

SCHRIFTENREIHE

DER STIFTUNG

DER HESSISCHEN

RECHTSANWALTSCHAFT

BAND 8

Die Internetkriminalität boomt
Braucht das Strafgesetzbuch ein Update?

Beiträge von
Turmandach Zeh
Sven Lehmann
Annemarie Hoffmann
Bianca Biernacik
Alexander Claudius Brandt
Dr. Sebastian J. Golla

Bibliografische Information der Deutschen Bibliothek

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

Herausgeber: Stiftung der Hessischen Rechtsanwaltschaft
Reihe: Schriftenreihe der Stiftung der Hessischen Rechtsanwaltschaft
Band 8

**Zeh, Turmandach / Lehmann, Sven / Hoffmann, Annemarie / Biernacik, Bianca /
Brandt, Alexander Claudius / Golla, Dr. Sebastian J.**

Die Internetkriminalität boomt
Braucht das Strafgesetzbuch ein Update?
ISBN 978-3-86376-195-0

Hinweis: Die Arbeit gibt ausschließlich die persönliche Ansicht der Autoren wieder.

Alle Rechte vorbehalten

1. Auflage 2017

© Optimus Verlag, Göttingen

URL: www.optimus-verlag.de

Printed in Germany

Papier ist FSC zertifiziert (holzfrei, chlorfrei und säurefrei,
sowie alterungsbeständig nach ANSI 3948 und ISO 9706)

Das Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes in Deutschland ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Vorwort des Herausgebers

Für nahezu 80 Prozent der Deutschen ist das Internet alltäglich und unverzichtbar geworden: Es macht uns vernetzter, intelligenter und kommunikativer. Facebook, LinkedIn, Xing und Twitter werden auch von Parlamentariern, Richtern, Staatsanwälten und Rechtsanwälten genutzt und geschätzt. Das Internet ist aber auch die perfekte Plattform zur Verbreitung von Falschmeldungen (der Begriff „Fake news“ ist erst jüngst in die deutsche Sprache eingegangen) oder gar zur Begehung von Straftaten: Es ist anonym, insbesondere im sogenannten Darknet, einem abgeschotteten Teil des Internets, schnell und weltweit vernetzt. Nach einer Untersuchung des Branchenverbandes Bitkom e.V. sind im Jahr 2015 rund 51% der Internetnutzer in Deutschland Opfer eines Angriffs mit Computer-Schadsoftware, eines Diebstahls von persönlichen Daten bzw. digitalen Identitäten etc. geworden und fast jeder Nutzer kennt entweder selbst oder in seinem Bekanntenkreis jemanden, der eine entsprechende Erfahrung machen musste. Unternehmen sind anfällig und ganze Infrastrukturen wie etwa die Stromversorgung sind Gegenstand von Cyber-Angriffen. Schwachstellen in IT-Systemen („Zero-Day-Exploits“) werden von außen illegal genutzt, um Geräte zu manipulieren oder wichtige Daten davon herunterzuziehen oder IT-Systeme anzugreifen. Auf dem Schwarzmarkt sollen sechs- bis siebenstellige Summen für Zero-Day-Exploits gezahlt werden.

Können wir es uns vor diesem Hintergrund leisten, dass der Begriff „Internet“ im deutschen Offline-Strafgesetzbuch weiterhin nicht vorkommt? Müssen in unserer heutigen IT-Gesellschaft persönliche Daten strafrechtlich nicht genauso umfassend geschützt werden wie körperliche Gegenstände? Brauchen wir – auch im Hinblick auf Art. 103 Abs. 2 GG – Online-Strafnormen wie digitaler Diebstahl oder digitaler Hausfriedensbruch?

Die Internetkriminalität entwickelt sich zudem ständig weiter. Nach den aktuellen Erkenntnissen des Bundeskriminalamts gewinnt das Geschäftsmodell „Cybercrime-as-a-Service“ im Internet mehr und mehr an Bedeutung. Die digitale Schattenwirtschaft im Internet („Underground Economy“) stellt auch technischen Laien eine große Bandbreite an Dienstleistungen zur Verfügung, welche die Durchführung jeder Art von Internetkriminalität ermöglichen. Das kriminelle Angebot umfasst die Bereitstellung von Kommunikationsforen über verschiedenste Anonymisierungsdienste bis hin zur Erstellung von individuellen Schadprogrammen und künstlichen Identitäten. Daneben floriert ein schwunghafter Handel mit ausgespähten Zugangskennungen, Sicherheitslücken in IT-Systemen und Kreditkartendaten, aber auch mit Waffen, Drogen, Falschgeld oder gefälschten Pässen. Internet-Kriminelle arbeiten heute weltweit als Hackergruppen arbeitsteilig zusammen, obwohl sie sich im realen Leben nie kennengelernt haben; virtuelle Hassattacken bedrohen die politische Debattenkultur.

Wie können diese neuen Kriminalitätsformen mit den traditionellen Kategorien von Täterschaft und Teilnahme erfasst werden? Ist bereits das Bereitstellen eines kriminellen Forums oder einer kriminellen Infrastruktur als Beihilfe strafbar? Gibt es eine digitale Bande? Oder braucht es ganz neuer Ansätze, um Unrecht und Schuld bei digitalen Straftaten zu erfassen?

