universität wien

Exposé

Zum Dissertationsvorhaben mit dem Arbeitstitel

Aktuelle Phänomene der Cyberkriminalität: Strafrechtslücken und strafrechtspolitische Überlegungen anhand einer rechtsvergleichenden Untersuchung

(Eine kritische Analyse der österreichischen Straftatbestände im Rechtsvergleich mit dem deutschen Recht)

Verfasserin:

Mag. iur. Claudia Grosse

angestrebter akademischer Grad

Doctor iuris (Dr. iur.)

Betreuer:

Univ. Prof. Dr. Frank Höpfel

Wien, März 2016
Studienkennzahl lt. Studienblatt: A 783 101
Studienrichtung lt. Studienblatt: Rechtswissenschaften
Dissertationsgebiet lt. Studienblatt: Strafrecht

1. Einführung in das Thema

Die kriminellen Erscheinungsformen im Zusammenhang mit Informations- und Kommunikationstechnologien haben sich in den letzten Jahren rasant weiterentwickelt.[1] Cyberkriminalität ist ein äußerst dynamisches und hochkomplexes Kriminalitätsphänomen, das die Ermittlungsbehörden ständig vor neue Herausforderungen stellt. Die effektive Bekämpfung von Cyberkriminalität erfordert nicht nur entsprechende Aus- und Fortbildungsmaßnahmen für die Bereitstellung hochqualifizierter Cybercrime-Ermittlungsexperten und IT-Forensiker, sondern auch die Ausstattung der Ermittlungsbehörden mit modernster Infrastruktur sowie den Ausbau von Präventions- und Forschungsprojekten. Aufgrund der Internationalität von Cybercrime bedarf es darüber hinaus auch internationaler Kooperationsmaßnahmen, insbesondere einer engen Zusammenarbeit nationaler Ermittlungs- und Strafverfolgungsbehörden mit Europol und Interpol zum Zweck der Durchführung operativer länderübergreifender Ermittlungen.

Die Tatmotive der Cyberkriminellen sind sehr unterschiedlich. Sie umfassen wirtschaftliche, destruktive, politisch-ideologische, religiös-ideologische und nachrichtendienstliche Ziele. Zur Verwirklichung dieser Ziele verwenden organisierte und arbeitsteilig agierende Gruppen von Kriminellen modernste Technik, wobei sie ihre Fähigkeiten und Leistungen auch anderen interessierten Kreisen im Rahmen von Auftragsarbeiten anbieten („Cybercrime as a Service"). Zum einen versuchen Cyberkriminelle, ua durch Ausspionieren und Verwendung von Identifikations- und Authentisierungsdaten auf fremden Computersystemen, durch Verwertung von ausspionierten Geschäfts- und Betriebsgeheimnissen oder durch digitale Erpressung einen monetären Gewinn zu erzielen. Zum anderen richten sich Cyberattacken gezielt gegen die Funktionsfähigkeit von Computersystemen, ohne dass die Täter mit Spionage- und Bereicherungsabsicht handeln. Sog. Hackivisten versuchen etwa durch gezieltes Lahmlegen von Internetseiten oder Internet-Services bestimmter Behörden oder Unternehmen im Rahmen sog. Distributed Denial-of-Service (DDos)-Attacken[2] ihren ideologischen Vorstellungen Ausdruck zu verleihen und Einfluss auf politische Entscheidungen zu nehmen. Darüber hinaus wird das Internet auch zunehmend für gezielte und systematische Angriffe gegen die Persönlichkeit und Privatsphäre von Personen benutzt. Hierunter fallen Phänomene wie das seit 01.01.2016[3] durch einen eigenen Straftatbestand (§ 107c StGB) erfasste Cybermobbing[4], das Cyberstalking[5] und das Happy Slapping[6].

---

[1] *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112.

[2] DoS-Attacken richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff. Die Lage der IT-Sicherheit in Deutschland 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), 19.11.2015, 30, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht 2015.pdf?__blob= publicationFile&v=2 (25.01.2016); *Ziegler*, Web Hacking: Sicherheitslücken in Webanwendungen – Lösungswege für Entwickler, Carl Hanser Verlag München 2014, 103; Bundeslagebericht Cybercrime 2014 des deutschen Bundeskriminalamts, 4, http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html (25.01.2016).

[3] Strafrechtsänderungsgesetz 2015 vom 13.08.2015, BGBl I 112/2015.

[4] Unter dem Begriff „Cybermobbing" versteht man die gezielte, wiederholte und damit anhaltende Bloßstellung, Belästigung oder Ausgrenzung eines Einzelnen durch mehrere andere Personen mittels Nutzung von Informations- und Kommunikationstechnologie, welche die Lebensgestaltung des Opfers beeinträchtigt. *Katzer*, Cybermobbing. Wenn das Internet zur W@ffe wird, Springer Verlag Berlin Heidelberg 2014; *Voskamp/Kipker*, Virtueller Pranger Internet, DuD 788.

[5] „Cyberstalking" bezeichnet ein Tatverhalten, bei dem das „klassische" Stalking auf den Bereich des Internets übertragen wird, um eine Person zu denunzieren, psychisch unter Druck zu setzen und ihr damit nachhaltig privat , sozial und beruflich zu schaden. Tatmittel ist das Internet; die Kontaktaufnahme zum Opfer erfolgt unter Nutzung Internet-basierter Kommunikationsmittel wie zB durch Versenden von E-Mails oder Verwenden von Instant Messengers. *Gapski/Schneider/Teksters*, Internet-Devianz, Strukturierung des Themenfeldes „Abweichendes Verhalten" im Kontext der Internetnutzung, Landesanstalt für Medien Nordrhein-Westfalen (Hrsg.), Düsseldorf 2009, 29, http://www.sainetz.at/dokumente/Internet_Devianz_2009.pdf (25.01.2016); *Wach* in *Triffterer/Rosbaud/Hinterhofer* Sbg-Kommentar StGB § 107a Rz 32 mwN; *Schwaighofer* in *Höfpel/Ratz* WK^2 StGB § 107a Rz 20.

