächsten Vorbereitungsschritt zu *ermöglichen*, ist denklogisch zugleich dazu bestimmt, die spätere Zieltat zu *ermöglichen*. Eine solche Vorrichtung erfüllt also nach der deutschen Sprachfassung den Tatbestand, auch wenn sie bei der Zieltat selbst nicht eingesetzt werden soll. Deshalb droht hier eine prinzipiell endlose und damit übermäßige Vorverlagerung der Strafbarkeit.[422] Die englische Sprachfassung spricht dagegen von Vorrichtungen, die dazu *designed* (entworfen) oder angepasst sind, den unautorisierten Zugang zu geschützten Diensten zu *verschaffen*. Damit sind nur solche Vorrichtungen tatbestandsmäßig, die bei der Ausführung der Zieltat

---

419 Siehe hierzu oben I.B.3.

420 Siehe hierzu oben I.B.3.a)aa).

421 Siehe hierzu oben I.B.4.a)aa).

422 Siehe die Problemerörterung oben I.B.3.a)dd).

unmittelbar eingesetzt werden, um die Zugangskontrolle des geschützten Dienstes letztlich zu überwinden.

Die englische Sprachfassung regelt damit genau das, was im „Eignungsmodell" des deutschen § 149 Abs. 1 StGB[423] erst durch die Rechtsprechung des Reichsgerichts strafbegrenzend eingeführt worden war: das Unmittelbarkeitskriterium.[424] Festzuhalten ist damit, dass in der englischen Sprachfassung – anders als in der deutschen – nur solche Vorrichtungen erfasst sind, die bei der Begehung der Zieltat selbst zur unmittelbaren Überwindung der Zugangskontrolle eingesetzt werden sollen.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Die Dual-Use-Problematik stellt sich hier in ähnlicher Weise wie in der deutschen Umsetzung der Conditional-Access-Richtlinie im ZKDSG.[425] Dass in der englischen Sprachfassung vom Design die Rede ist, ändert mit Blick auf die Dual-Use-Problematik kaum etwas.

Interessanterweise war die Dual-Use-Problematik in diesem Fall einer der maßgeblichen Gründe für den Erlass der Richtlinie. Die Kommission hatte in ihrem Grünbuch „Legal Protection For Encrypted Services In The Internal Market", COM(96) 76,[426] festgestellt, dass die unterschiedlichen rechtlichen Regelungen zu Entschlüsselungsgeräten in den Mitgliedsstaaten dazu führen, dass der freie Verkehr von Entschlüsselungsgeräten und von Dienstleistungen in Bezug zu Entschlüsselungsgeräten behindert wird.[427] Mit anderen Worten: Der Umgang mit Verschlüsselungsgeräten, also etwa deren Herstellung, Verkauf und Vermarktung, ist unter bestimmten Umständen in allen Ländern erwünscht. Da diese bestimmten Umstände aber in den Mitgliedsstaaten unterschiedlich normiert waren, konnte dasselbe Verhalten im einen Mitgliedsstaat zulässig, in einem anderen Mitgliedsstaat verboten sein. Die Conditional-Access-Richtlinie, in deren Erwägungsgründen 4 und 5 sich die Richtliniengeber auf das Grünbuch der Kommission beziehen, sollte zur Behebung dieser Behinderungen ein einheitliches Schutzniveau für verschlüsselte Dienste schaffen und hierzu die einzelstaatlichen Rechtsvorschriften harmonisieren.[428] Dies sollte den Effekt haben, dass ein Verhalten, das in einem Mitgliedsstaat verboten ist, auch in allen anderen Mitgliedsstaaten verboten ist.

---

[423] Siehe oben I.B.1.

[424] Siehe oben I.B.1.a)bb).

[425] Siehe oben I.B.3.b).

[426] Online abrufbar, allerdings nur in englischer Sprache, unter http://europa.eu/documents/comm/green_papers/pdf/com96_76_en.pdf [zuletzt aufgerufen am 16.11.2014].

[427] Siehe COM(96) 76, S. 35 f.

[428] Siehe Erwägungsgründe 11 und 12 Richtlinie 98/84/EG.

Hier wird deutlich, dass der Unterschied zwischen legalem und illegalem Umgang mit Entschlüsselungsvorrichtungen stets in den näheren Umständen besteht, insbesondere darin, ob der Verwender sie mit oder ohne Autorisierung einsetzt. Hier ist also der Mehrzweckaspekt des Dual-Use-Phänomens angesprochen. So wird auch evident, dass in diesem Modell nicht isoliert anhand der Eigenschaften oder Funktionen der Vorrichtung entschieden werden kann, ob das Computerprogramm tatbestandsmäßig ist oder nicht. Vielmehr können Eigenschaften und Funktionen des Computerprogramms nur insofern den Ausschlag geben, als sie Auskunft darüber geben, welche Ziele ein potentieller Täter verfolgt.

Die amtliche englische Fassung erfasst alle Computerprogramme, die dazu entworfen oder angepasst sind, eine Zieltat (hier: das Zugangverschaffen) unmittelbar zu verwirklichen („designed or adapted to give access […] without the authorisation of the service provider"). Daraus folgt, dass hier der Wille und die Zielsetzung des Entwerfers oder Anpassers im Vordergrund stehen und aus deren Wille und Zielsetzung folgt, ob ein Computerprogramm tatbestandsmäßig ist. Gleichwohl normiert der Tatbestand nicht unmittelbar deren Willen als maßgebliches Kriterium, sondern verknüpft dieses subjektive Kriterium mit der (objektiven) Handlung des Entwerfens und Anpassens. Damit muss also aus dem Entwurf des Computerprogramms oder seinem konkreten Angepasst-Sein die deliktische Zielsetzung der entsprechenden Akteure ablesbar sein. Ist dies der Fall, so ist das Computerprogramm tatbestandsmäßig.

Auch hier stellt sich damit das Problem „bemakelter und makelloser Software":[429] Computerprogramme, die den objektiven Tatbestand nicht erfüllen, können frei zirkulieren, auch wenn etwa Käufer und Verkäufer in deliktischer Absicht handeln und die konkreten Vorrichtungen geeignete Deliktswerkzeuge darstellen. Da der objektive Tatbestand nicht auf die Eignung für den deliktischen Einsatz abstellt, sondern allein die Intentionen des Herstellers oder Anpassers für maßgeblich erklärt, resultiert aus kriminell einsetzbarer Entschlüsselungssoftware eine erhebliche Gefahr für das Rechtsgut, wenn die Software von gutgläubigen Herstellern entworfen oder angepasst worden ist. Computerprogramme, die den objektiven Tatbestand erfüllen, sind dagegen bemakelt und IT-Sicherheitsbeauftragte oder Entwickler von Verschlüsselungstechniken sind darauf angewiesen, im Umgang mit solchen Computerprogrammen über den subjektiven Tatbestand Straffreiheit zu erlangen.

Bei der Ausarbeitung der Conditional-Access-Konvention ging man offenbar davon aus, die Dual-Use-Problematik bereits dadurch zu beheben, dass man die (Er-)Forschung und Entwicklung nicht unter Strafe stellte, selbst wenn sie auf die Herstellung illegaler Vorrichtungen abzielte. Man sah hier ein, dass eine Unterscheidung zwischen der Forschung zu legitimen Zwecken und Forschung zu illegi-

---

[429] Siehe dazu bereits oben I.B.2.b).

timen Zwecken nur schwer zu unterscheiden wäre.[430] Deshalb beschränkte man die Tatbestandshandlungen auf das Herstellen illegaler Vorrichtungen. Diese Eingrenzung überzeugt indes nicht, denn wenn man bei der *Herstellung* eines Entschlüsselungsprogramms normativ unterscheiden kann, ob sie zu legitimen oder illegitimen Zwecken erfolgt, dürfte dies ebenso bei seiner *Entwicklung* möglich sein. Unter dem Gesichtspunkt der Dual-Use-Problematik und der Frage, wie legitimes und illegitimes Verhalten tatbestandlich differenziert werden können, macht dies keinen erheblichen Unterschied.

Der Multifunktionsaspekt der Dual-Use-Problematik, also das Nebeneinander legitimer und deliktsgeeigneter Funktionen in einem Computerprogramm, wurde hier unberührt gelassen. Auf die Funktionen des Computerprogramms *neben* dem Zugangverschaffen kommt es nicht an. Auch das Verhältnis legaler und „illegaler" Funktionen des Computerprogramms zueinander spielt keine Rolle. Denn entscheidend ist allein, dass das Computerprogramm durch den Designer oder einen Anpasser *zumindest auch* dafür entworfen oder angepasst ist, unautorisierten Zugang zu geschützten Diensten zu verschaffen. Ob das Computerprogramm hierzu objektiv in der Lage ist, ist ebenfalls irrelevant.

Auch Ausschlussklauseln sind in diesem Tatbestandsmodell nicht vorgesehen. Dabei wäre dies gerade aufgrund der Tatsache empfehlenswert, dass die objektive Tatbestandsmäßigkeit häufig unabhängig von den Absichten des Vorfeldtäters zu beurteilen sein wird – nämlich immer dann, wenn der Vorfeldtäter nicht zugleich Designer oder Anpasser der Software ist. Dadurch wird die Chance ausgelassen, das Problem „bemakelter und makelloser Software" zumindest für IT-Sicherheitskreise abzuschwächen.

2. "A computer program, designed or adapted primarily for the purpose of committing [the offence]"

In einem zweiten Modell wird das Tatobjekt so beschrieben, dass Computerprogramme erfasst werden, die „in erster Linie" oder „besonders" zum Zwecke der Begehung von Zieltaten entworfen oder angepasst sind. Verwendet wird dieses Modell in Art. 3 Nr. 1 lit. (d) 1. Spiegelstrich RB 2000/383/JI über die Verstärkung des mit strafrechtlichen und anderen Sanktionen bewehrten Schutzes gegen Geldfälschung im Hinblick auf die Einführung des Euro, außerdem in Art. 4 1. Spiegelstrich des Rahmenbeschlusses 2000/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln. Es liegt daneben auch dem Art. 6 Abs. 1 lit. a. i. CCC zugrunde. Des Weiteren wird dieses Modell auch im aktuellen Vorschlag der EU-Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhe-

---

[430] Siehe Explanatory Report zur Conditional-Access-Konvention, Rn. 34.

bung des Rahmenbeschlusses 2005/222/JI des Rates[431] in Art. 7 übernommen. Beispielhaft sei hier Art. 6 CCC in der englischen Sprachfassung angeführt:

Article 6 – Misuse of devices

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

a. the production, sale, procurement for use, import, distribution or otherwise making available of:
   i. a device, **including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5**;
   ii. […]

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

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

[…]

In seiner deutschen Sprachfassung lautet Art. 6 CCC:

Artikel 6 – Missbrauch von Vorrichtungen

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

a. das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen
   i. einer Vorrichtung einschließlich eines **Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen**;
   ii. […]

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

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

In der deutschen Sprachfassung fällt zunächst ein grammatisches Redaktionsversehen auf: Laut Art. 6 Abs. 1 lit. a i. ist ein Computerprogramm erfasst, das „dafür

---

[431] KOM(2010) 517 endgültig vom 30.9.2010; dort wird zwar in Erwägungsgrund 9 von Werkzeugen gesprochen, die zur Tatbegehung *genutzt werden können*, jedoch kann dies den insoweit enger gefassten Tatbestand nicht weiten.

ausgelegt [...] worden ist, eine […] Straftat *zu begehen*". Damit müsste das Computerprogramm selbst die Straftat begehen, was offensichtlich nicht gemeint sein kann. Straftatbestände wenden sich ausschließlich an Menschen, und eine Straftat muss stets „Menschenwerk" sein.[432] Computerprogramme können keine Straftaten begehen. Allein anhand des deutschen Konventionstextes lässt sich jedoch nicht aufklären, welchen Inhalt der Konventionsgeber hier genau normieren wollte.

Die englische Sprachfassung sieht vor, dass Computerprogramme erfasst werden, die ausgelegt worden sind „for the purpose of committing any of the offences". Dies lässt sich übersetzen als Computerprogramme, die „für den Zweck der Begehung" oder „zur Begehung" von Zieldelikten ausgelegt worden sind.

In Art. 3 Nr. 1 lit. (d) 1. Spiegelstrich RB 2000/383/JI wird das Tatobjekt in der englischen Fassung umschrieben als „instruments, articles, *computer programs* and any other means *peculiarly adapted* for the counterfeiting or altering of currency". In Art. 4 1. Spiegelstrich des Rahmenbeschlusses 2001/413/JI geht es um „instruments, articles, *computer programmes* and any other means *peculiarly adapted* for the commission of any of the offences described".

a) Charakteristika dieses Regelungsmodells

Die Verfasser der Cybercrime Convention haben sich bei Abfassung des Art. 6 CCC an damals bereits bestehenden Instrumenten orientiert, namentlich der Conditional-Access-Richtlinie der EU und der entsprechenden Konvention des Europarats, aber auch an maßgeblichen nationalen Vorschriften einiger Staaten.[433] Auch auf das am 20. April 1929 in Genf geschlossene Internationale Abkommen zur Bekämpfung der Falschmünzerei wird Bezug genommen.[434] Auch dort wurde bereits in Art. 3 Abs. 5 die Strafbarkeit des Umgangs mit bestimmten Fälschungswerkzeugen vereinbart.

Zunächst ist auch in diesem Regelungsmodell entscheidend, mit welchen Zielen die „Vorrichtung einschließlich eines Computerprogramms" entworfen (*designed*, nur Art. 6 CCC) oder angepasst (*adapted*, Art. 6 CCC, Art. 3 RB 2000/383/JI, Art. 4 RB 2001/413/JI) worden ist. Insoweit entsprechen also die vorliegenden Regelungstechniken denen der Conditional-Access-Richtlinie und der Conditional-Access-Konvention.[435]

In der deutschen Sprachfassung der CCC wird *designed* mit „ausgelegt" übersetzt, während *adapted* zu „hergerichtet" wird. Inhaltlich dürfte dies deckungs-

---

[432] Siehe nur Jescheck/*Weigend*, Strafrecht AT, S. 218 ff.

[433] Explanatory Report zur CCC, Rn. 71, online abrufbar unter http://conventions.coe.int/treaty/en/reports/html/185.html [zuletzt abgerufen am 16.11.2014].

[434] Ebd.

[435] Vgl. oben II.B.1.a).

gleich mit den im deutschen Recht üblicheren Verben „entworfen“ und „angepasst“ sein.[436] In anderen Instrumenten wurde *designed* zuvor auch hin und wieder mit „bestimmt“ oder „entworfen“ übersetzt, während *adapted* regelmäßig mit „angepasst“ wiedergegeben wird. Die für das deutsche Recht ungewöhnliche Wortwahl der CCC ist möglicherweise dem Umstand geschuldet, dass es sich bei ihrer bereinigten deutschen Fassung um eine Gemeinschaftsübersetzung für die Europarats-Mitgliedsstaaten Deutschland, Österreich und die Schweiz handelt.[437] Im Rahmen dieses nicht ganz unkomplizierten Unterfangens wurden wohl in Einzelheiten Kompromisse eingegangen.[438] Es ist daher davon auszugehen, dass in Art. 6 CCC inhaltlich keine Änderung oder Akzentverschiebung im Vergleich zu den entsprechenden Merkmalen in Conditional-Access-Richtlinie und Conditional-Access-Konvention gewollt ist.[439]

In den Rahmenbeschlüssen 2000/383/JI und 2001/413/JI wird in den englischen Sprachfassungen jeweils ebenfalls das Merkmal *adapted* verwendet, welches im Deutschen jedoch jeweils mit „ihrer Beschaffenheit nach geeignet“ übersetzt wird. Die deutsche Sprachfassung legt damit eine objektivierte Betrachtungsweise nahe, welche auf die Beschaffenheit, also Funktionen, Eigenschaften und Design des Computerprogramms abstellt und danach beurteilt, ob es für (einen Einsatz bei der Begehung von) Zieltaten *geeignet* ist. Zweifellos kann man das Merkmal *adapted* auch in dieser objektivierten Weise verstehen.

Es ist aber fraglich, ob dies richtig ist. Teleologisch lässt sich keine Präferenz für die objektivierte oder subjektivierte Auslegung bilden. Bei objektivierter Auslegung entsteht ein subjektiv-objektives Gegensatzpaar, demzufolge Computerprogramme erfasst sind, die entweder vom Designer subjektiv als Deliktswerkzeuge gewollt oder nach ihrer Beschaffenheit objektiv hierzu geeignet sind. Legt man *adapted* dagegen subjektiviert aus, so ergibt sich ein zeitliches Gegensatzpaar, demzufolge Computerprogramme erfasst sind, die entweder von Anfang an als Deliktswerkzeuge gedacht waren oder nachträglich in deliktischer Absicht hierzu angepasst wurden.[440]

Gegen eine objektivierte Auslegung spricht die Systematik: In den übrigen Instrumenten, in denen ebenfalls das Merkmal *adapted* verwendet wird, wird in der Auslegung des Merkmals auf die Absichten und Intentionen desjenigen abgestellt, der das Computerprogramm anpasst.[441] Es liegt deshalb auch historisch nahe, dass die Verfasser der Rahmenbeschlüsse 2000/383/JI und 2001/413/JI im Rückgriff auf

---

[436] Vgl. oben I.B.4.

[437] Siehe http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm [zuletzt abgerufen am 16.11.2014].

[438] Siehe *Gercke*, CR 2004, 788.

[439] Siehe oben II.B.1.a).

[440] Siehe hierzu die Ausführungen zum deutschen § 4 ZKDSG, oben I.B.3.

[441] Siehe oben II.B.1.a) und unten II.B.3.a).

dieses Merkmal von einer subjektivierten Betrachtungsweise ausgingen. Hiergegen könnte man einwenden, dass zumindest der Rahmenbeschluss 2000/383/JI zu den älteren internationalen Instrumenten zählt, sodass sich zur Zeit seiner Erarbeitung die subjektivierende Auslegung noch nicht als Standard etabliert hatte. Hiergegen spricht jedoch wiederum, dass bereits in der Conditional-Access-Richtlinie 1998/84/EG, auf die auch der Rahmenbeschluss 2000/383/JI ausdrücklich Bezug nimmt, eine subjektivierte Auslegung vorgenommen wurde, und auch in den späteren Instrumenten der EG und EU das Merkmal *adapted* regelmäßig wiederverwendet wird, ohne dass sich die Verfasser einmal gegen dessen subjektivierte Auslegung wenden.

Dem Rahmenbeschluss 2000/383/JI ging außerdem eine Entschließung des Rates 1999/C 171/01 vom 28. Mai 1999 über die Verstärkung des strafrechtlichen Schutzes gegen Geldfälschung im Hinblick auf die Einführung des Euro voran, in deren Abschnitt B.3.(b) ausgeführt wird, dass unter anderem Computerprogramme erfasst werden sollen, „which are specifically *intended* for the counterfeiting of currency". Hier wird also ausdrücklich auf die Intentionen abgestellt. Die Verfasser des Rahmenbeschluss 2000/383/JI nehmen in Erwägungsgrund 10 Bezug zu den Leitlinien dieser Entschließung. Auch in Art. 3 Abs. 5 des Genfer Übereinkommens von 1929, auf das im Rahmenbeschluss hingewiesen wird, wird dieselbe englische Tatbestandskonstruktion (*peculiarly adapted*[442]) mit einer deutlicher subjektivierten Konstruktion ins Deutsche übertragen: „ihrer Beschaffenheit nach besonders *bestimmt*".[443]

Nach alledem ist also das Merkmal *adapted* subjektiviert auszulegen. Freilich ist dann nicht davon auszugehen, dass zwischen der englischen und deutschen Sprachfassung inhaltliche Unterschiede gewollt gewesen wären. Dies liefe dem Harmonisierungsgedanken evident zuwider. Das deutsche Merkmal „ihrer Beschaffenheit nach besonders geeignet" müsste dann also auch subjektiviert ausgelegt werden, sodass die Intentionen desjenigen den Ausschlag geben, der dem Computerprogramm die konkrete Beschaffenheit gibt. Für diesen Befund spricht auch die Genese des Rahmenbeschlusses 2001/413/JI. Diesem ging nämlich eine Mitteilung der Kommission als Entwurf voraus, wo das Englische „designed or adapted" von Anfang an im Deutschen schlicht mit „konstruiert oder angepasst" übersetzt wurde.[444] Im Rahmenbeschluss 2001/413/JI wird dieser Entwurf der Kommission in Erwägungsgrund 7 ausdrücklich zugrunde gelegt.

Gegenüber dem vorstehend erörterten Modell[445] ist aber ein anderes wesentliches Merkmal hinzugekommen, nämlich das Merkmal *primarily* in Art. 6 CCC bezie-

---

442 Zitiert nach *Fitz-Maurice*, 26 Am. J. Int'l L., 1932, 539.

443 Zitiert nach der Veröffentlichung der Bundesbehörden der Schweizerischen Eidgenossenschaft, online abrufbar unter http://www.admin.ch/ch/d/sr/0_311_51/a3.html [zuletzt abgerufen am 16.11.2014].

444 Siehe 23 KOM(1998) 395 endgültig.

445 Siehe oben II.B.1.

hungsweise *peculiarly* in Art. 3 RB 2000/383/JI und Art. 4 RB 2001/413/JI. Das Computerprogramm muss *in erster Linie* zur Begehung von Straftaten ausgelegt oder hergerichtet worden sein beziehungsweise *insbesondere* für die Begehung von Zieltaten angepasst sein. Im Erklärenden Bericht zur Cybercrime Convention wird ausgeführt, dass das englische Merkmal *primarily* als sinnvoller Mittelweg zur Feinjustierung der Dual-Use-Problematik angesehen wurde.[446] Eine Alternative sei gewesen, stattdessen die Merkmale *exclusively* oder *specifically* zu verwenden. Eine zweite Alternative sah man darin, gar keine normative Einschränkung im objektiven Tatbestand vorzunehmen, stattdessen alle geeigneten Computerprogramme zu erfassen und allein im subjektiven Tatbestand zwischen kriminellem und akzeptablem Verhalten zu diskriminieren. Während man davon ausging, dass die erste Alternative wegen ihrer starken Einengung faktisch zur Unanwendbarkeit der Vorschrift führen würde, lehnte man auch die zweite Alternative mit dem Hinweis ab, dass damit allein der subjektive Tatbestand über die Strafbarkeit entschiede.[447] Diesen Hinweis hielt man offenbar für selbsterklärend und überzeugend, denn eine Begründung dafür, warum man dies nicht wolle, fehlt an dieser Stelle. Es wird lediglich darauf verwiesen, dass man eine solche Lösung auch im Bereich der Geldfälschung nicht gewählt habe.[448]

In den Rahmenbeschlüssen 2000/383/JI und 2001/413/JI finden sich keine weiteren Ausführungen zum Merkmal *peculiarly*, insbesondere nicht zu seinem Bezugspunkt. Man könnte deshalb auch vertreten, dass es sich nicht auf die Begehung der Zieltaten bezieht, sondern auf das Angepasst-Sein. Dann müsste also eine Vorrichtung nicht „insbesondere für die Begehung von Zieltaten angepasst" sein, sondern müsste „für die Begehung von Zieltaten *besonders angepasst*" sein. Auch diese Variante würde jedoch eine objektivierte Auslegung darstellen, der wohl nach dem Willen der Verfasser des Rahmenbeschlusses nicht zu folgen ist.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Dieses Regelungsmodell unterscheidet sich maßgeblich durch das Primarily- oder das Peculiarly-Merkmal von den vorstehend erörterten Modellen. Diese Merkmale zielen auf den Multifunktionsaspekt der Dual-Use-Problematik, nämlich das Nebeneinander legitimer und deliktsgeeigneter Funktionen in demselben Computerprogramm.

---

446 Explanatory Report zur CCC, Rn. 73

447 Explanatory Report zur CCC, Rn. 73.

448 Ebd.; in Deutschland hat man dagegen bei der Geldfälschung in § 149 Abs. 1 StGB genau diesen Weg gewählt, siehe oben I.B.1. Dies mag aber auch der zweideutigen Übersetzung der englischen Originalfassung des Genfer Abkommens und des Rahmenbeschlusses 2000/383/JI geschuldet sein, vgl. oben a).

Die Verfasser der Cybercrime Convention gingen davon aus, durch das Attribut *primarily* die Dual-Use-Problematik angemessen gelöst zu haben. Im Explanatory Report wird angeführt, dass dadurch normalerweise Dual-Use-Vorrichtungen ausgeschlossen seien. Dieses Merkmal hat aber ebenso wie das Merkmal *peculiarly* unter zwei Gesichtspunkten problematische Konsequenzen: Erstens schränkt das Merkmal den Tatbestand möglicherweise stärker ein als man zunächst dachte. Die Ziele eines Software-Herstellers (Entwerfers, Anpassers) können nämlich vielfältig sein, seine Software wird aber immer nur dann erfasst, wenn er *in erster Linie* oder *insbesondere* kriminelle Ziele verfolgt. Das Computerprogramm ist also schon dann nicht tatbestandsmäßig, wenn sein Hersteller *gleichermaßen* kriminelle wie legale Ziele verfolgt. Zweitens ist das Computerprogramm nicht tatbestandsmäßig, wenn der Hersteller sich über dessen Einsatzmöglichkeiten gar keine Gedanken macht, sondern es vielleicht ursprünglich aus einem ganz bestimmten Anlass geschrieben hat, später aber zugänglich macht, ohne irgendwelche Ziele konkret herauszubilden und zu priorisieren.

Für den Mehrzweckaspekt der Dual-Use-Problematik liefern die Attribute *primarily* und *peculiarly* freilich keine Lösung. Wenn allein die Ziele des historischen Herstellers bei der Beurteilung multifunktionaler Computerprogramme beachtlich sind, spielt es von vornherein keine Rolle, welche Ziele ein späterer Verwender des Programms verfolgt. Das Merkmal *primarily* bezieht sich hierauf gar nicht und bringt deshalb keine Einschränkung. Das Problem „bemakelter und makelloser Software“[449] besteht also auch hier: Ein Computerprogramm, das (überwiegend) zu legalen Zwecken entworfen oder angepasst worden ist, wird nie vom Tatbestand erfasst, weshalb auch der kriminell intendierte Umgang damit nicht strafbar ist. Im Gegenzug ist ein Computerprogramm, welches ursprünglich (überwiegend) zu kriminellen Zwecken entworfen oder angepasst worden ist, stets erfasst, sodass auf der subjektiven Tatseite zwingend ein Korrektiv erforderlich wäre, um den Umgang mit solchen Programmen zu Test-, Analyse- und Demonstrationszwecken von der Strafbarkeit auszunehmen.

3. “A computer program which is primarily designed, produced or adapted for the purpose of enabling or facilitating [the offence]”

Im zuerst dargestellten Modell wurde darauf abgestellt, ob das Computerprogramm für die Begehung einer Zieltat hergestellt (entworfen oder angepasst) worden ist. Im zweiten Modell wurde ergänzt, dass das Programm „in erster Linie“ oder „insbesondere“ für die Begehung von Zieltaten hergestellt worden sein müsse. In einem dritten Modell wird nun der Tatbestand nun dahingehend geöffnet, dass es ausreicht, wenn das Computerprogramm in erster Linie für die *Ermöglichung* oder *Erleichterung* von Zieltaten hergestellt worden ist.

---

[449] Siehe dazu bereits oben 2.b).

Dieses Modell kommt in Art. 6 Nr. 2 lit. (c) der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft zum Einsatz. Daneben wird hier auch das Herstellen zusätzlich zum Entwerfen und Anpassen der Vorrichtung explizit angeführt. Eine inhaltliche Erweiterung dürfte sich hiermit aber kaum ergeben, da der Hersteller auch bisher bereits durch das Merkmal des Anpassens regelmäßig erfasst war. Der Wortlaut des Art. 6 Nr. 2 lit. (c) der Richtlinie 2001/29/EG heißt:

> **Article 6 – Obligations as to technological measures**
> Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of **devices**, products or components or the provision of services **which**:
> […]
> (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measures.

In seiner insoweit inhaltsgleichen deutschen Sprachfassung lautet der Artikel:

> **Artikel 6 – Pflichten in Bezug auf technische Maßnahmen**
> (2) Die Mitgliedstaaten sehen einen angemessenen Rechtsschutz gegen die Herstellung, die Einfuhr, die Verbreitung, den Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und den Besitz zu kommerziellen Zwecken von **Vorrichtungen**, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen vor,
> […]
> c) die hauptsächlich entworfen, hergestellt, angepasst oder erbracht werden, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen oder zu erleichtern.

Die Merkmale „performed" und „erbracht werden" jeweils unter lit. c) beziehen sich auf die „provision of services" beziehungsweise „Erbringung von Dienstleistungen" und sind deshalb mit Blick auf die hier interessierende Kriminalisierung von Computerprogrammen („devices" oder „Vorrichtungen") irrelevant.

a) Charakteristika dieses Regelungsmodells

Zwar kommt es wie in den vorangehenden Modellen auch hier auf die (in erster Linie deliktischen) Intentionen desjenigen an, der das Computerprogramm entwirft, herstellt oder anpasst. Neu ist aber, dass es in Art. 6 Nr. 2 lit. (c) der Richtlinie 2001/29/EG genügt, wenn die Intentionen des Designers, Herstellers oder Anpassers darauf gerichtet sind, die Zieltat zu *erleichtern* oder zu *ermöglichen*. Faktisch ist damit auch das mitnormierte „Ermöglichen" im Grunde gegenstandslos, da das Erleichtern eine niedrigere Schwelle darstellt und immer mitverwirklicht ist, wenn eine Ermöglichungsintention des Herstellers im weiteren Sinne vorliegt.

Damit erübrigt sich auch die im deutschen Recht geführte Diskussion, ob die Vorrichtung dazu hergestellt (etc.) sein muss, die Zieltat *unmittelbar* zu ermög-

lichen.[450] Denn der Begriff des Erleichterns erfasst geradezu typischerweise Handlungen, welche die Zieltat *mittelbar* ermöglichen und auch nur mittelbar zur Begehung der Zieltat vorgenommen werden.

Auf die Funktionen der Vorrichtung kommt es hier – wie in den beiden vorangehend dargestellten Modellen – nicht an. Insbesondere kommt es nicht darauf an, wie viele Funktionen die Vorrichtung hat und in welchem Verhältnis diese zueinander stehen.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Mit Blick auf die Dual-Use-Problematik ergibt sich in diesem Modell nichts wesentlich anderes als im vorangehend dargestellten Modell. Der entscheidende Nachteil liegt darin, dass maßgeblich auf die Intentionen des Herstellers im weiteren Sinne abgestellt wird. Damit besteht auch hier das Problem „bemakelter und makelloser Software".[451]

Die Tatsache, dass vorliegend auch Computerprogramme in den Tatbestand einbezogen werden, die dazu hergestellt worden sind, die Begehung der Zieltat zu *erleichtern*, verschärft dieses Problem. Daran ändert sich auch dadurch nichts, dass in Erwägungsgrund 47 der Richtlinie 2001/29/EG festgehalten wird, dass die Forschungsarbeiten im Bereich der Verschlüsselungstechniken nicht durch die Vorschrift behindert werden dürften. Denn dieser gesetzgeberische Wunsch drückt sich nicht im Tatbestand aus und lässt sich auch kaum hineinlesen.

4. "A computer program which is promoted, advertised or marketed for the purpose of [the offence]"

In den drei bislang erörterten Modellen wurde – mit unterschiedlichen normativen Einschränkungen – darauf abgestellt, ob das Computerprogramm für die Begehung, Ermöglichung oder Erleichterung einer Zieltat hergestellt, entworfen oder angepasst worden ist. Zu Beurteilung des Computerprogramms kam es also maßgeblich darauf an, welche Ziele der Hersteller (im weiteren Sinne) verfolgt hatte. In einem vierten Modell wird das Computerprogramm nun nicht mehr nach den Herstellerintentionen beurteilt, sondern die Werbetreibenden rücken in den Fokus: Die Strafbarkeit hängt hier davon ab, ob das Computerprogramm als deliktisches Tool beworben wird. Dieses Modell kommt in Art. 6 Nr. 2 lit. (a) der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft zum Einsatz. Dieser heißt im Wortlaut:

---

[450] Vgl. oben I.B.3.a)dd).

[451] Siehe dazu bereits oben 2.b).

Article 6 – Obligations as to technological measures

(2) Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of **devices**, products or components or the provision of services **which**:

(a) **are promoted, advertised or marketed for the purpose of circumvention of** […] **any effective technological measures**.

In der amtlichen deutschen Übersetzung lautet der Artikel:

Artikel 6 – Pflichten in Bezug auf technische Maßnahmen

(2) Die Mitgliedstaaten sehen einen angemessenen Rechtsschutz gegen die Herstellung, die Einfuhr, die Verbreitung, den Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und den Besitz zu kommerziellen Zwecken von **Vorrichtungen**, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen vor,

a) **die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind** […].

Die deutsche Umschreibung der tatgegenständlichen Computerprogramme erfolgt also anders als in der englischen Sprachfassung in substantivierter Form, im Übrigen aber wesentlich gleich.

a) Charakteristika dieses Regelungsmodells

Eine Vorrichtung muss also zum Zweck der Verwirklichung des Zieldelikts im Verkauf gefördert, beworben oder vermarktet werden, damit sie den Tatbestand erfüllt. Die Begriffe aus der Wirtschaft werden in der Richtlinie selbst nicht näher erläutert. Eine Definition der *Werbung* findet sich in Art. 2 Nr. 1 der Europäischen Irreführungsrichtlinie 84/450/EWG. Erfasst ist dort jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen zu fördern. Da vorliegend neben der Werbung aber auch jede Verkaufsförderung und Vermarktung erfasst sind, dürften im Ergebnis alle betriebswirtschaftlichen Instrumente der Marketingpolitik einschlägig sein. Dies sind insbesondere die Produkt-, Kommunikations-, Distributions- und Kontrahierungspolitik (Preis-, Lieferkonditionen- und Absatzfinanzierungspolitik).[452] Da weder Hersteller noch Händler tatbestandlich erwähnt sind, kann die erforderliche Werbung, Vermarktung und Verkaufsförderung grundsätzlich auch durch Dritte erfolgen.

Nach dem Wortlaut müsste eigentlich die Verkaufsförderung, Werbung oder Vermarktung zum Zweck der Umgehung wirksamer technischer Maßnahmen, also

---

[452] *Kirchgeorg*, in: Gabler Wirtschaftslexikon, „Marketingpolitische Instrumente“, online abrufbar unter http://wirtschaftslexikon.gabler.de/Archiv/1493/marketingpolitische instrumente-v6.html [zuletzt abgerufen am 16.11.2014].

dem Erfolg des Zieldelikts, erfolgen. Wie bereits oben dargelegt,[453] liegt jedoch das Ziel einer Verkaufsförderung, Werbung oder Vermarktung in aller Regel in der Absatzsteigerung für die Vorrichtung. Dem Hersteller, Verkäufer oder Werbetreibenden wird es kaum darauf ankommen, wozu der Erwerber die Vorrichtung letztlich einsetzt. Gemeint ist also offenbar, dass die Vorrichtung *als Tatmittel* vermarktet oder beworben werden muss.[454]

Nach dem Wortlaut der Regelung ist nicht zwingend erforderlich, dass die als Umgehungsmittel beworbene Vorrichtung auch zur Umgehung technischer Schutzmaßnahmen geeignet ist. In der deutschen Literatur wird dies stellenweise gefordert, weil es nicht im Schutzbereich der Norm liege, den Umgang mit Vorrichtungen zu verbieten, die *fälschlicherweise* als Umgehungsmittel beworben werden.[455] Das Argument ist zwar richtig, aber der Strafgrund muss hier nicht zwingend in einer tatsächlichen Bedrohung des geschützten Rechtsguts gesehen werden, sondern kann auch – ähnlich der Strafbegründung beim untauglichen Versuch – darin gesehen werden, dass der Vorfeldtäter seine rechtsfeindliche Gesinnung in die Tat umsetzt. Freilich schlösse man dann auf die rechtsfeindliche Gesinnung des Täters allein aufgrund der Marketingmaßnahmen des Werbetreibenden. Dies ist aber ein anderes Problem.[456]

b) Das Dual-Use-Phänomen unter diesem Regelungsmodell

Legt man dieses Modell streng nach seinem Wortlaut aus, so taugt wohl kaum ein Computerprogramm als Tatobjekt. Dies gilt selbst im oben genannten Beispiel des Programms *AnyDVD* von *Slysoft*.[457] Denn auch die Bewerbung mit dem Slogan „Entfernt analogen Kopierschutz (Macrovision)“ lässt wohl allenfalls darauf schließen, dass der Werbetexter damit das Computerprogramm anpreisen will, um dadurch Kunden zum Kauf zu bewegen. Ob ein Kunde tatsächlich den Macrovision-Kopierschutz mit *AnyDVD* entfernt, wird dem Werbetexter egal sein. Doch selbst wenn man solche Fälle in den Tatbestand lesen möchte, ergäbe sich in diesem Regelungsmodell – wie auch bei den vorstehenden Regelungstechniken – das Problem „bemakelter und makelloser Software“.[458]

Zu diesem Ergebnis kommt man auch, wenn man das Tatbestandsmodell von vornherein teleologisch so auslegt, dass nicht die Intention des Werbetexters, sondern der Inhalt der Werbeaussage maßgeblich ist, also ob das Computerprogramm

---

[453] Siehe oben I.B.6.a)bb).

[454] *Entelmann*, Verbot von Vorbereitungshandlungen, S. 68; *Trayer*, Technische Schutzmaßnahmen, S. 115, 132.

[455] Wandtke/Bullinger-*Wandtke/Ohst*, § 95a Rn. 83.

[456] Siehe hierzu oben I.C.2.a)bb).

[457] Siehe oben I.C.2.b).

[458] Siehe dazu bereits oben 2.b).

von irgendjemandem *als Tatmittel* beworben wird. Da dies jedoch ein rein deskriptives objektives Tatbestandsmerkmal ist, bezüglich dessen der Vorfeldtäter lediglich dolus eventualis haben müsste, kann dieses Merkmal keine echte Ausscheidungsfunktion erfüllen. Denn ein IT-Sicherheitsbeauftragter, der sich ein deliktisch einsetzbares Computerprogramm verschafft, wird dabei regelmäßig auch ernstlich in Betracht ziehen und sich damit abfinden, dass es auf irgendeiner Plattform auch als Tatmittel beworben wird, selbst wenn ihm keine konkreten Anhaltspunkte hierfür vorliegen. Im Grunde kann sich daher nur derjenige der Straflosigkeit sicher sein, der als Erster die deliktische Verwendbarkeit eines Computerprogramms erkennt – vorausgesetzt er weiß sicher, dass er der Erste ist. Im weit häufigeren Fall, dass IT-Sicherheitsbeauftragte sich bewusst Kopierschutzknacker zu Test-, Analyse- und Demonstrationszwecken beschaffen, ist der Tatbestand häufig erfüllt. Auch die Hersteller von Test- und Analysesoftware machen sich grundsätzlich strafbar, wenn ihre Software irgendwo auch als Tatmittel beworben wird. Denn dass sie dies ernstlich in Betracht gezogen und sich damit abgefunden haben, wird man ihnen relativ einfach nachweisen können. Kehrseite dieser Auslegung ist freilich, dass auch in den Fällen, in denen das Computerprogramm tatsächlich zu kriminellen Zwecken eingesetzt werden soll, der subjektive Tatbestand leicht zu beweisen sein wird.

5. "A computer program the purpose of which is the commission of [any of the offences]"

Die ersten drei dargestellten Modelle stellten maßgeblich darauf ab, welche Intentionen der Hersteller im weiteren Sinne (Designer, Hersteller, Anpasser) ursprünglich verfolgt hatte. Im vierten Modell gaben die Intentionen der Werbetreibenden den Ausschlag. Es war also jeweils von Dritten abhängig, ob ein Computerprogramm als Schadsoftware eingestuft wird. In einem fünften Modell löst sich der Gesetzgeber nun von diesem Prinzip der Intentionen Dritter und spricht abstrakt vom Zweck *(purpose)* eines Computerprogramms. Dieser Zweck müsse in der Begehung einer der Zieltaten liegen.

Dieses Modell kommt in Art. 4 2. Spiegelstrich RB 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln zum Einsatz. Dieser heißt im Wortlaut:

> **Article 4 – Offences related to specifically adapted devices**
>
> Each Member State shall take the necessary measures to ensure that the following conduct is established as a criminal offence when committed intentionally:
>
> the **fraudulent making, receiving, obtaining, sale or transfer to another person or possession of**:
>
> […]
>
> **— computer programmes the purpose of which is the commission of any of the offences described under Article 3**.

Die insoweit inhaltsgleiche deutsche Fassung lautet:

> **Artikel 4 – Straftaten bezogen auf spezielle Tatmittel**
> Jeder Mitgliedstaat trifft die erforderlichen Maßnahmen, um sicherzustellen, dass die folgenden Verhaltensweisen Straftaten darstellen, wenn sie vorsätzlich begangen wurden:
> **Betrügerisches Anfertigen, Annehmen, Sichverschaffen, Verkaufen, Weitergeben an eine andere Person oder Besitzen von**:
> […]
> **— Computerprogrammen, deren Zweck die Begehung einer der in Artikel 3 beschriebenen Straftaten ist**.

a) Charakteristika dieses Regelungsmodells

Der Begriff „Zweck" drückt typischerweise das Ziel aus, das ein Mensch mit einem bestimmten Verhalten verfolgt.[459] Deshalb können nur Handlungen einen Zweck haben, Gegenstände dagegen nicht. Spricht man aber – so wie vorliegend – vom Zweck des Computerprogramms, so ist damit eigentlich der Zweck gemeint, den ein bestimmter (gedachter) Personenkreis typischerweise mit einer bestimmten (gedachten) Handlung verfolgt, wobei die Handlung irgendeinen Bezug zum tatgegenständlichen Computerprogramm haben muss.

Damit ergeben sich ähnliche Auslegungsschwierigkeiten und -möglichkeiten wie im „Zweckmodell" des deutschen Strafrechts.[460] Freilich sind die eingangs angesprochenen Unterschiede[461] zu beachten: Erstens wendet sich der Rahmenbeschluss 2001/413/JI an den nationalen Gesetzgeber und verpflichtet diesen zum Erlass einer Sanktionsnorm. Soweit Auslegungsspielräume bestehen, ist also der nationale Gesetzgeber dazu aufgerufen, diese zu nutzen. Zweitens stellen die Normen des Rahmenbeschlusses selbst keine Strafnormen dar. Deshalb gilt bei der Auslegung dieser Normen nicht die strenge Wortlautbindung, die im nationalen Strafrecht aus Art. 103 Abs. 2 GG abgeleitet wird.

Es ist dem nationalen Gesetzgeber deshalb durchaus möglich, den „Zweck des Computerprogramms" freier auszulegen. Dies gilt umso mehr, da im Rahmenbeschluss 2001/413/JI und seinen Erwägungsgründen offengelassen wird, auf welchen Personenkreis und welche Handlung es bei der Beurteilung eines Computerprogramms ankommen soll. So könnte der Gesetzgeber auch einen völlig neuen Ansatz verfolgen: Er könnte das Merkmal des „Zwecks eines Computerprogramms" ausfüllen, indem er darauf abstellt, zu welchen Zwecken ein Computerprogramm *statistisch* eingesetzt wird. Er würde dann den Rahmenbeschluss umsetzen, indem er ein nationales Software-Delikt erlässt, in dem etwa der Umgang mit

---

459 Siehe dazu ausführlich oben, I.B.2.a).

460 Siehe wiederum oben I.B.2.a).

461 Siehe oben II. am Anfang.

Computerprogrammen unter Strafe gestellt wird, die „weit überwiegend zur Begehung von Straftaten eingesetzt werden".[462]

In den Vorarbeiten der Kommission findet sich aber die Ausführung, dass „Klassifizierungen auf der Basis oder in Abhängigkeit vom verwendeten Instrument" nicht mehr vorgenommen werden sollen.[463] Die Rede ist hier von der Klassifizierung eines bestimmten Verhaltens als strafbar oder straflos, und mit „Instrument" ist das jeweilige Tatwerkzeug gemeint, hier also ein Computerprogramm. Die Strafbarkeit soll also nicht mehr vom verwendeten Computerprogramm abhängen. Stattdessen sollen Straftaten „‚absichtsbezogen' und ‚instrumentneutral'" kodifiziert werden.[464] Dabei solle ohne Rückgriff auf herkömmliche Tatbestände möglichst das Verhalten des Täters beschrieben werden und seine kriminelle Intention ausschlaggebend sein.[465]

Legt man die Ausführungen der Kommission mangels anderweitiger Konkretisierungen in den Begleitmaterialien zugrunde, so ergibt sich, dass in der dreistrahligen Zweckbeziehung[466] der Vorfeldtäter selbst als Zwecksetzer maßgeblich ist. Dies kann im Einzelfall der Hersteller sein, sodass sich kein wesentlicher Unterschied zu den vorangehend erörterten Modellen ergibt. Es kann aber entsprechend anderen Tatvarianten auch der Annehmende, Sichverschaffende, Verkaufende, Weitergebende oder Besitzende sein. Als zweckgebundene Handlung kommt dann vor allem die konkrete Tathandlung in Betracht.[467]

Damit ist also zu fragen, ob beispielsweise ein konkreter Software-Hersteller mit dem Anfertigen eines konkreten Computerprogramms deliktische Ziele verfolgt. Ist das der Fall, so hat dieses Computerprogramm einen deliktischen Zweck und der Tatbestand ist in der Variante des Anfertigens eines Computerprogramms, dessen Zweck die Begehung von Straftaten ist, erfüllt. Wenn später eine andere Person sich dasselbe Computerprogramm verschafft, ist jedoch erneut zu fragen, ob diese Person mit dem Sichverschaffen des Computerprogramms deliktische Ziele verfolgt. Ist dies zu verneinen, so hat dasselbe Computerprogramm in diesem Moment *keinen* deliktischen Zweck mehr.

---

462 Ob dieses „Statistische Modell" sinnvoll wäre, steht auf einem anderen Blatt, da es auch das Problem „bemakelter und makelloser Software" schaffen würde: Die Minderheit, die das Computerprogramm legitim einsetzt, braucht einen verlässlichen Ausweg aus der Strafbarkeit. Außerdem könnten besonders potente Schadprogramme von immer mehr IT-Sicherheitsbeauftragten eingesetzt werden, sodass sich die Mehrheitsverhältnisse ändern: das Programm würde dann möglicherweise nicht mehr „weit überwiegend" sondern nur noch überwiegend deliktisch genutzt. Damit würden Computerprogramme ihre Tatbestandsmäßigkeit verlieren, weil und obwohl sie besonders schädlich sind.

463 Siehe KOM(1998) 395 endgültig, S. 9.

464 Siehe KOM(1998) 395 endgültig, S. 10.

465 Ebd.

466 Zur „dreistrahligen Zweckbeziehung" siehe oben I.B.2.a).

467 Zu anderen Interpretationsmöglichkeiten siehe wiederum oben I.B.2.a).

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Übernimmt man die Erläuterungen der Kommission, so taucht also das Problem „bemakelter und makelloser Software" in diesem Modell erstmals nicht mehr auf. Das entscheidende Tatbestandsmerkmal, nämlich der kriminelle Zweck, ist nicht mehr von Dritten, sondern jeweils vom einzelnen Vorfeldtäter selbst abhängig. Seine jeweils konkrete Zwecksetzung entscheidet zugleich darüber, ob das Verhalten strafbar ist. Damit wird legitimes Verhalten eines IT-Sicherheitsbeauftragten stets zuverlässig ausgeschlossen, da es ihm bei Vornahme seiner Handlung an der deliktischen Zwecksetzung mangelt. Es entsteht also weder bemakelte Software, deren Verkehrsfähigkeit in IT-Sicherheitskreisen eingeschränkt ist, noch entsteht ein Freifahrtschein für ursprünglich legitim hergestellte, aber deliktisch einsetzbare Computerprogramme.

Die Kehrseite dieses Modells ist der konturlose objektive Tatbestand, denn konsequenterweise ist hier grundsätzlich jedes Computerprogramm taugliches Tatobjekt. Entscheidend ist, welcher Zweck mit dem Programm verfolgt wird. Der objektive Tatbestand reduziert sich auf ein völlig unscheinbares Geschehen wie das Anfertigen *irgendeines* Computerprogramms oder dessen Verkauf. Weitere Konkretisierungen etwa der Eigenschaften und Funktionen des jeweiligen tatgegenständlichen Computerprogramms werden im objektiven Tatbestand nicht vorgenommen. So ist beispielsweise nicht festgelegt, ob ein Computerprogramm unmittelbar oder mittelbar bei Begehung der Zieltat einsetzbar sein muss oder ob es diese lediglich ermöglichen oder erleichtern muss. Genau genommen muss das Programm die Zieltat überhaupt nicht erleichtern, da allein der deliktische Zweck die Strafbarkeit auslöst. So kann grundsätzlich sogar der Umgang mit dem Windows-Taschenrechner strafbar sein.