Das Bundesverfassungsgericht hat sich in einem Urteil vom 2.3.2010 klar positioniert: „In einem Rechtsstaat darf auch das Internet keinen rechtsfreien Raum bilden.“ Was also tun?

Die Stiftung der Hessischen Rechtsanwaltschaft hat sich dieses Phänomens im Jahr 2016 angenommen und zum Thema „Die Internetkriminalität boomt – Braucht das Strafgesetzbuch ein Update?“ einen studentischen Aufsatzwettbewerb ausgeschrieben. Teilnahmeberechtigt waren alle an einer deutschen Universität eingeschriebenen Jurastudierenden (auch Promotionsstudierende) und Rechtsreferendare. Auch Gemeinschaftsarbeiten waren zugelassen. Die Teilnehmer des Wettbewerbs setzten sich mit der Frage, ob das Strafgesetzbuch ein Update braucht, intensiv auseinander.

Die Beiträge wurden von Dr. Benjamin Krause, Generalstaatsanwaltschaft Frankfurt am Main - Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), begutachtet. Die ZIT ist eine Sondereinheit der Generalstaatsanwaltschaft Frankfurt am Main. Mit ihr nimmt Hessen eine Vorreiterrolle bei der Bekämpfung der Internetkriminalität in Deutschland ein, und dies mag auch als Erklärung dafür dienen, warum sich die Stiftung der Hessischen Rechtsanwaltschaft mit diesem bundesweiten Phänomen auseinandersetzt.

Entsprechend ihrer Konzeption dient die ZIT den örtlich zuständigen Staatsanwaltschaften und der Polizei als Ansprechpartner in allen Fällen der Computer- und Internetkriminalität. In Einzelfällen kann die ZIT als Task-Force Verfahren mit Internetbezug aus allen Bereichen des Strafrechts mit besonders hohen Anforderungen an die technische Beweisführung übernehmen und damit die Staatsanwaltschaften in komplexen Verfahren entlasten.

Dr. Benjamin Krause ist als Staatsanwalt bei der ZIT bestens mit allen Facetten des Themas vertraut. Er hat aus den vielfältigen Einsendungen aus ganz Deutschland zum Aufsatzwettbewerb (Wettbewerbsbeiträge kamen dieses Mal vor allem aus Augsburg, Berlin, Bielefeld, Dresden, Frankfurt am Main, Frankfurt/Oder, Gießen, Halle, Jena, Köln, Leipzig, Marburg, Passau, Potsdam und Speyer) die hier vorgestellten Arbeiten ausgewählt. Im vorliegenden Band 8 der Schriftenreihe der Stiftung der Hessischen Rechtsanwaltschaft veröffentlichen wir die Beiträge der sechs Preisträger Bianca Biernacik, Alexander Claudius Brandt, Dr. Sebastian J. Golla, Annemarie Hoffmann, Sven Lehmann und Turmandach Zeh. Alle Preisträger wurden mit einem Geldpreis ausgezeichnet. Wir freuen uns, ihre Arbeiten mit dem vorliegenden Band einer breiteren Öffentlichkeit zugänglich zu machen.

Nach „Die deutsche Juristenausbildung unter dem Einfluss des Bologna-Prozesses“ (Band 1), „Elektronische Fußfessel – Fluch oder Segen der Kriminalpolitik“ (Band 2), „Schwimmen mit Fingerabdruck“ (Band 3), „Kulturflaute, Kulturwertmark oder Three Strikes and you are out: Wie soll mit Kreativität im Internet umgegangen werden?“ (Band 4), „Von der Kontrolle des Gerichts zur Befriedigung des Informationsbedürfnisses der Gesellschaft – Gibt es einen Funktionswandel der ‚Öffentlichkeit des Gerichtsverfahrens‘ (§ 169 GVG)?“ (Band 5) und „Deals im Strafverfahren – Darf sich ein Angeklagter im Strafverfahren ‚freikaufen‘?“ (Band 6), „Ist das derzeitige Versammlungsgesetz noch zeitgemäß?“ (Band 7) beleuchtet die Stiftung der Hessischen Rechtsanwaltschaft mit dem vorliegenden Band 8 ihrer Schriftenreihe wieder einen aktuellen Brennpunkt der Diskussion. Mit einem gewissen Stolz sei angemerkt, dass einige Themen des bisherigen Wettbewerbs inzwischen weit über Hessen hinaus Bedeutung erlangt

haben; verwiesen sei nur auf das Thema „Elektronische Fußfessel“, welches gerade in Zusammenhang mit der Überwachung politisch extremer Gefährder heute die Schlagzeilen beherrscht. Wir verbinden mit dem vorliegenden Band die Hoffnung, einen sachlichen Beitrag zur Lösung der strafrechtlichen Herausforderungen durch das Internet anbieten zu können.

Bedanken möchten wir uns für die Betreuung des Aufsatzwettbewerbs und die fachkundige Auswahl der Wettbewerbsbeiträge beim Juror, Herrn Staatsanwalt Dr. Benjamin Krause. Danken möchte ich persönlich meinen Vorstandskollegen, den Rechtsanwälten Dr. Rudolf Kriszeleit und Dr. Rudolf Lauda, welche mir den Rücken bei dem Aufsatzwettbewerb freigehalten haben. Ganz besonderer Dank gilt wiederum meinen Assistentinnen Denisa Gil und Judith Wilhelm, deren tatkräftige Unterstützung mir die ehrenamtliche Bewältigung der vielfältigen Aufgaben der Stiftung erst ermöglicht.