[6] Unter „Happy Slapping" sind körperliche Attacken auf Opfer an privaten oder öffentlichen Orten zu verstehen, welche gefilmt werden. Die Filme werden anschließend über Smartphones oder das Internet, zB auf YouTube, weiterverbreitet. *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112 (116); *Rauch*, „Happy Slapping" und Paparazzi – Die strafrechtliche Erfassung zweier ungleicher Phänomene, Jahrbuch Strafrecht BT 2010, 89; *Katzer*, Cybermobbing. Wenn das Internet zur W@affe wird, Springer Verlag Berlin Heidelberg 2014, 63.

Zur Verfolgung ihrer Ziele bedienen sich Cyber-Kriminelle vielfältiger Angriffsmethoden, die sich am technischen Fortschritt und an den bestehenden Abwehrmaßnahmen orientieren: Botnetze[7] werden im großen Stil für Angriffe auf die Verfügbarkeit von Computersystemen (DDos-Attacken), den Versand von Spam und die Suche nach personenbezogenen Daten von Opfern, insbesondere nach Zugangsdaten zu E-Mail-, Social Media- und Finanz-Accounts, genutzt. Beliebte Mittel zur Ausführung oder Unterstützung von Cyber-Angriffen sind auch das Social Engineering[8] und die Installation von Schadprogrammen (sog. Malware).

2. Aktueller Forschungsstand

In einer sehr technisch ausgerichteten Dissertation aus dem Jahr 2005 befasst sich *Bergauer*[9] mit den technischen Grundlagen und den strafrechtlichen sowie verwaltungsstrafrechtlichen Aspekten der Malware, eines kleinen Teilbereiches des in der gegenständlichen Dissertation zu behandelnden Untersuchungsgegenstands.[10] Eine an der Universität Konstanz 2012 erschienene Dissertation[11] untersucht die deutschen Straftatbestände § 202a dStGB (Ausspähen von Daten), § 202b dStGB (Abfangen von Daten), § 202c dStGB (Vorbereiten des Ausspähens und Abfangens von Daten), § 303a dStGB (Datenveränderung) und § 303b dStGB (Computersabotage) - somit die Computerstrafdelikte im engeren Sinn - und vergleicht diese mit den korrespondierenden österreichischen und schweizerischen Straftatbeständen. Gleiches gilt für eine rechtsvergleichende Arbeit aus der Schweiz[12] mit dem Schwerpunktthema „Hacking". Während letztere das österreichische Recht nur punktuell berücksichtigt, behandelt die deutsche Dissertation das österreichische Computertstrafrecht zwar eingehender, jedoch anhand einer tatbestandsbezogenen Rechtsvergleichung. Eine fallbasierte Strafrechtsvergleichung mittels konkreter Sachverhalte bzw. Angriffsmethoden ist nicht Gegenstand der genannten Arbeiten. Zudem konnten in beiden Publikationen aufgrund des Erscheinungsdatums die Neuerungen durch das StRÄG 2015 noch nicht berücksichtigt werden.

Die strafrechtliche Beurteilung des „Phishing" nach österreichischem Recht wurde von *Bergauer*[13] in einem wissenschaftlichen Artikel untersucht. In seinen Überlegungen behandelt der Autor nur das klassische „Phishing". Diese Methode ist dadurch charakterisiert, dass dem Opfer eine gefälschte E-Mail zugesendet wird, welche zur Eingabe vertraulicher Daten in ein innerhalb der E-Mail eingebundenes Formular auffordert und diese dann dem Absender der E-Mail übermittelt. Neben dieser Angriffsmethode gibt es mittlerweile fortgeschrittenere „Phishing"-Techniken und Sonderformen des „Phishing".[14] Diese Weiterentwicklungen des klassischen „Phishing" sowie andere Formen des Identi-

[7] Als Botnetz wird ein Verbund von Systemen bezeichnet, die mit Schadsoftware infiziert sind und ohne Wissen ihrer Besitzer über sog. Command&Control-Server ferngesteuert werden. ENISA, Botnets: Detection, Measurement, Disinfection & Defence, 07.03.2011, 24, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence (25.01.2016); Bundeslagebericht Cybercrime 2014 des deutschen Bundeskriminalamts, 8f, http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html (25.01.2016); Die Lage der IT-Sicherheit in Deutschland 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), 19.11.2015, 30, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob= publicationFile&v=2 (25.01.2016).

[8] Im Rahmen von Social Engineering-Angriffen werden gezielt menschliche Schwächen (zB Gutgläubigkeit, Unsicherheit) ausgenutzt, um sich Zugang zu einem Zielsystem zu verschaffen. *Ziegler*, Web Hacking: Sicherheitslücken in Webanwendungen – Lösungswege für Entwickler, Carl Hanser Verlag München 2014, 125ff.

[9] *Bergauer*, Malware aus strafrechtlicher und verwaltungsstrafrechtlicher Sicht, Diss. Universität Graz 2005.

[10] Siehe dazu das nachfolgende Kapitel Zielsetzung und zentrale Fragestellungen.

[11] *Schuh*, Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, Berlin 2012.

[12] *Pfister*, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, *Dannecker/Höpfel/Schwarzenegger* (Hrsg), NWV Wien 2008.

[13] *Bergauer*, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82.