Der einzige verbleibende Filter ist in dem konkreten hier behandelten Tatbestand das weitere subjektive Merkmal „betrügerisch". Dies ist aber kein IT-spezifisches Merkmal, welches genuin die Dual-Use-Problematik bewältigen oder die Vorfeldkriminalität allgemein begrenzen soll, sondern ist wohl dem Umstand geschuldet, dass dieses Vorfelddelikt in die Kategorie der Betrugsstraftaten eingefügt worden ist.

6. "A computer program which has only a limited commercially significant purpose or use other than [the offence]"

Alle bisher dargestellten Modelle bauten maßgeblich auf eine subjektive Zielsetzung auf, aus der die Bewertung eines Computerprogramms als Schadsoftware und damit taugliches Tatobjekt erfolgte. Entscheidend war dort entweder die subjektive Zielsetzung des Herstellers im weiteren Sinne, der Werbetreibenden oder des Vorfeldtäters selbst. In einem sechsten Modell löst sich der Gesetzgeber von diesem subjektiven Ansatz und macht eine objektive, wirtschaftliche Bewertung des Com-

puterprogramms zur Grundlage der Entscheidung. Dieses Modell kommt in Art. 6 Nr. 2 lit. (b) der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft zum Einsatz. Demnach soll zur Sicherstellung der Effektivität von technischen (Kopier-)Schutzmaßnahmen der Umgang mit „Kopierschutzknackern" verboten werden. Im Wortlaut heißt es dort:

> **Article 6 – Obligations as to technological measures**
>
> 1. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
>
> […]
>
> (b) have only a limited commercially significant purpose or use other than to circumvent […]
>
> any effective technological measures.

In der amtlichen deutschen Fassung lautet die Norm:

> **Artikel 6 – Pflichten in Bezug auf technische Maßnahmen**
>
> (2) Die Mitgliedstaaten sehen einen angemessenen Rechtsschutz gegen die Herstellung, die Einfuhr, die Verbreitung, den Verkauf, die Vermietung, die Werbung im Hinblick auf Verkauf oder Vermietung und den Besitz zu kommerziellen Zwecken von Vorrichtungen, Erzeugnissen oder Bestandteilen sowie die Erbringung von Dienstleistungen vor,
>
> […]
>
> b) die, abgesehen von der Umgehung wirksamer technischer Maßnahmen, nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben […].

In der deutschen Fassung wurde also *commercially significant* mit „wirtschaftlich" übersetzt und damit das Merkmal *significant* unterschlagen. Dass dies zu einer inhaltlichen Abweichung führt, kann bezweifelt werden. Legt man jedoch zunächst den Wortlaut der Norm in der englischen Sprachfassung eng aus, so sind Computerprogramme tatbestandslos, deren *wirtschaftlich beachtlicher* Nutzen *nicht begrenzt* ist. Dann kann man freilich argumentieren, dass ein nichtbegrenzter wirtschaftlicher Nutzen *stets* beachtlich ist und deshalb das Merkmal *significant* der englischen Sprachfassung überflüssig ist. Insofern wäre die deutschen Sprachfassung des Art. 6 konsequent, in der nur solche Computerprogramme tatbestandlich ausgegrenzt werden, die *keinen* begrenzten wirtschaftlichen Nutzen neben der Zieltat bieten, also wirtschaftlich unbegrenzt nutzbar sind.[468] Gemeint ist aber in beiden Sprachfassungen etwas anderes, das nun zu erörtern ist.

---

[468] Vgl. zur insoweit wortgleichen Tatbestandskonstruktion im deutschen Recht oben I.B.5.a).

a) Charakteristika dieses Regelungsmodells

Unterschlägt man das Merkmal *significant* nicht, so werden vorliegend alle Computerprogramme tatbestandlich erfasst, die abgesehen von der Umgehung von Schutzmaßnahmen einen begrenzten wirtschaftlich beachtlichen oder bedeutenden Zweck oder Nutzen haben. Das Merkmal „abgesehen von der Umgehung technischer Schutzmaßnahmen" setzt also zunächst voraus, dass die Vorrichtung überhaupt zur Umgehung technischer Schutzmaßnahmen geeignet ist. Der wirtschaftliche Nutzen folgt dann aus dem wirtschaftlichen Wert des Werkes, dessen Kopierschutz umgangen wird. Sollte die Vorrichtung daneben noch einen weiteren wirtschaftlich beachtlichen Nutzen aufweisen, so muss dieser laut Tatbestand „begrenzt" sein. Festzuhalten ist damit zunächst, dass jeder Nutzen, der unter wirtschaftlichen Gesichtspunkten unbeachtlich ist, in diesem Tatbestandsmodell keine Rolle spielt. Zweitens ist damit festgelegt, dass eine wirtschaftliche Analyse der Vorrichtung erfolgt, wobei ihr wirtschaftlich beachtlicher Nutzen bei legalem Einsatz und der wirtschaftlich beachtliche Nutzen bei illegalem Einsatz betrachtet werden.

Das Kriterium, dass der wirtschaftlich beachtliche Nutzen bei legalem Einsatz begrenzt sein müsse, ist wohl nicht wörtlich zu nehmen, da es sonst kaum eine Ausscheidungsfunktion hätte. In den Erwägungsgründen zur Richtlinie 2001/29/EG wird dieses Kriterium denn auch anders umschrieben. Dort heißt es, die Vorschrift solle nicht jene Vorrichtungen untersagen, „deren wirtschaftlicher Zweck und Nutzen nicht in der Umgehung technischer Schutzvorkehrungen besteht". In der englischen Sprachfassung wird an derselben Stelle genau umgekehrt formuliert, dass jene Vorrichtungen nicht erfasst werden sollen, „die einen wirtschaftlich beachtlichen Zweck oder Nutzen abgesehen von der Umgehung technischer Schutzvorkehrungen haben".[469]

Nach der englischen Sprachfassung würde also genügen, dass eine Vorrichtung überhaupt einen wirtschaftlich beachtlichen Zweck oder Nutzen neben dem illegalen Einsatz hat, denn dann soll sie nicht vom Tatbestand erfasst sein. Dagegen wäre nach der deutschen Sprachfassung hierfür erforderlich, dass man – wohl in einer Art Gesamtbetrachtung – positiv feststellt, dass der Zweck und Nutzen der Vorrichtung nicht in der Umgehung technischer Schutzvorkehrungen besteht. Dafür wäre es freilich ein Indiz, wenn ein wirtschaftlich beachtlicher Nutzen bei legalem Einsatz besteht – jedoch wäre dies kein zwingender Grund. Die Auslegung nach der englischen Sprachfassung des Erwägungsgrundes würde somit zu einer einfacheren Strafbefreiung führen.

Dies sind natürlich nur Nuancen. In der Sache geht es darum, überhaupt festzustellen, dass die Vorrichtung sowohl bei legalem als auch bei illegalem Einsatz einen wirtschaftlichen Wert hat. Sodann muss man abwägen, wie erheblich oder

---

[469] Erwägungsgrund 48 der Richtlinie 2001/29/EG.

gering der jeweilige Nutzen im Verhältnis zum anderen Nutzen ist und daraus Konsequenzen ziehen.

b) Das Dual-Use-Phänomen unter diesem Regelungsmodell

Dieses Modell unterscheidet sich von den anderen zunächst darin, dass es voraussetzt, dass das fragliche Computerprogramm bei illegalem Einsatz einen wirtschaftlichen Nutzen bietet. Folglich muss die Vorrichtung überhaupt zum illegalen Einsatz *geeignet* sein. Hat das Computerprogramm nun auch bei legalem Einsatz einen beachtlichen wirtschaftlichen Nutzen, so ist es entweder allein deshalb vom Tatbestand ausgenommen oder jedenfalls dann, wenn dieser Zweck oder Nutzen den wirtschaftlichen Zweck oder Nutzen bei illegalem Einsatz in den Hintergrund drängt.

Aus dem Blickwinkel der Dual-Use-Problematik hängt deshalb alles davon ab, wie die wirtschaftliche Abwägung vorgenommen werden soll. Denn jedes Umgehungsprogramm hat auch bei legalem Einsatz einen Nutzen, nämlich den, dass man analysieren kann, auf welche Weise es den Kopierschutz umgeht, um sodann in einem weiterentwickelten Kopierschutz diese Form der Umgehung zu versperren. Dieser Nutzen ist auch wirtschaftlich beachtlich, denn der weiterentwickelte Kopierschutz sichert die wirtschaftliche Verwertung des Schutzgegenstands.

Betrachtet man also einen Kopierschutzknacker abstrakt, so lässt sich festhalten, dass er sowohl bei legalem als auch bei illegalem Einsatz einen Nutzen hat. Dieser Nutzen ist bei illegalem Einsatz unmittelbar wirtschaftlich beachtlich, weil man unmittelbar den Nutzen aus dem geschützten Werk ziehen kann. Bei legalem Einsatz zu Analysezwecken tritt der wirtschaftlich beachtliche Nutzen mittelbar ein, nämlich nach entsprechender Weiterentwicklung des Kopierschutzes.

Bei konkreter Abwägung im Einzelfall könnte man dagegen darauf abstellen, ob sich für den konkreten Vorfeldtäter ein wirtschaftlich beachtlicher Nutzen einstellt, wenn er das Computerprogramm legal einsetzt. Dies ließe sich bei einem Entwickler von Kopierschutzmaßnahmen ohne Weiteres bejahen, während es bei allen anderen „Inhabern" eines Kopierschutzknackers schwer erklärbar wäre, wie sie durch den legalen Einsatz des Kopierschutzknackers einen wirtschaftlich beachtlichen Nutzen ziehen wollten. Für eine solche einzelfallbezogene Auslegung spricht auch hier, dass in der Richtlinie stets von „Zweck oder Nutzen" oder – wie in der deutschen Fassung von Erwägungsgrund 48 – vom „Zweck *und* Nutzen" die Rede ist. Der Zweck ist ein subjektives Merkmal und kann nur von einzelnen Personen mit einzelnen Handlungen verknüpft werden. Daher liegt es nahe, den wirtschaftlichen „Zweck oder Nutzen" jeweils anhand der konkreten subjektiven Zwecksetzung des Handelnden zu beurteilen. Ebenfalls spricht für die subjektivierte Auslegung im Einzelfall, dass sie das Problem „makelloser und bemakelter Software" vermeidet: Stufte man Computerprogramme allein aufgrund einer abstrakten wirtschaftlichen

Beurteilung als tatbestandsmäßig ein, so schüfe man erneut bemakelte Software einerseits und erteilte anderen Computerprogrammen einen Freifahrtschein, obwohl Computerprogramme beider Gruppen deliktisch nutzbar sind.[470]

Zuletzt ist fraglich, ob die wirtschaftliche Betrachtungsweise immer sinnvoll ist. In der subjektivierten Auslegung im Einzelfall kommt sie nur dann zu sinnvollen Ergebnissen, wenn man davon ausgeht, dass jede Person im Umgang mit dem Computerprogramm wirtschaftliche Ziele verfolgt. Sofern aber mögliche Vorfeldtäter ideelle oder politische Ziele verfolgen, kann die wirtschaftliche Betrachtungsweise dies nicht angemessen erfassen. Dieser Einwand ist nicht unerheblich, da gerade im Bereich der Kopierschutzknacker häufig Hackergruppen um Ruhm in der jeweiligen Szene ringen und gelegentlich auch aus „sportlichem Ehrgeiz" bestimmte Kopierschutzsysteme zu knacken versuchen, die nach dem Stand der Technik als unüberwindbar gelten.

Cracks, mit denen solche Kopierschutzsysteme überwunden werden können, werden häufig in speziellen Foren gratis zum Download gestellt, und zwar in einer Form, aus der die jeweilige Cracking-Gruppe ersichtlich ist. So führte etwa der Computerspieleverleger *Ubisoft* im März 2010 ein DRM-System als Kopierschutz für seine Computerspiele ein, welches zunächst als unüberwindbar galt. Einen Monat später wurde dieser Schutz jedoch von der Hackergruppe *Skid Row* geknackt, die einen *Crack* zur Überwindung des DRM-Systems programmierte und diesen kostenlos auf mehreren *Filesharing*-Plattformen zur Verfügung stellte. Dass die Hacker-Gruppierung nicht aus finanziellen, sondern aus politischen Motiven handelte, war auch an der Botschaft an *Ubisoft* zu erkennen, die die Gruppierung in dem Crack hinterließ: *Ubisoft* solle sich künftig wieder mehr um die Spielequalität als um DRM-Systeme kümmern.[471]

C. Die subjektive Tatseite der Software-Delikte

Auch die Regelungstechniken, die in den internationalen Instrumenten angewandt werden, lassen sich danach unterscheiden, ob die Tatbestände einen intentionalen Bezug zur Zieltat voraussetzen und wenn ja welchen. Innerhalb der Tatbestände, die einen intentionalen Bezug zur Zieltat voraussetzen, finden sich aber mehr Differenzierungen als im deutschen Recht, sodass insgesamt von drei Regelungsmodellen gesprochen werden kann. Im Folgenden werden sie dargestellt.

Auch hier werden die Charakteristika des Regelungsmodells herausgearbeitet (a). Sodann wird erörtert, wie diese Charakteristika sich auf die Dual-Use-

---

[470] Zum Problem „bemakelter und makelloser Software", siehe oben II.B.1. b).

[471] Siehe *Lowensohn*, Ubisoft's controversial 'always on' PC DRM hacked, online abrufbar unter http://news.cnet.com/8301-27076_3-20003120-248.html [zuletzt abgerufen am 16.11.2014];

Problematik auswirken (b). Strafbarkeitsrisiken der IT-Sicherheitsbeauftragten stehen auch hier im Vordergrund. Erneut soll keine Würdigung der Kriminalpolitik stattfinden,[472] sondern eine rechtliche Analyse der Regelungstechnik.

1. "Intent that the computer program be used for the purpose of committing any of the offences"

Art. 6 Ziff. 1 lit. a CCC sieht vor, dass der Vorfeldtäter seine Tathandlung mit *intent* dahingehend vornimmt, dass das Computerprogramm zum Zwecke der Begehung einer Zieltat verwendet wird. Die deutsche Sprachfassung macht aus dieser Regelung den „Vorsatz, das Computerprogramm zur Begehung einer Zieltat *zu verwenden*".

Sprachlich ist die deutsche Fassung nicht gelungen, da das Subjekt einer Infinitivkonstruktion mit dem Subjekt des Hauptsatzes identisch ist. Genau genommen erfordert daher die deutsche Übersetzung des Art. 6 CCC, dass der Vorfeldtäter Vorsatz dahingehend hat, dass *er selbst* das Computerprogramm deliktisch verwenden werde. Gegenüber dem englischen Wortlaut stellt dies eine Einengung dar, denn dort ist gerade nicht normiert, dass der Vorfeldtäter das Computerprogramm selbst verwenden wollen muss. Es handelt sich damit offensichtlich um ein Redaktions- oder Übersetzungsversehen. Die Ratio des Art. 6 CCC besteht nämlich gerade auch darin, dass Computerprogramme aus dem Verkehr gezogen werden, die einem unübersehbaren Kreis Dritter Zieltaten ermöglichen.[473]

a) Charakteristika dieses Regelungsmodells

Der Vorfeldtäter muss hier den Vorsatz haben, dass das Computerprogramm zum Zwecke der Begehung von Zieltaten verwendet werde. Das Intent-Merkmal drückt also eine Verwendungsabsicht aus, wobei sich diese auch darauf beziehen kann, dass *ein anderer* die Vorrichtung zum Zwecke der Begehung von Zieldelikten verwendet. Dieses Merkmal soll die Strafbarkeit weiter eingrenzen.

Im Explanatory Report wird das Merkmal als „specific (i.e. direct) intent" konkretisiert.[474] Auch wenn man dies als „bestimmten (also direkten) Vorsatz" übersetzen mag,[475] wäre es wohl voreilig, in der Terminologie der CCC und des Explanatory Report eine Übernahme der deutschen Dolus-Lehre zu sehen und diese auf die Tatbestände der CCC anzuwenden. Dementsprechend wird auch im Explanatory Report an früherer Stelle gesagt, dass man darin übereingekommen sei,

---

[472] Zur Kritik an der „europäischen Kriminalpolitik" siehe die Verweise oben Fn. 418.

[473] Explanatory Report zur CCC, Rn. 71.

[474] Explanatory Report zur CCC, Rn. 76.

[475] Eine amtliche Übersetzung des Explanatory Report ins Deutsche gibt es nicht.

dass zumindest das Merkmal *intentionally* der nationalstaatlichen Auslegung anheim zu stellen ist.[476]

Deshalb ist davon auszugehen, dass die Normierung des „specific (i.e. direct) intent" auf internationaler Ebene überhaupt keine nationale Vorsatzlehre inhaltlich übernehmen soll. Es kann mithin weder die deutsche Dolus-Lehre zur Auslegung des Merkmals der CCC herangezogen werden, noch kann auf die Dogmatik des Common Law zu *intent* und anderen Vorsatzformen abgestellt werden. Der konkrete Inhalt und die Wirkung des Merkmals „specific (i.e. direct) intent" muss sich vielmehr aus der Systematik der CCC selbst ergeben. Der so gefundene Inhalt des Merkmals muss sodann auf nationaler Ebene von dem jeweiligen Nationalstaat in die Dogmatik der heimischen Vorsatzarten transformiert werden.

Zwingend erforderlich ist damit, dass die Bezüge und Abstufungen innerhalb der CCC gewahrt werden. Deshalb muss der „specific (i.e. direct) intent" im Vergleich zum allgemeinen Vorsatzmerkmal der CCC, nämlich *intentionally*, eine besonders bestimmte, „direkte" oder „unmittelbare" Form annehmen.

Nach deutscher Dogmatik würde sich damit anbieten, neben dem allgemeinen Vorsatzerfordernis hier ein Absichtsmerkmal einzusetzen. Die Abstufung würde etwas deutlicher, wenn man das Absichtsmerkmal auf dolus directus 1. Grades oder 2. Grades begrenzt. Im Detail hat der deutsche Gesetzgeber hier aber einen erheblichen Auslegungsspielraum, da die CCC keine inhaltliche Vorgabe über das Gesagte hinaus macht.

Neben der Frage der Intensität des Vorsatzes stellt sich die Frage des Bezugspunktes. Hier ist fraglich, wie konkretisiert die Zieltat sein muss, auf die sich die deliktische „Absicht" *(intent)* bezieht. Der Tatbestand spricht von „einer nach den Artikeln 2 bis 5 umschriebenen Straftat". Damit kann eine bestimmte und in den Einzelheiten konkretisierte Zieltat gemeint sein, jedoch lässt der Wortlaut auch eine eher generalisierende Auslegung zu, bei der die Vorstellung von der beabsichtigten Zieltat nur in wesentlichen Umrissen konkretisiert ist.[477] Zudem bezieht sich die Absicht auf die Begehung (purpose of *committing*) einer Zieltat, nicht auf den Deliktserfolg einer der Zieltaten.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

Unter dem Blickwinkel der Dual-Use-Problematik kommt dem Intent-Merkmal höchste Bedeutung zu. Sowohl hinsichtlich des Multifunktionsaspekts als auch des Mehrzweckaspekts der Dual-Use-Problematik erlaubt dieses Merkmal eine sachgerechte Abgrenzung, da stets ein besonderes Vorsatzmerkmal auf die Begehung einer Zieltat gerichtet sein muss – unabhängig von den Eigenschaften des tatgegen-

---

476 Explanatory Report zur CCC, Rn. 39.

477 Zur Diskussion dieser beiden Auslegungen siehe oben I.C.1.a)dd).

ständlichen Computerprogramms und unabhängig davon, wie man damit verfährt, also insbesondere, ob man das Computerprogramm im eigenen Machtbereich behält oder es aus seinem Machtbereich entlässt. Damit wird legitimes und illegitimes Verhalten trennscharf voneinander abgegrenzt.

Die CCC überlässt es den Unterzeichnerstaaten, welche Vorsatzformen sie unter den *intent* fassen, der im Explanatory Report als „specific (i.e. direct) intent" beschrieben ist. Lässt man hier dolus eventualis genügen, so entstehen erhebliche Strafbarkeitsrisiken für IT-Sicherheitsbeauftragte. Denn als dolus eventualis würde bereits genügen, wenn ein IT-Sicherheitsbeauftragter es ernstlich für möglich und nicht ganz fernliegend hält, dass sein Computerprogramm zu Zieldelikten verwendet wird und er sich damit abfindet – und es hilft ihm nicht, wenn ihm diese deliktische Verwendung unerwünscht ist.[478]

IT-Sicherheitsbeauftragte geraten hier regelmäßig in den Bereich strafrechtlicher Haftung, wenn sie ein deliktisch einsetzbares Computerprogramm aus ihrem Machtbereich entlassen, also insbesondere wenn sie deliktisch verwendbare Analysesoftware zur Verfügung stellen. Gegebenenfalls wäre der subjektive Tatbestand schon im Moment der Herstellung des Computerprogramms zu bejahen, selbst wenn der IT-Sicherheitsbeauftragte etwa einen *Exploit* nur als *Proof of Concept* herstellt. Denn wenn er zu diesem Zeitpunkt beabsichtigt, das fertiggestellte Computerprogramm zur Verfügung zu stellen, wird er wohl auch schon zu diesem Zeitpunkt ernstlich für möglich halten, dass der *Exploit* bis zur Behebung der Sicherheitslücke auch deliktisch eingesetzt wird.

Möchte man dieses Strafbarkeitsrisiko zumindest mindern, so sollte „intent" als Absicht im Sinne direkten Vorsatzes interpretiert werden. Dies würde auch dem Ziel der Verfasser der CCC entsprechen, mit dem Intent-Merkmal höhere Anforderungen als den „Standardvorsatz" zu stellen. IT-Sicherheitsbeauftragte können sich dann stets darauf berufen, dass sie weder sicheres Wissen noch zielgerichtetes Wollen hinsichtlich der deliktischen Verwendung ihres Computerprogramms haben.

Eine Absicht im Sinne von dolus directus 1. Grades wird dagegen häufig als zu eng angesehen:[479] Kriminelle Vorfeldtäter werden häufig kein besonderes Interesse an der Begehung der Zieltat haben, jedenfalls immer dann, wenn sich ihr Interesse allein auf den eigenen Profit beschränkt. Dieser stelle sich aber – jedenfalls in den Tatvarianten des Herstellens, Verkaufens, Feilhaltens, Überlassens etc. – durch die Vorbereitungshandlung selbst ein und sei nicht abhängig von der späteren Begehung des Zieldelikts.

---

[478] Vgl. nur BGH NJW 89, 781, BGH NStZ 2007, 701, BGH NStZ 2008, 93; außerdem Schönke/Schröder-*Sternberg/Lieben*, § 15 Rn. 85 ff.; vgl. auch oben I.C.1.a)bb).

[479] Siehe *Popp*, GA 2008, 391 mit Verweis auf die entsprechende Diskussion bei § 267 StGB, wo „*zur* Täuschung im Rechtsverkehr" gehandelt werden muss, und sich entsprechende Fragen stellen. Das Argument zitiert *Popp* aus LK-*Tröndle*, 10. Aufl. 1982, § 267 Rn. 199.

Freilich schließt das Intent-Merkmal aus, dass schon die bloße Gefährdung strafrechtlich erfasst wird, die darin liegen kann, dass potentiell schädliche Gegenstände verfügbar gemacht werden und folglich zirkulieren. Dieser Fall wird typischerweise durch Anschließungsdelikte erfasst.[480] Sofern also deliktisch einsetzbare Computerprogramme schlicht zugänglich gemacht werden, ohne dass eine besondere Intention des Zugänglichmachenden vorliegt, so ist dies zunächst straflos. Dies gilt auch dann, wenn einem unbestimmten Personenkreis durch das zugänglich gemachte Computerprogramm die Begehung von Straftaten ermöglicht wird, also wenn dieser Personenkreis die Zieltaten andernfalls überhaupt nicht begehen könnte, etwa weil ihm hierzu die technischen Kenntnisse und Fähigkeiten fehlen. Dies spricht aber nicht zwingend gegen das Modell, denn diejenigen, die sich ein solches Computerprogramm beschaffen, machen sich wiederum strafbar, sobald sie *beabsichtigen*, eine Zieltat mittels des Computerprogramms zu begehen. Das Regelungsmodell gewährt damit eine im Umfang sachgerechte Bestrafung, allerdings um den Preis, dass deliktisch einsetzbare Computerprogramme grundsätzlich verfügbar sind.

2. "Acting for the purpose of committing any of the offences"

Eine leichte Veränderung erfährt das vorangehend dargestellte Regelungsmodell im Vorschlag der EU-Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, KOM(2010) 517 *endgültig*. Darin heißt es in der englischen Sprachfassung:

> **Article 7 – Tools used for committing offences**
>
> Member States shall take the necessary measure to ensure that the production, sale, procurement for use, import, possession, distribution or otherwise making available of the following is punishable as a criminal offence when committed intentionally and without right **for the purpose of committing any of the offences referred to in Articles 3 to 6**: […]

In der deutschen Sprachfassung lautet der Artikel:

> **Artikel 7 – Tatwerkzeuge**
>
> Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Besitzen, Verbreiten oder anderweitige Verfügbarmachen folgender **Instrumente, die zur Begehung von Straftaten im Sinne der Artikel 3 bis 6 genutzt werden**, unter Strafe gestellt werden: […]

In der deutschen Sprachfassung wichen die Übersetzer also erheblich von der englischen Vorlage ab. Während in der englischen Sprachfassung der subjektive Zweck maßgeblich ist, den der Täter mit seiner Tathandlung verfolgt, stellt die deutsche Sprachfassung rein empirisch darauf ab, wozu das Tatmittel objektiv

---

[480] Siehe *Sieber*, NStZ 2009, 358 f.

genutzt wird (von wem eigentlich?). Hierbei handelt es sich offensichtlich um ein grobes Übersetzungs- oder Redaktionsversehen, weshalb nachfolgend nur das Regelungsmodell der englischen Sprachfassung diskutiert werden soll.

a) Charakteristika dieses Regelungsmodells

Nach der englischen Sprachfassung macht sich also strafbar, wer die umschriebene Vorfeldtathandlung zum Zwecke der Begehung einer Zieltat vornimmt *(for the purpose of committing)*.

aa) „Zum Zwecke" ("for the purpose")

Dieses Tatbestandsmerkmal lässt sich so verstehen, dass der Vorbereitungstäter die Begehung der Zieltat *bezwecken* muss, also mindestens in seinen Vorsatz aufgenommen haben muss, möglicherweise sogar beabsichtigen muss. In Erwägungsgrund 10 des Richtlinienentwurfs wird davon gesprochen, dass „ohne kriminelle Absicht" keine Strafbarkeit vorliege. Da jedoch auch hier die europäische Terminologie nicht mit der deutschen gleichzusetzen ist, können aus der deutschen Auslegung des Absichtsmerkmals in den Straftatbeständen des StGB grundsätzlich keine Rückschlüsse auf das Absichtsmerkmal im jeweiligen internationalen Instrument gezogen werden. Das europäische Absichts- oder Zweckmerkmal muss daher in Einzelheiten offenbleiben. Fest steht aber, dass es auf die Begehung eines Zieldelikts gerichtet ist. Es genügt also nicht, wenn der Vorfeldtäter lediglich beabsichtigt, die Zieltat zu ermöglichen oder zu fördern. Andererseits ist es auch nicht erforderlich, dass der Vorfeldtäter den Erfolg des Zieldelikts bezweckt. Unabhängig von Grad und Richtung dieser deliktischen Absicht, kann das Merkmal erfüllt sein, sowohl wenn der Vorfeldtäter die Zieltat selbst begehen will als auch wenn er die Begehung durch *einen anderen* bezweckt.[481]

Im Vergleich zum vorhergehend erörterten Modell ergeben sich damit nur sehr feine Unterschiede. Dort musste der Vorsatz des Vorfeldtäters darauf gerichtet sein, dass irgendjemand das Computerprogramm zum Zwecke der Begehung einer Zieltat verwendet, Art. 6 Abs. 1a CCC a.E. Es genügte also auch, wenn dieser Verwender das Computerprogramm nur im Vorbereitungsstadium seines Zieldelikts einsetzen will. Denn er erfüllt in diesem Moment bereits das Merkmal des „Verwendens zum Zwecke der Begehung eines Zieldelikts". Deshalb erfüllt ein Vorfeldtäter bereits den subjektiven Tatbestand, wenn er beispielsweise ein Computerprogramm herstellt,

---

[481] Im deutschen Recht wird hieran mitunter eine Differenzierung in den subjektiven Anforderungen geknüpft: Bei einer bezweckten Selbstbegehung müsse der Vorfeldtäter bereits Tatentschluss hinsichtlich des Zieldelikts haben, während es bei der bezweckten Begehung durch einen anderen ausreiche, wenn der Vorfeldtäter Vorsatz hinsichtlich des Tatentschlusses des anderen habe, siehe SK-*Rudolphi/Stein*, § 149 Rn. 6a; siehe auch ausführlich oben I.C.1.a).

welches die Begehung eines Zieldelikts *ermöglicht* (=Vorbereitungsstadium) und er in seinen Vorsatz aufgenommen hat, dass ein anderer, der eine Zieltat begehen will, das Computerprogramm verwendet, um sich die Begehung der Zieltat zu ermöglichen.[482] Im vorliegenden Modell würde dies nicht ausreichen, weil hier der Vorfeldtäter die *Begehung* des Zieldelikts bezwecken muss, nicht bloß dessen Ermöglichung oder Förderung.

bb) Sonderfall: „fraudulent"

Eine Sonderform dieses intentionalen Bezugs stellt das Merkmal *fraudulent* (betrügerisch) dar. Es findet sich in Art. 3 Abs. 1 lit. (d) RB 2000/383/JI über die Verstärkung des mit strafrechtlichen und anderen Sanktionen bewehrten Schutzes gegen Geldfälschung im Hinblick auf die Einführung des Euro und in Art. 4 des Rahmenbeschlusses 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln. Darin heißt es, dass *betrügerisches* Anfertigen, Annehmen, Sichverschaffen oder Besitzen (in RB 2000/383/JI und RB 2001/413/JI) sowie das betrügerische Verkaufen und Weitergeben (nur RB 2001/413/JI) von bestimmten Tatmitteln mit Strafe bedroht werden solle.

Welchen genauen Regelungsinhalt die Verfasser des Rahmenbeschlusses vor Augen hatten, ist nicht zu klären. In der deutschen Umsetzung wurde das Merkmal schlicht weggelassen. Auch in der Mitteilung der Kommission „Schutz des Euro – Fälschungsbekämpfung",[483] der dazugehörigen Entschließung des Europäischen Parlaments[484] und der Empfehlung der EZB über die Verabschiedung bestimmter Maßnahmen zur Verbesserung des rechtlichen Schutzes der Euro-Banknoten und Euro-Münzen,[485] welche allesamt bedeutende Vorarbeiten zum Rahmenbeschluss darstellen,[486] finden sich hierzu keine weiteren Informationen.

Ausgehend vom Wortlaut kann „betrügerisch" jedoch verstanden werden als „zum Zwecke eines Betrugs" oder „zum Zwecke der Begehung eines Betrugs". Das betrügerische Annehmen eines Computerprogramms, das zur Geldfälschung besonders angepasst worden ist, wäre somit zu bejahen, wenn der Vorfeldtäter mit dem Annehmen den Zweck verfolgt, einen Betrug zu begehen. In dieser Auslegung ergibt sich Deckungsgleichheit mit dem oben unter aa) thematisierten Merkmal des Handelns zum Zwecke der Begehung einer Straftat.

Da der Rahmenbeschluss insoweit keine Vorgaben macht, kann *fraudulent* oder „betrügerisch" freilich auch im Sinne des Common Law ausgelegt werden und

---

482 Vgl. oben II.C.1.a).

483 KOM(1998) 474 endgültig.

484 Amtsblatt C 379 vom 7.12.1998, S. 39.

485 EZB/1998/7.

486 Vgl. EG 2, 3 und 4 des RB 2000/383/JI.

deshalb weniger voraussetzen als eine Betrugsbegehungsabsicht: Der Begriff kann auch als bloße Täuschungsabsicht verstanden werden, sodass sich die Intention des Vorfeldtäters nicht auf einen vollständigen Betrug beziehen muss. Gleichermaßen kann man für ausreichend halten, wenn der Vorfeldtäter irgendeine Vermögensschädigungsabsicht hat.

Für die Auslegung als Betrugsbegehungsabsicht spricht freilich eine Mitteilung der Kommission, die dem hier maßgeblichen Rahmenbeschluss 2001/413/JI zugrunde gelegt worden war:[487] Darin wird vorgeschlagen, dass das unbefugte Herstellen (etc.) von Fälschungsmitteln (dort „Herstellungsvorrichtungen") *zum Zwecke der Erzeugung oder Veränderung* eines beliebigen Zahlungsinstruments […] durch eine gemeinsame Maßnahme des Rates unter Strafe gestellt werde.[488] Auch hier wird also ein Handeln *zum Zwecke der Begehung einer Zieltat* angesprochen.

b) Das Dual-Use-Phänomen in diesem Regelungsmodell

In Straftatbeständen dieser Art wird das Handeln von IT-Sicherheitsbeauftragten zuverlässig ausgeschlossen, sofern unter dem tatbestandlichen Zweck eine Absicht verstanden wird, die mehr voraussetzt als dolus eventualis, dolus directus 2. Grades aber ausreichen lässt. Damit würden auch Personen als Vorfeldtäter erfasst, die um die deliktische Verwendung zwar positiv wissen (dolus directus 2. Grades), diesbezüglich aber keine zielgerichteten Absichten hegen, etwa weil ihr Handeln allein finanziellen Eigeninteressen folgt.[489] Idealerweise würde der Gesetzgeber eine solche Klarstellung bereits im Tatbestand schaffen, um etwaige Diskussionen um das Vorsatzerfordernis gar nicht erst aufkommen zu lassen.

3. Anschließungsdelikte

Auch in den internationalen Instrumenten wird nicht in allen Software-Delikten ein intentionaler Bezug des Vorfeldtäters zur Zieltat explizit vorausgesetzt. Vielmehr finden sich auch Anschließungsdelikte, nämlich in Art. 4 der Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten sowie in Art. 6 der Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

Hinsichtlich der Charakteristika dieses Modells gilt auf europäischer Ebene nichts anderes als auf nationaler: Unter Strafe soll jeweils ein in sich abgeschlosse-

---

487 Mitteilung der Kommission über eine Rahmenregelung zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln, EG 7 RB 2001/413/JI.

488 KOM(1998) 395 endgültig, S. 24.

489 Vgl. oben II.C.1.b).

nes Verhalten gestellt werden, nämlich ein bestimmter Umgang mit bestimmten Computerprogrammen, unabhängig von etwaigen Intentionen des Täters hinsichtlich der Begehung einer späteren Zieltat.[490] Auch in den internationalen Instrumenten werden mitunter intentionale Bezüge im Tatobjekt mitnormiert, die jedoch nicht zwingend im Vorfeldtäter selbst vorliegen müssen, sondern bezüglich derer er lediglich Vorsatz haben muss.[491] Aus Sicht der deutschen Strafrechtsdogmatik sind diese Konstruktionen ungewöhnlich.[492]

Hinsichtlich der Dual-Use-Problematik bei Normierung von Anschließungsdelikten gilt das oben Gesagte.[493] Rechtspolitisch stellen sich auch die oben erörterten Fragen nach einer Überkriminalisierung durch die Schaffung einer nichtakzessorischen Beihilfestrafbarkeit[494] sowie einer Unterkriminalisierung durch inkonsistente Kombinationen von Tatbestandsmerkmalen.[495] Insgesamt bestehen erhebliche Zweifel daran, dass hier tatsächlich nur solche Gefahrensituationen normiert worden sind, die derart unbeherrschbar sind, dass ihre Schaffung durchgehend kriminalisiert werden müsste.

III. Kriegswaffen- und Exportkontrollrecht

Die Dual-Use-Problematik ist keineswegs auf den Bereich des Software-Strafrechts beschränkt. Sie zeigt sich – in jeweils unterschiedlicher Ausprägung – überall dort, wo Gegenstände unter bestimmten Umständen als typische Tatwerkzeuge angesehen werden oder wo ihre (unter Umständen missbräuchliche) Verwendung als Tatwerkzeug zumindest besonders wahrscheinlich ist. Deshalb wird dort ein gewisser Umgang mit ihnen bei Strafe verboten.

Solche Konstellationen finden sich etwa im Waffen- und Sprengstoffrecht. Beispielsweise stellt § 40 Sprengstoffgesetz den nicht erlaubten Umgang mit explosionsgefährlichen Stoffen unter Strafe, wobei solche Stoffe darunter gefasst werden, die unter bestimmten Umständen zur Explosion gebracht werden *können*, aber nur soweit sie zu einer entsprechenden Verwendung als Explosivstoffe oder als pyrotechnische Sätze *bestimmt sind*. Auch hier spielen also Eignung und Bestimmung die entscheidende Rolle in der Abgrenzung zwischen tatbestandsmäßigen und tatbestandslosen Stoffen.

---

490 Vgl. ausführlich oben, I.C.2.a)aa).

491 Vgl. die oben erörterten Tatobjektmodelle II.B.1.–6.

492 Vgl. oben I.C.2.a)bb).

493 Vgl. oben I.C.2.b).

494 Vgl. oben I.C.2.c)aa).

495 Vgl. oben I.C.2.c)bb).

Das Verwaltungs- und das Strafrecht befassen sich also mit der Beurteilung von vorhandenen Gegenständen als besonders gefährlich oder missbrauchsanfällig. Solche Gegenstände müssen freilich zunächst entwickelt werden. Deshalb wird die Dual-Use-Problematik mittlerweile nicht mehr nur im Straf- und Verwaltungsrecht diskutiert, sondern schon im Bereich verfassungsrechtlich garantierter Forschungsfreiheit. Denn auch hier stellt sich die Frage, ob die Forschungsfreiheit unter gewissen Umständen einzuschränken ist. Einige Institutionen legen hier Grundsätze ethisch verantwortbarer Forschung fest und beschäftigen sich daher mit der Frage, unter welchen Umständen bestimmte *Forschungs*gegenstände als gefährlich oder missbrauchsanfällig eingestuft werden müssen und ob sie unter besonderen Gegebenheiten aus dem eigenen Forschungsprogramm ausgeschlossen werden müssen.[496]

Ein herausragendes Beispiel strafrechtlicher Regulation einer Dual-Use-Problematik stellen die ineinandergreifenden Regeln des Kriegswaffenkontrollrechts und des Außenwirtschaftsstrafrechts dar. In diesem Rechtsgebiet wird bereits seit dem CoCom-Regime von 1949 geregelt, dass ein bestimmter Umgang mit bestimmten Gegenständen, insbesondere ihr Export, immer dann verboten ist, wenn diese Gegenstände als Rüstungsgüter oder als Kriegswaffen anzusehen sind. CoCom steht für „Coordinating Committee" und bezeichnete ein Gentlemen's Agreement westlicher Mächte, wonach diese seit 1949 ihre Exportpolitik gegenüber kommunistischen Ländern abstimmten. Die Bundesrepublik trat 1950 bei, 1994 wurde das CoCom-Regime aufgelöst und 1996 durch das Wassenaar-Arrangement ersetzt.[497]

Dabei wurden und werden als Rüstungsgüter oder Kriegswaffen allerlei Gegenstände reguliert, darunter Munition, Zentrifugen, Bakterien, Viren, Pilze, DNA-Sequenzen und Toxine.[498] Stets stellt sich auch hier die Frage, wann ein konkretes Gut „zur Kriegsführung bestimmt" ist oder „besonders für militärische Zwecke konstruiert" worden ist – oder wann das Gut schlicht zivilen Nutzungszwecken dienen soll. Wird es als Kriegswaffe oder Rüstungsgut eingestuft, so ist für bestimmte Handlungen ein verwaltungsrechtliches Genehmigungsverfahren durchzuführen. Werden solche Handlungen ohne Genehmigung vorgenommen, so löst dies die Strafbarkeit aus. Es handelt sich also auch hier um Tatbestände, die den Umgang mit typischen Tatwerkzeugen schon im Vorfeld einer Rechtsgutsverletzung, also einer Zieltat, unter bestimmten Umständen bestrafen.

Für diese Arbeit sind die Regelungstechniken des Kriegswaffen- und Exportkontrollstrafrechts aus zwei vor-rechtlichen Erwägungen besonders interessant: Zum

---

[496] Siehe hierzu etwa die Hinweise und Regeln der Max-Planck-Gesellschaft zum verantwortlichen Umgang mit Forschungsfreiheit und Forschungsrisiken, online abrufbar unter http://www.mpg.de/200127/Regeln_Forschungsfreiheit.pdf [zuletzt abgerufen am 16.11.2014].

[497] Grabitz/Hilf-*Vedder/Lorenzmeier*, Art. 133 EGV, Rn. 17–19.

[498] Vgl. *Beck*, BIOspektrum 2011, 239.

einen sind die *legitimen Zwecke* im Umgang mit Rüstungsgütern seit Langem anerkannt. Dahinter stehen große Rüstungskonzerne ebenso wie kleine und mittlere Unternehmen, die mitunter seit mehreren Jahrzehnten auf dem Markt aktiv sind und mit großem wirtschaftlichem Erfolg einen erheblichen Beitrag zur Wohlfahrtssteigerung in der Bundesrepublik leisten. Zum anderen kann ein Einsatz von Rüstungsgütern zu *illegitimen Zwecken* desaströse Auswirkungen haben – nicht nur im Bereich der Nonproliferation von Nuklearwaffen und ihren Bauteilen. Es ist daher anzunehmen, dass der Gesetzgeber bei der Regulierung dieses Marktes besonders umsichtig vorgeht. Ebenso ist anzunehmen, dass er hierbei auf Erkenntnisse aus intensiver Lobbyarbeit der betroffenen Unternehmen, aber auch aus langjähriger Gesetzgebungserfahrung zurückgreift.

Im IT-Strafrecht entsteht ein solch greifbares Verständnis für Wert und Unwert gefährlicher Software erst noch. Gelegentlich wird sogar deutlich sichtbar, dass bei manchem Normgeber das Verständnis für Notwendigkeit und Wert etwa des *Penetration Testing* noch entwickelt werden musste.

Wie bereits angedeutet, unterschieden sich die jeweils legitimen Interessen in IT-Strafrecht und Rüstungskontrolle freilich nach Art und Ausmaß: Im IT-Strafrecht besteht das legitime Interesse in Test-, Analyse- und Demonstrationsverfahren, für die jeder IT-Sicherheitsbeauftragte Zugriff auf gefährliche Software benötigt. Dagegen gibt es freilich im Kriegswaffen- und Exportkontrollrecht keinen vergleichbar großen Personenkreis, der ein legitimes Interesse an einem ungehinderten Zugriff auf Kriegswaffen oder Rüstungsgüter hätte, und ebenso besteht hier das legitime Interesse des Waffenempfängers nicht vornehmlich in Test-, Analyse- und Demonstrationsverfahren. Im Vordergrund steht vielmehr das wirtschaftliche Interesse des Herstellers und Händlers von Kriegswaffen und Rüstungsgütern am Verkauf und Vertrieb solcher Gegenstände.

Auf einer höheren Abstraktionsebene ergeben sich jedoch vergleichbare rechtspolitische Herausforderungen: Bestimmte Handlungen haben ein beträchtliches Gefährdungspotential, jedoch gibt es unter gewissen Umständen erhebliche legitime Interessen an der Vornahme solcher Handlungen. Strafrechtspolitisch gilt es also auch hier, kriminelles und legitimes Verhalten tatbestandlich zu unterscheiden. Deshalb sollen nachfolgend die Regelungstechniken des Kriegswaffen- und Exportkontrollrechts eingehend analysiert werden. Konkret wird untersucht, welcher Techniken sich der deutsche Gesetzgeber bei der strafrechtlichen Regulierung dieser Bereiche bedient hat. Dabei soll nicht auf Besonderheiten und Details einzelner Tatbestände eingegangen werden, vielmehr soll das Regelungskonzept als solches analysiert werden.

Bei der Analyse des Kriegswaffen- und Exportkontrollrechts ist zu beachten, dass der Begriff des Dual-Use in diesem Bereich lediglich als Name, also deklaratorisch, gebraucht wird. Es gibt hier nämlich neben den rechtlichen Instrumenten zur Regulierung von Rüstungsgütern separate rechtliche Instrumente zur Regulie-

rung der sonstigen Exportgüter. Diese Güter werden zur Abgrenzung von den Rüstungsgütern Dual-Use-Güter genannt. Dagegen wird im IT-Strafrecht und insbesondere in der vorliegenden Arbeit der Begriff „Dual-Use“ normativ verwendet, nämlich um das Phänomen zu beschreiben, dass schädliche oder gefährliche Gegenstände auch zu legitimen Test-, Analyse- und Vorbeugezwecken benötigt werden, wodurch sich die besondere Herausforderung strafrechtlicher Regulierung ergibt. Damit kommt es zu Inkongruenzen in der Verwendung des Begriffs „Dual-Use“: Für die *Dual-Use-Problematik*, also die Frage, wie der Strafgesetzgeber den Umgang mit erforderlichen, aber potentiell schädlichen Gegenständen regulieren kann, sind auch die rechtlichen Instrumente zur Regulierung des Kriegswaffen- und Rüstungsgüterverkehrs von Interesse, weil sich gerade bei diesen Gütern die Frage stellt, wie der legitime Umgang, insbesondere ihr Export, von einer Strafbarkeit ausgenommen werden kann.

A. Überblick

Art. 26 GG statuiert in Abs. 1 Satz 1 ein verfassungsrechtliches Verbot von Handlungen, welche geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören. Im Vorfeld dieses Verbots regelt Abs. 2 Satz 1 GG, dass zur Kriegsführung bestimmte Waffen nur mit Genehmigung der Bundesregierung hergestellt, befördert und in Verkehr gebracht werden dürfen.

Näheres wird entsprechend Art. 26 Abs. 2 Satz 2 GG durch ein Bundesgesetz geregelt. Diese Aufgabe erfüllt das Gesetz über die Kontrolle von Kriegswaffen (KWKG), welches die Vorbereitung eines Angriffskrieges sowie Handlungen, die geeignet sind, das friedliche Zusammenleben der Völker zu stören, verhindern soll.[499] Das KWKG listet alle als Kriegswaffen einzustufenden Gegenstände abschließend auf und regelt den Umgang damit. Daneben tritt das allgemeinere Außenwirtschaftsgesetz, das zur Verhinderung von Störungen des friedlichen Zusammenlebens der Völker den Umgang mit Waffen anderer Art sowie Munition und sonstigem Kriegsgerät reguliert.[500] Konkretisierte Regelungen zur Exportkontrolle finden sich in der nach § 27 Abs. 1 AWG erlassenen Außenwirtschaftsverordnung, welche den Umgang mit Rüstungsgütern betrifft, sowie in der EG-Dual-Use-Verordnung,[501] soweit es um die Ausfuhr von Gütern mit doppeltem, also zivi-

---

[499] Erbs/Kohlhaas-*Lampe*, K. 189 Rn. 1.

[500] von Mangoldt/Klein/Starck-*Fink*, Art. 26 Rn. 77; Martinek/Semler/Habermeier/Flohr-*Haeberlin*, § 45 Rn. 40; Maunz/Dürig-*Herdegen*, Art. 26 Rn. 35.

[501] Verordnung (EG) Nr. 428/2009 des Rates über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (Amtsbl. 2009 Nr. L 134, Satz 1); im Folgenden Dual-Use-Verordnung.

lem und militärischem Verwendungszweck innerhalb der EU geht (Intra-EU-Verkehr von Dual-Use-Gütern).[502] Neben das Kriegswaffenkontrollgesetz, die Dual-Use-Verordnung, das Außenwirtschaftsgesetz und die Außenwirtschaftsverordnung treten im Bereich der Ausfuhrkontrolle zahlreiche völkervertragliche Rechtsakte wie das B- und C-Waffen-Übereinkommen, das Genfer Giftgasprotokoll und das Antipersonenminenübereinkommen.[503] Das Regelungsgefüge aus völkerrechtlichen und europarechtlichen Instrumenten sowie deutschen Rechtsakten im Bereich der Ausfuhrkontrolle ist deshalb mitunter komplex, weshalb hier nur zentrale Strafnormen des Kriegswaffen- und Exportkontrollrechts auf ihre Regelungstechniken hin untersucht werden sollen.

Straftatbestände in der Kontrolle von Kriegswaffen und Rüstungsgütern finden sich vor allem in den §§ 19 ff. KWKG sowie in § 33 ff. AWG. Zentrale Norm des Kriegswaffenkontrollstrafrechts ist dabei § 22a KWKG, der in Abs. 1 unter anderem die ungenehmigte Herstellung von Kriegswaffen sowie den Erwerb, die Ausübung oder die Überlassung der tatsächlichen Gewalt über Kriegswaffen unter Strafe stellt. Kernvorschrift des Außenwirtschaftsstrafrechts ist § 34 AWG,[504] der die ungenehmigte Ausfuhr und Verbringung von Rüstungsgütern unter Strafe stellt. Die Norm erfasst zum einen Güter der Ausfuhrliste, zum anderen verweist sie auf sogenannte Catch-all-Klauseln, die nicht auf das jeweilige Gut, sondern auf Wissen und Intentionen des Ausführers abstellen.