Frankfurt am Main, im Mai 2017

Dr. Mark C. Hilgard

- Vorsitzender des Vorstands -

- Rechtsanwalt -

Vorwort des Gutachters Dr. Benjamin Krause

„Das Internet ist für uns alle Neuland¹“. Dieses Zitat von Bundeskanzlerin Dr. Angela Merkel aus dem Jahr 2013 führte zu heiteren und spöttischen Reaktionen, da zu diesem Zeitpunkt bereits über 75 Prozent der Deutschen online waren und im Schnitt über 2,5 Stunden täglich im Internet verbrachten.² Doch jedenfalls für das Strafgesetzbuch ist das Internet auch im Jahr 2017 nach wie vor Neuland. Denn der Begriff „Internet“ existiert in unserem „Offline“-Strafgesetzbuch nicht.

Die Politik will dieses Neuland erschließen und diskutiert aktuell darüber, ob angesichts immer neuer Phänomene von Internetkriminalität auch neue internetspezifische Strafnormen oder gar neue Kategorien von Täterschaft und Teilnahme erforderlich sind. Auf Initiative des Bundeslandes Hessen etwa hat der Bundesrat aktuell einen Gesetzentwurf zur „Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme“ in den Bundestag eingebracht.³ Damit soll ermöglicht werden, dass etwa Smartphones mit besonders sensiblen Daten strafrechtlich genauso geschützt werden, wie körperliche Gegenstände bei Einbruch oder Diebstahl. Und die Justizministerinnen und Justizminister haben sich auf ihrer Herbstkonferenz 2016 dafür ausgesprochen, im Internet bereits das öffentliche Feilbieten von Waffen, Betäubungsmitteln, Fälsfikaten oder kriminellen Dienstleistungen zur Vorbereitung von Straftaten durch Anpassungen des materiellen Strafrechts, namentlich des Waffengesetzes, zu unterbinden.⁴ Dagegen ist die Bundesregierung der Auffassung, dass die Phänomene von Internetkriminalität bereits von den Regelungen des Strafgesetzbuches erfasst werden und zumindest keine gravierenden Strafbarkeitslücken bestehen.⁵

In diesem hochaktuellen rechtspolitischen Spannungsfeld fand der diesjährige Aufsatzwettbewerb der Stiftung der Hessischen Rechtsanwaltschaft zu dem Thema „*Die Internetkriminalität boomt - Braucht das Strafgesetzbuch ein Update?*“ statt und führte wieder zu einer erfreulichen Zahl an eingereichten Beiträgen. Der heterogene Teilnehmerkreis von Studierenden in Anfangssemestern bis hin zu bereits promovierten wissenschaftlichen Mitarbeitern setzte dabei ganz unterschiedliche Schwerpunkte. Die prämierten und nachfolgend abgedruckten Beiträge haben jedoch eines gemeinsam: die Entwicklung jeweils eigener Ideen und neuer Impulse für die aktuelle Diskussion.

¹ Vgl. https://de.wikiquote.org/wiki/Angela_Merkel.

² <http://www.ard-zdf-onlinestudie.de/>.

³ <http://dip21.bundestag.de/dip21/btd/18/101/1810182.pdf>

⁴ https://www.justiz.nrw/JM/leitung/jumiko/beschluesse/2016/Herbstkonferenz-2016/top_ii_8_-_effektivitaet_strafrechtlicher_ermittlungen_in_getarnten_computernetzwerken_sog_darknet_herbstkonferenz.pdf

⁵ <http://dip21.bundestag.de/dip21/btd/18/101/1810182.pdf>, Anlage 2.

Der Beitrag von *Turmandach ZEH* verfügt über eine flott geschriebene Einleitung in das Thema und gibt einen guten Überblick über die wichtigsten Phänomene der Internetkriminalität. Er kommt zu dem Ergebnis, dass der allgemeine Teil des Strafgesetzbuchs dem Internet durchaus gewappnet ist. Ein Update des Strafgesetzbuches sei jedoch für das digitale Rechtsgut „informationstechnisches System“ erforderlich, damit die Strafbarkeit zukünftig nicht mehr von dem Verhalten der Opfer und der Effektivität ihrer Schutzmechanismen, sondern rein von dem Verhalten der Täter abhängig ist.

Auch *Sven LEHMANN* prüft in seinem Beitrag die wichtigsten Phänomene der Internetkriminalität. Er ist - ganz im Sinne der Bundesregierung - der Auffassung, dass aufgrund des weiten Datenbegriffs des Strafgesetzbuchs bereits ein Großteil der Phänomene strafbar ist, obwohl das Wort „Internet“ im Strafgesetzbuch nicht vorkommt. Ein Update sei nur dort geboten, wo einzelne Strafbarkeitslücken bestehen wie etwa beim Schutz informationstechnischer Systeme oder bei der unbefugten Weitergabe von anvertrauten Daten. Eine umfassende Reform hält er nicht für erforderlich.