[14] Beim „Pharming" greift der Angreifer in die Kommunikation zwischen dem PC des Opfers und dem DNS (Domain Name System)-Server ein, welcher für die Übersetzung von Domain-Namen in IP-Adressen zuständig ist (sog. DNS Spoofing). Die Verbindung, die das Opfer aufbauen wollte, wird so auf eine vom Angreifer gewählte Website umgeleitet. Bei der Man-in-the-middle-Attacke schaltet sich der Angreifer mit Hilfe von Malware in den Kommunikationsweg zwischen Opfer und zB einer Bank und fängt Daten direkt auf dem Übertragungsweg ab. Beim „Vishing" wird die Phishing-Attacke unter Zuhilfenahme von Voice over Internet Protocol (VoIP)-Telefonie ausgeführt. Beim „SMishing" wird per SMS zB eine Abobestätigung an das Opfer versendet und eine Internet-Adresse zur Abmeldung von diesem Service genannt. Bei Besuch dieser Website wird dann zB ein Trojaner eingeschleust. *Gercke*, Legal Approaches to Criminalize Identity Theft, in: UNODC, Handbook on

tätsdiebstahls wurden bislang in der österreichischen strafrechtlichen Literatur noch nicht eingehend analysiert. In der deutschen Literatur hat sich insbesondere *Brandt*[15] mit der Strafbarkeit des klassischen „Phishing" nach deutschem Recht befasst. Für das Versenden der Phishing-Mail kommt nach Ansicht der Autorin eine Strafbarkeit nach § 269 dStGB (Fälschung beweiserheblicher Daten) nicht in Betracht, weil es an einer dauerhaften Verkörperung der Webseite fehlt, da diese nur für kurze Zeit online gestellt und gespeichert wird. Auch *Graf*[16] problematisiert in einem kurzen wissenschaftlichen Beitrag die Anwendbarkeit des § 269 dStGB auf den Fall des klassischen „Phishing". *Graf* geht davon aus, dass das für die Verwirklichung von § 269 dStGB relevante Tatbestandsmerkmal der Ausstellererkennbarkeit nur dann erfüllt sei, wenn bundesweit agierende Großbanken als Absender der Phishing-Mail gewählt werden, bei denen sich ein etwaiger Auszahlungsanspruch des Kunden direkt gegen die Bank als solche richten würde. Den strafrechtlichen Aspekten des „Pharming"[17] widmet sich *Popp*[18] in einem kurzen wissenschaftlichen Beitrag. Er verneint eine Strafbarkeit nach § 269 dStGB wegen fehlender Beeinträchtigung der Garantiefunktion, da im Fall des „Pharming" lediglich der für die Authentizität unverbindliche Domänenname und nicht – sofern nicht zusätzlich IP-Spoofing[19] vorliegt – die angebene IP-Adresse gefälscht ist. Die strafrechtliche und zivilrechtliche Qualifikation von DoS-Attacken[20] nach österreichischem Recht ist Gegenstand eines wissenschaftlichen Artikels von *Öhlböck/Esztegar*[21], die in diesem Beitrag ihre Rechtsansicht darlegen, dass der Begriff der „schweren Störung" iSd § 126b öStGB anhand eines beweglichen Systems mehrerer Kriterien zu beurteilen sei.

In einem vor Beschluss des StRÄG 2015 publizierten Artikel setzt sich *Salimi*[22], aufbauend auf dem Ministerialentwurf zum StRÄG 2015[23], mit dem geplanten Tatbestand des § 120a öStGB auseinander. *Reisinger*[24] gibt in dem bislang einzigen nach Beschluss des StRÄG 2015 zum Thema „Cybermobbing" erschienenen rechtswissenschaftlichen Artikel einen kritischen Überblick über den aufgrund von Vorschlägen im Begutachtungsverfahren letztlich abgeänderten und den Delikten gegen die Freiheit zugeordneten Tatbestand des § 107c öStGB. In einem kurzen Übersichtsartikel stellt *Bernreiter*[25] unter Bezugnahme auf die Gesetzesmaterialien und die bisher erschienene Literatur, jedoch im Wesentlichen ohne eigene kritische Würdigung die wichtigsten Neuerungen durch das StRÄG 2015 im Bereich des Computerstrafrechts vor. Sämtliche Kommentare[26] zu den einschlägigen Computerstraftatbeständen des öStGB sind zum Zeitpunkt des Schreibens noch auf dem Stand der vor Inkrafttreten des StRÄG 2015 geltenden Rechtslage. Unter den Lehrbüchern behandeln zwar Neuauflagen von *Fuchs/Reindl-Krauskopf*[27], *Birklbauer/Hilf/Tipold*[28] und *Bertel/Schwaighofer*[29] bereits die Änderungen durch das StRÄG 2015 im österreichischen Computerstrafrecht, jedoch im Wesentlichen unter Wiedergabe der Gesetzesmaterialien und ohne eigene kritische Stellungnahmen.

Identity-related Crime, April 2011, 17, https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf (25.01.2016); Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), University of Ottawa, Faculty of Law 2007, 15, https://cippic.ca/sites/default/files/bulletins/Techniques.pdf (25.01.2016); OECD Scoping Paper on Online Identity Theft, Seoul, June 2008, 19f, http://www.oecd.org/sti/40644196.pdf (25.01.2016).

[15] *Brandt*, Zur Strafbarkeit des Phishing. Gesetzgebung vs. Technologie, Verlag Dr. Kovac, Hamburg 2010.

[16] *Graf*, „Phishing" derzeit generell nicht strafbar!, NStZ 2007, 129.

[17] Siehe dazu Fn 14.

[18] *Popp*, „Phishing", „Pharming" und das Strafrecht, MMR 2006, 84.

[19] Beim IP-Spoofing wird die IP-Adresse eines beteiligten Rechners gefälscht.

[20] Siehe FN 2.

[21] *Öhlböck/Esztegar*, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126.

[22] *Salimi*, Cybermobbing – Auf dem Weg zu einem neuen Straftatbestand, JSt 2015, 191.

[23] ME StRÄG 2015, 98/ME 25. GP.

[24] *Reisinger*, „Cybermobbing" – Eine Analyse von § 107c StGB, jusIT 2015, 169.

[25] *Bernreiter*, Zum „StRÄG 2015" und den Änderungen im Bereich des Computerstrafrechts, jusIT 2015, 128.

[26] Salzburger Kommentar zum Strafgesetzbuch: Kommentar, 32. Auflage, herausgegeben von *Triffterer, Rosbaud, Hinterhofer*, Wien 2015; *Höpfel/Ratz* (Hrsg.), Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, Wien 1999ff.