Die Regelungstechniken dieser Normen werden im Folgenden analysiert, damit im anschließenden Teil 4 der Arbeit alle Regelungstechniken des Teils 3 losgelöst von den einzelnen Regelungsmaterien für die Software-Delikte in Betracht gezogen und bewertet werden können.

B. Objektive Regelungstechniken

Das Kriegswaffenkontrollstrafrecht ist geprägt von der verfassungsrechtlichen Maßgabe, dass zur Kriegsführung bestimmte Waffen nur mit Genehmigung der Bundesregierung hergestellt, befördert und in Verkehr gebracht werden dürfen, Art. 26 Abs. 2 Satz 1 GG. Damit würde sich eigentlich zunächst die Frage stellen, wie diese Maßgabe konkretisierend ausgelegt werden kann. Der Bundesgesetzgeber hat dem Rechtsanwender jedoch die Auslegung dieses Merkmals erspart, indem er zur Konkretisierung des Kriegswaffenbegriffs kurzerhand eine abschließende Liste erstellt hat, welche die erfassten Gegenstände einzeln bezeichnet. Auch

---

[502] Martinek/Semler/Habermeier/Flohr-*Haeberlin*, § 45 Rn. 4; MüKo-*Wagner*, Außenwirtschaftsgesetz, vor § 34 Rn. 14.

[503] Maunz/Dürig-*Herdegen*, Art. 26 Rn. 45; Sachs-*Streinz*, Art. 26 Rn. 47.

[504] So *Bieneck*, wistra 2011, 89.

im Außenwirtschaftsstrafrecht ist die Ausfuhrliste das zentrale rechtstechnische Element. Ebenso wurde auf europäischer Ebene in Anlage I zur EG-Dual-Use-Verordnung eine Liste mit allen tatbestandsmäßigen Dual-Use-Gütern erstellt. Diese beiden objektiven Regelungstechniken, nämlich die abstrakte Charakterisierung von Gegenständen als „zur Kriegsführung bestimmt" und die konkrete Benennung von Gegenständen in Listen sind Gegenstand der folgenden Analyse.

1. Zur Kriegsführung bestimmt

Art. 26 Abs. 2 Satz 1 GG statuiert abstrakt, dass zur Kriegsführung bestimmte Waffen nur mit Genehmigung der Bundesregierung hergestellt, befördert und in Verkehr gebracht werden dürfen. Ähnlich wie beim oben erörterten „Zweckmodell" der deutschen Straftatbestände[505] gehen die Literaturmeinungen beim „Bestimmungsmodell" des Art. 26 Abs. 2 Satz 1 GG im Detail weit auseinander. Überwiegend wird unter der Bestimmung zur Kriegsführung quasi objektiviert eine *Eignung* zur Kriegsführung verstanden.[506] Diese soll etwa vorliegen, wenn der betreffende Gegenstand „zumindest in einem signifikanten Teil der Staatenwelt" militärisch verwendet wird.[507] Ein signifikanter Teil der Staatenwelt soll wohl deshalb erforderlich sein, weil fast jeder Gegenstand – zumindest in Bürgerkriegen und Befreiungskämpfen – auch als Waffe verwendbar ist.[508] Diese Auslegung ist dennoch bedenklich: Zwar ist es konsistent, von der tatsächlichen Verwendung eines Gegenstands auf seine entsprechende Eignung zu schließen, jedoch wird nirgends begründet, weshalb im Wege der Auslegung die *Eignung* den grundgesetzlichen Begriff der *Bestimmung* ersetzen soll. Auch wenn hier kein Straftatbestand streng am Wortlaut ausgelegt wird, sondern vielmehr der grundgesetzliche Minimalrahmen für den Gesetzgeber abgesteckt wird, wäre von den Autoren eine stärkere Begründung dafür zu erwarten, dass sie das normierte Kriterium des Bestimmt-Seins im Wege der Auslegung durch ein Aliud wie die Eignung ersetzen.

Bei den Autoren, die die kriegerische Eignung eines Gegenstands für entscheidend halten, zeigt sich sodann dasselbe Unmittelbarkeitsproblem wie im Eignungsmodell der deutschen Software-Delikte:[509] Es stellt sich die Frage, ob der Gegenstand zum kriegerischen Einsatz unmittelbar geeignet sein muss oder ob es genügt, wenn er mittelbar (also nach Umbau oder Weiterverarbeitung) kriegerisch eingesetzt werden kann. Im Rahmen von Art. 26 Abs. 2 GG wird vertreten, dass Gegenstände, die zur Herstellung von Kriegswaffen verwendet werden können, jedoch

---

505 §§ 202c Abs. 1 Nr. 2, 263a StGB, 22b Abs. 1 Nr. 3 StVG; vgl. oben I.B.2.

506 Maunz/Dürig-*Herdegen*, Art. 26 Rn. 47; Dreier-*Pernice*, Art. 26 Rn. 22; Sachs-*Streinz*, Art. 26 Rn. 39.

507 Maunz/Dürig-*Herdegen*, Art. 26 Rn. 47.

508 Sachs-*Streinz*, Art. 26 Rn. 39.

509 Vgl. § 149 Abs. 1 StGB, ausführlich oben I.B.1.a)bb).

selbst nicht *unmittelbar* im Krieg eingesetzt werden können, nicht erfasst seien.[510] Etwas anderes soll jedoch gelten, wenn Gegenstände ohne großen technischen Aufwand in eine Kriegswaffe verwandelt werden können.[511]

Schwer nachzuvollziehen ist *Pernices* Abgrenzung, wonach alle Waffen, die objektiv bei der Kriegsführung verwendet werden können, von Art. 26 Abs. 2 GG erfasst sein sollen,[512] wohingegen Waffen, die sowohl ziviler als auch militärischer Nutzung dienen können, aus dem Anwendungsbereich von Art. 26 Abs. 2 GG fallen sollen.[513] Denn einer Waffe, die (unter anderem) *militärischer Nutzung dienen kann*, wird man nicht absprechen können, dass sie *objektiv bei der Kriegsführung verwendet werden kann*.

Insgesamt wird bei den Autoren kaum zwischen Zweck, Bestimmung und Zweckbestimmung unterschieden, noch werden diese Begriffe von dem der Eignung sauber getrennt. Einig ist man sich jedoch wiederum darin, dass es weder auf einen Willen zum militärischen Einsatz noch auf eine Absicht der Störung des friedlichen Zusammenlebens der Völker im Sinne von Art. 26 Abs. 1 GG ankommen solle.[514] Mit anderen Worten bedarf es keines subjektiven Bezugs des Vorfeldtäters zur Verletzung des eigentlichen Rechtsguts.

Ausgehend von diesen abstrakten Erwägungen hat der Bundesgesetzgeber das Kriegswaffenkontrollgesetz ausgestaltet. Zur Ausfüllung des Merkmals „zur Kriegsführung bestimmte Waffen“ hat er eine Kriegswaffenliste angehängt, auf die in § 1 Abs. 1 KWKG verwiesen wird.

2. Güterliste mit Genehmigungsvorbehalt

Bei dieser Regelungstechnik wird ein nicht genehmigter Umgang mit Gütern, die auf einer bestimmten Liste stehen, unter Strafe gestellt. Es müssen also zwei Merkmale vorliegen, damit der Umgang mit dem Tatobjekt strafbar ist: Das Tatobjekt muss auf einer bestimmten Liste aufgeführt sein, und der Täter darf für seine Handlung keine Genehmigung haben. Diese Regelung findet sich etwa in § 34 Abs. 1 Satz 1 AWG i.V.m. §§ 7, 2 Abs. 1 Nr. 1 AWG, wiederum i.V.m. § 5 AWV und Anhang AL zur AWV (= Ausfuhrliste).

Die Ermächtigung zu einer Beschränkung von Rechtsgeschäften und Handlungen im Außenwirtschaftsverkehr findet sich in § 7 AWG. Gründe für eine Beschränkung sind die Gewährleistung der wesentlichen Sicherheitsinteressen der

---

510 von Mangoldt/Klein/Starck-*Fink*, Art. 26 Rn. 62.

511 Ebd.

512 Sachs-*Pernice*, Art. 26 Rn. 22.

513 Sachs-*Pernice*, Art. 26 Rn. 23.

514 von Mangoldt/Klein/Starck-*Fink*, Art. 26 Rn. 60; Maunz/Dürig-*Herdegen*, Art. 26 Rn. 47.

Bundesrepublik Deutschland (Nr. 1), die Verhütung einer Störung des friedlichen Zusammenlebens der Völker (Nr. 2), die Verhütung einer erheblichen Störung der auswärtigen Beziehungen der Bundesrepublik Deutschland (Nr. 3) und die Gewährleistung der öffentlichen Ordnung oder Sicherheit der Bundesrepublik im Sinne von Art. 46, Art. 58 Abs. 1 EGV.

§ 2 Abs. 1 AWG sieht sodann vor, dass diese Beschränkungen im Rahmen einer Rechtsverordnung als Verbot mit Genehmigungsvorbehalt (Nr. 1) oder als Verbot ohne Genehmigungsvorbehalt (Nr. 2) ausgestaltet werden können. Als entsprechende Rechtsverordnung wurde die Außenwirtschaftsverordnung erlassen, die zur Ausfüllung des § 7 AWG eine Genehmigungspflicht für bestimmte Güter in § 5 AWV statuiert. Welche Güter von dieser Genehmigungspflicht erfasst werden, ergibt sich sodann aus der Ausfuhrliste, die als Anlage AL der Außenwirtschaftsverordnung angehängt ist. Offen bleibt dabei jedoch, für welches Exportgut aus der Liste welcher Beschränkungsgrund aus § 7 AWG einschlägig ist. Die in § 7 Abs. 1 Nr. 1–3 AWG vorgenommene Differenzierung wird in § 5 AWV und der entsprechenden Ausfuhrliste völlig aufgehoben.[515]

Im Kriegswaffenkontrollgesetz gibt es eine ganz ähnliche Struktur. Dort statuiert § 22a Abs. 1 KWKG, dass bestraft wird, wer Kriegswaffen herstellt, erwirbt, einem anderen überlässt, befördert oder befördern lässt, ohne dass er eine entsprechende Genehmigung erhalten hat. Als Kriegswaffen werden laut der Legaldefinition des § 1 Abs. 1 KWKG „zur Kriegsführung bestimmte Waffen“ verstanden. Welche Waffen hierunter wiederum fallen, wird sodann durch die Kriegswaffenliste in der Anlage zum KWKG abschließend festgelegt. Damit ist die Legaldefinition „zur Kriegsführung bestimmt“ obsolet.

Freilich folgt die Legaldefinition dem Wortlaut des Art. 26 Abs. 2 GG und in diesem Sinne erlangt das Merkmal „zur Kriegsführung bestimmt“ doch wieder eine Geltung: Wenn eine Waffe als Kriegswaffe in die Kriegswaffenliste aufgenommen wird, so ist jedenfalls grundgesetzlich überprüfbar und zu überprüfen, ob diese Waffe tatsächlich zur Kriegsführung bestimmt ist. Ist dies nicht der Fall, so verstößt ihre Aufnahme in die Liste zwar nicht gegen das KWKG selbst, kann aber auch nicht mit Art. 26 Abs. 2 Satz 1 GG gerechtfertigt werden.[516]

Anders als in AWG und AWV besteht bei Kriegswaffen allerdings auch bei Nichtvorliegen von Versagungsgründen kein Anspruch auf eine Genehmigung, § 6 Abs. 1 KWKG. Nach überwiegender Auffassung ist dies jedoch auf eine verfassungsrechtliche Besonderheit zurückzuführen: Art. 26 Abs. 2 GG stellt ein repressives Verbot mit Befreiungsvorbehalt auf, sodass die allgemeine Handlungs-

---

515 So auch *Bieneck*, wistra 2011, 90.

516 So auch Maunz/Dürig-*Herdegen*, Art. 26 Rn. 48.

freiheit ins Gegenteil verkehrt wird und kein subjektives öffentliches Recht auf Erteilung einer Genehmigung entstehen kann.[517]

§ 34 Abs. 1 Satz 1 AWG regelt, dass bestraft wird, wer Güter aus bestimmten Abschnitten der Ausfuhrliste ohne Genehmigung ausführt oder verbringt. Da § 34 Abs. 1 Satz 1 AWG die abstrakten Kriterien nicht nennt, nach denen ein Gegenstand als Tatobjekt infrage kommt, handelt es sich hierbei um eine Blankettnorm.[518] In § 34 Abs. 1 Satz 1 Nr. 1 AWG sind dabei die Abschnitte der Ausfuhrliste genannt, in denen Güter aus den Bereichen der nationalen Ausfuhrkontrolle aufgeführt sind, während in Nr. 2 die Güter aufgeführt sind, die nach der EG-Dual-Use-Verordnung der Ausfuhrkontrolle unterworfen sind.[519] Grundsätzlich erfasst die Ausfuhrliste in Abschnitt C alle Güter der Liste zur EG-Dual-Use-Verordnung (Anhang I) in vollem Umfang.[520] Zu inhaltlichen Abweichungen kann es allenfalls aufgrund zeitlicher Verschiebungen zwischen den Aktualisierungen der Listen kommen.[521]

Damit bestimmen allein die einzelnen Einträge in der Ausfuhrliste über das Tatobjekt des § 34 Abs. 1 Satz 1 AWG. Diese lassen sich unterteilen in rein deskriptive und normative Einträge.

a) Deskriptive Listeneinträge

Die deskriptiven Einträge in der Ausfuhrliste beschreiben Eigenschaften, Maße oder Funktionen von Gegenständen rein deskriptiv so, dass man im Grunde durch Nachmessen überprüfen kann, ob ein bestimmter Gegenstand von der einschlägigen Listenposition erfasst ist.[522]

Gleich der erste Eintrag in Teil I A, Position 0001 etwa erfasst „Handfeuerwaffen mit glattem Lauf mit einem Kaliber kleiner als 20 mm, andere Handfeuerwaffen und Maschinenwaffen mit einem Kaliber von 12,7 mm oder kleiner […]", sofern sie eines der nachfolgenden Merkmale a)–d) erfüllen. Unter Buchstabe c) findet sich dann etwa die Ausführung „Waffen, die hülsenlose Munition verwenden". Hier ist es einer Tatsachenfeststellung zugänglich, ob eine Waffe einen glatten Lauf hat, ob ihr Kaliber kleiner als 20 mm ist und ob die verwendete Munition

---

[517] Siehe von Mangoldt/Klein/Starck-*Fink*, Art. 26, Rn. 75. Differenzierend Maunz/Dürig-*Herdegen*, Art. 26 Rn. 55.

[518] *Bieneck*, wistra 2008, 209; Erbs/Kohlhaas-*Diemer*, A 217 Außenwirtschaftsgesetz, § 34 Rn. 2; MüKo-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 1; für § 22a KWKG gilt dies entsprechend, siehe Erbs/Kohlhaas-*Lampe*, K 189 KWKG, § 22a Rn. 2 ff.

[519] MüKo-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 1.

[520] *Bieneck*, wistra 2010, 10.

[521] *Schlegel/Schanze*, Compliance in der Außenwirtschaft, S. 103.

[522] In der Literatur wird freilich feinsinnig diskutiert, ob es überhaupt deskriptive Tatbestandsmerkmale geben kann, siehe dazu *Roxin*, AT I, S. 308 f.

Hülsen hat oder hülsenlos ist. Der Sinngehalt dieser Merkmale erschließt sich unmittelbar aus der Anschauung, deshalb sind dies nach überkommener Auffassung deskriptive Tatbestandsmerkmale.[523]

b) Normative Listeneinträge: „besonders konstruiert für militärische Zwecke"

An derselben Position findet sich aber unter Buchstabe b) 1. auch ein Eintrag, der jedenfalls auslegungsbedürftig ist und eine Wertung voraussetzt: „Waffen mit glattem Lauf, besonders konstruiert für militärische Zwecke". Wann eine Waffe besonders für militärische Zwecke konstruiert ist, ist schon wegen des Zweckbegriffs keine rein deskriptive, sondern eine normative Frage.

In der englischen Fassung internationaler Rechtsinstrumente der Rüstungskontrolle wie dem CoCom-Regime vom 1. Januar 1950 *(Coordinating Committee for East-West-Trade Policy)*, dessen Nachfolger, dem *Wassenaar-Arrangement*,[524] dem *Missile Technology Control Regime* MTCR oder auch der englischen Fassung des Anhangs zur Dual-Use-Verordnung lautet dieses Merkmal stets „specially designed". Damit wird die Parallele zur Regelungstechnik der Software-Delikte und der dortigen Dual-Use-Problematik augenfällig.[525] Im Recht der Exportkontrolle zeigen sich nämlich dieselben Auslegungsprobleme wie im Software-Strafrecht, allerdings bereits seit einigen Jahrzehnten: das *Designed*-Sein – unabhängig davon, ob man es als Hergestellt-Sein, Ausgelegt-Sein oder Konstruiert-Sein übersetzt – kann man subjektiviert oder objektiviert auslegen. Legt man es subjektiviert aus, so ist der konkrete Wille des historischen Herstellers (genauer: *designers*) maßgeblich. Legt man es objektiviert aus, so ist eine wertende Betrachtung der Funktionen des Gegenstands ausschlaggebend – allerdings wirft dies das Problem auf, nach welchen Wertmaßstäben sich die zweckgebundene Konstruktion des Gegenstands von seiner schlichten oder auch besonderen Eignung für bestimmte Einsatzarten abgrenzen lässt.

Im Exportkontrollrecht wurde von Anfang an eine objektivierte Auslegung des Merkmals „specially designed" vorgenommen: So wurde im CoCom-Regime definiert, dass besonders zu militärischen Zwecken konstruierte Gegenstände sich *körperlich* von anderen Gegenständen unterscheiden. Dies müsse materiell und physisch offensichtlich sein und sich in strukturellen Eigenheiten des Gegenstands widerspiegeln.[526] Im Anhang zum MTCR findet sich ebenfalls eine objektive Defi-

---

523 Vgl. Jescheck/*Weigend*, S. 130, 269 f.

524 Vgl. dazu *Harder*, in: Wabnitz/Janovsky, 21. Kapitel, Rn. 13 ff.

525 Vgl. dazu oben I.B.3. und 4. sowie II.B.2. und 3.

526 Nach *Bieneck*, wistra 2010, 12 f.; dieser zitiert wiederum aus *Welzien*, Overruled!, The Export Practitioner, Vol. 10 Nr. 3 (März 1996), die tatsächliche Definition des CoCom-Regime ist aus Geheimhaltungsgründen nicht bekannt.

nition, die besagt, dass ein Gegenstand nur dann besonders zu einem militärischen Zweck konstruiert ist, wenn er *keine andere Funktion oder Gebrauchsweise* hat.[527]

Auch das Verwaltungsgericht Frankfurt a.M. entschied sich am 17.2.2005 für eine objektivierte Auslegung des Begriffs.[528] Es komme nicht auf die subjektive Nutzungsabsicht des Eigentümers an,[529] sondern auf objektive Merkmale, die man dem Gegenstand selbst (in diesem Falle: einem Hubschrauber) ansehen müsse.[530] Als Beurteilungsmaßstab wandte das Gericht eine Kosten-Nutzen-Rechnung an: Der Rückschluss auf die *besonders zu militärischen Zwecken erfolgte Konstruktion* des Gegenstands sei zulässig, wenn die konkrete Konstruktion oder die Änderungen am Gegenstand für die zivile Nutzung entweder *keine Vorteile* bieten oder nur solche, auf die ein ziviler Nutzer im Hinblick auf die *Kosten der Anschaffung und des Betriebs vernünftigerweise verzichten* würde.[531] Auch hält das Verwaltungsgericht Faktoren außerhalb des fraglichen Gegenstands selbst für irrelevant. So komme es nicht darauf an, *für wen* oder auf wessen Wunsch der Gegenstand konstruiert oder geändert wird. Die Konstruktion diene nicht schon deshalb militärischen Zwecken, weil sie von einem Militär gesondert in Auftrag gegeben werde.[532] Ebensowenig komme es auf die Betitelung des Gegenstands durch seinen Hersteller an, selbst wenn der Gegenstand den Zusatz „M“ im Namen trägt (im konkreten Fall wurden Hubschrauber für militärische Abnehmer als „BO 105 M“ bezeichnet, während die Hubschrauber im Übrigen das „M“ nicht im Namen trugen).[533]

Hiervon wich der 5. Strafsenat des BGH jedoch ab, als er am 28. März 2007 einen Revisionsbeschluss in einem anderen Verfahren fasste.[534] Zunächst hielt er dort fest, dass „die Zweckbestimmung“ auch eine subjektive Komponente habe.[535] Gemeint ist damit, dass die Rede von einem besonders für militärische Zwecke konstruierten Gegenstand voraussetze, dass der Konstrukteur wohl irgendwie subjektiv eine militärische Verwendung des Gegenstands oder zumindest die Eignung hierfür ins Auge gefasst haben müsse. Konkretere Aussagen lassen sich hieraus

---

527 MTCR Equipment, Software and Technology Annex vom 13.4.2011, Kapitel 3.a) (S. 15), online abrufbar unter http://www.mtcr.info/english/MTCR-April2011-Technical-Annex.pdf [zuletzt aufgerufen am 14.11.2014].

528 VG Frankfurt a.M. Urteil vom 17.2.2005, Az. 1 E 7512/03, online abrufbar unter http://www.lareda.hessenrecht.hessen.de/jportal/portal/t/s15/page/bslaredaprod.psml?&doc.id=MWRE060001872%3Ajuris-r01&showdoccase=1&doc.part=L [zuletzt aufgerufen am 16.11.2014].

529 Erst recht kommt es wohl nicht auf Absichten des Herstellers an. Allerdings wird dies vom VG nicht ausdrücklich gesagt.

530 A.a.O., Rz. 31.

531 A.a.O., Leitsatz Nr. 3. Dem schließt sich *Bieneck*, wistra 2010, 17, an.

532 A.a.O., Rz. 30.

533 A.a.O., Rz. 33.

534 BGH NStZ 2007, 645 ff.

535 A.a.O., 646 (Rz. 4).

wohl nicht ableiten. Der Senat führt sodann aber fort, dass es auf diese subjektive Komponente ohnehin nicht ankommen könne, da ein individueller Zweck kaum jemals zweifelsfrei festzustellen sei. Stattdessen füllten „die detaillierten Beschreibungen der Ausfuhrliste“ das Merkmal „besonders konstruiert für militärische Zwecke“ aus. Deshalb seien alle in der Ausfuhrliste genannten Gegenstände tatbestandlich erfasst, es sei denn, eine der Ausnahmen in den Anmerkungen der Ausfuhrliste liege vor. Diese beschrieben nämlich Verwendungszwecke, „die die Liste selbst als nicht ‚besonders konstruiert für militärische Zwecke‘ bezeichnet und damit von dem Genehmigungserfordernis ausnimmt“.[536]

Bei genauer Betrachtung des konkreten Falls zeigt sich jedoch, dass sich diese Auslegung nicht aufrechthalten lässt: Gegenstand dieses Verfahrens waren umgebaute Autos, die mit schutzsicherer Panzerung, schusssicheren Reifen und einer besonderen Kommunikationstechnik ausgerüstet worden waren. Tatsächlich normiert Position 0006 des Teils I A der Ausfuhrliste, welche Landfahrzeuge und Bestandteile für Landfahrzeuge vom Genehmigungserfordernis und damit vom Tatbestand des § 34 Abs. 1 Nr. 1 AWG erfasst werden. Position 0006a enthält „Landfahrzeuge und Bestandteile hierfür, besonders konstruiert oder geändert für militärische Zwecke“. Position 0006b enthält „geländegängige Fahrzeuge mit Allradantrieb, die nicht von Unternummer 0006a erfasst werden, die mit metallischen oder nicht-metallischen Werkstoffen hergestellt oder ausgerüstet wurden, um einen [bestimmten] ballistischen Schutz […] zu bewirken“.

Es folgen mehrere Anmerkungen zu Position 0006. Anmerkung 1 beginnt mit den Worten „Unternummer 0006a schließt ein:“ und nennt sodann einige Fahrzeuge und deren Spezifika, darunter „b) gepanzerte Fahrzeuge“. Anmerkung 2 besagt, unter welchen Umständen eine Änderung eines Fahrzeugs das Merkmal „Änderung für militärische Zwecke“ im Sinne der Unternummer 0006a erfüllt. Dies ist dann der Fall, wenn Bestandteile geändert werden, die ihrerseits wiederum „besonders konstruierte militärische Bestandteile“ sind. Es folgt der Zusatz „Solche Bestandteile schließen ein:“ und daran schließt die Aufzählung einiger Bestandteile, darunter „b) Panzerschutz von wichtigen Teilen (z.B. Kraftstofftanks oder Fahrzeugkabinen)“. Hierauf folgt Anmerkung 3, die besagt: „Nummer 0006 erfasst keine zivilen Sonderschutzlimousinen und Werttransporter mit Schutzpanzerung“.

Der 5. Strafsenat ging in diesem Beschluss offenbar davon aus, dass die Aufzählungen in Anmerkung 1 und Anmerkung 2 jeweils abschließend seien. Nur so lässt sich seine Behauptung deuten, die „detaillierten Beschreibungen“ der AL füllten das Merkmal „konstruiert für militärische Zwecke“ aus. Es spricht jedoch nichts dafür, dass diese Aufzählungen abschließend seien. Vielmehr legt die Formulierung „schließt ein“ nahe, dass es daneben noch weitere Gegenstände geben kann, die das Merkmal erfüllen. Auch systematisch lässt sich diese These nicht halten: In

---

[536] Ebd.

Teil I A Position 0001b 1. der AL werden „Waffen mit glattem Lauf, besonders konstruiert für militärische Zwecke“ erfasst, ohne dass im Nachgang durch irgendwelche Beschreibungen das Merkmal „konstruiert für militärische Zwecke“ ausgefüllt würde. Auch interpretiert der BGH die Ausnahmeregelung in Anmerkung 3 zu Position 0006 so, als bestünde ihr Sinn darin, konkrete Fälle zu bestimmen, in denen keine besondere militärische Konstruktion vorliegt. Diese Auffassung kann aber schon deshalb nicht richtig sein, weil Anmerkung 3 gleichermaßen für Position 0006a und 0006b gilt und in Position 0006b die besondere Konstruktion zu militärischen Zwecken gar nicht vorausgesetzt wird, also auch nicht von Anmerkung 3 ausgeschlossen werden kann. Anmerkung 3 ist daher ein *allgemeiner* Ausnahmetatbestand.

Der 5. Strafsenat konnte hier wohl nur deshalb eine Auslegung des Merkmals „besonders konstruiert für militärische Zwecke“ vermeiden, weil in dem konkreten Fall die verfahrensgegenständlichen Autos unzweifelhaft unter eine der aufgezählten Kategorien in den Anmerkungen 1 und 2 fielen. Möglicherweise wollte der BGH diesen schwierigen Auslegungsfragen auch nicht zuviel Aufmerksamkeit schenken, weil eine Strafbarkeit des Angeklagten ohnehin daran scheiterte, dass er die Autos nie ausgeführt hatte.

Brauchbar ist aber die eingangs getroffene Klarstellung des BGH, dass es nicht auf die historischen Intentionen des Herstellers ankommen könne. Da zudem im konkreten Fall das Merkmal des militärischen Zwecks bejaht worden ist, obwohl die Autos tatsächlich zu zivilen Schutzzwecken in den Zielländern verwendet werden sollten,[537] lässt sich der Entscheidung weiterhin entnehmen, dass es für die Beurteilung des Zweckmerkmals auch nicht auf die Verwendungsabsichten des Empfängers ankommen kann. Im Übrigen lässt sich die vom BGH (nicht) vorgenommene Auslegung jedoch nicht verallgemeinern.

In einer Entscheidung vom 23.11.1995 hatte der 1. Strafsenat des BGH das Merkmal „besonders konstruiert für militärische Zwecke“ auch noch ganz anders ausgelegt.[538] Darin hielt der BGH noch fest, dass es für die Beurteilung der „besonderen Konstruktion zu militärischen Zwecken“ darauf ankomme, welchen Zwecken der Gegenstand *nach den Vorstellungen des Erbauers* dienen soll. Die militärische oder zivile Eignung des Gegenstands entfalte zwar Indizwirkung für das Vorliegen eines militärischen beziehungsweise zivilen Zwecks, sodass es gegen eine Konstruktion zu militärischen Zwecken spreche, wenn der Gegenstand *auch zivil* nutzbar sei, jedoch sei diese Indizwirkung widerlegt, wenn zweifelsfrei feststehe, dass der Hersteller den Gegenstand zu militärischen Zwecken erdacht und

---

[537] Vgl. *Bieneck*, wistra 2010, 17.

[538] BGH NJW 1996, 1355 ff.

geliefert habe.[539] Die Abgrenzung folge also nicht allein der Konstruktion, vielmehr sei der vom Hersteller gesetzte Zweck maßgebend.[540]

Der BGH diskutiert dann noch die objektivierte Auslegung, wie sie in der Genehmigungspraxis des (damals zuständigen) Bundesamtes für Wirtschaft gängig war, und lehnt diese mit knapper Begründung ab. In der Auslegung des Bundesamts waren Gegenstände nur dann „besonders konstruiert für militärische Zwecke", wenn sie ausschließlich für einen militärischen Zweck entworfen und auch *nur dafür verwendbar* waren.[541] Diese Auslegung hält der BGH für zu eng, insbesondere weil sich auch zufällig oder jedenfalls unbeabsichtigt eine zivile Nutzbarkeit eines Gegenstands ergeben könne. Mit Blick auf den Regelungszweck der AL und ihren Wortlaut seien solche Gegenstände nicht vom Tatbestand auszunehmen.[542]

Die Kritik an dieser subjektivierten, konkret-historischen Auslegung hatte der BGH in seiner oben dargestellten Entscheidung vom 28.3.2007[543] selbst gebracht: Der individuelle und subjektive Zweck, den der historische Hersteller mit seiner Konstruktion verfolgt hat, lässt sich nur schwer nachvollziehen und kaum nachweisen. Vor allem aber geht von einer solchen subjektiven Zweckvorstellung des Herstellers allein überhaupt keine Gefahr für die Rechtsgüter-Trias des Exportkontrollrechts gemäß § 7 AWG aus, nämlich die Sicherheit der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker und die auswärtigen Beziehungen der Bundesrepublik Deutschland.[544] Betrachtet man allein die Konstruktion des Exportgutes, so birgt diese nur dann ein objektives Gefahrenpotential für die geschützten Rechtsgüter, wenn sie *objektiv* auf militärische Zwecke ausgerichtet ist.

Nachdem sich der 5. Strafsenat des BGH also in dem Beschluss vom 28.3.2007 zumindest von der subjektivierten Auslegung des 1. Strafsenats aus dem Jahr 1995 distanziert hatte, erging im Jahr 2010 zuletzt ein Beschluss des 3. Strafsenats, in dem auch dessen eigener Beschluss von 2007 eine wichtige Korrektur erhielt.[545] Zunächst hält der 3. Strafsenat des BGH dort fest, dass das Merkmal „besonders konstruiert für militärische Zwecke" ein auslegungsbedürftiger unbestimmter

---

539 BGH NJW 1996, 1355.

540 Ebd.

541 Ebd., unter Verweis auf *Thietz-Bartram*, RIW 1994, 840.

542 Ebd.

543 BGH NStZ 2007, 645 ff.

544 *Bieneck*, wistra 2010, 15; der vermutet, dass die subjektivierte Auslegung in diesem Verfahren aus politischen Gründen angewandt worden ist. Nach intensiver medialer Berichterstattung zu dubiosen Rüstungsexporten in den Irak war das Exportkontrollrecht zum Urteilszeitpunkt erheblich verschärft worden (§§ 5c, 5d AWV, siehe dazu I.C.) Offensichtlich wollte man den angeklagten Irak-Exporteur so wenig wie möglich in den Genuss des milderen Tatzeitrechts kommen lassen.

545 BGH NJW 2010, 2365 ff.

Rechtsbegriff sei.[546] Damit widerspricht er dem Beschluss des 5. Strafsenats, wonach allein anhand der deskriptiven Listeneintragungen und ihren Anmerkungen das Merkmal des militärischen Zwecks ausgefüllt werde. Sodann spricht sich der 3. Senat für den in der Literatur einhellig vertretenen objektiven Ansatz zur Auslegung des Tatbestandsmerkmals aus.[547]

Möchte man die drei Beschlüsse zusammenfassen, so lässt sich festhalten, dass die subjektivierte Auslegung des Merkmals „besonders konstruiert für militärische Zwecke" wohl *nicht* weiter aufrechterhalten wird. Insofern dürfte der Beschluss von 1995 eine (möglicherweise politisch motivierte) Eintagsfliege gewesen sein. Darüber hinaus dürfte es als geklärt angesehen werden, dass dem Merkmal des „besonders für militärische Zwecke Konstruiert-Seins" dann keine eigenständige Bedeutung zukommt, wenn sein Inhalt durch die konkretisierenden Aufzählungen in den Anmerkungen zu den Positionen der AL ausgefüllt ist. Damit bleibt aber die Bewertung von Gegenständen fraglich, welche keine Beschreibung aus einer der Anmerkungen erfüllen. Zur Beurteilung dieser Gegenstände muss das Merkmal „besonders für militärische Zwecke konstruiert" ausgelegt werden. Hierfür stellt die wirtschaftliche Betrachtungsweise des Verwaltungsgerichts Frankfurt a.M. bislang den einzigen gerichtlich angewandten Auslegungs- und Beurteilungsmaßstab dar.

Ausgehend vom geschützten Rechtsgut hat das Merkmal des militärischen Zwecks offensichtlich die Funktion, solche Gegenstände zu erfassen, bei denen entweder ein militärischer Einsatz wahrscheinlich ist oder ein möglicher militärischer Einsatz besonders schädlich für die geschützten Rechtsgüter wäre. Nach diesem Befund könnten aber auch die vom VG verworfenen Aspekte eine Rolle bei der Beurteilung des Zwecks spielen: So ist es durchaus denkbar, bei einem militärisch einsetzbaren Gegenstand aufgrund seiner Betitelung oder Vermarktung darauf zu schließen, dass er wahrscheinlich militärisch eingesetzt werden wird und besonders hierfür konstruiert worden ist.[548] In diesen Fällen besteht also ein Restrisiko für die Konstrukteure. Allerdings ist im Exportkontrollrecht für diese Fälle noch eine weitere Sicherung eingebaut: Liegt ein taugliches Tatobjekt vor, so löst dies zunächst eine Genehmigungspflicht für die geplante (Tat-)Handlung aus.

3. Zusammenfassung der objektiven Regelungstechniken

Auffällig ist die stark ausgeprägte deskriptive Regelungstechnik im Rüstungskontrollrecht. Zu einem erheblichen Teil werden technische Spezifika exakt festgelegt, die einen Gegenstand zum Tatobjekt machen. Diese Spezifika gehen so stark

---

546 A.a.O., Rz. 44.

547 A.a.O., Rz. 46.

548 Wenn – wie im konkreten Fall – die Betitelung lediglich lizenzrechtliche Gründe hat, ist dieses Argument freilich entwertet.

ins Detail, dass sie für Laien technisch oftmals nicht verständlich sind.[549] In Teil 4 der Arbeit soll verglichen werden, wie gut sich eine solche Regelungstechnik auch im Software-Strafrecht einsetzen ließe.

Daneben gibt es im Wesentlichen zwei normative Regelungstechniken, die denen des Software-Strafrechts ähneln: Zum einen wird darauf abgestellt, wozu ein Gegenstand *bestimmt* ist, zum anderen wird darauf abgestellt, wozu er *konstruiert* ist. Damit wird die Parallele zu den Regelungstechniken des Software-Strafrechts deutlich, in denen maßgeblich ist, wozu ein Gegenstand bestimmt,[550] *designed*/ entworfen[551] oder hergestellt[552] ist oder was der vom Hersteller bestimmte Zweck des Computerprogramms ist.[553] Dementsprechend konnte gezeigt werden, dass hier wie dort ähnliche Auslegungsprobleme entstehen und ähnliche Lösungsvorschläge angeboten werden. Auch dies wird im Vergleich der Regelungstechniken in Teil 4 der Arbeit näher erörtert.

C. Subjektives Modell: "Catch-all" bei Kenntnis von geächteten Verwendungszwecken

Neben dem Listenmodell findet sich im Außenwirtschaftsstrafrecht ein subjektives Modell, bei dem die Strafbarkeit des Ausführers maßgeblich darauf beruht, dass er *weiß*, dass die Güter im Käufer- oder Bestimmungsland militärisch verwendet werden sollen. In diesen Fällen spielt es keine Rolle, ob sie in der Ausfuhrliste genannt sind, weil in diesem Falle *alle* Güter erfasst werden. Man spricht daher auch von „Catch-all-Klauseln".[554] Solche „Catch-all-Klauseln finden sich nicht nur in Außenwirtschaftsgesetz und Außenwirtschaftsverordnung, sondern etwa auch in Art. 4[555] und Art. 5[556] der EG-Dual-Use-Verordnung.

Die zwei prominentesten Catch-all-Klauseln des Außenwirtschaftsstrafrechts finden sich in § 5c Abs. 1 Satz 1 und Abs. 2 Satz 1, 2 AWV. Die „Mechanik" von AWV und AWG ist allerdings etwas kompliziert: Gemäß § 34 Abs. 2, § 33 Abs. 1, § 2 Abs. 1 i.V.m. § 7 Abs. 1 AWG wird wiederum i.V.m. § 70 Abs. 1 Nr. 2 AWV ein Verstoß gegen § 5c Abs. 1, 2 AWV zu einem Teil eines Straftatbestands. Denn

---

[549] Beispiel: „elastomermodifizierte, gegossene, zweibasige ‚Treibstoffe' (EMCDB), die bei 233 K (–40 °C) eine Dehnungsfähigkeit von mehr als 5 % bei größter Beanspruchung aufweisen", Ausfuhrliste Teil I A, Position 0008, Nr. 2 b) 5.

[550] Siehe oben I.B.3.

[551] Siehe oben I.B.4.

[552] Siehe oben I.B.4.

[553] Siehe oben I.B.2.

[554] Siehe nur MüKo-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 62.

[555] Siehe Grabitz/Hilf-*U. Karpenstein*, E 16 Dual-Use-Verordnung, Art. 4 Rn. 1 ff.

[556] Siehe MüKo-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 67.

§ 34 Abs. 2 AWG regelt, dass Verstöße gegen § 33 Abs. 1 AWG unter bestimmten Umständen Straftaten darstellen. § 33 Abs. 1 AWG regelt wiederum, dass es sich hierbei um Verstöße gegen eine Rechtsverordnung nach § 2 Abs. 1 i.V.m. § 7 Abs. 1 AWG handeln muss, vorliegend also die AWV, jedoch nur soweit die AWV wiederum auf § 33 Abs. 1 AWG verweist. Der eigentliche Verstoß ist sodann in § 5c Abs. 1 Satz 1, Abs. 2 Satz 1, 2 AWV normiert. Der erforderliche Verweis auf § 33 Abs. 1 AWG findet sich schließlich in § 70 Abs. 1 Nr. 2 AWV. Diese Regelungs- und Verweisungstechnik ist unübersichtlich und kompliziert. Die Bundesregierung plant deshalb eine Reform von AWG und AWV im Interesse der deutschen Exporteure, insbesondere der kleinen und mittelständischen Unternehmen in Deutschland. Die Regelungen von AWG und AWV sollen gestrafft und ihre Lesbarkeit verbessert werden.[557]

§ 5c AWV besagt im Groben, dass auch die Ausfuhr *aller* Güter, die *nicht* in der Ausfuhrliste genannt sind, genehmigungspflichtig ist, wenn der Ausführer *weiß*, dass sie für eine militärische Endverwendung bestimmt sind. Für dieses „Wissen um die militärische Endverwendung" normiert § 5c AWV eine formelle und eine materielle Art des Wissens: Abs. 1 Satz 1 sieht eine entsprechende Unterrichtung des Ausführers durch das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) vor, Abs. 2 Satz 1 spricht von Kenntnis. Abs. 1 Satz 2 präzisiert, was unter einer militärischen Endverwendung zu verstehen ist, zu der die Güter mit Wissen des Ausführers bestimmt sein müssen. Liegt all dies vor, so muss die Tathandlung des Ausführers geeignet sein, die geschützten Rechtsgüter des § 34 Abs. 2 AWG (erheblich) zu gefährden. Erst dann wird die Strafbarkeit ausgelöst.

1. Formell: Unterrichtung des Ausführers

§ 5c Abs. 1 Satz 1 AWV besagt, dass die Ausfuhr von Gütern, die nicht in der Ausfuhrliste genannt sind, der Genehmigung bedarf, wenn der Ausführer vom BAFA *unterrichtet worden ist*, dass diese Güter ganz oder teilweise für eine militärische Endverwendung bestimmt sind oder bestimmt sein können.[558] Diese Unterrichtung des Ausführers durch das BAFA ist konstitutiv für die Genehmigungsbedürftigkeit, damit stellt also das BAFA selbst die Genehmigungsbedürftigkeit her.[559]

---

[557] Siehe Pressemitteilung des BMWi vom 15.8.2012, online abrufbar unter http://www.bmwi.de/DE/Presse/pressemitteilungen,did=503568.html [zuletzt abgerufen am 22.2.2013].

[558] Zusätzlich muss das Käufer- oder Bestimmungsland auf der Länderliste K genannt sein. Auf dieser Liste, die als Anlage L zur Außenwirtschaftsverordnung geführt wird, ist derzeit nur Kuba genannt [Stand: 17.11.2011]. Die Begrenzung auf Exporte in bestimmte Länder soll hier nicht weiter vertieft werden, da sie für die Dual-Use-Problematik weniger relevant ist.

[559] Vgl. *Bieneck*, wistra 2008, 210; MK-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 29.

2. Materiell: Kenntnis des Ausführers

§ 5c Abs. 2 Satz 1 AWV normiert zusätzlich, dass der Ausführer das BAFA unterrichten muss, wenn ihm *bekannt ist*, dass die Güter, die er ausführen möchte, für eine militärische Endverwendung im Sinne des Absatzes 1 bestimmt sind. Im Gegensatz zu Abs. 1 Satz 1 wurde hier also auf die Erweiterungen „ganz oder teilweise" sowie „oder bestimmt sein können" verzichtet. Kenntnis bedeutet hier nach allgemeiner Auffassung positives Wissen.[560] Hierzu muss er alle ihm vorliegenden Erkenntnisquellen nach allgemeiner Lebenserfahrung realistisch bewerten.[561] Zu diesen Erkenntnisquellen zählen die sogenannten Frühwarnschreiben des BMWi nicht, solange sie keine konkreten Belege für eine Bestimmung zur militärischen Endverwertung enthalten, sondern lediglich generelle Warnsignale geben.[562]

Besteht nun eine solche Kenntnis des Ausführers, so wird dadurch allerdings keine Genehmigungspflicht ausgelöst, sondern ein unmittelbares Ausfuhrverbot und zunächst eine Unterrichtungspflicht gegenüber dem BAFA. Dieses entscheidet sodann darüber, ob eine Genehmigungspflicht besteht, § 5c Abs. 2 Satz 1 Hs. 2 AWV. Das Ausfuhrverbot endet erst, wenn das BAFA eine Genehmigung erteilt oder entscheidet, dass keine Genehmigung erforderlich ist, Abs. 2 Satz 2.

Diese Regelungstechnik ist im Detail etwas unsauber, denn streng genommen besteht hier ex ante zu keinem Zeitpunkt eine Genehmigungspflicht. Die Kenntnis löst zunächst nur die Unterrichtungspflicht aus. Ab der Unterrichtung beginnt eine Phase, in der die Behörde zu einer Entscheidung kommen muss, ob eine Genehmigungspflicht besteht. Diese Phase wird dadurch beendet, dass die Behörde entweder eine Genehmigung erteilt oder entscheidet, dass keine Genehmigungspflicht besteht.

Würde also der Ausführer seine Güter noch vor der Entscheidung durch die Behörde ausführen, so würde er zwar gegen das Verbot aus § 5c Abs. 2 Satz 2 AWV verstoßen, allerdings ist fragwürdig, ob er auch eine Ordnungswidrigkeit nach § 33 Abs. 1 AWG oder gar eine Straftat nach § 34 Abs. 2 AWG begeht. Denn diese Tatbestände sehen vor, dass er *ohne Genehmigung* die Tathandlung vornimmt. Da zum Zeitpunkt der Ausfuhr aber noch keine Entscheidung der Behörde darüber vorlag, ob eine Genehmigung überhaupt erforderlich ist, kann der Ausführer im Grunde kein Genehmigungserfordernis verletzen. Teleologisch könnte § 5c Abs. 2 Satz 2 AWV jedoch so interpretiert werden, dass die Ausfuhr der Güter als genehmi-

---

560 Siehe nur *Bieneck*, wistra 2008, 211, mit ausführlichen Nachweisen; Erbs/Kohlhaas-*Diemer*, A 217a Außenwirtschaftsverordnung, § 5c Rn. 1.

561 Vgl. *Bieneck*, wistra 2008, 212.

562 Siehe hierzu a.a.O., 211 f.

gungsbedürftig gilt, bis das BAFA die Ausfuhr genehmigt oder entschieden hat, dass es einer Genehmigung nicht bedarf.[563]

3. Anknüpfungspunkt: „für eine militärische Endverwendung bestimmt"

§ 5c Abs. 1 Satz 2 AWV normiert, worauf sich die Kenntnis des Ausführers beziehen muss. Als militärische Endverwendung gilt demnach der Einbau in Güter der Ausfuhrliste (Nr. 1), die Verwendung von Herstellungs-, Test- oder Analyseausrüstung sowie Bestandteilen hierfür für die Entwicklung, die Herstellung oder die Wartung von Gütern der Ausfuhrliste (Nr. 2) sowie die Verwendung von unfertigen Erzeugnissen in einer Anlage für die Herstellung von Gütern der Ausfuhrliste (Nr. 3).

Auffällig ist hier vor allem die Regelung der Nr. 2, die besagt, dass auch das Verwenden von Test- und Analyseausrüstung *für* die Entwicklung (etc.) von Gütern der Ausfuhrliste als militärische Verwendung anzusehen ist. Damit wird also insbesondere auch Analyseausrüstung erfasst, wenn der Ausführer Kenntnis davon hat, dass der Abnehmer diese Analyseausrüstung für die Entwicklung von gelisteten Gütern verwenden will. Geht der Ausführer aber davon aus, dass der Abnehmer die Analyseausrüstung für zivile Zwecke verwenden will, so benötigt er demnach keine Genehmigung.

4. Gefährdungseignungsvorsatz

Jedoch reicht das subjektive Wissen des Ausführers allein selbst in der Catch-all-Klausel nicht aus, um die Strafbarkeit im Rahmen des § 34 Abs. 2 AWG auszulösen. Vielmehr muss die vorsätzlich begangene und ungenehmigte[564] Tathandlung gemäß § 34 Abs. 2 AWG geeignet sein, die äußere Sicherheit der Bundesrepublik Deutschland oder das friedliche Zusammenleben der Völker zu gefährden oder die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich zu gefährden. Auch hierauf muss sich also der Tätervorsatz beziehen. Der Täter muss deshalb hinsichtlich dieser *Eignung zur Gefährdung* einen Vorsatz haben. Typischerweise wird dieser in Form von dolus eventualis oder dolus directus 2. Grades vorliegen.

§ 34 Abs. 2 AWG ist damit ein abstrakt-konkretes Gefährdungsdelikt: Die beschriebene Handlung ist stets abstrakt gefährlich, jedoch ist erforderlich, dass der

---

[563] Nach *Bieneck* sind das Nichtbeachten einer Genehmigungspflicht und das „Nichtherbeiführen der Genehmigungspflicht" äquivalent. Dem kann jedoch nicht gefolgt werden, da von Anfang an keine „Pflicht zum Herbeiführen der Genehmigungspflicht" besteht, wohl aber eine Pflicht zur Beachtung einer Genehmigungspflicht. Die Unterrichtungspflicht ist auch offensichtlich kein Äquivalent zu einem „Nichtherbeiführen der Genehmigungspflicht", da das BAFA im Anschluss an die Unterrichtung ergebnisoffen das Bestehen einer Genehmigungspflicht prüft.

[564] Dazu sogleich D.