Annemarie HOFFMANN beschäftigt sich in ihrem Beitrag mit der Frage, ob das allgemeine System von Täterschaft und Teilnahme im Strafgesetzbuch das Betreiben einer Plattform im sog. Darknet erfassen kann. Ausgehend von der (wohl nicht haltbaren) Prämisse, dass für Darknet-Plattformbetreiber de lege lata keine Strafbarkeit existiert, entwickelt sie mit einem Vorschlag für einen neuen Fahrlässigkeits-Tatbestand des Unterlassens der Löschung oder der Sperrung von illegalen Inhalten einen durchaus interessanten Denkansatz für die aktuelle Diskussion.

Mit der Erfassung „neuer“ Straftaten am Beispiel von Diebstählen in Onlinespielen befasst sich *Bianca BIERNACIK*. Nach einer auch für technische Laien verständlichen Darstellung dieses „virtuellen Diebstahls“ stellt sie zunächst fest, dass dieser nicht von den auf körperliche Gegenstände ausgerichteten Tatbeständen des Strafgesetzbuchs erfasst wird. In Anlehnung an das niederländische Strafrecht entwickelt *Bianca BIERNACIK* schließlich einen eigenen Gesetzesvorschlag zur zukünftigen Erfassung virtueller Diebstähle.

Noch weiter geht *Alexander Claudius BRANDT*, der mit seinem Beitrag zur digitalen Wirtschaftsspionage nicht nur einen einzelnen Gesetzesvorschlag, sondern unter Berücksichtigung der aktuellen politischen Gesetzesinitiativen ein gänzlich neues System der Datendelikte des Strafgesetzbuches entwirft. Um die Verfolgung von Wirtschaftsspionage auch praktisch durchsetzen zu können, entwickelt *Alexander Claudius BRANDT* zudem ein neues Verfahren für die Gewährung von Akteneinsicht mit dem Ziel des besseren Schutzes von Geschäfts- und Betriebsgeheimnissen. Auch dieser Beitrag wird mit seinen völlig neuen Ansätzen für die rechtspolitische Diskussion der kommenden Jahre interessant sein.

Den herausragenden und mit dem ersten Preis prämierten Beitrag liefert *Dr. Sebastian J. GOLLA* mit seinem meinungsfreudigen Aufsatz „Risiken und Nebenwirkungen bei der Fortbildung des Internetstrafrechts“ ab. Bei seiner kritischen Überprüfung der „Datenhehlerei“ und des „digitalen Hausfriedensbruchs“ erkennt *Dr. Sebastian J. GOLLA* nicht nur eine Tendenz zur Expansion des Strafrechts und der Symbolik, sondern auch ein von ihm als „Hypertrophie“ bezeichnetes Anwachsen des materiellen Rechts aufgrund von Schwierigkeiten bei der praktischen Durchsetzung. Nach Auffassung von *Dr. Sebastian J. GOLLA* müsse das Ziel vielmehr eine „minimal-invasive Anpassung“ des Strafgesetzbuches sein, für die er sieben verblüffend einfache, aber höchst überzeugende Leitlinien erarbeitet.

Insgesamt wäre es daher nicht überraschend, wenn die mit diesem Buch vorgelegten Ideen und Impulse, Gesetzesentwürfe und Leitlinien demnächst in der rechtspolitischen Diskussion, aber auch in der Rechtspraxis Gehör finden. Denn: *„Einst lebten wir auf dem Land, dann in Städten und von jetzt an im Netz.“*⁶

Frankfurt am Main/Gießen, im Mai 2017

Dr. Benjamin Krause

⁶ Zitat aus dem Facebook-Film „The Social Network“ aus dem Jahr 2010 (Regie: David Fincher).

Inhaltsübersicht

| | |
|--------------------------|-----|
| Inhaltsverzeichnis | III |
|--------------------------|-----|

Turmandach Zeh – Informationstechnische Systeme als Herausforderung des modernen Rechtsgüterschutzes – eine riskante Gratwanderung

| | |
|---|----|
| I. Die Entdeckung des „Neulands“ | 1 |
| II. Braucht das Strafgesetzbuch ein Update? | 3 |
| III. Schluss..... | 18 |
| Literaturverzeichnis | 20 |

Sven Lehmann – Internetkriminalität – kein strafrechtliches „Neuland“

| | |
|---|----|
| I. Einleitung | 23 |
| II. Derzeitige Phänomene der Internetkriminalität | 24 |
| III. Stellungnahme | 41 |
| IV. Fazit und Ausblick..... | 44 |
| Literaturverzeichnis | 46 |

Annemarie Hoffmann – Kann das allgemeine System von Täterschaft und Teilnahme im Strafgesetzbuch die Betreiber einer Plattform im Darknet erfassen?

| | |
|--|----|
| I. Einleitung | 49 |
| II. Definition, Chancen und Probleme des Darknets | 50 |
| III. Strafrechtliche Bewertung der Plattformbetreiber de lege lata | 52 |
| IV. Strafrechtliche Verantwortung de lege ferenda..... | 65 |
| V. Fazit..... | 71 |
| Literaturverzeichnis | 72 |

*Bianca Biernacik – Erfassung „neuer“ Straftaten
am Beispiel von Diebstählen in Onlinespielen*

| | |
|--------------------------------------|----|
| I. Hinführung zum Thema | 75 |
| II. "Diebstahl" im Cyberspace | 76 |
| III. Zusammenfassung und Fazit | 94 |
| Literaturverzeichnis | 97 |