[27] *Fuchs/Reindl-Krauskopf*, Österreichisches Strafrecht, Besonderer Teil I (Delikte gegen den Einzelnen), 5. Aufl. 2015.

[28] *Birklbauer/Hilf/Tipold*, Strafrecht Besonderer Teil I, 3. Aufl. 2015.

[29] *Bertel/Schwaighofer*, Strafrecht, Besonderer Teil I, 13. Aufl. 2015.

Abgesehen von den erwähnten rechtsvergleichenden Arbeiten zum Hacking bzw. Computerstrafrecht im engeren Sinn[30] und der Arbeit über die Strafbarkeit des „Phishing" nach deutschem Recht[31] wurden aktuelle Cyber-Phänomene großteils nur punktuell in wissenschaftlichen Beiträgen abgehandelt.[32] Eine systematische zusammenfassende und überdies rechtsvergleichende Darstellung der strafrechtlichen Erfassung aktueller Cyber-Phänomene unter Einbezug der Neuerungen im österreichischen Computerstrafrecht durch das StRÄG 2015 findet sich bislang nicht in der österreichischen Literatur.

3. Zielsetzung

Die aufgezeigten Forschungslücken lassen sich in folgende Themenfelder einteilen:

Hinsichtlich der Computerstraftatbestände im engeren Sinn erfolgte bislang eine bloß theoretische Rechtsvergleichung auf Basis einer Gegenüberstellung korrespondierender Straftatbestände. Ziel der Dissertation ist es, die Praxistauglichkeit anhand einer fallbasierten Strafrechtsvergleichung mittels konkreter Sachverhalte bzw. Angriffsmethoden zu prüfen, wobei der Schwerpunkt der Arbeit nicht auf dem deutschen bzw. schweizerischen, sondern auf dem österreichischen Recht unter Berücksichtigung der Neuerungen durch das StRÄG 2015 liegt.

Bestimmte Phänomene wie das klassische „Phishing" und Dos-Attacken wurden zwar punktuell in einzelnen wissenschaftlichen Beiträgen[33] – das klassische „Phishing" zudem in einer deutschen Hochschulschrift[34] – behandelt, aber noch nicht einer rechtsvergleichenden Analyse unterzogen. In diesem Zusammenhang werden für die gegenständliche Dissertation zum einen eine Gegenüberstellung der §§ 269 dStGB und 225a öStGB, welcher für das Versenden von Phishing-Mails nach österreichischem Recht als einschlägig erachtet wird[35], zum anderen eine Analyse der durch das StRÄG 2015 neu eingeführten Bestimmung des § 241h öStGB (Ausspähen von Daten eines unbaren Zahlungsmittels) von besonderem Interesse sein.

Die neueren Formen des „Phishing" sowie weitere Angriffsformen des Identitätsdiebstahls waren bislang noch nicht Gegenstand einer (deutschen oder österreichischen) juristischen Dissertation. Auch zu den Computerstrafdelikten gegen die Persönlichkeit und Privatsphäre existiert bislang weder in der deutschen noch in der österreichischen Literatur eine umfassende strafrechtswissenschaftliche Untersuchung. Ebenso fehlt eine diesbezügliche rechtsvergleichende Arbeit.

Um die im Forschungsstand dargestellten Lücken zu schließen, konzentriert sich die Untersuchung auf Phänomene folgender Kategorien

- Digitale Erpressung[36]

---

[30] *Pfister*, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, *Dannecker/Höpfel/Schwarzenegger* (Hrsg), NWV Wien 2008; *Schuh*, Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, Berlin 2012.

[31] *Brandt*, Zur Strafbarkeit des Phishing. Gesetzgebung vs. Technologie, Verlag Dr. Kovac, Hamburg 2010.

[32] Insb *Bergauer*, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82; *Graf*, „Phishing" derzeit generell nicht strafbar!, NStZ 2007, 129; *Öhlböck/Esztegar*, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126; *Popp*, „Phishing", „Pharming" und das Strafrecht, MMR 2006, 84; *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112; *Reisinger*, „Cybermobbing" – Eine Analyse von § 107c StGB, jusIT 2015, 169; *Salimi*, Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012/115, 998; *Salimi*, Cybermobbing – Auf dem Weg zu einem neuen Straftatbestand, JSt 2015, 191.

[33] Insbes *Bergauer*, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82; *Graf*, „Phishing" derzeit generell nicht strafbar!, NStZ 2007, 129; *Öhlböck/Esztegar*, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126.

[34] *Brandt*, Zur Strafbarkeit des Phishing. Gesetzgebung vs. Technologie, Verlag Dr. Kovac, Hamburg 2010.

[35] *Bergauer*, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 89 (82).

[36] Die Installation einer spezifischen Schadsoftware („Ransomware") bewirkt, dass der berechtigte Nutzer eines IT-Systems dieses ganz oder teilweise nicht mehr nutzen kann und/oder auf die darauf gespeicherten Daten nicht mehr zugreifen kann. Für die vermeintliche Freigabe des IT-Systems oder der Daten wird ein Lösegeld gefordert. *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112f; Bundeslagebericht Cybercrime 2014 des deutschen Bundeskriminalamts, 10, http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime __node.html (25.01.2016).

- Bedrohung durch Botnetze[37]: Distributed Denial-of-Service (DDos)-Attacken[38]
- Identitätsdiebstahl[39] (klassisches Phishing[40] und Varianten des Phishing, Identitätsdiebstahl durch Installation von Schadprogrammen wie Trojanischen Pferden, durch Einsatz von Keyloggern[41] oder Spyware[42] sowie durch Einbruch auf Servern und Kopieren der Anmeldeinformationen)
- Angriffe gegen die Persönlichkeit und Privatsphäre (Cybermobbing, Happy Slapping, Cyberstalking[43])

Es handelt sich hierbei einerseits um die laut aktuellen Sicherheitsberichten[44]verbreitetsten Cyber-Angriffsformen in Österreich[45] (und weltweit[46]), andererseits – wie bei den Verletzungen der Persönlichkeit und Privatsphäre – um „neuere" cyberkriminelle Erscheinungsformen, welche sich entsprechend facheinschlägiger Literatur[47] erst in den letzten Jahren aufgrund zunehmender Vernetzung via Social Media und Internetforen zu einem massiven Problem entwickelt haben.