Tatrichter feststellt, dass die konkrete Handlung im Einzelfall generell geeignet ist, die genannten Schutzgüter zu gefährden.[565] Dabei muss innerhalb eines überschaubaren Zeitraums mit überwiegender Wahrscheinlichkeit die Rechtsgutsbeeinträchtigung drohen, und es ist irrelevant, ob tatsächlich bereits Reaktionen außenpolitischer oder sicherheitspolitischer Relevanz eingetreten sind.[566] Zur Beurteilung einer Eignung zur erheblichen Gefährdung der auswärtigen Beziehungen der Bundesrepublik Deutschland können Sachverständigengutachten des Auswärtigen Amts für die wertende Gesamtschau herangezogen werden.[567]

Kritisiert wird an dieser Lösung, dass im Vergleich zur früheren Rechtslage, in der die Norm als Erfolgsdelikt ausgestaltet war, die Strafbarkeit weit vorverlagert worden ist.[568] Im Vergleich zu den Straftatbeständen des Software-Strafrechts jedoch,[569] insbesondere den Anschließungsdelikten, in denen regelmäßig nicht einmal eine Gefährdungseignung mitnormiert worden ist, stellt dieses Merkmal noch eine deutliche Strafbarkeitsbegrenzung dar. In Anbetracht des im Übrigen konturlosen objektiven Tatbestands (alle Güter sind grundsätzlich erfassbar) trüge andernfalls fast ausschließlich das subjektive Täterwissen die Strafbarkeit.

5. Zusammenfassung der Catch-all-Klauseln

Zwei wesentliche Merkmale prägen die hier erörterten Catch-all-Klauseln: Zunächst ist das *Wissen* des Vorfeldtäters um die deliktischen Pläne des Zieltäters erforderlich. Sodann braucht es den *Vorsatz* des Vorfeldtäters, dass seine Vorfeldhandlung grundsätzlich die geschützten Rechtsgüter gefährden kann. Freilich ist dieser Gefährdungseignungsvorsatz weniger als ein Gefährdungsvorsatz, bei dem der Vorfeldtäter mit seiner Handlung den Vorsatz verknüpfen würde, die geschützten Rechtsgüter tatsächlich zu gefährden. Auf die Eigenheiten des Tatgegenstands kommt es in Catch-all-Klauseln nicht an. Jeder Gegenstand ist taugliches Tatobjekt.

In dieser Konturlosigkeit des objektiven Tatbestands haben die Catch-all-Klauseln wesentliche Gemeinsamkeiten mit der Auslegung des „Zweckmodells“ im Rahmenbeschluss 2001/413/JI durch die EU-Kommission:[570] Auch dort legte die Kommission den „Zweck des Computerprogramms“ als Zweck des Vorfeld-

---

565 Siehe BGH NJW 1999, 2129 mit Verweis auf BGH NJW 1994, 672; Erbs/Kohlhaas-*Diemer*, A 217 Außenwirtschaftsgesetz, § 34 Rn. 14; siehe im Ergebnis auch MüKo-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 86, der aber die „Eignung zur Gefährdung der Rechtsgüter“ mit einer „Beeinträchtigung der Rechtsgüter“ gleichsetzt.

566 MüKo-*Wagner*, Außenwirtschaftsgesetz, § 34 Rn. 86.

567 So geschehen etwa im Fall BGH NJW 2009, 1684.

568 Erbs/Kohlhaas-*Diemer*, A 217 Außenwirtschaftsgesetz. § 34 Rn. 14.

569 Dazu unten Teil 4.

570 Siehe oben II.B.2.b).

täters aus, sodass das Tatobjekt keine Beschränkung mehr hatte und letztlich jedes Computerprogramm zum tauglichen Tatobjekt wurde.

Diese Besonderheit muss in Teil 4 der Arbeit beim Vergleich der Regelungstechniken für Software-Delikte erwogen und bewertet werden. Im Rüstungskontrollrecht knüpft hieran noch keine Strafbarkeit, sondern zunächst wird ein verwaltungsrechtlicher Genehmigungsvorbehalt ausgelöst.

D. Zwischenstufe: Genehmigungsvorbehalt

Sowohl im objektiven Regelungsmodell der § 22a KWKG und § 34 Abs. 1 Satz 1 AWG als auch im subjektiven Regelungsmodell des § 34 Abs. 2 AWG ist das *Fehlen einer Genehmigung* tatbestandlich mitnormiert. Im objektiven Regelungsmodell muss der Täter bei Vorliegen eines tauglichen Tatobjekts die Tathandlung ohne Genehmigung vornehmen. Im subjektiven Regelungsmodell muss der Täter bei entsprechendem Täterwissen die Tathandlung ohne Genehmigung vornehmen. Die fehlende Genehmigung ist damit in beiden Regelungsmodellen Tatbestandsmerkmal.[571]

Da die Genehmigung nach dem Verwaltungsrecht erteilt wird, schützt die Strafnorm hier nicht nur das eigentliche Rechtsgut, sondern auch den staatlichen Genehmigungsvorbehalt und man spricht entsprechend von verwaltungsakzessorischem Strafrecht[572] oder genauer: verwaltungs*akt*akzessorischem Strafrecht.[573]

Die Legitimität verwaltungs*akt*akzessorischen Strafrechts wird mitunter wegen des behördlichen Einflusses auf das Strafrecht per se bestritten.[574] In den vorliegenden Fällen erlaubt sie aber vor allem eine Vorab-Feinjustierung der Strafbarkeit in jedem Einzelfall, indem die zuständige Behörde durch ihre außenpolitischen Erwägungen die Möglichkeit und den Grad einer Gefährdung der Schutzgüter beurteilt. Insbesondere gibt die Verwaltungs*akt*akzessorietät hier den Adressaten der Strafnormen die Möglichkeit, durch einen Antrag auf Genehmigung beim zuständigen Bundesamt für Wirtschaft und Ausfuhrkontrolle und wahlweise die Eröffnung des Verwaltungsrechtswegs im Voraus klären zu lassen, ob ein geplantes Verhalten straflos ist. So konnte etwa in dem oben beschriebenen Verfahren vor dem VG Frankfurt a.M.[575] der Streit über das Vorliegen des Tatbestandsmerkmals

---

571 Erbs/Kohlhaas-*Diemer*, A 217 Außenwirtschaftsgesetz, § 34 Rn. 11; MüKo-*Wagner*, Außenwirtschaftsgesetz § 34 Rn. 7.

572 Vgl. *Bieneck*, wistra 2011, 90.

573 MüKo-*Schmitz*, Vor §§ 324 ff., Rn. 37 ff.

574 Vgl. *Schall*, NJW 1990, 1266 ff.; differenzierend *Fischer*, StGB, Vor § 324 Rn. 6; MüKo-*Schmitz*, Vor §§ 324 ff. Rn. 38 ff.; *Rudolphi*, NStZ 1984, 249 ff.

575 VG Frankfurt a.M. Urteil vom 17.2.2005, 1 E 7512/03, online abrufbar unter http://www.lareda.hessenrecht.hessen.de/jportal/portal/t/s15/page/bslaredaprod.psml?&doc.id=M

„besonders konstruiert oder geändert für militärische Zwecke“ vor dem Verwaltungsgericht beigelegt statt vor Strafgerichten ausgetragen werden. Dadurch wird also das Strafbarkeitsrisiko für Exporteure minimiert. Freilich werden im Gegenzug Entscheidungslast und Entscheidungsverantwortung zu großen Teilen auf die Exekutive abgewälzt.[576]

E. Freistellungs- und Bagatellklauseln

Weiterhin wird der Bereich strafbaren Handelns durch einige Freistellungs- und Bagatellklauseln eingegrenzt und präzisiert. Diese Klauseln sind unterschiedlich konstruiert. Teilweise heben sie die Genehmigungspflicht auf und hebeln somit auch den jeweiligen Straftatbestand aus. Teilweise normieren sie, dass die Verbotsnorm für bestimmte Fälle nicht gilt, folglich läuft auch die Strafnorm leer, soweit sie auf die Verbotsnorm bezugnimmt.

Eine solche Klausel findet sich etwa in § 22 KWKG, der normiert, dass die §§ 18, 20 und 21 KWKG nicht gelten für *dienstliche Handlungen* bestimmter Mitglieder der NATO-Kräfte. § 18 KWKG stellt eine Verbotsnorm dar, § 20 KWKG ist die dazugehörige Strafnorm und § 21 KWKG regelt den universellen Geltungsbereich des § 20 KWKG für Handlungen Deutscher. Da § 20 KWKG nicht auf § 18 KWKG verweist, ist seine gesonderte Aufzählung in § 22 KWKG erforderlich. Wäre in § 20 KWKG die häufig anzutreffende Verweisungstechnik angewandt worden („wer entgegen § 18 …“), so hätte es in § 22 KWKG der gesonderten Nennung der §§ 20 und 21 KWKG nicht bedurft.

Zwei weitere Ausschlussklauseln finden sich in § 19 Abs. 6 Nr. 1 und 2 KWKG. Diese wenden sich gegen die Absätze 1–5 und damit gegen einzelne Strafnormen. Nr. 1 normiert zunächst, dass die Strafnormen nicht für Handlungen gelten, die *zur Vernichtung von Tatgegenständen* (hier: Atomwaffen) *durch die dafür zuständigen Stellen* vorgenommen werden. Nr. 2 besagt, dass die Strafnormen nicht für solche Handlungen gelten, die *zum Schutz* gegen Wirkungen von Atomwaffen oder zur Abwehr dieser Wirkungen geeignet und bestimmt sind. Während also bei der Vernichtung von Tatgegenständen nur die zuständigen Stellen in den Genuss der Straffreiheit kommen, gilt die zweite Ausschlussklausel personell uneingeschränkt. Mit anderen Worten darf sich jedermann tatbestandsmäßig verhalten, wenn er beabsichtigt damit die Wirkungen von Atomwaffen abzuwehren oder davor zu schützen und wenn seine Handlung zu Schutz oder Abwehr auch geeignet ist. Eine Ausschlussklausel gleicher Art ist auch in § 20 Abs. 4 KWKG enthalten, dort für chemische Waffen.

WRE060001872%3Ajuris-r01&showdoccase=1&doc.part=L [zuletzt abgerufen am 16.11. 2014], siehe auch oben B.2.b).

[576] Vgl. hierzu *Jaeckel*, JZ 2011, 121.

Eine dritte Art von Ausschlussklauseln findet sich in der Ausfuhrliste (Anlage AL zur Außenwirtschaftsverordnung) als Zusatz zu einigen Listeneinträgen. Demnach sollen Gegenstände ausgenommen sein, die für bestimmte, als legitim erachtete Zwecke, besonders konstruiert (worden) sind. Beispielsweise normiert Position 0003a in Teil I A der Ausfuhrliste, dass Munition für die Waffen der Positionen 0001, 0002 und 0012 erfasst ist. Anmerkung 3 zu dieser Position legt jedoch fest, dass Patronen dann nicht erfasst sind, wenn sie besonders konstruiert sind „für einen der folgenden Zwecke: […] b) Vogelschreck-Munition (bird scaring)".

Anders als die voranstehend genannten ist diese Klausel nicht personen- oder handlungsbezogen, sondern gegenstandsbezogen. Die Auslegung des „Zwecks" bereitet bei einer Ausschlussklausel grundsätzlich dieselben Schwierigkeiten wie bei einem Tatbestandsmerkmal der normativen Listeneinträge. Allerdings lassen sich Ausschlussklauseln gestützt auf Art. 103 Abs. 2 GG im Zweifel immer weit auslegen, sodass die Auslegungsschwierigkeiten hier weniger dramatisch sind.

Da die Klausel gegenstandsbezogen ist und in der Ausfuhrliste selbst normiert wird, schließt sie sowohl in der Verbotsnorm als auch in der Strafnorm ein taugliches Tatobjekt aus. Eine solche Ausschlussklausel ist freilich vornehmlich bei den deskriptiven Listeneinträgen sinnvoll. Bei den normativen konstruktionsbezogenen Listeneinträgen wäre sie regelmäßig gegenstandslos, da kaum vorstellbar ist, dass ein Gegenstand besonders für militärische und zugleich besonders für einen nichtmilitärischen Zweck konstruiert ist.

Eine letzte – ebenfalls gegenstandsbezogene – Ausschlussklausel findet sich beispielsweise in § 5 Abs. 3 Satz 1 AWV. Dieser besagt, dass das Genehmigungserfordernis nach Abs. 2 nicht gilt, wenn nach dem der Ausfuhr zugrunde liegenden Vertrag derartige Güter im Werte von nicht mehr als 2500 € geliefert werden sollen. Allerdings ist in Satz 3 festgelegt, dass diese preismäßige Beschränkung nicht für Datenverarbeitungsprogramme gilt.

Teil 4

Optimierung der Straftatbestände

Ziel dieser Arbeit ist es, eine Regelungstechnik für Vorfelddelikte des Computerstrafrechts zu finden, die angesichts der Dual-Use-Problematik zu einer angemessenen Kriminalisierung führt. Die Regelungstechnik soll also gemäß den gesetzgeberischen Zielen gefährliches Vorfeldverhalten so weit wie möglich unter Strafe stellen, ohne dabei das Handeln von IT-Sicherheitsbeauftragten und andere sozialnützliche Verhaltensweisen zu erfassen. Insbesondere sollen Grauzonen und Unklarheiten vermieden werden, damit keine Rechtsunsicherheit und damit *Chilling Effects* aufkommen.

Zu diesem Zweck werden im folgenden Kapitel alle Regelungstechniken des vorstehenden Teils 3 hinsichtlich ihrer Rechtsklarheit und Legitimität verglichen (I.). Anschließend sollen weiterführende Fragen angesprochen werden (II.). Schließlich wird hierauf aufbauend ein Modellstraftatbestand für ein optimiertes Software-Delikt vorgeschlagen (III.).

I. Wertender Vergleich der angewandten Regelungstechniken

In diesem Kapitel werden die Regelungstechniken wertend verglichen. Hierzu wird zunächst ein Wertmaßstab für den Vergleich der Regelungstechniken entwickelt (A.). Sodann wird das gesamte Arsenal der Regelungstechniken aus Teil 3 systematisch dargestellt (B.). Hieran schließt der Vergleich dieser Regelungstechniken anhand des entwickelten Wertmaßstabs (C.) an.

A. Bewertungsmaßstab für den Rechtsvergleich

In dieser Arbeit werden Rechtsklarheit (I.) und Legitimität (II.) als Maßstab für den wertenden Rechtsvergleich zugrunde gelegt.

1. Rechtsklarheit

Rechtsklarheit wird hier festgelegt als Effektivität, Effizienz und Verständlichkeit der Norm. Es wird also analysiert, ob die konkrete Regelungstechnik im Ver-

gleich zu den alternativen Regelungstechniken zu einer effektiveren, effizienteren und verständlicheren Norm führt.

Als *effektiv* wird dabei eine Norm angesehen, wenn sie überhaupt einen Anwendungsbereich hat. Die Norm soll also kein leerlaufendes Symbolgesetz sein, sondern materiell ein Verhalten umschreiben, welches stimmig und lebensnah ist und sich prozessual nachweisen lässt. Zur Effektivität gehört auch, dass der Wortlaut der Norm nicht *enger* ist, als der vom Gesetzgeber (historisch-teleologisch) anvisierte Sachverhalt. Denn ein zu enger Wortlaut eröffnet den Rechtsunterworfenen Umgehungsstrategien, die dazu führen können, dass eine Bestrafung aus dieser Norm mit wenig Aufwand vermieden werden kann, sodass der *Effekt* der Norm insgesamt anzuzweifeln wäre.

Als *effizient* soll eine Regelungstechnik erachtet werden, wenn ihr Effekt unter geringem Aufwand erzielt werden kann. Dies ist der Fall, wenn der Anwendungsbereich der Norm möglichst präzise beschrieben ist und die Grenzen der Strafbarkeit möglichst unmittelbar ersichtlich sind. Ineffizient wären demnach unpräzise, missverständliche oder irreführende Ausdrücke im Wortlaut der Norm. Solche Ausdrücke müsste der Rechtsanwender nämlich erst im Wege der Auslegung zurechtstutzen, also teleologisch reduzieren, um das präzise Ausmaß der Kriminalisierung zu erfassen. Dies gilt insbesondere auch im Falle umgangssprachlicher Ausdrücke im Tatbestand. Zur Effizienz gehört insbesondere, dass der Wortlaut der Norm nicht *weiter* ist, als der vom Gesetzgeber anvisierte Sachverhalt. Ein zu weiter Wortlaut müsste teleologisch reduziert werden, was für die Rechtsunterworfenen bedeutet, dass sie einen erhöhten Aufwand betreiben müssen, um zu einem klaren Verständnis der Norm zu kommen.

Verständlich soll eine Regelungstechnik sein, wenn ihre Bedeutung und ihr Inhalt auch dem juristisch gebildeten Laien zugänglich sind. Schwerer verständlich ist demnach eine Norm, die nicht alle Tatbestandsmerkmale selbst beschreibt, sondern im Einzelnen auf andere Normen verweist, welche wiederum auf andere Normen in anderen Gesetzen verweisen.[1] Ebenso ist eine Norm schwerer verständlich, die *zum Teil* selbst erklärt, in welchen Bereichen sie anwendbar ist, *zum Teil* aber auch in wiederum anderen Normen für entsprechend anwendbar erklärt wird.[2] Verständlich ist dagegen eine Norm, die von sich aus auf alle Fälle verweist, in denen sie anwendbar ist.

---

[1] So etwa die Konzeption in §§ 34 Abs. 2, 33 Abs. 1, 2 Abs. 1 i.V.m. § 7 Abs. 1 AWG wiederum in Verbindung mit §§ 5c Abs. 1 und 2, 70 Abs. 1 Nr. 2 AWV.

[2] So etwa § 202c Abs. 1 Nr. 2 StGB, der selbst nur erklärt, für Vorfeldtaten zu §§ 202a und 202b StGB zu gelten, andernorts aber wiederum für „entsprechend anwendbar“ erklärt wird: § 303a Abs. 3 und § 303b Abs. 5 StGB.

2. Legitimität

Legitim ist eine Regelungstechnik nach den im 2. Teil der Arbeit entwickelten Indikatoren. Optimal ist also die Regelungstechnik, die im Vergleich zu den anderen Regelungstechniken die stärkste Risikoerhöhung und den stärksten „deliktischen Sinnbezug" impliziert.

Risikoerhöhung soll dabei bedeuten, dass die Regelungstechnik ein Geschehen beschreibt, bei dem ein Risiko für das geschützte Rechtsgut eintritt oder erhöht wird. Ein „deliktischer Sinnbezug" ergibt sich, wenn das tatbestandsmäßige Geschehen bei objektiver Betrachtung nur den Schluss zulässt, dass der Handelnde sich als Vorfeldtäter begreift und in einen deliktischen Vorgang integrieren will.[3]

B. Modelle gesetzgeberischer Regelungstechniken

Zunächst werden die gesetzgeberischen Regelungstechniken aus allen hier analysierten Delikten zusammengefasst und systematisiert. Auf die Techniken zur Regelung der objektiven Tatseite (1.) folgen die Techniken zur Regelung der subjektiven Tatseite (2.). Schließlich werden der Genehmigungsvorbehalt (3.) und die Freistellungs- und Ausschlussklauseln (4.) aufgeführt.

1. Die objektive Tatseite

Auf der objektiven Tatseite stehen zunächst materielle Gesetzestechniken, welche also *der Materie nach* festlegen, welche Verhaltensweisen erfasst werden. Sie werden sogleich unter a) konkret benannt. Sodann finden sich auch formelle Regelungstechniken, die das tatbestandliche Verhalten also *der Form nach* beschreiben. Sie werden sogleich unter b) konkret benannt.

Die Regelungstechniken lassen sich außerdem gruppieren in abstrakte und konkrete, normative und deskriptive Techniken. Soweit nachfolgend solche – stets strittigen – Schematisierungen vorgenommen werden, dient dies lediglich der Übersicht und Ordnung und soll noch nicht der Bewertung vorgreifen.

a) Materielle Regelungstechniken

Unter den materiellen Regelungstechniken werden hier zunächst die positiven Techniken verstanden, die festlegen, welche *Eigenschaften* das Tatobjekt, also hier das Computerprogramm, aufweisen muss, damit es eingeschlossen ist.[4]

---

[3] Siehe hierzu oben Teil 2, IV.B.2.

[4] Auch die Tat*handlungen* stellen materielle Regelungen auf der objektiven Tatseite dar, werden aber in dieser Arbeit mit Blick auf die Dual-Use-Problematik nicht als maßgeblich angesehen.

Die Beschreibung der Eigenschaften eines als Tatobjekt tauglichen Computerprogramms macht das Kernstück vieler Tatbestände des Teils 3 dieser Arbeit aus. Hier finden sich zunächst Regelungstechniken von eher deskriptiver Art, die darauf abstellen, ob ein Computerprogramm *für eine deliktische Verwendung geeignet* ist („Eignungsmodell"). Ebenso ist es eine empirisch feststellbare Eigenschaft eines Computerprogramms, ob es *als Deliktswerkzeug beworben* oder *vermarktet* wird („Marketingmodell"). Auch der *wirtschaftliche Nutzen* eines Computerprogramms bei deliktischer Verwendung ist ein eher deskriptives Merkmal. Sofern man danach fragt, ob der wirtschaftliche Nutzen bei legalem Einsatz im Vergleich zum entsprechenden Nutzen bei illegalem Einsatz *signifikant* ist („ökonomisches Modell"), bewegt man sich in Richtung normativer Merkmale, und die Diskussion ist eröffnet, welche Aspekte hier in die Signifikanzberechnung einzubeziehen sind. Ebenso stehen die Merkmale im deskriptiv-normativen Grenzbereich, die darauf abstellen, ob das Computerprogramm *für eine deliktische Verwendung angepasst* worden ist. Ob es angepasst worden ist, lässt sich (deskriptiv) aus der Versionsgeschichte ablesen, die Zielsetzung des Anpassers (normativ) jedoch nicht.

Normative Eigenschaften eines Computerprogramms sind dann die Merkmale *für eine deliktische Verwendung designed/entworfen* oder *hergestellt* (jeweils in Software-Delikten), *hierfür bestimmt* (Software-Delikte und Exportkontrollstrafrecht) sowie *hierfür konstruiert* (Exportkontrollstrafrecht). Normativ sind diese „Entstehungsmodelle", weil die Feststellung dieser Merkmale eine Bewertung des jeweiligen Gegenstandes – zumeist aus Sicht des Verkehrs oder eines verständigen Durchschnittsnutzers – zwingend voraussetzt: Es lässt sich nicht ablesen oder nachmessen, welche Ziele die historischen Hersteller in der Entstehungsphase des Tatgegenstands verfolgt hatten. Dies trifft auch für die Merkmale des *deliktischen Zwecks* („Zweckmodell") und des *wirtschaftlichen Zwecks bei krimineller Verwendung* eines Computerprogramms zu.

Weitere normative Einfallstore sind in den Merkmalen *hauptsächlich*, *besonders* und *in erster Linie* zu sehen, die sowohl im deutschen als auch im internationalen Software-Strafrecht sowie im Exportkontrollrecht mit anderen normativen Merkmalen kombiniert werden. Mitunter wird auch der Anknüpfungspunkt nochmals vorverlagert, indem das jeweilige Computerprogramm nicht für eine *deliktische Verwendung* entworfen/hergestellt/angepasst/etc. worden sein muss, sondern für deren *Ermöglichung* oder gar deren *Erleichterung*.

b) Formelle Regelungstechniken

Formelle Regelungstechniken machen den Verstoß gegen eine bestimmte äußere Form oder ein Verfahren zum tatbestandlich erfassten Verhalten. Im Software-Strafrecht werden solche Techniken bislang nicht verwandt. Im Exportkontrollstrafrecht finden sich aber listenbasierte Blankettgesetze, nach denen der Umgang mit einem *aufgelisteten Gegenstand* strafbar ist („Listenmodell"). Maßgeblich ist

also allein das formelle Merkmal, dass der Gegenstand auf einer bestimmten Liste geführt wird.

Freilich ist die Einordnung als formelle Regelungstechnik nur insoweit zutreffend, als auf der Liste bestimmte Gegenstände schlicht benannt werden. Sofern auf der Liste selbst abstrakte Umschreibungen der Gegenstände eingesetzt werden, handelt es sich um materielle Regelungstechniken, bei denen eine Vielzahl materieller Tatobjekt-Umschreibungen in Listen zusammengefasst wird. Es zeigt sich also, dass formelle und materielle Regelungstechniken gemischt werden können und die Übergänge fließend sind.

2. Die subjektive Tatseite

Auf der subjektiven Tatseite haben die Gesetzgeber grob unterschieden zwischen Vorfelddelikten ohne subjektiven Bezug des Täters zur Zieltat (sogleich a)) und Vorfelddelikten mit einem solchen Bezug (sogleich b)). Unter diesen Letzten bestehen Unterschiede nach Art des subjektiven Bezugs.

a) Verzicht auf einen subjektiven Bezug zum Zieldelikt

Namentlich im Exportkontrollstrafrecht sowie in den Software-Delikten zum Schutze des Urheberrechts und verwandter Schutzrechte haben die Gesetzgeber auf die Normierung intentionaler Bezüge zu Zieldelikten verzichtet. Die entsprechenden Delikte stellen damit ein unschädliches, aber möglicherweise später gefährliches Verhalten unter Strafe – unabhängig von den Zielen und Interessen des Handelnden. Dogmatisch betrachtet haben die Gesetzgeber hier eine strafbare vollendete *nicht-akzessorische* Beihilfe konstruiert, da hier die Förderung eines Zieldeliktes unter Strafe gestellt wird, ohne dass das Zieldelikt nachgewiesen werden oder überhaupt stattgefunden haben muss und ohne dass der Vorfeldtäter diesbezüglich irgendeinen Vorsatz haben muss.[5]

b) Regelungstechniken subjektiver Bezüge zum Zieldelikt

In den deutschen Software-Delikten finden sich vielfach Vorbereitungsdelikte, deren intentionaler Bezug zur Zieltat darin besteht, dass der Vorfeldtäter hinsichtlich des Zieldelikts einen *Vorbereitungsvorsatz* hat. Dogmatisch sollen sie Fälle versuchter Beihilfe erfassen, der genaue Regelungsinhalt des Vorbereitungsvorsatzes ist jedoch unklar.[6] Art. 6 Ziff. 1 lit. a CCC sieht als subjektiven Bezug des Vorfeldtäters zur Zieltat vor, dass er mit *Verwendungsabsicht* handelt, wobei sich die Absicht lediglich darauf beziehen muss, dass irgendjemand das Computer-

---

[5] Siehe oben Teil 3, I.C.2.a)bb).

[6] Siehe oben Teil 3, I.C.1.a).

programm zu einem kriminellen Zweck benutzt. Der Kommissionsvorschlag KOM(2010) 517 *endgültig* sieht dagegen einen *Begehungsvorsatz* vor. Demnach muss der Vorfeldtäter selbst zum Zweck der späteren Zieltatbegehung handeln. In den sogenannten Catch-all-Klauseln des Exportkontrollstrafrechts wird als subjektiver Bezug des Vorfeldtäters schließlich der Umgang mit bestimmten Gegenständen im *Wissen um eine spätere kriminelle Verwendung* normiert.

3. Der Genehmigungsvorbehalt

Im Kriegswaffen- und Exportkontrollstrafrecht findet sich eine Art zwischengeschaltetes Prüfverfahren. Dort besteht eine verwaltungsrechtliche Pflicht, ein geplantes tatbestandsmäßiges Verhalten genehmigen zu lassen. Erst der Verstoß gegen diese Genehmigungspflicht ist strafbewehrt. Systematisch könnte man diese Regelungstechnik auch als objektive formelle Regelungstechnik betrachten. Allerdings setzt der Genehmigungsvorbehalt das Vorliegen der objektiven und subjektiven Tatseite voraus, sodass es konsequenter erscheint, ihn als selbstständige, zwischen- oder nachgeschaltete Regelungstechnik einzuordnen.

4. Freistellungs- und Ausschlussklauseln

Freistellungs- und Ausschlussklauseln können sowohl objektiv als auch subjektiv ausgestaltet sein, zudem können sie objektiv materielle wie formelle Aussagen zu Inhalt und Grenzen des strafbaren Verhaltens treffen. Die bislang eingesetzten Klauseln knüpfen an die handelnde Person, den Tatgegenstand, die Tathandlung oder die subjektiven Ziele der handelnden Person an.

§ 95a Abs. 4 UrhG statuiert, dass die Aufgaben und Befugnisse *öffentlicher Stellen* (personenbezogen) zum Zwecke des *Schutzes der öffentlichen Sicherheit oder der Strafrechtspflege* (subjektive Ziele) unberührt bleiben.[7] Derselben Struktur folgen § 19 Abs. 6 Nr. 1 und § 20 Abs. 4 Nr. 1 KWKG mit dem Ausschluss von Handlungen *zuständiger Stellen* (personenbezogen), die zur *Vernichtung tatbestandsmäßiger Gegenstände* vorgenommen werden (subjektive Ziele). Losgelöst von bestimmten Personen besagen § 19 Abs. 6 Nr. 2 und § 20 Abs. 4 Nr. 2 KWKG, dass die Strafnormen nicht für solche Handlungen gelten, die zum Schutz vor oder zur Abwehr von Wirkungen der Tatgegenstände *geeignet* (handlungsbezogen) und *bestimmt* (subjektive Ziele) sind. § 22 KWKG löst sich dagegen von den subjektiven Zielen und schließt *dienstliche Handlungen* (handlungsbezogen) bestimmter *NATO-Kräfte* (personenbezogen) von der Strafbarkeit aus.

Auch die Ausfuhrliste (Anlage AL zur AWV) enthält Ausschlussklauseln für Gegenstände, deren *Konstrukteur* (personenbezogen) besondere *nichtmilitärische*

---

[7] Dieser Ausschlusstatbestand findet allerdings im Rahmen des § 108b Abs. 2 UrhG keine Anwendung, da dieser nur auf § 95a Abs. 3 UrhG verweist.

Zwecke verfolgt hat (subjektive Ziele). Allerdings werden diese vom Konstrukteur verfolgten Zwecke objektiviert als Eigenschaften des Tatobjekts angesehen, sodass es sich bei der Klausel genaugenommen um eine gegenstandsbezogene Ausschlussklausel handelt. Ebenso gegenstandsbezogen ist die Bagatellklausel des § 5 Abs. 3 Satz 1 AWV, die das für die Strafnorm konstitutive Genehmigungserfordernis ausschließt, wenn der Wert des Tatgegenstands 2500 € nicht übersteigt.[8]

Eine Tatbestandsausschlussklausel kann man zudem in Art. 6 Abs. 2 CCC sehen. Dieser stellt klar, dass Abs. 1 nicht so ausgelegt werden dürfe, dass er eine strafrechtliche Haftung in den Fällen begründet, in denen die Tathandlungen „nicht zum Zweck der Begehung" einer Zieltat vorgenommen werden, sondern beispielsweise zum „genehmigten Testen oder zum Schutz eines Computersystems". Rechtsnatur und Regelungsgehalt dieser Klausel sind jedoch ungewiss.[9]

C. Vergleich der Regelungsmodelle

Im Folgenden werden alle gesetzgeberischen Regelungsmodelle einem wertenden Vergleich unterzogen. Die hieraus gewonnenen Erkenntnisse sind Grundlage des zu entwerfenden Modellstraftatbestandes.

Eine solche vergleichende Bewertung ist keine politische Würdigung. Zur Diskussion steht hier nicht die politische Motivation des Gesetzgebers, überhaupt Vorfelddelikte im IT-Strafrecht zu erlassen. Denn mit einer solchen politischen Diskussion wäre die Rechtswissenschaft überfordert. Hier wird die politische Motivation des Gesetzgebers vorausgesetzt. Untersucht werden soll allein, mit welchen Mitteln er seine Ziele umsetzt.

1. Die Gestaltung des Tatobjekts

Zur Regelung des Tatobjekts stehen das „Eignungsmodell", das „Zweckmodell", das „Entstehungsmodell", das „ökonomische Modell", das „Marketingmodell" und das „Listenmodell" zur Verfügung. Vergleicht man die Regelungstechniken, mit denen das Tatobjekt in den analysierten Straftatbeständen bestimmt wurde, so erscheint das „Eignungsmodell" mit Blick auf Rechtsklarheit und Legitimität optimal (sogleich a)). Dies liegt zu einem beträchtlichen Teil an den erheblichen Defiziten, die die anderen Regelungstechniken bezüglich Rechtsklarheit und Legitimität im Vergleich aufweisen (sodann im Einzelnen b)–e)).

---

[8] Eine Rückausnahme von dieser Klausel gilt freilich für Datenverarbeitungsprogramme, siehe oben Teil 3, III.E.

[9] Siehe unten C.4.b).

a) Vorzugswürdiges Tatobjektsmodell: das „Eignungsmodell“

Nach den Maßstäben der Rechtsklarheit und Legitimität erscheint es vorzugswürdig, in einem Software-Delikt den Umgang mit solchen Computerprogrammen unter Strafe zu stellen, die unmittelbar zur Begehung von Zieltaten verwendet werden können. In den bisherigen Software-Delikten wird dies im „Eignungsmodell“ ausgedrückt, etwa wenn es im Wortlaut des Vorfelddelikts heißt, das Computerprogramm müsse *seiner Art nach zur Begehung der Zieltat geeignet sein*.[10]

aa) Bewertung am Maßstab der Rechtsklarheit

Diese Regelungstechnik führt zu einer vergleichsweise hohen Rechtsklarheit. Sie ist auch und besonders mit Blick auf die Dual-Use-Problematik effektiv, effizient und verständlich.

Zunächst ist diese Regelungstechnik *effektiver* als diejenigen, die mehr als die bloße Eignung des Computerprogramms erfordern (insbesondere das „Zweckmodell“). Das „Eignungsmodell“ beinhaltet keine Einschränkungen und hat damit einen weiteren Anwendungsbereich. Damit wird verhindert, dass Kriminelle etwaige Einschränkungen im objektiven Tatbestand böswillig ausnutzen, indem sie kriminelle Handlungen mit deliktsgeeigneten, aber objektiv tatbestandslosen Computerprogrammen vornehmen. Mit dieser Möglichkeit bestünde die Gefahr, dass das Vorfelddelikt insgesamt umgangen würde und damit zum nicht anwendbaren, ineffektiven Symbolgesetz verkäme. Dies ist hier nicht der Fall.

Freilich erkennt diese Rechtstechnik an, dass der Multifunktionsaspekt der Dual-Use-Problematik[11] nicht im objektiven Tatbestand zu lösen ist. Für den kriminellen Einsatz eines Computerprogramms ist allein entscheidend, *dass* es sich hierzu eignet. In welchem Gewicht die deliktische Funktion zu anderen Funktionen steht, spielt weder für den Vorfeldtäter noch für den Zieltäter eine Rolle. Auch die befürchteten Schwarzmärkte würden weiter existieren, wenn deliktsgeeignete Computerprogramme allein dadurch tatbestandslos würden, dass sie überwiegend rechtmäßige Funktionen aufweisen. Sie bleiben deliktsgeeignet und damit für Vorfeld- und Zieltäter interessant. Der Mehrzweckaspekt der Dual-Use-Problematik ist ohnehin nicht im objektiven Tatbestand zu lösen, da dieser ja besagt, dass auch das schädlichste und gefährlichste Computerprogramm zu Test-, Analyse- und

---

[10] Das „Eignungsmodell“ wird in § 149 Abs. 1 Nr. 1 StGB eingesetzt, also im Vorfeld der Fälschung von Geld (§ 146 StGB), Wertzeichen (§ 148 StGB), Wertpapieren (§§ 151, 152 StGB), Schecks, Wechseln, Zahlungskarten ohne Garantiefunktion (alle § 152a StGB) und Zahlungskarten mit Garantiefunktion (§ 152b StGB). Es erfasst dort „Computerprogramme, die ihrer Art nach zur Begehung der Tat geeignet sind“. Siehe im Einzelnen oben Teil 3, I.B.1.

[11] Multifunktionsaspekt = ein Computerprogramm kann mehrere Funktionen haben, von denen einige zweifellos sozialnützlich sind, andere jedoch zweifellos schädlich.

Demonstrationszwecken bestimmten Personen zur Verfügung stehen muss. Auch wenn es banal erscheint: Der Mehrzweckaspekt ist zweckabhängig, also auf der subjektiven Tatseite verortet und damit auch dort zu lösen.

Unter dem Gesichtspunkt der *Effizienz* ist es nachteilig, wenn ein Tatbestand so weit ist, dass er im Wege der Auslegung teleologisch reduziert werden muss. Gegen das „Eignungsmodell" wird dieser Einwand erhoben: Zwar ergeben sich erste Einschränkungen dadurch, dass das Computerprogramm zur Verwendung *zur* Zieltatbegehung geeignet sein muss und nicht lediglich zur Verwendung *bei* der Zieltatbegehung. Dennoch lässt sich einwenden, dass dadurch Betriebssysteme wie Windows und Linux noch nicht tatbestandlich ausgeschlossen sind, und eine allein von subjektiven Kriterien abhängige Kriminalisierung dem Gesinnungsstrafrecht nahekäme.[12] Diesem Einwand ist jedoch dadurch zu begegnen, dass das Unmittelbarkeitskriterium, das im entsprechenden Tatbestand des § 149 Abs. 1 Nr. 1 StGB bereits reichsgerichtlich entwickelt worden ist, mitnormiert wird.[13]

Demnach ist ein Computerprogramm nur dann tatbestandsmäßig, wenn es sich dazu eignet, bei der *unmittelbaren* Zieltatbegehung eingesetzt zu werden. Hierunter ist sowohl die Fallgruppe zu zählen, in der ein Computerprogramm (auf Befehl des Verwenders) die Zieltat vollumfänglich verwirklicht,[14] als auch die Fallgruppe, in der ein Computerprogramm lediglich funktionale Teile *der Zieltat* unmittelbar selbst ausführt, also wenn es für die Verwirklichung des Zieltaterfolgs erforderlich ist, dass seine Funktionen und menschliche Handlungen oder auch Funktionen weiterer unmittelbar beteiligter Computerprogramme ineinandergreifen.

Nicht erfasst ist dagegen jedes unspezifische Computerprogramm wie ein Betriebssystem, das in keinem konkreten Zusammenhang zur Zieltat steht. Dieses stellt nämlich lediglich eine Arbeitsplattform zur Verfügung. Windows wäre also nur in einem Sinne „zur Begehung einer Straftat verwendbar", in dem es schlicht zu jeder anderen Computertätigkeit auch verwendbar ist. Bei funktionaler Betrachtung ist Windows nämlich nicht (unmittelbar) zur Begehung der Straftat verwendbar, sondern nur (unmittelbar) zum Betrieb des Schadprogramms und zu dessen (unmittelbarer) Steuerung. Damit ist Windows ersichtlich nur *mittelbar* zur Begehung der Straftat verwendbar.

Freilich könnte man bei Computerprogrammen argumentieren, dass die bloßen Programmbibliotheken oder komprimierten Archive eines noch nicht installierten Computerprogramms stets noch einer Umgestaltung oder Weiterverarbeitung bedürften, nämlich der Installation. Erst dann könnten sie unmittelbar zur Begehung der Zieltat verwendet werden. Eine solch technische Argumentation würde jedoch dem Sinn des Unmittelbarkeitskriteriums zuwiderlaufen, welches evident auf einer

---

[12] Vgl. *Rackow*, FS für Maiwald, S. 628.

[13] Siehe eingehend oben Teil 3, I.B.1.a)bb).

[14] Etwa bei einem *DDoS-Angriff*, der auf Befehl des Verwenders automatisiert abläuft.

funktionalen Betrachtung beruht. Eine solche funktionale Betrachtungsweise wurde im Falle des unautorisierten Empfangs von Pay-TV auch vom OLG Hamburg hinsichtlich der FTA-Receiver[15] sowie vom LG Karlsruhe hinsichtlich der dort streitgegenständlichen OPOS-Karten[16] bei der Subsumption „geeigneter Vorrichtungen" angelegt. Anknüpfungspunkt für die Beurteilung der Software muss daher ihr – gegebenenfalls gedachter – Zustand nach Installation sein. So ist zwar ein ungepatchter Receiver wie im Hamburger Verfahren kein taugliches Tatobjekt, wohl aber der Patch, der auf den Receiver aufgespielt wird. Denn das bloße Aufspielen (oder Installieren) solcher Software muss bei funktionaler Betrachtung außer Acht bleiben und kann die Unmittelbarkeit nicht unterbrechen.

Das „Eignungsmodell" ist auch vergleichsweise *verständlich*. Es wird einem Laien kaum Schwierigkeiten bereiten, zu erkennen oder zu recherchieren, ob ein Computerprogramm zur Begehung einer Straftat verwendet werden kann. Das Unmittelbarkeitskriterium mag dem Rechtsunterworfenen besondere Kenntnisse abverlangen, jedoch wird jedenfalls der juristisch informierte Laie hier vor vergleichsweise niedrige Verständnishürden gestellt. Für eine hohe Verständlichkeit des „Eignungsmodells" spricht außerdem, dass es alle prägenden Merkmale (deliktische Verwendbarkeit, Unmittelbarkeit) im Tatbestand nennt und ohne Verweise auf andere Normen oder andere Gesetze auskommt.

bb) Bewertung am Maßstab der Legitimität

Das „Eignungsmodell" erscheint zudem vergleichsweise legitim, weil das tatbestandsmäßige Computerprogramm ohne Weiteres eine Risikoerhöhung setzt. Zugleich ist ein „deliktischer Sinnbezug" der Vorfeldhandlung möglich, der allerdings maßgeblich von der Ausgestaltung der subjektiven Tatseite abhängen wird.

Zunächst impliziert das im „Eignungsmodell" normierte Tatobjekt ohne weitere Bedingungen eine erhebliche *Risikoerhöhung* für das Rechtsgut: Das Rechtsgut ist schon allein dadurch gefährdet, dass ein Computerprogramm existiert, das unmittelbar zu einer Verletzung des Rechtsguts eingesetzt werden kann. Dieses Risiko ist auch zumeist der Auslöser dafür, dass der Gesetzgeber überhaupt aktiv wird: Er will stets verhindern, dass Computerprogramme zirkulieren, die als Deliktswerkzeuge verwendbar sind, denn diese Computerprogramme versetzen bestimmte Personenkreise überhaupt erst in die Lage, konkrete Straftaten zu begehen, oder verhelfen ihnen dazu, ihre Straftaten in Maß und Intensität erheblich zu steigern. Besonders augenfällig ist dies im Bereich der Urheberrechtsdelikte. Urheberrechtlich geschützte Filme, Musikalben und Computerprogramme würden wohl kaum illegal verbreitet, wenn ihre Kopierschutzmechanismen effektiv wären. Sie sind es

---

[15] OLG Hamburg GRUR-RR 2010, 153 f.

[16] LG Karlsruhe NStZ-RR 2007, 19.

aber faktisch nicht, weil massenweise kostenlose *Cracks* im Internet zirkulieren, die es auch einem technisch wenig versierten Nutzer ermöglichen, mit wenig Aufwand selbst den aktuellsten Kopierschutz auszuhebeln.[17] Eine erhebliche Risikoerhöhung tritt aber auch bei Hackingtools im engeren Sinne ein, die häufig dazu eingesetzt werden, einem Hacker bestimmte Arbeitsabläufe automatisiert abzunehmen, deren manuelle Durchführung einen erheblichen Aufwand bedeuten würde.[18]

Die spezifische Gefahr eines Schadprogramms liegt also stets in seinen objektiven Funktionen. Diese erlauben es dem Verwender, das Computerprogramm unmittelbar deliktisch einzusetzen, kurz: Die Gefahr liegt in der unmittelbar deliktischen Eignung des Computerprogramms.

Dieses Risiko für das Rechtsgut ist je nach Vorfeldverhalten unterschiedlich hoch: Durch das bloße Herstellen eines deliktsgeeigneten Computerprogramms wird ein vergleichsweise geringes Risiko geschaffen (Fallgruppe: gefährliches Computerprogramm im eigenen Kontrollbereich). Beim Verbreiten eines solchen Computerprogramms wird das durch die Herstellung geschaffene Risiko nochmals erheblich gesteigert (Fallgruppe: Bewusster Kontrollverlust über gefährliches Computerprogramm). Es lässt sich somit festhalten, dass ein Risiko für das Rechtsgut immer und ohne weitere Bedingungen besteht – unabhängig davon, ob der Vorfeldtäter das Computerprogramm im eigenen Kontrollbereich behält oder daraus entlässt.

Auch ein *deliktischer Sinnbezug* ist im „Eignungsmodell" möglich. Es ist zweifellos denkbar, dass sich jemand als Vorfeldtäter begreift, der ein unmittelbar deliktisch einsetzbares Computerprogramm herstellt oder sonstwie damit verkehrt und sich gerade durch diese Handlung in ein deliktisches Gesamtgeschehen integrieren will. Freilich kann hier nicht aufgrund des Tatobjekts schon davon ausgegangen werden, dass dieser *deliktische* Handlungswille die einzige plausible Erklärung für das Geschehen wäre. Auch das „Eignungsmodell" ist daher darauf angewiesen, im subjektiven Tatbestand so eingegrenzt zu werden, dass die deliktische Interpretation des Geschehens die einzig plausible Interpretation ist. Dies unterscheidet das „Eignungsmodell" jedoch nicht von anderen Modellen,[19] sodass es deshalb nicht weniger legitim ist als diese anderen.

Diese übrigen Tatobjektsmodelle basieren im Wesentlichen auf subjektiv-objektiven Mischtechniken, welche kriminelle Intentionen Einzelner für maßgeblich erklären, wenn sie sich objektiv im Computerprogramm manifestieren. Sie büßen allein deshalb an Rechtsklarheit ein, es mangelt ihnen aber im Vergleich auch an Legitimität. Dies wird nachfolgend im Einzelnen gezeigt.

---

[17] Siehe dazu oben Teil 1, I.B.1.a).

[18] Siehe dazu oben Teil 1, I.B.1.b).

[19] Siehe im Einzelnen sogleich b)–e).

b) Abzulehnen: das „Zweckmodell" und das „Entstehungsmodell"

Abzulehnen ist zunächst das „Zweckmodell", in dem es darauf ankommt, ob der *Zweck des Computerprogramms* die Begehung von Zieltaten ist.[20] In der Auslegung des § 202c Abs. 1 Nr. 2 StGB durch das Bundesverfassungsgericht bestehen weitgehende Ähnlichkeiten zwischen „Zweckmodell" und „Entstehungsmodell". In Letzterem kommt es darauf an, ob das Computerprogramm *dazu bestimmt, designed, entworfen, konstruiert, hergestellt* oder *angepasst* worden ist, zur Begehung der Zieltat eingesetzt zu werden.[21] Gegen das „Entstehungsmodell" sprechen daher die wesentlich gleichen Kritikpunkte: Die Rechtsklarheit ist vergleichsweise geringer, da die Effektivität dieser Modelle beeinträchtigt ist. Ihre Legitimität leidet darunter, dass nur ein potentielles, und kein tatsächliches Risiko vorausgesetzt wird. Das „Zweckmodell" ist überdies wegen Unverständlichkeit abzulehnen.

aa) Bewertung am Maßstab der Rechtsklarheit

Schon hinsichtlich der *Effektivität* bestehen Zweifel, weil sowohl das „Zweckmodell" als auch das „Entstehungsmodell" umgehungsanfällig sind. Diese Modelle erfassen nämlich nicht alle deliktisch einsetzbaren Computerprogramme. Der Gesetzgeber wollte hier offensichtlich den Multifunktionsaspekt des Dual-Use-Phänomens berücksichtigen und deshalb den freien Verkehr bestimmter Computerprogramme, die nicht in erster Linie als Deliktswerkzeuge bekannt sind, nicht beschränken.

Diese gutgemeinte gesetzgeberische Zurückhaltung macht das Vorfelddelikt jedoch umgehungsanfällig, da Vorfeldtäter nunmehr auf solche Computerprogramme

---

[20] Das „Zweckmodell" wird in § 202c Abs. 1 Nr. 2 StGB, in § 263a Abs. 3 StGB und in § 22b Abs. 1 Nr. 3 StVG eingesetzt, also im Vorfeld des Ausspähens von Daten (§ 202a StGB), des Abfangens von Daten (§ 202b StGB), der Datenveränderung (§ 303a StGB), der Computersabotage (§ 303b StGB), des Computerbetrugs (§ 263a StGB) und des „Missbrauchs" von Wegstreckenzählern und Geschwindigkeitsbegrenzern (§ 22b Abs. 1 Nr. 1 und 2 StVG). Außerdem wird das „Zweckmodell" im EU-Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln verwendet. Es erfasst „Computerprogramme, deren Zweck die Begehung einer solchen Tat ist". Siehe im Einzelnen oben Teil 3, I.B.2. sowie II.B.5.