*Alexander Claudius Brandt – Gedanken zur Anpassung des Strafrechts
an die zunehmende Bedrohung von Geschäfts- und Betriebsgeheimnissen
durch Cyberkriminalität*

| | |
|--|-----|
| I. Einleitung | 99 |
| II. Beispielfälle | 103 |
| III. Strafbarkeit des Systemzugriffs, § 207 StGB-E..... | 104 |
| IV. Datenmanipulation, § 208 StGB-E..... | 116 |
| V. Datenhandel, § 209 StGB-E..... | 123 |
| VI. Vorbereitungstaten, § 210 StGB-E..... | 127 |
| VII. Strafantrag, § 210 a Abs. 5 StGB-E | 127 |
| VIII. Beschränkung des Akteneinsichtsrechts des Verteidigers | 127 |
| IX. Fazit..... | 135 |
| Literaturverzeichnis | 149 |

*Dr. Sebastian J. Golla – Risiken und Nebenwirkungen bei der Fortbildung
des Internetstrafrechts – Datenhehlerei, Digitaler Hausfriedensbruch
und alternative Regelungsansätze*

| | |
|--|-----|
| I. Internetstrafrecht und das Risiko einer kompensatorischen Hypertrophie | 153 |
| II. Datenhehlerei und Digitaler Hausfriedensbruch: Angemessene Erweiterungen? | 156 |
| III. „Minimalinvasive“ Anpassungen als alternativer Regelungsansatz..... | 170 |
| IV. Befund: Leitlinien für eine Fortbildung des Internetstrafrechts..... | 177 |
| Literaturverzeichnis | 179 |

Inhaltsverzeichnis

*Turmandach Zeh – Informationstechnische Systeme als Herausforderung
des modernen Rechtsgüterschutzes – eine riskante Gratwanderung*

| | |
|--|----------|
| I. Die Entdeckung des „Neulands“ | 1 |
| A. „Neuland“ oder nicht eher „Altlast“? | 1 |
| B. „Neulandexpedition“ – ein Weg ins Abenteuer? | 2 |
| II. Braucht das Strafgesetzbuch ein Update? | 3 |
| A. Die Anwendbarkeit des deutschen Strafrechts | 3 |
| 1. Territorialprinzip | 3 |
| 2. Schutzprinzip | 4 |
| 3. Weltrechtsprinzip | 4 |
| 4. Strafanwendung | 4 |
| B. Die Akteure im Internet | 4 |
| C. (Un-)Rechtsbewusstsein im Internet | 5 |
| D. Strafbarkeitslücke de lege ferenda | 6 |
| 1. „Cybercrime as a Service“ und das „Darknet“ | 6 |
| 2. Digitale Bande | 7 |
| 3. Erscheinungsformen | 9 |
| a) (Tat-) Mittel zum Zweck - Cyberbullying | 9 |
| b) Ein notwendiger Dietrich – Cybercrime | 10 |
| c) Schattenwelt Internet – Cyberterrorism | 12 |
| d) Zusammenfassung | 12 |
| 4. Lösungsansätze | 12 |
| a) Gesetzesentwurf Hessen | 12 |
| b) Kritik am Gesetzesentwurf | 14 |
| c) Digitaler Hausfriedensbruch gemäß § 123 StGB | 15 |
| d) Datenhehlerei § 202d StGB | 16 |

| | |
|-----------------------------------|-----------|
| E. Fazit | 17 |
| III. Schluss | 18 |
| Literaturverzeichnis | 20 |

Sven Lehmann – Internetkriminalität – kein strafrechtliches „Neuland“

| | |
|---|-----------|
| I. Einleitung | 23 |
| II. Derzeitige Phänomene der Internetkriminalität | 24 |
| A. Eindringen in und Störung von informationstechnischen Systemen | 24 |
| 1. Hacker/Cracker | 24 |
| a) Begriffliche Abgrenzung..... | 24 |
| b) Strafrechtliche Relevanz | 24 |
| c) Zustimmung durch Betroffene | 25 |
| d) Anstiftung..... | 26 |
| 2. DoS-Attacken und Bot-Netze..... | 27 |
| a) Vorbereitungshandlungen und Versuch..... | 27 |
| b) Täterschaft durch Nutzung eines infizierten Rechners | 28 |
| c) Qualifikation und Regelbeispiele..... | 28 |
| d) Strafbarkeit der Bekämpfung von Bot-Netzen | 29 |
| 3. Trojaner | 31 |
| B. Erlangen und Verwenden von Daten | 32 |
| 1. Erlangen der Daten durch Eindringen in IT-Systeme | 32 |
| 2. Datenhehlerei..... | 32 |
| 3. Phishing | 33 |
| a) Tatbegehung..... | 33 |
| b) Erfolgreiches Phishing einschließlich Überweisung | 33 |
| c) Zugriff auf Online-Bankkonto und Eingabe der Überweisungsdaten | 34 |
| d) Verwenden der Zugangsdaten durch Einloggen in Online-Bankkonto | 34 |
| e) Versenden der Phishing-E-Mail und Erlangen der Zugangsdaten..... | 34 |
| f) Man-in-the-Middle-Angriff | 36 |
| 4. Identitätsdiebstahl..... | 37 |

| | |
|--|-----------|
| C. Internetkriminalität und Erpressungsdelikte | 38 |
| 1. Ransomware | 38 |
| 2. Schutzgeldzahlung bei DDoS-Attacken | 39 |
| 3. Erpressung mit erlangten Daten | 39 |
| D. Ehrverletzungen und Soziale Medien | 40 |
| 1. Herabwürdigende Äußerungen..... | 40 |
| 2. Betreiber von Onlineportalen oder Foren..... | 40 |
| III. Stellungnahme | 41 |
| IV. Fazit und Ausblick | 44 |
| Literaturverzeichnis | 46 |