---

[37] Siehe FN 7.

[38] DDoS-Angriffe sind Angriffe auf die Verfügbarkeit von Internetdiensten und Webseiten und erfolgen in der Regel unter Einsatz von zu einem Botnetz zusammengeschlossenen Computern, siehe FN 2.

[39] Der Begriff „Identitätsdiebstahl" wird für Szenarien verwendet, in denen sich Täter unbefugt Zugang zu Identifikations- und Authentisierungsdaten verschaffen und diese für kriminelle Zwecke verwenden. Die Lage der IT-Sicherheit in Deutschland 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), 19.11.2015, 34, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob= publicationFile&v=2 (25.01.2016); Europäische Kommission, Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, 11.12.2012, 11, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies /organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf (25.01.2016); EU Fraud Prevention Expert Group (FPEG), Report on Identity Theft/Fraud, 22.10.2007, 7, http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf (25.01.2016); *Gercke*, Legal Approaches to Criminalize Identity Theft, in: UNODC, Handbook on Identity-related Crime, April 2011, 25ff, https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf (25.01.2016); Bundeslagebericht Cybercrime 2014 des deutschen Bundeskriminalamts, 6f, http://www.bka.de/ DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime __node.html (25.01.2016); OECD Policy Guidance on Online Identity Theft, Seoul, June 2008, 2f, http://www.oecd.org/sti/consumer/40879136.pdf (25.01.2016).

[40] Unter „Phishing" versteht man Vorgehensweisen, bei denen die Täter versuchen, über gefälschte Webseiten, E-Mails oder Kurznachrichten an Zugangsdaten von Internetnutzern zu gelangen, um damit Identitätsdiebstahl zu begehen. Siehe auch FN 14. Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), University of Ottawa, Faculty of Law 2007, 13ff, https://cippic.ca/sites/default/files/bulletins/Techniques.pdf (25.01.2016); *Gercke*, Legal Approaches to Criminalize Identity Theft, in: UNODC, Handbook on Identity-related Crime, April 2011, 17, https://www.unodc.org/documents/treaties/UNCAC /Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf (25.01.2016); OECD Policy Guidance on Online Identity Theft, Seoul, June 2008, 3, http://www.oecd.org/sti/consumer/40879136.pdf (25.01.2016).

[41] Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet.

[42] Als Spyware werden Programme bezeichnet, die heimlich Informationen über die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten.

[43] Siehe FN 4-6.

[44] Vgl Die Lage der IT-Sicherheit in Deutschland 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), 19.11.2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf? __blob=publicationFile&v=2 (25.01.2016); Annual Incident Reports 2014, Europäische Agentur für Netz- und Informationssicherheit (ENISA) (Hrsg.), 14.09.2015, https://www.onlinesicherheit.gv.at/services/publikationen/sicherheitsberichte/ 183166.html?2 (25.01.2016); Cybercrime Report 2014, Bundeskriminalamt (BK) (Hrsg.), 04.09.2015, http://www.bmi.gv.at/cms/BK/publikationen/files/Web_Cybercrime_2014.pdf (25.01.2016).

[45] Vgl Cybercrime-Reporte des österreichischen Bundeskriminalamts 2014, 2013, 2012, http://www.bmi.gv.at/cms/BK/publikationen/files/Web_Cybercrime_2014.pdf, http://www.bmi.gv.at/cms/bk/publikationen/files/cybercrime_report_2013.pdf, http://www.bmi.gv.at/cms/BK/publikationen/files/Cybercrime_Report2012_Web.pdf (25.01.2016).

[46] Vgl ua UNODC, Handbook on Identity-related Crime, April 2011, 17, https://www.unodc.org/documents/treaties /UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf (25.01.2016); Die Lage der IT-Sicherheit in Deutschland 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), 19.11.2015, 34, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht 2015.pdf?__blob= publicationFile&v=2 (25.01.2016); Bundeslagebericht Cybercrime 2014 des deutschen Bundeskriminalamts, 8f, http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html (25.01.2016).

[47] Insb *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112.

Die gegenständliche Dissertation wird zunächst aufzeigen, welche Angriffsmethoden und –mittel diesen aktuellen Phänomenen der Cyberkriminalität zugrunde liegen. Dies ist deshalb notwendig, weil die Beurteilung, welche Straftatbestände für die rechtliche Subsumtion in Betracht kommen, stark von der konkreten Vorgehensweise der Cyberkriminellen abhängt. Der Schwerpunkt der Arbeit liegt in der kritischen Auseinandersetzung mit den für die strafrechtliche Subsumtion der Cyber-Phänomene einschlägigen Bestimmungen des öStGB und dStGB einschließlich ausgewählter Nebengesetze (insb des österreichischen Datenschutzgesetzes [öDSG] und des deutschen Bundesdatenschutzgesetzes [dBDSG]). Im Rahmen der rechtsvergleichenden Analyse soll geklärt werden, wo sich Unterschiede in der strafrechtlichen Erfassung der entsprechenden Cyber-Phänomene nach deutschem Recht im Vergleich zum österreichischen Recht ergeben. Anhand einer kritischen Betrachtung der einschlägigen Straftatbestände werden Vor- und Nachteile der unterschiedlichen strafrechtlichen Erfassung der Phänomene im deutschen und österreichischen Recht herausgearbeitet. Ausgehend vom *status quo* der österreichischen bzw. deutschen Rechtsordnung wird der Frage nachgegangen, ob und wo nach geltender Rechtslage Strafrechtslücken festzustellen sind. Zudem werden die einschlägigen Strafbestimmungen auch im Hinblick auf eine eventuell bestehende überschießende Ausgestaltung[48] geprüft, welche zu möglichen Problemen in der Anwendungspraxis und einem daraus resultierenden unzureichenden strafrechtlichen Schutz führt. In einer abschließenden Diskussion widmet sich die Arbeit Vorschlägen zur systemkonformen Lückenschließung und Stärkung des strafrechtlichen Schutzes gegen Cyber-Angriffe.