[21] Das „Entstehungsmodell" wird in § 4 ZKDSG und § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 3 UrhG eingesetzt, also im Vorfeld der unerlaubten Nutzung eines zugangskontrollierten Dienstes (§§ 1, 3 ZKDSG) und des Eingriffs in den technischen Schutz von Werken (§ 108b Abs. 1 UrhG). Außerdem wird das „Entstehungsmodell" verwendet in Art. 4 der EG-Richtlinie 98/84/EG, in Art. 6 der EG-Richtlinie 2001/29/EG (Urheberrecht), in Art. 3 EU-Rahmenbeschluss 2000/383/JI (Schutz des Euro), in Art. 4 EU-Rahmenbeschluss 2000/413/JI (Unbare Zahlungsmittel) und im aktuellen Kommissionsvorschlag für eine EU-Richtlinie über Angriffe auf Informationssysteme KOM(2010) 517 endgültig. Schließlich findet es sich in Art. 4 Conditional-Access-Konvention des Europarats ETS Nr. 178 und in Art. 6 Cybercrime-Konvention des Europarates ETS Nr. 185. Siehe im Einzelnen oben Teil 3, I.B.3. und 4. sowie II.B.1.–3.

zurückgreifen können, die zwar deliktisch einsetzbar sind, jedoch ursprünglich nicht hierfür hergestellt worden sind. Diese Umgehungsanfälligkeit wird noch gesteigert, wenn es nicht ausreichen soll, dass das Tatobjekt *auch* zu deliktischen Zwecken hergestellt worden ist, sondern der historische Hersteller *hauptsächlich*, *in erster Linie* oder *besonders* deliktische Ziele verfolgt haben muss. Dabei macht es keinen großen Unterschied, ob diese deliktischen Ziele des historischen Herstellers in einer Begehung, Ermöglichung oder Erleichterung von Zieltaten liegen muss. Es mindert die Effektivität des Vorfelddelikts, wenn Kriminelle die Möglichkeit haben, mit deliktsgeeigneten Computerprogrammen zu hantieren und dabei eine Bestrafung aus dem Vorfelddelikt zu umgehen.

Diesem Problem begegnet die englische Fassung des „Zweckmodells" mit dem Wortlaut „a computer program, the purpose of which is the commission of any of the offences".[22] Dieser ist zwar im Wesentlichen deckungsgleich mit dem deutschen Wortlaut, soll nach Ansicht der EU-Kommission jedoch „absichtsbezogen und instrumentenneutral"[23] ausgelegt werden. Positiv zu würdigen ist, dass demnach konsequent berücksichtigt wird, ob der *Vorfeldtäter* selbst deliktische Ziele verfolgt oder etwa zu Test-, Analyse- und Demonstrationszwecken handelt. Wenn damit aber jede objektive Konturierung des Tatgegenstands aufgegeben wird, weckt dies Zweifel an der Legitimität des Delikts.[24] Zudem ist es rechtspolitisch kaum nachzuvollziehen, weshalb eine instrumentenneutrale Absicht adjektivisch als Eigenschaft des Instruments normiert wird. Effizienter wäre es, eine solche Absicht *als Absicht* zu normieren – im subjektiven Tatbestand.

Hinsichtlich der *Effizienz* gibt es gegen das „Entstehungsmodell" grundsätzlich wenige Einwände. Der Wortlaut ist nicht unpräzise, missverständlich, umgangssprachlich oder irreführend. Auch schießt der Tatbestand nicht über die Ziele des Gesetzgebers hinaus, sodass eine teleologische Reduktion nötig wäre. Völlig anders stellt sich dies jedoch beim „Zweckmodell" dar: Dort muss ein massiver Aufwand betrieben werden, um dem Tatbestand im Wege der Auslegung überhaupt Konsistenz und Sinn zu geben. Dies hängt maßgeblich mit dessen kaum vorhandener Verständlichkeit zusammen.

Das „Zweckmodell" ist bereits grammatisch kaum *verständlich*. Die adjektivische Rede vom „Zweck eines Computerprogramms" ist paradox. Noch während des Gesetzgebungsverfahrens wurden in der juristischen Fachliteratur unterschiedlichste Vorschläge formuliert, nach welcher Struktur ein „gegenstandsbezogener Zweck" ausgelegt werden könnte. Erst das Bundesverfassungsgericht konnte in relativ freier Rechtsfindung im Wege des Beschlusses Klarheit darüber schaffen, welche Struktur der Auslegung hier zugrunde zu legen ist. Diese Schwierigkeiten

---

22 Vgl. oben Teil 3, II.B.5.

23 Siehe KOM(1998) 395 endgültig, S. 9.

24 Siehe sogleich bb).

gründeten auch darin, dass es dem Gesetzgeber nicht einmal in den Gesetzesmaterialien gelungen war, darzulegen, was er eigentlich regeln wollte. So blieb auch bis zuletzt unverständlich, welchen Akteur der Gesetzgeber eigentlich als maßgeblichen Zwecksetzer erachtete. Da schon die juristische Fachliteratur keine Handhabe für dieses Regelungsmodell fand, muss es für den juristisch gebildeten Laien völlig unverständlich sein.

bb) Bewertung am Maßstab der Legitimität

„Zweckmodell" und „Entstehungsmodell" erscheinen auch weniger legitim als das „Eignungsmodell". Sie setzen nämlich kein tatsächliches, sondern nur ein potentielles Risiko voraus. Ein „deliktischer Sinnbezug" liegt jedenfalls nicht näher als im „Eignungsmodell".

Das Risiko, das in „Zweckmodell" und „Eignungsmodell" zum Ausdruck kommt, ist lediglich ein *potentielles Risiko*. Die tatbestandlichen Kriterien dieser Modelle sagen nämlich nichts darüber aus, ob das Tatobjekt tatsächlich eine Gefahr für das Rechtsgut ausstrahlt. Die Kriterien besagen lediglich, dass das Tatobjekt *ursprünglich* nach dem Willen seiner Schöpfer einmal eine Gefahr für das Rechtsgut ausstrahlen *sollte*. Ob das Rechtsgut von dem Computerprogramm tatsächlich noch bedroht wird, ist zum Zeitpunkt der Tathandlung ungewiss. Es ist noch nicht einmal Voraussetzung, dass das Computerprogramm überhaupt je zur Begehung von Straftaten eingesetzt werden konnte – es genügt ja bereits, wenn die historischen Hersteller dies (auch vergeblich) beabsichtigt haben und sich dies im Computerprogramm äußerlich manifestiert hat.

In der Auslegung des „Zweckmodells" nach der EU-Kommission[25] verkörpert das Tatobjekt sogar überhaupt keine Risikoerhöhung mehr. Denn nach dieser Auslegung drückt sich der „kriminelle Zweck des Computerprogramms" allein in subjektiven Intentionen aus und muss nicht im Computerprogramm manifestiert sein, sodass das Tatobjekt jegliche Kontur verliert. Jedes Computerprogramm ist tatbestandsmäßig. Da in dieser Auslegung sowohl die Risikoerhöhung als auch der „deliktische Sinnbezug" allein aus der subjektiven Tatseite gewonnen werden müssten, wäre das „Zweckmodell" in dieser Auslegung von allen Tatobjektsmodellen am wenigsten legitim.

Ein *deliktischer Sinnbezug* ist in „Zweckmodell" und „Entstehungsmodell" grundsätzlich denkbar. Möglicherweise begreift sich jemand als Vorfeldtäter, der mit einem Computerprogramm umgeht, das zu deliktischen Zwecken geschaffen wurde. Möglicherweise sieht er seine Handlung zudem als Teil eines deliktischen Gesamtgeschehens.[26] Dies liegt hier aber nicht näher als im „Eignungsmodell",

---

[25] Vgl. oben Teil 3, II.B.2.b).

[26] Möglicherweise ist er auch IT-Sicherheitsbeauftragter und handelt sozialnützlich.

denn das „Zweckmodell“ zeichnet sich ja im Wesentlichen dadurch aus, dass es die Intentionen des historischen Herstellers objektiv mit berücksichtigt. Diese sind aber grundsätzlich unabhängig von denen des Vorfeldtäters, sodass sie keine Rückschlüsse auf einen deliktischen Handlungswillen des Vorfeldtäters zulassen. Unter diesem Aspekt spricht also nichts dafür, dass das „Zweckmodell“ eher legitim wäre als das „Eignungsmodell“.

c) Abzulehnen: das „ökonomische Modell“

Ebenso abzulehnen ist das „ökonomische Modell“. Nach diesem Modell ist ein Computerprogramm tatbestandsmäßig, wenn sein *wirtschaftlicher Zweck oder Nutzen neben der Zieltat begrenzt ist*.[27] Im Vergleich zum „Eignungsmodell“ mangelt es dem „ökonomischen Modell“ nicht grundsätzlich an Rechtsklarheit und Legitimität, jedoch erscheint sein effektiver Anwendungsbereich zu klein.

aa) Bewertung am Maßstab der Rechtsklarheit

Das „ökonomische Modell“ legt eine wirtschaftliche Sichtweise zugrunde und ist deshalb nur *effektiv*, soweit man davon ausgeht, dass ein Vorfeldtäter sich kein Computerprogramm verschafft, wenn er die Anschaffungskosten nicht durch den deliktischen Einsatz kompensieren kann. Folglich setzt diese Regelungstechnik voraus, dass ein Computerprogramm bei deliktischem Einsatz stets einen wirtschaftlichen Nutzen hat. Dadurch werden solche Vorfeldtäter nicht erfasst, die ihre Straftaten aus ideeller Überzeugung begehen und hierfür Computerprogramme einsetzen, die gar keinen wirtschaftlichen Zweck oder Nutzen haben. Der Anwendungsbereich des „ökonomischen Modells“ ist daher geringer als der des „Eignungsmodells“. Die Regelungstechnik ist weniger effektiv.

Unter dem Gesichtspunkt der *Effizienz* ist das „ökonomische Modell“ nicht grundsätzlich kritikwürdig. Dies gilt jedenfalls dann, wenn im Tatbestand präzise und unmissverständlich klargemacht wird, worauf es ankommen soll: Bei einem Computerprogramm, das sowohl legal als auch illegal eingesetzt werden kann, sollen die daraus jeweils resultierenden wirtschaftlichen Vorteile verglichen werden. Die konkreten Ausgestaltungen des „ökonomischen Modells“ drücken dies freilich unpräzise und umgangssprachlich aus, und zwar sowohl im deutschen § 95a Abs. 3 Nr. 2 UrhG als auch in seinem Vorläufer in Art. 6 Nr. 2 lit. (b) der RL 2001/29/EG.

---

[27] Das „ökonomische Modell“ wird in § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 2 UrhG eingesetzt und erfasst damit das Vorfeld des Eingriffs in den technischen Schutz von Werken (§ 108b Abs. 1 UrhG). Tatbestandsmäßig sind demnach Computerprogramme, „die abgesehen von der Umgehung wirksamer technischer Maßnahmen nur einen begrenzten wirtschaftlichen Zweck oder Nutzen haben“. Das „ökonomische Modell“ wird auch in Art. 6 der EG-Richtlinie 2001/29/EG (Urheberrecht) verwendet. Siehe im Einzelnen oben Teil 3, I.B.5 und II.B.6.

Dies liegt zunächst am Begriff des wirtschaftlichen „Zwecks oder Nutzens“. Der Gesetzgeber hat mit dem Zweck ein sehr komplexes Tatbestandsmerkmal aufgenommen, ohne dieses vom Nutzen sauber abzugrenzen. Es ist auch nicht ersichtlich, weshalb die Normgeber das Zweck-Merkmal überhaupt neben dem Nutzen-Merkmal für erforderlich hielten. Das Doppelmerkmal „Zweck *oder* Nutzen“ erscheint daher als überflüssige Tatbestandsblähung.

Sodann ist die verwendete Umgangssprache zu kritisieren: Die Tatbestände erheben zum entscheidenden Kriterium, ob ein Computerprogramm bei nichtkriminellem Einsatz einen *unbegrenzten* wirtschaftlichen Nutzen hat. Dies ist offensichtlich nicht so gemeint. Höchstwahrscheinlich sollte hier maßgeblich sein, ob der Nutzen bei legalem Einsatz *erheblich* ist oder *überwiegt*, nicht aber ob er unbegrenzt ist.

Eine effiziente Regelung nach dem „ökonomischen Modell“ würde also beispielsweise Computerprogramme erfassen, die *neben der Zieltat nur einen unerheblichen wirtschaftlichen Nutzen bieten*. Solange dieser Inhalt erst im Wege der Auslegung gewonnen werden muss, weil der tatsächliche Tatbestand von einem „begrenzten wirtschaftlichen Zweck oder Nutzen“ spricht, ist diese Regelungstechnik vergleichsweise ineffizient.

Das „ökonomische Modell“ ist als solches nach dem Maßstab der Rechtsklarheit nicht zwingend kritikwürdig. Kritikwürdig ist in erster Linie seine unsaubere Umsetzung.

bb) Bewertung am Maßstab der Legitimität

Das „ökonomische Modell“ bietet ein vergleichsweise hohes Maß an Legitimität. Es impliziert, dass das tatbestandsmäßige Computerprogramm bei deliktischem Einsatz einen erheblichen wirtschaftlichen Vorteil generiert. Damit setzt es nicht nur die Eignung des Computerprogramms zum kriminellen Einsatz voraus, sondern auch einen – zumindest wirtschaftlichen – Anreiz. Darin liegt eine beträchtliche Risikoerhöhung für das geschützte Rechtsgut.

Auch ein „deliktischer Sinnbezug“ ist in diesem Regelungsmodell denkbar, vielleicht sogar naheliegend. Denn auf den ersten Blick erscheint es als wahrscheinlich, dass jemand den erheblichen wirtschaftlichen Nutzen auch erzielen will, den das Computerprogramm in seinem Kontrollbereich bei kriminellem Einsatz bietet. Wenn er das Computerprogramm aus seinem Kontrollbereich entlässt, findet er sich offensichtlich damit ab, dass möglicherweise ein Dritter diesen wirtschaftlichen Nutzen erzielen wollen wird. Gleichwohl müssen IT-Sicherheitsbeauftragte auch auf solche Computerprogramme zu Test- und Analysezwecken zugreifen und sie gegebenenfalls Kollegen zur Verfügung stellen. Deshalb kann auch in diesem Regelungsmodell nicht allein anhand des objektiven Tatbestands ein *eindeutig* „deliktischer Sinnbezug“ festgestellt werden.

Zusammenfassend kann die wirtschaftliche Betrachtung im „ökonomischen Modell“ zur Unterscheidung zwischen legitimem und illegitimem Vorfeldverhalten sinnvoll sein. Das Modell kann zudem in einem rechtsklaren Tatbestand von hoher Legitimität umgesetzt werden. Dem „Eignungsmodell“ ist dennoch der Vorzug gegenüber dem „ökonomischen Modell“ zu geben, weil das „Eignungsmodell“ auch Vorfeldverhalten angemessen erfassen kann, das von wirtschaftlichen Motiven losgelöst ist.

d) Abzulehnen: das „Marketingmodell“

Im Ergebnis ist auch das „Marketingmodell“ abzulehnen, das darauf abstellt, ob ein Computerprogramm als Deliktswerkzeug vermarktet wird.[28] Im Tatbestand wird dieser Ansatz de lege lata so ausgedrückt, dass das Computerprogramm *Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel einer Zieltat* sein muss.

aa) Bewertung am Maßstab der Rechtsklarheit

Unter dem Aspekt der Effektivität ist hier derselbe Kritikpunkt anzubringen wie in „Zweckmodell“ und „Entstehungsmodell“: Auch hier wird die Intention eines Dritten zum maßgeblichen Kriterium dafür gemacht, ob das Computerprogramm, mit dem der Vorfeldtäter hantiert, objektiv ein taugliches Tatobjekt darstellt. Damit entsteht auch hier das Problem makelloser Software, die völlig frei zirkulieren kann, obwohl sie unmittelbar zur Begehung von Straftaten eingesetzt werden kann. Realistischerweise wird man aber annehmen müssen, dass jedes Computerprogramm, das deliktisch eingesetzt werden kann und aus diesem Grunde zwischen Vorfeldtätern zirkuliert, wohl zuvor auch einmal in diesem Sinne angepriesen worden ist. Es liegt außerdem die Vermutung nahe, dass der Gesetzgeber auch umgekehrt davon ausging, dass Computerprogramme, die als Deliktswerkzeug beworben werden, wohl regelmäßig tatsächlich zur Deliktsbegehung eingesetzt werden.

Unter dem Gesichtspunkt der *Effizienz* ist die Weite des „Marketingmodells“ bedenklich, da es den Kreis der beachtlichen Werbetreibenden nicht beschränkt. Dadurch kann ein auf dem Markt etabliertes Computerprogramm tatbestandsmäßig werden, sobald es in irgendeinem Blog oder Forum als Deliktswerkzeug angepriesen wird. Wenn dieses Modell in einem Anschließungsdelikt eingesetzt wird, ver-

---

[28] Das „Marketingmodell“ wird in § 108b Abs. 2 UrhG i.V.m. § 95a Abs. 3 Nr. 1 UrhG eingesetzt und erfasst damit das Vorfeld des Eingriffs in den technischen Schutz von Werken (§ 108b Abs. 1 UrhG). Tatbestandsmäßig sind demnach Computerprogramme, „die Gegenstand einer Verkaufsförderung, Werbung oder Vermarktung mit dem Ziel der Umgehung wirksamer technischer Maßnahmen sind“. Dieses Regelungsmodell wird auch in Art. 6 der EG-Richtlinie 2001/29/EG (Urheberrecht) verwendet. Siehe im Einzelnen oben Teil 3, I.B.6. und II.B.4.

liert das Computerprogramm umgehend seine Verkehrsfähigkeit und jeder, der von dem Blog- oder Foreneintrag gehört hat und dennoch mit dem Computerprogramm hantiert, es also herstellt, nutzt oder damit handelt, ist einem erheblichen Haftungsrisiko ausgesetzt. Bei enger Auslegung am Wortlaut gilt dies sogar dann, wenn der Blogeintrag falsch ist und das Computerprogramm gar nicht zur Deliktsbegehung eingesetzt werden kann. Hält man diese tatbestandliche Weite für unverhältnismäßig, so ist in diesen Fällen das „Marketingmodell" ineffizient: Es muss erst im Wege der Auslegung auf ein erträgliches Strafbarkeitsmaß reduziert werden und die eigentliche Strafbarkeitsgrenze geht nicht aus dem Tatbestand selbst hervor.

Nach dem Kriterium der *Verständlichkeit* ist das „Marketingmodell" nicht grundsätzlich zu beanstanden. Wenn im Tatbestand benannt ist, dass es auf die Vermarktung als Deliktswerkzeug ankommt, kann der Rechtsunterworfene auch ohne juristische Fachkunde ein Gefühl dafür entwickeln, ob ein konkretes Computerprogramm tatbestandsmäßig ist oder nicht.

Verständnisprobleme ergeben sich freilich in der konkreten Umsetzung des „Marketingmodells" in § 95a Abs. 3 UrhG. Dieser verbietet eingangs unter anderem, für Vorrichtungen zu werben, die den Nrn. 1–3 entsprechen („Verboten sind …, die Werbung im Hinblick auf Verkauf oder Vermietung […] von Vorrichtungen [i.S.d. Nummern 1–3]"). Also verbietet § 95a Abs. 3 Nr. 1 UrhG auch, für solche Vorrichtungen zu werben, die (schon) als Deliktswerkzeug beworben werden.

Insofern ist es zumindest konsequent, wenn das LG München I einen Verstoß des Unternehmens *Slysoft* gegen § 95a Abs. 3 Nr. 1 (!) UrhG annimmt, weil es auf seiner Homepage für das Computerprogramm *AnyDVD* als Kopierschutzknacker wirbt.[29] Nach dieser Auffassung würde aber *Slysoft* durch exakt dasselbe Verhalten (Werbung auf der Homepage) sowohl ein taugliches Verbotsobjekt erzeugen (Vorrichtung, die als Umgehungsmittel beworben wird, Nr. 1) als auch eine taugliche Verbotshandlung begehen (Werbung im Hinblick auf den Verkauf einer solchen Vorrichtung).

Hiergegen kann man allerdings einwenden, dass ein taugliches Verbotsobjekt zumindest eine logische Sekunde vor Vornahme der verbotenen Handlung vorliegen müsste. Dann ergibt sich aber die eigenartige Konsequenz, dass ein erster Werbetreibender nie die Alternative des § 95a Abs. 3 Nr. 1 UrhG erfüllen kann, weil zu diesem Zeitpunkt noch kein taugliches Verbotsobjekt vorliegt. Erst ein zweiter Werbetreibender erfüllt dann den Tatbestand, da aufgrund der Werbung des ersten Werbetreibenden nun auch ein taugliches Verbotsobjekt vorliegt. Am Unrechtsgehalt ändert es freilich wenig, ob der Täter der erste oder der zweite ist, der ein Deliktswerkzeug als solches bewirbt.

Wenn man in dieser Konstellation einen Verstoß des Unternehmens Slysoft prüft, ist es schlüssiger, das Werbungsverbot des § 95a Abs. 3 Nr. 3 (!) UrhG zu

---

[29] LG München I MMR 2008, 194.

prüfen und zu bejahen: Slysoft wirbt im Hinblick auf den Verkauf einer Vorrichtung, die hauptsächlich entworfen und hergestellt wird, um die Umgehung wirksamer technischer Maßnahmen zu ermöglichen.[30] Konkret ging es in dem Verfahren jedoch nicht um Verstöße der Firma Slysoft, sondern um einen etwaigen Verstoß der Nachrichtenplattform *heise-online*. Zurecht prüft daher das OLG München in seiner Entscheidung, ob *heise-online* entgegen § 95a Abs. 3 UrhG für eine Vorrichtung „im Hinblick auf Verkauf wirbt", die gemäß § 95a Abs. 3 Nr. 1 UrhG von *Slysoft* mit dem Ziel der Umgehung technischer Schutzmaßnahmen angepriesen wird.[31] Dem LG Köln ist hier nur beizupflichten, wenn es in anderem Zusammenhang annimmt, dass „sich weder der europäische noch der nationale Gesetzgeber offenbar verstärkte Gedanken über die Tatbestandsalternativen gemacht" haben.[32]

bb) Bewertung am Maßstab der Legitimität

Im „Marketingmodell" schafft der Täter nicht durchweg ein *Risiko für das Rechtsgut*. Wenn ein Computerprogramm als Deliktswerkzeug beworben wird, ist dies für das Rechtsgut jedenfalls dann völlig ungefährlich, wenn das Computerprogramm *kein Deliktswerkzeug ist*. Diese Konstellation wird im „Marketingmodell" nicht ausgeschlossen: Ein entsprechend beworbenes Computerprogramm bleibt tatbestandsmäßig, auch wenn beispielsweise die Sicherheitslücke mittlerweile geschlossen ist, die es ursprünglich ausgenutzt hatte und das Computerprogramm dadurch untauglich geworden ist. In diesem Fall mag eine Verbrauchertäuschung vorliegen (wobei man mit dem Verbraucher, der sich hier täuschen lässt, wohl wenig Mitgefühl hat), nicht jedoch ein Risiko für das geschützte Rechtsgut.

Man kann deshalb sagen, dass das „Marketingmodell" keine Risikoschaffung oder -erhöhung normiert, sondern eine *Risikopotenz*: Liegt tatsächlich ein Risiko in Form eines deliktsgeeigneten Computerprogramms vor, so wird dieses Risiko durch die Marketinghandlungen *potenziert* und erhöht. Ist das Computerprogramm dagegen nicht deliktsgeeignet, so ist das Risiko für das Rechtsgut gleich Null. Wird dieses Risiko durch Marketinghandlungen *potenziert*, so bleibt es gleich Null. Da also nicht durchweg ein Risiko für das Rechtsgut geschaffen wird, erscheint

---

[30] Zur Auslegung der Nr. 3 des § 95a Abs. 3 UrhG siehe oben, I.B.4.a).

[31] OLG München ZUM 2005, 898 f.

[32] LG Köln MMR 2006, 416. Interessant ist zudem der Wandel des Verbraucherbilds: In der Conditional-Access-Richtlinie 98/84/EG sollte der „naive" Verbraucher davor geschützt werden, von Kriminellen getäuscht zu werden und dadurch ein illegales Computerprogramm für legal zu halten. In der Urheberrechtsrichtlinie 2001/29/EG wird dem Verbraucher verboten, sich von „deliktischer" kommerzieller Kommunikation verführen zu lassen. Man geht inzwischen offenbar von einem Bürger aus, der Deliktswerkzeugen offen gegenübersteht und sich möglicherweise gerade durch die entsprechende Vermarktung zu ihrem Kauf und Einsatz hinreißen lässt.

das „Marketingmodell“ unter diesem Aspekt weniger legitim als das „Eignungsmodell“.

Ein *deliktischer Sinnbezug* ist freilich auch in diesem Modell denkbar. Möglicherweise will der Handelnde sich als Vorfeldtäter in ein deliktisches Gesamtgeschehen integrieren und ist gerade durch die Marketinghandlungen darauf aufmerksam geworden, dass dieses Computerprogramm das rechte Werkzeug sein könnte. Möglicherweise ist der Handelnde aber auch als IT-Sicherheitsbeauftragter durch die Marketinghandlungen auf das Computerprogramm aufmerksam geworden und will überprüfen, ob sein System durch dieses Programm kompromittiert werden kann. Wie im „Eignungsmodell“ muss also auch im „Marketingmodell“ der Tatbestand noch subjektiv beschränkt werden, damit der „Sinnbezug“ *eindeutig* deliktisch ist.

e) Abzulehnen: das „Listenmodell“

Das „Listenmodell“ setzt *Blankettgesetze* ein, deren einzelne Tatobjekte sich sodann aus einer konkreten Liste ergeben.[33] Dieses Modell zeichnet sich durch eine vergleichsweise geringere Rechtsklarheit und Legitimität aus und ist deshalb nicht dem „Eignungsmodell“ vorzuziehen.

aa) Bewertung am Maßstab der Rechtsklarheit

Das „Listenmodell“ ist vergleichsweise effektiv und effizient. Es fehlt ihm jedoch an Verständlichkeit. Unter dem Schlagwort der *Effektivität* wird hier gefordert, dass ein Straftatbestand kein Symbolgesetz darstellt und sein Anwendungsbereich nicht zu eng ist. Unter diesem Aspekt ist freilich nichts gegen ein Blankettgesetz einzuwenden, da dieses ja typischerweise konturlos ist und seinen relevanten Inhalt aus anderer Quelle bezieht. Ineffektiv wäre ein Blankettgesetz daher nur, wenn die bezogene Liste nicht umfassend wäre. Im Bereich des Software-Strafrechts würde die Unterhaltung einer effektiven Liste freilich erheblichen administrativen Aufwand bedeuten, da Schadsoftware von einer Vielzahl von Tätern weltweit entwickelt wird, deren Arbeit zudem von hoher Professionalität und Innovationsfreude geprägt ist.[34] Dennoch wäre grundsätzlich denkbar, etwa nach Art der Antiviren-Hersteller die Signaturen von Schadsoftware nach bestimmten Methoden zu ermitteln und in eine entsprechende Schadsoftware-Liste aufzunehmen. Da von einem enormen Dunkelfeld im gesamten Bereich des Cybercrime ausge-

---

[33] Das „Listenmodell“ wird für Software-Delikte de lege lata nicht verwendet. Es findet sich aber im Rüstungskontrollrecht, etwa in § 34 Abs. 1 Satz 1 AWG i.V.m. §§ 7, 2 Abs. 1 Nr. 1 AWG, wiederum i.V.m. § 5 AWV und Anhang AL zur AWV (= Ausfuhrliste). Erfasst sind demnach „in Teil [x] Abschnitt [y] der Ausfuhrliste (Anlage AL zur Außenwirtschaftsverordnung) genannte Güter“. Siehe im Einzelnen oben Teil 3, III.B.2.

[34] Vgl. oben, Einleitung, I.

gangen werden muss,[35] wäre eine solche Liste freilich immer unvollständig, selbst wenn sie stets aktuell wäre.

Das „Listenmodell" ist nicht *ineffizient*. Dies wäre der Fall, wenn sein Inhalt unpräzise und missverständlich wäre, sodass eine präzisierende oder einschränkende Auslegung erforderlich wäre. Das „Listenmodell" zeichnet sich jedoch gerade durch seine hohe Präzision aus. Das Blankettgesetz erlaubt es, dass Einzelfälle als präzise Tatobjekte in einer Liste beschrieben werden. Zudem kann eine Liste wie die Ausfuhrliste (Anhang AL zur AWV) schnell und flexibel angepasst werden.[36] Auch bestehen keine grundsätzlichen verfassungsrechtlichen Bedenken mehr gegen die Weite und Bestimmtheit einer solchen Blankettnorm.[37]

Zu kritisieren ist jedoch die mangelnde *Verständlichkeit* des „Listenmodells": Seine inhaltliche Reichweite ist nicht aus dem Straftatbestand selbst ersichtlich, denn dieser ist blank. Die Grenzen der Strafbarkeit werden erst durch den Verweis auf eine Verordnung bestimmt, die ihrerseits wieder auf die Blankettnorm und daneben auf einen Anhang zur Verordnung verweist, in dem sich dann eine Liste der tauglichen Tatobjekte befindet. Diese „Mechanik" schadet der Lesbarkeit.

Der blanke Straftatbestand birgt zudem die Gefahr, dass es für den Rechtsunterworfenen nicht mehr nachvollziehbar ist, *warum* ein bestimmter Gegenstand überhaupt in die Liste im Anhang der Verordnung aufgenommen worden ist. Diese verminderte Nachvollziehbarkeit muss im „Listenmodell" durch Vertrauen in den Verordnungsgeber und Listenersteller kompensiert werden.

Das „Listenmodell" leidet also an seiner mangelnden Verständlichkeit. Würde man das Modell auf die Software-Delikte übertragen, so wäre zudem seine Rechtsklarheit wegen der eingeschränkten Effektivität gemindert.

bb) Bewertung am Maßstab der Legitimität

Das „Listenmodell" lässt sich nicht abschließend hinsichtlich seiner Legitimität beurteilen, da es eine rein formelle Regelungstechnik vorsieht.[38] Der Umgang mit einem aufgelisteten Gegenstand schafft per se weder ein Risiko für irgendein Rechtsgut, noch beinhaltet er irgendwelche Vorwertungen hinsichtlich eines „deliktischen Sinnbezugs". Hier hängt alles davon ab, wie gefährlich dieser aufgelistete Gegenstand ist. Also hängt die Legitimität davon ab, nach welchen Kriterien ein Computerprogramm im Einzelfall in die Liste aufgenommen worden ist.

---

[35] Vgl. Bundeskriminalamt, Cybercrime Bundeslagebild 2010, S. 7.

[36] Erbs/Kohlhaas-*Diemer*, A 217 Außenwirtschaftsgesetz, § 34 Rn. 2.

[37] BVerfG NJW 1993, 1909; BGH NJW 1965, 769; BGH NJW 1992, 3114 f.; NJW 1996, 602 f.; *Bieneck*, wistra 1994, 173.

[38] Siehe oben B.1.b).

Damit muss im „Listenmodell“ bei jeder Aufnahme eines Computerprogramms in die Liste gefragt werden, ob dieses Computerprogramm eine Risikoerhöhung für die geschützten Rechtsgüter darstellt und ob ein „eindeutig deliktischer Sinnbezug“ bei diesem konkreten Computerprogramm naheliegend oder zumindest denkbar ist. Erst wenn der Gesetzgeber (konkreter: der „Verordnungsanhanggeber“) beides bejaht, kann er das Computerprogramm legitim in den Anhang der Verordnung aufnehmen. Ob der Sinnbezug dann *eindeutig* deliktisch ist, wird sich – wie in den anderen Regelungsmodellen auch – nicht an dem Tatobjekt allein festmachen lassen, sondern nur unter Rückgriff auf den subjektiven Tatbestand bestimmen lassen.

Damit wird deutlich: Das „Listenmodell“ ist als formeller Ansatz nur potentiell legitim. Seine Legitimität hängt in jedem Einzelfall davon ab, ob der konkrete Listeneintrag legitim vorgenommen worden ist.

f) Zusammenfassung: Regelung des Tatobjekts

Es hat sich gezeigt, dass zur Regelung des Tatobjekts das „Eignungsmodell“ vorzugswürdig ist. Es hat einen umfassenden Anwendungsbereich, der präzise und unmissverständlich formuliert werden kann. Seine Legitimität bezieht das Modell aus einer objektiv durchweg vorhandenen Risikoschaffung oder -erhöhung, bei der ein „deliktischer Sinnbezug“ stets möglich ist.

Eine vergleichbare Rechtsklarheit erreichen nur das „ökonomische Modell“ und das „Listenmodell“. Gegen das „ökonomische Modell“ spricht aber, dass es Konstellationen nicht erfassen kann, in denen wirtschaftliche Erwägungen keine Rolle spielen. Gegen das „Listenmodell“ spricht, dass es die maßgeblichen Entscheidungen nicht im Tatbestand trifft, sondern – etwas verschleiernd – in eine Anlage zu einer Verordnung zu einem Tatbestand verschiebt.

Erhebliches Missbrauchspotential weisen insbesondere das „Zweckmodell“, das „Entstehungsmodell“ und das „Marketingmodell“ auf. Sie erfassen nicht alle Computerprogramme, die sich zur Begehung von Straftaten verwenden lassen, sondern nur diejenigen, die aus Sicht eines Dritten nach bestimmten Kriterien als „bösartig“ eingestuft werden. Hierin liegt die Umgehungsanfälligkeit, denn kriminelle Vorfeldtäter können auf deliktsgeeignete Computerprogramme zugreifen, die von diesem Dritten (noch) als makellos beurteilt werden. Rechtstechnisch wird dies dadurch verursacht, dass die Intentionen eines Dritten zu adjektivischen Eigenschaften des Tatobjekts erklärt werden: Fragt man danach, wozu das Computerprogramm konstruiert, entworfen oder hergestellt worden ist, so fragt man im Grunde objektiviert nach den Intentionen des Herstellers. Im „Marketingmodell“ fragt man objektiviert nach den Intentionen des Werbetreibenden. Auffällig ist hier zudem, dass sich die obergerichtliche und höchstrichterliche Rechtsprechung in der Auslegung der einzelnen Tatbestände gar nicht an das konkret eingesetzte Modell gehalten hat. Vielmehr hat sie zur Rechtsfindung die Aspekte aller drei Modelle zusam-

mengeworfen.[39] So wurde eine Abgrenzung von Eignung, Zweck, Bestimmung und Zweckbestimmung regelmäßig gar nicht erst versucht, sondern die Entstehungsgeschichte und Vermarktung des Computerprogramms wurden als Einzelaspekte einer wertenden Gesamtschau herangezogen.[40]

Dies bestätigt den Befund, dass die Kriterien der Tatobjektsmodelle (Zweck, Entstehungsgeschichte, Vermarktung) eigentlich Abwägungskriterien und Indizien sind, die Rückschlüsse darauf zulassen, ob der Vorfeldtäter selbst mit seiner Handlung kriminelle Absichten verfolgt. Dies ist auch der eigentlich ausschlaggebende Punkt! Entscheidend ist in allen vom Gesetzgeber anvisierten Lebenssachverhalten, ob der Vorfeldtäter selbst die Begehung von Straftaten beabsichtigt. Nur ist es eben ein konzeptioneller Fehler, wenn man die Indizien für diese maßgebliche Absicht objektiviert und zu objektiven Tatbestandsmerkmalen umfunktioniert, statt auf die Absicht selbst abzustellen.

Erklärlich ist der gesetzgeberische Versuch einer normativen Eingrenzung des objektiven Tatbestandes freilich daraus, dass er wohl diese Vorfeldstrafbarkeit nicht zu stark auf den subjektiven Tatbestand stützen wollte. Zudem sollte wohl – ironischerweise – besondere Rechtssicherheit für IT-Sicherheitsbeauftragte geschaffen werden, indem diese möglichst schon im objektiven Tatbestand von einer Strafbarkeit ausgenommen werden. Dieser gutgemeinte Ansatz übersieht aber, dass man sich im Rahmen von Angriffssimulationen faktisch objektiv tatbestandsmäßig verhalten muss.[41] Ein simulierter Angriff, der sich schon objektiv von einem echten Angriff unterscheidet, ist eine schlechte Simulation.

Es hat sich daneben gezeigt, dass in keinem Tatobjektsmodell ein *eindeutiger* „deliktischer Sinnbezug“ vorhanden ist und auch nicht vorhanden sein kann, weil der Umgang mit den tatbestandsmäßigen Computerprogrammen stets auch als legitim interpretiert werden kann – insbesondere als Test- und Analyseverhalten eines IT-Sicherheitsbeauftragten oder etwa auch als wissenschaftliche Neugier.[42] Alle Software-Delikte müssen deshalb im subjektiven Tatbestand so beschränkt werden, dass für das tatbestandliche Verhalten keine plausible, rechtmäßige Alternativerklärung gefunden werden kann.

---

[39] Zum „Entstehungsmodell“: LG Karlsruhe NStZ-RR 2007, 19 ff.; zum „Zweckmodell“: BVerfG, 2 BvR 1589/05; BVerfG, 2 BvR 2233/07; OLG Frankfurt a.M. GRUR-RR 2003, 287 ff.; zum „Marketingmodell“: OLG Hamburg MMR 2009, 851 ff; LG München I MMR 2008, 192 ff.; OLG München MMR 2009, 118.

[40] So explizit BVerfG 2 BvR 2233/07, Rn. 68.

[41] So auch *Trayer*, Technische Schutzmaßnahmen, S. 116.

[42] Etwas anderes mag gelten, wenn nicht Computerprogramme das Tatobjekt sind, sondern etwa Kreditkartendatensätze von Dritten. Hier gibt es regelmäßig keine rechtmäßige Alternativerklärung dafür, dass ein Vorfeldtäter solche Datensätze in großen Mengen bezieht oder hortet. Wenn in solchen Konstellationen Vorfelddelikte geschaffen oder diskutiert werden, vgl. § 202c Abs. 1 Nr. 1 (!) StGB, können die Ausführungen dieser Arbeit nicht ohne Weiteres übertragen werden.

2. Die Gestaltung der subjektiven Tatseite

Zur Regelung der subjektiven Tatseite stehen das „Handeln in Verwendungsabsicht", das „Vorbereiten", die „Begehungsabsicht" oder der Verzicht auf einen subjektiven Bezug als Regelungsmodelle zur Verfügung. Im vorangehenden Kapitel wurde ermittelt, dass zur Regelung des Tatobjekts das „Eignungsmodell" vorzugswürdig ist, da es eine vergleichsweise hohe Rechtsklarheit gewährleistet und zudem eine erhebliche Risikoschaffung oder -erhöhung enthält. Im subjektiven Tatbestand muss nun ein Bezug des Vorfeldtäters zur Zieltat ausgedrückt werden, der ebenfalls ein hohes Maß an Rechtsklarheit gewährleistet und zudem das tatbestandliche Verhalten so prägt, dass eine plausible, rechtmäßige Alternativerklärung des Geschehens undenkbar erscheint („eindeutig deliktischer Sinnbezug").

Nachfolgend wird gezeigt, dass sich hierfür die Normierung einer Verwendungsabsicht anbietet (sogleich a)). Andere subjektive Bezüge, insbesondere ein Vorbereitungsvorsatz oder eine Begehungsabsicht bewähren sich dagegen weniger. Unzulässig erscheint der völlige Verzicht auf einen subjektiven Bezug.

a) Vorzugswürdiges Vorsatzmodell: das Handeln in Verwendungsabsicht

Als vorzugswürdig erweist sich die Normierung einer Verwendungsabsicht, wie sie sich in der englischen Fassung des Art. 6 Ziff. 1 lit. a CCC findet.[43] Danach muss der Vorfeldtäter mit der *Absicht* handeln, dass das Computerprogramm *für die Begehung einer Zieltat verwendet werde*.

aa) Bewertung am Maßstab der Rechtsklarheit

Die Regelung einer Verwendungsabsicht wahrt die *Effektivität* des Software-Delikts, da sie den weiten objektiven Tatbestand des „Eignungsmodells" zwar eingrenzt, ihm aber nicht den Anwendungsbereich entzieht. Auf eine solche Absicht des Vorfeldtäters kann aufgrund objektiver Anhaltspunkte erkannt werden, wobei insbesondere die heimlichen Ermittlungsmethoden die Beweisführung erleichtern.[44] Das entsprechende Software-Delikt wird dadurch also nicht zum Symbolgesetz.

Diese Regelung sichert zudem die *Effizienz* des Software-Delikts, da sie den Tatbestand auf ein erträgliches Maß reduziert. Es ist nicht denkbar, dass ein Vorfeldtäter mit einem deliktsgeeigneten Computerprogramm in der Absicht hantiert,

---

[43] Das Regelungsmodell der Verwendungsabsicht findet sich nur in der englischen, nicht aber der deutschen Fassung des Art. 6 Ziff. 1 lit. a CCC. Siehe im Einzelnen oben Teil 3, III.C.1.

[44] So auch *Sieber*, NStZ 2009, 361.

dass dieses Computerprogramm zur Begehung von Straftaten eingesetzt werde und dieses Geschehen dennoch im Wege teleologischer Reduktion des Tatbestandes von der Strafbarkeit ausgenommen werden müsste. Auch ist das Merkmal der Verwendungsabsicht nicht unpräzise.

Schließlich ist das Merkmal auch *verständlich*. Da hier als Handlungsrichtung *(Diathese)* das Passiv gewählt wird, ist unmittelbar deutlich gemacht, dass sich die Absicht des Vorfeldtäters auch darauf erstrecken kann, dass *ein anderer* als er selbst das Computerprogramm zur Begehung einer Straftat einsetzt.

bb) Bewertung am Maßstab der Legitimität

Unter dem Aspekt der Legitimität kommt dem subjektiven Merkmal vor allem die Aufgabe zu, einen *eindeutig deliktischen Sinnbezug* herzustellen. Dies gelingt dem Merkmal der Verwendungsabsicht, jedoch sind hier Differenzierungen nach den Kategorien von Vorfeldverhalten[45] erforderlich.

Grundsätzlich werden durch die Verwendungsabsicht der subjektive Tatbestand und die subjektive Lebenswirklichkeit unter dem Mehrzweckaspekt der Dual-Use-Problematik kongruent. Denn dies ist der entscheidende Unterschied zwischen einem IT-Sicherheitsbeauftragten und einem Vorfeldtäter: Der IT-Sicherheitsbeauftragte hat kein Interesse an der Begehung der Zieltaten. Er handelt vielmehr mit dem Fernziel, solche Zieltaten bereits auf technischer Ebene unmöglich zu machen. Nur deshalb simuliert er Angriffe, analysiert dabei Arbeits- und Wirkungsweise der Schadsoftware und weist somit gegebenenfalls Schwachstellen nach. Ein Vorfeldtäter dagegen plant entweder selbst die Begehung von Zieltaten oder er profitiert davon, dass andere mit dem tatgegenständlichen Computerprogramm Zieltaten begehen wollen.

Es bietet sich freilich an, bereits bei der Schaffung eines Software-Delikts näher auszuführen, welche Vorsatzformen unter den Absichtsbegriff gefasst werden sollen. Denn oben wurde bereits dargelegt, dass die Rechtsprechung dazu tendiert, im Einzelfall zu entscheiden, ob dolus directus 1. Grades oder 2. Grades oder sogar dolus eventualis dem Absichtserfordernis genügt.[46] Um diesbezüglich keine Unsicherheit in der IT-Sicherheitsbranche aufkommen zu lassen, kann der Gesetzgeber diese Entscheidung in Tatbestand und Gesetzesmaterialien vorzeichnen.

Hierfür sollte obige Fallgruppenbildung berücksichtigt werden: In der Fallgruppe der „gefährlichen Gegenstände im eigenen Kontrollbereich“[47] sollten an die Absicht höhere Anforderungen gestellt werden, da hier das objektive Risiko relativ gering ist und die Strafbarkeit ihre Legitimation im Wesentlichen aus der subjekti-

---

[45] Siehe oben Teil 2, III.

[46] Siehe nur BGHSt 16, 1 ff. sowie oben ausführlich Teil 2, I.C.1.b).

[47] Siehe oben Teil 2, III.D.

ven Komponente bezieht. Zu dieser Fallgruppe zählen etwa die Tathandlungen des Herstellens, Sichverschaffens, Verwahrens und Einführens. In der Fallgruppe des „bewussten Kontrollverlusts über gefährliche Gegenstände“[48] können aufgrund des vergleichsweise höheren Risikos geringere Anforderungen an die Absicht gestellt werden. In diese Fallgruppe gehören die Tathandlungen des Verkaufens und Feilhaltens, Vermietens, einem anderen Verschaffens oder Überlassens sowie des Zugänglichmachens und Verbreitens.[49]

In der Fallgruppe der „gefährlichen Gegenstände im eigenen Kontrollbereich“ sollte Absicht als dolus directus 1. oder 2. Grades verstanden werden. Solange der Vorfeldtäter die alleinige Kontrolle über das Computerprogramm ausübt, kommt auch nur er selbst als Zieltäter in Betracht. Bei lebensnaher Betrachtung wird er in solchen Konstellationen also stets entweder zielgerichtet wollen oder sicher wissen, dass das Computerprogramm zur Begehung von Zieltaten verwendet werden wird. Für dolus-eventualis-Konstellationen bleibt hier wenig Raum: Solange jemand ein deliktsgeeignetes Computerprogramm unter alleiniger Kontrolle hält und dabei nur ernstlich für möglich hält, dass das Computerprogramm später zu Straftaten eingesetzt wird, kann daraus nicht geschlossen werden, dass er sich selbst als Vortäter versteht und sich in ein deliktisches Gesamtgeschehen integrieren will. Dies ist jedenfalls nicht die einzig plausible Interpretation, weshalb hier bei bloßem dolus eventualis ein „eindeutig deliktischer Sinnbezug“ fehlt.

In der Fallgruppe des „bewussten Kontrollverlusts über gefährliche Gegenstände“ stellt sich dies etwas anders dar, da hier als Zieltäter vielmehr Dritte in Betracht kommen. Es ist deshalb nicht durchgehend zu erwarten, dass ein krimineller Vorfeldtäter sicheres Wissen hinsichtlich der Begehung einer Zieltat hat, denn er muss nicht zwingend in die Pläne seiner „Kunden“ eingeweiht sein. Auch zielgerichtetes Wollen hinsichtlich der Begehung einer Zieltat wird regelmäßig dann nicht vorliegen, wenn ein krimineller Vorfeldtäter maßgeblich aus wirtschaftlichen Interessen handelt. Auch wenn ein Vorfeldtäter also einen „eindeutig deliktischen Sinnbezug“ setzt, äußert sich dies nicht zwingend in einem dolus directus.

So werden etwa Steuerungseinheiten für Botnets vielfach vermietet und auf Stundenbasis abgerechnet. Wozu der Zieltäter ein Botnet letztlich einsetzt, dürfte dem Vorfeldtäter hier gleichgültig sein. Dolus directus ist dann zu eng. Der sozialethische Unwert dieser Handlungen liegt darin, dass es sich dem Vorfeldtäter geradezu aufdrängt, dass sein Abnehmer deliktische Ziele verfolgt und dennoch überlässt der Vorfeldtäter ihm die Kontrolle über das entsprechende Werkzeug. Der Vorfeldtäter wird regelmäßig die Einzelheiten der Zieltaten nicht kennen, noch sich

---

[48] Siehe oben Teil 2, III.C.

[49] Auch wenn zivilrechtlich mit dem Verkaufen, Vermieten und Feilhalten noch kein Besitzwechsel einhergeht, sind diese Handlungen doch auf die Einräumung der tatsächlichen Verfügungsgewalt über das Computerprogramm ausgerichtet, was ihre Einordnung in die Fallgruppe des bewussten Kontrollverlusts rechtfertigt.

besonders dafür interessieren. Gegebenenfalls hat er eine abstrakte Vorstellung von den Zieltaten.

Eine solche innere Disposition wird gerade durch dolus eventualis hinsichtlich der Verwendung des Computerprogramms zur Begehung von Zieltaten ausgedrückt. Der Täter hält es ernstlich für möglich, dass sein Computerprogramm zu Straftaten verwendet wird, und findet sich damit ab. So ist ein „eindeutig deliktischer Sinnbezug" schon dann zu bejahen, wenn in dieser Fallgruppe der Täter mit dolus eventualis handelt.

In Randbereichen kann dies freilich dazu führen, dass auch ein IT-Sicherheitsbeauftragter in den Bereich strafrechtlicher Haftung gerät, wenn er einen *Proof of Concept* führt und anderen zugänglich macht: Solange die nachgewiesene Sicherheitslücke nicht behoben ist, muss auch er ernstlich für möglich halten, dass sein *Proof of Concept* zur Begehung von Straftaten verwendet wird. Dieses Verhalten entspricht aber dem in der IT-Sicherheitsbranche verbreiteten *Full-Disclosure-Prinzip*: Eine entdeckte Schwachstelle soll umfassend *(full)* bekanntgemacht *(disclosure)* werden, damit so der Zeitdruck auf denjenigen steigt, in dessen Macht es steht, die Schwachstelle – etwa durch ein Update des angreifbaren Programms – zu beheben. Dass der IT-Sicherheitsbeauftragte mittelbar IT-Angriffe verhindern möchte, nimmt seinem Verhalten jedoch nicht den unmittelbaren deliktischen Sinnbezug. Möchte man solche Verhaltensweisen nach dem *Full-Disclosure-Prinzip* nicht unter Strafe stellen, muss man für diese Konstellationen eine Freistellungsklausel[50] normieren.