*Annemarie Hoffmann – Kann das allgemeine System von Täterschaft
und Teilnahme im Strafgesetzbuch die Betreiber einer Plattform
im Darknet erfassen?*

| | |
|--|-----------|
| I. Einleitung | 49 |
| II. Definition, Chancen und Probleme des Darknets | 50 |
| A. Was ist das Darknet? | 50 |
| B. Probleme und Chancen des Darknet | 51 |
| III. Strafrechtliche Bewertung der Plattformbetreiber de lege lata | 52 |
| A. Strafbarkeit aufgrund des Errichtens der Plattform | 52 |
| B. Haftung aufgrund der Inhalte: Die Privilegierungen des Telemediengesetzes.. | 53 |
| 1. Anwendbarkeit des Telemediengesetzes auf Plattformbetreiber im Darknet? | 53 |
| 2. Anwendbare Vorschrift | 54 |
| 3. Verpflichtung nach den „allgemeinen Gesetzen“ | 55 |
| C. Strafbarkeit nach den „allgemeinen Gesetzen“? | 56 |
| 1. Strafvereitelung durch Unterlassen, §§ 258 Abs. 1, 13 Abs. 1 StGB?..... | 56 |
| 2. Erfassung der Unterlassensstrafbarkeit über die Regeln von Täterschaft und Teilnahme | 57 |
| a) Mittäterschaft durch Unterlassen | 58 |
| b) Beihilfe durch Unterlassen..... | 58 |

| | |
|--|-----------|
| (1) Vorsätzliche rechtswidrige Haupttat | 58 |
| (2) Hilfeleisten durch Unterlassen | 59 |
| (3) Garantenstellung des Plattformbetreibers im Darknet | 61 |
| (4) Subjektiver Tatbestand: Doppelter Gehilfenvorsatz | 63 |
| D. Ergebnis..... | 65 |
| IV. Strafrechtliche Verantwortung de lege ferenda | 65 |
| A. „Präventiver“ Ansatz: Sollte das Errichten einer Plattform im Darknet per se unter Strafe gestellt werden? | 65 |
| 1. Problem: Nachweis des Vorsatzes..... | 65 |
| 2. Rechtspolitische Bedenken..... | 65 |
| B. „Repressiver“ Ansatz - Unterlassen der Löschung oder Sperrung des Inhalts..... | 67 |
| 1. Objektive Bedingung der Strafbarkeit..... | 68 |
| 2. Fahrlässigkeitstatbestand | 69 |
| 3. Vorschlag einer neuen Regelung..... | 70 |
| V. Fazit | 71 |
| Literaturverzeichnis | 72 |

*Bianca Biernacik – Erfassung „neuer“ Straftaten
am Beispiel von Diebstählen in Onlinespielen*

| | |
|--|-----------|
| I. Hinführung zum Thema | 75 |
| II. "Diebstahl" im Cyberspace..... | 76 |
| A. (Soziale) Virtuelle Welten und Onlinespiele | 76 |
| 1. Aufbau | 77 |
| a) MMORPGs | 77 |
| (1) Allgemeiner Aufbau | 77 |
| (2) Kostenmodelle..... | 78 |
| b) Soziale virtuelle Welten..... | 78 |
| (1) Allgemeiner Aufbau | 78 |
| (2) Kostenmodelle..... | 78 |

| | |
|---|----|
| 2. Technische Besonderheiten | 79 |
| 3. Handel..... | 79 |
| B. Juristische Problematik | 80 |
| 1. Möglichkeiten eines "Diebstahls" | 80 |
| a) Outworld-Methoden..... | 80 |
| b) Inworld-Methoden | 81 |
| c) Zusammenfassung..... | 81 |
| 2. Anwendbarkeit deutschen Strafrechts | 81 |
| 3. § 242 StGB | 82 |
| a) Sache | 82 |
| b) Erweiterte Auslegung..... | 82 |
| c) Ergebnis | 83 |
| 4. Weitere Straftatbestände..... | 83 |
| a) § 263 StGB..... | 83 |
| (1) Vermögensverfügung | 84 |
| (2) Vermögensschaden..... | 85 |
| (3) Ergebnis..... | 85 |
| b) § 263a StGB | 85 |
| c) § 303 StGB..... | 85 |
| d) § 303a StGB | 86 |
| (1) Anwendung in der Rechtsprechung | 86 |
| (2) Literaturmeinungen | 87 |
| 5. Kritische Würdigung der Alternativen | 88 |
| a) § 265 StGB..... | 88 |
| b) § 303a StGB | 88 |
| (1) Verfassungskonformität | 88 |
| (2) Strafraumen | 88 |
| (3) Schlussfolgerung | 89 |
| C. Regelung de lege ferenda | 89 |
| 1. Entwicklung der Onlinespiele | 89 |