Da sich zwei rechtsvergleichende Dissertationen[49] bereits mit der Erscheinungsform des Hackings auseinandergesetzt haben, wird dieses Phänomen nicht Gegenstand einer eigenen Untersuchungskategorie sein, sondern lediglich als eine der möglichen Angriffsmethoden im Rahmen der Erörterung der anderen Cyber-Phänomene behandelt. Von Cyberkriminellen mit schädlichen sexuellen Neigungen begangene Straftaten werden nicht in die strafrechtliche Analyse einbezogen. Eine Untersuchung dieser Phänomene ist, soweit ersichtlich, ua Gegenstand einer in Arbeit befindlichen Dissertation.[50] Zudem würde aufgrund der Vielzahl der damit verbundenen Problemfelder eine umfassende Behandlung im Rahmen dieser Arbeit nicht möglich sein.

4. Methode und vorläufige Grobgliederung

Die Untersuchung der einschlägigen Strafbestimmungen erfolgt unter Verwendung klassischer juristischer Interpretationsmethoden. Neben den Tatbeständen des Kernstrafrechts werden auch die Strafnormen des öDSG bzw. des dBDSG einschließlich der Gesetzesmaterialien näher untersucht. Die Relevanz des in Ausarbeitung befindlichen österreichischen Cyber-Sicherheitsgesetzes[51] kann noch nicht beurteilt werden, ist aber jedenfalls zu berücksichtigen. Zudem umfasst die Analyse auch internationale und europäische Rechtsakte samt der dazugehörigen Dokumente der zuständigen Institutionen sowie einschlägige Literatur und Rechtsprechung. Als Literaturquellen dienen Lehrbücher, fachliche Monografien, Kommentare, Datenbanken sowie Beiträge und Aufsätze in Zeitschriften. Anhand der Analyse der einzelnen Strafbestimmungen mittels gängiger juristischer Interpretationsmethoden sowie einer fallbasierten Strafrechtsvergleichung wird aufgezeigt, wo sich Strafrechtslücken im österreichischen bzw. deutschen Recht ergeben und welche Bestimmungen möglicherweise überschießend ausgestaltet sind. Etwaige Anwendungsschwierigkeiten einzelner Computerstraftatbestände in der Praxis sollen in erster Linie anhand einer rechtsdogmatischen und rechtsvergleichenden Untersuchung geprüft werden. Darüber hinaus werden aber auch Auswertungen der im Bereich

[48] Ein Beispiel für eine derartige überschießende Ausgestaltung ist § 118a StGB BGBl I 60/1974 idF BGBl I 109/2007. § 118a StGB war vor Inkrafttreten des StRÄG 2015 (BGBl I 112/2015) aufgrund der hohen subjektiven Schranken dieser Bestimmung in der Praxis kaum anwendbar.

[49] *Schuh*, Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, Berlin 2012; *Pfister*, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, *Dannecker/Höpfel/Schwarzenegger* (Hrsg), NWV Wien 2008.

[50] Vgl *Steinhardt,* Expose zu Pornographische Darstellungen Minderjähriger – Eine dogmatische und empirische Untersuchung zur Problematik „Kinderpornographie“ - § 207a StGB, Wien 2011.

[51] Vgl Pressemitteilung des Bundesministeriums für Inneres, Artikel-Nr. 12230, 09.04.2015, http://www.bmi.gv.at/cms/bmi_presse/_news/bmi.aspx?id=6B6C5A6A674C61434172733D&page=0&view=1 (14.03.2016).

des Computerstrafrechts aufgrund einer hohen Dunkelziffer nur eingeschränkt aussagekräftigen gerichtlichen und polizeilichen Kriminalstatistiken für Österreich und die Bundesrepublik Deutschland[52] herangezogen. Auch Interviews mit Experten aus der Praxis sind vorgesehen.[53]

Für die Rechtsvergleichung mit dem deutschen Recht wird die Auslegungsmethode der funktionalen Rechtsvergleichung angewandt. Diese erschöpft sich nicht im punktuellen Vergleich von Rechtsbegriffen oder Rechtsinstituten, sondern erfordert eine umfassende und systematische Vergleichung funktional übereinstimmender Regelungen, da ein Regelungsergebnis vielfach durch unterschiedliche Regelungsmechanismen und Anknüpfungspunkte erreicht werden kann. Ein solcher systematischer Vergleich wird durch eine fallbasierte Strafrechtsvergleichung anhand konkreter Fallgruppen und Sachverhalte ermöglicht.

Deutschland wird als Referenzrechtsordnung gewählt, weil es – wie Österreich – sowohl die Cybercrime Convention[54] als auch den EU-Rahmenbeschluss und die Richtlinie über Angriffe auf Informationssysteme[55] sowie weitere europäische Rechtsakte umgesetzt hat. Es stellt deswegen und wegen der auch sonst dem österreichischen Rechtssystem ähnlichen Entwicklung der deutschen Rechtsordnung eine geeignete Ausgangsbasis dar, um die oft im Detail liegenden Unterschiede in der nationalen Umsetzung der internationalen und europäischen Vorgaben im Bereich des Computerstrafrechts aufzuzeigen. Die Referenzrechtsordnung soll nämlich im Vergleich zum österreichischen Rechtssystem nicht derart große Unterschiede aufweisen, dass eben wegen dieser keine Aussage über eine mögliche Eignung divergenter nationaler Regelungen zur Umsetzung im österreichischen Recht getroffen werden kann.