Diese Normierung einer Verwendungsabsicht greift eigentlich die Idee der Catch-all-Klauseln des Kriegswaffen- und Exportkontrollstrafrechts[51] auf, präzisiert und beschränkt diese jedoch. In den Catch-all-Klauseln ist die Täterintention konstituierend für die Strafandrohung (der Täter weiß, zu welchem Zweck die Gegenstände eingesetzt werden sollen), und während jeder beliebige Gegenstand taugliches Tatobjekt ist, muss das tatbestandliche Geschehen insgesamt geeignet sein, die geschützten Rechtsgüter zu gefährden. Nach dem hiesigen Vorschlag ergibt sich jedoch diese „Eignung zur Gefährdung der Rechtsgüter" aus dem Tatobjekt, denn hier muss das Computerprogramm deliktsgeeignet sein.

Damit zeigt sich, dass die Normierung einer Verwendungsabsicht ein hohes Maß an Rechtsklarheit schafft. Versteht man unter Absicht dolus directus, solange das Tatobjekt sich im Kontrollbereich des Vorfeldtäters befindet, und dolus eventualis, sobald er die Kontrolle einem Dritten einräumt, so erfasst der Straftatbestand zuverlässig nur solche Konstellationen, in denen ein „eindeutig deliktischer Sinnbezug" des Vorfeldtäters gegeben ist. Deshalb sichert die Normierung einer Verwendungsabsicht auch eine vergleichsweise hohe Legitimität.

---

[50] Siehe dazu unten 4.

[51] Siehe oben Teil 3, III.C.

b) Abzulehnen: Die Begehungsabsicht

Das Regelungsmodell, welches voraussetzt, dass der Vorfeldtäter *zum Zweck der Begehung einer Zieltat* handelt, deckt sich inhaltlich weitgehend mit dem oben favorisierten Modell der Verwendungsabsicht.[52] Mit Blick auf *Rechtsklarheit* ist gegen diese Regelungstechnik wenig einzuwenden, jedoch wäre auch hier ratsam, in den Gesetzesmaterialien zu klären, welche Vorsatzform unter dem verfolgten Zweck zu verstehen ist. Insbesondere sollte deutlich gemacht werden, ob dieses Merkmal Absicht im Sinne eines dolus directus 1. oder 2. Grades erfordert.

Letztlich wird hier jedoch das Modell der Verwendungsabsicht dem Modell der Begehungsabsicht vorgezogen, weil die Verwendungsabsicht noch mehr Rechtsklarheit schafft. Sie lässt nämlich einen deutlicheren Zusammenhang zu dem tatgegenständlichen Computerprogramm erkennen und schafft somit einen gewissen Parallellauf des objektiven und subjektiven Tatbestands: Das Computerprogramm kann objektiv zur Begehung von Straftaten verwendet werden, deshalb soll es unter Strafe stehen, wenn der Vorfeldtäter subjektiv beabsichtigt, dass es entsprechend verwendet werde.

c) Abzulehnen: Das Vorbereitungsmodell

Das „Vorbereitungsmodell" ist wegen seiner schwächeren Legitimität, vor allem aber wegen seiner gravierenden Rechtsunklarheit abzulehnen. In diesem Modell wird das *Vorbereiten* einer Zieltat im Wortlaut geführt und überwiegend als subjektives Tatbestandsmerkmal ausgelegt.[53]

aa) Bewertung am Maßstab der Rechtsklarheit

Nach dem Maßstab der Rechtsklarheit ist das „Vorbereitungsmodell" abzulehnen. Es verursacht massive Rechtsunsicherheit, weil es in seiner inhaltlichen Bedeutung und Reichweite völlig unklar ist. Dies ist freilich kein Problem der *Effektivität*. Zwar beschränkt das subjektive Vorbereitungsmerkmal wohl den objektiven Tatbestand des Vorfelddelikts, entzieht diesem jedoch nicht den Anwendungsbereich. Das „Vorbereitungsmodell" hat aber ein Problem der *Effizienz*, da

---

[52] Das Regelungsmodell der Verwendungsabsicht findet sich *de lege lata* in keinem Software-Delikt, jedoch wird es in Art. 7 des Vorschlags der EU-Kommission für eine Richtlinie über Angriffe auf Informationssysteme, KOM(2010) 517 endgültig, eingesetzt. Siehe im Einzelnen oben Teil 3, II.C.2.

[53] Das Vorbereitungsmodell wird eingesetzt in §149 Abs. 1 StGB, § 202c Abs. 1 Nr. 2 StGB, § 263a Abs. 3 StGB und § 22b Abs. 1 Nr. 3 StVG. Internationale Vorläufer dieses Modells gibt es nicht. In diesem Modell wird bestraft, „wer eine [Zieltat] vorbereitet, indem er …". Siehe im Einzelnen dazu oben Teil 3, I.C.1.

Inhalt, Bedeutung und Reichweite aus dem Tatbestand nicht unmittelbar ersichtlich sind.

Die Indem-Konstruktion („wer … vorbereitet, indem er …“) legt eigentlich nahe, dass das Vorbereiten-Merkmal überhaupt keine eigenständige objektive oder subjektive Bedeutung haben soll.[54] Im Wege historischer und möglichst sinnstiftender Auslegung wurde aber das Ergebnis gefunden, dass dem Merkmal eine eigenständige subjektive Bedeutung beizumessen ist: Der Täter muss mindestens dolus eventualis dahingehend haben, dass er mit seiner Handlung die Begehung einer Zieltat vorbereitet, also begünstigt oder irgendwie fördert.[55] Diese Auslegung konnte wiederum nur durch Rückgriff auf die Gesetzesmaterialien[56] gefunden werden, nach denen der Gesetzgeber durch die Vorbereitungsdelikte eine „Strafbarkeitslücke“[57] schließen wollte, nämlich Fälle *versuchter* Beihilfe.[58]

Die Gesetzesmaterialien stiften nun aber ihrerseits Verwirrung: Obwohl der Gesetzgeber die Parallele zum Versuch ausdrücklich zieht und damit konsequenterweise einen „Tatentschluss zu einer Beihilfe“ normieren müsste, will er augenscheinlich keinen doppelten Gehilfenvorsatz[59] beim Vorbereitungstäter voraussetzen. Dieser doppelte Vorsatz müsste sich beim Vorbereitungstäter nicht nur auf das Fördern einer fremden Tat, sondern zusätzlich auf die vorsätzliche rechtswidrige Haupttat selbst beziehen.[60] Der Gesetzgeber verlangt dem Vorbereitungstäter dagegen keinen Vorsatz hinsichtlich der Begehung einer Zieltat ab, sondern hier soll ein In-Aussicht-Nehmen genügen.

Freilich könnte der Gesetzgeber eine effiziente und verständliche Lösung konstruieren. Hierfür müsste das Vorbereitungsdelikt von der Beihilfe-Strafbarkeit nur dahingehend abweichen, dass eine Bestrafung unabhängig davon möglich ist, ob objektiv ein Zieldelikt verwirklicht wird. Dafür wäre es folglich nicht erforderlich, den Vorsatz des Vorbereitungstäters hinsichtlich der Begehung und Vollendung der Zieltat vollends zu streichen. Vielmehr liegt es nahe, die subjektive Seite im We-

---

[54] Siehe oben Teil 3, C.1.a)aa).

[55] Siehe oben Teil 3, C.1.a).

[56] Versuchte Beteiligung ist im AT nur bei versuchter Anstiftung zu Verbrechen strafbar, § 30 Abs. 1 Satz 1 StGB. Die „versuchte Beihilfe“ in den Vorbereitungsdelikten bezieht sich auch auf *Vergehen*.

[57] Der Begriff „Strafbarkeitslücke“ legt nahe, dass es hier etwas zu schließen gäbe, vgl. etwa *Kauder*, ZRP 2009, 20. Da das Strafrecht aber wegen seines Ultima-Ratio-Charakters per se lückenhaft ist und sein muss, wird hier der Begriff der Strafbarkeitslücke in Anführungszeichen gesetzt, vgl. exemplarisch zum fragmentarischen Vermögensschutz durch Strafrecht *Sieber*, Computerkriminalität und Strafrecht, S. 338 f.; siehe auch *Hefendehl*, JA 2011, 401 ff.

[58] BT-Drucks. 16/3656, S. 12 linke Spalte.

[59] Siehe nur Schönke/Schröder-*Heine*, § 27 Rn. 19; MüKo-*Joecks*, § 27 Rn. 74.

[60] Vgl. MüKo-*Joecks*, § 27 Rn. 82; *Roxin*, AT II, S. 224 f.; LK-*Schünemann*, Vor § 26 Rn. 19 ff.

sentlichen unverändert zu lassen. Doch wären auch leichte Abstriche bei den Anforderungen des Vorsatzes denkbar: Für den Grad der Konkretisierung hat der Gesetzgeber jedenfalls bei Schaffung des § 89a StGB festgehalten, dass das vorbereitete Delikt nicht so stark konkretisiert sein müsse wie die vorsätzliche rechtswidrige Haupttat bei der versuchten Anstiftung nach § 30 Abs. 2 StGB.[61] Es ist auch denkbar, die Anforderungen an die Konkretisierung der geförderten Tat in den Vorbereitungsdelikten im Vergleich zur Beihilfe nochmals zu senken, sodass sich ein Stufenverhältnis vom Tätervorsatz über den Anstiftervorsatz und den Gehilfenvorsatz zum Vorbereitervorsatz ergibt.

Ob dies jedoch gemeint ist, wenn der Gesetzgeber davon spricht, dass der Vorbereitungstäter eine Zieltat „in Aussicht nehmen" müsse,[62] ist ungewiss. Mit dieser Wendung wurde ein Begriff eingeführt, der in der Vorsatzterminologie bislang unbekannt war und deshalb als Auslegungshilfe kaum taugt. Der Gesetzgeber hätte hier einfach auf bewährte Fachtermini zurückgreifen können und hätte damit mehr Rechtsklarheit geschaffen.

bb) Bewertung am Maßstab der Legitimität

Das „Vorbereitungsmodell" stellt zudem einen misslungenen Versuch des Gesetzgebers dar, einen „eindeutig deliktischen Sinnbezug" in den Vorfelddelikten festzuschreiben. Zwar ist offenkundig, dass der Gesetzgeber bei der tatbestandlichen Normierung des „Vorbereitens" die Dual-Use-Problematik im Blick hatte: dieses Regelungsmodell war gerade dazu gedacht, sachlich angemessen zwischen legitimem und strafbarem Vorfeldverhalten zu differenzieren. Das Vorbereiten ist hierfür jedoch kein geeignetes Kriterium.

Sofern man „Vorbereiten" als *Schaffen einer günstigeren Ausgangslage* versteht, ist dies nicht die Stellschraube zur angemessenen Behandlung der Dual-Use-Problematik. Ein Vorfeldtäter und ein IT-Sicherheitsbeauftragter schaffen gleichermaßen günstigere Ausgangslagen für die Begehung einer Zieltat, wenn sie ein *Exploit* programmieren. Ebensowenig unterscheiden sie sich beim Vorbereiten im Maß der Konkretisierung oder dem Grad des Vorsatzes. Deshalb gibt es für das „Vorbereiten" in diesem Sinne stets eine plausible rechtmäßige Alternativerklärung. Die wirkliche Stellschraube, durch die ein „eindeutig deliktischer Sinnbezug" normiert werden kann, ist nämlich der Vorsatz des Vorbereitungstäters hinsichtlich der Begehung und Vollendung der Zieltat oder der Verwendung des Computerprogramms zur Begehung und Vollendung der Zieltat. Nur ein solcher Vorsatz kann nicht plausibel als rechtmäßig erklärt werden.

---

[61] BT-Drucks. 16/12428, S. 14 rechte Spalte; dies liegt allerdings schon deshalb nahe, da ja bereits bei der („vollendeten") Beihilfe die Konkretisierung weniger stark ist als bei der Anstiftung.

[62] BT-Drucks. 16/3656, S. 19 linke Spalte.

Zusammenfassend fehlt es dem „Vorbereitungsmodell“ also schon an Rechtsklarheit, weil der Gesetzgeber auf ungewohnte Termini zurückgreift, diese in den Gesetzesmaterialien missverständlich erläutert und in der konkreten grammatischen Tatbestandskonstruktion verschleiert, dass er dem Vorbereiten-Merkmal überhaupt inhaltliche Bedeutung beimisst. Am legitimierenden „eindeutig deliktischen Sinnbezug“ fehlt es in diesem Regelungsmodell, weil das *Schaffen einer günstigeren Ausgangslage* faktisch nicht das Unterscheidungskriterium zwischen kriminellem Vorfeldtäter und legitim handelndem IT-Sicherheitsbeauftragten darstellt.

d) Abzulehnen: Der Verzicht auf einen subjektiven Bezug (Anschließungsdelikte)

Anschließungsdelikte verzichten vollends auf einen subjektiven Bezug des Vorfeldtäters zur Zieltat, sodass gerade nicht erforderlich ist, dass er in der Absicht, dem Wissen oder einer irgendwie gearteten Intention hinsichtlich einer kriminellen Verwendung des Computerprogramms handelt.[63] Dieses Regelungsmodell ist abzulehnen, weil es nur scheinbar Rechtsklarheit schafft und nicht in der Lage ist, einen „eindeutig deliktischen Sinnbezug“ herzustellen.

aa) Bewertung am Maßstab der Rechtsklarheit

Mangelnde *Effektivität* kann man Anschließungsdelikten nicht nachsagen, schließlich lassen sie den weiten objektiven Tatbestand unberührt, statt ihn zu begrenzen. Auch die *Verständlichkeit* kann nicht grundsätzlich kritisiert werden, da der Verzicht auf ein subjektives Merkmal den Tatbestand nicht weniger verständlich macht. Bedenken bestehen jedoch hinsichtlich der *Effizienz* der Anschließungsdelikte. Ihr Tatbestand ist wegen der fehlenden Unterscheidung von sozialnützlichem und sozialschädlichem Verhalten unbillig weit, muss deshalb in vielen Einzelfällen reduziert werden und erfordert somit einen vermeidbaren Auslegungsaufwand.

Anschließungsdelikte schaffen nämlich eine unbedingte und unabwendbare strafrechtliche Haftung für *potentielle* Gefahren.[64] Deshalb erfassen sie in großem

---

[63] Anschließungsdelikte werden in § 4 ZKDSG und § 108b UrhG eingesetzt, also im Vorfeld der unerlaubten Nutzung eines zugangskontrollierten Dienstes (§§ 1, 3 ZKDSG) und des Eingriffs in den technischen Schutz von Werken (§ 108b Abs. 1 UrhG). Die Regelungstechnik findet sich auch in Art. 4 der EG-Richtlinie 98/84/EG (Conditional Access) und in Art. 6 der EG-Richtlinie 2001/29/EG (Urheberrecht), wobei in diesen Richtlinien freilich keine Delikte normiert sind. Siehe im Einzelnen oben Teil 3, I.C.2 sowie II.C.3.

[64] Der Begriff der *potentiellen* Gefahr ist hier bewusst gewählt: eine Gefahr besteht, wenn ein Schaden möglich ist. Eine *potentielle* Gefahr besteht, wenn ein Schaden erst *unter zusätzlichen Umständen* möglich wird. Das Sichverschaffen eines deliktsgeeigneten Computerprogramms ist ungefährlich, solange keine deliktische Intention des Handelnden

Umfang das Verhalten von IT-Sicherheitsbeauftragten. Kennzeichnend für deren Handeln ist der sichere und kunstgerechte Umgang mit gefährlichen Computerprogrammen ohne deliktische Intentionen.[65] Da in diesen Fällen Anschließungsdelikte jedoch grundsätzlich greifen, muss ihr Tatbestand hier stets teleologisch reduziert werden. Dann geht die Strafbarkeitsgrenze nicht mehr aus dem Gesetzeswortlaut hervor.

Deshalb schaffen Anschließungsdelikte nur eine scheinbare Rechtsklarheit. Zugleich resultiert aus dieser „vorläufigen Überkriminalisierung" ein massives Legitimitätsproblem.

bb) Bewertung am Maßstab der Legitimität

Die Anschließungsdelikte leiden vor allem an einem erheblichen Mangel an Legitimität. Dies liegt daran, dass der „eindeutig deliktische Sinnbezug" nicht im subjektiven Tatbestand normiert wird.

Bei Anschließungsdelikten kann sich der „eindeutig deliktische Sinnbezug" nur aus dem objektiven Tatbestand ergeben. Hierfür müsste der objektive Tatbestand ein Verhalten des Täters umschreiben, das unter allen Umständen für jedermann und ohne weitere Bedingungen sozialethisch vorwerfbares Unrecht darstellt – denn andernfalls wäre das Gesamtgeschehen alternativ als rechtmäßig zu interpretieren. Denkbar wäre dies allenfalls in unkontrollierbaren Gefahrensituationen, die solch massive Schäden befürchten lassen, dass schon die Unterhaltung der Gefahrensituation schlechterdings unerträglich ist.[66]

Nun hat aber obige Fallgruppenbildung gezeigt, dass ein wesentlicher Teil der Tathandlungen sich gerade dadurch auszeichnet, dass der Vorfeldtäter das Computerprogramm (noch) unter alleiniger und voller Kontrolle behält. Jemand, der ohne deliktische Absicht ein tatbestandsmäßiges Computerprogramm herstellt,[67] schafft dadurch zwar eine (überschaubare) Gefahr für das Rechtsgut,[68] jedoch liegt deshalb nicht zugleich ein „deliktischer Sinnbezug" vor – selbst wenn das Computerprogramm noch so gefährlich oder schädlich ist. Denn dieser „deliktische Sinnbezug" setzt gerade voraus, dass der Handelnde sich als Täter begreift, dass er sich in ein kriminelles Gesamtgeschehen integrieren will. Dies kann aber nicht allein daraus geschlossen werden, dass er mit einem gefährlichen Computerprogramm hantiert,

---

oder ein Kontrollverlust hinzukommen. Erst wenn diese vorliegen, könnte man von einer Gefahr sprechen. Dies ist in Anschließungsdelikten jedoch regelmäßig nicht normiert.

[65] Siehe oben Teil 1, I.B.

[66] Siehe nur *Sieber*, NStZ 2009, 359; *Wohlers*, Deliktstypen, S. 296 ff.

[67] Beispielsweise im Falle des § 95a Abs. 3 Nr. 1 UrhG, wenn der Täter ein Computerprogramm herstellt, das schon vor seiner Fertigstellung als Umgehungsvorrichtung beworben wird.

[68] Vgl. oben 1.a)bb).

da dies auch für IT-Sicherheitsbeauftragte typisch ist. Es gibt also eine plausible rechtmäßige Alternativerklärung für solches Verhalten. Dies gilt freilich umso mehr, wenn noch nicht einmal die Deliktseignung des Computerprogramms normiert ist.[69] Folglich fehlt es den Anschließungsdelikten jedenfalls in dieser Fallgruppe an einem „eindeutig deliktischen Sinnbezug" und damit auch an Legitimität.

Dieser Befund wird bestätigt, wenn man die Fallgruppen, in denen der Vorfeldtäter sein Anschließungsdelikt im Vorfeld eines *fremden* Zieldelikts verwirklicht,[70] den Kategorien des Allgemeinen Teils zuordnet: Der Gesetzgeber schafft hier eine Art „nichtakzessorische Beihilfe".[71] Eine solche Ausdehnung der Teilnahmestrafbarkeit wird gemeinhin abgelehnt,[72] vorwiegend aber mit einem spezifisch beihilferechtlichen Argument: Es lasse sich nicht rechtfertigen, dass die Strafe des Gehilfen sich nach der Strafdrohung für den Täter richtet, § 27 Abs. 2 Satz 1 StGB, wenn die Bestrafung des Gehilfen gar nicht von der Tat eines anderen abhängt, es also möglicherweise gar keinen Täter gibt. Dieses Argument ließe sich hier relativieren, da sich die Strafe des Vorfeldtäters in den Anschließungsdelikten nicht nach der Strafandrohung der Zieldelikte richtet. Mit dem Schlagwort der Akzessorietät der Beihilfe wird jedoch nicht nur ein Bestrafungszusammenhang zwischen Haupttäter und Teilnehmer ausgedrückt, sondern vorgeschaltet ein Unrechtszusammenhang. Beihilfe ist Teilnahme an fremdem Unrecht. Bei Anschließungsdelikten, die per Definition an kein fremdes Unrecht gekoppelt sind, fragt sich, worin eigentlich das spezifische Unrecht bestehen soll, wenn noch nicht einmal eine abstrakte Gefährdung eines Rechtsguts eingetreten ist.

Ob der Gesetzgeber diese Entscheidung jeweils bewusst getroffen hat, ist freilich ungewiss. Die Gesetzesmaterialien zum ZKDSG enthalten nur den pauschalen Verweis auf die Gefahren durch die einfache Verbreitung von Hacker-Werkzeugen und die niedrigen Hemmschwellen der späteren Verwender zum Einsatz dieser Programme. Sodann wird konzediert, dass es sich in der Regel zwar um Vorbereitungshandlungen zu anderen Straftaten („§ 265a oder § 202a StGB") handelt, allerdings stehe „dem Charakter der bloßen Vorbereitungshandlung" der „gewerbsmäßige Charakter der Taten" gegenüber.[73] Auch die Gesetzesbegründung zu den Tatbeständen des UrhG schweigt sich zu Einzelheiten aus; spricht zwar von einem umfassenden Verbot und der Notwendigkeit einer (teilweisen) Strafbewehrung dieses Verbots, sieht aber in der Beschränkung auf gewerbsmäßiges Handeln eine erhebliche – und damit wohl ausreichende – Strafbarkeitsbegrenzung. Im Übrigen wird darin auf die Materialien zum ZKDSG verwiesen.[74] Damit wird erkennbar,

---

69 Siehe insbesondere oben Teil 3, I.B.3., 4., 6.

70 Siehe oben Teil 2, III.A.

71 Siehe oben Teil 3, I.C.2.a)bb).

72 Siehe dazu statt aller *Roxin*, AT II, S. 131 f.

73 BT-Drucks. 14/7229, S. 8 linke und rechte Spalte.

74 BT-Drucks. 15/38, S. 28 rechte Spalte.

was der Gesetzgeber bei Schaffung dieser Tatbestände offenbar vor Augen hatte: Er wollte organisierte Schwarzhändler und Hersteller von Umgehungsvorrichtungen erfassen, die durch ihre Produkte nicht nur technische Schutz- und Verschlüsselungsmaßnahmen leerlaufen lassen können, sondern dies auch noch kaufmännisch organisieren und daraus beträchtliche Gewinne erzielen. Gegen dieses gesetzgeberische Ziel ist nichts einzuwenden, nur hätte es zu seiner Umsetzung keiner Anschließungsdelikte bedurft, die eine „nichtakzessorische Beihilfestrafbarkeit" einführen.

Diese erweist sich als vergleichsweise illegitim, da den Anschließungsdelikten insbesondere wegen des Mehrzweckaspekts des Dual-Use-Phänomens immer ein „*eindeutig* deliktischer Sinnbezug" fehlt.[75] Das gesetzgeberische Ziel einer effektiven Abschreckung[76] lässt sich durch eine solche Überkriminalisierung jedenfalls nicht erreichen.

e) Zusammenfassung: Regelung der subjektiven Tatseite

Es hat sich gezeigt, dass das Vorsatzmodell des „Handelns in Verwendungsabsicht" vorzugswürdig ist, weil es – insbesondere in Kombination mit dem objektiven „Eignungsmodell" – ein hohes Maß an Rechtsklarheit wahrt und dabei verlässlich einen „eindeutig deliktischen Sinnbezug" herstellt. Nach diesem Wertmaßstab ist nur das Modell der Begehungsabsicht ebenbürtig, das aber den Parallellauf von objektivem und subjektivem Tatbestand weniger stark kennzeichnet. Dagegen erhält das Verzichtsmodell der Anschließungsdelikte den Nachzug, da dieses bei Software-Delikten keinen „eindeutig deliktischen Sinnbezug" herstellt. Abzulehnen ist insbesondere auch das Vorbereitungsmodell, da es massive Rechtsunsicherheit verursacht und überdies durch die Wahl einer falschen Stellschraube ebenfalls keinen „eindeutig deliktischen Sinnbezug" herstellt.

3. Feinjustierung durch Genehmigungsvorbehalt?

Im Kriegswaffen- und Exportkontrollrecht liegt das vielleicht wichtigste Instrument zur Steuerung der Strafbarkeit im Genehmigungsvorbehalt. Weder die objektiven Merkmale noch die subjektive Tatseite lösen dort die Strafbarkeit alleine aus. Vielmehr verursachen sie zunächst nur eine Genehmigungspflicht, die den Ausführer oder Hersteller von Kriegswaffen faktisch dazu verpflichtet, verwaltungsrecht-

---

[75] Auch hier ist obiger Hinweis (Fn. 887) angebracht, dass diese Ausführungen möglicherweise nicht mehr gelten, wenn der Umgang mit anderen Gegenständen als Computerprogrammen unter Strafe gestellt werden soll. So kann es etwa legitim sein, Anschließungsdelikte zu normieren, um jeglichen Umgang mit fremden Kreditkartendatensätzen, Login-Daten oder Passwörtern unter Strafe zu stellen. Hier kann sich der „eindeutig deliktische Sinnbezug" sehr wohl allein aus dem Tatobjekt ergeben.

[76] Vgl. BT-Drucks. 14/7229, S. 8 rechte Spalte.

lich überprüfen zu lassen, ob sein Vorhaben mit den Regulierungszielen vereinbar ist. Erst die Verletzung dieser Genehmigungspflicht löst die Strafbarkeit aus. Freilich ist es weiterhin denkbar, dass sich ein Ausführer in dem Glauben, keiner Genehmigung zu bedürfen, unversehens strafbar macht. Allerdings kann er im Zweifel stets bei der zuständigen Behörde oder einem Verwaltungsgericht feststellen lassen, dass sein Vorhaben keiner Genehmigung bedarf. Durch diese verwaltungsrechtliche Vorabkontrolle können die *Chilling Effects* vermieden werden, die bei unmittelbarer Kriminalisierung drohen würden.

Im Software-Strafrecht erscheint aber ein solcher Genehmigungsvorbehalt schon deshalb zweifelhaft, weil es dem Computerstrafrecht insgesamt an einer vergleichbaren verwaltungsrechtlichen Unterfütterung fehlt. Diese wäre aber notwendig, wollte man in diesem Ausmaß Entscheidungsverantwortung auf die Verwaltung übertragen.[77] Zudem dürfte der Genehmigungsvorbehalt hier wenig praktikabel sein. Einerseits würde er angesichts der schieren Anzahl neu entstehender Computerprogramme, die häufig für ganz konkrete Einzelziele maßgeschneidert und laufend angepasst werden, einen massiven administrativen Aufwand bedeuten. Diesen könnte man zwar einerseits minimieren, indem man eine generelle Genehmigung unter bestimmten Voraussetzungen erteilt, etwa durch einen „Waffenschein für Schadsoftware“,[78] andererseits ist eine solche Regelungstechnik umso überflüssiger, je mehr Rechtsklarheit und Rechtssicherheit auch im Einzelfall durch einen herkömmlichen Straftatbestand geschaffen werden kann.

4. Freistellungsklauseln

Freistellungsklauseln sind im Software-Strafrecht aufgrund des oben vorgeschlagenen Regelungsmodells weitgehend überflüssig (siehe b)). Allein für Fälle, in denen IT-Sicherheitsbeauftragte nach dem *Full-Disclosure-Prinzip* Schwachstellen nachweisen und veröffentlichen, erscheint es ratsam, eine Ausschlussklausel zu verwenden, die auf die mittelbaren subjektiven Ziele der konkret handelnden Person abstellt (sogleich a)).

a) Vorzugswürdige Freistellungsklauseln: handlungs- und zielbezogen

Unter dem Mehrzweckaspekt der Dual-Use-Problematik ist vor allem die Klausel aus dem Kriegswaffenkontrollrecht interessant, welche für Handlungen gilt, die dem *Schutz* vor Atomwaffen selbst[79] oder deren Wirkungen dienen. Denn diese

---

[77] *Jaeckel*, JZ 2011, 121.

[78] Vgl. §§ 7, 35 WaffG, siehe hierzu auch *Hefendehl*, Kollektive Rechtsgüter, S. 145 f.

[79] Respektive chemischen Waffen, siehe oben B.4.

Freistellungsklausel zielt gleichermaßen darauf ab, *Chilling Effects* bei denjenigen zu vermeiden, die zum Schutz der Rechtsgüter mitunter tatbestandsmäßig handeln (müssen).

Relevant ist eine solche Klausel im Software-Strafrecht namentlich in den Tatvarianten, in denen dolus eventualis hinsichtlich einer kriminellen Verwendung des Computerprogramms ausreichen soll.[80] Unter Umständen kann nämlich auch bei einem IT-Sicherheitsbeauftragten, der einen *Zero-Day-Exploit* veröffentlicht oder zumindest einem bestimmten Personenkreis zur Verfügung stellt, dolus eventualis dahingehend angenommen werden, dass ein Dritter diesen *Exploit* zur Begehung von Straftaten verwendet, solange die entsprechende Sicherheitslücke noch nicht geschlossen ist. Denn auch wenn sich dies aus Sicht des IT-Sicherheitsbeauftragten als Missbrauch des Computerprogramms darstellt, ist es doch ernstlich möglich. Und auch wenn eine solche Verwendung dem IT-Sicherheitsbeauftragten eigentlich unerwünscht ist, findet er sich doch damit ab. Darin besteht schließlich der Wert des *Full-Disclosure-Prinzips*: Durch die Weitergabe des *Zero-Day-Exploits* wird die Sicherheitslücke bekannter und die Wahrscheinlichkeit entsprechender Angriffe steigt kurzfristig. Gleichzeitig steigt der Druck auf denjenigen, der die konkrete Sicherheitslücke nun kennt und schließen kann. Sobald er dies tut, ist die Gefahr dauerhaft gebannt. Damit handelt es sich um eine typische Erscheinungsform von dolus eventualis.

Da dieses Vorgehen jedoch berufstypisch ist,[81] bliebe jedenfalls den Gerichten die Möglichkeit, solches Verhalten im Wege der richterrechtlichen Figur der strafrechtlichen Neutralisierung berufstypischen Verhaltens straflos zu stellen. Nimmt der Vorfeldtäter eine berufstypische oder berufsadäquate Handlung vor und hat er dabei dolus eventualis hinsichtlich der Begehung einer Zieltat, so wird diese Handlung neutralisiert und der Vorfeldtäter nicht bestraft (was jedoch nicht gelten soll, wenn der Vorfeldtäter einem erkennbar Tatgeneigten zur Hand geht).[82]

Diese Rechtsprechung wurde in Beihilfekonstellationen entwickelt und lässt sich möglicherweise auf IT-Sicherheitsbeauftragte in Vorbereitungskonstellationen übertragen. Jedoch ist zu befürchten, dass allein durch diese Abhängigkeit der IT-Sicherheitsbeauftragten von einem Richter im Einzelfall schon im Voraus Unsicherheit entsteht. Auch ist nicht garantiert, dass die Staatsanwaltschaft dieselbe rechtliche Würdigung vornimmt, und für ein IT-Sicherheitsunternehmen kann schon ein staatsanwaltschaftliches Ermittlungsverfahren eine erhebliche Belastung darstellen. Für diese Konstellation drängt sich daher eine Freistellungsklausel auf.

---

[80] Siehe oben I.C.2.a).

[81] Siehe heise Security vom 6.7.2010, „Microsoft-Lücken: mal Full Disclosure, mal Null Disclosure“, online abrufbar unter http://heise.de/-1033462 [zuletzt abgerufen am 16.11.2014].

[82] BGH NStZ 2000, 34; *Rackow*, Neutrale Handlungen, S. 71 ff.

Der Nachteil mag darin liegen, dass sich auch kriminelle Vorfeldtäter auf die Klausel berufen könnten, sodass es dem Richter im Einzelfall obliegt, Schutzbehauptungen als solche zu entlarven. Es erscheint jedoch insgesamt vorzugswürdig, eine entsprechende Freistellungsklausel einzurichten und den Richter mit der Entlarvung von Schutzbehauptungen zu betrauen, als auf eine solche Klausel zu verzichten und die gesamte IT-Sicherheitsbranche darauf zu verweisen, dass die richterrechtliche Neutralisierung berufstypischer Handlungen auch schon im Ermittlungsverfahren berücksichtig würde.

Bei der Normierung könnte man etwa an den Wortlaut des § 20 Abs. 4 Nr. 2 KWKG anknüpfen: „[Dies] gilt nicht für eine Handlung, die zum Schutz gegen Wirkungen von Computerprogrammen i.S.d. Abs. 1 oder zur Abwehr dieser Wirkungen geeignet ist und vorgenommen wird."

b) Abzulehnende Freistellungsklauseln

Zunächst ist die Ausschlussklausel des Art. 6 Abs. 2 CCC abzulehnen, die besagt, dass der Tatbestand „nicht so ausgelegt werden [dürfe], als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen [die Tathandlung] nicht zum Zweck der Begehung [einer Zieltat], sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt".[83] Abzulehnen ist diese Klausel wegen ihrer unklaren Rechtsnatur und der daraus entstehenden Unsicherheit über Inhalt und Weite der Regelung: Dem Wortlaut nach handelt es sich hierbei um eine Auslegungsregel, die an bestimmte *Tathandlungen* anknüpft. Im Explanatory Report werden jedoch zwei andere Aspekte angesprochen: Dort wird gesagt, dass bestimmte *Tatmittel (tools)* nicht von der Vorschrift erfasst würden, wobei im Grunde lediglich der Umkehrschluss aus Art. 6 Abs. 1 CCC gezogen wird.[84] Es wäre also inkonsequent, diesen Regelungsinhalt auch der Ausschlussklausel in Abs. 2 beizumessen. Unmittelbar anschließend findet sich im Explanatory Report der Hinweis, dass dieser Haftungsausschluss aber schon aus dem Merkmal „unbefugt" *(without right)* folge.[85] Wenn dies zuträfe, wäre Abs. 2 allerdings insgesamt gegenstandslos und deshalb überflüssig.

Diese Thesen, die im Explanatory Report auch nicht begründet werden, überzeugen nicht vollends. Zwar ist richtig, dass das Merkmal „unbefugt" tatsächlich nicht vorliegen kann, wenn eine Tathandlung im Rahmen „genehmigten Testens" vorgenommen wird. Abs. 2 enthält jedoch darüber hinaus eine Freizeichnung für den Fall, dass eine Tathandlung zum Schutz eines Computersystems vorgenommen wird. In dieser Konstellation liegt aber nicht zwingend auch eine entsprechende Befugnis vor. Wenn etwa ein IT-Sicherheitsbeauftragter für den Schutz eines

---

[83] Siehe auch oben I.B.4.

[84] Explanatory Report zur CCC, Rn. 77.

[85] Ebd.

Unternehmenscomputers zuständig ist, sind Konstellationen denkbar, in denen eine Handlung des IT-Sicherheitsbeauftragten zum Schutz des Unternehmenscomputers vorgenommen werden, gleichzeitig aber nicht von einer konkreten Befugnis der Unternehmensführung gedeckt sind. In anderen Tatvarianten wie etwa dem Herstellen eines Computerprogramms ist schon nicht offensichtlich, auf wessen Befugnis es hier ankommen soll, sodass schon deshalb kein Gleichlauf des Merkmals „(un-)befugt" und des Merkmals „zum Schutz eines Computersystems" anzunehmen ist. Richtigerweise hätte deshalb im Explanatory Report ausgeführt werden müssen, dass in den Fällen des genehmigten Testens und der Handlungen zum Schutze eines Computersystems der besondere Vorsatz bezogen auf die Begehung einer Zieltat fehlt. Im Ergebnis erlangt Abs. 2 dann freilich keine eigene Bedeutung neben Abs. 1.[86] Da er in dieser Form nur Verwirrung und Rechtsunsicherheit stiftet, ist er abzulehnen.

Auch die personenbezogenen Freistellungsklauseln des Exportkontrollstrafrechts, die insbesondere bestimmte *staatliche Bedienstete* oder *zuständige Stellen* betreffen, sind im Rahmen der Software-Delikte nicht brauchbar. Die Dual-Use-Problematik besteht vor allem in der Privatwirtschaft, namentlich der IT-Sicherheitsbranche. Zwar sind auch dort personenbezogene Ausschlussklauseln, etwa für *registrierte* IT-Sicherheitsunternehmen denkbar, jedoch ist von einer erheblichen Fluktuation zwischen sogenannten Black-Hat-Hackern und White-Hat-Hackern auszugehen. Angesichts der Tatsache, dass IT-Sicherheitsunternehmen deliktsgeeignete Software in der Regel nach Auftragslage maßschneidern, ist in jedem Einzelfall zu prüfen, welcher Auftraggeber von dem IT-Sicherheitsunternehmen bedient wird und welche Zwecke dieser verfolgt: So programmierte beispielsweise das hessische Unternehmen *DigiTask GmbH* eine umstrittene Überwachungssoftware für das Zollkriminalamt und das bayerische Landeskriminalamt, verkaufte diese Software jedoch auch an mehrere ausländische Regierungen.[87] Mittlerweile wird die Software von allen gängigen Antivirenprogrammen als Schadsoftware eingestuft.[88] Aus diesem Grunde erscheint ein genereller Tatbestandsausschluss für registrierte IT-Sicherheitsunternehmen zu grob.[89]

---

[86] So auch *Spannbrucker*, CCC, S. 81.

[87] Vgl. NZZ vom 15.10.2011, „‚Staatstrojaner' im Fall Stauffacher eingesetzt", online abrufbar unter http://www.nzz.ch/nachrichten/politik/schweiz/trojaner_im_fall_stauffacher_eingesetzt_1.12994241.html [zuletzt abgerufen am 16.11.2004] sowie *Cyrus Farivar*, "German company behind government spyware admits sale to Bavaria", online abrufbar unter http://www.dw.de/dw/article/0,,15453150,00.html [zuletzt abgerufen am 16.11.2004].

[88] dpa-Meldung vom 11.10.2011, „Staatstrojaner-Hersteller Digitask: Entwickler für besondere Aufgaben", online abrufbar unter http://heise.de/-1359326 [zuletzt abgerufen am 16.11.2004].

[89] Gleiches gälte freilich für einen Tatbestandsausschluss durch eine generelle Genehmigung, ähnlich wie im Waffenrecht (§§ 7, 35 WaffG), vgl. hierzu *Hefendehl*, Kollektive Rechtsgüter, S. 145 f.

Hier müsste etwa eine handlungsbezogene Klausel ergänzt werden, wonach zu prüfen wäre, ob im Einzelfall rechtmäßige berufliche oder dienstliche Pflichten erfüllt werden.[90] Eine solche Ausschlussklausel verschöbe allerdings das wertungsmäßige Problem unnötig auf die nächsthöhere Abstraktionsebene: Wann die berufliche Entwicklung gefährlicher Software rechtmäßig ist, kann konkreter und damit transparenter auf Tatbestandsebene sowie durch oben genannte Ausschlussklausel ausgedrückt werden.

Auch die Bagatellklausel aus dem Exportkontrollstrafrecht, die Güter im Wert bis zu 2.500 € vom Tatbestand ausnimmt, bietet sich nicht an. Statt legitimes von illegitimem Verhalten zu scheiden, soll hier eine gewisse Erheblichkeitsschwelle eingezogen werden: Die Klausel ist vor allem unter der Annahme sinnvoll, dass Güter, die tatsächlich die geschützten Rechtsgüter[91] verletzen können, in aller Regel zu höheren Preisen gehandelt werden. Dass diese Bagatellklausel auch im Exportkontrollstrafrecht selbst nicht auf Datenverarbeitungsprogramme angewandt wird, mag aus der Annahme folgen, dass die Preise auch hochgradig gefährlicher Computerprogramme noch nicht das Niveau herkömmlicher Waffen oder Rüstungsgüter erreicht haben.

Es ist zwar zweifelhaft, dass dies nach wie vor den Tatsachen entspricht. Zumindest beim Computerwurm Stuxnet wurde nämlich vermutet, dass zur Entwicklung eines solchen Computerprogramms bis zu zehn IT-Spezialisten etwa sechs Monate zusammenarbeiten mussten,[92] weshalb schon die Entwicklungskosten auf einen siebenstelligen Euro-Betrag geschätzt werden.[93] Jedoch scheint es nicht wirklichkeitsnah, einen so starken Zusammenhang zwischen der Gefährlichkeit und dem Handelspreis eines Computerprogramms zu konstruieren, dass man hieran eine strafbarkeitsauslösende Erheblichkeitsschwelle ausrichten könnte.

Normative Ausschlussklauseln erweisen sich vor allem dort als wertvoll, wo schon die tatbestandlichen Einschlusskriterien normativ geprägt sind. Wenn Munition, die einem militärischen Zweck dienen soll, tatbestandsmäßig sein soll, erscheint es folgerichtig, Munition auszunehmen, die dem Zweck des Vögelaufschreckens dienen soll.[94] Im hier zu entwerfenden Software-Delikt sind solch normative Ausschlussklauseln freilich aus denselben Gründen abzulehnen, aus denen normative Elemente schon bei der positiven Regelung des Tatbestandes abgelehnt worden

---

[90] Vgl. § 184b Abs. 5 StGB; Vorschlag auch bei *Holzner*, ZRP 2009, 178.

[91] Dort: das friedliche Zusammenleben der Völker, die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland und ihre auswärtigen Beziehungen.

[92] Siehe "Stuxnet worm is the 'work of a national government agency'", The Guardian vom 24. September 2010, online abrufbar unter http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency [zuletzt abgerufen am 16.11.2004].

[93] Siehe „Der digitale Erstschlag ist erfolgt", FAZ vom 22. September 2010, online abrufbar unter http://www.faz.net/-gsi-xua1 [zuletzt abgerufen am 16.11.2004].

[94] Vgl. oben Teil 3, III.E.

sind: Entscheidend sind unter dem Multifunktionsaspekt und dem Mehrzweckaspekt des Dual-Use-Phänomens die objektive (funktionelle) Eignung eines Computerprogramms und die Intention (Zwecksetzung) des Vorfeldtäters. Jede normative Verschiebung dieser Kriterien, sei es im Tatbestand, sei es in einer Ausschlussklausel, führt mindestens zur Umgehungsanfälligkeit des gesamten Delikts.

c) Zusammenfassung: Normierung einer Freistellungsklausel

Es konnte gezeigt werden, dass ein optimiertes Software-Delikt eine Freistellungsklausel enthalten sollte, die IT-Sicherheitsbeauftragte dort von der Strafbarkeit ausnimmt, wo sie mit tatbestandlichen Computerprogrammen umgehen und nach dem *Full-Disclosure-Prinzip* im Einzelfall auch einen Verwendungsvorsatz in Form von dolus eventualis haben. Die Freistellungsklausel sollte daran anknüpfen, dass die Tathandlung (mittelbar) zum Schutze vor den Wirkungen von Schadsoftware oder der Abwehr solcher Wirkungen geeignet ist und auch zu diesem Zweck vorgenommen wird.

II. Weitere Fragen

Bevor ein Modellstraftatbestand entworfen wird, der alle Software-Delikte zusammenführt und gemäß den oben durchgeführten Analysen optimiert, sollen einige ergänzende Fragen kurz angesprochen werden. Im Rahmen einer grundlegenden Reform des Software-Strafrechts würden diese Punkte vertiefte Erörterung verdienen.

A. All-Crime-Ansatz?

Bislang hat der deutsche Gesetzgeber für mehrere Deliktsbereiche je einzelne Software-Delikte geschaffen und hierbei regelmäßig neue Regelungstechniken erfunden und angewandt. Sachlich ist die Motivation für die Schaffung der Software-Delikte jedoch jeweils ähnlich: Die Verbreitung von Schadsoftware, also Deliktswerkzeugen, soll eingedämmt, Schwarzmärkte trockengelegt und Massenkriminalität verhindert werden. Allgemein soll verhindert werden, dass Personen in die Lage versetzt werden, Straftaten zu begehen, die hierzu ohne solche Computerprogramme nicht fähig wären. Dies lässt sich abstrakt jeweils gleichartig normieren, unabhängig davon, in welchem Kriminalitätsbereich man ein Vorfelddelikt normieren möchte. Dem entspricht, dass der Gesetzgeber bei der Schaffung neuer Software-Delikte auch regelmäßig auf Gemeinsamkeiten zu anderen IT-Straftatbeständen hingewiesen hat.

Es bietet sich damit ein All-Crime-Ansatz an, bei dem alle Zieldelikte in ein Software-Delikt aufgenommen werden.[95] Der entsprechende Straftatbestand könnte in einem ersten deliktsneutralen Absatz das tatbestandsmäßige Computerprogramm beschreiben, die inkriminierten Tathandlungen benennen und den subjektiven Bezug des Täters zur Zieltat festlegen. In einem zweiten Absatz könnte sodann benannt werden, für welche Zielstraftaten das Vorfelddelikt des ersten Absatzes gelten soll.

„All-Crime" würde hier also bedeuten, dass das Softwarespezifische Vorfelddelikt in allen Deliktsbereichen eingesetzt werden kann, in denen Straftaten mittels Computerprogrammen begangen werden. Es müsste immer nur ein entsprechender Verweis auf das jeweilige Zieldelikt in das Softwarespezifische Vorfelddelikt aufgenommen werden.

Ein solcher Ansatz würde die Rechtsklarheit nochmals erhöhen, indem er die Regelungstechnik der einzelnen Software-Delikte vereinheitlicht und durch eine einheitliche Verweisungstechnik den Geltungsbereich dieses Vorfelddelikts deutlich macht. Zudem ließe sich ein solcher Vorfeldtatbestand ohne Systembruch erweitern, wenn die gesellschaftliche Entwicklung zeigt, dass auch in anderen Deliktsbereichen ein Software-Delikt erforderlich wird.

Das eingangs[96] erwähnte *Ubiquitous Computing* wird zu einer erheblichen Ausdehnung von Computertechnik in heute noch informationstechnikfreie Lebensbereiche führen. Der oben erörterte § 22b StVG[97] zeigt, dass mit der Digitalisierung von Tachometern und Geschwindigkeitsbegrenzern in Autos ein entsprechendes kriminelles Einsatzfeld für Schadsoftware entstanden ist. Gleiches steht bei der anstehenden Digitalisierung von Stromzählern *(smart meter)* zu befürchten. Digitale Schließanlagen für Wohnhäuser lassen an ein Software-Delikt im Vorfeld eines Wohnungseinbruchsdiebstahls denken, etwa weil man mit der passenden Schadsoftware künftig mit einem Mausklick die Schließanlage hacken und die Wohnungstür öffnen könnte. Aber auch Medizintechnik wird digitalisiert, sodass zumindest theoretisch Leib und Leben durch Hacking angegriffen werden können. Nicht zuletzt hat der Computerwurm *Stuxnet* gezeigt, dass auch Uran-Anreicherungsanlagen mittels Schadsoftware sabotiert werden können.[98] Dies führt schließlich zu der Befürchtung, dass auch schwere staatsgefährdende Gewalttaten mittels Schadsoftware begangen werden können.

---

[95] So auch *Sieber*, Straftaten und Strafverfolgung im Internet, S. C 90.

[96] Siehe oben Einleitung, I.

[97] Siehe oben Teil 3, I.B.2.

[98] Siehe dazu *Zetter*, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, wired.com vom 7.11.2011, online abrufbar unter http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 [zuletzt abgerufen am 27.2.2013].

Ein All-Crime-Ansatz könnte es überflüssig machen, in jedem strafrechtlichen Teilgebiet neu über die konkrete Ausgestaltung eines Software-Delikts nachzudenken. Zudem würde durch den skizzierten All-Crime-Ansatz vermieden, dass in mehreren Straftatbeständen unterschiedliche Formulierungen verwandt werden, bei denen zunächst der Eindruck entsteht, es handle sich um bewusste Nuancierungen, obwohl in Wirklichkeit bloße Sprachversehen vorliegen. Schließlich würde sich auch die Abhängigkeit von möglicherweise unsauber übersetzten internationalen Instrumenten reduzieren.