| | |
|---|-----------|
| 2. Erfasste Fälle von Kriminalität in Bezug auf Onlinespiele..... | 90 |
| a) Deutschland..... | 90 |
| b) Exkurs: Fälle in anderen Ländern..... | 91 |
| c) Notwendigkeit einer Reform..... | 91 |
| 3. Konkrete Möglichkeiten einer Reform..... | 91 |
| a) Reform des Sachbegriffs..... | 92 |
| (1) Niederländisches Recht..... | 92 |
| (2) Umsetzung auf Deutsches Recht..... | 92 |
| b) Einführung eines neuen Straftatbestandes..... | 93 |
| c) Reform des § 303a StGB..... | 93 |
| d) Ergebnis..... | 94 |
| III. Zusammenfassung und Fazit..... | 94 |
| Literaturverzeichnis..... | 97 |

*Alexander Claudius Brandt – Gedanken zur Anpassung des Strafrechts
an die zunehmende Bedrohung von Geschäfts- und Betriebsgeheimnissen
durch Cyberkriminalität*

| | |
|--|------------|
| I. Einleitung..... | 99 |
| A. Internet und Cyberkriminalität..... | 99 |
| B. Vermutung für oder Entscheidung gegen die Freiheit?..... | 100 |
| C. „Cultural lag“ und begrenzte Entwicklungsoffenheit des Strafrechts..... | 100 |
| D. Themenstellung: Bedrohung von Geschäfts- und Betriebsgeheimnissen durch Cyberkriminalität..... | 101 |
| II. Beispielfälle..... | 103 |
| III. Strafbarkeit des Systemzugriffs, § 207 StGB-E..... | 104 |
| A. Verschllossenheit und Untätigkeit des Gesetzgebers..... | 104 |
| B. Die Reichweite des § 202 a StGB am Maßstab europäischer Bestrebungen.... | 105 |
| C. Was ist ein informationstechnisches System?..... | 106 |
| 1. Definitionen der Cybercrime-Convention sowie der Richtlinie 2013/40/EU..... | 106 |
| 2. Definitionsversuch des Landes Hessen in § 202 e Abs. 6 Nr. 1 StGB-E..... | 106 |

| | |
|---|------------|
| 3. Versuch eigener Herleitung..... | 106 |
| a) Entscheidung des BVerfG zur Online-Durchsuchung..... | 107 |
| b) Schussfolgerungen | 107 |
| D. Grundtatbestand, § 207 Abs. 1 StGB-E | 108 |
| 1. Zugang zu einem informationstechnischen System..... | 108 |
| 2. Fremdheit des informationstechnischen Systems..... | 109 |
| 3. Zugangssicherung..... | 109 |
| 4. Verzicht auf das Merkmal „unbefugt“ bzw. „rechtswidrig“ | 110 |
| 5. Schädigungsabsicht | 110 |
| 6. Strafmaß..... | 111 |
| E. Einbeziehung des heutigen § 202 b StGB in § 207 Abs. 2 StGB-E | 111 |
| F. Qualifikation durch das Ausspähen von Daten, § 207 Abs. 3 StGB-E..... | 112 |
| 1. Zugang zu besonders gesicherten Daten | 112 |
| a) Daten | 112 |
| b) Exkurs zu § 17 Abs. 2 Nr. 1 lit. a) UWG..... | 113 |
| 2. Überwindung einer besonderen Zugangssicherung | 114 |
| 3. Schädigungsabsicht | 114 |
| G. Strafbarkeit des Versuchs, § 207 Abs. 4 StGB-E | 114 |
| H. Strafzumessung in besonders schweren Fällen, § 207 Abs. 5 StGB-E..... | 115 |
| IV. Datenmanipulation, § 208 StGB-E | 116 |
| A. Grundtatbestand, § 208 Abs. 1 StGB-E | 117 |
| 1. Manipulation bestehender Daten, § 208 Abs. 1 Nr. 1 StGB-E | 117 |
| a) Löschen | 117 |
| b) Bearbeiten und Unterdrücken | 118 |
| 2. Manipulation durch Hinzufügen neuer Daten, § 208 Abs. 1 Nr. 2 StGB-E..... | 118 |
| 3. Datenzugang des Berechtigten erschwert oder unmöglich | 119 |
| B. Beeinträchtigung eines Datenverarbeitungsvorgangs, § 208 Abs. 2 StGB-E... | 119 |
| 1. Datenverarbeitungsvorgang..... | 119 |
| 2. Nicht unerhebliche Beeinträchtigung..... | 120 |