Nach einleitenden Worten zu Forschungsgegenstand, -ziel und –methoden widmet sich die Dissertation zunächst den Grundlagen und Begriffen der Computer-, Netzwerk- und Internettechnik. Zudem wird ein Überblick über die aktuellen Entwicklungen und Bedrohungsszenarien im Bereich der Computerkriminalität gegeben. Anschließend erfolgt im Hauptteil der Dissertation die Untersuchung der einzelnen Cyber-Phänomene, wobei zunächst das jeweilige Phänomen, die möglichen Angriffsformen und die technischen Grundlagen der Angriffsmethoden erläutert werden. Im zweiten Schritt folgt die kritische Auseinandersetzung mit den für die rechtliche Beurteilung einschlägigen österreichischen Straftatbeständen. Von besonderem Interesse sind hierbei die Neuerungen durch das StRÄG 2015, welche einer eingehenden Analyse unterzogen werden. Diese schließt auch die Prüfung ein, ob und inwiefern durch die erfolgten Änderungen eine Umsetzung internationaler bzw. europarechtlicher Vorgaben erfolgte. Nach der Darstellung der zu untersuchenden österreichischen Computerstrafdelikte befasst sich die Arbeit mit den Unterschieden zur deutschen Rechtslage. Zum Schluss werden die anhand der juristischen Analyse und Rechtsvergleichung erarbeiteten Erkenntnisse zusammengefasst und unter Berücksichtigung der Untersuchungsergebnisse Änderungsvorschläge unterbreitet, um den strafrechtlichen Schutz gegen Cyber-Angriffe in der Praxis noch effektiver gestalten zu können.

---

[52] Bundesministerium für Inneres, Bundeskriminalamt (Hrsg.), Polizeiliche Kriminalstatistik, http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/start.aspx (25.01.2016); Statistik Austria (Hrsg), Gerichtliche Kriminalstatistik, http://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/kriminalitaet/index.html (25.01.2016); Bundeskriminalamt (Hrsg.), Polizeiliche Kriminalstatistik, https://www.bka.de/DE/Publikationen/Polizeiliche Kriminalstatistik/pks__node.html?__nnn=true (25.01.2016); Statistisches Bundesamt, Strafverfolgungsstatistik, Wiesbaden 2015, https://www.destatis.de/DE/Publikationen/Thematisch/Rechtspflege/StrafverfolgungVollzug/Strafverfolgung2100300137004.pdf?__blob=publicationFile (25.01.2016).

[53] Nähere Angaben zu den geplanten Experteninterviews sind im Zeitpunkt des Schreibens noch nicht möglich.

[54] Convention on Cybercrime des Europarates vom 23.11.2001 (ETS 185), http://conventions.coe.int/Treaty/EN/reports/html/185.htm (25.01.2016).

[55] Rahmenbeschluss 2005/222/JI des Rates vom 24.1.2005 über Angriffe auf Informationssysteme, ABl L 69/67 vom 16.03.2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:DE:NOT (25.01.2016); Richtlinie 2013/40/EU des Europäischen Parlamentes und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl L 218, 8-14 vom 14.08.2013, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=DE (25.01.2016).

I. Einleitung
- A. Forschungsgegenstand
- B. Forschungsziel
- C. Forschungsmethode
- D. Gang der Untersuchung

II. Technische Grundlagen und Begriffe

III. Entwicklung der Cyberkriminalität in Österreich, Deutschland und weltweit

IV. Aktuelle Phänomene des Computerstrafrechts

A. Digitale Erpressung
1. Beschreibung des Phänomens
2. Strafrechtliche Erfassung im österreichischen Recht
3. Unterschiede zum deutschen Recht

B. Bedrohung durch Botnetze: Distributed Denial-of-Service (DDos)-Attacken
1. Begriffsdefinition und technische Grundlagen
2. Strafrechtliche Beurteilung nach österreichischem Recht
3. Unterschiede zur strafrechtlichen Beurteilung nach deutscher Rechtslage

C. Identitätsdiebstahl
1. Begriffsdefinition und Formen des Identitätsdiebstahls
2. „Klassisches" Phishing und Weiterentwicklungen des Phishing
   a. Angriffsmethoden
   b. Strafrechtliche Beurteilung nach österreichischem Recht
   c. Unterschiede zum deutschen Recht
3. Identitätsdiebstahl unter Verwendung von E-Mail-Accounts und Social Media-Accounts
   a. Angriffsformen
   b. Strafrechtliche Beurteilung nach österreichischem Recht
   c. Unterschiede zum deutschen Recht

D. Verletzungen der Persönlichkeit und Privatsphäre
1. Cybermobbing
   a. Begriff und Angriffsformen
   b. Strafrechtliche Betrachtung nach österreichischem Recht
   c. Unterschiede zum deutschen Recht
2. Happy Slapping
   a. Begriffsdefinition
   b. Strafrechtliche Erfassung im österreichischen Recht
   c. Unterschiede zum deutschen Recht
3. Cyberstalking (§ 107a öStGB)
   a. Begriff
   b. Rechtliche Beurteilung nach österreichischem Recht
   c. Unterschiede zum deutschen Recht

V. Schlussfolgerungen

5. Literatur

Beck, Lehrermobbing durch Videos im Internet – ein Fall für die Staatsanwaltschaft? MMR 2008, 79

Beer, Die Convention on Cybercrime und österreichisches Strafrecht, Diss. Johannes Kepler Universität Linz, 2005

Bergauer, Gesetzgebungsmonitor Computerstrafrecht: Ratifikation des Übereinkommens über Computerkriminalität, jusIT 2012, 205

Bergauer, Viren, Würmer, Trojanische Pferde – Computerstrafrecht auf dem Prüfstand, in: 35. Ottensteiner Fortbildungsseminar aus Strafrecht und Kriminologie, BMJ (Hrsg) 2007, 27

Bergauer, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82

Bergauer, Malware aus strafrechtlicher und verwaltungsstrafrechtlicher Sicht, Diss. Universität Graz, 2005

Bergauer, Kritische Anmerkungen zu §126c StGB, ÖJZ 2007, 45

Bernreiter, Zum „StRÄG 2015" und den Änderungen im Bereich des Computerstrafrechts, jusIT 2015, 128

Bertel/Schwaighofer, Strafrecht, Besonderer Teil I, 13. Aufl. 2015.