In diesem Zusammenhang wäre wohl auch der Strafrahmen der Software-Delikte zu überprüfen, der momentan eine Freiheitsstrafe bis zu einem beziehungsweise zwei Jahren oder Geldstrafe vorsieht. Öffnet man das Software-Delikt auch für das Vorfeld von schweren staatsgefährdenden Gewalttaten oder Angriffen auf Leib und Leben, so erscheint es angezeigt, den Strafrahmen anzuheben oder jedenfalls Qualifizierungen vorzusehen. Diese könnten anknüpfen an eine (abstrakte) Gefährdung hochwertiger Rechtsgüter, an das Hinwirken auf Schäden großer Zahl oder großen Ausmaßes oder an eine bandenmäßige oder gewerbsmäßige Begehung.[99] Ebenso könnte eine Vorschrift über tätige Reue ähnlich dem § 149 Abs. 2 StGB normiert werden.[100]

B. Computerprogramm oder Vorrichtung?

Eine weitere Frage betrifft die Bezeichnung des Tatgegenstands. In einigen Normen verwendet der Gesetzgeber den Begriff der *Vorrichtung*, der jedoch schillernd ist. Es ist unklar, ob ihm überhaupt eine Ausscheidungsfunktion zukommt. In den Gesetzesmaterialien und dem Großteil der Literatur wird nicht näher erläutert, was eine Vorrichtung im Sinne des Gesetzes ausmacht oder wodurch sie sich konkret auszeichnet. Jedenfalls versteht der deutsche Gesetzgeber den Begriff der Vorrichtung in den hier thematisierten Software-Delikten weiter als den Begriff des Computerprogramms. Bei der Umsetzung der Cybercrime Convention, die im Originaltext auch von Vorrichtungen[101] spricht, hat der deutsche Gesetzgeber nämlich noch explizit einen Vorbehalt gemäß Art. 42, Art. 6 Abs. 3 CCC gegen diese Vorgabe formuliert, um den deutschen § 202c Abs. 1 Nr. 2 StGB auf Computerprogramme beschränken zu können.[102]

Der Begriff „ähnliche Vorrichtungen“ wird dagegen auch in § 149 Abs. 1 Nr. 1 und § 275 Abs. 1 Nr. 1 StGB verwandt, wird dort aber durch die unmittelbar zuvor genannten Vorrichtungen inhaltlich konturiert. In § 275 Abs. 1 Nr. 1 StGB, dessen

---

[99] Siehe dazu *Sieber*, Straftaten und Strafverfolgung im Internet, S. C 92.

[100] Ebd.

[101] In der englischen Originalfassung wird der Begriff „device“ gebraucht.

[102] Siehe BT-Drucks. 16/3656, S. 12 linke Spalte.

Tatobjekte – anders als in § 149 Abs. 1 Nr. 1 StGB – nie um Computerprogramme ergänzt wurden, sind diese nach herrschender Auffassung vom Begriff der Vorrichtungen *nicht* erfasst.[103] Dass in anderen Tatbeständen wie § 2 ZKDSG oder § 95a UrhG der Begriff „Vorrichtung" gewählt wurde und hierunter in erster Linie Computerprogramme gefasst werden sollten,[104] zeigt deutlich, dass die Terminologie insgesamt wenig griffig ist und der Begriff nicht konsistent verwendet wird.

Teilweise wird die Vorrichtung in der Literatur auch definiert als ein Hilfsmittel, das zu einem bestimmten Zweck gefertigt wurde und insoweit einen spezifischen Anwendungsbereich hat.[105] Definiert man die Vorrichtung so, so nimmt man hier Spezifika der Vorrichtung vorweg, die im Gesetzeswortlaut noch als eigene Tatbestandsmerkmale explizit formuliert sind: nämlich Zweck, Bestimmung oder Eignung. Dies unterstreicht, dass der Begriff konturlos ist und nicht eigenständig stehen kann. Was eine Vorrichtung ist, wird erst im Kontext klar, wenn ausgeführt wird, wozu die Vorrichtung dienen soll.

Soll der Begriff der Vorrichtung weiter sein als der des Computerprogramms, müsste das Merkmal also Gegenstände erfassen, welche unter der Entwicklungsstufe eines betriebsbereiten IT-Geräts liegen. Denn dieses beinhaltet regelmäßig eine *Firmware*, also ein Computerprogramm. Konkret kämen einzelne Bauteile wie etwa Kabel oder Speicherchips in Betracht. Dagegen wären *Prozessor*chipkarten zweifelhaft, da dort notwendigerweise eine Art Betriebssystem (COS) aufgespielt ist, das die Kommunikation der CPU mit RAM, ROM, EEPROM und I/O durch einzelne Befehle verwaltet. Bei diesem Betriebssystem handelt es sich also um ein Computerprogramm im Sinne der WIPO-Mustervorschriften.[106] Im Falle von Kabeln und Speicherchips wäre hingegen eine Bestrafung aus einem Vorfelddelikt regelmäßig ausgeschlossen, da es an der nötigen Nähe zur späteren Rechtsgutsverletzung, also an der Unmittelbarkeit fehlt. Solche Gegenstände sind nämlich nicht gebrauchsfertig, sondern bedürfen weiterer Bearbeitung.[107]

Mit dieser Betrachtung steht auch in Einklang, dass in den nationalen Gesetzesmaterialien an keiner Stelle Beispiele für Vorrichtungen unterhalb der Schwelle eines computerprogrammgesteuerten Geräts genannt werden. Vielmehr wird stets betont, dass insbesondere Computerprogramme dem Begriff der Vorrichtung unter-

---

[103] Dölling/Duttge/Rössner-*A. Koch*, § 275 Rn. 2.

[104] Siehe oben Teil 3, I.B.3.–6.

[105] Spindler/Schuster-*Gercke*, § 108b UrhG Rn. 28; übereinstimmend auch Duden online, http://www.duden.de/rechtschreibung/Vorrichtung [zuletzt aufgerufen am 16.11.2004].

[106] Danach ist ein Computerprogramm eine *Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt*, vgl. GRUR 1979, 306; ohne Verweis auf die WIPO-Mustervorschriften auch LG Karlsruhe NStZ-RR 2007, 19.

[107] Vgl. sinngemäß RGSt 48, 161, 165; RGSt 55, 46, 47; RGSt 55, 283, 284; RG LZ 1922, 163; RGSt 65, 203, zuletzt wiederholt in BGH 1 StR 297/03 (= wistra 2004, 266).

fallen sollen. In den Erläuterungen zu § 2 Nr. 3 ZKDSG heißt es, dass als Umgehungsvorrichtungen vor allem Computerprogramme, manipulierte Set-Top-Boxen oder „neu gebaute Geräte" in Betracht kommen.[108] Später wird wieder explizit auf die Gefahr der „einfachen Verbreitung von Hackerwerkzeugen wie z.B. Entschlüsselungs*programmen*" hingewiesen.[109] Dies liegt auch nahe, da man bei Set-Top-Boxen deren *Firmware* manipulieren muss, damit sie verschlüsselte Inhalte in verständlicher Form wiedergeben.[110] Erst in Kombination mit dem manipulierten Computerprogramm wird die Set-Top-Box also einsatztauglich.

Neben Gerätebauteilen könnte auch „Code" unter den Begriff der Vorrichtung fallen, auch wenn dieser Code in seiner Gesamtheit nicht als Computerprogramm angesehen werden kann. Ein konkretes Beispiel hierfür wären Webseiten: Eine gefälschte Webseite könnte im Vorfeld eines Computerbetrugs eine tatbestandsmäßige Vorrichtung sein.

Solche gefälschten Webseiten sind häufig den Originalwebseiten von Banken nachempfunden und fordern den Webseitenbesucher auf, seine Login-Daten samt PIN und TAN einzugeben. Bankkunden werden in der Regel zuvor durch eine ebenfalls gefälschte E-Mail aufgefordert, die vermeintliche Bank-Homepage aufzusuchen, um dort die entsprechenden Angaben zu machen. Tatsächlich wird diese Webseite von Betrügern betrieben, die durch die angegebenen Daten Zugriff auf ein fremdes Konto erhalten und sich dort bereichern können.

Freilich handelt es sich bei solchen Webseiten eher um Täuschungsmittel, durch die ein Täter in direkten Kontakt mit dem Opfer tritt, um dessen Vertrauen zu gewinnen und letztlich auszunutzen. Damit handelt es sich phänomenologisch um eine andere Kategorie als die Kategorie der Schadsoftware, also der deliktsgeeigneten Computerprogramme, die als Tatwerkzeug und Angriffsmittel eingesetzt werden. Vor allem aber gilt für Webseiten nicht dieselbe gesetzgeberische Motivation wie für deliktsgeeignete Computerprogramme: Ein umfangreiches und leicht verfügbares Angebot an „Tools" im Internet lässt massive Rechtsgutsverletzungen, Massenkriminalität und Schwarzmärkte befürchten.[111] Dies ist nicht ohne Weiteres auf Webseiten übertragbar, da bislang kein umfangreiches Angebot gefälschter Bank-Webseiten, kein entsprechender Schwarzmarkt und auch keine massenhafte Unterhaltung solcher Webseiten festgestellt werden konnten.

De lege lata ist deshalb festzuhalten, dass vor allem Computerprogramme als „Vorrichtung" in Betracht kommen – sei es isoliert, sei es als Firmware oder als installiertes Betriebssystem auf einem Gerät. Der Begriff der Vorrichtung kann im Grunde nur unterhalb der Schwelle zur Software einen eigenen Bedeutungsgehalt

---

[108] BT-Drucks. 14/7229, S. 7 rechte Spalte.

[109] BT-Drucks. 14/7229, S. 8 linke Spalte.

[110] Vgl. LG Karlsruhe NStZ-RR 2007, 19.

[111] BT-Drucks. 14/7229, S. 7 linke Spalte.

erhalten. Sofern es sich dabei um körperliche Bauteile handelt, ist zweifelhaft, dass solche Gegenstände je das Unmittelbarkeitskriterium des „Eignungsmodells“ erfüllen können. Soweit Webseiten-Code als Vorrichtung betrachtet wird, handelt es sich um eine andere phänomenologische Kategorie, deren Kriminalisierung unter anderen Voraussetzungen als denen der Software-Delikte erörtert werden muss.

C. Überprüfung der Tathandlungen

Auch die Tathandlungen der Software-Delikte verdienen eine kritische Überprüfung. In dieser Arbeit wurden sie aus den bestehenden Software-Delikten schlicht übernommen und nur analysiert, soweit sie für die Dual-Use-Problematik relevant sind.

Gegen die konkret normierten Tathandlungen gibt es freilich erhebliche Einwände abseits der Dual-Use-Problematik: Sie sind relativ stark konkretisiert, überschneiden sich aber vielfach und lassen keine überlegene Systematik erkennen.[112] So ist es beispielsweise fraglich, ob das Verkaufen und Vermieten tatsächlich als eigene Tathandlung aufgeführt werden muss oder ob deren Anwendungsbereiche nicht durch das Einem-anderen-Verschaffen ausreichend abgedeckt werden, zumal es hier auf keine speziell schuldrechtliche Sicht ankommen kann.[113] Ähnlich verhält es sich mit dem Einführen, das wohl ebenfalls durch das Sich- oder Einem-anderen-Verschaffen abgedeckt ist.

Überhaupt ist fraglich, was unter dem Einführen eines (nichtkörperlichen!) Computerprogramms verstanden werden kann. Man könnte darunter verstehen, dass das Computerprogramm von einem ausländischen Server auf den in der Bundesrepublik befindlichen PC heruntergeladen wird. Dann stellt sich allerdings die Frage, ob diese Sichtweise bei Internetvorgängen wirklich passt, da dort nationalstaatliche Grenzen so weit an Bedeutung verloren haben, dass schon die bloße Rede von „Ein- und Ausfuhr von Daten über das Internet“ eigenartig anmutet. Zudem weiß ein Nutzer des *World Wide Web* häufig gar nicht, ob sich der physische Server, von dem er etwas herunterlädt, im In- oder Ausland befindet.

Insgesamt stellt sich die Frage, ob die Tathandlungen nicht durch eine etwas stärkere Abstraktion übersichtlicher und konsistenter gehalten werden könnten. So wäre zu prüfen, ob der bestehende Anwendungsbereich gewahrt bliebe, wenn zugunsten einer besseren Lesbarkeit und Konsistenz lediglich das Herstellen, Sichverschaffen und Zugänglich-Machen unter Strafe gestellt würden.

---

[112] *Scheffler* erhebt hier den Vorwurf der Schrotschusstechnik, ZStW 117 (2006), 766.

[113] Siehe nur NK-*Kargl*, § 202c Rn. 11; Schönke/Schröder-*Eisele*, § 202c Rn. 5 m.w.N.

D. Verletzung internationaler Umsetzungspflichten?

Zuletzt stellt sich die Frage, ob die Bundesrepublik Deutschland ihre internationalen Verpflichtungen verletzt, wenn sie die Software-Delikte in einem einzigen Tatbestand zusammenführt. Solches könnte man meinen, weil die Bundesrepublik sich verpflichtet hat, die internationalen Instrumente ordnungsgemäß umzusetzen, und dies in der Regel dadurch getan hat, die deutschen Gesetzeswortlaute eng an die internationalen Vorgaben zu anzupassen. Führt man nun alle bestehenden Software-Delikte in einem einheitlichen Tatbestand zusammen, so könnten sich auf Ebene des Wortlauts nicht nur sprachlich-formale, sondern auch leichte inhaltliche Abweichungen zu den internationalen Instrumenten ergeben. Sämtliche internationalen Instrumente sind jedoch ausschließlich hinsichtlich ihrer Ziele verbindlich, nicht hinsichtlich der Umsetzungsmittel.[114] Abweichungen im Wortlaut sind demnach unschädlich, solange die deutschen Gesetze das Ziel der Harmonisierung weiterhin erreichen.

Zudem hat die obige Analyse der internationalen Instrumente gezeigt, dass mitunter schon innerhalb desselben Instruments auf formaler und inhaltlicher Ebene Abweichungen zwischen den amtlichen Übersetzungen bestehen.[115] So sieht Art. 7 KOM(2010) 517 *endgültig* nur in seinem englischen Wortlaut ein Absichtsdelikt, im deutschen jedoch ein abstraktes Gefährdungsdelikt vor. Vorrangregelungen gibt es bei abweichenden Sprachfassungen jedenfalls im Recht der EU nicht.[116] Bei evidenten Übersetzungsfehlern spricht allerdings schon die teleologisch-historische Auslegung dafür, das fehlerfreie Originaldokument stärker zu berücksichtigen. Damit würde das oben vorgezogene „Eignungsmodell" mit Verwendungsabsicht zwar die englische Fassung der Richtlinie korrekt umsetzen, nicht jedoch die fehlerhaft ins Deutsche übersetzte Fassung. Dieser Umstand sowie der grundsätzliche Umsetzungsspielraum des Gesetzgebers lassen eine Verletzung der Implementierungspflichten folglich abwegig erscheinen.

III. Entwurf eines Modellstraftatbestandes

Der Vergleich der Regelungsmodelle hat ergeben, dass ein optimiertes Software-Delikt einen All-Crime-Ansatz verfolgt, das „Eignungsmodell" mit einer Verwendungsabsicht kombiniert sowie eine handlungs- und zielbezogene Freistellungsklausel normiert.[117] Damit ergibt sich ein Modellstraftatbestand mit dem folgenden Wortlaut:

---

[114] Siehe oben Teil 3, II.A.

[115] Siehe insbesondere Teil 3, II.B.2. und II.B.6.

[116] Siehe oben Teil 3, II. am Anfang und Fn. 661.

[117] Siehe oben I.C. sowie II.A.

Missbrauch von Computerprogrammen

(1) Wer ein Computerprogramm, das unmittelbar zur Begehung einer strafbaren Handlung nach Abs. 2 verwendet werden kann,

1. in der Absicht, dass es hierzu verwendet werde, herstellt, sich verschafft, verwahrt oder einführt, oder
2. mit dem Vorsatz, dass es hierzu verwendet werde, verkauft, vermietet, einem anderen verschafft oder überlässt, zugänglich macht oder verbreitet,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Strafbare Handlungen im Sinne des Abs. 1 sind

1. Vergehen nach den §§ 202a Abs. 1, 202b, 303a Abs. 1, 303b Abs. 1 StGB,
2. Vergehen nach § 263a Abs. 1 StGB,
3. Vergehen und Verbrechen nach den §§ 146, 148, 151, 152, 152a, 152b StGB,
4. Vergehen nach §§ 106, 108, 108a, 108b UrhG,
5. Vergehen nach § 22b Abs. 1 Nr. 1 und 2 StVG,
6. […]

(3) Abs. 1 gilt nicht für eine Handlung, die zum Schutz gegen Wirkungen von Computerprogrammen im Sinne des Abs. 1 oder zur Abwehr dieser Wirkungen geeignet ist und vorgenommen wird.

Der objektive Tatbestand wird hier geprägt von der unmittelbar deliktischen Eignung des Computerprogramms. Korrespondierend wird subjektiv eine Verwendungsabsicht oder ein Verwendungsvorsatz des Vorfeldtäters verlangt. Die Tathandlungen werden danach untergliedert, ob der Vorfeldtäter die Kontrolle über das Computerprogramm selbst ausübt (Nr. 1) oder Dritten einräumt (Nr. 2). Der subjektive Bezug des Vorfeldtäters zur Zieltat soll in Nr. 1 als Absicht vorliegen, in Nr. 2 soll einfacher Vorsatz genügen. Durch die Ausschlussklausel des Abs. 3 werden letzte Unsicherheiten in der IT-Sicherheitsbranche auch bei Verfahren nach dem *Full-Disclosure-Prinzip* beseitigt. Die Aufzählung der Zieldelikte in Abs. 2 beendet die intransparente Verweisungstechnik der bestehenden Software-Delikte. Durch Ergänzungen des Abs. 2 können entsprechende Vorfelddelikte ohne Systembruch auch in weiteren Deliktsbereichen eingeführt werden. Dies macht zudem deutlich, dass es sich bei solchen Straftatbeständen um Delikte im Grenzbereich zwischen Besonderem und Allgemeinem Teil des Strafgesetzbuchs handelt.

Dieses Regelungsmodell schafft ein hohes Maß an *Rechtsklarheit* und *Legitimität*. Rechtsklarheit schafft es, weil es effektiv, effizient und verständlich ist. Legitim ist es, weil es eine Risikoerhöhung impliziert und stets einen „eindeutig deliktischen Sinnbezug“ herstellt.

Zunächst ist dieses Tatbestandsmodell *effektiv*, da es den weiten Anwendungsbereich des „Eignungsmodells“[118] zugrunde legt und durch die Verwendungsabsicht nicht übermäßig einschränkt.[119] Es ist außerdem *effizient*, weil sich sein Anwendungsbereich mit relativ geringem Auslegungsaufwand aus dem Wortlaut ergibt. Dies liegt daran, dass keine unpräzisen, ungeklärten oder umgangssprachlichen Termini eingesetzt werden und der Wortlaut nicht so weit ist, dass er grundsätzlich teleologisch reduziert werden müsste. Zwar existiert die Wendung „mit dem Vorsatz“ aus Abs. 1 Nr. 2 in dieser Form nicht in Tatbeständen des Strafgesetzbuches, jedoch ist die Wendung „in der Absicht“ seit langem etabliert.[120] Es muss daher nur „Absicht“ durch „Vorsatz“ ersetzt werden, also durch einen Terminus mit ebenfalls gefestigtem Inhalt. Die Regelungstechnik ist schließlich auch *verständlich*, da sie die maßgeblichen Tatbestandsmerkmale selbst und unmittelbar benennt, ohne die Grenzen der Strafbarkeit durch intransparente Verweisungen zu verschleiern. Dieses Tatbestandsmodell schafft folglich höchste Rechtsklarheit.

Sodann beschreibt dieses Tatbestandsmodell stets eine *Risikoerhöhung* für das geschützte Rechtsgut: Deliktsgeeignete Computerprogramme gefährden schon durch ihre Existenz (Nr. 1) das Rechtsgut, vor allem aber, wenn der Täter sie nicht mehr alleine kontrollieren kann (Nr. 2). Tatbestandsmäßiges Verhalten nach diesem Modell hat außerdem ausnahmslos einen „eindeutig deliktischen Sinnbezug“: Der Handelnde hat mindestens den Vorsatz, dass das fragliche Computerprogramm zu einer Straftat eingesetzt wird (Abs. 1 Nr. 2) und handelt dabei nicht zum Schutz gegen Wirkungen deliktsgeeigneter Computerprogramme (sonst griffe Abs. 3). Damit ist sichergestellt, dass der Handelnde sich in jedem Falle als Vorfeldtäter versteht und in ein kriminelles Gesamtgeschehen integrieren will – eine andere plausible Erklärung für sein Verhalten gibt es nicht. Folglich erzielt dieses Tatbestandsmodell im Vergleich zu allen gegenwärtigen Software-Delikten die höchste Legitimität.

---

118 Vgl. oben I.C.1.a).

119 Vgl. oben I.C.2.a).

120 Siehe etwa § 124, § 146 Abs. 1 Nr. 1, § 164 Abs. 1, § 176a Abs. 3, § 219b Abs. 1, § 241a Abs. 4, 242 Abs. 1 StGB und viele mehr.

Teil 5

Zusammenfassung: die angemessene Kriminalisierung von Dual-Use-Software

Im deutschen Haupt- und Nebenstrafrecht sind seit dem Jahre 2002 mehrere Straftatbestände geschaffen worden, die schon im Vorfeld einer Rechtsgutsverletzung den Umgang mit Computerprogrammen unter Strafe stellen, die als Deliktswerkzeuge bei späteren Straftaten fungieren. Zum Teil gehen diese Software-Delikte[1] auf Vorgaben europäischer Rechtsgeber, insbesondere des Europarats und der Europäischen Union, zurück.

Dass diese Software-Delikte notwendig seien, schlossen europäische wie nationale Gesetzgeber aus der Feststellung, dass solche Computerprogramme auch technisch weniger versierte Nutzer in die Lage versetzen, in erheblichem Ausmaß Straftaten zu begehen. Man erkannte, dass ein beachtlicher Teil der Schadsoftware im Internet für jedermann kostenlos zur Verfügung steht und rasend schnelle, weltweite Verbreitung finden kann. Daneben gibt es hochspezialisierte Hacker oder Hackergruppierungen, die spezielle Schadsoftware maßschneidern und zu hohen Preisen verkaufen oder gar stundenweise vermieten.

Die Gesetzgeber befürchten deshalb zweierlei: Einerseits drohe durch die massenweise Verfügbarkeit kostenloser Schadsoftware eine regelrechte Massenkriminalität.[2] Durch den Handel mit hochspezieller Schadsoftware könnten daneben Schwarzmärkte für solche *Tools* entstehen.[3] Um dies zu verhindern, sollte die Strafbarkeit von der eigentlichen Rechtsgutsverletzung vorverlagert werden und bereits den Umgang mit Deliktswerkzeugen erfassen. Ein weiterer Effekt dieser Vorverlagerung der Strafbarkeit liegt darin, dass Ermittlungsmaßnahmen zu einem früheren Zeitpunkt möglich werden. Freilich könnte dies nicht als Begründung und Rechtfertigung für eine Strafbarkeitsvorverlagerung vorgetragen werden,[4] und wird es auch nicht.[5]

---

[1] Software-Delikte im deutschen Haupt- und Nebenstrafrecht: § 149 Abs. 1 StGB, § 202c Abs. 1 Nr. 2 StGB, § 263a Abs. 3 StGB, § 22b Abs. 1 Nr. 3 StVG, § 108b Abs. 2 UrhG, § 4 ZKDSG.

[2] Siehe nur BT-Drucks. 16/3656, S. 12 linke Spalte.

[3] Siehe nur Explanatory Report zur CCC, Rn. 71.

[4] Vgl. zu diesem Argument *Deckers* ZRP 2008, 170; kritisch zu diesem Aspekt auch *Heinrich*, ZStW 121 (2009), 116; *Rackow*, FS für Maiwald, S. 618.

[5] Eine Ausnahme hiervon bildet *Kauder*, ZRP 2009, 21, allerdings scheint er von einem grundsätzlich präventiven Strafrecht auszugehen. In seiner Argumentation setzt er nämlich

Die Gefahr einer solchen Vorverlagerung besteht in sogenannten *Chilling Effects*: Unternehmen und Entwickler der IT-Sicherheitsbranche könnten bestimmte Verhaltensweisen aufgeben, weil sie befürchten, sich selbst wegen eines Vorfelddelikts strafbar zu machen. Eine solche Kriminalitätsfurcht ist freilich nur dann wahrscheinlich und gerechtfertigt, wenn die Vorfelddelikte rechtstechnisch so gestaltet sind, dass man überhaupt das Verhalten der IT-Sicherheitsberater, insbesondere das Testen, Analysieren und Demonstrieren von Sicherheitslücken zum Zwecke ihrer Behebung, unter den Tatbestand fassen kann. Damit besteht die gesetzgeberische Herausforderung darin, Vorfeldtatbestände so zu formulieren, dass solche *Chilling Effects* nicht entstehen, gleichzeitig aber ein effektiver Anwendungsbereich des Vorfeldtatbestandes erhalten bleibt. Dies wird durch das Schlagwort der Dual-Use-Problematik ausgedrückt.

Teil 1 der Arbeit hat gezeigt, dass sich das Dual-Use-Phänomen in zwei Ausprägungen zeigt: Computerprogramme können mehrere *Funktionen* haben, von denen nur ein Teil deliktisch einsetzbar ist (Multifunktionsaspekt). Außerdem kann und muss eine deliktisch einsetzbare Funktion auch immer zu *Test-, Analyse- und Demonstrationszwecken* in der IT-Sicherheitsbranche eingesetzt werden (Mehrzweckaspekt).

In Teil 2 wurde dargelegt, dass die Legitimität von Software-Delikten danach verglichen werden kann, ob sie eine Risikoerhöhung für das Rechtsgut implizieren und ob das tatbestandlich umschriebene Verhalten einen „eindeutig deliktischen Sinnbezug“ herstellt. Für die spätere Bewertung der Vorfelddelikte wurde das tatbestandliche Vorfeldverhalten abstrahiert und kategorisiert.

In Teil 3 der Arbeit wurden die Rechtstechniken analysiert, mit denen die Dual-Use-Phänomene in den deutschen Software-Delikten, ihren internationalen Vorläufern und den Vorfelddelikten des Rüstungskontrollrechts reguliert werden. Schon hier konnte gezeigt werden, dass die Regelungstechniken der deutschen Software-Delikte die beiden Ausprägungen des Dual-Use-Phänomens nur sehr inkonsequent berücksichtigen. Sie führen deshalb stellenweise zu einer erheblichen Überkriminalisierung, lassen andererseits aber auch beachtliche Schutzlücken.

In Teil 4 der Arbeit wurden die Regelungstechniken aus dem Teil 3 danach vergleichend bewertet, wieviel Rechtsklarheit sie schaffen und wieviel Legitimität sie gewährleisten. Hier wurde gezeigt, dass die bestehenden Software-Delikte nach diesem Maßstab gravierende Schwächen aufweisen, solche Schwächen jedoch keineswegs zwingend sind. Sie können durch eine optimierte Regelungstechnik behoben werden, die hier auch unter Rückgriff auf die Regelungstechniken des Rüstungskontrollrechts gewonnen und in einem Modellstraftatbestand ausformuliert

---

das „frühzeitige Eingreifen“ als Aufgabe des Strafrechts voraus und schlussfolgert hieraus sodann die grundsätzliche Legitimität der Strafbarkeit von solchen Vorbereitungshandlungen, die „auf das Delikt hinweisen, auf das sie abzielen“ – offenbar ohne die Tautologie zu erkennen.

wurden. Dieser Modellstraftatbestand kann im Wege eines All-Crime-Ansatzes alle bestehenden Software-Delikte vereinen und ersetzen.

I. Kein zwingendes Problem der Legitimation

Im 2. Teil der Arbeit wird davon ausgegangen, dass die Legitimationsdiskussion nach ihrem aktuellem Stand noch keine absoluten Kriterien liefern kann, nach denen die Legitimität eines Vorfelddelikts, wie es in den Software-Delikten normiert worden ist, verbindlich beurteilt werden könnte. Es besteht aber strukturell Einigkeit unter den Autoren, dass ein gewisses Maß an objektiver Risikoschaffung ebenso erforderlich ist wie ein irgendwie gearteter „deliktischer Sinnbezug".[6]

Hieraus wurden für die Ziele dieser Arbeit Leitideen für einen Legitimitätsvergleich entwickelt. Demnach wird ein Regelungsmodell als *vergleichsweise legitim* angesehen, wenn es ein höheres Risiko voraussetzt als ein anderes Regelungsmodell. Gleiches gilt, wenn ein Regelungsmodell einen „eindeutig deliktischen Sinnbezug" deutlicher kennzeichnet als ein anderes Regelungsmodell. Über den Indikator der Risikoerhöhung wurde insbesondere völlig ungefährliches Verhalten ausgeschieden. Über den Indikator des „eindeutig deliktischen Sinnbezugs" wurde Verhalten ausgeschieden, das objektiv auch als sozialnützliches Verhalten plausibel erklärt werden kann.[7]

Nachdem im 3. Teil die Regelungstechniken der Software-Delikte des deutschen Strafrechts, der internationalen Vorläufer sowie des Rüstungskontrollrechts analysiert wurden, konnten diese im 4. Teil der Arbeit in Modelle zusammengefasst[8] und hinsichtlich ihrer Legitimität verglichen werden. Dieser Vergleich hat zunächst gezeigt, dass sich die Risikoerhöhung im Wesentlichen aus der objektiven Umschreibung des Tatobjekts ergeben muss, während der „eindeutig deliktische Sinnbezug" im subjektiven Tatbestand zu konstruieren ist.[9] Damit konnten Anschließungsdelikte schon als vergleichsweise illegitimes Regelungsmodell ausgeschlossen werden, da sie auf die Normierung eines subjektiven Bezuges gänzlich verzichten. Daneben konnten auch Vorbereitungsdelikte keinen eindeutig „deliktischen Sinnbezug" herstellen und waren deshalb ebenfalls als vergleichsweise illegitim abzulehnen. Als vorzugswürdig erwies sich die Normierung einer Verwendungsabsicht.[10]

---

6 Siehe oben Teil 2, IV.A.

7 Siehe oben Teil 2, IV.B.

8 Siehe oben Teil 4, I.B.

9 Siehe oben Teil 4, I.C.1.f).

10 Siehe oben Teil 4, I.C.2.a).

Bei der tatbestandlichen Beschreibung des Computerprogramms zeigt sich, dass das „Zweckmodell“ und das „Entstehungsmodell“ nur potentielle Risiken festlegen, während das „Marketingmodell“ eine Risikopotenz umschreibt. Diese drei Modelle wurden dementsprechend als vergleichsweise illegitim bewertet. Das „Eignungsmodell“ vertatbestandlicht durchweg eine Risikoerhöhung und ist deshalb am ehesten als legitim zu werten.[11] Die Risiken wurden hier in Abhängigkeit von verschiedenen Kategorien von Vorfeldverhalten[12] bewertet.

II. Kein zwingendes Problem der Rechtsklarheit

Aufbauend auf der Analyse von Inhalt, Bedeutung und Weite der einzelnen Regelungstechniken in Teil 3 der Arbeit konnte in Teil 4 auch deren Rechtsklarheit bewertet werden. Hierbei wurden als Indikatoren für die Rechtsklarheit einer Regelungstechnik deren Effektivität, Effizienz und Verständlichkeit herangezogen.[13] Unter dem Schlagwort der *Effektivität* wurde dabei gefordert, dass die Regelungstechnik überhaupt einen Anwendungsbereich hat und nicht etwa ein Symbolgesetz darstellt. Auch durfte die Norm nicht enger sein als vom Gesetzgeber gewollt, da dies Umgehungsmöglichkeiten schaffen würde. Unter *Effizienz* wurde verstanden, dass der Sinn des Tatbestandes möglichst direkt und ohne großen Auslegungsaufwand ermittelt werden kann. Hierfür sollte der Wortlaut präzise und ohne umgangssprachliche Wendungen formuliert sein, außerdem sollte er nicht weiter sein als vom Gesetzgeber gewollt, da er sonst eine grundsätzliche teleologische Reduktion im Wege der Auslegung erforderlich macht. Schließlich wurde unter dem Schlagwort der *Verständlichkeit* des Regelungsmodells gefordert, dass die wesentlichen Merkmale des Tatbestands und die Grenzen der Strafbarkeit im Wortlaut selbst kenntlich gemacht werden und nicht durch intransparente Verweise auf andere Normen in anderen Gesetzen oder Verordnungen verschleiert werden.

Auch nach diesem Maßstab hat sich gezeigt, dass bei der Normierung des Tatobjekts das „Eignungsmodell“ vorzugswürdig ist. Insbesondere wurden das „Zweckmodell“, das „Entstehungsmodell“ und das „Marketingmodell“ abgelehnt, da sie auf einer Fehlkonzeption des Gesetzgebers basieren: Sie stützen sich auf Kriterien zur Ermittlung von subjektiven Absichten. Es handelt sich deshalb eigentlich um Abwägungsmaterial aus einer Beweiswürdigung, verpackt in das Gewand eines objektiven Tatbestandsmerkmals – was die Rechtsklarheit unter allen Aspekten erheblich mindert.[14] Während das „Listenmodell“ zwar hohe Effektivität und Effi-

---

[11] Siehe oben Teil 4, I.C.1.f).

[12] Siehe oben Teil 2, III.

[13] Siehe oben Teil 4, I.A.1.

[14] Siehe im Einzelnen oben Teil 4, I.C.1.

zient verspricht, leidet es durch die langen Verweisungsketten an mangelnder Verständlichkeit. Das „ökonomische Modell“ wurde abgelehnt, weil es nur dort effektiv ist, wo wirtschaftliche Beweggründe überhaupt eine Rolle spielen.

In den subjektiven Regelungsmodellen wurde vor allem das Modell der Vorbereitungsdelikte als ineffizient und unverständlich verworfen. Das Modell schafft massive Rechtsunsicherheit; es ist weder klar, ob das Merkmal des Vorbereitens überhaupt eine inhaltliche Bedeutung hat, wenn ja, woran diese anknüpft, wie intensiv der subjektive Bezug vorliegen muss und wie stark der Bezugspunkt konkretisiert sein muss.[15] Als vorzugswürdig wurde die Normierung einer Verwendungsabsicht bewertet, da diese die Effektivität des objektiven „Eignungsmodells“ wahrt, den Tatbestand auf das nötige Maß reduziert und dabei auf etablierte Termini zurückgreift.[16]

III. Lösung durch optimierte Regelungstechniken

Damit ergibt sich, dass ein legitimes und rechtsklares Software-Delikt geschaffen werden kann, wenn ihm das „Eignungsmodell“ und eine Verwendungsabsicht zugrunde gelegt werden. Eine Ausschlussklausel sollte für Verhaltensweisen geschaffen werden, in denen ein IT-Sicherheitsbeauftragter mit dolus eventualis nach dem *Full-Disclosure-Prinzip* vorgeht.

A. Hinwendung zum „Eignungsmodell“

IT-Sicherheitsbeauftragte benötigen für Test-, Analyse- und Demonstrationszwecke Zugriff auf alle potentiell schädlichen Computerprogramme. Es ist gerade ihr Ziel, Angriffe zu simulieren, also sich objektiv so zu verhalten wie ein krimineller Angreifer. Damit liegt es auch in der Natur der Sache, dass sie sich objektiv tatbestandsmäßig verhalten müssen.

IT-Sicherheitsbeauftragte können deshalb auch schon gar kein Interesse daran haben, bereits auf objektiver Tatseite vom Tatbestand ausgeschlossen zu werden. Grenzt man dennoch bestimmte Computerprogramme trotz ihrer deliktischen Verwendbarkeit aus dem objektiven Tatbestand aus, so ist der einzige Effekt, dass diese der Allgemeinheit wieder zur Verfügung stehen – auch zu deliktischen Zwecken.

Zudem hat der Blick ins Kriegswaffen- und Exportkontrollstrafrecht gezeigt, dass im objektiven Tatbestand die Konturen eines subjektiv-normativen Merkmals

---

[15] Siehe oben Teil 4, I.C.2.c)aa) sowie Teil 3, I.C.1.

[16] Siehe oben Teil 4, I.C.2.e) sowie Teil 3, II.C.1.

wie des „Zwecks eines Gegenstands“ auch durch langjährige höchstrichterliche Rechtsprechung kaum zu schärfen sind. Sachgerecht ist es deshalb, konsequent die unmittelbare deliktische Verwendbarkeit (oder: Eignung zur Deliktsbegehung) zum maßgeblichen Kriterium des objektiven Tatbestands zu machen.

B. Normierung einer Verwendungsabsicht

Die Verwendungsabsicht ist das Hauptkriterium, das einen IT-Sicherheitsbeauftragten von einem kriminellen Vorfeldtäter unterscheidet. Denn der IT-Sicherheitsbeauftragte weist eine IT-Schwachstelle mittels *Exploit* als *Proof of Concept* nach, damit diese Schwachstelle geschlossen werden kann. Er will folglich nicht, dass sein *Exploit* zur Begehung von Zieltaten verwendet wird. Ein krimineller Vorfeldtäter hantiert dagegen mit seinem *Exploit*, weil er weiß, dass man damit die Schwachstelle ausnutzen kann, weil er die Zieltat möglicherweise sogar selbst begehen will oder weil er ahnt und billigt, dass ein Dritter seinen *Exploit* zur Ausnutzung einer Schwachstelle verwenden wird. Deshalb ist auf subjektiver Tatseite zu normieren, dass der Täter nur bestraft wird, wenn er in der Absicht oder mit dem Vorsatz handelt, dass das Computerprogramm zur Begehung von Zieltaten verwendet werde.

Welche Vorsatzform hier ausreicht, sollte danach differenziert werden, an welche Tathandlung die Intention geknüpft wird. In Fällen, in denen der Vorfeldtäter die alleinige Kontrolle über das tatgegenständliche Computerprogramm ausübt, sollte dolus directus 1. oder 2. Grades gefordert werden. In Konstellationen, in denen der Vorfeldtäter Dritten die Kontrolle über das tatgegenständliche Computerprogramm einräumt, sollte dagegen einfacher Vorsatz genügen: Insbesondere bei den Tathandlungen des Verkaufens, Vermietens und so weiter wird sich die Absicht des Vorfeldtäters regelmäßig allein auf die erfolgreiche Durchführung des Geschäfts beziehen.[17]

Im Randbereich wird diese Konstruktion freilich dazu führen, dass auch ein IT-Sicherheitsbeauftragter, der einen *Proof of Concept* führt und anderen zugänglich macht, in den Bereich strafrechtlicher Haftung gerät. Denn solange die Sicherheitslücke nicht behoben ist, mag auch hier sein dolus eventualis hinsichtlich einer deliktischen Verwendung des *Proof of Concepts* nicht zu verneinen sein. Für diese Fälle sollte eine Ausschlussklausel normiert werden.

---

[17] Siehe oben Teil 3, II.C.1.b).

C. Normierung einer Ausschlussklausel

Angesichts der teils ausufernden, teils unklaren objektiven und subjektiven Regelungstechniken stünde eigentlich zu erwarten, dass der deutsche Gesetzgeber Ausschlussklauseln einsetzt, um legitime Interessen der IT-Sicherheit nicht zu beeinträchtigen. Während die internationalen Gesetzgeber solche Klauseln verwenden und diese auch im Rüstungskontrollstrafrecht etabliert sind,[18] sind sie im deutschen Software-Strafrecht jedoch nicht vorhanden. In dieser Arbeit wurden sie maßgeblich aus dem Rüstungskontrollrecht gewonnen, verglichen und übertragen.

Um in der soeben genannten Konstellation einen sicheren Tatbestandsausschluss für IT-Sicherheitsbeauftragte zu erreichen, ist eine Freistellungsklausel zu normieren. Als zuverlässig erwies sich im wertenden Vergleich eine Klausel, die den Tatbestand bei einer Handlung ausschließt, die zum Schutz gegen Wirkungen der tatgegenständlichen Computerprogramme oder zur Abwehr dieser Wirkungen geeignet ist und vorgenommen wird.[19] Sie enthält mit dem Ziel des Handelnden eine subjektive Komponente und mit der Eignung eine objektive Komponente. Damit bietet sie IT-Sicherheitsbeauftragten einen zuverlässigen Ausweg aus der Strafbarkeit.

Ein derart optimiertes Software-Delikt gewährleistet so viel Legitimität und Rechtsklarheit, dass es im Wege eines All-Crime-Ansatzes sämtliche bestehenden Software-Delikte vereinheitlichen und ablösen kann. Dabei bietet es sich an, in einem ersten Absatz das tatbestandliche Verhalten, das tatbestandsmäßige Computerprogramm und den subjektiven Bezug zur Zieltat deliktsneutral zu umschreiben. In einem zweiten Absatz könnten dann die Zieldelikte einzeln aufgeführt werden, in deren Vorfeld das Software-Delikt angewendet werden soll. Dadurch kann der Gesetzgeber dessen Geltungsbereich ohne Systembrüche auf andere Deliktsbereiche ausdehnen, sollte dies etwa als Begleiterscheinung des *Ubiquitous Computing* erforderlich werden.[20]

Sobald der Gesetzgeber seine Rechtstechnik in diesem Sinne optimiert, können Software-Delikte tatsächlich einen Beitrag zur Vermeidung von Massenkriminalität und Schwarzmärkten für Schadsoftware leisten. Auch können dann IT-Sicherheitsunternehmen ihrer Arbeit nachgehen, ohne auf den guten Willen der Strafverfolgungsorgane oder einzelner Tatrichter angewiesen zu sein. Auch der Hersteller des WLAN-Sniffers KisMAC wird dann möglicherweise nach Deutschland zurückkehren. Mit In-Kraft-Treten des § 202c StGB hatte dieser nämlich seine Tätigkeiten in Deutschland aufgegeben und seine Server ins Ausland abgezogen.

---

[18] Siehe oben Teil 4, I.B.3.

[19] Siehe oben Teil 4, I.B.4.

[20] Siehe oben Teil 4, II.A.

Glossar

Backdoor	„Hintereingang“ in ein Zielsystem. Ein Hacker, der in ein IT-System eingedrungen ist, kann dort eine Backdoor einrichten, damit er später wieder auf das Zielsystem zugreifen kann, ohne erneut etwaige Sicherheitsmechanismen überwinden zu müssen.
Black-Hat-Hacker	→Hacker, der kriminelle Ziele verfolgt, im Gegensatz zum →White-Hat-Hacker, der sozialnützliche Ziele verfolgt.
Botnet oder Botnetz	Netz von mehreren tausend bis Millionen Einzelcomputern *(Bots)*, die von einem Zentralcomputer (→Command and Control Server) ferngesteuert werden können. Die Einzelcomputer gehören oft Privatpersonen und sind ungewollt und unbemerkt Teil des Botnets geworden, etwa indem Viren oder Würmer in die Privatcomputer eingeschleust wurden.
Brute-Force-Attacke	Methode zum Knacken von Passwörtern. Bei dieser Methode werden alle logisch möglichen Passwörter nacheinander ausprobiert. Die Methode ist deshalb in der Regel sehr rechen- und zeitintensiv.
Chilling Effects	Chilling Effects beschreiben im Bereich der IT-Sicherheit das Phänomen, dass IT-Sicherheitsunternehmen oder →White-Hat-Hacker aus Furcht vor Bestrafung bestimmte (auch offensive) Tätigkeiten aufgeben. Dadurch könnte die Entwicklung von IT-Sicherheitsmaßnahmen verlangsamt werden, sodass die jeweiligen Straftatbestände ihr eigentliches Ziel unterminieren. Der Begriff der Chilling Effects wurde ursprünglich in der US-amerikanischen Grundrechtslehre in der Frage geprägt, ob die Bürger wegen Furcht vor Bestrafung aus Beleidigungstatbeständen großteils auf ihre Meinungsfreiheit verzichten würden.
CIA-Delikte	Delikte gegen die Vertraulichkeit *(Confidentiality)*, die Intergrität *(Integrity)* und die Verfügbarkeit *(Availability)* von Daten.
Codec	Technik, auf die bestimmte Anwendungen zugreifen müssen, damit sie digitale Medien (z.B. Video- oder Audiodaten) wieder geben können. Kofferwort aus ***co****der* und ***dec****oder*.

Command and Control Server	Zentralcomputer *(Server)*, der mit allen Einzelcomputern eines →Botnets verbunden ist. Über diesen Zentralcomputer können Befehle *(command)* an die Bots geschickt und somit das gesamte Botnet kontrolliert *(control)* werden.
CPU	Hauptprozessor, zentrale Verarbeitungseinheit eines Computers *(central processing unit)*.
Crack	Kleines Computerprogramm, das es ermöglicht, ein illegales Exemplar eines konkreten Computerprogramms zu nutzen.
Denial-of-Service-Angriff (auch: DoS-Angriff)	Angriff, bei dem ein Computer über ein Netzwerk mit einem Zielsystem Kontakt aufnimmt, dabei aber sinnlos viele Kontaktanfragen gleichzeitig an das Zielsystem schickt, sodass das Zielsystem mit der Beantwortung dieser vielen simultanen Kontaktanfragen überfordert wird und deshalb gar keine Anfrage mehr beantwortet (also den Dienst *[Service]* verweigert *[denial]*).
DDoS-Angriff	Distributed Denial-of-Service-Angriff.
Distributed Denial-of-Service-Angriff (auch: DDoS-Angriff)	Denial-of-Service-Angriff, bei dem nicht ein einzelner, sondern mehrere tausend bis Millionen Computer gleichzeitig massiv auf das Zielsystem zugreifen.
DoS-Angriff	Denial-of-Service-Angriff.
DRM-System	*Digital Rights Management*-System. Teil eines kommerziellen Computerprogramms, der technisch sicherstellt, dass der Nutzer das Computerprogramm nur zu Zwecken benutzt, zu denen er eine Lizenz erworben hat.
EEPROM	Speicherbaustein in elektrischen Geräten *(Electrically Erasable Programmable Read-Only Memory)*.
Exploit	Computerprogramm, das eine Schwachstelle auf einem Zielsystem ausnutzt *(exploit)*.
Filehoster	Anbieter von Speicherplatz im Internet. Nutzer können hier Daten hochladen und erhalten im Gegenzug einen Link, unter dem die Daten wieder heruntergeladen werden können. Wird dieser Link an Dritte weitergegeben, können auch diese die Daten herunterladen.
Firmware	Software zum Betrieb eines elektrischen Geräts. Im Vergleich zu einem Betriebssystem ist die Firmware fester mit dem Gerät verbunden, kann also nicht so einfach ausgetauscht werden.
Fix	Meist kleine Dateien oder Programme, die es ermöglichen, ein illegales Exemplar eines kommerziellen Computerprogramms trotz dessen Kopierschutzmechanismen zu nutzen.
FTA-Receiver	Empfangsgerät für Pay-TV *(Free-to-air)*.

FTP	Technik für die Übermittlung von Dateien im Internet *(File Transfer Protocol)*. Während man beim HTTP *(Hypertext Transfer Protocol)* typischerweise einen Browser verwendet, um Webseiten des WWW *(World Wide Web)* darzustellen, verwendet man beim FTP kleine Programme, um einen FTP-Server direkt anzusteuern und etwa sein Dateiverzeichnis zu durchstöbern sowie Dateien hoch- oder herunterzuladen.
Full-Disclosure-Prinzip	Verhaltensregel in der IT-Sicherheitsbranche: Eine entdeckte Schwachstelle soll umfassend *(full)* bekanntgemacht *(disclosure)* werden, damit so der Zeitdruck auf denjenigen steigt, der die Schwachstelle – etwa durch ein Update – beheben kann.
Hack	In der Informationstechnik gebrauchter Begriff, der bei wertungsfreier Verwendung bedeutet, ein Ziel auf einem nicht dafür vorgesehenen Wege zu erreichen.
Hacker	Jemand, der einen →Hack ausführt.
Hacking	Das Ausführen von →Hacks.
Hacking-Tool	Computerprogramm, das einen Hack ermöglicht, erleichtert oder ganz oder teilweise durchführt.
Hash	Zeichenfolge mit fester Länge, die nach einer bestimmten mathematischen Formel aus einem Passwort mit beliebiger Länge gebildet wird. Das Passwort wird also „maskiert“. So können Hashfunktionen dazu dienen, in Datenbanken die Original-Passwörter zu verschleiern. Es wird dann nicht das Passwort selbst, sondern nur sein Hashwert in der Datenbank abgelegt.
I/O	Kommunikationsschnittstelle *(Input/Output)*, über die ein →IT-System mit dem Benutzer oder anderen IT-Systemen kommuniziert.
IT-System	System, das auf Informationstechnik (IT; Computertechnik) basiert. Also etwa PCs, Laptops, Tablets, Handys, aber auch bspw. Steuerelemente von Industrieanlagen (sog. Speicherprogrammierbare Steuerungen, englisch: PLC), und digitaler Unterhaltungselektronik wie Fernseher, WLAN-Radios etc.
Keygen	Computerprogramm, das Seriennummern *(Keys)* generiert *(gen)* und damit dem Nutzer ermöglicht, die Schutzfunktion der Seriennummernabfrage bei der Installation eines kommerziellen Computerprogramms mit einer „falschen Nummer“ ins Leere laufen zu lassen.
Layer Break Flag	Die Layer Break Flag signalisiert *(Flag)* einem DVD-Player, dass er am Ende einer Schicht *(Layer)* der DVD

	angekommen ist und deshalb in die nächste Schicht springen *(Break)* und dort weiterlesen soll. Als Kopierschutz können Original-DVDs so hergestellt werden, dass die Layer Break Flag der Original-DVD bei einem Brennvorgang falsch auf die kopierte DVD übernommen wird. Ein herkömmlicher DVD-Player wird dann beim Abspielen der kopierten DVD an falschen Stellen in falsche Schichten springen, sodass beispielsweise ein Film auf der DVD nicht ordnungsgemäß abgespielt werden kann.
P2P-Netzwerk (auch: Peer-to-peer-Netzwerk)	Netzwerk, in dem alle Teilnehmer gleichrangig *(peer)* sind. P2P-Netzwerke können eingerichtet werden, um Daten untereinander zugänglich zu machen. Grundsätzlich kann in solchen Netzwerken jeder von jedem Daten kopieren. Dies gewährleistet, dass die Daten nicht auf einem zentralen Server liegen, wo sie relativ einfach gelöscht oder unzugänglich gemacht werden könnten.
Patch	Update zu einem Computerprogramm, das der Nutzer im Nachhinein installieren kann, etwa um Schwachstellen oder Fehlfunktionen des Programms zu beheben. Häufig wird eine Schwachstelle in einem Computerprogramm (Microsoft Windows, Adobe Flash Player, etc.) bekannt, kurz darauf veröffentlicht der Hersteller (Microsoft, Adobe, etc.) einen Patch, den der Nutzer herunterladen und installieren kann, um die Schwachstelle auf seinem Computer zu schließen.
Patch-Level	Das Patch-Level besagt, wie viele der verfügbaren →Patches auf ein System aufgespielt wurden. Installiert ein Nutzer nicht alle verfügbaren Patches, so hat sein IT-System ein niedrigeres Patch-Level, weist also u.U. bekannte Schwachstellen auf und kann leichter kompromittiert werden.
Penetration Testing	Angriffssimulation, bei der ein IT-Sicherheitsbeauftragter in die Rolle eines Angreifers schlüpft und überprüft *(test)*, ob man von außen in das Zielsystem eindringen *(penetration)* kann.
Port	Schnittstelle, über die ein IT-System in Netzwerken Daten sendet oder empfängt.
Proof of Concept	Nachweis, dass eine bestimmte Sicherheitslücke auf eine bestimmte Art ausgenutzt werden kann. Häufig werden Sicherheitslücke und potentieller Angriff nicht nur theoretisch beschrieben, sondern auch praktisch demonstriert, etwa indem ein entsprechendes Angriffs-Programm geschrieben und verfügbar gemacht wird.
RAM	Arbeitsspeicher eines Computers *(Random-access memory)*.

Ripper	Computerprogramm, das eine Kopie von einer kopiergeschützten CD/DVD/BD anfertigen kann.
ROM	Nichtflüchtiger Speicher in einem Computer, auf den grundsätzlich nur ein Lesezugriff möglich ist *(Read-only memory)*.
Rootkit	→Exploit, der nicht nur eine Schwachstelle auf dem Zielsystem ausnutzt, sondern dem Verwender auch vollen Zugriff *(root)* auf das Zielsystem einräumt.
Sandbox	Testumgebung (etwa auf einem Computer), die vollkommen nach außen abgeschottet ist. Durch die Sandbox stellt man sicher, dass keine ungewollten Gefährdungen nach außen treten können, während man etwa zu Analysezwecken „in der Sandbox" Schadensroutinen ungehemmt ablaufen lässt.
Sharehoster	→Filehoster.
Smart-Card	Chipkarte, die ein Pay-TV-Nutzer zur Autorisierung in einen →FTA-Receiver steckt, der sodann das verschlüsselte Fernsehsignal entschlüsselt an den Fernseher weitergibt.
Tool	→Hacking-Tool.
Torrents	Kleine Dateien, in denen ein →P2P-Netzwerk verzeichnet ist, in dem der Nutzer konkrete Daten bekommt. Möchte ein Nutzer etwa einen aktuellen Kinofilm herunterladen, kann er sich die entsprechende Torrent-Datei für diesen Film besorgen, sich in das Torrent-Netzwerk einbinden und den Film von den verzeichneten Netzwerkteilnehmern herunterladen. Dabei können einzelne Datenpakete von verschiedenen Netzwerkteilnehmern heruntergeladen und auf dem Empfängerrechner zusammengesetzt werden. Die Torrent-Technik ist so konfiguriert, dass der Nutzer alle Datenfragmente, die er heruntergeladen hat, gleichzeitig auch anderen Netzwerkteilnehmern zur Verfügung stellt.
Ubiquitous Computing	Schlagwort, das ausdrücken soll, dass Informationstechnik im Alltag allgegenwärtig wird, etwa weil jeder alltägliche Gegenstand mit Computertechnik angereichert wird. Auch „Internet der Dinge" genannt.
Usenet	Netzwerk innerhalb des Internets. Das Usenet besteht nicht aus Webseiten, die mit herkömmlichen Browsern durchstöbert werden können, sondern aus „Newsgroups" die direkt durch „Newsreader" angesteuert werden müssen. Im Usenet können auch Dateien übertragen werden.
White-Hat-Hacker	→Hacker, der sozialnützliche Ziele verfolgt, im Gegensatz zum →Black-Hat-Hacker, der kriminelle Ziele verfolgt.

Workaround	Anleitung zur vorläufigen Behebung einer Sicherheitslücke.
Zero-Day-Exploit	→Exploit, der eine noch unbekannte Sicherheitslücke ausnutzt. Die Sicherheitslücke ist seit Null *(zero)* Tagen *(day)* bekannt.

Literaturverzeichnis

Aharoni, Mati/Kearns, Devon/Kennedy, David/O'Gorman, Jim, Metasploit. Die Kunst des Penetration Testing. Heidelberg u.a. 2012.

Albrecht, Frank, Begleitetes Fahren mit 17 und neue Straftatbestände im Straßenverkehrsgesetz. SVR 2005, 281–286.

Anastasopoulou, Ioanna, Deliktstypen zum Schutz kollektiver Rechtsgüter. München 2005.

Appel, Ivo, Verfassung und Strafe. Zu den verfassungsrechtlichen Grenzen staatlichen Strafens. Berlin 1998.

Arlt, Christian, Digital Rights Management Systeme. Der Einsatz technischer Maßnahmen zum Schutz digitaler Inhalte. München 2006.

Arnold, Bernhard, Rechtmäßige Anwendungsmöglichkeiten zur Umgehung von technischen Kopierschutzmaßnahmen? MMR 2008, 144–148.

– Das Verbot von Umgehungsmitteln. § 95a UrhG erstmals auf dem Prüfstand beim BGH. NJW 2008, 3545–3546.

– Die Gefahr von Urheberrechtsverletzungen durch Umgehungsmittel nach Wettbewerbsrecht und Urheberrecht. Zum rechtlichen Schutz technischer Maßnahmen zum Schutz vor Urheberrechtsverletzungen. Frankfurt a.M. 2006.

Auer, Günter, Rechtsschutz für technischen Schutz im Gemeinschaftsrecht. In: Helmuth Tades (Hrsg.), Ein Leben für Rechtskultur. Festschrift für Robert Dittrich zum 75. Geburtstag. Wien 2000.

Bär, Wolfgang/Hoffmann, Helmut, Das Zugangskontrolldiensteschutz-Gesetz. Ein erster Schritt auf dem richtigen Weg. MMR 2002, 654–658.

Beck, Volker, Dual-Use-Problematik und Verhaltenskodex. BIOspektrum 2011, 239–240.

Berinato, Scott, Software Vulnerability Disclosure: The Chilling Effect. CSO Magazine, Ausgabe 1/2007, 18–25. Online abrufbar unter http://www.csoonline.com/article/221113/software-vulnerability-disclosure-the-chilling-effect [Stand: 1.1.2007; zuletzt abgerufen am 16.11.2014].

Bernnat, Rainer et al., Die IT-Sicherheitsbranche in Deutschland. Aktuelle Lage und ordnungspolitische Handlungsempfehlungen. Online veröffentlicht unter http://bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheitsbranche-de-aktuelle-lage,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf [Stand: Februar 2010; zuletzt abgerufen am 16.11.2014].

Bieneck, Klaus, Der Schutz der auswärtigen Beziehungen Deutschlands durch das Außenwirtschaftsrecht. Zugleich Anmerkungen zum Beschluss des BGH vom 13.1.2009. wistra 2011, 89–96.

Bieneck, Klaus, Die militärische Konstruktion im Außenwirtschaftsrecht. Die Auslegungshistorie des Begriffs „besonders konstruiert für militärische Zwecke" im internationalen Kontext. wistra 2010, 10–17.

– Catch-All im Strafrecht. Die Kriminalisierung der Ausfuhr ungelisteter Dual-Use-Güter im Außenwirtschaftsrecht. wistra 2008, 208–213.

Binding, Karl, Die Normen und ihre Übertretung, Band I: Normen und Strafgesetze. 1. Aufl. Leipzig 1872.

Birnbaum, Johann Michael Franz, Ueber das Erforderniß einer Rechtsverletzung zum Begriffe des Verbrechens. Archiv des Kriminalrechts, Neue Folge 1834, 149–194.

Borges, Georg/Stuckenberg, Carl-Friedrich/Wegener, Christoph, Bekämpfung der Computerkriminalität. Zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität. DuD 2007, 275–278.

Brodowski, Dominik/Freiling, Felix C., Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Online veröffentlicht unter http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf [Stand: März 2011; zuletzt abgerufen am 16.11.2014].

Bundesamt für Sicherheit in der Informationstechnik, Durchführungskonzept für Penetrationstests, online veröffentlicht unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest_pdf.pdf?__blob=publicationFile [Stand: November 2003; zuletzt abgerufen am 16.11.2014].

– IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, 1992. Online als gezippte HTM-Version veröffentlicht unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sicherheitshandbuch/sichhandbuch_zip.zip?__blob=publicationFile [Stand: 1992; zuletzt abgerufen am 14.5.2012].

Bundeskriminalamt, Cybercrime Bundeslagebild 2010. Online abrufbar unter http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf [Stand: 2011; zuletzt abgerufen am 14.5.2012].

Bung, Jochen, Wissen und Wollen im Strafrecht. Frankfurt a.M. 2009.

Bunzel, Michael, Die Potenz des verfassungsrechtlichen Verhältnismäßigkeitsprinzips als Grenze des Rechtsgüterschutzes in der Informationsgesellschaft. In: Roland Hefendehl (Hrsg.), Die Rechtsgutstheorie. Baden-Baden 2003, S. 96–118.

Canellopoulou-Bottis, Maria, Disclosing Software Vulnerabilities. In: Kenneth Einar Himma (Hrsg.), Internet Security: Hacking, Counterhacking and Society. Sudbury 2007, S. 255–268.

Chiampi Ohly, Diana D., SoftwareRecht: Von der Entwicklung zum Export. Frankfurt a.M. 2010.

Cornelius, Kai, Zur Strafbarkeit des Anbietens von Hackertools. Was nach dem 41. Strafrechtsänderungsgesetz noch für die IT-Sicherheit getan werden darf. CR 2007, 682–688.

Dahm, Georg [Begr.], Völkerrecht, Band I/3: Die Formen des völkerrechtlichen Handelns; Die inhaltliche Ordnung der internationalen Gemeinschaft. 2. Aufl. Berlin 2002.

Deckers, Rüdiger, Strafbarkeit terroristischer Vorbereitungshandlungen. Rechtsstaatlich nicht tragbar. ZRP 2008, 169–173.

Dölling, Dieter/Duttge, Gunnar/Rössner, Dieter (Hrsg.), Gesamtes Strafrecht. Handkommentar. StGB, StPO, Nebengesetze. 2. Aufl. Baden-Baden 2011. Zit.: Dölling/Duttge/Rössner-*Bearbeiter*.

Dreier, Thomas, Die Umsetzung der Urheberrechtsrichtlinie 2001/29/EG in deutsches Recht. ZUM 2002, 28–43.

Dreier, Thomas/Schulze, Gernot (Hrsg.), Urheberrechtsgesetz: UrhG. Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz. Kommentar. 3. Aufl. München 2008.

Dressel, Christian/Scheffler, Hauke (Hrsg.), Rechtsschutz gegen Dienstepiraterie. Das ZKDSG in Recht und Praxis. München 2003. Zit.: *Bearbeiter*, in: Dressel/Scheffler, ZKDSG.

Dreyer, Gunda/Kotthoff, Jost/Meckel, Astrid (Hrsg.), Urheberrecht, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz. (Heidelberger Kommentar) 2. Aufl. Heidelberg u.a. 2009. Zit.: Dreyer/Kotthoff/Meckel-*Bearbeiter*.

Duttge, Gunnar, Vorbereitung eines Computerbetrugs. Auf dem Weg zu einem „grenzenlosen" Strafrecht. In: Bernd Heinrich (Hrsg.), Festschrift für Ulrich Weber zum 70. Geburtstag, 18. September 2004. Bielefeld 2004, S. 285–310.

– Zur Bestimmtheit des Handlungsunwerts von Fahrlässigkeitsdelikten. Tübingen 2001.

Enders, Theodor, Digital Rights Management Systeme (DRMS) als besondere Herausforderung an das Urheberrecht. ZUM 2004, 593–605.

Entelmann, Lars, Das Verbot von Vorbereitungshandlungen zur Umgehung technischer Schutzmaßnahmen. Baden-Baden 2009.

Erbs, Georg (Begr.)/*Kohlhaas, Max* u.a. (Hrsg.), Strafrechtliche Nebengesetze. Loseblattsammlung, Stand: 187. Ergänzungslieferung, München 2011. Zit.: Erbs/Kohlhaas-*Bearbeiter*.

Ernst, Stefan, Computerstrafrecht 2007. DS 2007, 335–340.

– Das neue Computerstrafrecht. NJW 2007, 2661–2666.

– Kopierschutz nach neuem UrhG. Bedeutung und Tragweite des Verbots von Umgehungsmaßnahmen und Hacking-Werkzeugen für die Praxis. CR 2004, 39–43.

Ewaida, Bashar, Pass-the-hash attacks: Tools and Mitigation. Online veröffentlicht unter http://www.sans.org/reading_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation_33283 [Stand 21.1.2010; zuletzt abgerufen am 16.11.2014].

Fischer, Thomas, Strafgesetzbuch und Nebengesetze. Mit Straf- und Bußgeldvorschriften des Wirtschafts- und Verwaltungsrechts 58. Aufl. München 2011.

Fitz-Maurice, Ernestine, Convention for the Suppression of Counterfeiting Currency. An Analysis. 26 Am. J. Int'l L., 1932, 533–551.

Fox, Dirk, Realisierung, Grenzen und Risiken der „Online-Durchsuchung". DuD 2007, 827–834.

Frenz, Walter, Handbuch Europarecht, Bd. 6: Institutionen und Politiken. Berlin u.a. 2011.

Frisch, Wolfgang, Rechtsgut, Recht, Deliktsstruktur und Zurechnung im Rahmen der Legitimation staatlichen Strafens. In: Roland Hefendehl (Hrsg.), Die Rechtsgutstheorie. Baden-Baden 2003, S. 215–238.

Frisch, Wolfgang, An den Grenzen des Strafrechts. In: Wilfried Küper/Walter Stree/Johannes Wessels (Hrsg.), Festschrift für Walter Stree und Johannes Wessels zum 70. Geburtstag. Heidelberg 1993, S. 69–106.

– Tatbestandsmäßiges Verhalten und Zurechnung des Erfolgs. Heidelberg 1988.

Fromm, Friedrich Karl/Nordemann, Wilhelm (Hrsg.), Urheberrecht. Kommentar zum Urheberrechtsgesetz, Verlagsgesetz, Urheberrechtswahrnehmungsgesetz. 10. Aufl. Stuttgart 2008. Zit.: Fromm/Nordemann-*Bearbeiter*.

Gazeas, Nikolaos/Grosse-Wilde, Thomas/Kießling, Alexandra, Die neuen Tatbestände im Staatsschutzstrafrecht – Versuch einer ersten Auslegung der §§ 89a, 89b und 91 StGB. NStZ 2009, 593–604.

Gehrig, Klaus, Der Absichtsbegriff in den Straftatbeständen des Besonderen Teils des StGB. Berlin 1986.

Gercke, Marco, Die Cybercrime Konvention des Europarats. CR 2004, 782–791.

Gercke, Marco/Brunst, Phillip W., Praxishandbuch Internetstrafrecht. Stuttgart 2009.

Gierhake, Katrin, Zur geplanten Einführung neuer Straftatbestände wegen der Vorbereitung terroristischer Straftaten. ZIS 2008, 397–405.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union. Kommentar (Loseblatt-Sammlung), Band II, München 2009. Zit.: Grabitz/Hilf-*Bearbeiter*.

Gröseling, Nadine/Höfinger, Frank, Computersabotage und Vorfeldkriminalisierung. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität. MMR 2007, 626–630.

Gruber, Urs Peter, Methoden des internationalen Einheitsrechts. Tübingen 2004.

Grunst, Bettina, Moderne Gesetzestechniken in StGB und StPO aus kritischer Sicht der juristischen Methodenlehre. GA 2002, 214–227.

Gutman, Daniel, Rechtliche Flankierung technischer Schutzmöglichkeiten. K&R 2003, 491–496.

Haedicke, Maximilian, Die Umgehung technischer Schutzmaßnahmen durch Dritte als mittelbare Urheberrechtsverletzung. In: Ganea, Peter (Hrsg.), Urheberrecht gestern – heute – morgen. Festschrift für Adolf Dietz zum 65. Geburtstag. München 2001, S. 349–364.

Hassemer, Ines M./Ingeberg, Thorsten, Dual-Use-Software aus der Perspektive des Strafrechts (§ 202c StGB). ITRB 2009, 84–87.

Hassemer, Winfried, Sicherheit durch Strafrecht. HRRS 2006, 130–143.

– Strafrecht, Prävention, Vergeltung. ZIS 2006, 266–273.

Hecker, Bernd, Europäisches Strafrecht. 3. Aufl. Berlin, Heidelberg 2010.

Heger, Martin, Fünf Jahre §§ 152a Abs. 2, 263a Abs. 3 StGB: Ein Plädoyer für die Korrektur handwerklicher Mängel bei der innerstaatlichen Umsetzung von EU-Vorgaben. ZIS 2008, 496–499.

Hefendehl, Roland, Der fragmentarische Charakter des Strafrechts. JA 2011, 401–407.

– Über die Pönalisierung des Neutralen – zur Sicherheit. In: Roland Hefendehl (Hrsg.), Grenzenlose Vorverlagerung des Strafrechts? Berlin 2010, S. 89–105.

– Kollektive Rechtsgüter im Strafrecht. Köln u.a. 2002.

Hegel, Georg Wilhelm Friedrich, Logik für die Mittelklasse des Gymnasiums. Nürnberg 1810/1811.

Heinrich, Bernd, Die Grenzen des Strafrechts bei der Gefahrprävention. Brauchen oder haben wir ein „Feindstrafrecht"? ZStW 121 (2009), 94–130.

Heintschel-Heinegg, Bernd von (Hrsg.), Beck'scher Online-Kommentar StGB. Edition 14, München 2011. Zit.: BeckOK-*Bearbeiter*.

Herbert, Sarah, Grenzen des Strafrechts bei der Terrorismusgesetzgebung. Berlin 2013.

Hilgendorf, Eric/Frank, Thomas/Valerius, Brian, Computer- und Internetstrafrecht. Berlin, Heidelberg 2005.

Hilty, Reto, Urheberrecht in der Informationsgesellschaft: „Wer will was von wem woraus?". Ein Auftakt zum „zweiten Korb". ZUM 2003, 983–1006.

Hirsch, Andrew von/Wohlers, Wolfgang, Rechtsgutstheorie und Deliktsstruktur. Zu den Kriterien fairer Zurechnung. In: Roland Hefendehl (Hrsg.), Die Rechtsgutstheorie, Baden-Baden 2003, S. 196–214.

Hirsch, Hans Joachim, Tatstrafrecht – ein hinreichend beachtetes Grundprinzip? In: Cornelius Prittwitz u.a. (Hrsg.), Festschrift für Klaus Lüderssen. Zum 70. Geburtstag am 2. Mai 2002. Baden-Baden 2002, S. 253–268.

– Der Streit um Handlungs- und Unrechtslehre, insbesondere im Spiegel der Zeitschrift für die gesamte Strafrechtswissenschaft. ZStW 93 (1981), 831–863.

Hoeren, Thomas, Entwurf einer EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft. Überlegungen zum Zwischenstand der Diskussion. MMR 2000, 515–521.

Höfinger, Frank, Anmerkung zu BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07. ZUM 2009, 751–753.

Holzner, Stefan, Klarstellung strafrechtlicher Tatbestände durch den Gesetzgeber erforderlich. ZRP 2009, 177–178.

Hörnle, Tatjana, Das Verbot des Geschwisterinzests. Verfassungsgerichtliche Bestätigung und verfassungsrechtliche Kritik. NJW 2008, 2085–2088.

Hoyer, Andreas, Die Eignungsdelikte. Berlin 1987.

Husemann, Stephan, Die Verbesserung des strafrechtlichen Schutzes des bargeldlosen Zahlungsverkehrs durch das 35. Strafrechtsänderungsgesetz. NJW 2004, 104–109.

Ipsen, Knut, Völkerrecht. 5. Aufl. München 2004.

Jakobs, Günther, Terroristen als Personen im Recht? ZStW 117 (2006), 839–851.

– Kriminalisierung im Vorfeld einer Rechtsverletzung. ZStW 97 (1985), 751–785.

Jaeckel, Liv, Risiko-Signaturen im Recht. Zur Unterscheidbarkeit von Gefahr und Risiko. JZ 2011, 116–124.

Jhering, Rudolph von, Der Zweck im Recht. 4. Aufl. Leipzig 1904.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Münchener Kommentar zum Strafgesetzbuch. Band 2/1 München 2005; Band 3/1 München 2012; Band 3/2 München 2003; Band 5 München 2007. Zit.: MK-*Bearbeiter*.

Jung, Heike, Konturen und Perspektiven des europäischen Strafrechts. JuS 2000, 417–424.

Kalinowski, Martin B., Zivil-militärisches Dual-use am Beispiel des iranischen Nuklearprogramms. Online veröffentlicht unter http://www.znf.uni-hamburg.de/Folien230408.pdf [Stand: 23.4.2008; zuletzt abgerufen am 14.5.2012].

Kauder, Siegfried, Strafbarkeit terroristischer Vorbereitungshandlungen. Erwiderung zu Deckers/Heusel, ZRP 2008, 169. ZRP 2009, 20–21.

Kersten, Heinrich/Reuter, Jürgen/Schröder, Klaus-Werner, IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung. 2. Aufl. Wiesbaden 2009.

Kindhäuser, Urs, Gefährdung als Straftat. Rechtstheoretische Untersuchungen zur Dogmatik der abstrakten und konkreten Gefährdungsdelikte. Frankfurt a.M. 1989.

Kindhäuser, Urs u.a. (Hrsg.), Strafgesetzbuch. NomosKommentar Band 2 §§ 146–358. 3. Aufl. Baden-Baden 2010. Zit.: NK-*Bearbeiter*.

Kluge, Friedrich, Etymologisches Wörterbuch der deutschen Sprache. 24. Aufl. Berlin, New York 2002.

Kohler-Gehrig, Eleonora, Europarecht und nationales Recht. Auslegung und Rechtsfortbildung. JA 1998, 807–812.

Koriath, Heinz, Zum Streit um die Gefährdungsdelikte. GA 2001, 51–74.

Kruth, Wilhelm, Grundlagen der Informationstechnik. Kompaktwissen für Datenschutz- und Security-Management. 3. Aufl. Heidelberg u.a. 2009.

Kühl, Kristian, Strafgesetzbuch. Kommentar. 27. Aufl. München 2011. Zit.: Lackner/*Kühl*.

Kröger, Detlef, Die Urheberrechtsrichtlinie für die Informationsgesellschaft. Bestandsaufnahme und kritische Bewertung. CR 2001, 316–324.

Kudlich, Hans/Christensen, Ralph, Wortlaut, Wörterbuch und Wikipedia – wo findet man die Wortlautgrenze? JR 2011, 146–151.

Ladeur, Karl-Heinz/Gostomzyk, Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäußerungen in Blogs. Geht die große Zeit des privaten Presserechts im Internet zu Ende? NJW 2012, 710–716.

Ladner, Ralf/Schillo, Franz-Josef, Neues zum Hackerparagrafen. Online veröffentlicht unter http://www.crn.de/service/recht/artikel-80263.html [Stand 25.2.2010; zuletzt abgerufen am 14.5.2012].

Lagodny, Otto, Strafrecht vor den Schranken der Grundrechte. Tübingen 1996.

Leisner, Walter Georg, Die subjektiv-historische Auslegung des Gemeinschaftsrechts. Der „Wille des Gesetzgebers" in der Judikatur des EuGH. EuR 2007, 689–707.

Lenckner, Theodor, Zum Begriff der Täuschungsabsicht in § 267 StGB. NJW 1967, 1890–1895.

Lesch, Heiko, Die Begründung mittäterschaftlicher Haftung als Moment der Zurechnung. ZStW 105 (1993), 271–294.

Leupold, Andreas/Glossner, Silke (Hrsg.), Münchener Anwaltshandbuch IT-Recht. 2. Aufl. München 2011. Zit.: Leupold/Glossner-*Bearbeiter*.

Lindner, Felix, Stellungnahme zum Gesetzentwurf der Bundesregierung zu einem Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (BT-Drucks. 16/3656). Online veröffentlicht unter http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/straendg_computer/Stellungnahme_Lindner.pdf [Stand: 19.3.2007; zuletzt abgerufen am 16.11.2014].

Lüderssen, Klaus, Das Strafrecht zwischen Funktionalismus und „alteuropäischem" Prinzipiendenken. ZStW 107 (1995), 877–906.

Luhmann, Niklas, Zweckbegriff und Systemrationalität. Frankfurt a.M. 1973.

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian (Hrsg.), Kommentar zum Grundgesetz: GG, Band 2. 6. Aufl. München 2010. Zit.: von Mangoldt/Klein/Starck-*Bearbeiter*.

Marberth-Kubicki, Annette, Computer- und Internetstrafrecht. 2. Aufl. München 2010.

Martinek, Michael (Hrsg.), Handbuch des Vertriebsrechts. 3. Aufl. München 2010. Zit.: Martinek/Semler/Habermeier/Flohr-*Bearbeiter*.

Mattern, Friedemann, Ubiquitous Computing: Schlaue Alltagsgegenstände. Die Vision von der Informatisierung des Alltags. Online veröffentlicht unter http://www.vs.inf.ethz.ch/publ/papers/mattern2004_sev.pdf [Stand: 17.9.2004; zuletzt abgerufen am 16.11.2014].

Maunz, Theodor/Dürig, Günter [Begr.], Grundgesetz Kommentar. 63. Lieferung München 2011. Zit.: Maunz/Dürig-*Bearbeiter*.

Mayer, Hans-Peter, Richtlinie 2001/29/EG zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft. EuZW 2002, 325–329.

Mayer-Wegelin, Clemens, Käuferrechte bei Computerspielen. Technische Kopierschutzmaßnahmen und End User License Agreements. JurPC Web-Dok. 28/2009, Abs. 1–175.

Meschede, Thomas, Der Schutz digitaler Musik- und Filmwerke vor privater Vervielfältigung nach den zwei Gesetzen zur Regelung des Urheberrechts in der Informationsgesellschaft. Frankfurt a.M. u.a. 2006.

Minhardt, Klaus, Windows kollidiert mit Urheberrecht. Spiegel-Online vom 22.10.2003. Online veröffentlicht unter http://www.spiegel.de/netzwelt/web/0,1518,270719,00.html [Stand: 22.10.2003; zuletzt abgerufen am 16.11.2014].

Mink, Martin, Ist Angriff besser als Verteidigung? Der richtige Weg für IT-Sicherheitsausbildung. Online veröffentlicht unter http://pi1.informatik.uni-mannheim.de/filepool/publications/BSI-Kongress2007_Mink.pdf [Stand: 2007; zuletzt abgerufen am 14.5.2012].

Müller, Klaus-Rainer, IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement, Sicherheitspyramide, Standards und Practices, SOA und Softwareentwicklung. 4. Aufl. Wiesbaden 2011.

Muncan, Michael/Schreiber, Sebastian, Interne Penetrationstests. Sicherheitstests im Firmennetz. DuD 2009, 218–221.

Mylonopoulos, Christos, Internationalisierung des Strafrechts und Strafrechtsdogmatik. Legitimationsdefizit und Anarchie als Hauptcharakteristika der Strafrechtsnormen mit internationalem Einschlag. ZStW 121 (2009), 68–93.

Nestler, Cornelius, Rechtsgüterschutz und Strafbarkeit des Besitzes von Schusswaffen und Betäubungsmitteln. In: Peter-Alexis Albrecht (Hrsg.), Vom unmöglichen Zustand des Strafrechts. Frankfurt a.M. 1995, S. 65–77.

Pawlik, Michael, Der Terrorist und sein Recht. Zur rechtstheoretischen Einordnung des modernen Terrorismus. München 2008.

Pleister, Christian C.-W./Ruttig, Markus, Neues Urheberrecht – neuer Kopierschutz. Anwendungsbereich und Durchsetzbarkeit des § 95a UrhG. MMR 2003, 763–767.

Pohl, Hartmut, Zur Technik der heimlichen Online-Durchsuchung. DuD 2007, 684–688.

Popp, Andreas, Informationstechnologie und Strafrecht. JuS 2011, 385–392.

– § 202c StGB und der neue Typus des europäischen Software-Delikts. GA 2008, 375–393.

– Computerstrafrecht in Europa. MR-Int 2007, 84–88.

Prechtl, Peter/Burkard, Franz-Peter (Hrsg.), Metzler-Philosophie-Lexikon. Stuttgart/Weimar 1996.

Puschke, Jens, Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte. In: Roland Hefendehl (Hrsg.), Grenzenlose Vorverlagerung des Strafrechts? Berlin 2010, S. 9–39.

Rackow, Peter, Strafrechtliche Terrorismusbekämpfung durch Pönalisierung von Vorbereitungshandlungen. In: René Bloy et al. (Hrsg.), Gerechte Strafe und legitimes Strafrecht: Festschrift für Manfred Maiwald zum 75. Geburtstag. Berlin 2010, S. 615–641.

– Neutrale Handlungen als Problem des Strafrechts. Frankfurt a.M. u.a. 2007.

Radtke, Henning/Steinsiek, Mark, Bekämpfung des internationalen Terrorismus durch Kriminalisierung von Vorbereitungshandlungen? – Zum Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren Gewalttaten (Referentenentwurf des BMJ vom 21.4.2008). ZIS 2008, 383–396.

Redeker, Helmut, IT-Recht. 4. Aufl. München 2004.

Regenbogen, Arnim/Meyer, Uwe (Hrsg.), Wörterbuch der philosophischen Begriffe. Hamburg 1998.

Renzikowski, Joachim, Restriktiver Täterbegriff und fahrlässige Beteiligung. Tübingen 1997.

Rheinbote, Jörg, Die EG-Richtlinie zum Urheberrecht in der Informationsgesellschaft. GRUR-Int 2001, 733–745.

Roxin, Claus, Strafe und Strafzwecke in der Rechtsprechung des Bundesverfassungsgerichts. In: Hassemer et al. (Hrsg.), In dubio pro libertate – Festschrift für Klaus Volk zum 65. Geburtstag. München 2009, S. 601–616.

– Strafrecht Allgemeiner Teil Band I, Grundlagen – Der Aufbau der Verbrechenslehre. 4. Aufl. München 2006.

Rudolphi, Hans-Joachim, Primat des Strafrechts im Umweltschutz? NStZ 1984, 248–254.

Rudolphi, Hans-Joachim (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch. Loseblatt-Ausgabe München/Unterschleißheim 2009. Zit.: *Bearbeiter*, in: SK-StGB.

Sachs, Michael [Begr.], Grundgesetz Kommentar. 6. Aufl. München 2011. Zit.: Sachs-*Bearbeiter*.

Schäfer, Janina, Die kartellrechtliche Kontrolle des Einsatzes von technischen Schutzmaßnahmen im Urheberrecht. Bern 2008.

Schall, Hero, Umweltschutz durch Strafrecht: Anspruch und Wirklichkeit. NJW 1990, 1263–1273.

Scheffler, Uwe, Strafgesetzgebungstechnik in Deutschland und Europa. ZStW 117 (2006), 766–800.

Schippan, Martin, § 95a UrhG – eine Vorschrift (erstmals richtig) auf dem Prüfstand. Zugleich Anmerkung zu LG Frankfurt a.M., Urteil vom 31. Mai 2006. ZUM 2006, 853–864.

Schlegel, Volker/Schanze, Gwenn, Compliance in der Außenwirtschaft: Exportkontrolle. In: Gregor Wecker/Hendrik van Laak (Hrsg.), Compliance in der Unternehmerpraxis. 2. Aufl. Wiesbaden 2009.

Schneier, Bruce, America's Dilemma: Close Security Holes, or Exploit Them Ourselves, wired.com vom 1.5.2008. Online veröffentlicht unter http://archive.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0501 [Stand: 1.5.2008; zuletzt abgerufen am 15.11.2014].

Schönke, Klaus/Schröder, Horst, Strafgesetzbuch. 28. neu bearb. Aufl. von Albin Eser. München 2010. Zit.: Schönke/Schröder-*Bearbeiter*.

Schreibauer, Marcus/Hessel, Tobias J., Das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität. K&R 2007, 616–620.

Schreiber, Sebastian, Kosten und Nutzen von Penetrationstests. HMD Heft 248, April 2006. Online veröffentlicht unter: http://www.syss.de/fileadmin/downloads/artikel/HMD_Kosten_PenTests_APRIL_2006.pdf [Stand: April 2006, zuletzt abgerufen am 16.11.2014].

Schreiber, Sebastian/Heinrich, Katrin, Penetrationstests als Instrument zur Qualitätssicherung. IT-Sicherheit und Datenschutz 2007, 452–455.

Schricker, Gerhard/Loewenheim, Ulrich (Hrsg.), Urheberrecht. Kommentar. 4. neu bearb. Aufl. München 2010. Zit.: Schricker/Loewenheim-*Bearbeiter*.

Schroeder, Werner, Die Auslegung des EU-Rechts. JuS 2004, 180–186.

Schulenburg, Johanna, Dogmatische Zusammenhänge von Rechtsgut, Deliktsstruktur und objektiver Zurechnung. In: Roland Hefendehl (Hrsg.), Die Rechtsgutstheorie. Baden-Baden 2003, S. 244–255.

Schumann, Heribert, Strafrechtliches Handlungsunrecht und das Prinzip der Selbstverantwortung der Anderen. Tübingen 1986.

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

Schuster, Heidi, Der Hackerparagraph – ein kurzes Intermezzo? DuD 2009, 742–746.

Schultz, Alexander, Neue Strafbarkeiten und Probleme – Der Entwurf des Strafrechtsänderungsgesetzes (StrafÄndG) zur Bekämpfung der Computerkriminalität vom 20.9.2006. DuD 2006, 778–784.

Seeger, Mark M., Three Years Hacker Paragraph – A review. DuD 2010, 476–478.

Sieber, Ulrich, Straftaten und Strafverfolgung im Internet. In: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages, Band 1 – Gutachten. München 2012, S. C 1-157.

– Rechtliche Ordnung in einer globalen Welt. Rechtstheorie 41 (2010), 151–198.

– Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt. Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten". NStZ 2009, 353–364.

– Grenzen des Strafrechts. Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht. ZStW 119 (2007), 1–68.

– Computerkriminalität und Strafrecht. 2. Aufl. Köln u.a. 1980.

Sieber, Ulrich/Brüner, Franz-Hermann/Satzger, Helmut/von Heintschel-Heinegg, Bernd (Hrsg.), Europäisches Strafrecht. 1. Aufl. Baden-Baden 2011. Zit.: *Bearbeiter*, in: *Sieber*, Europäisches Strafrecht.

Spannbrucker, Christian, Convention on Cybercrime (ETS 185). Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht. Online veröffentlicht unter http://epub.uni-regensburg.de/10281/1/CCC.pdf [Stand: Mitte 2004; zuletzt abgerufen am 16.11.2014].

Spindler, Gerald, Europäisches Urheberrecht in der Informationsgesellschaft. GRUR 2002, 105–120.

Spindler, Gerald/Leistner, Matthias, Die Verantwortlichkeit für Urheberrechtsverletzungen im Internet. Neue Entwicklungen in Deutschland und den USA. GRUR-Int 2005, 733–796.

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien. 2. Aufl. München 2011. Zit.: Spindler/Schuster-*Bearbeiter*.

Stadler, Thomas, Redaktioneller Link auf Anbieter von Software zur Umgehung von Kopierschutzmaßnahmen. JurPC Web-Dok. 126/2005, Abs. 1–33.

Stickelbrock, Barbara, Die Zukunft der Privatkopie im digitalen Zeitalter. GRUR 2004, 736–743.

Stuckenberg, Carl-Friedrich, Stellungnahme zum Gesetzentwurf der Bundesregierung – Entwurf eines … Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (… StrÄndG), BT-Drucks. 16/3656. Online veröffentlicht unter http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/straendg_computer/Stellungnahme_Stuckenberg.pdf [Stand: 13.3.2007; zuletzt abgerufen am 16.11.2014].

Thietz-Bartram, Jochim, Vereinbarkeit strafbewehrter Ausfuhrbeschränkungen mit dem Recht der Europäischen Union. RIW 1994, 839–849.

Trayer, Martin, Technische Schutzmaßnahmen und elektronische Rechtewahrnehmungssysteme. Baden-Baden 2003.

Valerius, Brian, Anmerkung zu BVerfG 2 BvR 2233/07. JR 2010, 79–86.

Vogel, Joachim, Europäische Kriminalpolitik – europäische Strafrechtsdogmatik. GA 2002, 517–534.

Wabnitz, Heinz-Bernd/Janovsky, Thomas (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts. 3. Aufl. München 2007. Zit.: Wabnitz/Janovsky-*Bearbeiter*.

Wahrig, Gerhard [Begr.], Deutsches Wörterbuch. 7. Aufl. Gütersloh, München 2000.

Wand, Peter, Technische Schutzmaßnahmen und Urheberrecht. Vergleich des internationalen, europäischen, deutschen und US-amerikanischen Rechts. München 2001.

Wandtke, Artur-Axel (Hrsg.), Urheberrecht. Berlin 2009. Zit.: *Bearbeiter*, in: Wandtke, Urheberrecht.

Wandtke, Artur-Axel/Bullinger, Winfried, Praxiskommentar zum Urheberrecht. 3. Aufl. München 2009. Zit.: Wandtke/Bullinger-*Bearbeiter*.

Wang, Ying, Der strafrechtliche Schutz des Urheberrechts. Eine vergleichende Untersuchung zum deutschen und chinesischen Strafrecht. Berlin 2011.

Weber, Ulrich, Die Vorverlegung des Strafrechtsschutzes durch Gefährdungs- und Unternehmensdelikte. In: Hans-Heinrich Jescheck (Hrsg.), Die Vorverlegung des Strafrechtsschutzes durch Gefährdungs- und Umweltdelikte. ZStW-Beiheft 1987, 1–36.

Weißer, Bettina, Über den Umgang des Strafrechts mit terroristischen Bedrohungslagen. ZStW 121 (2009), 131–161.

Wermke, Matthias u.a. (Hrsg.), Duden. Das Synonymwörterbuch, Dudenband 8. 5. Aufl. Mannheim, Zürich 2010.

Westphalen, Friedrich Graf von, Auslegung von Gesetzen: Vom nationalen zum europäischen Privatrecht. AnwBl 2008, 1–7.

Witzigmann, Tobias, Mögliche Funktionen und Bedeutungen des Absichtsbegriffs im Strafrecht. JA 2009, 488–493.

Wohlers, *Wolfgang,* Deliktstypen des Präventionsstrafrechts. Zur Dogmatik „moderner" Gefährdungsdelikte. Berlin 2000.

Zabel, Benno, Interventionsstrafrecht? Anmerkungen zum Funktionswandel des Strafrechts im Sicherheitsregime des modernen Staates. StraFo 2011, 20–22.

Ziemann, Sascha/Ziethen, Jörg, Was tun mit „verbotenen Gegenständen"? Strafrechtliche Risiken der Besitzaufgabe an Drogen, Waffen, Pornographie. JR 2011, 65–69.

Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht

Die zentralen Veröffentlichungen des Max-Planck-Instituts für ausländisches und internationales Strafrecht werden in Zusammenarbeit mit dem Verlag Duncker & Humblot in den folgenden vier Unterreihen der „Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht“ vertrieben:

- „Strafrechtliche Forschungsberichte“,
- „Kriminologische Forschungsberichte“,
- „Interdisziplinäre Forschungen aus Strafrecht und Kriminologie“ sowie
- „Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung“.

Diese Publikationen können direkt über das Max-Planck-Institut unter <www.mpicc.de> oder über den Verlag Duncker & Humblot unter <www.duncker-humblot.de> erworben werden.

Darüber hinaus erscheinen im Hausverlag des Max-Planck-Instituts in der Unterreihe „research in brief“ zusammenfassende Kurzbeschreibungen von Forschungsergebnissen und in der Unterreihe „Arbeitsberichte“ Veröffentlichungen vorläufiger Forschungsergebnisse. Diese Veröffentlichungen können über das Max-Planck-Institut bezogen werden.

Detaillierte Informationen zu den einzelnen Publikationen des Max-Planck-Instituts für ausländisches und internationales Strafrecht sind unter <www.mpicc.de> abrufbar.

The main research activities of the Max Planck Institute for Foreign and International Criminal Law are published in the following four subseries of the “Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht” (Research Series of the Max Planck Institute for Foreign and International Criminal Law), which are distributed in cooperation with the publisher Duncker & Humblot:

- “Strafrechtliche Forschungsberichte” (Reports on Research in Criminal Law),
- “Kriminologische Forschungsberichte” (Reports on Research in Criminology),
- “Interdisziplinäre Forschungen aus Strafrecht und Kriminologie” (Reports on Interdisciplinary Research in Criminal Law and Criminology), and
- “Sammlung ausländischer Strafgesetzbücher in deutscher Übersetzung” (Collection of Foreign Criminal Laws in German Translation).

These publications can be ordered from the Max Planck Institute at <www.mpicc.de> or from Duncker & Humblot at <www.duncker-humblot.de>.

Two additional subseries are published directly by the Max Planck Institute for Foreign and International Criminal Law: “research in brief” contains short reports on results of research activities, and “Arbeitsberichte” (working materials) present preliminary results of research projects. These publications are available at the Max Planck Institute.

Detailed information on all publications of the Max Planck Institute for Foreign and International Criminal Law can be found at <www.mpicc.de>.

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aus dem strafrechtlichen Veröffentlichungsprogramm:

S 143 *Zunyou Zhou*
Balancing Security and Liberty
Counter-Terrorism Legislation in Germany and China
2014 • 352 Seiten • ISBN 978-3-86113-813-6 € 35,00

S 142 *Nadine Dombrowski*
Extraterritoriale Rechtsanwendung im Internet
2014 • 206 Seiten • ISBN 978-3-86113-814-3 € 31,00

S 141 *Gang Wang*
Die strafrechtliche Rechtfertigung von Rettungsfolter
Ein Rechtsvergleich zwischen Deutschland und den USA
2014 • 428 Seiten • ISBN 978-3-86113-815-0 € 41,00

S 140 *Ulrich Sieber / Marc Engelhart*
Compliance Programs for the Prevention of Economic Crimes
An Empirical Survey of German Companies
2014 • 312 Seiten • ISBN 978-3-86113-816-7 € 40,00

S 139 *Susanne Rheinbay*
Die Errichtung einer Europäischen Staatsanwaltschaft
2014 • 347 Seiten • ISBN 978-3-86113-819-8 € 35,00

S 138 *Sarah Herbert*
Grenzen des Strafrechts bei der Terrorismusgesetzgebung
Ein Rechtsvergleich zwischen Deutschland und England
2014 • 300 Seiten • ISBN 978-3-86113-820-4 € 35,00

S 137 *Nadine Zurkinden*
Joint Investigation Teams
Chancen und Grenzen von gemeinsamen Ermittlungsgruppen
in der Schweiz, Europa und den USA
2013 • 396 Seiten • ISBN 978-3-86113-821-1 € 41,00

S 136 *Nico Herbert*
Strafrechtlicher Schutz von EU-Subventionen
Reichweite und Grenzen in Deutschland, Österreich und England
am Beispiel nicht wirtschaftsfördernder Subventionen
2013 • 320 Seiten • ISBN 978-3-86113-823-5 € 38,00

S 135 *Nandor Knust*
Strafrecht und Gacaca
Entwicklung eines pluralistischen Rechtsmodells
am Beispiel des ruandischen Völkermordes
2013 • 423 Seiten • ISBN 978-3-86113-824-2 € 41,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aus dem strafrechtlichen Veröffentlichungsprogramm:

S 128.1.1 *Ulrich Sieber / Konstanze Jarvers / Emily Silverman* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 1.1: Introduction to National Systems
2013 • 314 Seiten • ISBN 978-3-86113-822-8 € 40,00

S 128.1.2 Volume 1.2: Introduction to National Systems
2013 • 363 Seiten • ISBN 978-3-86113-826-6 € 43,00

S 128.1.3 Volume 1.3: Introduction to National Systems
2014 • 297 Seiten • ISBN 978-3-86113-818-1 € 40,00

S 128.2.1 *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 2.1: General limitations on the application of criminal law
2011 • 399 Seiten • ISBN 978-3-86113-834-1 € 43,00

S 128.3.1 *Ulrich Sieber / Susanne Forster / Konstanze Jarvers* (eds.)
National Criminal Law in a Comparative Legal Context
Volume 3.1: Defining criminal conduct
2011 • 519 Seiten • ISBN 978-3-86113-833-4 € 46,00

S 114.1 *Ulrich Sieber/Karin Cornils* (Hrsg.)
Nationales Strafrecht in rechtsvergleichender Darstellung
– Allgemeiner Teil –
Band 1: Grundlagen
2009 • 790 Seiten • ISBN 978-3-86113-849-5 € 55,00

S 114.2 Band 2: Gesetzlichkeitsprinzip – Internationaler Geltungsbereich – Begriff und Systematisierung der Straftat
2008 • 470 Seiten • ISBN 978-3-86113-860-0 € 41,00

S 114.3 Band 3: Objektive Tatseite – Subjektive Tatseite – Strafbares Verhalten vor der Tatvollendung
2008 • 490 Seiten • ISBN 978-3-86113-859-4 € 41,00

S 114.4 Band 4: Tatbeteiligung – Straftaten in Unternehmen, Verbänden und anderen Kollektiven
2010 • 527 Seiten • ISBN 978-3-86113-842-6 € 45,00

S 114.5 Band 5: Gründe für den Ausschluss der Strafbarkeit – Aufhebung der Strafbarkeit – Verjährung
2010 • 718 Seiten • ISBN 978-3-86113-841-9 € 55,00

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Auswahl aktueller Publikationen aus dem kriminologischen Veröffentlichungsprogramm:

K 166 *Ramin Tehrani*
Die „Smart Sanctions" im Kampf gegen den Terrorismus und als Vorbild einer präventiven Vermögensabschöpfung
Berlin 2014 • 256 Seiten • ISBN 978-3-86113-247-9 € 35,00

K 165 *Daniela Cernko*
Die Umsetzung der CPT-Empfehlungen im deutschen Strafvollzug
Eine Untersuchung über den Einfluss des Europäischen Komitees zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe auf die deutsche Strafvollzugsverwaltung
Berlin 2014 • 455 Seiten • ISBN 978-3-86113-246-2 € 39,00

K 164 *Franziska Kunz*
Kriminalität älterer Menschen
Beschreibung und Erklärung auf der Basis von Selbstberichtsdaten
Berlin 2014 • 387 Seiten • ISBN 978-3-86113-244-8 € 35,00

K 163 *David Jensen*
Maras
A study of their origin, international impact, and the measures taken to fight them
Berlin 2013 • 245 Seiten • ISBN 978-3-86113-243-1 € 35,00

K 161 *Gunda Wößner, Roland Hefendehl, Hans-Jörg Albrecht* (Hrsg.)
Sexuelle Gewalt und Sozialtherapie
Bisherige Daten und Analysen zur Längsschnittstudie „Sexualstraftäter in den sozialtherapeutischen Abteilungen des Freistaates Sachsen"
Berlin 2013 • 274 Seiten • ISBN 978-3-86113-241-7 € 35,00

K 159 *Andreas Armborst*
Jihadi Violence
A study of al-Qaeda's media
Berlin 2013 • 266 Seiten • ISBN 978-3-86113-119-9 € 35,00

K 158 *Martin Brandenstein*
Auswirkungen von Hafterfahrungen auf Selbstbild und Identität rechtsextremer jugendlicher Gewalttäter
Berlin 2012 • 335 Seiten • ISBN 978-3-86113-118-2 € 35,00

K 157 *Ghassem Ghassemi*
Criminal Policy in Iran Following the Revolution of 1979
A Comparative Analysis of Criminal Punishment and Sentencing in Iran and Germany
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-116-8 € 35,00

K 156 *Gunther Olt*
Pressefreiheit im Kontext strafrechtlicher Ermittlungsmaßnahmen
Berlin 2013 • 265 Seiten • ISBN 978-3-86113-114-4 € 35,00