| | |
|--|------------|
| 3. Wesentliche Bedeutung für Lebensgestaltung oder Erwerb | 120 |
| C. Qualifikation durch fremdes Unternehmen oder Behörde als Tatopfer, § 208 Abs. 3 StGB-E | 121 |
| D. Strafbarkeit des Versuchs, § 208 Abs. 4 StGB-E | 121 |
| E. Strafzumessung durch besonders schwere Fälle, § 208 Abs. 5 StGB-E..... | 121 |
| 1. „große Anzahl“ von Datenverarbeitungsvorgängen..... | 122 |
| 2. Weitere Regelbeispiele..... | 122 |
| F. Folgen für § 303 a und § 303 b StGB | 122 |
| V. Datenhandel, § 209 StGB-E..... | 123 |
| A. Dogmatische Probleme des § 202 d StGB | 123 |
| B. Welchem Zweck dient § 209 StGB-E? | 124 |
| C. Grundtatbestand des Datenhandels, § 209 Abs. 1 und 2 StGB-E..... | 125 |
| 1. Datenbegriff und Anknüpfung an informationstechnischem System | 125 |
| 2. Tathandlungen | 125 |
| a) Sicherung, § 209 Abs. 1 Nr. 1 StGB-E | 125 |
| b) Tathandlungen nach § 209 Abs. 1 Nrn. 2 und 3 StGB-E..... | 126 |
| 3. Bereicherungs- oder Schädigungsabsicht und Versuch | 126 |
| D. Strafzumessung in besonders schweren Fällen, § 209 Abs. 4 StGB-E..... | 126 |
| VI. Vorbereitungstaten, § 210 StGB-E | 127 |
| VII. Strafantrag, § 210 a Abs. 5 StGB-E..... | 127 |
| VIII. Beschränkung des Akteneinsichtsrechts des Verteidigers | 127 |
| A. Problemstellung..... | 127 |
| B. Verfassungsrechtliche Bedeutung des Akteneinsichtsrechts | 128 |
| C. Was ist eine „Akte“ im Sinne des § 147 StPO?..... | 129 |
| D. Rechtfertigung der Beschränkung des Akteneinsichtsrechts | 130 |
| E. Wie soll der Ausschluss des Akteneinsichtsrechts erfolgen? | 132 |
| 1. Ausschluss durch § 147 a StPO-E..... | 132 |
| 2. Feststellung der Geheimhaltungsbedürftigkeit „in camera“ | 132 |
| 3. Ausgestaltung des „in-camera“-Aktenprüfungsverfahrens | 133 |
| a) Antrag auf Eröffnung, § 199 a StPO-E..... | 134 |

| | |
|--|------------|
| b) Ablauf und Ausgestaltung des Aktenprüfungsverfahrens, § 199 b StPO-E | 134 |
| c) Gerichtliche Verwahrung der Nebenakte, § 199 c StPO-E | 134 |
| d) Rechtsschutz gegen die Entscheidung des Gerichts, § 199 d StPO-E.... | 135 |
| 4. Beschränkung auch der Akteneinsicht des Verletzten, § 406 e | 135 |
| IX. Fazit | 135 |
| Literaturverzeichnis | 149 |

*Dr. Sebastian J. Golla – Risiken und Nebenwirkungen bei der Fortbildung
des Internetstrafrechts – Datenhehlerei, Digitaler Hausfriedensbruch
und alternative Regelungsansätze*

| | |
|--|------------|
| I. Internetstrafrecht und das Risiko einer kompensatorischen Hypertrophie..... | 153 |
| II. Datenhehlerei und Digitaler Hausfriedensbruch: Angemessene Erweiterungen? | 156 |
| A. Der Straftatbestand der Datenhehlerei | 156 |
| 1. Zielrichtung | 157 |
| 2. Beitrag zur Problemlösung..... | 158 |
| a) Kein Schutz der „formellen Verfügungsbefugnis an Daten“ durch § 202d StGB möglich | 158 |
| b) Schließung von Schutzlücken..... | 159 |
| (1) §§ 43, 44 BDSG | 159 |
| (2) § 202c Abs. 1 Nr. 1 StGB..... | 160 |
| (3) § 17 UWG..... | 161 |
| 3. Expansive Wirkung | 161 |
| a) Weite des Tatbestandes..... | 162 |
| b) Auswirkungen auf die Pressefreiheit | 163 |
| B. Das Vorhaben zum Digitalen Hausfriedensbruch..... | 164 |
| 1. Zielrichtung | 165 |
| 2. Beitrag zur Problemlösung..... | 166 |
| 3. Expansive Wirkung | 168 |

| | |
|---|------------|
| C. Zwischenergebnis..... | 169 |
| III. „Minimalinvasive“ Anpassungen als alternativer Regelungsansatz | 170 |
| A. Anpassung des strafrechtlichen Schutzes der informationellen Selbstbestimmung | 170 |
| 1. Bestehende Defizite..... | 171 |
| a) Strafandrohung..... | 171 |
| b) Komplexität und Unbestimmtheit der §§ 43, 44 BDSG | 172 |
| c) Regelung im BDSG | 173 |
| d) Absolutes Antragserfordernis | 173 |
| 2. Lösung durch Anpassung und Regelung im StGB..... | 173 |
| a) Regelung im StGB | 173 |
| b) Präzisierung und Anpassung des Tatobjektes..... | 174 |
| c) Regelung als relatives Antragsdelikt | 174 |
| d) Notwendigkeit einer Neuregelung aufgrund der EU-Datenschutz-Grundverordnung | 175 |
| B. Anpassung von § 202c Abs. 1 StGB..... | 176 |
| IV. Befund: Leitlinien für eine Fortbildung des Internetstrafrechts..... | 177 |
| Literaturverzeichnis | 179 |