Birklbauer/Hilf/Tipold, Strafrecht Besonderer Teil I, 3. Aufl. 2015.

Borges, Rechtsfragen des Phishing – Ein Überblick, NJW 2005, 3313

Brandt, Zur Strafbarkeit des Phishing. Gesetzgebung vs. Technologie, Verlag Dr. Kovac, Hamburg 2010

Ernst, Hacker und Computerviren im Strafrecht, NJW 2003, 3233

Fuchs/Reindl-Krauskopf, Österreichisches Strafrecht, Besonderer Teil I (Delikte gegen den Einzelnen), 5. Aufl. 2015.

Gercke, Die Strafbarkeit von Phishing und Identitätsdiebstahl. Eine Analyse der Reichweite des geltenden Strafrechts, CR 2005, 606

Graf, „Phishing" derzeit generell nicht strafbar!, NStZ 2007, 129

Gröseling/Höfinger, Computersabotage und Vorfeldkriminalisierung. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 626

Gröseling, Hacking und Computersabotage. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 549

Hoeren, Virenscanning und Spamfilter – Rechtliche Möglichkeiten im Kampf gegen Viren, Spammails & Co, NJW 2004, 3513

Höpfel/Ratz (Hrsg.), Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, Wien 1999ff

Hoyer, Die Verletzung des höchstpersönlichen Lebensbereichs bei § 201a StGB, ZIS 2006/1, 1

Jahnel, IT-Recht, 3. Auflage, Wien 2012

Jahnel, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 2004, 21

Katzer, Cybermobbing. Wenn das Internet zur W@affe wird, Springer Verlag Berlin Heidelberg 2014

Knupfer, Phishing for Money, MMR 2004, 641

Kolbe, Die Umsetzung der Cybercrime-Konvention des Europarates in Österreich in rechtsvergleichender Sicht, Diss. Universität Innsbruck 2006

Münchner Kommentar zum Strafgesetzbuch: Kommentar, 2. Auflage, *Joecks Wolfgang/Miebach Klaus* (Hrsg.), München 2003 ff

Neuhauser, Die Strafbarkeit des Bereithaltens und Weiterleitens des durch „Phishing" erlangten Geldes, NStZ 2008, 492

Öhlböck/Esztegar, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126

Pfister, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, *Dannecker/Höpfel/Schwarzenegger* (Hrsg), NWV Wien 2008

Popp, Computerstrafrecht in Europa. Zur Umsetzung der Convention on Cybercrime in Deutschland und Österreich, MR-Int 2007, 84

Popp, „Phishing", „Pharming" und das Strafrecht, MMR 2006, 84

Popp, Von „Datendieben“ und „Betrügern“ – Zur Strafbarkeit des so genannten „phishing“, NJW 2004, 3517

Rauch, „Happy Slapping“ und Paparazzi – Die strafrechtliche Erfassung zweier ungleicher Phänomene, Jahrbuch Strafrecht BT 2010

Reindl, E-Commerce und Strafrecht: zur Strafbarkeit des Missbrauchs elektronischer Dienste, Wien, 2003

Reindl-Krauskopf, Computerstrafrecht im Überblick, 2. Auflage, Wien 2009

Reindl-Krauskopf, Cyberstrafrecht im Wandel, ÖJZ 2015/19, 112

Reisinger, „Cybermobbing“ – Eine Analyse von § 107c StGB, jusIT 2015, 169;

Salimi, Zahnloses Cyberstrafrecht? Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012/115, 998

Salimi, Cybermobbing – Auf dem Weg zu einem neuen Straftatbestand, JSt 2015, 191

Salzburger Kommentar zum Strafgesetzbuch: Kommentar, 32. Auflage, herausgegeben von *Triffterer, Rosbaud, Hinterhofer*, Wien 2015

Schmölzer, Strafrecht, in: Dietmar Jahnel/Alfred Schramm/Elisabeth Staudegger (Hrsg.), Wien [u.a.], 2003

Schmölzer, Straftaten im Internet: eine materiell-rechtliche Betrachtung, ZStW 2011, 123

Schuh, Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz, Berlin, 2012

Sonntag, Die EU-Richtlinie über Angriffe auf Informationssysteme, jusIT 2014, 8

Studer, Netzwerkmanagement und Netzwerksicherheit: Ein Kompaktkurs für Praxis und Lehre, vdf Hochschulverlag Zürich 2010.

Ziegler, Web Hacking: Sicherheitslücken in Webanwendungen – Lösungswege für Entwickler, Carl Hanser Verlag München 2014.

Online-Quellen

Bundeslagebericht Cybercrime 2014 des deutschen Bundeskriminalamts, 8f, http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html

Cybercrime-Reporte des österreichischen Bundeskriminalamts 2014, 2013, 2012, http://www.bmi.gv.at/cms/BK/publikationen/files/Web_Cybercrime_2014.pdf, http://www.bmi.gv.at/cms/bk/publikationen/files/cybercrime_report_2013.pdf, http://www.bmi.gv.at/cms/BK/publikationen/files/Cybercrime_Report2012_Web.pdf

Die Lage der IT-Sicherheit in Deutschland 2015, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), 19.11.2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob= publicationFile&v=2

EU Fraud Prevention Expert Group (FPEG), Report on Identity Theft/Fraud, 22.10.2007, http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf

Europäische Kommission, Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, 11.12.2012, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_ december_2012_en.pdf

Gapski/Schneider/Tekster, Internet-Devianz, Strukturierung des Themenfeldes „Abweichendes Verhalten“ im Kontet der Internetnutzung, Landesanstalt für Medien Nordrhein-Westfalen (Hrsg.), Düsseldorf 2009, 29, http://www.sainetz.at/dokumente/Internet_Devianz_2009.pdf

OECD Policy Guidance on Online Identity Theft, Seoul, June 2008, http://www.oecd.org/sti/consumer/40879136.pdf

Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), University of Ottawa, Faculty of Law 2007, https://cippic.ca/sites/default/files/bulletins/Techniques.pdf

UNODC, Handbook on Identity-related Crime, April 2011, https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf